Платформа Радар

Руководство по работе с источниками событий информационной безопасности

Версия 4.2.4

ООО «Пангео Радар»

Оглавление

1. Общие сведения о «Платформе Радар»

Специализированное программное обеспечение «**Платформа Радар**» (далее – **СПО РАДАР**, **Платформа Радар**, платформа) является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, и предназначено для автоматизации процессов сбора, обработки и корреляции событий информационной безопасности (далее – ИБ) с целью выявления инцидентов и организации реагирования на них.

Платформа обеспечивает решение следующих задач:

- сбор информации об активах, их учет и управление записями об активах;
- сбор событий ИБ от активов и/или от установленного на активах ПО;
- автоматическая обработка поступивших событий (нормализация, обогащение);
- загрузка и анализ результатов работы сканеров уязвимостей;
- корреляция событий, создание записей об инцидентах и управление ими;
- автоматизированный контроль реагирования на инциденты, контроль устранения;
- получение, обновление и использование информации об угрозах;
- ручной анализ событий ИБ при расследовании инцидентов;
- формирование отчетов, в том числе в графическом виде (рабочие столы).

СПО РАДАР имеет сертификат соответствия ФСТЭК России № 4210 от 05 февраля 2020 г. (переоформлен 22 марта 2022 г.), срок действия: пять лет.

2. Обработка событий

2.1 Общие сведения

Обработка событий ИБ в **Платформе Радар** состоит из следующих этапов:

- **Сбор событий**.

  Этап, на котором собираются события от источника одним из методов сбора: активным или пассивным.

  За этап отвечает сервис **Pangeoradar-Logcollector** (далее лог-коллектор).

  Подробнее о работе и настройке лог-коллектора см. раздел «Лог-коллектор».

- **Разбор событий**.

  Преобразование входящего события на пары «Ключ-Значение» согласно правилам разбора.

  Подробнее о работе с правилами разбора см. раздел «Правила разбора».

- **Нормализация событий**.

  Передача полученных на этапе разбора пары «Ключ-Значение» в таксономию, согласно правилам разбора. Настройка таксономии выполняется в разделе «Поля события».

  Поля таксономии по умолчанию приведены в разделе **Источники → Поля события**».

- **Обогащение событий**.

  Наполнение нормализованных событий дополнительной информацией (например, geo ip, dns, табличные списки и т.д.) согласно правилам обогащения.

  Подробнее о работе с правилами обогащения см. раздел «Обогащение».

- **Корреляция событий**.

  Процесс обнаружения инцидентов информационной безопасности путем анализа потока нормализованных событий согласно правилам корреляции.

  Коррелятор выявляет последовательности в потоке событий, отфильтрованных с помощью фильтров потока событий и удовлетворяющих условиям, описанным в правиле корреляции.

  Результатом работы коррелятора является "сработка" правила корреляции, на основании которой может быть создан инцидент и проведен анализ.

Схема обработки и корреляции событий приведена в разделе «Схема обработки и корреляции событий».

2.2 Схема обработки и корреляции событий

Схема взаимодействия подсистем, отвечающих за сбор, обработку и корреляцию событий приведена на «Рис. 1».

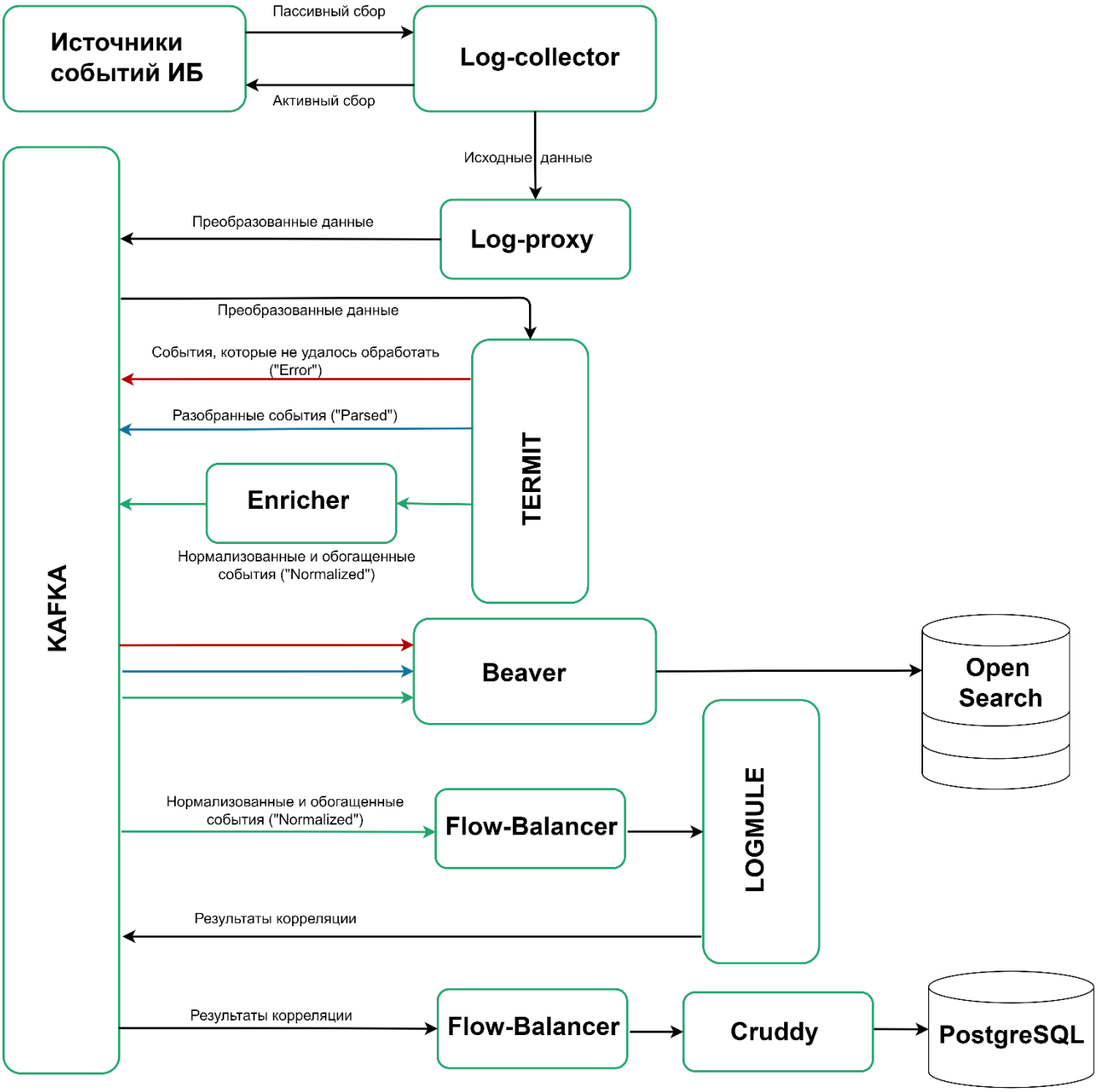


Рис. 1 – Схема обработки и корреляции событий

Принцип работы:

1. **Источники событий ИБ** – это любой актив, устройство, программное обеспечение в инфраструктуре организации, которое может создавать журналы работы.
2. **Log-Collector** (лог-коллектор) осуществляет сбор событий от источников. Сбор может выполняться двумя способами:
    - Активный сбор – лог-коллектор обращается к источнику для сбора событий;
    - Пассивный сбор – источник самостоятельно отправляет события в лог-коллектор.
3. **Log-proxy** обрабатывает полученные события и оптимизирует их для быстрой пересылки в сервис **Kafka**.
4. **Kafka** направляет полученный поток событий в обработчик **Termit**.

5. **Termit** обрабатывает события согласно правилам разбора и распределяет их по трем топикам:
    - **Error** – в ходе разбора события возникли ошибки и его не удалось разобрать;
    - **Parsed** – событие разобрано на пары **«Ключ-Значение»**;
    - **Normalized** – полученные пары **«Ключ-Значение»** подготовлены для передачи в таксономию.
6. Топики **Error**, **Parsed** и **Normalized** возвращаются в **Kafka**. При этом топик **Normalized** дополнительно проходит процедуру обогащения сервисом **Enricher**.
7. Балансировщик **Beaver** забирает все топики из сервиса **Kafka** и направляет их в базу данных **OpenSearch**. При этом **Beaver** по меткам времени раскладывает события в индексы **OpenSearch**.
8. Балансировщик **FlowBalancer** работает параллельно **Beaver** и забирает из сервиса **Kafka** только события из топика **Normalized**. Затем фильтрует их согласно фильтрам потока событий и если событие подходит под условие, то оно пересылается в коррелятор (сервис **Logmule**).
9. **Logmule** осуществляет корреляцию событий согласно правилам корреляции. Результаты корреляции возвращаются в сервис **Kafka**.
10. Балансировщик **FlowBalancer** забирает результаты корреляции и через центр управления API они отправляются в базу данных платформы.

2.3 Источники

2.3.1 Описание

Примечание: перед работой с разделом ознакомьтесь со разделом «Схема обработки и корреляции событий».

Источники событий ИБ – это любой актив, устройство, программное обеспечение в инфраструктуре организации, которое может создавать журналы работы.

В **Платформе Радар** источники делятся на типовые и нетиповые:

- **Типовые** – источники, сведения о которых настроены в платформе по умолчанию. Со списком типовых источников можно ознакомиться в разделе «Перечень поддерживаемых источников».
- **Нетиповые** – источники, сведения о которых необходимо добавить в платформу самостоятельно.

Для корректной обработки данных, поступающих от источников, каждый источник в платформе обладает уникальным **номером**. Номер источника – это **Message ID** (уникальный идентификатор сообщения), который приходит от лог-коллектора, и по которому все события от данного источника будут помещаться в один топик для дальнейшей обработки. Обычно, номер источника идентичен порту, который необходимо открыть в платформе для приема событий от источника.

Для источников можно выбрать один из двух способов преобразования данных:

- **RAW-JSON** – сервис **Log-proxy** обернет входящий поток событий в формат json и дополнит технической информацией;
- **JSON-JSON** – сервис **Log-proxy** дополнит входящий поток событий дополнительными полями с технической информацией.

Подробнее о работе сервиса Log-proxy смотрите раздел «Настройка сервиса Log-proxy».

Для каждого источника можно настроить опцию **Не сохранять сырое событие**:

- если опция включена, то сырое событие не будет сохраняться в потоке при передаче от лог-коллектора в платформу;
- если опция выключена, то каждое сырое событие будет сохранено в потоке для дальнейшей обработки.

Работа с источниками событий ИБ включает в себя следующие процессы:

1. «Включение источника».
2. «Добавление источника».
3. «Редактирование источника».
4. «Экспорт источников».
5. «Импорт источников».
6. «Удаление источников».

Для работы с источниками перейдите в раздел **Источники → Источники** (см. «Рис. 2»).

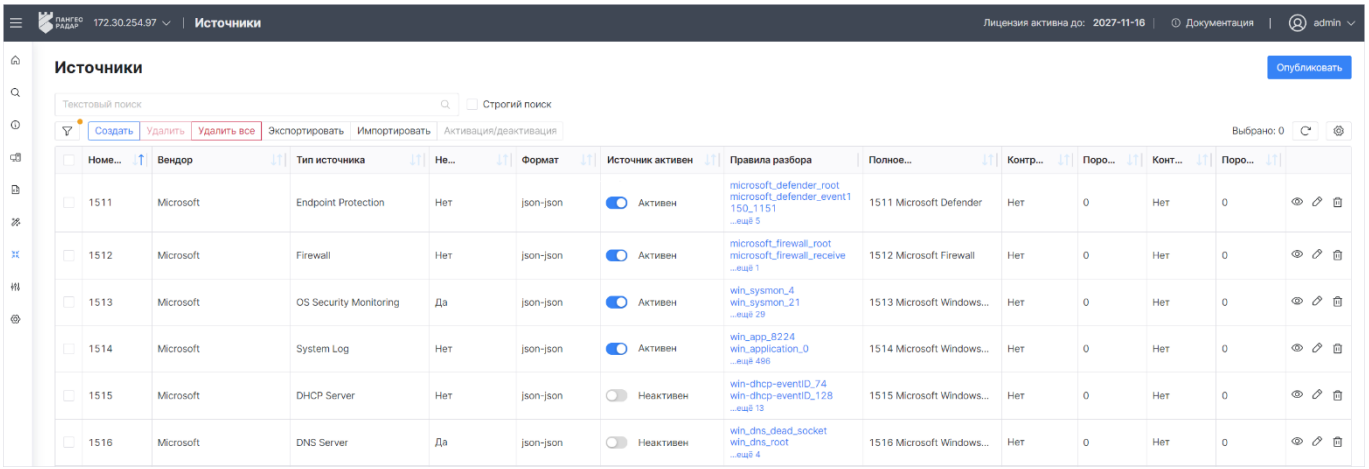


Рис. 2 – ***Раздел "Источники"***

В разделе отображается следующая информация:

- **Номер источника** – уникальный номер источника в платформе;
- **Вендор** – наименование поставщика источника;
- **Тип источника** – дополнительная классификация источников внутри платформы. Это могут быть как системы, например, операционные, антивирусные, так и сервисы, так и устройства;
- **Не сохранять сырое событие** – опция, не сохранять сырые события для дальнейшей обработки: да, нет;

- **Формат** – формат преобразования входящего потока событий;
- **Источник активен** – активен ли источник: да, нет;
- **Правила разбора** – список используемых правил разбора;
- **Полное наименование** – наименование и номер источника;
- **Контроль минимальных поступлений** – отправлять ли оповещения при достижении порога минимальных поступлений событий: да, нет;
- **Порог минимальных поступлений** – порог минимальных поступлений, при достижении которых будут отправляться уведомления;
- **Контроль максимальных поступлений** – отправлять ли оповещения при достижении порога максимальных поступлений событий: да, нет;
- **Порог максимальных поступлений** – порог максимальных поступлений, при достижении которых будут отправляться уведомления.

2.3.2 Включение источника

Для того, чтобы источник был включен, а именно поток событий от источника обрабатывался **Платформой Радар**, должны быть соблюдены следующие условия:

1. Источник настроен на отправку событий в лог-коллектор. К описанию настроек типовых источников можно перейти по соответствующим ссылкам из раздела «Перечень поддерживаемых источников».
2. В случае использования платформы в режиме мультиарендности, настроена пересылка событий (см. раздел «Включение пересылки событий через сервис Log-proxy»).
3. Источник добавлен и настроен через веб-интерфейс платформы (см. раздел «Добавление источника»).
4. Для источника настроены и опубликованы профили сбора (см. раздел «Профили сбора»).
5. Для источника настроены безусловные и условные правила разбора (см. раздел «Правила разбора»).
6. Для источника настроены правила обогащения (см. раздел «Обогащение»).
7. Параметр источника **Источник активен** установлен в состояние "*Включен*".
8. Опубликованы все изменения, внесенные в источники (нажата кнопка **Синхронизировать**).

Корректность работы правил разбора и обогащения можно проверить с помощью механизма «Отладка источников».

Для проверки наличия потока событий от источника выполните следующие действия:

1. Перейдите в раздел **Администрирование** → **Мониторинг** и откройте рабочий стол **Поток событий**.
2. Найдите топик с соответствующим номером (в примере 1514) и удостоверьтесь, что появился поток событий от источника (см. «Рис. 3» - «Рис. 5»).

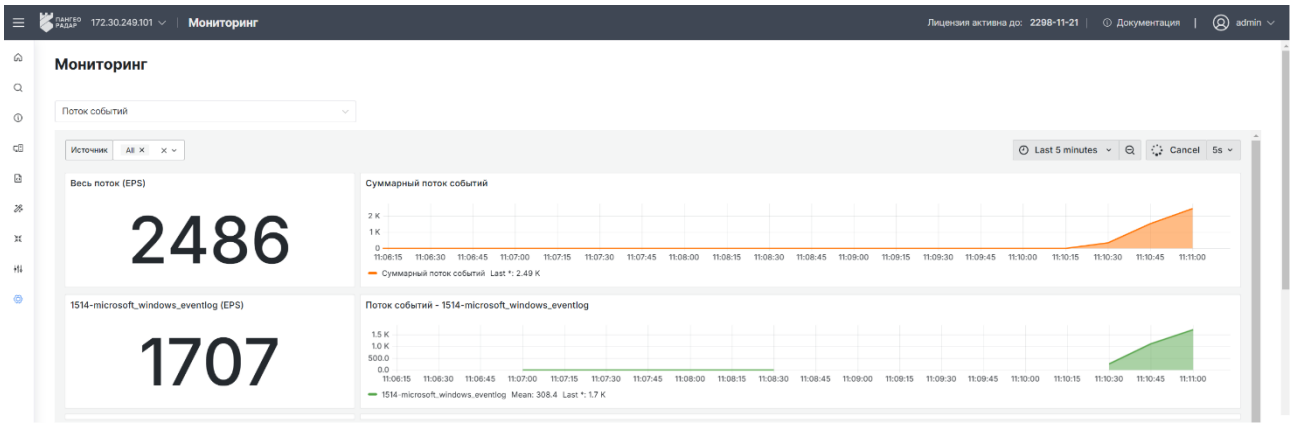


Рис. 3 – Проверка потока событий от источника. Часть 1

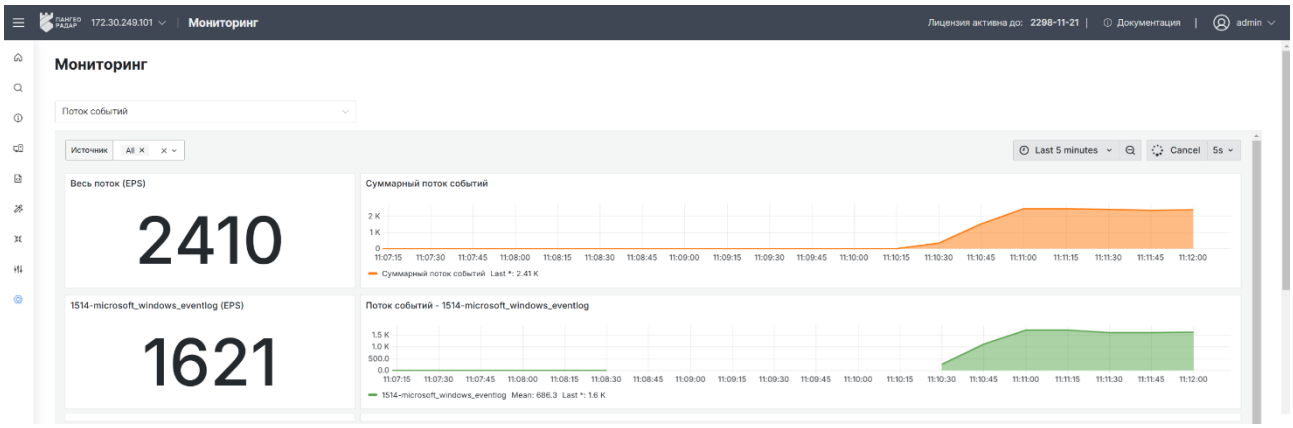


Рис. 4 – Проверка потока событий от источника. Часть 2

Рис. 5 – Проверка потока событий от источника. Часть 3

2.3.3 Добавление источника

1. Нажмите кнопку **Создать**. Откроется окно **Создание источника** (см. «Рис. 6»).

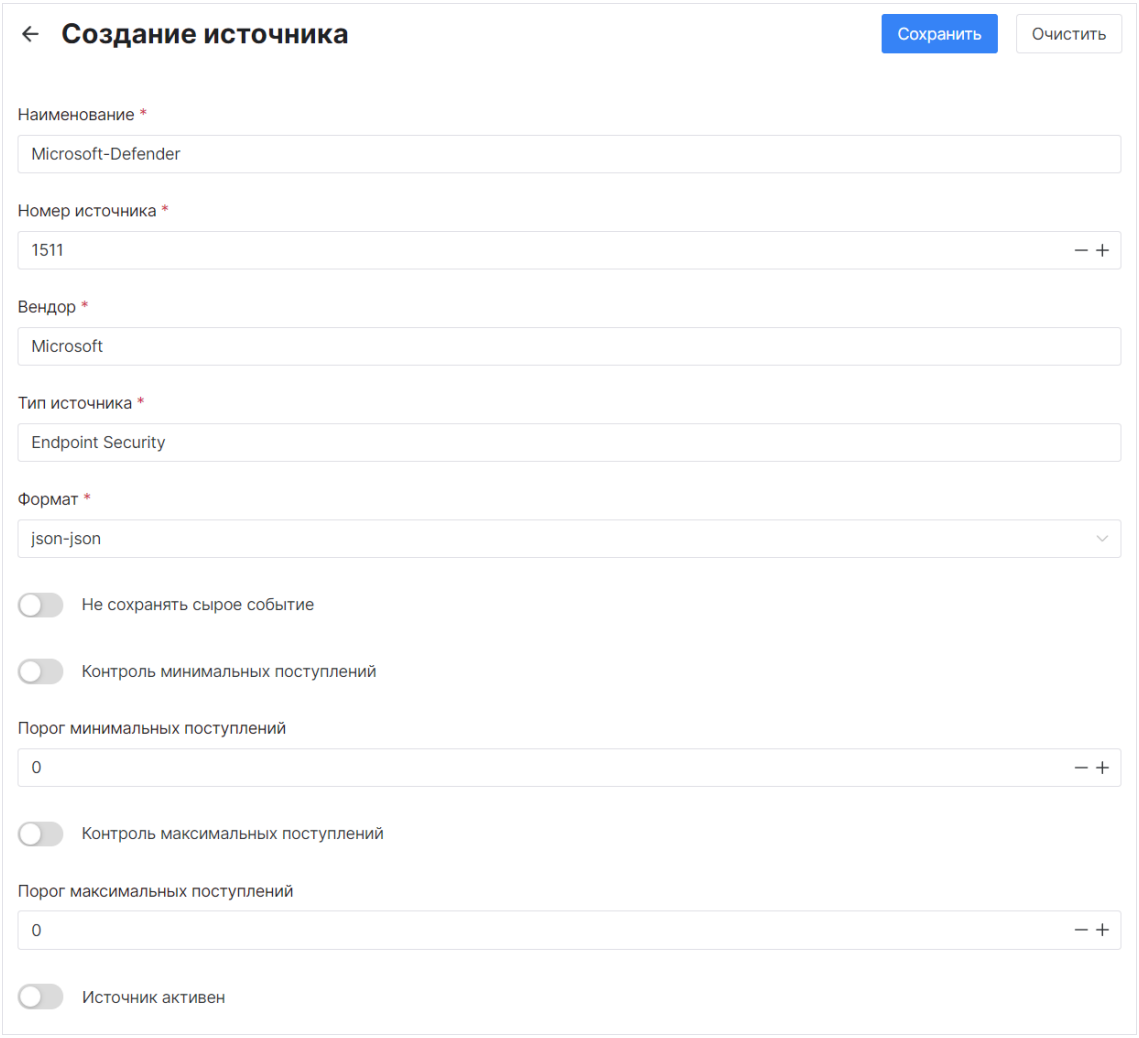


Рис. 6 – Форма "Создание источника"

2. Укажите на форме информацию об источнике:
   - **Наименование** – укажите наименование источника;
   - **Номер источника** – укажите уникальный номер источника;
   - **Вендор** – укажите поставщика источника;
   - **Тип источника** – укажите тип источника;
   - **Формат** – из выпадающего списка выберите формат преобразования потока событий: RAW-JSON или JSON-JSON;
   - **Не сохранять сырое событие** – при необходимости отключите сохранение сырых событий от данного источника;
   - Настройка оповещений о поступающем потоке событий:
     - **Контроль минимальных поступлений** – включение отправки оповещения при достижении минимального порога поступлений событий;
     - **Порог минимальных поступлений** – укажите порог минимальных поступлений, при достижении которого нужно отправлять оповещения;
     - **Контроль максимальных поступлений** – включение отправки оповещения при достижении максимального порога поступлений событий;

- **Порог максимальных поступлений** – укажите порог максимальных поступлений, при достижении которого нужно отправлять оповещения.

- **Источник активен** – включите источник.

Примечание: безусловно исполняемое правило для источника должно быть создано и настроено в разделе «Правила разбора».

3. Нажмите кнопку **Сохранить**.
4. Нажмите кнопку **Синхронизировать**.

2.3.4 Редактирование источника

1. В строке нужного источника нажмите кнопку  .
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.
4. На главной странице раздела нажмите кнопку **Синхронизировать**.

2.3.5 Экспорт источников

Для массового экспорта источников установите нужные флаги и нажмите кнопку **Экспортировать**. Будет сформирован архив с источниками в формате .zip.

Для экспорта всех источников нажмите кнопку **Экспортировать все**.

Для экспорта источников в формат CSV нажмите кнопку **Экспортировать в csv**.

2.3.6 Импорт источников

1. Нажмите кнопку **Импортировать**.
2. В открывшемся окне укажите путь к архиву с источниками.
3. Нажмите кнопку **Открыть**.
4. Чтобы все изменения вступили в силу нажмите кнопку **Синхронизировать**.

2.3.7 Удаление источников

Примечание: *для корректной работы **Платформы Радар** не рекомендуется удалять источники, установленные по умолчанию*.

Для удаления источника нажмите кнопку  в соответствующей строке.

Для массового удаления источников установите нужные флаги и нажмите кнопку **Удалить**.

Для удаление всех источников нажмите кнопку **Удалить все**.

Чтобы все изменения вступили в силу нажмите кнопку **Синхронизировать**.

2.4 Отладка источников

Платформа Радар позволяет комплексно проверить работу правил разбора и обогащения, настроенных для источника событий.

Для выполнения проверки выполните следующие действия:

1. Перейдите в раздел **Источники → Отладка источников** (см. «Рис. 7»).

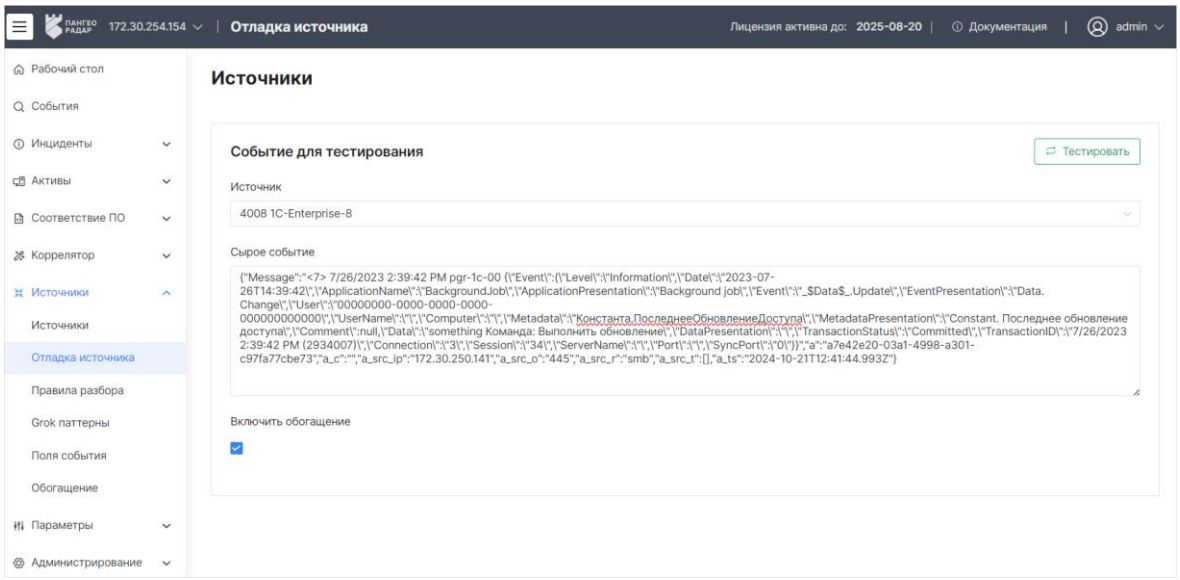
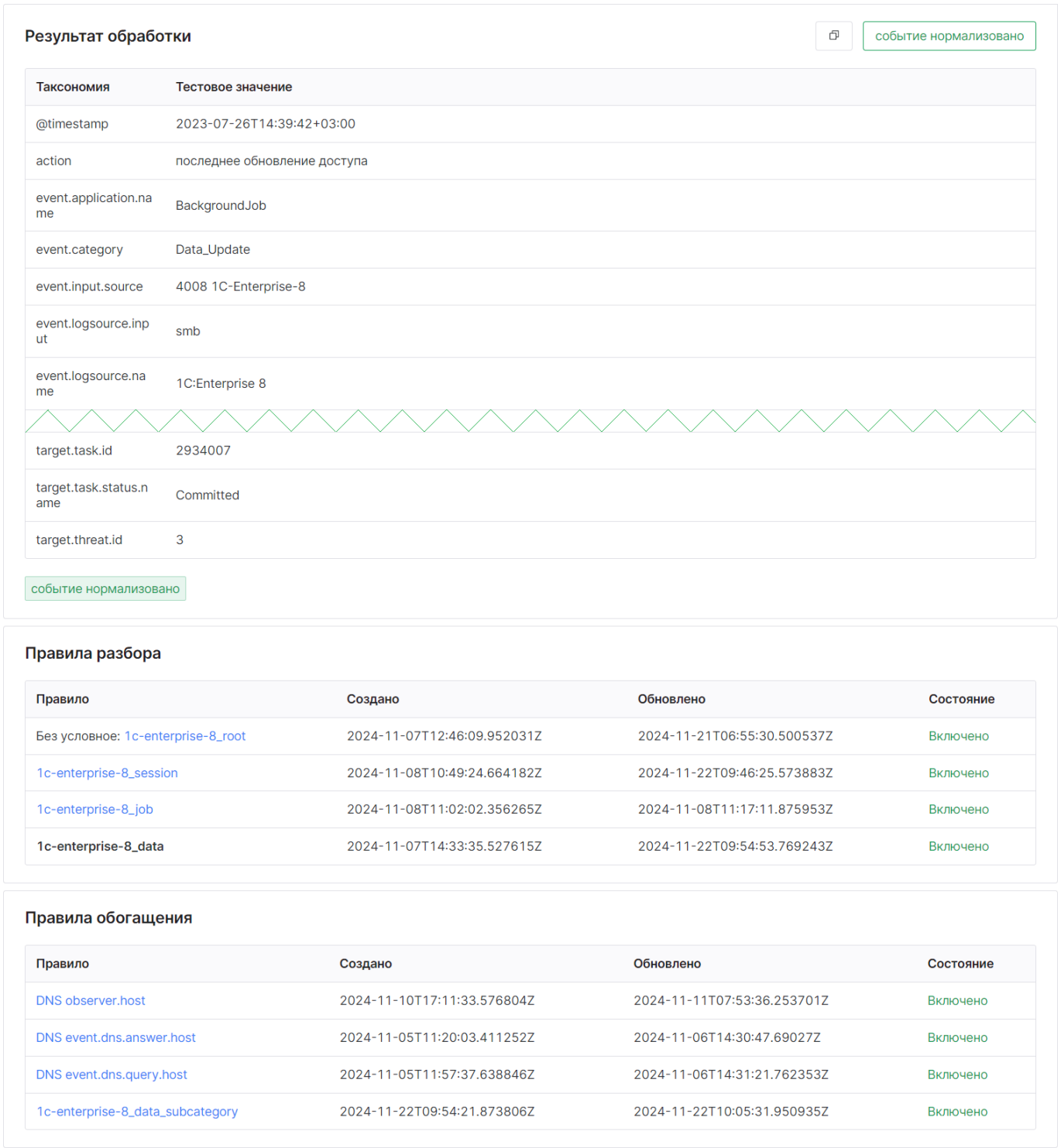


Рис. 7 – Раздел "Отладка источника"

2. В поле **Источник** из выпадающего списка выберите источник. Будет проверяться работа всех правил разбора, настроенных для выбранного источника.
3. В поле **Сырое событие** укажите пример сырого события, которое будет приходить от источника (см. раздел «Получение сырого события»).
4. Если во время проверки необходимо применить правила обогащения, то установите соответствующий флаг.
5. Нажмите кнопку **Тестировать**.
6. Механизм применит к событию от источника все настроенные для него правила разбора и обогащения.

Пример результата проведения тестирования приведен на «Рис. 8».



Результат обработки

событие нормализовано

Таксономия	Тестовое значение
@timestamp	2023-07-26T14:39:42+03:00
action	последнее обновление доступа
event.application.name	BackgroundJob
event.category	Data_Update
event.input.source	4008 1C-Enterprise-8
event.logsource.input	smb
event.logsource.name	1C:Enterprise 8
target.task.id	2934007
target.task.status.name	Committed
target.threat.id	3

событие нормализовано

Правила разбора

Правило	Создано	Обновлено	Состояние
Без условное: 1c-enterprise-8_root	2024-11-07T12:46:09.952031Z	2024-11-21T06:55:30.500537Z	Включено
1c-enterprise-8_session	2024-11-08T10:49:24.664182Z	2024-11-22T09:46:25.573883Z	Включено
1c-enterprise-8_job	2024-11-08T11:02:02.356265Z	2024-11-08T11:17:11.875953Z	Включено
1c-enterprise-8_data	2024-11-07T14:33:35.527615Z	2024-11-22T09:54:53.769243Z	Включено

Правила обогащения

Правило	Создано	Обновлено	Состояние
DNS observer.host	2024-11-10T17:11:33.576804Z	2024-11-11T07:53:36.253701Z	Включено
DNS event.dns.answer.host	2024-11-05T11:20:03.411252Z	2024-11-06T14:30:47.69027Z	Включено
DNS event.dns.query.host	2024-11-05T11:57:37.638846Z	2024-11-06T14:31:21.762353Z	Включено
1c-enterprise-8_data_subcategory	2024-11-22T09:54:21.873806Z	2024-11-22T10:05:31.950935Z	Включено

Рис. 8 – Пример результата проведения тестирования

Результат проведения тестирования содержит следующую информацию:

- Информацию о состоянии разбора события. Может принимать следующие значения:
    - **событие нормализовано** – означает, что событие было успешно преобразовано на пары **«Ключ-Значение»**, которые были успешно переданы в поля события (таксономию);
    - **событие разобрано** – означает, что событие было успешно преобразовано на пары **«Ключ-Значение»**, но они не были переданы в таксономию;

- **событие не разобрано** – означает, что событие не удалось преобразовать на пары **«Ключ-Значение»**, используя текущие правила.

- Блок **Результат обработки** содержит информацию о полученных парах "Ключ-Значение" в результате разбора события:
  - **Таксономия** – наименование поля события, в которое будет подставлено значение;
  - **Тестовое значение** – значение, которое будет подставлено в результате исполнения правил.
- Блок **Правила Разбора** содержит список созданных правил разбора для выбранного источника:
  - **Правило** – наименование правила разбора;

Примечание: "Жирным" шрифтом будет выделено сработавшее правило разбора.

  - **Создано** – дата и время создания правила разбора;
  - **Обновлено** – дата и время изменения информации о правиле разбора;
  - **Состояние** – текущее состояние правила разбора: включено, выключено.
- Блок **Правила Обогащения** содержит список созданных правил обогащения для выбранного источника:
  - **Правило** – наименование правила обогащения

    Примечание: *если правило обогащение попало в список, то считается, что оно было применено.*
  - **Создано** – дата и время создания правила обогащения;
  - **Обновлено** – дата и время изменения информации о правиле обогащения;
  - **Состояние** – текущее состояние правила обогащения: включено, выключено.

Результаты проверки события, которое было нормализовано, можно скопировать как JSON. Для этого нажмите кнопку  .

Пример результатов тестирования, скопированных в json:

```
{"@timestamp":"2023-07-26T14:39:42+03:00","action":"последнее обновление
доступа","event":{"application":{"name":"BackgroundJob"},"category":"Data_Update","
input":{"source":"4008 1C-Enterprise-
8"},"logsource":{"input":"smb","name":"1C:Enterprise
8","product":"ERP","vendor":"1C"},"session":{"id":"34"},"severity":7,"subcategory":
"ОБОГАЩЕНИЕ if \"доступ\" in Data => \"access\", else \"other\"","uuid":"c9a7cb96-
9c0c-43a5-9240-42e1e2902b9e"},"id":"c9a7cb96-9c0c-43a5-9240-
42e1e2902b9e","initiator":{"command":{"executed":"Выполнить
обновление"},"host":{"hostname":""},"user":{"id":"00000000-0000-0000-0000-
000000000000","name":""}},"observer":{"host":{"hostname":"pgr-1c-
00"}},"raw":"{\"Message\":\"<7> 7/26/2023 2:39:42 PM pgr-1c-00
{\\\"Event\\\":{\\\"Level\\\":\\\"Information\\\",\\\"Date\\\":\\\"2023-07-
26T14:39:42\\\",\\\"ApplicationName\\\":\\\"BackgroundJob\\\",\\\"ApplicationPresen
tation\\\":\\\"Background
job\\\",\\\"Event\\\":\\\"_$Data$_.Update\\\",\\\"EventPresentation\\\":\\\"Data.
Change\\\",\\\"User\\\":\\\"00000000-0000-0000-0000-
000000000000\\\",\\\"UserName\\\":\\\"\\\",\\\"Computer\\\":\\\"\\\",\\\"Metadata\\
\":\\\"Константа.ПоследнееОбновлениеДоступа\\\",\\\"MetadataPresentation\\\":\\\"Co
nstant. Последнее обновление
доступа\\\",\\\"Comment\\\":null,\\\"Data\\\":\\\"something Команда: Выполнить
обновление\\\",\\\"DataPresentation\\\":\\\"\\\",\\\"TransactionStatus\\\":\\\"Comm
itted\\\",\\\"TransactionID\\\":\\\"7/26/2023 2:39:42 PM
(2934007)\\\",\\\"Connection\\\":\\\"3\\\",\\\"Session\\\":\\\"34\\\",\\\"ServerNam
e\\\":\\\"\\\",\\\"Port\\\":\\\"\\\",\\\"SyncPort\\\":\\\"0\\\"}}\",\"a\":\"a7e42e2
0-03a1-4998-a301-
c97fa77cbe73\",\"a_c\":\"\",\"a_src_ip\":\"172.30.250.141\",\"a_src_o\":\"445\",\"a
_src_r\":\"smb\",\"a_src_t\":[],\"a_ts\":\"2024-10-
21T12:41:44.993Z\"}","reportchain":{"collector":{"host":{"ip":"172.30.250.141"},"ti
mestamp":"2024-10-21T12:41:44+03:00"},"reciever":{"timestamp":"2024-12-
17T18:23:42+03:00"}},"target":{"host":{"hostname":""},"socket":{"port":""},"task":{
"id":2934007,"status":{"name":"Committed"}},"threat":{"id":"3"}}}
```


2.5 Правила разбора

2.5.1 Описание

Привила разбора определяют параметры этапов разбора и нормализации выбранного сырого события от конкретного источника.

Правило разбора может быть безусловно применяемым и обычным.

Безусловно применяемое правило будет применяться для всех событий, которые поступают от источника. Безусловно применяемое правило для источника может быть только одно.

Правило разбора состоит из двух частей:

- Процедура разбора – параметры преобразования входящего события на пары **«Ключ-Значение»**;
- Процедура нормализации – параметры передачи полученных пар **«Ключ-Значение»** в таксономию. Информация о работе с полями события (таксономией) приведена в разделе «Поля события».

Для максимальной эффективности использования платформы рекомендуется настроить правила разбора для каждого источника, события от которых будут обрабатываться платформой.

Работа с правилами разбора включает в себя следующие процессы:

1. Добавление правила разбора.
2. Редактирование правила разбор.
3. Удаление правила разбора.

Для работы с правилами разбора перейдите в раздел **Источники → Правила разбора** (см. «Рис. 9»).

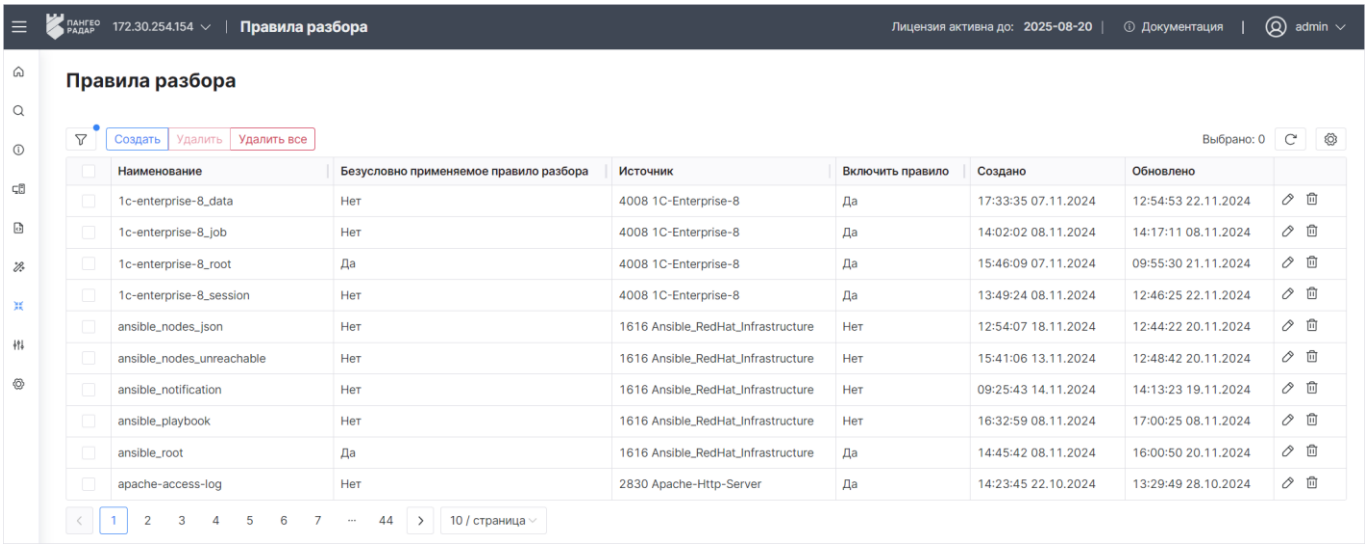


Рис. 9 – Раздел "Правила разбора"

В разделе отображается следующая информация:

- **Наименование** – наименование правила разбора;
- **Безусловно применяемое правило** – является ли правило безусловно применяеым для источника: да, нет;
- **Источник** – наименование источника, к событиям от которых применяется правило;
- **Включить правило** – используется ли правило для разбора событий: да, нет;
- **Создано** – дата и время создания правила;
- **Обновлено** – дата и время изменения информации о правиле.

2.5.2 Добавление правила

Для создания правила разбора нажмите кнопку **Создать**. Начнется процесс создания правила, который состоит из следующих шагов:

- «Шаг 1. Основные настройки»;
- «Шаг 2. Настройка условий фильтрации»;
- «Шаг 3. Настройка параметров процедуры разбора»;
- «Шаг 4. Настройка параметров процедуры нормализации»;

- «Шаг 5. Тестирование правила»;
- «Шаг 6. Включение правила».

Пример формы создания правила разбора приведен на «Рис. 10».

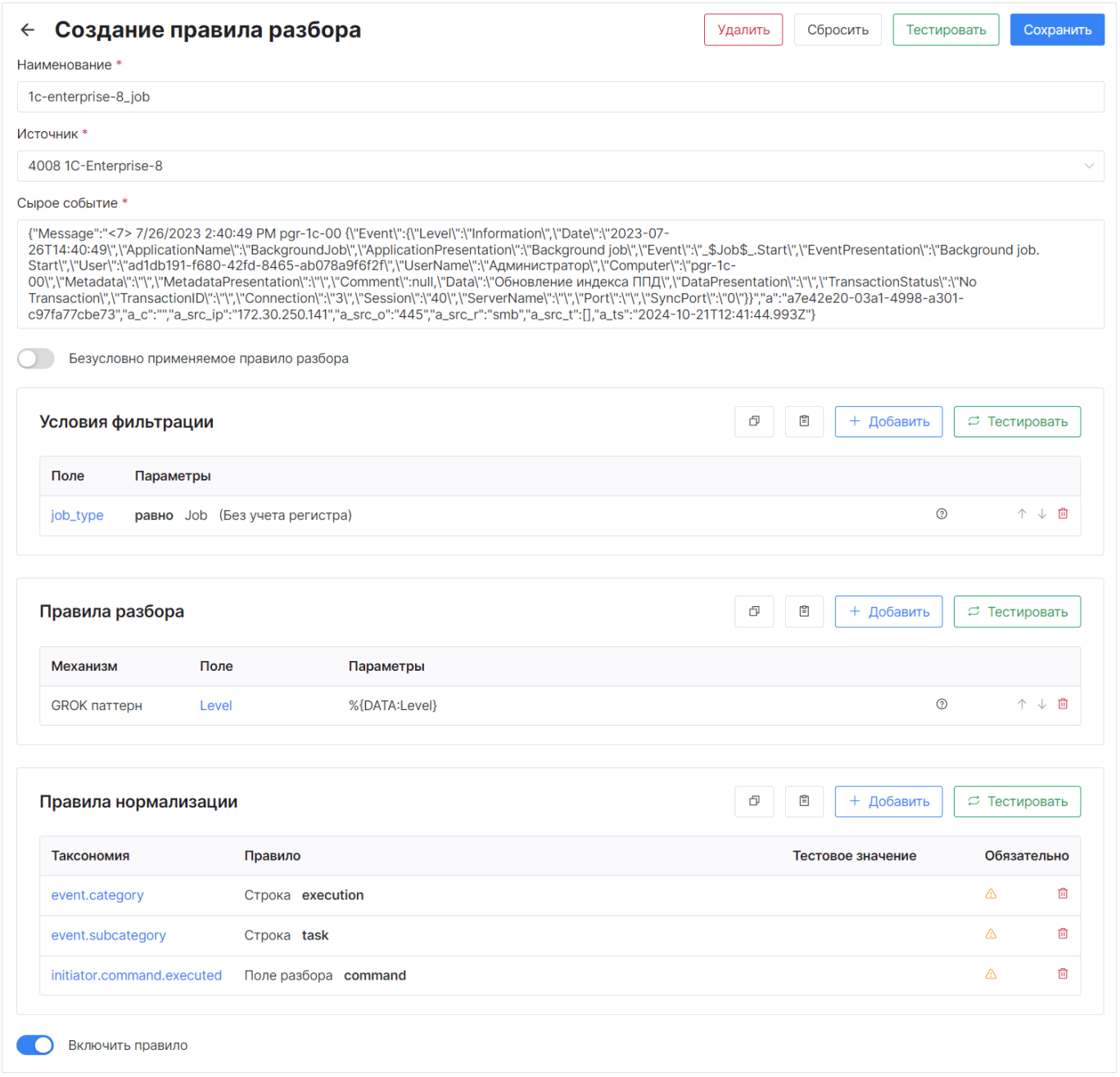


Рис. 10 – Форма создания правила разбора

2.5.2.1 Шаг 1. Основные настройки

Пример основных настроек правила разбора приведен на «Рис. 11».

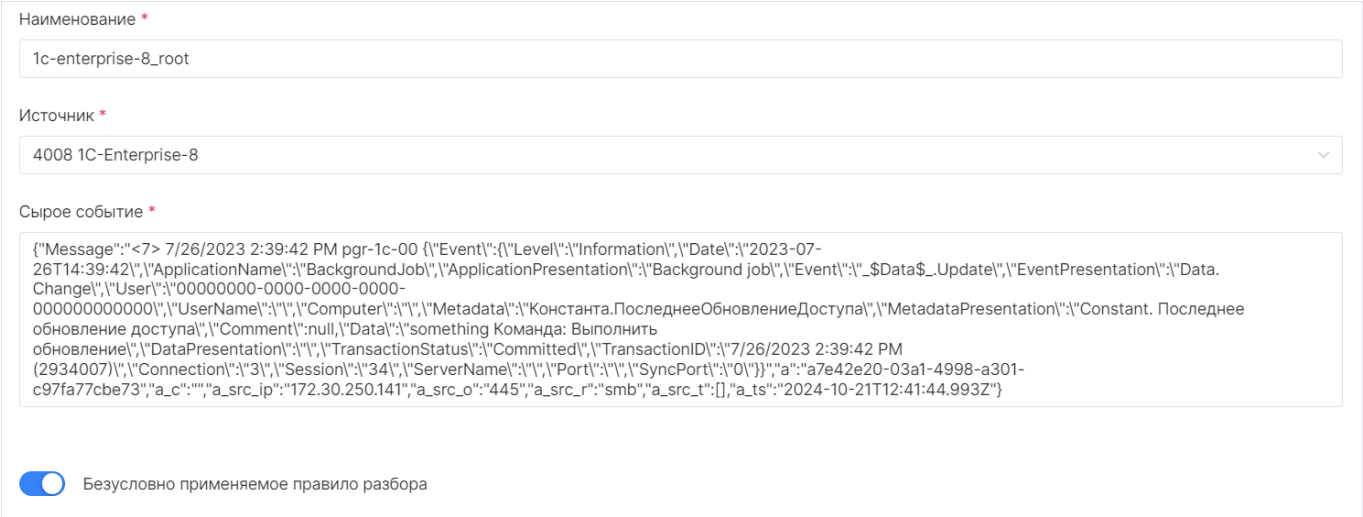


Рис. 11 – Форма создания правила разбора. Основные настройки

Выполните следующие действия:

1. В поле **Наименование укажите** наименование правила.
2. В поле **Источник** из выпадающего списка выберите источник, сырые события от которого будут проходить процессы разбора и нормализации.
3. В поле **Сырое событие** (см. раздел «Получение сырого события») укажите пример сырого события, которое будет приходить от источника.
4. Если правило должно безусловно применяться для выбранного источника, то установите соответствующий переключатель в положение **Включен**.

2.5.2.2 Шаг 2. Настройка условий фильтрации

Пример блока **Условия фильтрации** приведен на «Рис. 12».

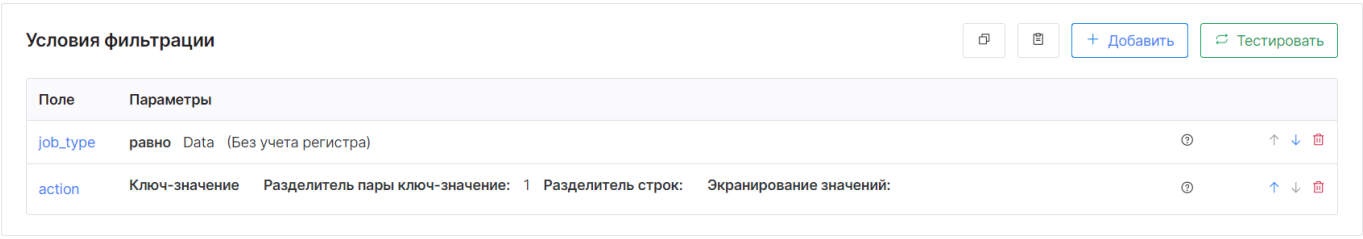


Рис. 12 – Форма создания правила. Блок "Условия фильтрации"

В блоке отображается следующая информация:

- **Поле** – наименование поля, по которому будет применяться фильтр;
- **Параметры** – используемая функция сравнения и ее параметры;
- Информация о тестировании условий, представленная в виде специальных символов:
  - ✓ – условие применимо;
  - ✗ – условие применить невозможно;
  - ? – тестирование не выполнялось.

  Подробнее о механизме тестирования см. «Шаг 5. Тестирование правила».

Условия фильтрации задаются одной из следующих функций сравнения:

- **GROK Паттерн** – фильтрация будет выполняться согласно заданному «GROK паттерн»;
- **Проверить равенство выражений** – будет выполняться сравнение значения поля события, с указанным в условиях фильтрации;
- **Проверить наличие значения** – будет проверяться наличие значения (отличное от "0") в поле события;
- **Проверить наличие в массиве** – будет проверяться наличие значения в поле события из указанного массива значений в условиях фильтрации. Проверка выполняется до первого вхождения значения в массив;
- **Поиск подстроки в строке** – будет проверятся наличие указанного значения в подстроке поля события;
- **Ключ-Значение** – фильтрация будет выполняться согласно заданным параметрам механизма «Ключ значение»;
- **Функция преобразования** – фильтрация будет выполняться согласно заданным параметрам механизма «Функция преобразования».

Дополнительно, для функций сравнения **GROK Паттерн** и **Ключ-Значение** можно настроить следующие параметры:

- Префикс (см. раздел «Механизм работы префикса»);
- Группа результата (см. раздел «Механизм работы функции группировки»).

Для функций сравнения доступны следующие настройки:

- **без учета регистра** – если функция включена, то при выполнении функции сравнения не будет учитываться регистр;
- для каждой функции можно включить **отрицание**: "не равно", "не существует".

Созданные условия фильтрации можно скопировать, а затем применить в другом правиле:

- – скопировать условия фильтрации;
- – вставить скопированные условия фильтрации. Скопированные условия фильтрации можно вставить только в блок **Условия фильтрации**.

В правило может быть добавлено несколько условий фильтрации. Условия будут исполняться по порядку.

Для изменения порядка исполнения условий фильтрации используйте кнопки ↓ / ↑.

Внимание! *Если не сработало какое-то из условий фильтраций (при тестировании получен флаг), добавленных в правило, то правило исполняться не будет.*

Для добавления условий фильтрации выполните следующие действия:

1. В блоке **Условия фильтрации** нажмите кнопку **Добавить**. Откроется окно "Добавить условие фильтрации" (см. «Рис. 13»).

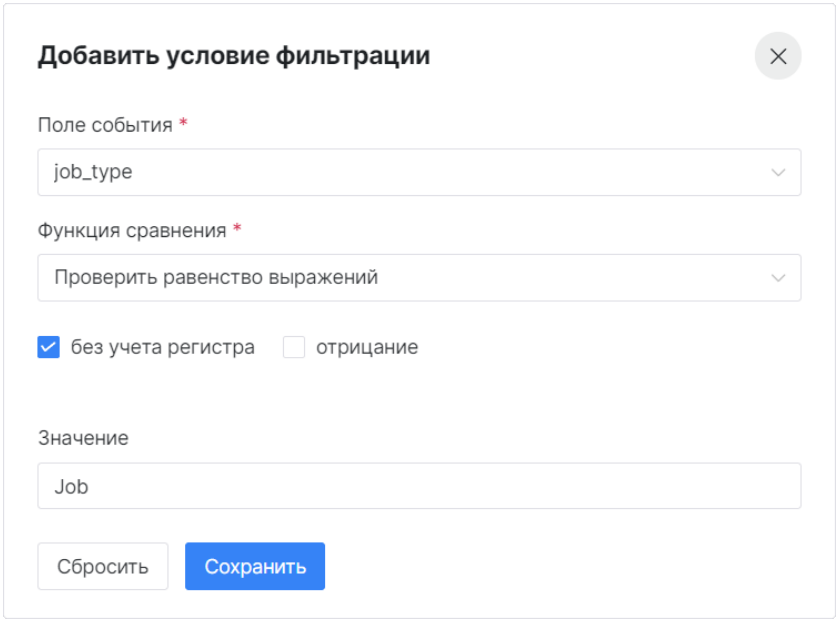


Рис. 13 – Окно "Добавить условие фильтрации"

2. Выполните в окне следующие действия:
    - **Поле события** – из выпадающего списка выберите поле события, по которому будет выполняться фильтрация;
    - **Функция сравнения** – из выпадающего списка выберите функцию сравнения. В зависимости от выбранной функции сравнения, укажите дополнительную информацию:
        - GROK Паттерн:
            - в поле **Паттерн** укажите тело GROK паттерна;
            - в поле **Префикс** укажите префикс, который будет использоваться для получившихся значений;
            - в поле **Группа результатов** укажите группу результатов, к которой будет относится получивший результат работы условий.
        - Проверить равенство выражений. В поле **Значение** укажите значение поля, по которому будет выполняться функция сравнения:
            - если значение, пришедшее в поле, будет равно указанному в условии фильтрации, то условие применится;
            - в обратном случае условие фильтрации применено не будет.
        - Проверить наличие значения. Дополнительных действий не требуется. Функция будет проверять что в пришедшем поле присутствует значение:
            - если значение в поле есть, то условие применится;
            - в обратном случае условие фильтрации применено не будет.
        - Проверить наличие в массиве. Функция сравнения будет проверять значения, пришедшие в поле, с указанным массивом. После первого вхождения

значения в массив, условие фильтрации будет выполнено. Выполните следующие действия:

- в поле **Значение** нажмите кнопку **Создать**. Появится поле для указания значения;
- создайте массив значений добавив и указав необходимое количество полей.

- Поиск подстроки в строке. В поле **Значение** укажите значение подстроки поля, по которому будет выполняться функция сравнения:
  - если значение, указанное в условии фильтрации, является частью (или полностью равно) пришедшему текстовому полю, то условие применится;
  - в обратном случае условие фильтрации применено не будет.
- Ключ-значение. Заполните следующие поля:
  - **Разделитель пары ключ-значение** – укажите символ, который будет являться разделителем внутри пары ключ-значение;
  - **Разделитель строк** – укажите символ, который будет являться разделителем строк;
  - **Экранирование значений** – укажите способ экранирования значений;
  - **Префикс** – укажите префикс, который будет использоваться для получившихся значений;
  - **Группа результатов** – укажите группу результатов, к которой будет относится получивший результат работы условий
- Функция преобразования. На данный момент доступна только функция **HEX to Text**, которая используется для преобразования шестнадцатеричной строки в текст.
- При необходимости включите настройки **Без учета регистра** и **Отрицание**, установив соответствующие флаги.

3. Нажмите кнопку **Сохранить**.

2.5.2.3 Шаг 3. Настройка параметров процедуры разбора

Пример блока **Правила разбора** приведен на «Рис. 14».

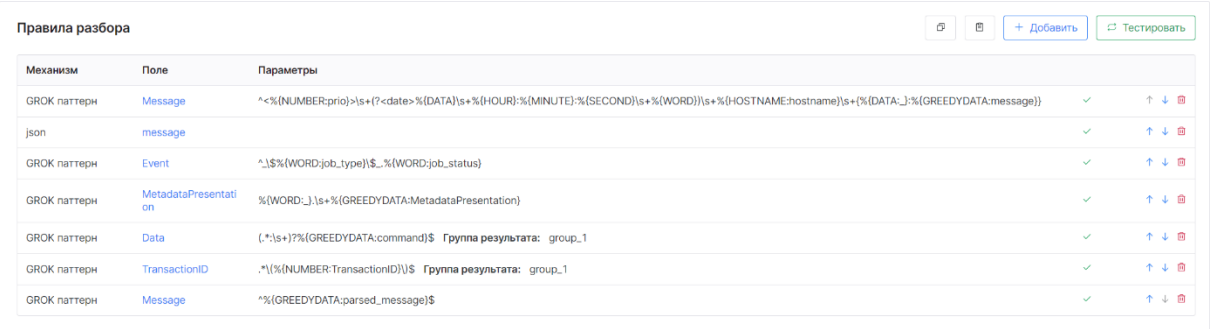


Рис. 14 – Форма создания правила. Блок "Правила разбора"

В блоке отображается следующая информация:

- **Механизм** – используемый механизм разбора (подробнее о механизмах разбора см. раздел «Механизмы разбора»);
- **Поле** – наименование поля, к которому применяется механизм разбора;
- **Параметры** – параметры механизма разбора;
- Информация о тестировании процедур разбора, представленная в виде специальных символов:
  - ✓ – правило применимо;
  - ✗ – правило применить невозможно;
  - ? – тестирование не выполнялось.

  Подробнее о механизме тестирования см. «Шаг 5. Тестирование правила».

Дополнительно, для каждого механизма разбора, за исключением **Функции преобразования**, можно настроить следующие параметры:

- Префикс (см. раздел «Механизм работы префикса»);
- Группа результата (см. раздел «Механизм работы функции группировки»).

Созданные процедуры разбора можно скопировать, а затем применить в другом правиле:

- – скопировать параметры процедуры разбора;
- – вставить скопированные параметры процедуры разбора. Скопированные параметры разбора можно вставить только в блок **Правила разбора**.

Для изменения порядка исполнения процедур разбора используйте кнопки ↓ / ↑.

В правило может быть добавлено несколько процедур разбора. Процедуры разбора будут исполняться по порядку. Если все заданные процедуры разбора были успешно применены (получен флаг ✓ при тестировании) тогда событие будет считаться разобранным и попадет в соответствующий "топик".

Процедуры разбора можно **сгруппировать**. Для этого необходимо выставить последовательность так, чтобы применение механизмов разбора на одно и тоже поле шло **последовательно** (см. «Рис. 15»).

Единственным допустимым механизмом, который может дать отрицательный результат тестирования (получен флаг ✗) и при этом правило разбора будет считаться успешно примененным – это GROK-Паттерн. При этом должно быть соблюдено условие: GROK-Паттерны на конкретное поле должны быть сгруппированы (см. «Рис. 15»).

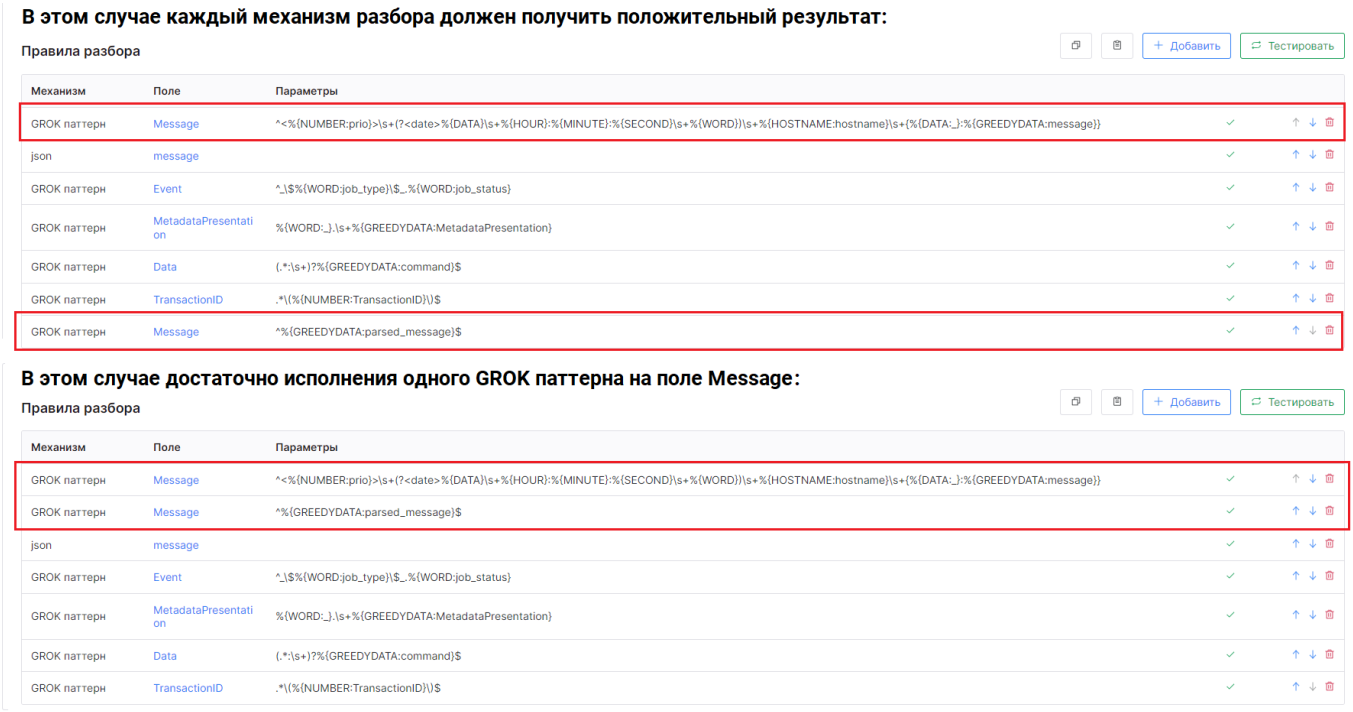


Рис. 15 – Пример группировки механизма разбора на конкретное поле

Для добавления процедуры разбора выполните следующие действия:

1. В блоке **Правила разбора** нажмите кнопку **Добавить**. Откроется окно "Добавить правило разбора" (см. «Рис. 16»).

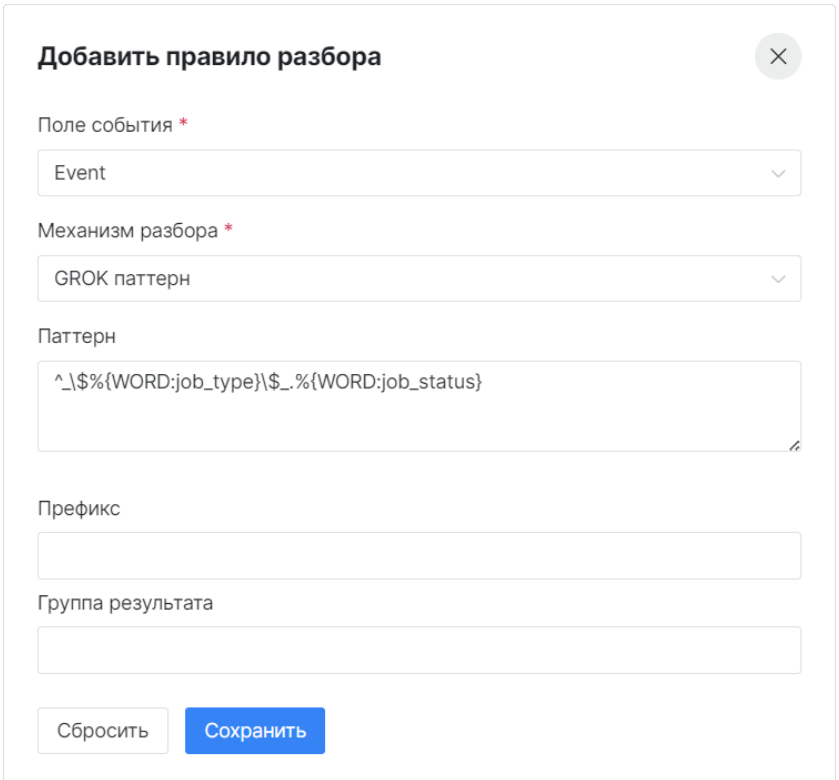


Рис. 16 – Добавление правила разбора. Механизм "GROK-паттерн"

2. В открывшемся окне выполните следующие действия:

   - **Поле события** – из выпадающего списка выберите поле события, к которому будет выполняться механизм разбора;

- **Механизм разбора** – из выпадающего списка выберите механизм, который будет применяться для разбора выбранного поля. В зависимости от выбранного механизма, укажите дополнительную информацию:
  - «GROK паттерн»;
  - «CEF»;
  - «EXECVE»;
  - «Ключ значение»;
  - «CSV»;
  - «SYSLOG»;
  - «XML»;
  - «JSON»;
  - «Функция преобразования».

  Примечание: *В основном, все источники посылают события в формате RAW-JSON. При разборе событий в этом формате необходимо в качестве первой процедуры разбора использовать механизм «JSON», а потом любые из доступных в платформе, в зависимости от типа данных в исходном событии.*

3. Нажмите кнопку **Сохранить**.

2.5.2.4 Шаг 4. Настройка параметров процедуры нормализации

На данном этапе выполняется настройка параметров передачи полученных пар **«Ключ-Значение»** в таксономию.

Пример блока **Правила нормализации** приведен на «Рис. 17».

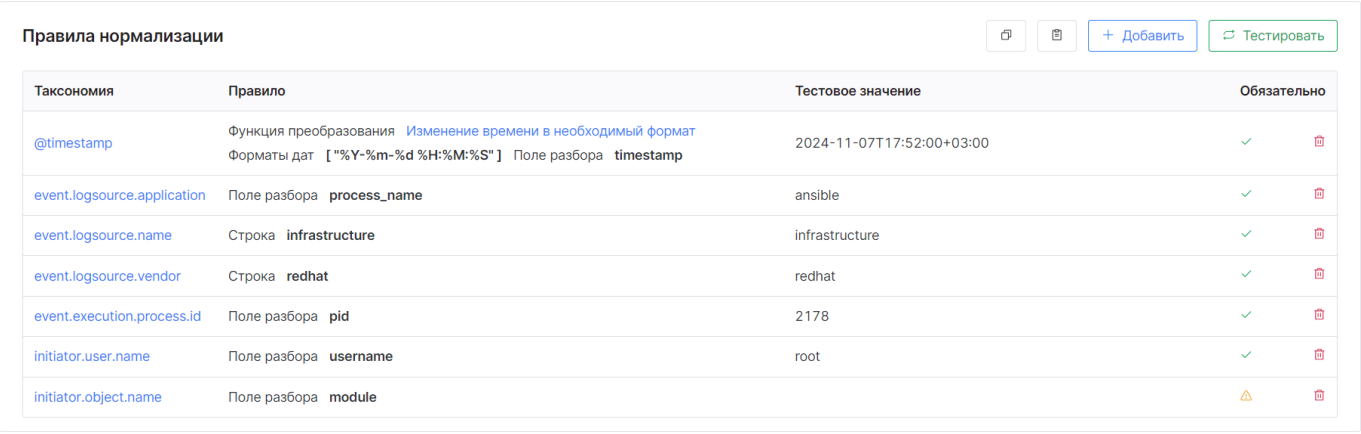


Рис. 17 – Форма создания правила. Блок "Правила нормализации"

В блоке отображается следующая информация:

- **Таксономия** – наименование поля события, в которое будет подставлено значение. Информация о работе с полями события (таксономией) приведена в разделе «Поля события»;

- **Правило** – параметры процедуры нормализации. Процедура нормализации может использовать следующие методы передачи (подстановки) пары **«Ключ-Значение»** в таксономию:
  - «Функции преобразования»;
  - «Строка»;
  - «Поле разбора».
- **Тестовое значение** – значение, которое будет подставлено в таксономию. Данное значение отображается после проведения процедуры тестирования правила;
- **Обязательно** – является ли поле обязательным к заполнению при выполнении нормализации: да нет. Признак обязательности отображается с помощью следующих флагов:
  - ✓ – поле обязательно для заполнения;
  - ⚠ – поле не обязательно.

Созданные процедуры нормализации можно скопировать, а затем применить в другом правиле:

- – скопировать параметры процедуры нормализации;
- – вставить скопированные параметры процедуры нормализации. Скопированные параметры нормализации можно вставить только в блок **Правила нормализации**.

Для добавления процедуры нормализации выполните следующие действия:

1. В блоке **Правила нормализации** нажмите кнопку **Добавить**. Откроется окно "Добавить правило нормализации" (см. «Рис. 18»).

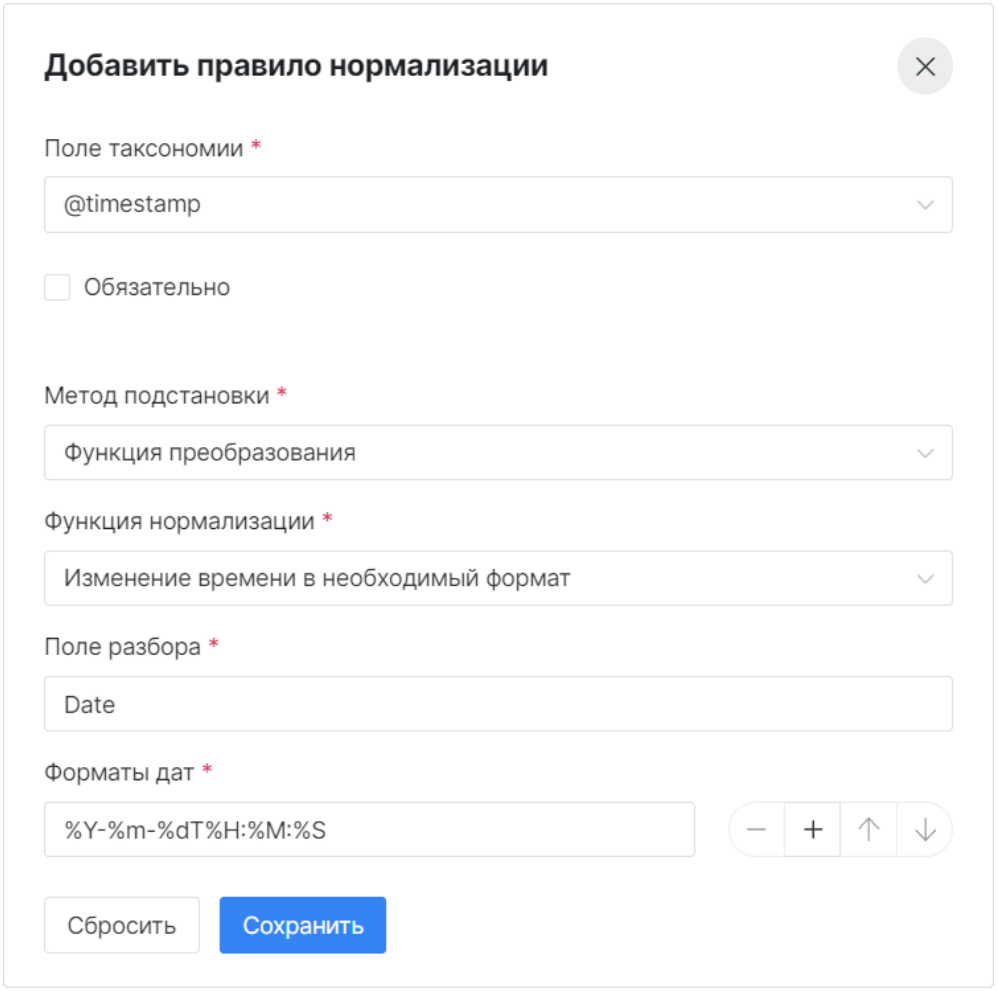


Рис. 18 – Добавление правила нормализации. Метод подстановки "Функция преобразования"

2. В открывшемся окне выполните следующие действия:
    - **Поле таксономии** – из выпадающего списка выберите поле таксономии, на которое будет выполняться механизм нормализации;
    - Если заполнение выбранного поля таксономии должно быть обязательным, то установите флаг **Обязательно**;
    - **Метод подстановки** – из выпадающего списка выберите способ подстановки пар "Ключ-Значение" в таксономию. В зависимости от выбранного механизма, укажите дополнительную информацию:
        - «Функции преобразования»;
        - «Строка»;
        - «Поле разбора».
3. Нажмите кнопку **Сохранить**.

2.5.2.5 Шаг 5. Тестирование правила

Функция тестирования позволяет проверить корректность созданных процедур разбора и нормализации, а также условий фильтрации. Она наглядно демонстрирует преобразование сырого события на пары "Ключ-Значение".

Для этого в блоках **Условия Фильтрации**, **Правила Разбора** и **Правила Нормализации** есть кнопка **Тестировать**. Механизм тестирования является централизованным, поэтому не имеет значения из какого блока он будет запущен. Процесс тестирования последовательно применит все параметры правила и выдаст результаты в соответствующие блоки. После чего в блоках станет доступна кнопка **Показать результаты**.

Поскольку безусловно применяемое правило выполняется в первую очередь, то и при тестировании правил, которые не являются безусловными, это будет учитываться. При просмотре результатов у таких правил будет отображена информации о работе "Безусловно применяемого правила разбора".

2.5.2.5.1 Тестирование условия

При просмотре результатов тестирования условий фильтрации, информация будет разделена по следующим вкладкам:

- "Сырое событие" – информация о парах **Ключ-Значение** приходящая от сырого события;
- "Безусловно применяемое правило разбора" (только для не безусловно применяемых правил) – информация о парах **Ключ-Значение** сформированных после сработки безусловно применяемого правила разбора для данного источника;
- "Поля текущего условия фильтрации" – информация о парах **Ключ-Значение** сформированных после применения условий фильтрации.

Пример результатов тестирования условий фильтрации приведен на «Рис. 19».

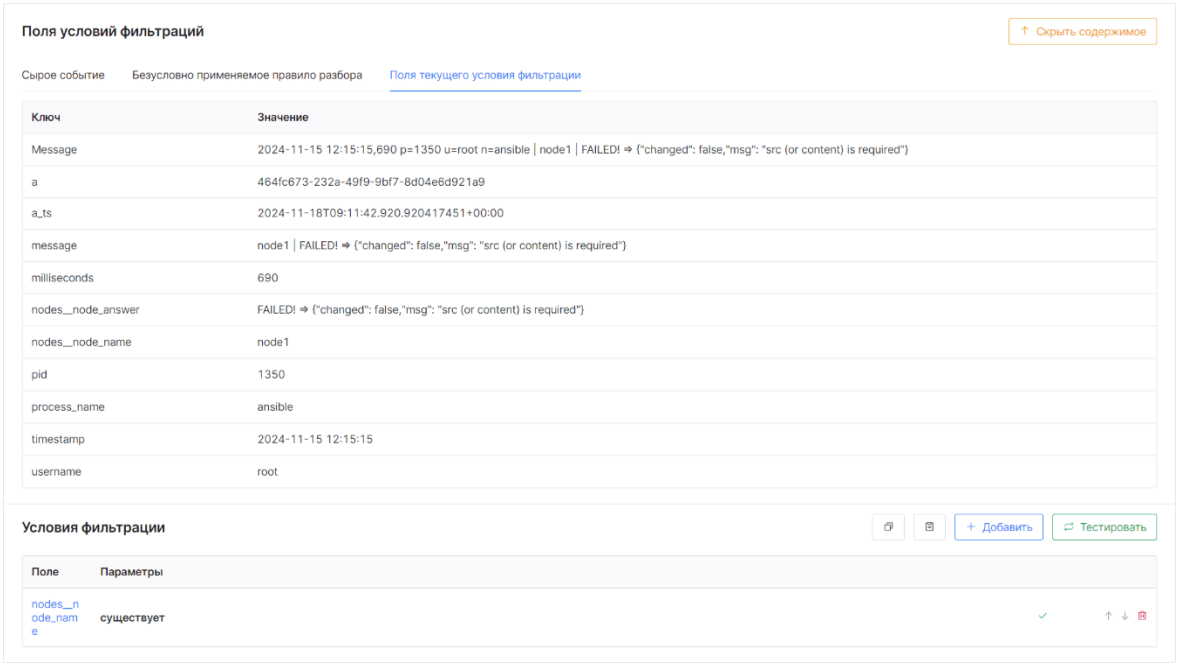


Рис. 19 – Пример результатов тестирования условий фильтрации

2.5.2.5.2 Тестирование процедуры разбора

При просмотре результатов работы процедур разбора, информация будет разделена по следующим вкладкам:

- "Сырое событие" – информация о парах **Ключ-Значение** приходящая от сырого события;

- "Безусловно применяемое правило разбора" (только для не безусловно применяемых правил) – информация о парах **Ключ-Значение** сформированных после применения безусловно исполняемого правила разбора для данного источника;
- "Поля текущего условия фильтрации" – информация о парах **Ключ-Значение** сформированных после применения условий фильтрации.

Пример результатов тестирования процедур разбора приведен на «Рис. 20».

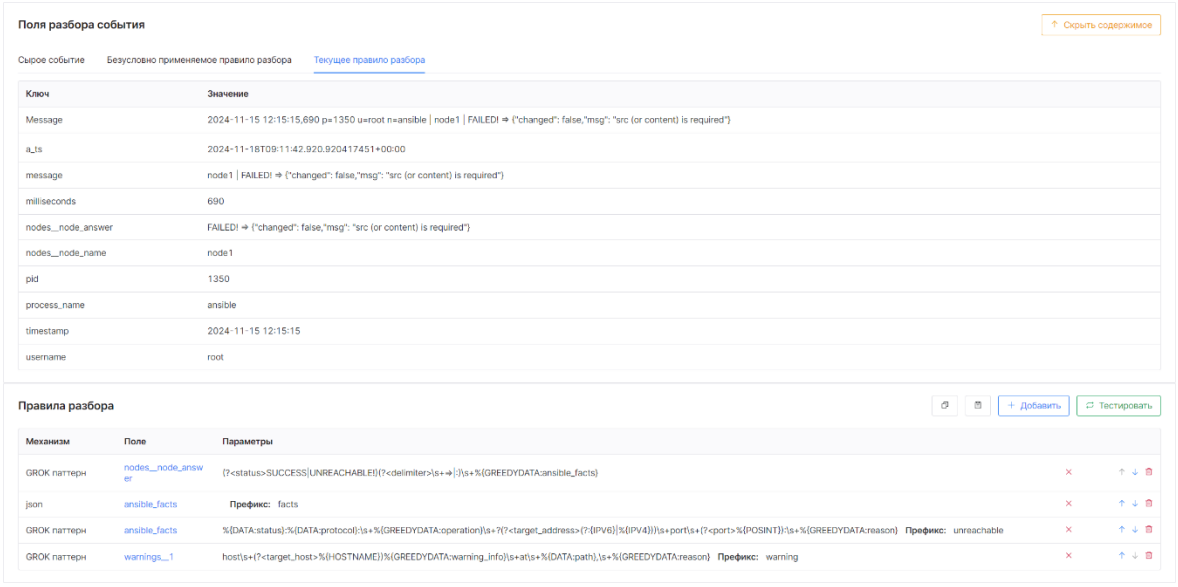


Рис. 20 – Пример результатов тестирования процедур разбора

2.5.2.5.3 Тестирование процедуры нормализации

В блоке показывается результат применения безусловно применяемого правила разбора. Поэтому информация в блоке будет отображаться только для правил, которые не являются безусловно исполняемыми.

При попытке тестировать безусловно исполняемое правило будут выданы пустые значения.

Пример тестирования процедуры нормализации приведен на «Рис. 21».

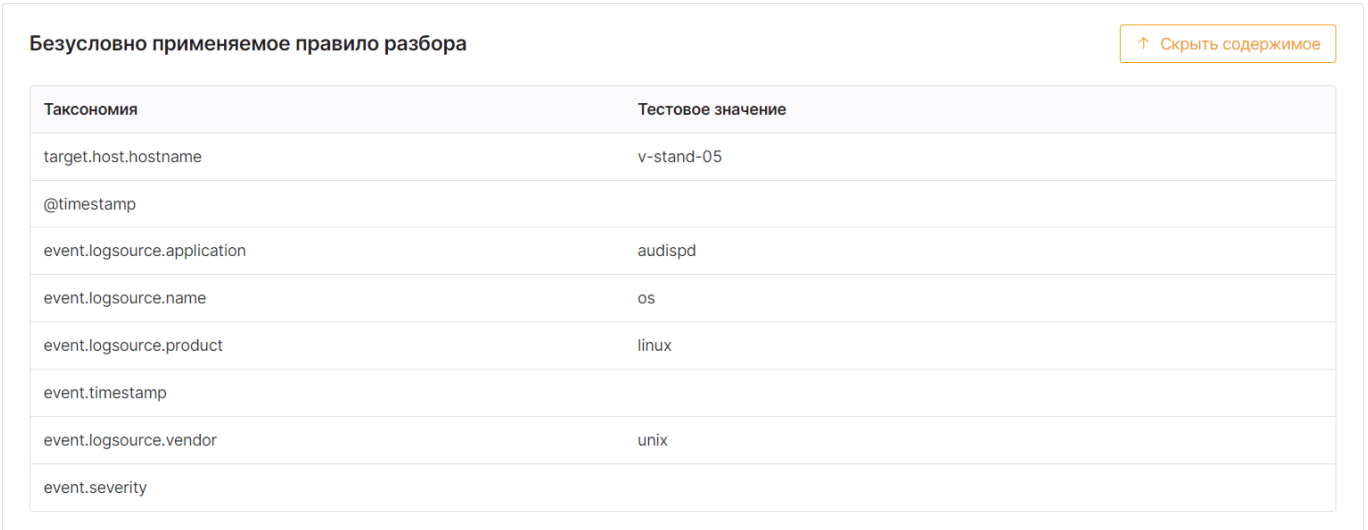


Рис. 21 – Пример результатов тестирования процедур нормализации

В блоке отображается следующая информация:

- **Таксономия** – наименование поля события, в которое будет подставлено значение;
- **Тестовое значение** – значение, которое будет подставлено в результате исполнения правила.

2.5.2.6 Шаг 6. Включение правила

После настройки всех параметров и достижения необходимых результатов тестирования включите правило. Для этого установите переключатель **Включить правило** в положение "включен", а за тем нажмите кнопку **Сохранить**.

После настройки всех необходимых правил для источника рекомендуется выполнить процедуру «Отладка источников».

2.5.3 Редактирование правила разбора

1. В строке нужного правила нажмите кнопку  .
2. Внесите необходимые изменения.
3. Выполните тестирование правила.
4. После достижения необходимых результатов, нажмите кнопку **Сохранить**.

2.5.4 Удаление правила разбора

Примечание: *для корректной работы **Платформы Радар** не рекомендуется удалять правила разбора, установленные по умолчанию*.

Для удаления правила нажмите кнопку  в соответствующей строке.

Для массового удаления правил установите нужные флаги и нажмите кнопку **Удалить**.

Для удаление всех правил нажмите кнопку **Удалить все**.

2.6 Обогащение

2.6.1 Описание

Обогащение событий – это процесс заполнения полей нормализованных событий согласно правилам обогащения.

В **Платформе Радар** правила могут быть настроены по следующим типам обогащения:

- «Обогащение по произвольному скрипту». Наполнение событий дополнительной информацией на основе пользовательского скрипта;
- «DNS обогащение». Наполнение событий дополнительной информацией на основе данных DNS-сервера;
- «GeoIP-обогащение». Добавление информации о географическом местоположении IP-адресов, например, о стране и городе расположения;
- «Обогащение по табличному списку». Наполнение событий дополнительной информацией на основе данных табличных списков, добавленных в платформу;

- «Обогащение по справочнику». Наполнение событий дополнительной информацией на основе данных локальных справочников;
- «Обогащение по локальному адресу». Обогащение данных об IP-адресе: входит ли он в локальную сеть или нет;
- «Корректировка времени». Добавление информации о смещении времени в выбранном поле события.

Поток событий перед обработкой предварительно фильтруется с помощью условий. Условия настраиваются для каждого правила.

Платформа Радар позволяет дополнять событие **тегами** при "сработке" правила обогащения. Теги служат для отслеживания сработавших правил обогащения при просмотре и анализе событий, при построении рабочих столов, а также могут использоваться для настройки правил корреляции.

Правила обогащения исполняются в определенном порядке. Последовательность исполнения правил обогащения выглядит следующим образом:

1. Правила обогащения исполняются только на потоке нормализованных событий от источников.
2. Выбираются все правила обогащения, которые подходят для источников, от которых идет поток событий.
3. Для каждого правила фильтруется поток событий по условиям фильтрации, заданных в правилах.
4. Если не сработало какое-то из условий фильтраций, добавленных в правило, то правило исполняться не будет.
5. Исполняются все правила по конкретным источникам в следующем порядке: **DNS-обогащение → GeoIP-обогащение → По табличному списку → По справочнику → По локальному адресу**.
6. Затем применяются условия, заданные в правилах, например, выставление тегов.

Платформа Радар поставляется с набором правил обогащения, необходимых для работы. При необходимости вы можете настроить свои правила обогащения нормализованных событий.

Работа с правилами обогащения включает в себя следующие процессы:

1. Создание правила.
2. Редактирование правила.
3. Удаления правила

Для работы с правилами обогащения перейдите в раздел **Источники → Обогащение** (см. «Рис. 22»).

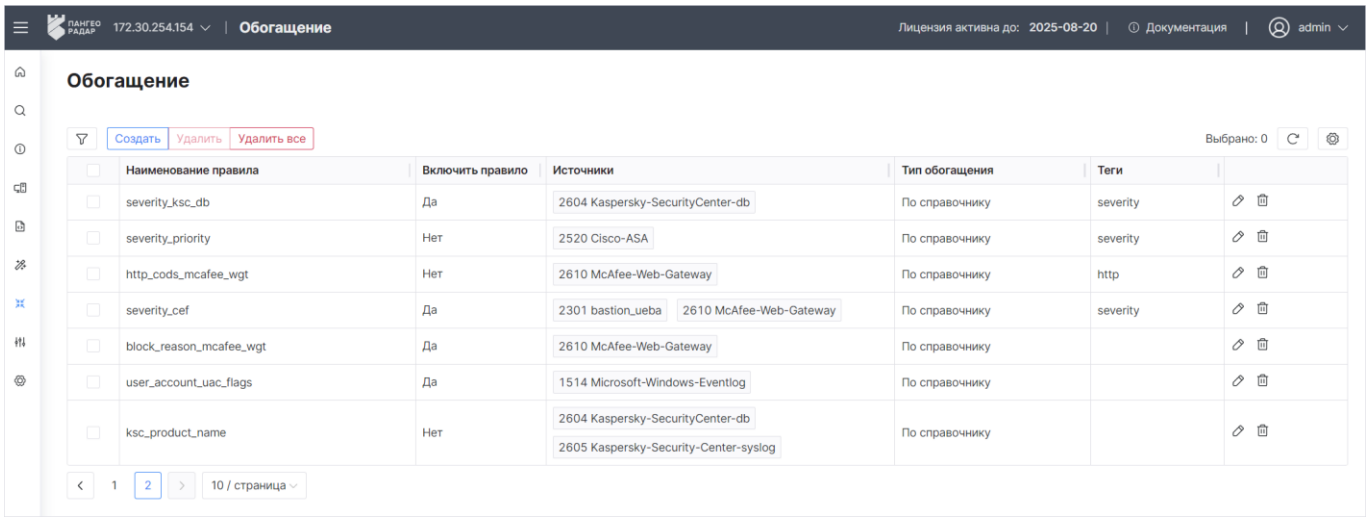


Рис. 22 – Раздел "Обогащение"

В разделе отображается следующая информация:

- **Наименование правила** – наименование правила в интерфейсе платформы;
- **Включить правило** – используется ли правило для обогащения событий: да, нет;
- **Источники** – список источников, поток событий от которых обрабатывается правилом;
- **Тип обогащения** – тип обогащения, используемый правилом;
- **Теги** – список тегов.

2.6.2 Создание правила

Для создания правила обогащения нажмите кнопку **Создать**. Начнется процесс создания правила, который состоит из следующих шагов:

- «Шаг 1. Основные настройки»;
- «Шаг. 2 Настройка условий фильтрации»;
- «Шаг 3. Настройка параметров обогащения».

Пример формы создания правила обогащения приведен на Рис. 23.

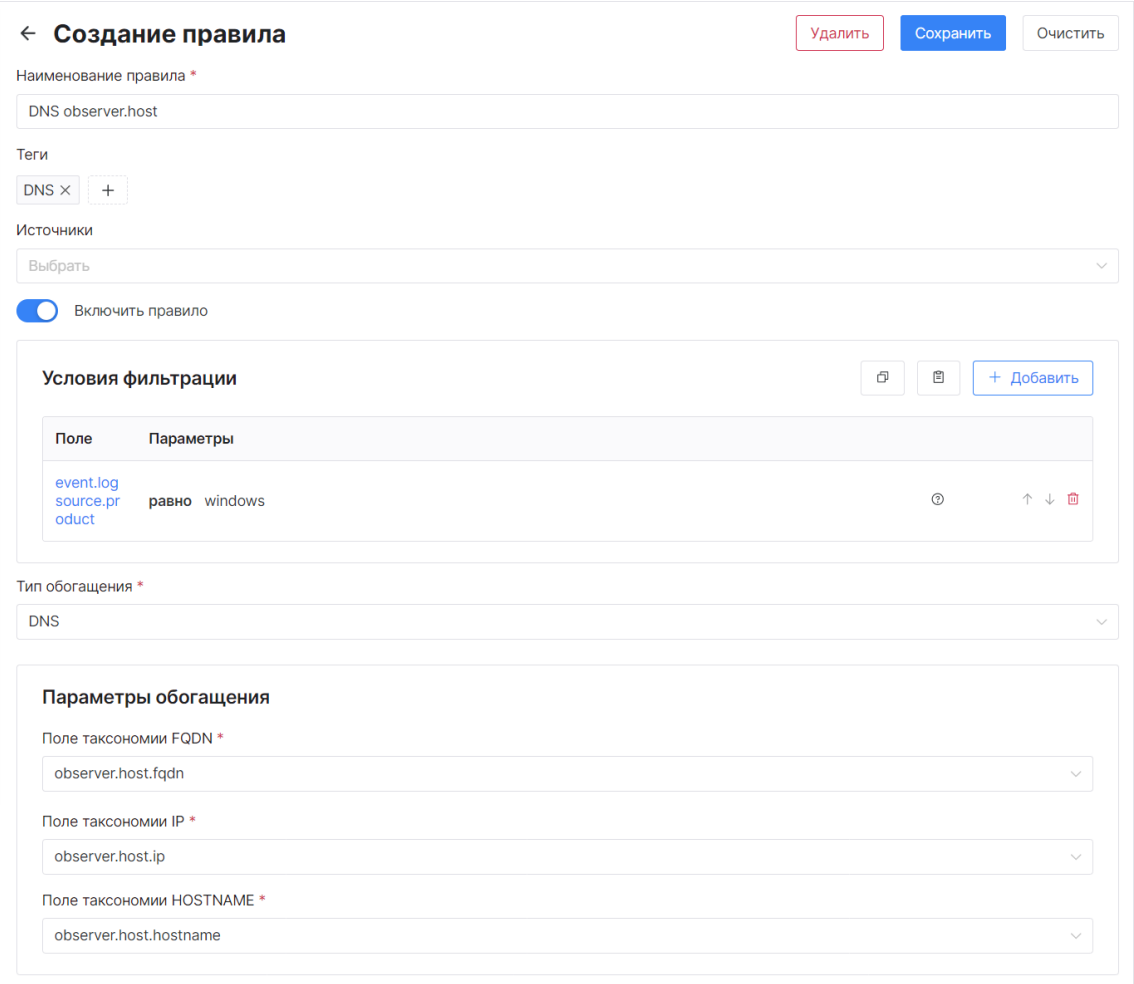


Рис. 23 – Форма создания правила обогащения

2.6.2.1 Шаг 1. Основные настройки

1. В поле **Наименование правила** укажите наименование правила.
2. В поле **Теги** добавьте теги, которые будут характеризировать правило. **Платформа Радар** позволяет использовать одни и те же теги в разных правилах.
3. В поле **Источники** из выпадающего списка выберите источники, нормализованные события от которых будут проходить процесс обогащения данным правилом.
4. Для того, чтобы правило учувствовало в процессе обогащения событий, установите переключатель **Включить правило** в положение "включен".

2.6.2.2 Шаг. 2 Настройка условий фильтрации

На данном шаге настраивается фильтрация потока событий по заданным условиям.

Условия фильтрации задаются одной из следующих функций сравнения:

- **Проверить равенство выражений** – будет выполняться сравнение значения поля события, с указанным в условиях фильтрации;
- **Проверить наличие значения** – будет проверяться наличие значения (отличное от "0") в поле события;

- **Проверить наличие в массиве** – будет проверяться наличие значения в поле события из указанного массива значений в условиях фильтрации. Проверка выполняется до первого вхождения значения в массив;
- **Поиск подстроки в строке** – будет проверятся наличие указанного значения в подстроке поля события.

Для функций сравнения доступны следующие настройки:

- **без учета регистра** – если функция включена, то при выполнении функции сравнения не будет учитываться регистр;
- для каждой функции можно включить **отрицание**: "не равно", "не существует".

Созданные условия фильтрации можно скопировать, а затем применить в другом правиле:

- – скопировать условия фильтрации;
- – вставить скопированные условия фильтрации.

В правило может быть добавлено несколько условий фильтрации. Условия будут исполняться по порядку (см. «Рис. 24»).

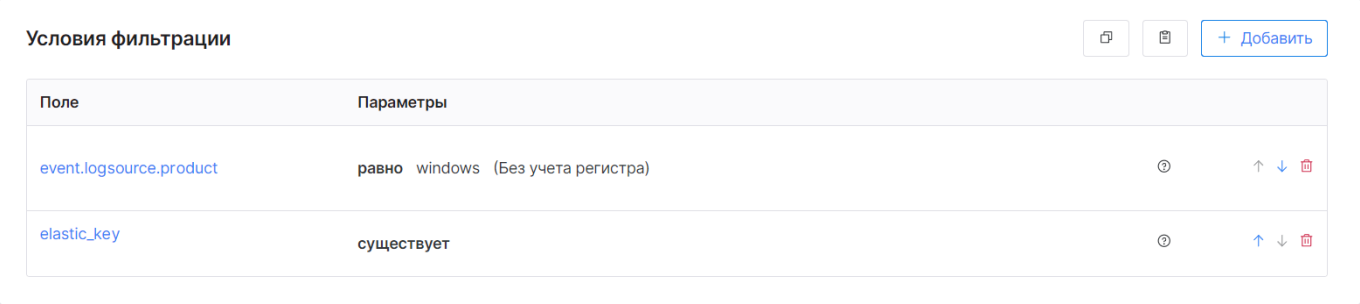


Рис. 24 – Порядок исполнения условий фильтрации

Внимание! *Если не сработало какое-то из условий фильтраций, добавленных в правило, то правило исполняться не будет.*

Для изменения порядка исполнения условий фильтрации используйте кнопки ↓ / ↑.

Для добавления условий фильтрации выполните следующие действия:

1. В блоке **Условия фильтрации** нажмите кнопку **Добавить**. Откроется окно "Добавить условие фильтрации" (см. «Рис. 25»).

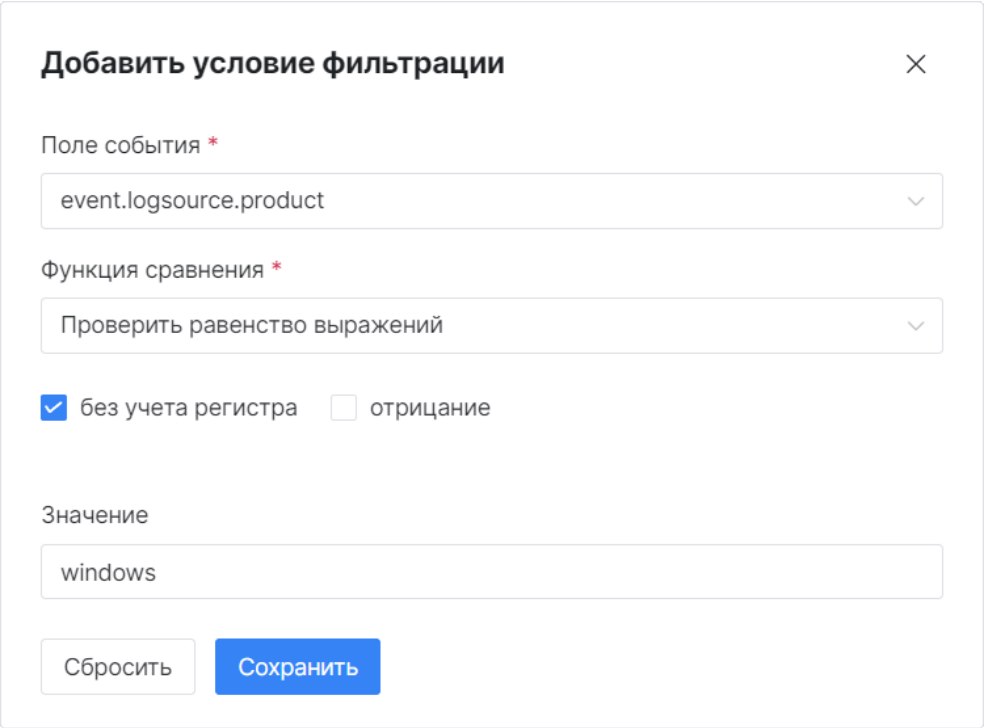


Рис. 25 – Окно "Добавить условие фильтрации"

2. Выполните в окне следующие действия:
    - **Поле события** – из выпадающего списка выберите поле события, по которому будет выполняться фильтрация;
    - **Функция сравнения** – из выпадающего списка выберите функцию сравнения. В зависимости от выбранной функции сравнения, укажите дополнительную информацию:
        - для функции **Проверить равенство выражений** в поле **Значение** укажите значение поля, по которому будет выполняться функция;
        - для функции **Проверить наличие в массиве** добавьте массив и укажите соответствующие значения;
        - для функции **Поиск подстроки в строке** в поле **Значение** укажите значение подстроки поля, по которому будет выполняться функция;
        - при необходимости включите настройки **Без учета регистра** и **Отрицание**, установив соответствующие флаги.
3. Нажмите кнопку **Сохранить**.

2.6.2.3 Шаг 3. Настройка параметров обогащения

1. В поле **Тип обогащения** из выпадающего списка выберите способ, который будет применяться для обогащения событий при сработке правила.
2. В зависимости от выбранного типа обогащения будет сформировать блок **Параметры обогащения**. Укажите в блоке соответствующие параметры в зависимости от типа обогащения.
3. Нажмите кнопку **Сохранить**.

2.6.3 Редактирование правила

1. В строке нужного правила обогащения нажмите кнопку .
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

2.6.4 Удаление правила

Для удаления правила нажмите кнопку в соответствующей строке.

Для массового удаления правил, установите соответствующие флаги и нажмите кнопку **Удалить**.

Для удаление всех правил нажмите кнопку **Удалить все**.

2.7 GROK паттерны

2.7.1 Описание

GROK паттерны – это именованные регулярные выражения, которые позволяют пользователям сопоставлять конкретные шаблоны в тексте. С их помощью можно быстро идентифицировать и извлекать поля из поступающих событий без необходимости писать сложные регулярные выражения с нуля.

GROK паттерны являются одним из механизмов разбора событий, используемых в правилах разбора (подробнее см. раздел «GROK паттерн»).

В **Платформе Радар** GROK паттерны делятся на системные и пользовательские.

Пользовательский GROK паттерн состоит из уникального ключа и непосредственно паттерна.

Ключ используется для идентификации GROK паттернов при использовании в правилах разбора.

Для классификации и упрощения работы, пользовательские GROK паттерны помещаются в группы.

Работа с пользовательскими GROK паттернами включает в себя следующие процессы:

- Управление группами GROK;
- Управление паттернами GROK.

Список GROK паттернов, используемых в **Платформе Радар** по умолчанию, приведен в разделе «Системные GROK паттерны».

2.7.2 Группы GROK

Для упрощения управления и каталогизации пользовательских GROK паттернов используются группы GROK.

Работа с группами GROK включает в себя следующие процессы:

1. «Создание группы паттернов».
2. «Редактирование группы GROK паттернов».

3. «Импорт групп GROK паттернов».
4. «Экспорт групп GROK паттернов».
5. «Удаление группы GROK паттернов».

Для работы с группами GROK перейдите в раздел **Источники → Группы GROK** (см. «Рис. 26»).

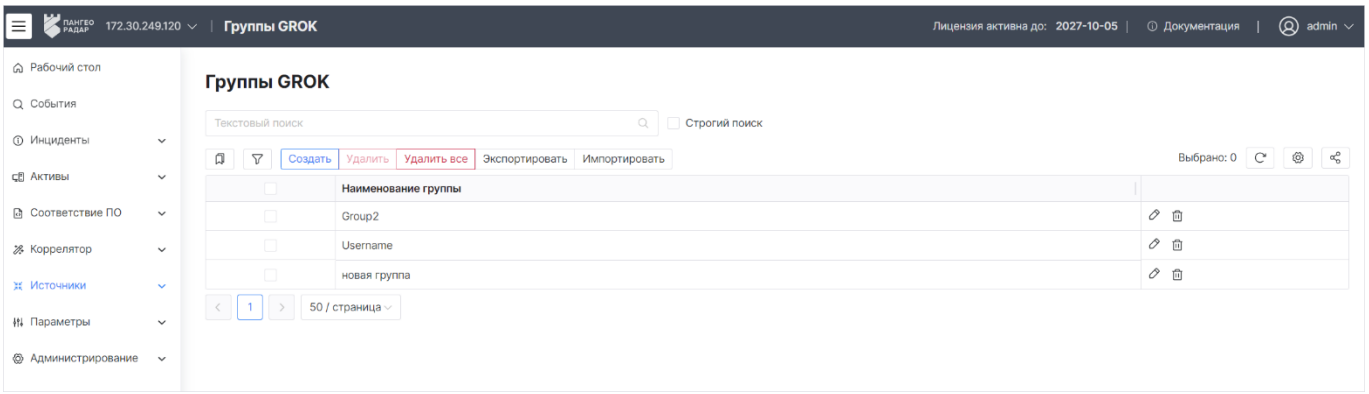


Рис. 26 – Раздел "Группы GROK"

2.7.2.1 Создание группы паттернов

1. Нажмите кнопку **Создать**. Откроется форма "Создание группы GROK паттернов" (см. «Рис. 27»).

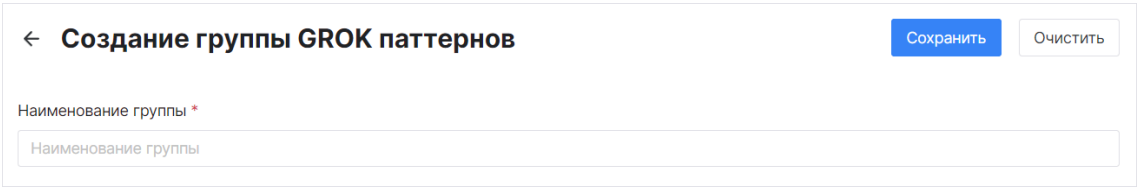


Рис. 27 – Форма "Создание группы GROK паттернов"

2. В поле **Наименование группы** укажите название группы.
3. Нажмите кнопку **Сохранить**.

2.7.2.2 Редактирование группы GROK паттернов

1. Нажмите кнопку  в строке нужной группы.
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

2.7.2.3 Импорт групп GROK паттернов

1. Нажмите кнопку **Импортировать**.
2. В открывшемся укажите путь к архиву с группами паттернов.
3. Нажмите кнопку **Открыть**.

2.7.2.4 Экспорт групп GROK паттернов

Для экспорта конкретных групп, установите нужные флаги и нажмите кнопку **Экспортировать**.

Для экспорта всех групп GROK паттернов нажмите кнопку **Экспортировать все**.

Будет сформирован архив с группами GROK паттернов в формате `.zip`. В открывшемся окне нажмите кнопку **Скачать** и укажите путь для сохранения архива.

2.7.2.5 Удаление группы GROK паттернов

Для удаления группы GROK паттернов нажмите кнопку в соответствующей строке.

Для удаление всех групп GROK паттернов нажмите кнопку **Удалить все**.

Для удаления конкретных групп установите нужные флаги и нажмите кнопку **Удалить**.

2.7.3 Паттерны GROK

Платформа Радар позволяет создать свой набор GROK паттернов для использования их в правилах разбора.

Работа с GROK паттернами включает в себя следующие процессы:

1. «Создание GROK паттерна».
2. «Редактирование GROK паттерна».
3. «Активация GROK паттерна».
4. «Импорт GROK паттернов».
5. «Экспорт GROK паттернов».
6. «Удаление GROK паттернов».

Для работы с GROK паттернами перейдите в раздел **Источники → Паттерны GROK** (см. «Рис. 28»).

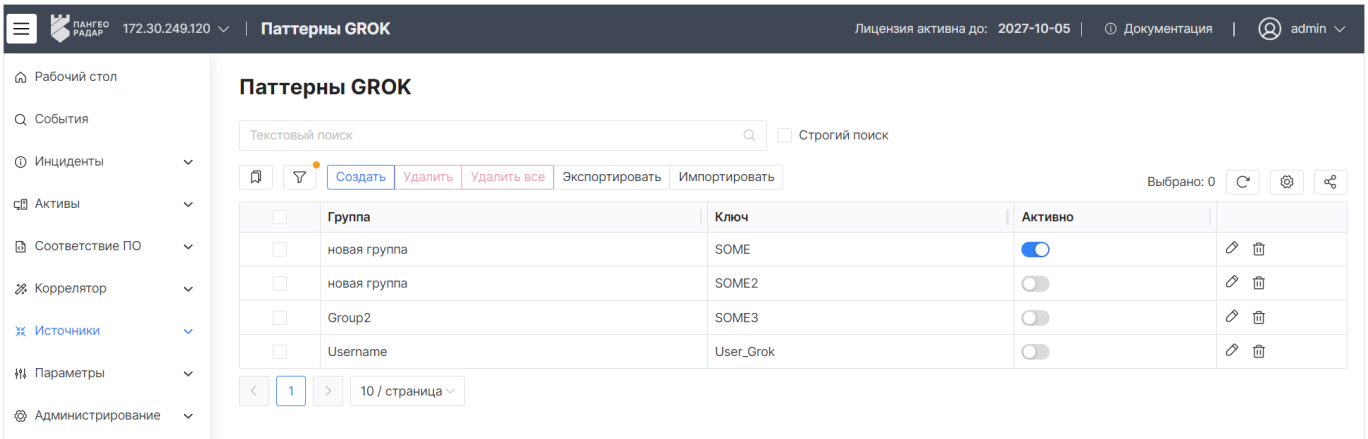


Рис. 28 – Раздел "Паттерны GROK"

2.7.3.1 Создание GROK паттерна

1. Нажмите кнопку **Создать**. Откроется форма "Создание паттерна GROK" (см. «Рис. 29»).

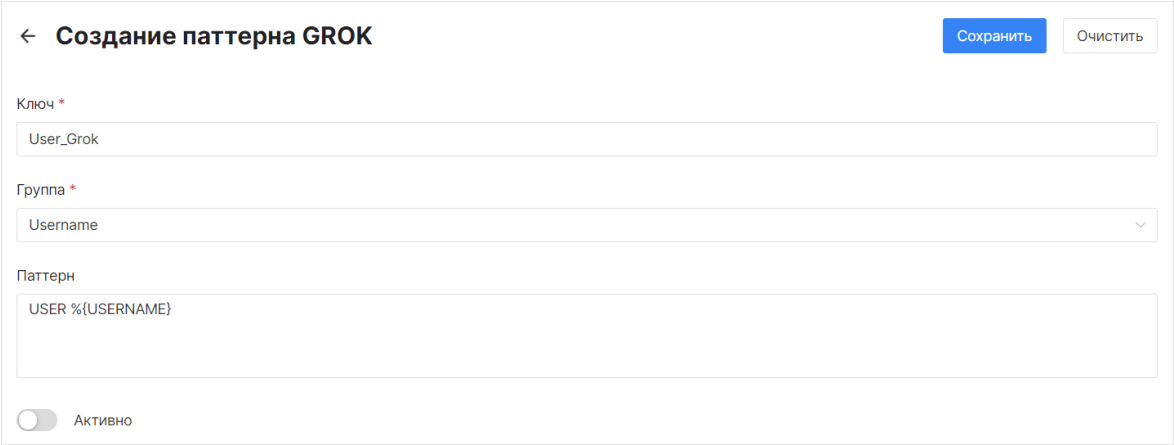


Рис. 29 – Форма "Создание паттерна GROK"

2. Укажите в окне следующую информацию:
    - в поле **Ключ** укажите уникальное наименование GROK паттерна. Данное наименование будет являться ключом при добавлении паттерна в правило разбора;
    - в поле **Группа** из выпадающего списка выберите группу GROK;
    - в поле **Паттерн** укажите тело GROK паттерна;
    - для активации GROK паттерна в поле **Активно** измените соответствующий переключатель на состояние "Включен".
3. Нажмите кнопку **Сохранить**.

2.7.3.2 Редактирование GROK паттерна

1. Нажмите кнопку  в строке нужного GROK паттерна.
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

2.7.3.3 Активация GROK паттерна

Чтобы использовать пользовательский GROK паттерн при настройке правила разбора, его необходимо активировать.

Для активации GROK паттернов в графе **Активно** измените соответствующие переключатели на состояние "Включен".

2.7.3.4 Импорт GROK паттернов

1. Нажмите кнопку **Импортировать**.
2. В открывшемся укажите путь к архиву с GROK паттернами.
3. Нажмите кнопку **Открыть**.

2.7.3.5 Экспорт GROK паттернов

Для экспорта конкретных GROK паттернов, установите нужные флаги и нажмите кнопку **Экспортировать**.

Для экспорта всех GROK паттернов нажмите кнопку **Экспортировать все**.

Будет сформирован архив с GROK паттернами в формате `.zip`. В открывшемся окне нажмите кнопку **Скачать** и укажите путь для сохранения архива.

2.7.3.6 Удаление GROK паттернов

Для удаления GROK паттерна нажмите кнопку в соответствующей строке.

Для удаление всех GROK паттернов нажмите кнопку **Удалить все**.

Для удаления конкретных GROK паттернов установите нужные флаги и нажмите кнопку **Удалить**.

2.7.4 Системные GROK паттерны

В разделе приведен список используемых в **Платформе Радар** GROK паттернов по умолчанию.

2.7.4.1 Основные (General)

№	Паттерн	Тип реализации
1	USERNAME	`[a-zA-Z0-9._-]+`
2	USER	`%{USERNAME}`
3	INT	`(?:[+-]?(?:[0-9]+))`
4	BASE10NUM	`(?<![0-9.+-])(?>[+-]?(?:(?:[0-9]+(?:\.[0-9]+)?)|(?:\.[0-9]+)))`
5	NUMBER	`(?:%{BASE10NUM})`
6	BASE16NUM	`(?<![0-9A-Fa-f])(?:[+-]?(?:0x)?(?:[0-9A-Fa-f]+))`
7	BASE16FLOAT	`\b(?<![0-9A-Fa-f.])(?:[+-]?(?:0x)?(?:(?:[0-9A-Fa-f]+(?:\.[0-9A-Fa-f]*)?)|(?:\.[0-9A-Fa-f]+)))\b`
8	POSINT	`\b(?:[1-9][0-9]*)\b`
9	NONNEGINT	`\b(?:[0-9]+)\b`
10	WORD	`\b\w+\b`
11	NOTSPACE	`\S+`
12	SPACE	`\s*`
13	DATA	`.*?`
14	GREEDYDATA	`.*`
15	QUOTEDSTRING	`(?>(?<!\\)(?>"(?>\\.|[^\\"]+)+"|""|(?>'(?>\\.|[^\\']+)+')|''|(?>`(?>\\.|[^\\`]+)+`)|``))

№	Паттерн	Тип реализации
16	UUID	`[A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}`

2.7.4.2 Локальная сеть (Networking)

№	Паттерн	Тип реализации
1	MAC	`(?:%{CISCOMAC}|%{WINDOWSMAC}|%{COMMONMAC})`
2	CISCOMAC	`(?:(?:[A-Fa-f0-9]{4}\.){2}[A-Fa-f0-9]{4})`
3	WINDOWSMAC	`(?:(?:[A-Fa-f0-9]{2}-){5}[A-Fa-f0-9]{2})`
4	COMMONMAC	`(?:(?:[A-Fa-f0-9]{2}:){5}[A-Fa-f0-9]{2})`
5	IPV6	`((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?`
6	IPV4	`(?<![0-9])(?:(?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]{1,2})[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]{1,2})[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]{1,2})[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]{1,2}))(?![0-9])`
7	IP	`(?:%{IPV6}|%{IPV4})`
8	HOSTNAME	`\b(?:[0-9A-Za-z][0-9A-Za-z-]{0,62})(?:\.(?:[0-9A-Za-z][0-9A-Za-z-]{0,62}))*(\.?|\b)`
9	HOST	`%{HOSTNAME}`
10	IPORHOST	`(?:%{HOSTNAME}|%{IP})`
11	HOSTPORT	`%{IPORHOST}:%{POSINT}`

2.7.4.3 Пути (Paths)

№	Паттерн	Тип реализации

№	Паттерн	Тип реализации
1	PATH	`(?:%{UNIXPATH}|%{WINPATH})`
2	UNIXPATH	`(?>/(?>[\w_%!$@:.,-]+|\\.)*)+`
3	TTY	`(?:/dev/(pts|tty([pq])?)(\w+)?/?(?:[0-9]+))`
4	WINPATH	`(?>[A-Za-z]+:|\\)(?:\\[^\\?*]*)+`
5	URIPROTO	`[A-Za-z]+(\+[A-Za-z+]+)?`
6	URIHOST	`%{IPORHOST}(?::%{POSINT:port})?`
7	URIPATH	`(?:/[A-Za-z0-9$.+!*'(){},~:;=@#%_\-]*)+`
8	URIPARAM	`\?[A-Za-z0-9$.+!*'|(){},~@#%&/=:;_?\-\[\]]*`
9	URIPATHPARAM	`%{URIPATH}(?:%{URIPARAM})?`
10	URI	`%{URIPROTO}://(?:%{USER}(?::[^@]*)?@)?(?:%{URIHOST})?(?:%{URIPATHPARAM})?`

2.7.4.4 Месяцы (Months)

Пример написания: `January, Feb, 3, 03, 12, December`.

№	Паттерн	Тип реализации
1	MONTH	`\b(?:Jan(?:uary)?|Feb(?:ruary)?|Mar(?:ch)?|Apr(?:il)?|May|Jun(?:e)?|Jul(?:y)?|Aug(?:ust)?|Sep(?:tember)?|Oct(?:ober)?|Nov(?:ember)?|Dec(?:ember)?)\b`
2	MONTHNUM	`(?:0?[1-9]|1[0-2])`
3	MONTHNUM2	`(?:0[1-9]|1[0-2])`
4	MONTHDAY	`(?:(?:0[1-9])|(?:[12][0-9])|(?:3[01])|[1-9])`

2.7.4.5 Дни (Days)

Пример написания: `Monday, Tue, Thu` и т.д.

№	Паттерн	Тип реализации
1	MONTH	`(?:Mon(?:day)?|Tue(?:sday)?|Wed(?:nesday)?|Thu(?:rsday)?|Fri(?:day)?|Sat(?:urday)?|Sun(?:day)?)`

2.7.4.6 Годы (Years)

№	Паттерн	Тип реализации
1	YEAR	`(?>\d\d){1,2}`
2	HOUR	`(?:2[0123]|[01]?[0-9])`
3	MINUTE	`(?:[0-5][0-9])`
4	SECOND	`(?:(?:[0-5]?[0-9]|60)(?:[:.,][0-9]+)?)`
5	TIME	`(?!<[0-9])%{HOUR}:%{MINUTE}(?::%{SECOND})(?![0-9])`
6	DATE_US	`%{MONTHNUM}[/-]%{MONTHDAY}[/-]%{YEAR}`
7	DATE_EU	`%{MONTHDAY}[./-]%{MONTHNUM}[./-]%{YEAR}`
8	ISO8601_TIMEZONE	`(?:Z|[+-]%{HOUR}(?::?%{MINUTE}))`
9	ISO8601_SECOND	`(?:%{SECOND}|60)`
10	TIMESTAMP_ISO8601	`%{YEAR}-%{MONTHNUM}-%{MONTHDAY}[T ]%{HOUR}:?%{MINUTE}(?::?%{SECOND})?%{ISO8601_TIMEZONE}?`
11	DATE	`%{DATE_US}|%{DATE_EU}`
12	DATESTAMP	`%{DATE}[- ]%{TIME}`
13	TZ	`(?:[PMCE][SD]T|UTC)`
14	DATESTAMP_RFC822	`%{DAY} %{MONTH} %{MONTHDAY} %{YEAR} %{TIME} %{TZ}`
15	DATESTAMP_RFC2822	`%{DAY}, %{MONTHDAY} %{MONTH} %{YEAR} %{TIME} %{ISO8601_TIMEZONE}`
16	DATESTAMP_OTHER	`%{DAY} %{MONTH} %{MONTHDAY} %{TIME} %{TZ} %{YEAR}`
17	DATESTAMP_EVENTLOG	`%{YEAR}%{MONTHNUM2}%{MONTHDAY}%{HOUR}%{MINUTE}%{SECOND}`

2.7.4.7 Даты Syslog (Syslog Dates)

№	Паттерн	Тип реализации
1	SYSLOGTIMESTAMP	`%{MONTH} +%{MONTHDAY} %{TIME}`
2	PROG	`(?:[\w._/%-]+)`
3	SYSLOGPROG	`%{PROG:program}(?:\[%{POSINT:pid}\])?`

№	Паттерн	Тип реализации
4	SYSLOGHOST	`%{IPORHOST}`
5	SYSLOGFACILITY	`<%{NONNEGINT:facility}.%{NONNEGINT:priority}> HTTPDATE %{MONTHDAY}/%{MONTH}/%{YEAR}:%{TIME} %{INT}`

2.7.4.8 Кратчайшие пути (Shortcuts)

№	Паттерн	Тип реализации
1	QS	`%{QUOTEDSTRING}`

2.7.4.9 Форматы журналов (Log formats)

№	Паттерн	Тип реализации
1	SYSLOGBASE	`%{SYSLOGTIMESTAMP:timestamp} (?:%{SYSLOGFACILITY} )?%{SYSLOGHOST:logsource} %{SYSLOGPROG}:`
2	COMMONAPACHELOG	`%{IPORHOST:clientip} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb} %{NOTSPACE:request}(?: HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})" %{NUMBER:response} (?:%{NUMBER:bytes}|-)`
3	COMBINEDAPACHELOG	`%{COMMONAPACHELOG} %{QS:referrer} %{QS:agent}`

2.7.4.10 Уровни журналирования (Log Levels)

№	Паттерн	Тип реализации
1	LOGLEVEL	`([Aa]lert|ALERT|[Tt]race|TRACE|[Dd]ebug|DEBUG|[Nn]otice|NOTICE|[Ii]nfo|INFO|[Ww]arn?(?:ing)?|WARN?(?:ING)?|[Ee]rr?(?:or)?|ERR?(?:OR)?|[Cc]rit?(?:ical)?|CRIT?(?:ICAL)?|[Ff]atal|FATAL|[Ss]ever e|SEVERE|EMERG(?:ENCY)?|[Ee]merg(?:ency)?)`

2.8 Поля события

Внимание! *После запуска **Платформы Радар** в боевом режиме, изменение полей событий потребует переиндексации всей базы данных структуры хранения. Крайне не рекомендуется менять настроенные параметры полей событий, если платформа работает в боевом режиме*.

Платформа Радар позволяет управлять полями события (таксономии), используемых в процессах разбора и нормализации.

Маппинг – это карта полей нормализованного или распаршенного события.

Список предустановленных полей, используемых при нормализации, приведен в разделе **Источники → Поля события** .

В таксономии (маппинг полей) используется 3 типа полей:

- `datetime` – для полей хранения времени;
- `keyword` – все остальные поля;

- `group` – для верхне-уровневых полей в иерархии. Например, поле `event` является группой, содержащей поля `event.id`, `event.alert`, `event.anomaly`.

Поле события может принадлежать к следующим шаблонам:

- Разобрано;
- Нормализовано;
- Ошибка.

Работа с полями событий включает в себя следующие процессы:

1. «Просмотр поля события».
2. «Создание поля события».
3. «Редактирование поля события».
4. «Объединение полей события в группы».
5. «Удаление поля события».

Для работы с полями события перейдите в раздел **Источники → Поля события** (см. «Рис. 30»).

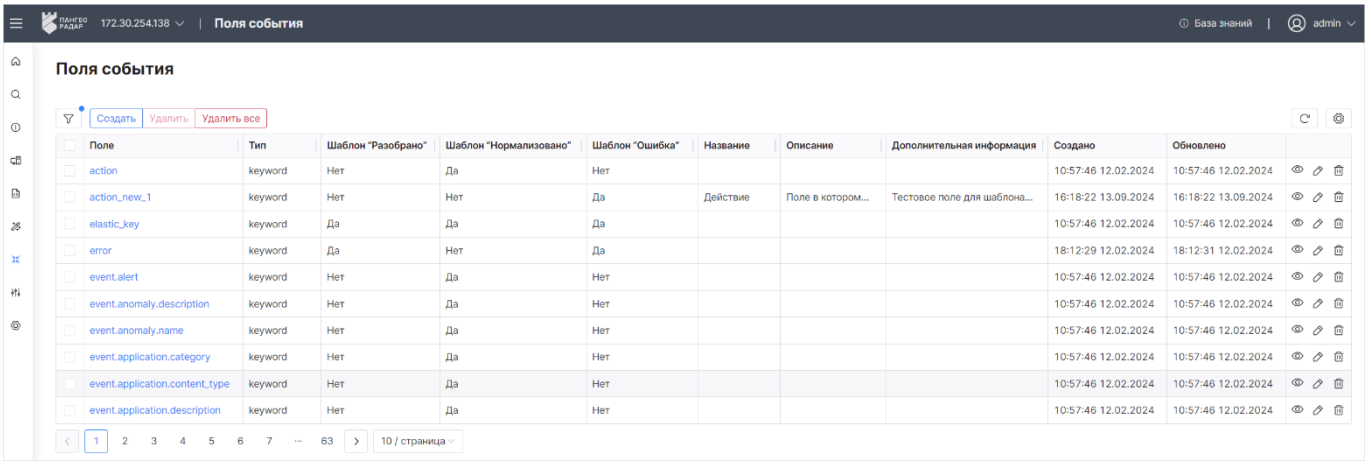


Рис. 30 – Раздел "Поля события"

В разделе отображается следующая информация о полях события:

- **Поле** – уникальный ключ поля, используемый при нормализации;
- **Тип** – тип поля: datetime, keyword, group;
- **Шаблон "Разобрано"** – признак принадлежности поля к шаблону "Разобрано";
- **Шаблон "Нормализовано"** – признак принадлежности поля к шаблону "Нормализовано";
- **Шаблон "Ошибка"** – признак принадлежности поля к шаблону "Ошибка";
- **Название** – наименование поля;
- **Описание** – описание поля;
- **Дополнительная информация** – дополнительные сведения о поле;
- **Создано** – дата и время создания поля;
- **Обновлено** – дата и время обновления поля.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
	просмотр поля события
	редактирование информации о поле события
	удаление поля события

2.8.1 Просмотр поля события

Открыть поле события на просмотр можно двумя способами:

- нажмите кнопку  ;
- по ссылке в графе "Поле".

Откроется форма просмотра поля события (см. «Рис. 31»).

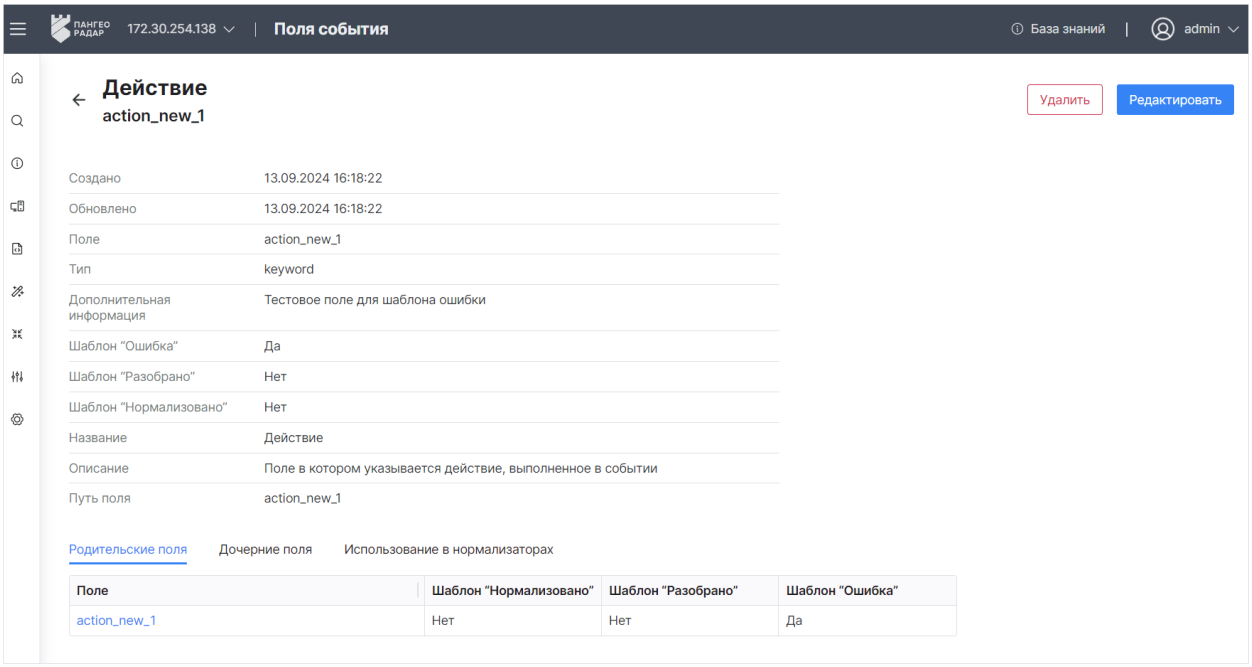


Рис. 31 – Форма "Просмотр поля события"

Помимо общей информации о поле события на форме отображается следующая информация:

- Информация о родительском поле. По ссылке произойдет переход к просмотру родительского поля;
- Информация о дочерних полях. По ссылке произойдет переход к просмотру дочернего поля;
- Информация об использовании поля в нормализаторах.

2.8.2 Создание поля события

1. Нажмите кнопку **Создать**. Откроется форма "Создание поля события" (см. Рис. 32).

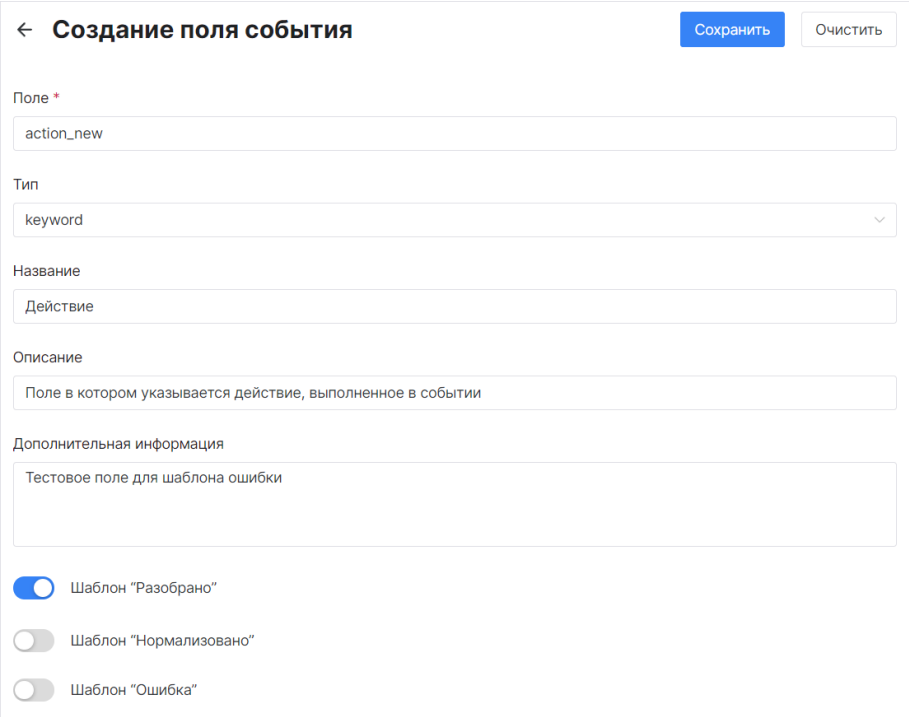


Рис. 32 – Форма "Создание поля события"

2. Укажите на форме следующую информацию:
    - в поле **Поле** укажите уникальный ключ поля. Допускается указывать ключ только на английском языке. Указанный ключ должен быть уникальным в рамках платформы;
    - в поле **Тип** из выпадающего списка выберите тип поля;
    - в поле **Название** укажите название поля;
    - в поле **Описание** укажите описание поля;
    - в поле **Дополнительная информация** укажите дополнительные сведения о поле;
    - укажите принадлежность поля к шаблонам, включив соответствующие переключатели.
3. Нажмите кнопку **Сохранить**.

2.8.3 Редактирование поля события

1. Выберите из списка необходимое поле и нажмите кнопку .
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

2.8.4 Объединение полей события в группы

Поля события можно объединить в группы с помощью типа group. Объединение выполняется по следующем принципу:

1. Создается поле, например `test`.
2. Полю присваивается тип `group`.
3. Затем создается поле, например `test.[наименование дочернего поля]`.

4. Поле `test` автоматически назначается родительским полем, а созданное - дочерним.

2.8.5 Удаление поля события

Для удаления поля нажмите кнопку в соответствующей строке.

Для удаление всех записей нажмите кнопку **Удалить все**.

Для удаления конкретных записей таблицы установите нужные флаги и нажмите кнопку **Удалить**.

2.9 Справочные материалы

2.9.1 Получение сырого события

Сырое событие – это событие, поступившее от источника в сервис KAFKA и еще не прошедшее процедуру разбора.

Пример сырого события можно получить следующим способом:

1. Пустите поток событий от нужного источника.
2. Перейдите в раздел **Просмотр событий**.
3. При необходимости примените фильтр для показа событий от нужного источника.
4. В поле **raw** будет содержаться сырое событие.
5. Для удобства сырое событие из поля **raw** продублировано сразу под графиком потока события и есть возможность скопировать его по соответствующей кнопке (см. «Рис. 33»).

Рис. 33 – Получение сырого события

2.9.2 Механизмы разбора

Данный раздел используется как справочный материал по работе в разделе **Источники** → **Правила разбора**.

В **Платформе Радар** для выполнения процедуры разбора событий, поступающих от источников, используются следующие механизмы:

- «GROK паттерн»;
- «CEF»;
- «EXECVE»;
- «Ключ значение»;
- «CSV»;
- «SYSLOG»;
- «XML»;
- «JSON»;
- «Функция преобразования».

2.9.2.1 GROK паттерн

GROK паттерны – это именованные регулярные выражения, которые позволяют пользователям сопоставлять конкретные шаблоны в тексте. С их помощью можно быстро идентифицировать и извлекать поля из поступающих событий без необходимости писать сложные регулярные выражения с нуля.

В **Платформе Радар** GROK паттерны делятся на системные и пользовательские. Подробнее см. раздел «GROK паттерны».

GROK паттерн представляет собой шаблон. Синтаксис шаблонов GROK, при использовании следующий:

```
%{SYNTAX:SEMANTIC}
```

где

- `SYNTAX` – имя паттерна, который будет применен;
- `SEMANTIC` – имя объекта (поле, группа), к которому будет применен паттерн.

Пример настройки данного механизма приведен на «Рис. 34».

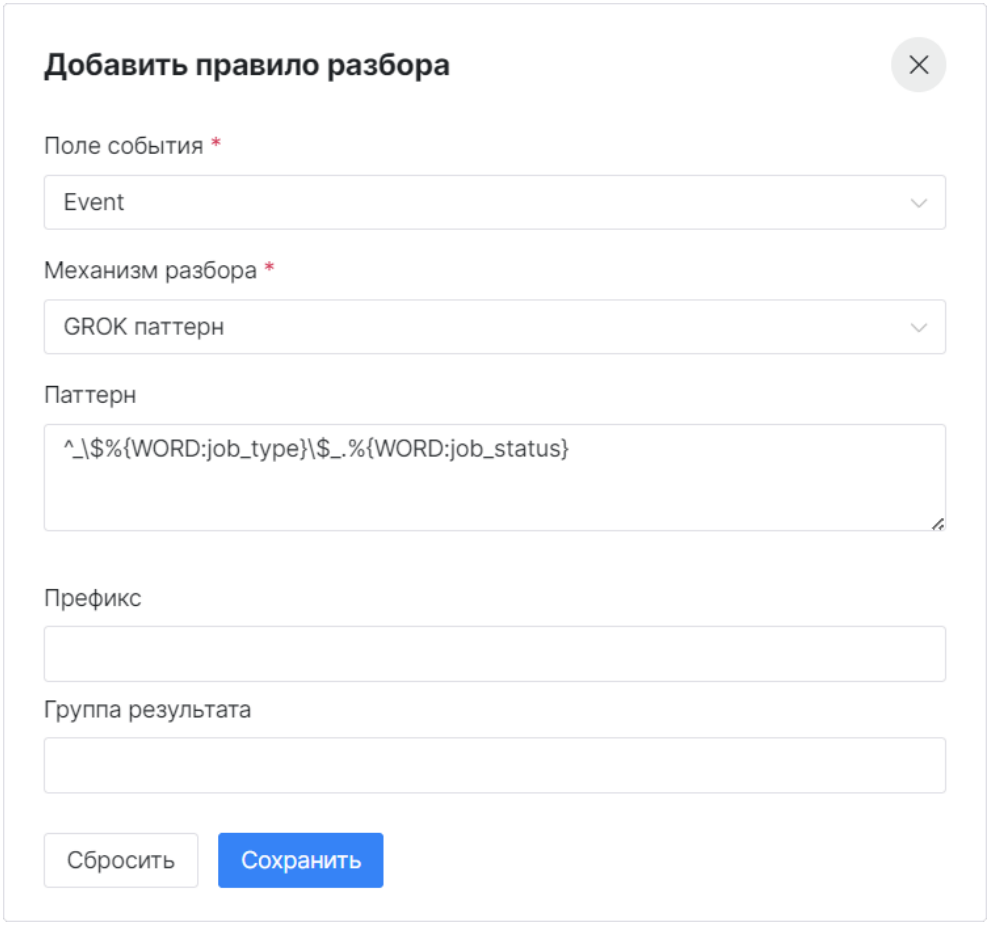


Рис. 34 – Добавление правила разбора. Механизм "GROK паттерн"

Для настройки механизма в поле **Паттерн** укажите GROK паттерн. Для использования пользовательских или системных GROK паттернов введите символ {, откроется список ключей поддерживаемых GROK паттернов. Сначала будут выведены пользовательские, а затем – системные.

Пример работы:

Сырое событие:


```
{"Message":"<7>          7/26/2023          2:39:42          PM          pgr-1c-00
{\"Event\":{\"Level\":\"Information\",\"Date\":\"2023-07-
26T14:39:42\",\"ApplicationName\":\"BackgroundJob\",\"ApplicationPresentation\":\
"Background     job\",\"Event\":\"_$Data$_.Update\",\"EventPresentation\":\"Data.
Change\",\"User\":\"00000000-0000-0000-0000-
000000000000\",\"UserName\":\"\",\"Computer\":\"\",\"Metadata\":\"Константа.После
днееОбновлениеДоступа\",\"MetadataPresentation\":\"Constant. Последнее обновление
доступа\",\"Comment\":null,\"Data\":\"something        Команда:        Выполнить
обновление\",\"DataPresentation\":\"\",\"TransactionStatus\":\"Committed\",\"Tran
sactionID\":\"7/26/2023                          2:39:42                          PM
(2934007)\",\"Connection\":\"3\",\"Session\":\"34\",\"ServerName\":\"\",\"Port\":
\"\",\"SyncPort\":\"0\"}}","a":"a7e42e20-03a1-4998-a301-
c97fa77cbe73","a_c":"","a_src_ip":"172.30.250.141","a_src_o":"445","a_src_r":"smb
","a_src_t":[],"a_ts":"2024-10-21T12:41:44.993Z"}
```


Поле сырого события, к которому будет применен GROK паттерн:

```
\"Event\":\"_$Data$_.Update\"
```

Применяемый GROK паттерн:

```
^_\$%{WORD:job_type}\$_.%{WORD:job_status}
```

Результат работы приведен на «Рис. 35».

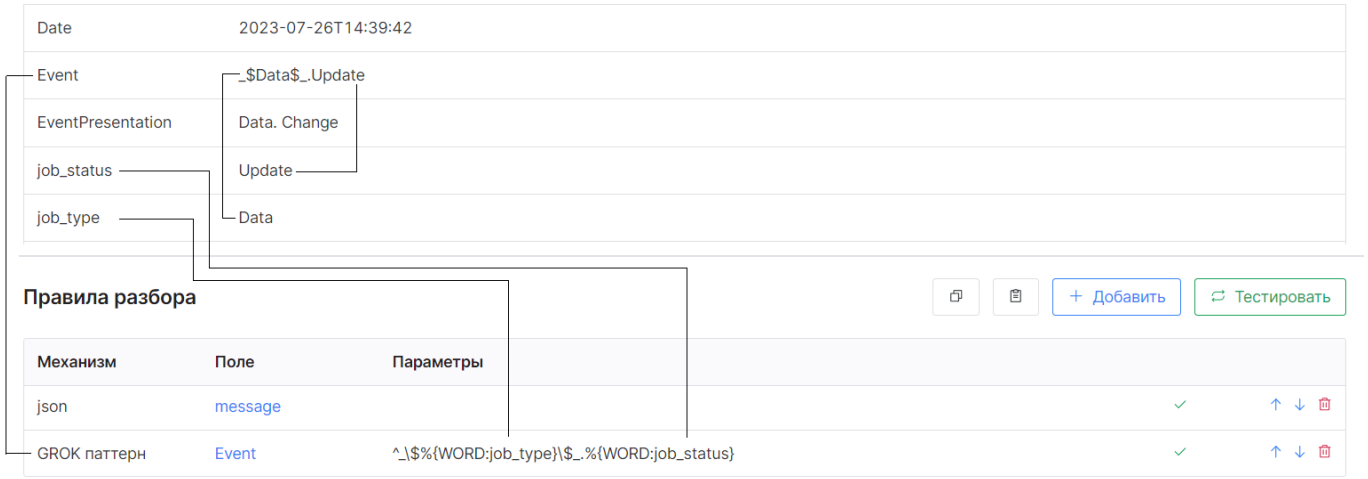


Рис. 35 – Пример работы механизма "GROK паттерн"

2.9.2.2 CEF

Общий формат событий (Common Event Format (CEF)) – это расширяемый текстовый формат, предназначенный для поддержки нескольких типов устройств, предлагая наиболее актуальную информацию.

Синтаксис сообщений сокращен для работы с нормализацией ESM. CEF специально определяет синтаксис для записей журнала, содержащих стандартный заголовок и расширение переменной, отформатированные как пары "Ключ-Значение". Формат CEF может использоваться с локальными устройствами и с поставщиками облачных услуг.

При использовании данного механизма при создании правил разбора дополнительных настроек не требуется.

2.9.2.3 EXECVE

Данный механизм будет разбирать тип событий EXECVE от auditd для Unix систем.

Пример настройки данного механизма приведен на рисунке 3.

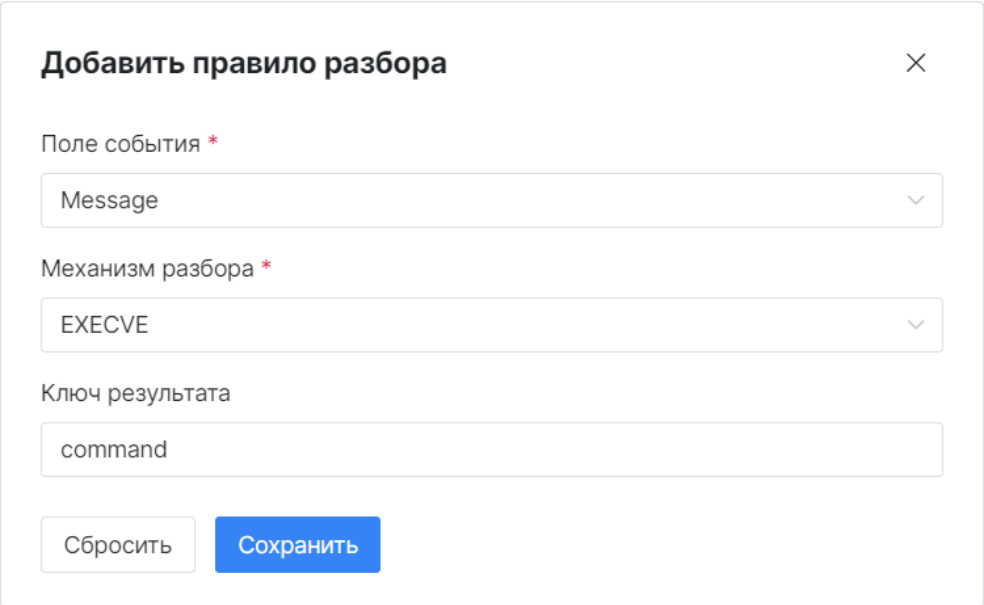


Рис. 36 – Добавление правила разбора. Механизм "EXECVE"

Пример события в формате EXECVE имеет следующий вид:

```
{"b_ts":"2025-10-14T11:18:26.000+03:00","a_m":"2671","Message":"<190>Oct 14 11:18:26
deb12-auditd audit: node=172.30.250.165 type=EXECVE msg=audit(1760435954.705:104635):
argc=2                                                    a0="/usr/bin/printf"
a1=D0A2D0B5D181D182D0BED0B2D0B0D18F5FD181D182D180D0BED0BAD0B05C6E","a":"c2795d7b-
1415-47bc-be88-
4bf922a0b362","a_c":"","a_src_ip":"172.30.250.165","a_src_o":"37983","a_src_r":"udp_i
nput","a_src_t":[],"a_ts":"2025-10-14T08:18:26.211Z"}
```

Для описания примера работы механизма разбора возьмем часть:

```
a0="/usr/bin/printf"
a1=D0A2D0B5D181D182D0BED0B2D0B0D18F5FD181D182D180D0BED0BAD0B05C6E"
```

Механизм разбора выполнит следующие действия:

1. Извлечет все параметры a0, a1, a2 и т.д.
2. Применит механизм **Hex to text** к каждому полю, которое не имеет кавычек в значении:

   ```
   a0="/usr/bin/printf"

   a1=D0A2D0B5D181D182D0BED0B2D0B0D18F5FD181D182D180D0BED0BAD0B05C6E" --> Hex to
   text: Тестовая_строка\n
   ```

3. Последовательно склеит через пробел все полученные поля и выведет в таксономию. Итоговый результат преобразования:

   ```
   node=<ip-адрес узла платформы> type=EXECVE msg=audit(a0="/usr/bin/printf"
   a1=D0A2D0B5D181D182D0BED0B2D0B0D18F5FD181D182D180D0BED0BAD0B05C6E"):
   a0="/usr/bin/printf" a1="Тестовая_строка\n"
   ```

2.9.2.4 Ключ значение

Данный механизм будет разбирать пришедшее поле на пары "Ключ-Значение" в соответствии с заданными параметрами.

Пример настройки данного механизма приведен на «Рис. 37».

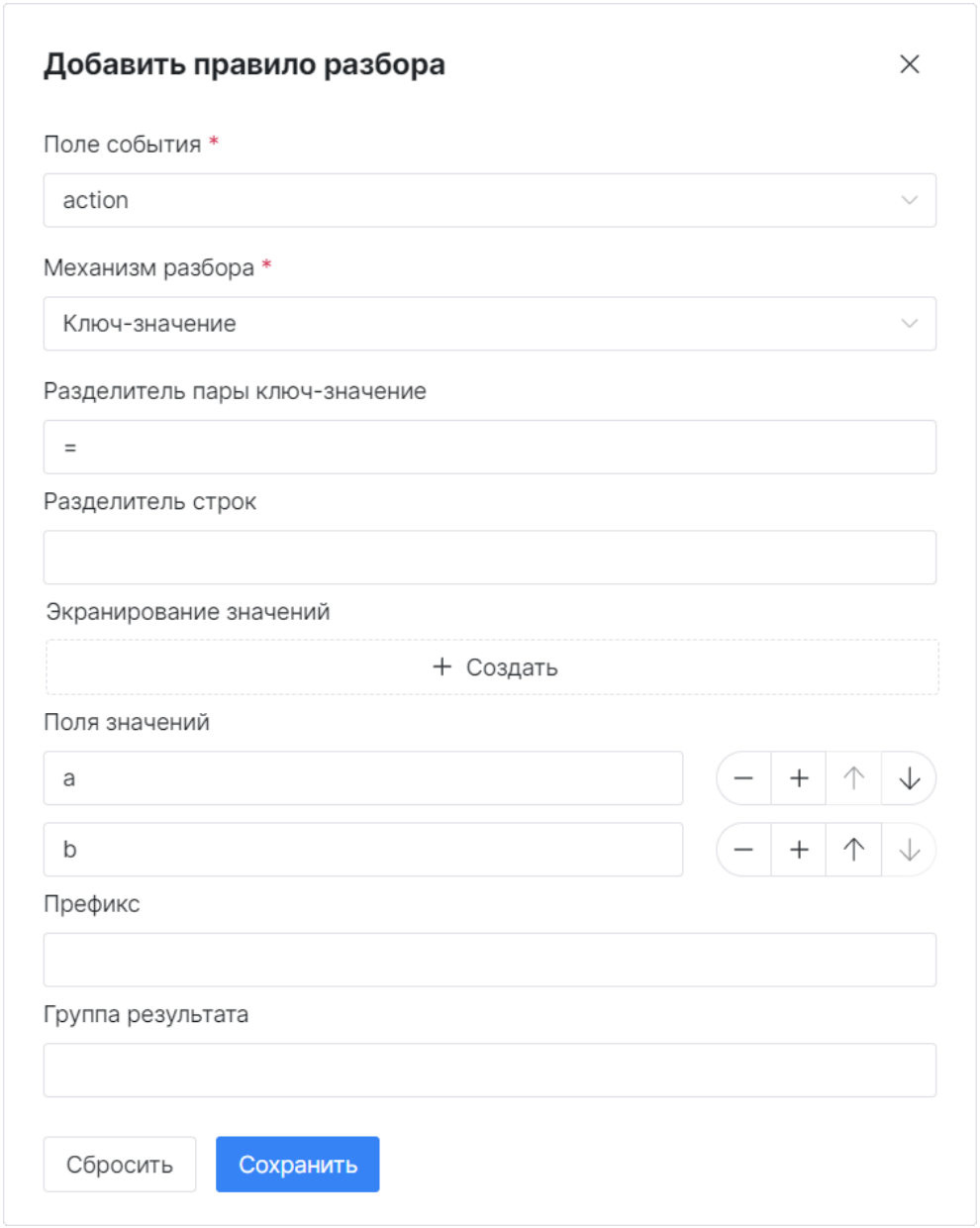


Рис. 37 – Добавление правила разбора. Механизм "Ключ-Значение"

Для настройки механизма разбора "Ключ-Значение" указывается следующая информация:

- **Разделитель пары "Ключ-Значение"** – укажите символ, который будет являться разделителем пары "Ключ-Значение". Например:

```
Приходящая пара "Ключ-Значение":
"a":"1"
Разделитель пары "="
Результат:
a=1
```

- **Разделитель строк** – укажите символ, который будет являться разделителем строк. Например:

```
Приходящие пары Ключ-Значение:
"a":"1" "b":"2"
Разделитель строк ","
Результат:
a=1,b=2
```

Примечание: если оставить поле пустым, то в качестве разделителя строк будет использоваться "перенос строки".

- **Экранирование значений** – задается последовательный набор символов, которые будут стоять перед каждым значением в паре и после него;
- **Поля значений**. Задается последовательный список, по которому будут переопределяться "ключи" из пары "Ключ-Значение". Например:

```
Приходящие пары Ключ-Значение:
"a":"1" "b":"2"

Поля значений:
value_1
value_2
value_3

Результат:
value_1=1
value_2=2

value_3 - поле применено не будет, так как пришло всего две пары "Ключ-Значение"
```

Пример работы механизма разбора приведен на «Рис. 38».

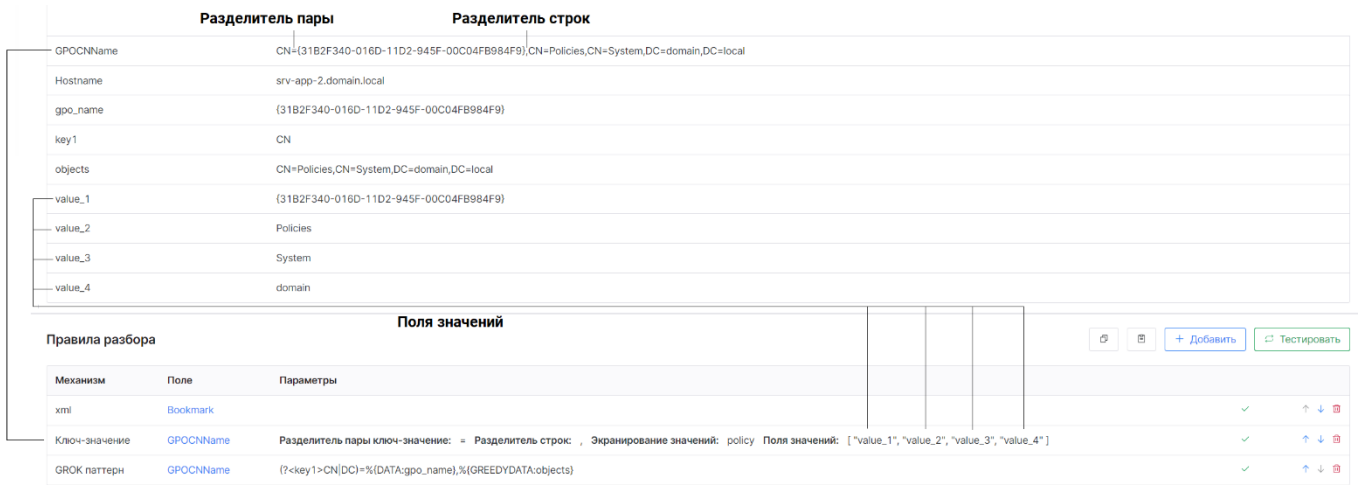


Рис. 38 – Пример работы механизма разбора "Ключ-Значение"

2.9.2.5 CSV

Механизм используется в случае, если в поле сырого события вложены данные в формате CSV.

Механизм работает и настраивается аналогично механизму «Ключ значение».

2.9.2.6 SYSLOG

Если источником событий является «ОС семейства Unix», то с наибольшей вероятностью события будут журналироваться одной из следующих служб:

- rsyslog;
- syslog-ng;
- auditd.

Если используются данные механизмы журналирования, то для разбора событий рекомендуется использовать механизм SYSLOG.

Для создания правила разбора, с использованием данного механизма, дополнительных настроек не требуется.

Пример сырого события от ОС Linux:


```
{"a_src_ip":"172.30.249.201","a_src_o":"2671","a_c":"","a_src_t":[""],"a_src_r":
"","a_ts":"2024-09-25T10:09:51.088.088144459+00:00","a":"a1a1795a-6a18-4345-
9020-77723a724d38","Message":"<22>Sep 18 16:55:01 v-stand-05 audispd:
node=172.30.254.95 type=EXECVE msg=audit(1663937111.702:73702361): argc=5
a0=\"ps\" a1=\"-o\" a2=\"rss=\" a3=\"-p\" a4=\"1736\""}
```


Пример успешного применения механизма разбора, примененного к полю **Message** сырого события, приведено на «Рис. 39».

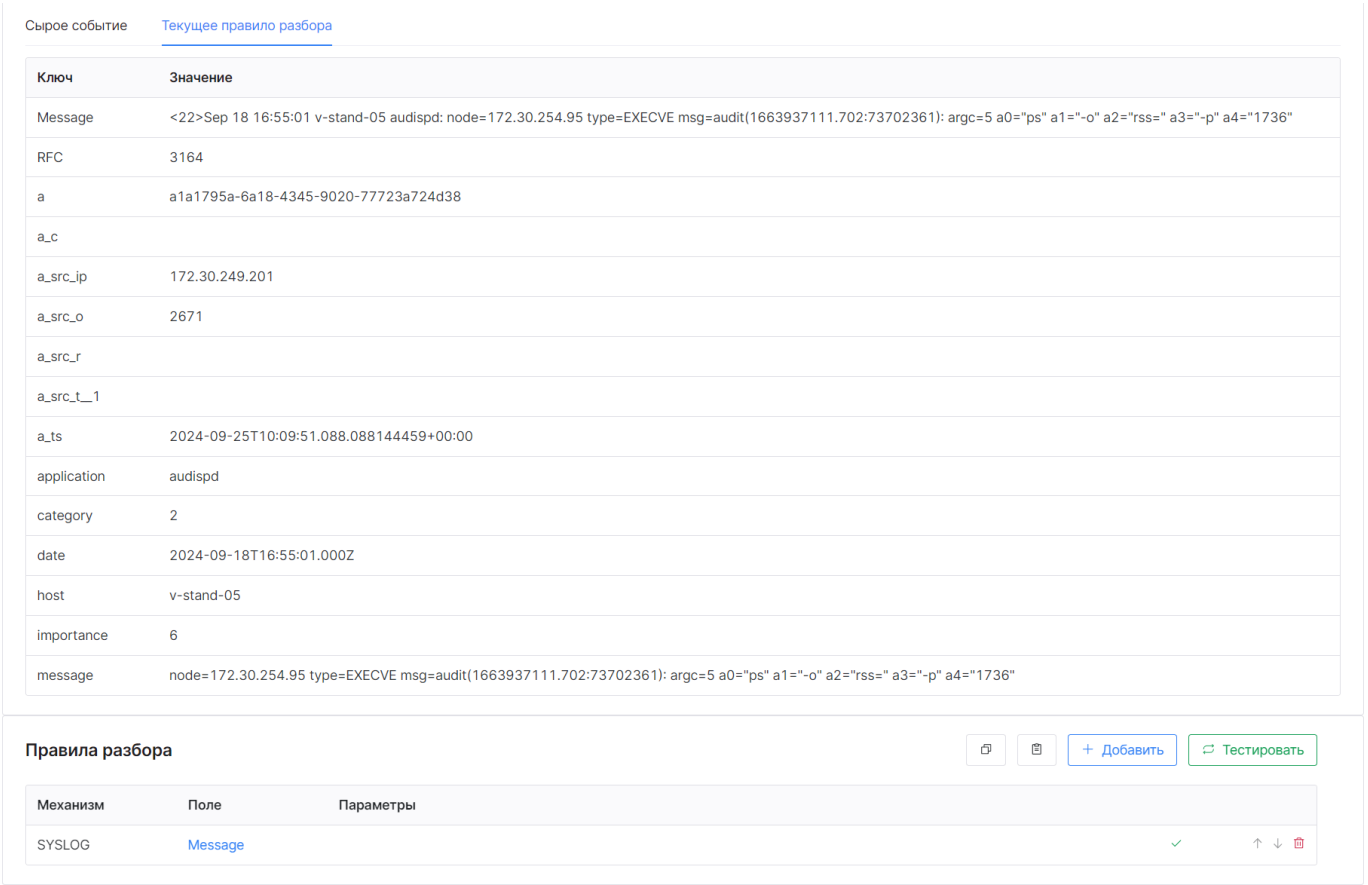


Рис. 39 – ***Пример работы механизма разбора "SYSLOG"***

2.9.2.7 XML

Механизм используется в случае, если в поле сырого события вложено XML-выражение.

При использовании данного механизма при создании правил разбора дополнительных настроек не требуется.

Особенностью данного механизма является то, что XML может быть вложенный, то есть в ключ может быть вложен ключ, в который также вложен ключ.

Результатом применения данного механизма будет ключ следующего вида:

```
"Ключ первого уровня"__"Ключ второго уровня"__"Ключ n-уровня"="Значение"
```

Пример события со вложенными ключами:


```
{"a_src_ip":"172.30.249.201","a_src_o":"1217","a_c":"","a_src_t":[""],"a_src_r":"",
"a_ts":"2024-09-13T14:09:12.731.731790640+00:00","a":"fdf1c240-ecfe-4d76-9ac9-
0d2c315b744c","Message":"{\"AccountDomain\":\"IMG-
WIN2019\",\"AccountName\":\"Administrator\",\"Bookmark\":\"\",\"Channel\":\"Securit
y\",\"ChannelText\":\"Security\",\"ClientAddress\":\"172.30.253.104\",\"ClientName\
":\"DESKTOP-
FJ5FBMT\",\"EventData\":\"\",\"EventDataErr\":null,\"EventID\":4778,\"EventTime\":\
"2024-08-
14T10:07:28.86689Z\",\"EventType\":\"AUDIT_SUCCESS\",\"ExecutionProcessID\":620,\"H
ostname\":\"img-
win2019\",\"IDText\":\"\",\"Keywords\":null,\"KeywordsRaw\":\"0x8020000000000000\",
\"Level\":0,\"LevelText\":\"Information\",\"LogonID\":\"0x000000000004b543\",\"Msg\
":\"\",\"OpcodeText\":\"Info\",\"OpcodeValue\":0,\"ProviderText\":\"\",\"PublisherH
andleErr\":null,\"Qualifiers\":0,\"RecordID\":17728,\"RenderedFieldsErr\":null,\"Se
ssionName\":\"RDP-Tcp#1\",\"SourceName\":\"Microsoft-Windows-Security-
Auditing\",\"SubscribedChannel\":\"Security\",\"TaskText\":\"\",\"TaskValue\":12551
,\"ThreadID\":680,\"User\":\"\",\"UserData\":\"\",\"Version\":0,\"XML\":\"\\u003cEv
ent
xmlns=\\\"http:\/\/schemas.microsoft.com\/win\/2004\/08\/events\/event\\\"\\u003e\\
u003cSystem\\u003e\\u003cProvider  Name=\\\"Microsoft-Windows-Security-Auditing\\\"
Guid=\\\"54849625-5478-4994-a5ba-
3e3b0328c30d\\\"\/\\u003e\\u003cEventID\\u003e4778\\u003c\/EventID\\u003e\\u003cVer
sion\\u003e0\\u003c\/Version\\u003e\\u003cLevel\\u003e0\\u003c\/Level\\u003e\\u003c
Task\\u003e12551\\u003c\/Task\\u003e\\u003cOpcode\\u003e0\\u003c\/Opcode\\u003e\\u0
03cKeywords\\u003e0x8020000000000000\\u003c\/Keywords\\u003e\\u003cTimeCreated
SystemTime=\\\"2024-08-
14T10:07:28.866890+00:00\\\"\/\\u003e\\u003cEventRecordID\\u003e17728\\u003c\/Event
RecordID\\u003e\\u003cCorrelation          ActivityID=\\\"ee7f716d-ee30-0003-9971-
7fee30eeda01\\\"\/\\u003e\\u003cExecution                  ProcessID=\\\"620\\\"
ThreadID=\\\"680\\\"\/\\u003e\\u003cChannel\\u003eSecurity\\u003c\/Channel\\u003e\\
u003cComputer\\u003eimg-
win2019\\u003c\/Computer\\u003e\\u003cSecurity\/\\u003e\\u003c\/System\\u003e\\u003
cEventData\\u003e\\u003cData
Name=\\\"AccountName\\\"\\u003eAdministrator\\u003c\/Data\\u003e\\u003cData
Name=\\\"AccountDomain\\\"\\u003eIMG-WIN2019\\u003c\/Data\\u003e\\u003cData
Name=\\\"LogonID\\\"\\u003e0x000000000004b543\\u003c\/Data\\u003e\\u003cData
Name=\\\"SessionName\\\"\\u003eRDP-Tcp#1\\u003c\/Data\\u003e\\u003cData
Name=\\\"ClientName\\\"\\u003eDESKTOP-FJ5FBMT\\u003c\/Data\\u003e\\u003cData
Name=\\\"ClientAddress\\\"\\u003e172.30.253.104\\u003c\/Data\\u003e\\u003c\/EventDa
ta\\u003e\\u003c\/Event\\u003e\",\"XMLErr\":null}"}
```


Пример успешного применения механизма разбора, примененного к полю **XML**, приведено на «Рис. 40».

Event__EventData__Data__10__Name	DisplayName
Event__EventData__Data__10__value	%%1793
Event__EventData__Data__11__Name	UserPrincipalName
Event__EventData__Data__11__value	-
Event__EventData__Data__12__Name	HomeDirectory
Event__EventData__Data__12__value	%%1793
Event__EventData__Data__13__Name	HomePath
Event__EventData__Data__13__value	%%1793
Event__EventData__Data__14__Name	ScriptPath

Ключ 1 **Ключ 2** **Ключ n**

Рис. 40 – Пример работы механизма разбора "XML"

2.9.2.8 JSON

В основном, все источники посылают события в формате RAW-JSON. При разборе событий в этом формате необходимо в качестве первого этапа использовать механизм JSON, а потом любые из доступных в платформе, в зависимости от типа данных в исходном событии.

Обычно все сырые события помещаются в поле **Message**.

Примечание: *для просмотра наименования поля, в которое приходит сырое событие, запустите механизм тестирования и в результатах просмотра перейдите на вкладку "Сырое событие". Найдите пару "Ключ-Значение", в которой значением будет являться сырое событие*.

Пример настройки данного механизма приведен на «Рис. 41».

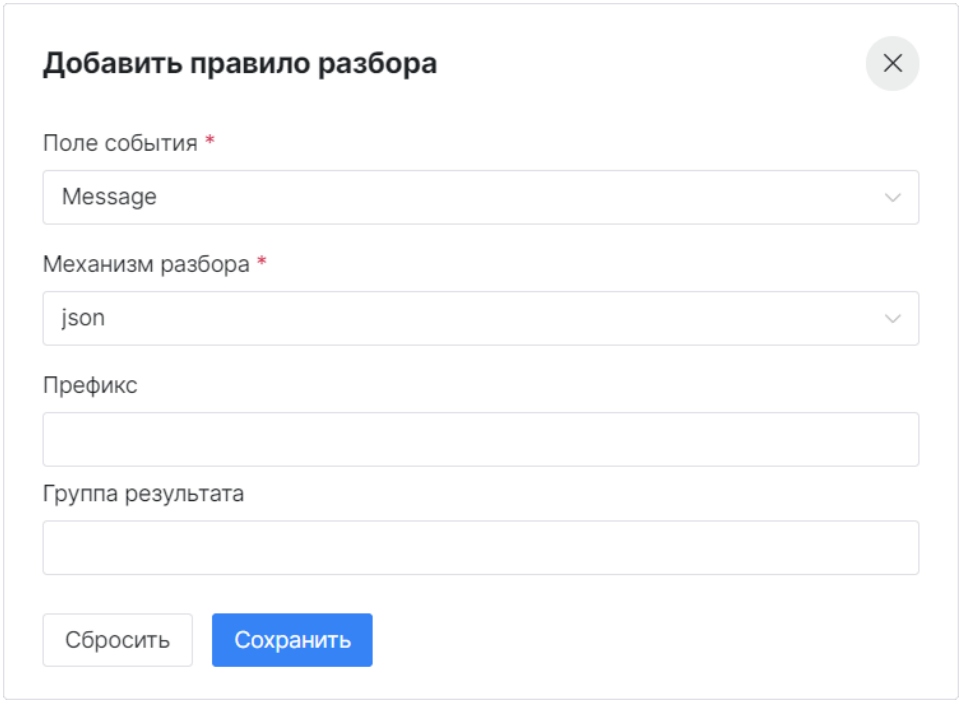


Рис. 41 – Добавление правила разбора. Механизм разбора "JSON"

Для настройки механизма разбора укажите следующие значения:

- в поле **Поле события** укажите поле, в которое пришло сырое событие;
- в поле **Механизм разбора** выберите значение "json".

2.9.2.9 Функция преобразования

Поддерживается функция преобразования `HEX to Text` которая при разборе события преобразует числовое представление последовательности номеров и символов в текстовое.

Пример настройки данного механизма приведен на «Рис. 42».

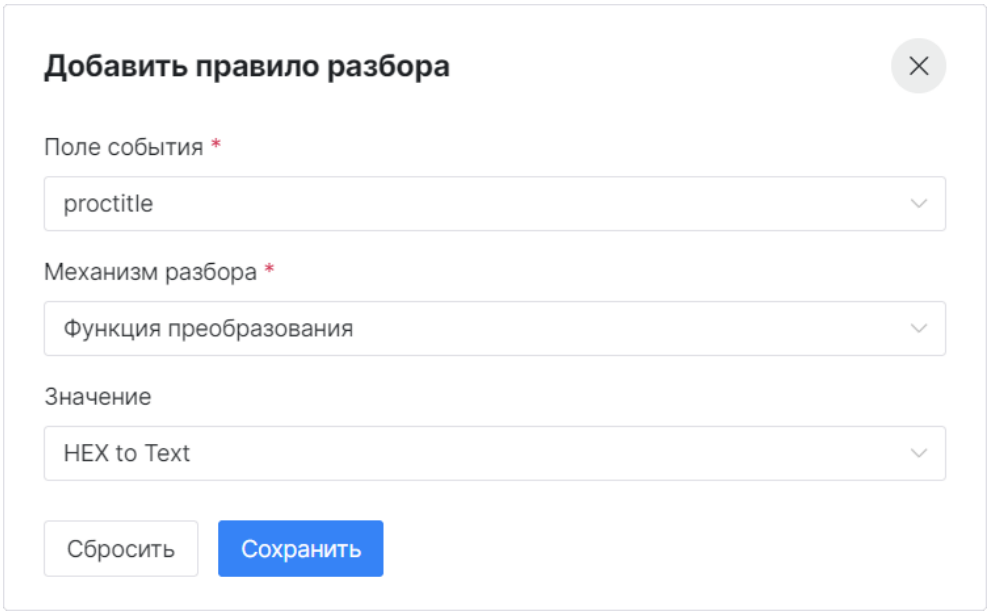


Рис. 42 – Добавление правила разбора. Механизм разбора "Функция преобразования"

Пример сырого события с HEX представлением:

```
{"a_src_ip":"172.30.249.201","a_src_o":"2671","a_c":"","a_src_t":[""],"a_src_r":
"","a_ts":"2024-12-04T12:12:06.382.382328581+00:00","a":"8b3beadb-c7bc-48f2-
9bf1-d2012ed9d17e","Message":"Dec        4    12:50:40    v-stand-05    audispd:
node=172.30.254.95        type=PROCTITLE        msg=audit(1733305840.550:51886):
proctitle=757365726D6F64002D61002D470076696C61696E73007261766573"}
```

Где:

- ключ поля – proctitle;
- значение поля – 757365726D6F64002D61002D470076696C61696E73007261766573.

Пример успешного применения правила разбора приведен на «Рис. 43».

Ключ	Значение
message	node=172.30.254.95 type=PROCTITLE msg=audit(1733305840.550:51886): proctitle=757365726D6F64002D61002D470076696C61696E73007261766573
msg	audit(1733305840.550:51886):
node	172.30.254.95
proctitle	usermod -a -G vilains raves

Рис. 43 – Пример успешного выполнения механизма разбора "Функция преобразования"

2.9.2.10 Не требуется

В случае, если нет необходимости использовать специфические парсеры для какого-либо поля, то можно использовать имеющиеся значение поля "как есть". Для этого необходимо выбрать значение **Не требуется** при выборе механизма разбора (см. «Рис. 44»).

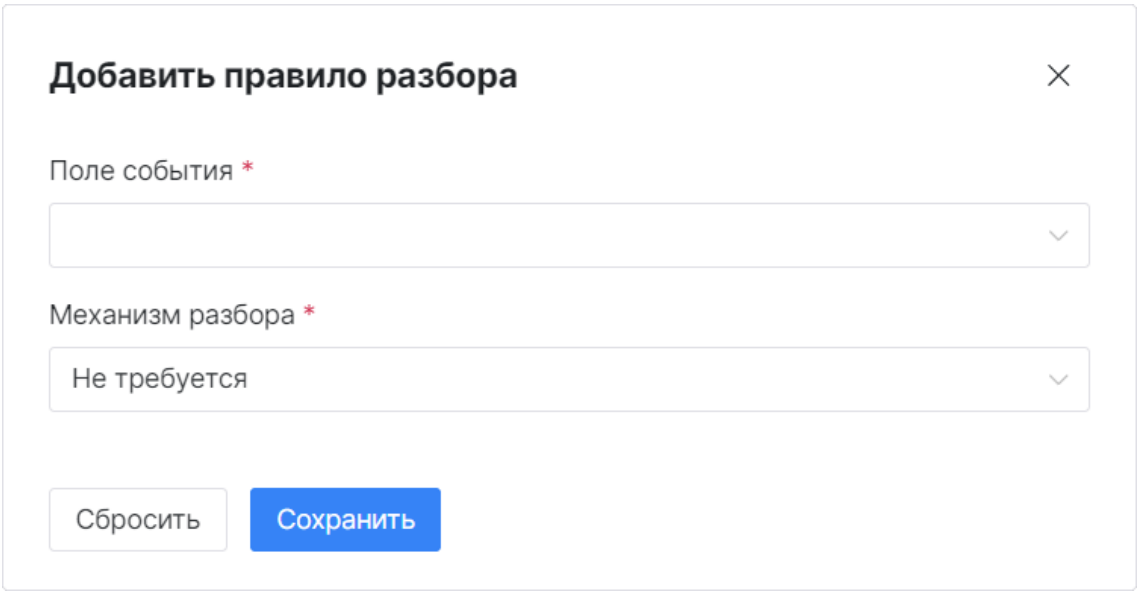


Рис. 44 – Добавление правила разбора. Механизм разбора "Не требуется"

2.9.3 Механизм работы префикса

Префикс добавляет в поле разобранного события соответствующую дополнительную информацию. Префиксы можно использовать для однозначной идентификации сработавшего механизма разбора. Например:

1. Начальные условия (см. «Рис. 45»):
    - **Механизм разбора** – GROK Паттерн;
    - **Поле** – Message;
    - **Параметр** – `^%{GREEDYDATA:parsed_message}$.`

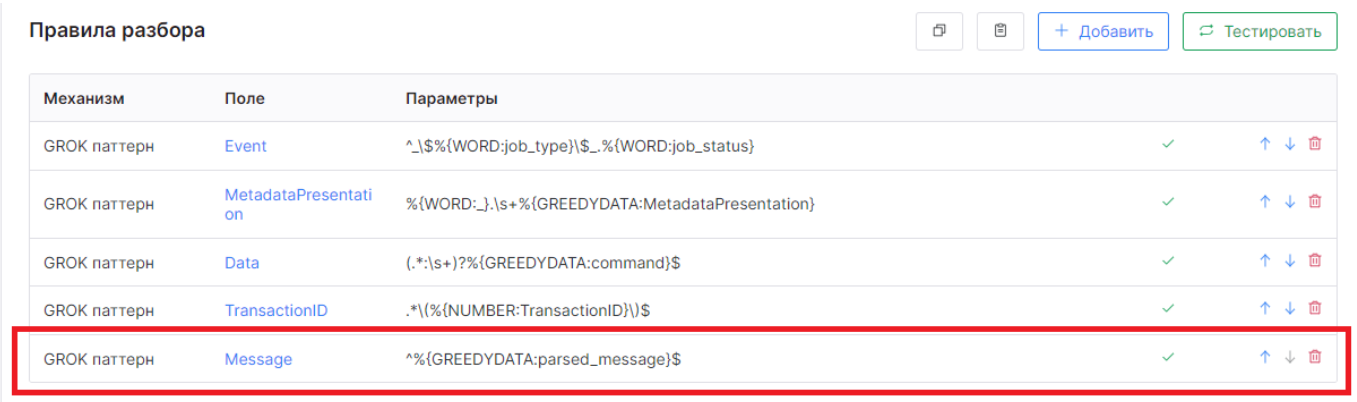


Рис. 45 – Начальные условия механизма разбора

2. Результатом работы этого механизма является поле `parsed_message`. Для просмотра нажмите на кнопку **Тестировать**, а затем кнопку **Показать результаты**, перейдите на вкладку "Текущее правило разбора" и найдите нужное поле (см. «Рис. 46»).

date	7/26/2023 2:39:42 PM
hostname	pgr-1c-00
job_status	Update
job_type	Data
message	{"Level":"Information","Date":"2023-07-26T14:39:42","ApplicationName":"BackgroundJob","ApplicationPresentation":"Background job","Event":"_$Data$_.Update","EventPresentation":"Data. Change","User":"00000000-0000-0000-0000-000000000000","UserName":"","Computer":"","Metadata":"Константа.ПоследнееОбновлениеДоступа","MetadataPresentation":"Constant. Последнее обновление доступа","Comment":null,"Data":"something Команда: Выполнить обновление","DataPresentation":"","TransactionStatus":"Committed","TransactionID":"7/26/2023 2:39:42 PM (2934007)","Connection":"3","Session":"34","ServerName":"","Port":"","SyncPort":"0"}
parsed_message	<7> 7/26/2023 2:39:42 PM pgr-1c-00 {"Event":{"Level":"Information","Date":"2023-07-26T14:39:42","ApplicationName":"BackgroundJob","ApplicationPresentation":"Background job","Event":"_$Data$_.Update","EventPresentation":"Data. Change","User":"00000000-0000-0000-0000-000000000000","UserName":"","Computer":"","Metadata":"Константа.ПоследнееОбновлениеДоступа","MetadataPresentation":"Constant. Последнее обновление доступа","Comment":null,"Data":"something Команда: Выполнить обновление","DataPresentation":"","TransactionStatus":"Committed","TransactionID":"7/26/2023 2:39:42 PM (2934007)","Connection":"3","Session":"34","ServerName":"","Port":"","SyncPort":"0"}}

Рис. 46 – Результат работы механизма разбора

3. Допустим, нам необходимо данное поле выделить и однозначно определять как получившееся в результате работы конкретного механизма разбора. Для этого добавляем ему префикс. Для этого выполните следующие действия:

   a. В блоке **Правила разбора** нажмите по нужному механизму в списке.

   b. В открывшемся окне в поле **Префикс** укажите префикс для данного механизма (см. «Рис. 47»).

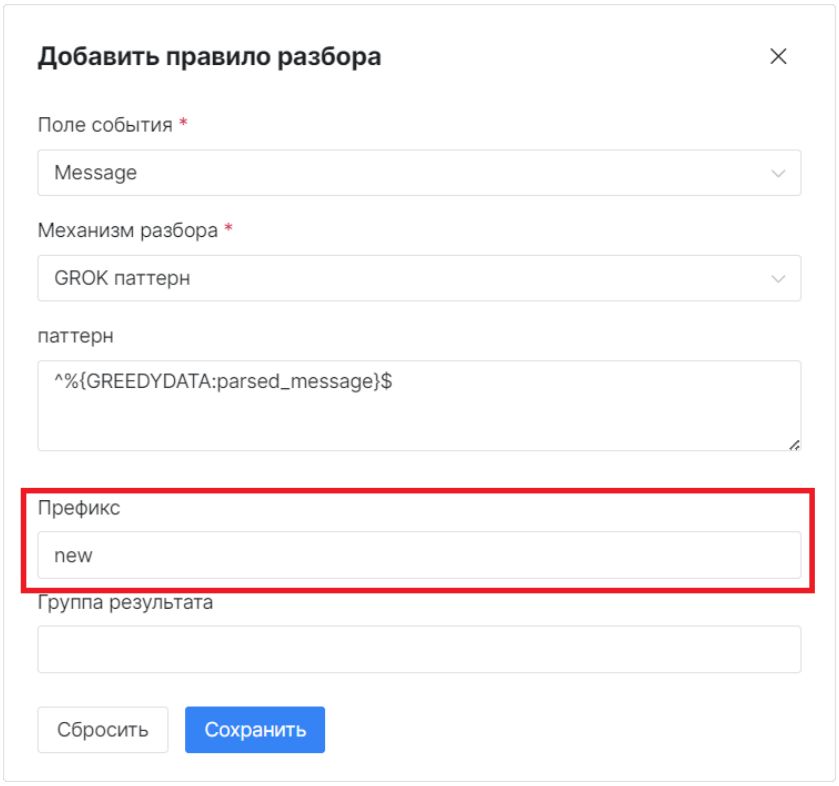


Рис. 47 – Добавление префикса

   c. Нажмите кнопку **Сохранить**.

4. Нажмите на кнопку **Тестировать**, а затем кнопку **Показать результаты**, перейдите на вкладку "Текущее правило разбора". Теперь нужное поле будет иметь соответствующий префикс (см. «Рис. 48»).

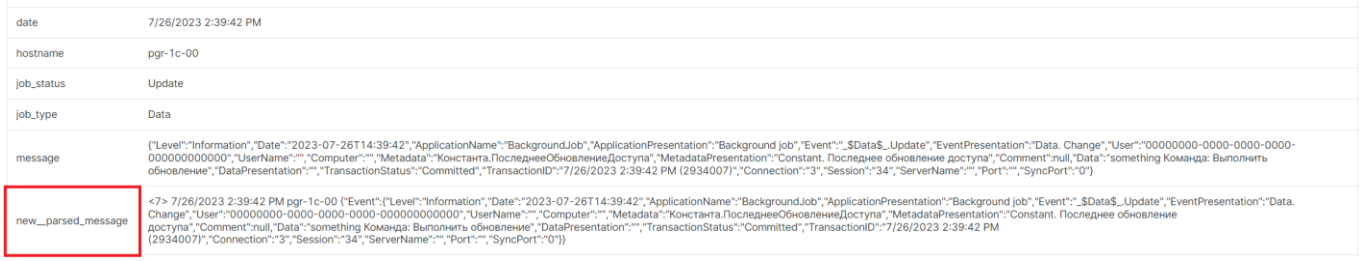


Рис. 48 – Результат добавления префикса в механизм разбора

2.9.4 Механизм работы функции группировки

Результатом работы функции группировки является создание новой переменной. Ключом для переменной будет являться наименование группы, а значение будет включать результаты работы правил разбора. Результаты работы правила будут перечислены через "**;**".

Данную функцию нельзя использовать для нормализации событий. Функция используются только для последующей обработки данных.

Пример работы:

Необходимо сгруппировать результаты работы следующих правил: (см. «Табл. 1»).

Табл. 1 – Результаты работы правил разбора, которые необходимо сгруппировать

Механизм	Поле	Параметры	Результат (ключ)	Результат (Значение)
GROK паттерн	Data	`(.*:\s+)?%{GREEDYDATA:command}$`	command	Выполнить обновление
GROK паттерн	TransactionID	`.*\(%{NUMBER:TransactionID}\)$`	TransactionID	2934007

1. В блоке **Правила разбора** нажмите по наименованию нужного механизма (см. «Рис. 49»).

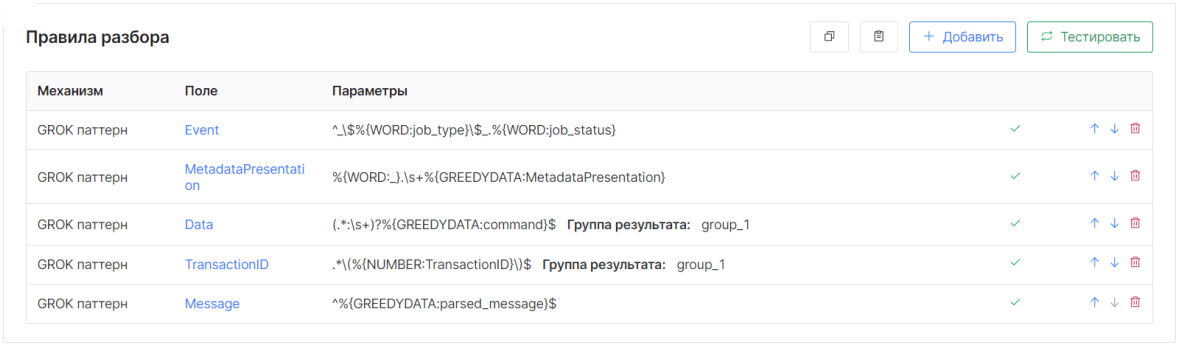


Рис. 49 – Правила разбора, результаты которых необходимо объединить в группу

2. В открывшемся окне в поле **Группа результата** укажите наименование группы (см. «Рис. 50») и нажмите кнопку **Сохранить**.

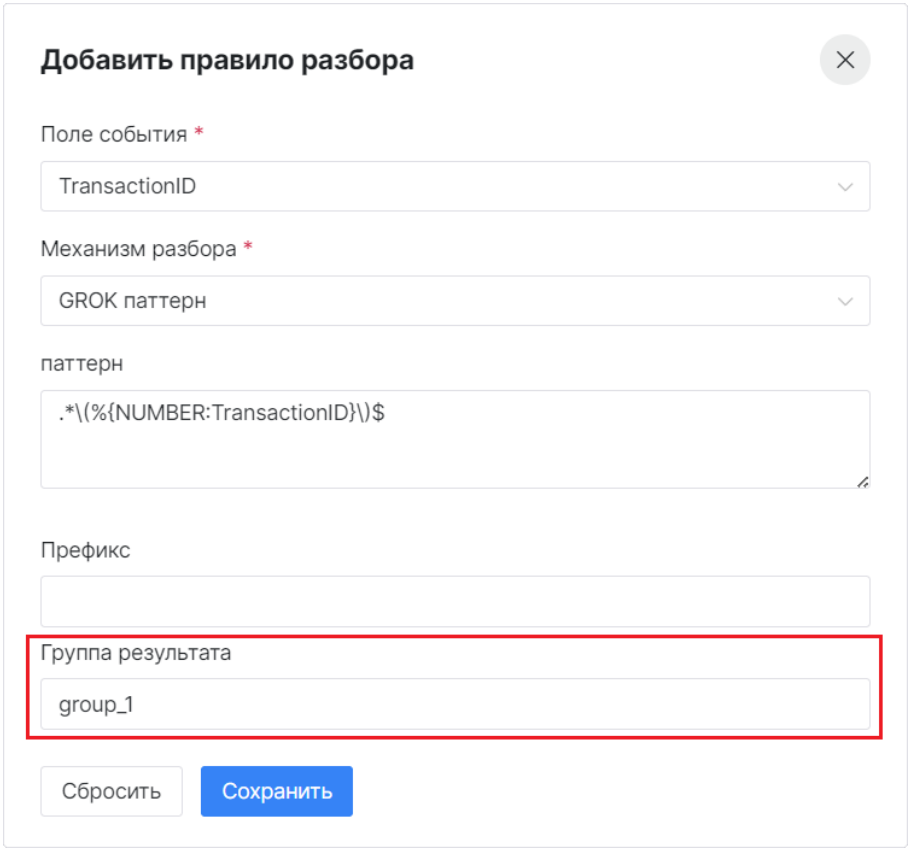


Рис. 50 – Добавление группы результата

3. Укажите группу результата для нужных правил разбора. В графе **Параметры** будет отображена информация о группах результата (см. «Рис. 49»).
4. Нажмите на кнопку **Тестировать**, а затем кнопку **Показать результаты**, перейдите на вкладку "Текущее правило разбора". Будет создана новая переменная, значением которой будет являться перечень результатов работы правил (см. «Рис. 51»).

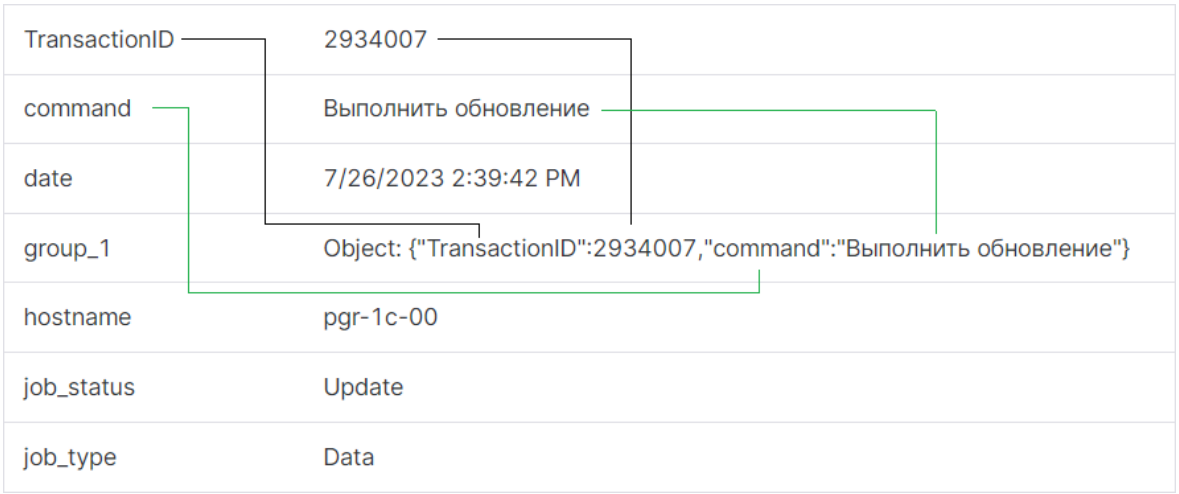


Рис. 51 – Результат работы функции группировки

2.9.5 Механизмы нормализации

Данный раздел используется как справочный материал по работе в разделе **Источники** → **Правила разбора**.

В **Платформе Радар** для передачи полученных на этапе разбора пар "Ключ-Значение" в таксономию, могут использоваться следующие методы подстановки:

- «Функции преобразования»;
- «Строка»;
- «Поле разбора».

2.9.5.1 Функции преобразования

Данный способ позволяет применить к полю (паре"Ключ-Значение"), которое будет передаваться в таксономию, выбранное преобразование.

Применить преобразование к выбранному полю можно единожды в рамках правила разбора.

В платформе радар поддерживаются следующие функции преобразования:

- «Изменение времени в необходимый формат»;
- «Перевод текста в нижний регистр»;
- «Декодирование строки из base64»;
- «Декодирование строки из HEX»;
- «Math. Сложение»;
- «Math. Вычитание»;
- «Склейка строки».

2.9.5.1.1 Изменение времени в необходимый формат

Данный способ позволяет задать перечень форматов времени, в которые будет преобразовываться значение выбранного поля при подстановке в таксономию.

При реализации способа будет выполняться попытка преобразовать время, в указанный формат. После первого успешного преобразования процесс считается выполненным.

Если ни один из заданных форматов времени не сработает, то будет подставлено текущее время обработки в формате по умолчанию.

Пример настройки данного механизма приведен на «Рис. 52».

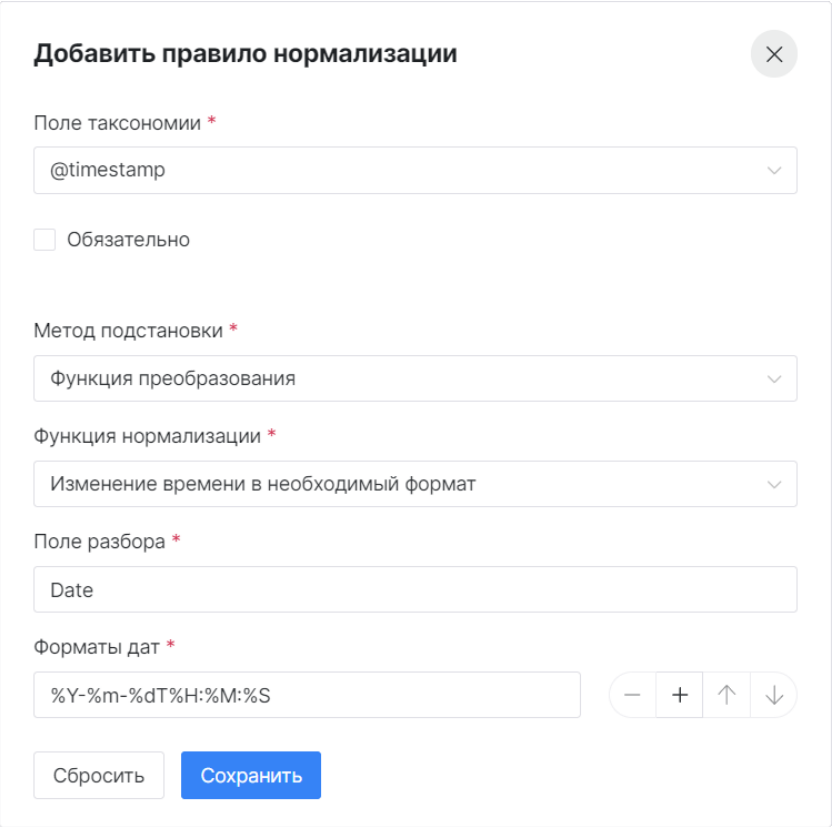


Рис. 52 – Метод подстановки "Функция преобразования". Функция преобразования "Изменение времени в необходимый формат"

Для настройки способа преобразования укажите следующие данные:

- **Поле разбора** – укажите поле (полученное на этапе разбора), значение которого будет передаваться в таксономию;
- **Формат дат** – задайте последовательный список форматов дат и времени.

Перечень поддерживаемых форматов дат приведен в таблице:

Формат	Описание
%y	Сокращенная запись года. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 25.
%Y	Полная запись года. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 2025.
%b	Сокращенная запись названия месяца. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать Mar.
%B	Полное название месяца. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать Mar.
%m	Полная запись месяца. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 03.
%d	Полная запись даты. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 02.
%e	Сокращенная запись даты. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 2.
%a	Сокращенная запись названия дня. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать Sun.

Формат	Описание
%A	Полная запись названия дня. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать Sunday.
%u	Количество дней с начала недели, начиная с понедельника. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 7.
%w	Количество дней с начала недели, начиная с воскресенья. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 0.
%W	Количество недель с начала года. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 09.
%j	Количество дней с начала года. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 061.
%D	D Эквивалент записи формата %m/%d/%y. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 03/02/25.
%F	Эквивалент записи формата %Y-%m-%d. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 2025-03-02.
%H	Полная запись количество часов с начала суток. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 15.
%I	Час времени суток, в 12-часовом формате. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 03.
%M	Полная запись количества минут. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 44.
%S	Полная запись количества секунд. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 32.
%s	Полная запись количества миллисекунд. Пример: 2025-03-02 15:44:32.032 GMT+0300 будет соответствовать 032.
%p	Эквивалент обозначения AM/PM, связанным с 12-часовым форматом времени. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать PM.
%R	Эквивалент записи формата %H:%M. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 15:44.
%T	Эквивалент записи формата %H:%M:%S. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 15:44:32.
%r	12-часовой формат локального времени. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать 03:44:32 PM.
%c	Стандартная интерпретация локальной даты и времени. Пример: 2025-03-02 15:44:32 GMT+0300 будет соответствовать Sun Mar 2 15:44:32 2025.
%o	Формат [+|-]h[h][:mm] (т.е. требуется разделитель (:), между часами и минутами с начальным необязательным нулём, для часа). Пример: 2025-03-02 15:44:32 GMT+03:00 будет соответствовать +03:00.
%z	Запись -0430 означает 4 часа 30 минут перед UTC смещения, а 04 означает 4 часа после UTC смещения.
%Z	Аббревиатура или название часового пояса, взятое как самая длинная последовательность символов, содержащая только символы от A до Z, от a до z. Пример: 2025-03-02 15:44:32 MSK будет соответствовать MSK

2.9.5.1.2 Перевод текста в нижний регистр

При реализации способа все передаваемые значения будут преобразовываться в нижний регистр.

Пример настройки данного механизма приведен на «Рис. 53».

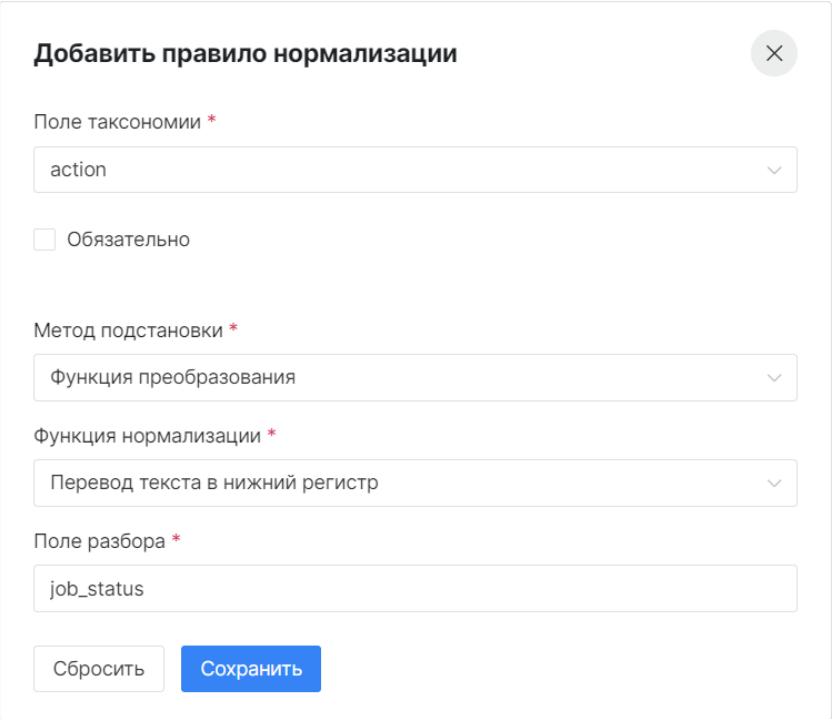


Рис. 53 – Метод подстановки "Функция преобразования". Функция преобразования "Перевод текста в нижний регистр"

Для настройки данного способа, в поле **Поле разбора** необходимо указать поле (полученное на этапе разбора), значение которого будет передаваться в таксономию.

2.9.5.1.3 Декодирование строки из base64

При реализации способа передаваемые значения, которые были закодированы в представление `base64` будут декодироваться и подставляться в соответствующую таксономию.

Пример настройки данного механизма приведен на «Рис. 54».

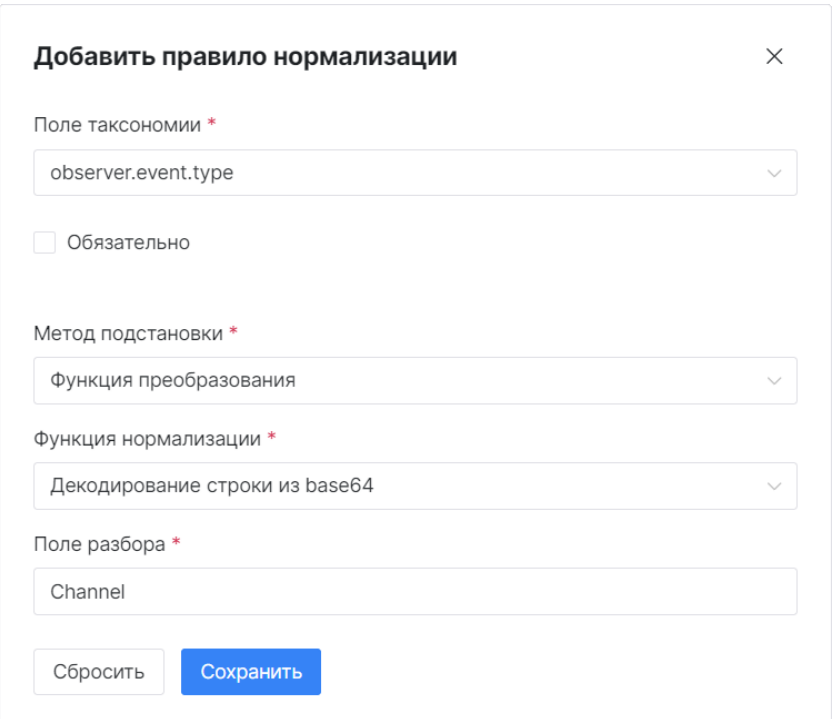


Рис. 54 – Метод подстановки "Функция преобразования". Функция преобразования "Декодирование строки в base64"

Для настройки данного способа, в поле **Поле разбора** необходимо указать поле (полученное на этапе разбора), значение которого будет передаваться в таксономию.

2.9.5.1.4 Декодирование строки из HEX

При реализации способа передаваемые значения, которые были закодированы в представление HEX будут декодироваться и подставляться в соответствующую таксономию.

Пример настройки данного механизма приведен на «Рис. 55».

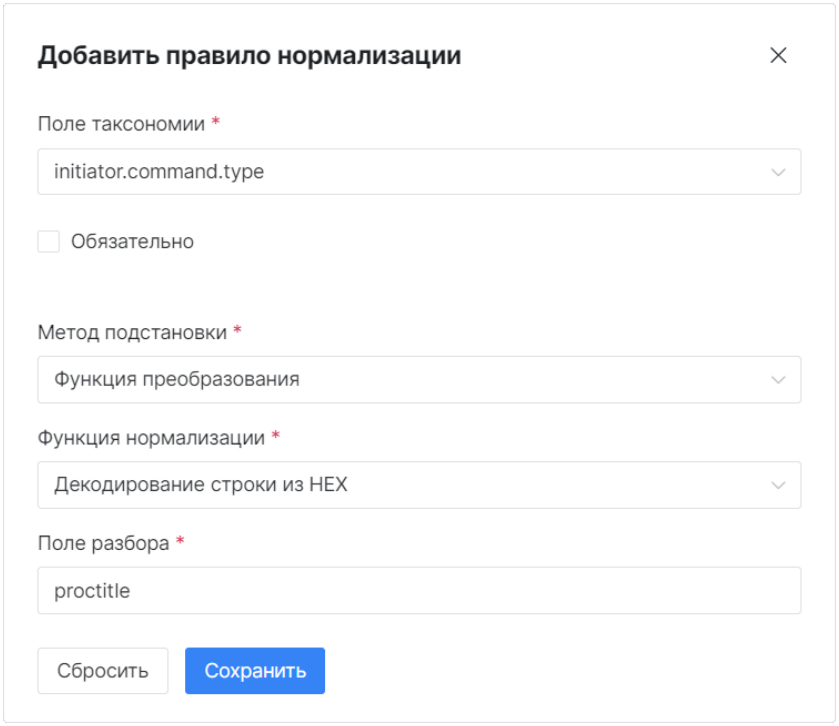


Рис. 55 – Метод подстановки "Функция преобразования". Функция преобразования "Декодирование строки из HEX"

Для настройки данного способа, в поле **Поле разбора** необходимо указать поле (полученное на этапе разбора), значение которого будет передаваться в таксономию.

2.9.5.1.5 Math. Сложение

Данный способ позволяет выполнить арифметическое сложение значений двух полей и поместить результат в таксономию.

Пример настройки данного механизма приведен на «Рис. 56».

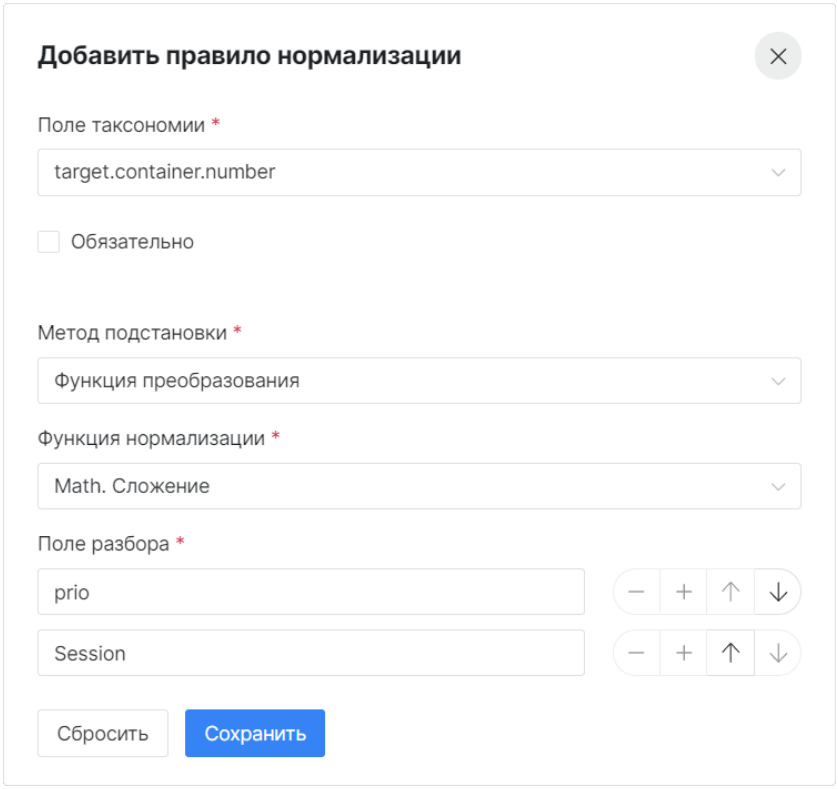


Рис. 56 – Метод подстановки "Функция преобразования". Функция преобразования "Math. Сложение"

Чтобы настроить этот метод, необходимо указать два поля разбора, значения которых будут складываться, а затем помещаться в таксономию.

Пример:

```
Начальные условия
  "поле таксономии": "target.container.number"
Поля разбора "Ключ-Значение":
  "prio": "7",
  "Session": "34",
Результат
  target.container.number=41
```

2.9.5.1.6 Math. Вычитание

Данный способ позволяет выполнить арифметическое вычитание значения одного поля из другого и поместить результат в таксономию.

Пример настройки данного механизма приведен на «Рис. 57».

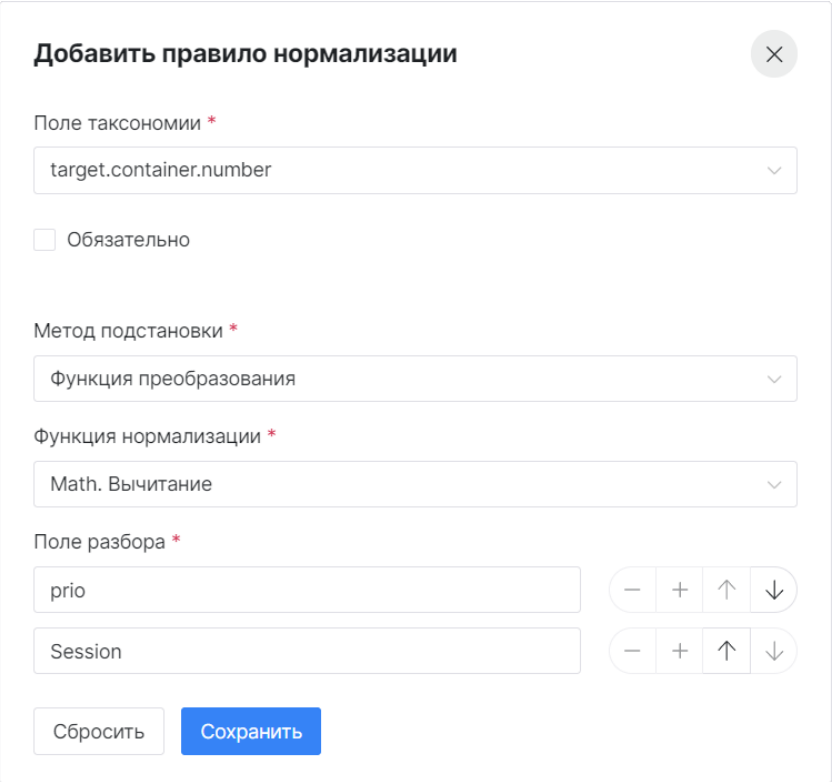


Рис. 57 – Метод подстановки "Функция преобразования". Функция преобразования "Math. Вычитание"

Чтобы настроить этот метод, необходимо указать два поля разбора. Значение второго поля из списка будет вычитаться из значения первого, а результат вычитания будет помещен в таксономию.

Пример:

```
Начальные условия
  "поле таксономии": "target.container.number"
Поля разбора "Ключ-Значение":
  "prio": "7",
  "Session": "34",
Результат
  target.container.number= -27
```

2.9.5.1.7 Склейка строки

Если в одно значение в результате разбора было помещено в несколько полей, то при добавлении в таксономию, их необходимо предварительно объединить (склеить).

Данный способ позволяет настроить способ склеивания.

Пример настройки данного механизма приведен на «Рис. 58».

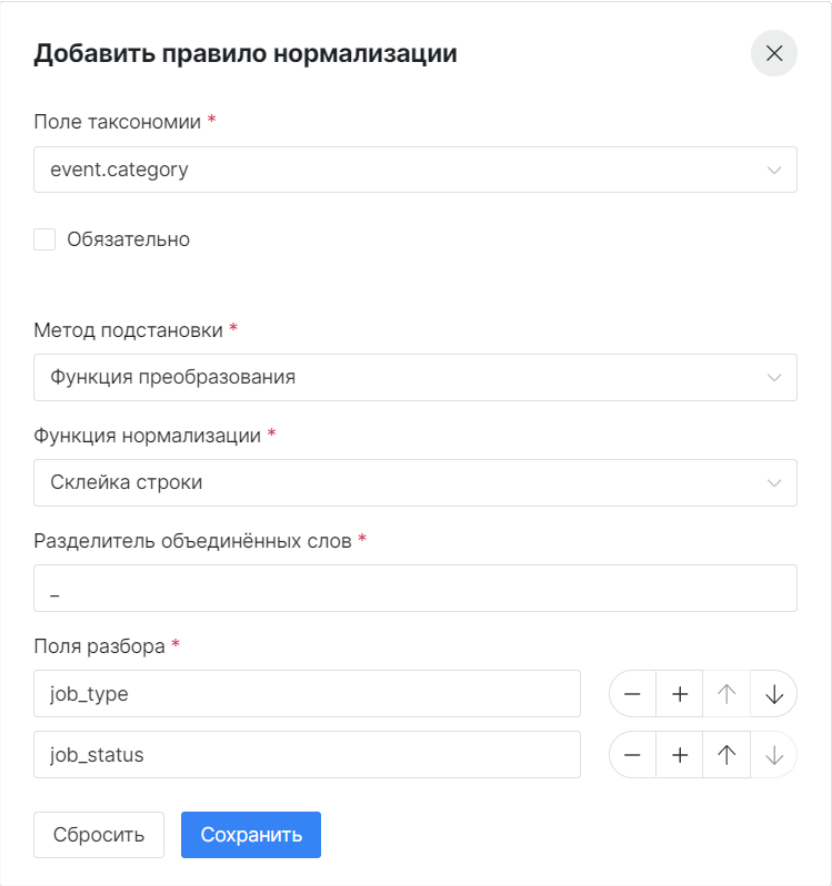


Рис. 58 – Метод подстановки "Функция преобразования". Функция преобразования "Склейка строки"

Для настройки способа выполните следующие действия:

- **Разделитель объединённых слов** – укажите способ, которым будут объединяться значения полей. Это может быть произвольное слово или символ.
- **Поля разбора**. Задается последовательный список полей, значения которых будут "склеиваться" разделителем объединенных слов.

Пример:

```
Начальные условия
  "поле таксономии": "event.category"
  "разделитель объединённых слов": "_",
  "поле разбора": "job_type"
  "поле разбора": "job_status"
Ключ-Значение полей разбора:
  "job_type":"Data"
  "job_status":"Update"
Результат
  event.category=Data_Update
```

2.9.5.2 Строка

Данный способ будет передавать в таксономию произвольное значение, указанное в виде константной строки.

Пример настройки данного механизма приведен на «Рис. 59».

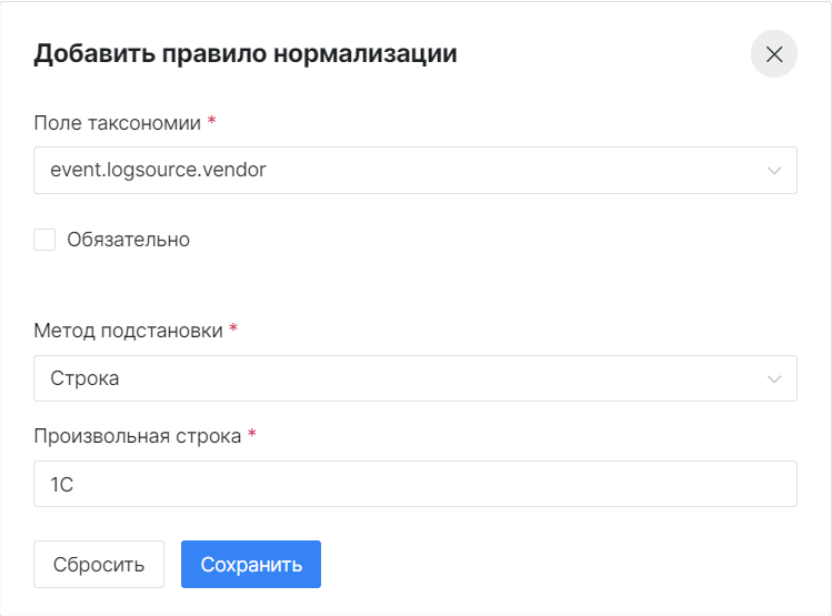


Рис. 59 – Метод подстановки "Строка"

Для настройки метода подстановки необходимо в поле **Произвольная строка**, указать значение, которое будет передаваться в таксономию.

Пример:

```
Начальные условия
  "поле таксономии": "event.logsource.vendor"
  "произвольная строка": "Вендор 1С",
Результат
  event.logsource.vendor=Вендор 1С
```

2.9.5.3 Поле разбора

Данный способ будет передавать значение выбранного поля в таксономию без какого-либо преобразования. Пример настройки данного механизма приведен на «Рис. 60».

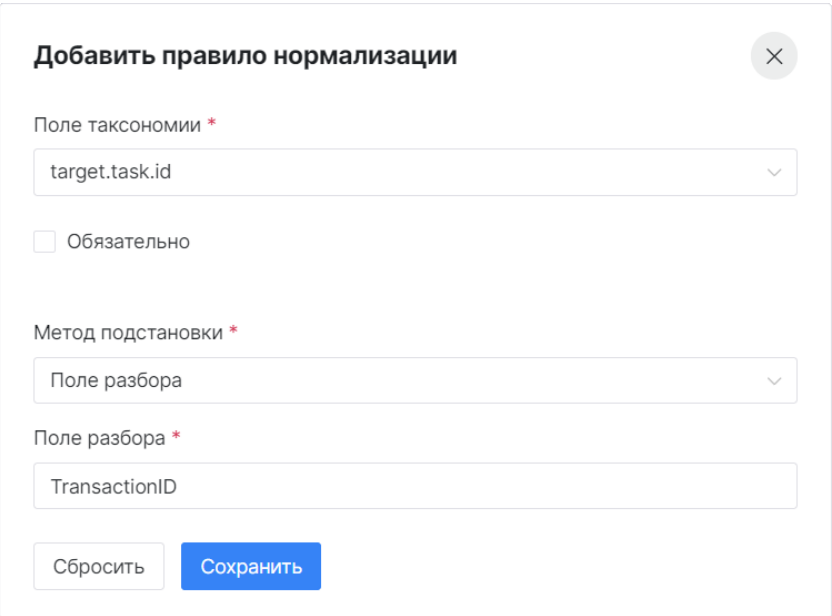


Рис. 60 – Метод подстановки "Поле разбора"

Для настройки метода подстановки необходимо в поле **Поле разбора**, указать поле (полученное на этапе разбора), значение которого будет передаваться в таксономию.

```
Начальные условия
  "поле таксономии": "target.task.id"
Поле разбора:
  "ключ": "TransactionID",
  "значение": "2934007",
Результат
  target.task.id=2934007
```

2.9.6 Механизмы обогащения

2.9.6.1 Обогащение по произвольному скрипту

Платформа Радар позволяет использовать скрипты, подготовленные пользователями платформы, для обогащения событий.

Возможность использования произвольных скриптов для обогащения событий настраивается в разделе **Администрирование → Управление конфигурацией →** вкладка **Параметры сервисов**, где в древовидном списке нужно выбрать **Enrich → Custom** (см. «Рис. 61»).

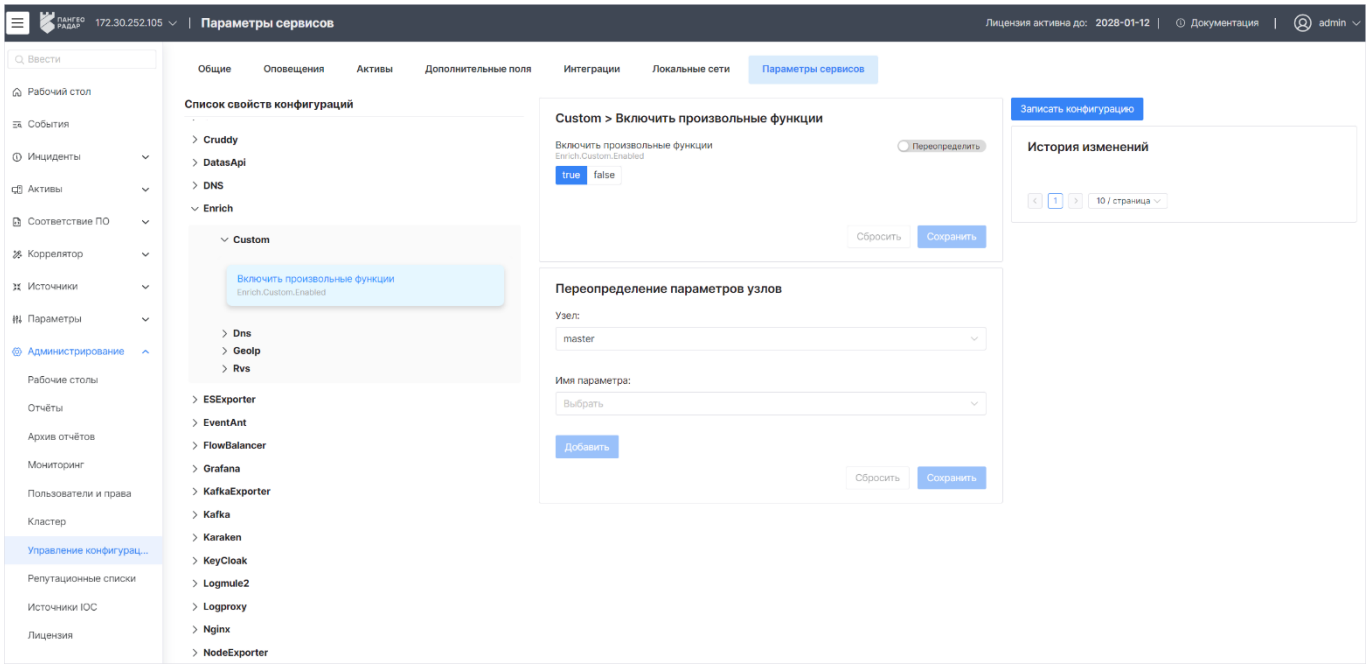


Рис. 61 – Включение обогащения по произвольному скрипту

Пример настройки параметров обогащения по произвольному скрипту, при создании правила обогащения, приведен на «Рис. 62».

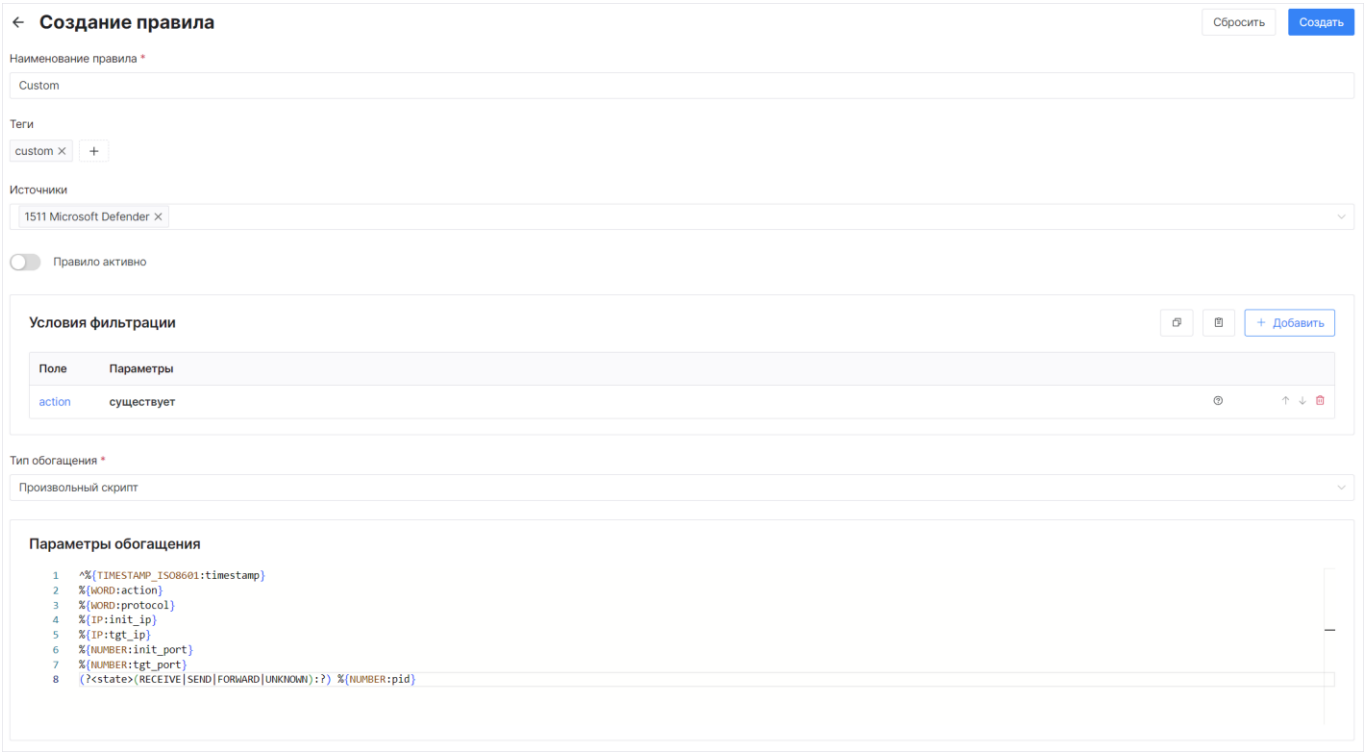


Рис. 62 – Пример параметров обогащения по произвольному скрипту

Для настройки параметров обогащения укажите скрипт в соответствующем поле.

Принцип работы:

1. Сервис будет проверять есть ли совпадения в полях нормализованного события и в скрипте.
2. Если совпадения найдены, то событие обогащается значениями, указанными в скрипте.

2.9.6.2 DNS обогащение

DNS обогащение — это процесс наполнения событий дополнительной информацией на основе DNS-записей о доменах и IP-адресах.

При поступлении событий, в зависимости от источника, может быть, разная комбинация заполненных полей. Обогащение выполняется только для комбинации из трех полей IP, hostname, fqdn.

Возможность использования DNS обогащения настраивается в разделе **Администрирование** → **Кластер** → вкладка **Управление конфигурацией**, где в древовидном списке нужно выбрать **Enrich** → **DNS** и настроить следующие параметры:

- Включить обогащение с DNS сервера;
- Предзагрузка из файла;
- Список локальных DNS серверов.

Пример параметров DNS обогащения, при создании правила обогащения, приведен на «Рис. 63».

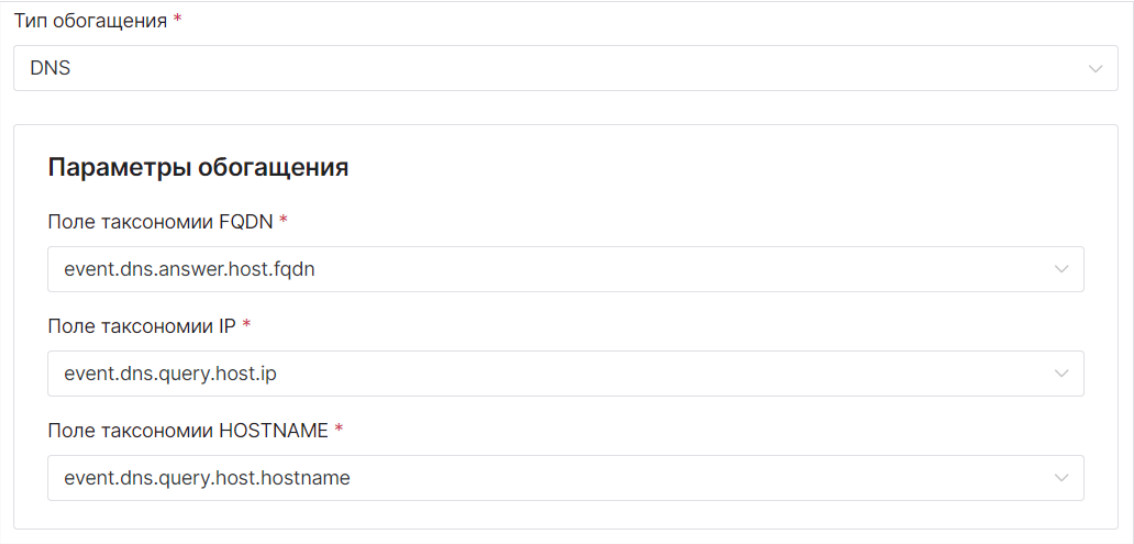


Рис. 63 – Параметры DNS обогащения

Для DNS обогащения настраиваются следующие поля:

- **Поле таксономии FQDN**;
- **Поле таксономии IP**;
- **Поле таксономии HOSTNAME**.

Принцип работы: Если при сработке правила, хотя бы одно из выбранных полей заполнится значением/значениями, то сервис обработки событий попробует восстановить остальные поля. При этом сервис будет использовать DNS-сервер, который задается в разделе **Администрирование** → **Кластер** → вкладка **Управление конфигурацией**.

В случаях, когда все три поля таксономии заполнены, или наоборот - пустые, обогащение завершается.

2.9.6.3 GeoIP-обогащение

GeoIP-обогащение — это процесс добавления информации о географическом местоположении IP-адресов, например, о стране и городе расположения, владельцах IP-адресов и другом.

Платформа Радар позволяет загрузить список соответствий IP-адресов или диапазонов IP-адресов географическим данным, чтобы затем использовать эту информацию при обогащении событий.

Для работы GeoIP-обогащения необходимо выполнить следующие действия:

1. Получите базу GeoLite2 Free Geolocation Data | MaxMind Developer Portal.
2. Поместите ее на узел платформы, на котором установлен сервис TERMIT.
3. Перейдите в раздел **Администрирование** → **Кластер** → вкладка **Управление конфигурацией**.
4. В древовидном списке перейдите **Enrich** → **GeoIP** (см. «Рис. 64»).

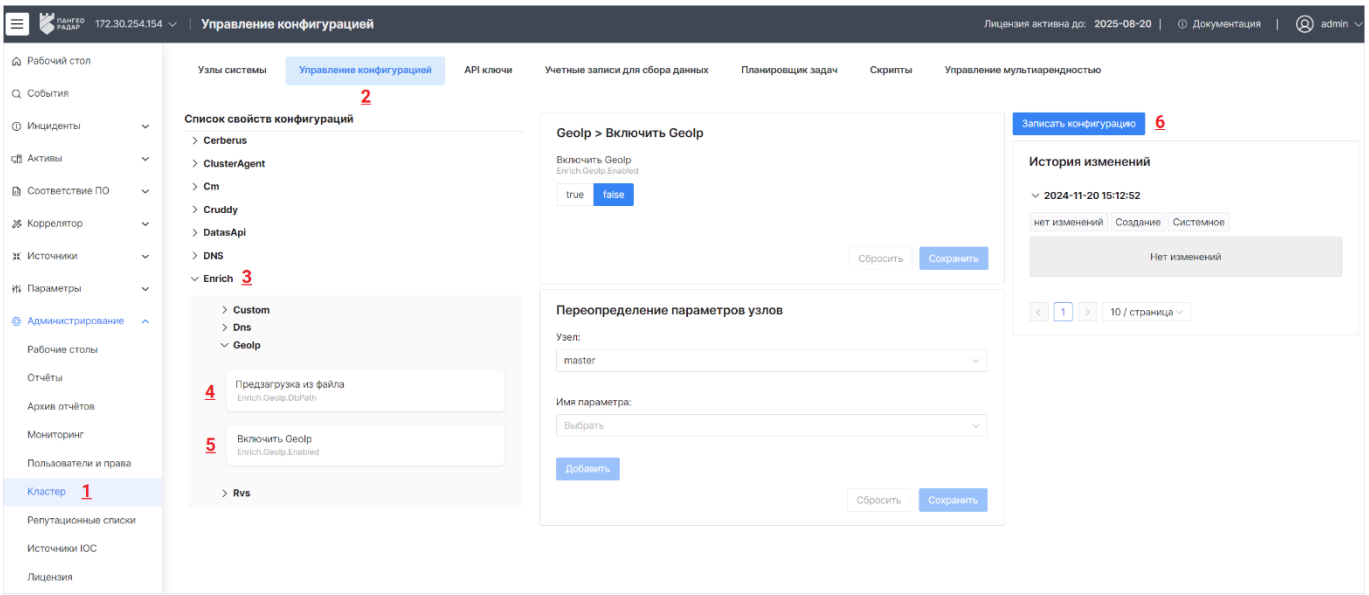


Рис. 64 – Включение GeoIP-обогащения

5. Настройте следующие параметры:
    - в параметре **Предзагрузка из файла** укажите путь к скаченной базе;
    - установите параметр **Включить GeoIp** в значение `true`.
6. Нажмите кнопку **Записать конфигурацию**.

Пример параметров GeoIP-обогащения, при создании правила обогащения, приведен на «Рис. 65».

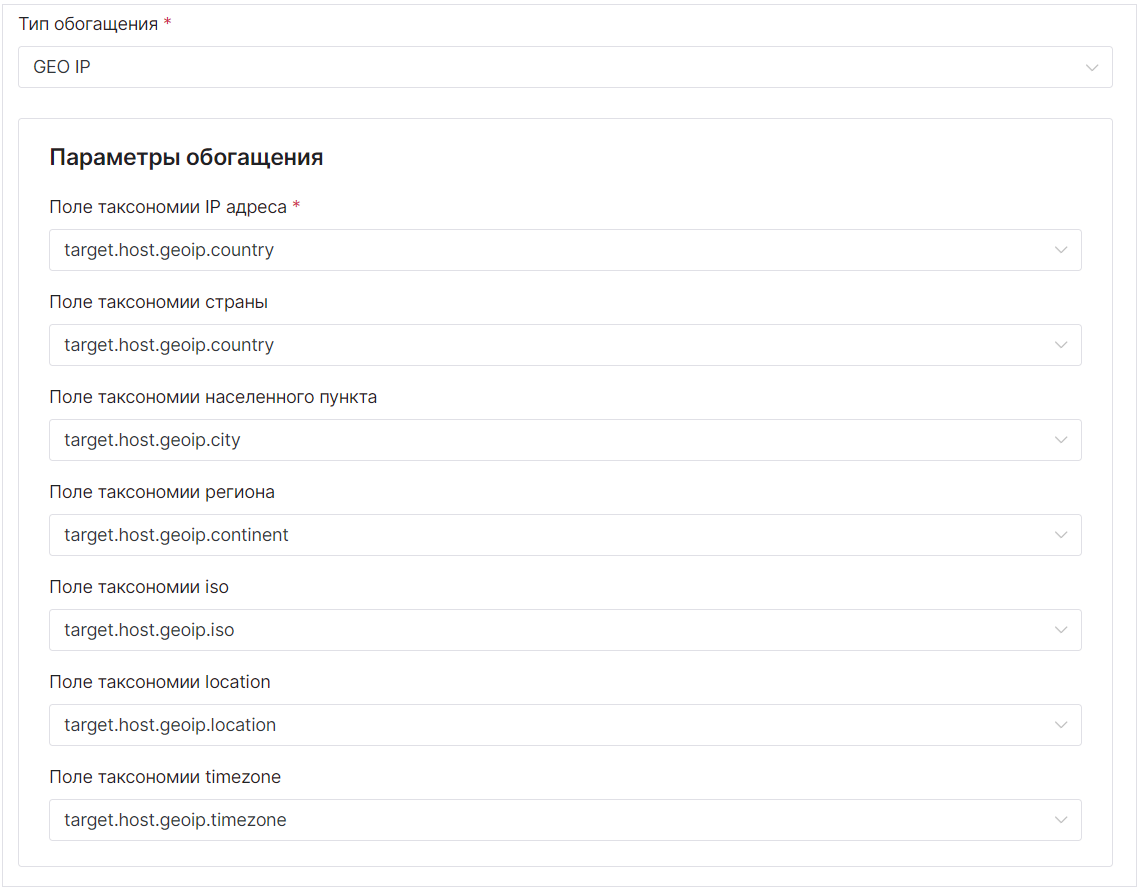


Рис. 65 – Параметры GeoIP-обогащения

Для GeoIP-обогащения настраиваются следующие поля:

- **Поле таксономии IP адреса** (обязательное поле);
- **Поле таксономии страны**;
- **Поле таксономии населенного пункта**;
- **Поле таксономии региона**;
- **Поле таксономии iso**;
- **Поле таксономии location**;
- **Поле таксономии timezone**.

Принцип работы: Если при поступлении события, поле таксономии IP адреса заполняется значением, то выполняется поиск данного IP в скачанной базе данных GeoIP. По результатам поиска событие может быть обогащено соответствующими данными (страна, населенный пункт, регион и т.д.).

2.9.6.4 Обогащение по табличному списку

Табличные списки (Rapid Value Store), являются видом активного хранилища -- автоматически изменяемого, в зависимости от условий. Работа с табличными списками выполняется в разделе **Коррелятор → Табличные списки**.

Платформа Радар позволяет использовать записи табличных списков для обогащения событий.

Возможность использования табличных списков для обогащения событий настраивается в разделе **Администрирование → Кластер →** вкладка **Управление конфигурацией**, где в древовидном списке нужно выбрать **Enrich → Rvs** (см. «Рис. 66»).

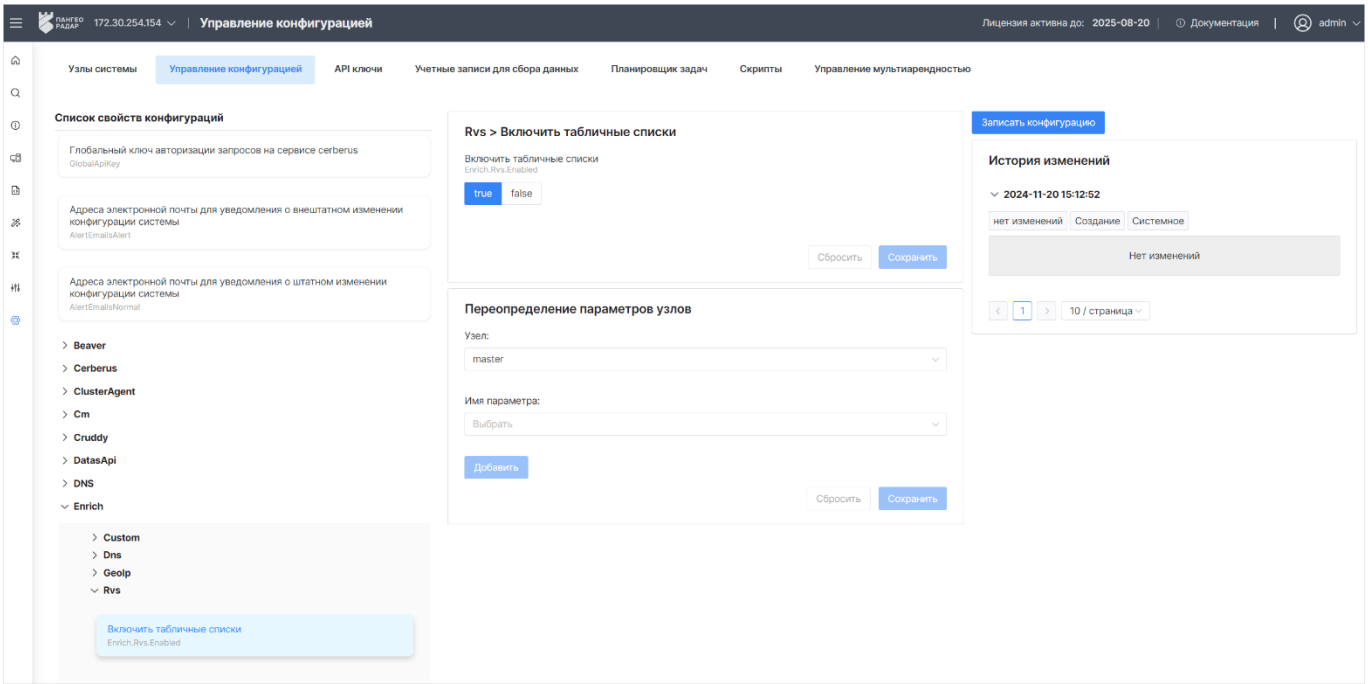


Рис. 66 – ***Включение Rvs-обогащения***

Пример настройки параметров обогащения по табличному списку, при создании правила обогащения, приведен на «Рис. 67».

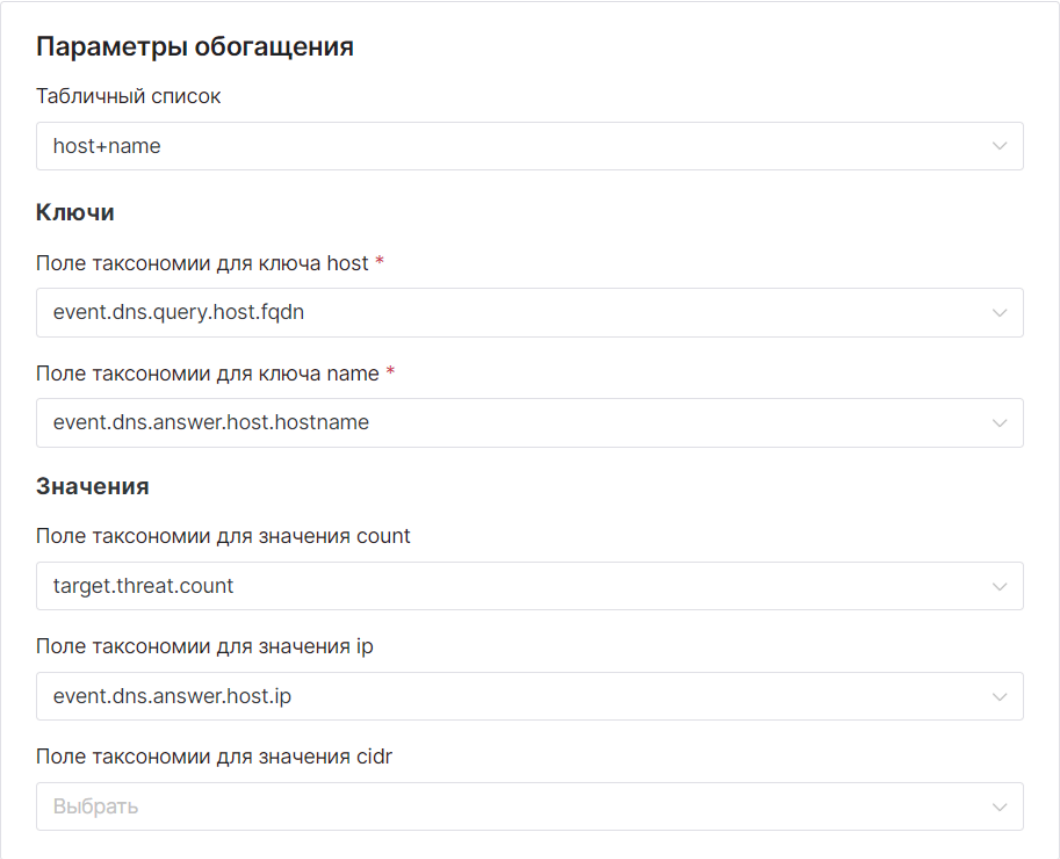


Рис. 67 – Параметры Rvs-обогащения

Для настройки параметров обогащения выполните следующие действия:

1. В поле **Табличный список** из выпадающего списка выберите табличный список. Будет сформирован список полей таксономии для ключей и значений табличного списка.
2. В поле/полях **Ключи** укажите какую таксономию использовать для ключей табличного списка (из ключей формируется уникальный идентификатор записи табличного списка).
3. В поле/полях **Значения** укажите какую таксономию использовать для значений табличного списка.

Принцип работы:

1. Сервис будет проверять есть ли значения в полях ключей нормализованного события.
2. Если значение в поле есть, то сервис обращается к табличному списку и по ключу, который формируется из указанных значений, пытается найти соответствующую запись.
3. Если запись найдена, то событие обогащается значениями, указанными в данной записи.

2.9.6.5 Обогащение по справочнику

Обогащение по справочнику – это процесс наполнения событий дополнительной информацией на основе данных локальных справочников.

Пример настройки параметров обогащения по справочнику, при создании правила обогащения, приведен на «Рис. 68».

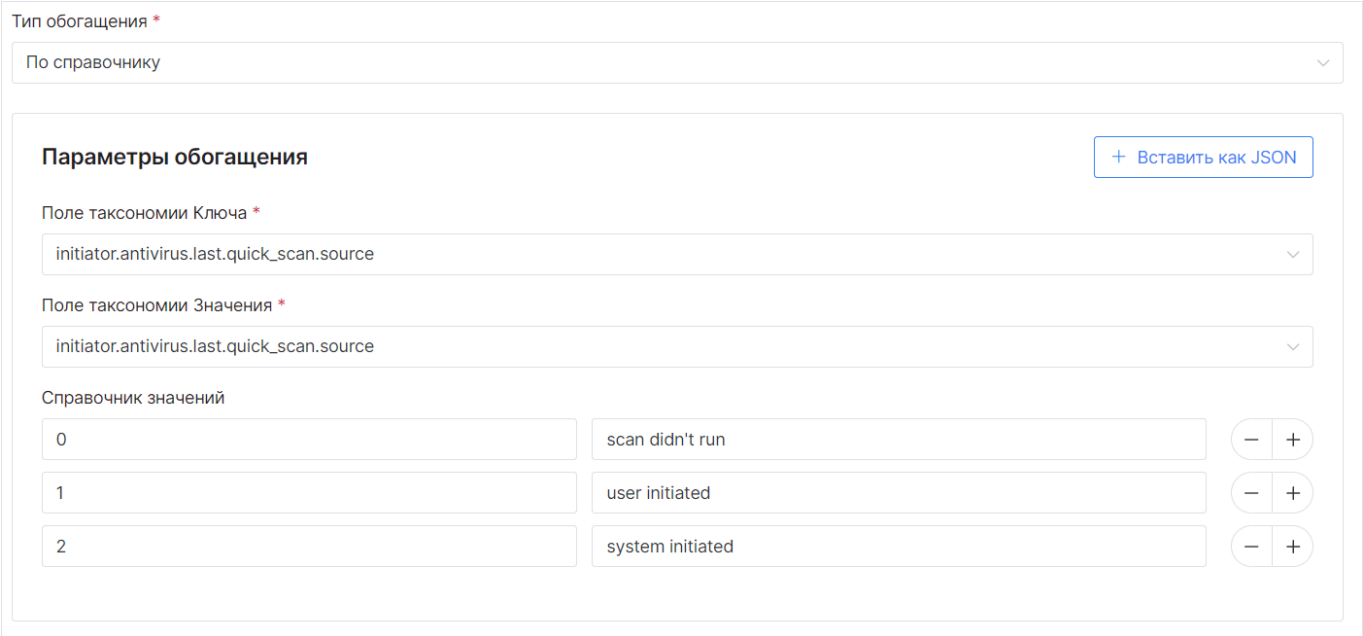


Рис. 68 – Параметры обогащения по справочнику

Для настройки параметров обогащения выполните следующие действия:

1. Выберите поле таксономии, которое будет являться **Ключом**, по которому будет выполняться обогащение.
2. Выберите поле таксономии, которое будет являться **Значением**, которое будет обогащаться.
3. В таблице **Справочник значений** нажмите кнопку **Создать** и в соответствующих полях укажите **Ключи** и **Значения,** которыми будет обогащено событие.

Платформа Радар позволяет вставить справочник значений с помощью JSON. Для этого нажмите кнопку **Вставить как JSON** и в открывшемся окне укажите справочник значений в соответствующем формате.

Принцип работы: Если в поле таксономии ключа придет значение, которое есть в справочнике, тогда поле таксономии значения, будет обогащено соответствующим значением из справочника.

Пример:

Начальные условия:

- Поле таксономии ключа: `initiator.antivirus.last.quick_scan.source`;
- Поле таксономии значения: `initiator.antivirus.last.quick_scan.source`.

Справочник значений:

Ключ	Значение
0	`scan didn't run`
1	`user initiated`
2	`system initiated`

В формате JSON:

```
[
  {
    "0": "scan didn't run",
    "1": "user initiated",
    "2": "system initiated"
  }
]
```

Пример обогащения:

- если при получении нормализованного события поле таксономии `initiator.antivirus.last.quick_scan.source` = **1**;
- то поле `initiator.antivirus.last.quick_scan.source` будет обогащено значением **user initiated**.

2.9.6.6 Обогащение по локальному адресу

В процессе обогащение по локальному адресу проверяется является ли пришедший в событии адрес локальным или нет.

Возможность использования обогащения по локальному адресу настраивается в разделе **Администрирование** → **Кластер** → вкладка **Управление конфигурацией**, где в древовидном списке нужно выбрать **Enrich** → **DNS** и настроить следующие параметры:

- Список локальных сетей;
- Список локальных доменов.

Пример настройки параметров обогащения по локальному адресу, при создании правила обогащения, приведен на рисунке 1.

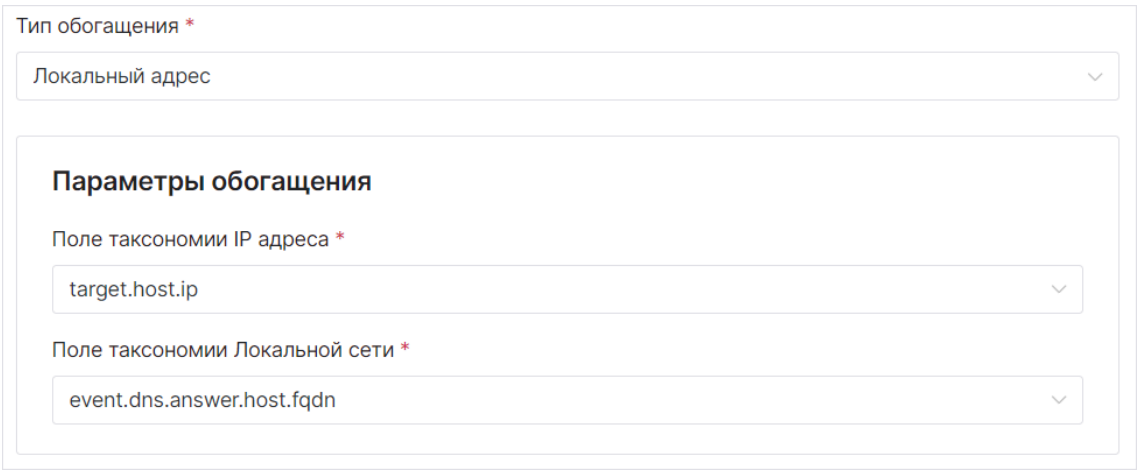


Рис. 69 – Параметры обогащения по локальному адресу

Для настройки параметров обогащения выполните следующие действия:

1. Выберите поле таксономии IP адреса.
2. Выберите поле для указания результата операции: входит ли значение из поля таксономии IP адреса в локальную сеть.

Принцип работы: Сервис берет значение, пришедшее в поле таксономии IP адреса и сравнивает его со списком IP адресов в локальной сети. Если совпадение найдено, то поле таксономии локальной сети обогащается информацией о том, входит ли IP-адрес в локальную сеть.

2.9.6.7 Корректировка времени

Обогащение событий с корректировкой времени — это процесс, при котором в события добавляются данные, связанные со смещением времени, например, сведения о часовом поясе.

Обогащение будет работать только для полей, в которых указывается метка времени, например `@timestamp, event.endtime, event.starttime, event.session.endtime` и т.д.

При указании смещения времени используется один из следующих форматов:

Формат записи	Пример	Результат
c	10800	Время в выбранном поле будет смещено на +10800 секунд
-c	-10800	Время в выбранном поле будет смещено на -10800 секунд

Пример настройки параметров обогащения по произвольному скрипту, при создании правила обогащения, приведен на «Рис. 70».

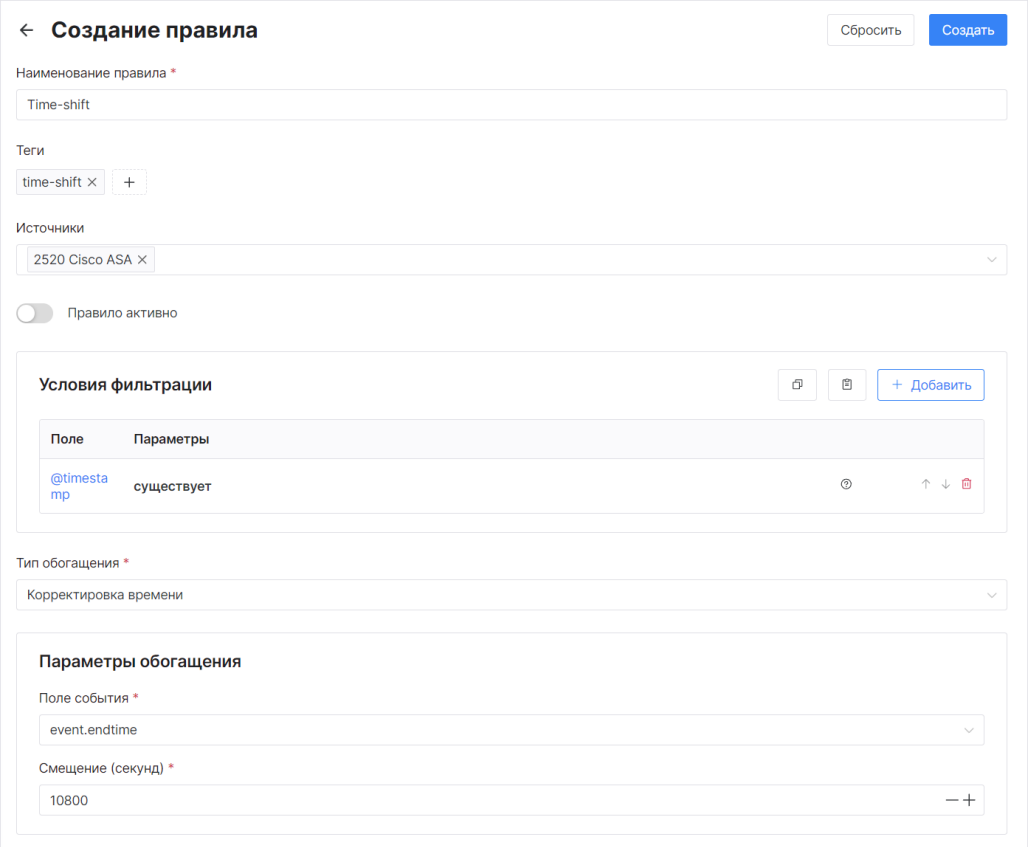


Рис. 70 – Параметры обогащения "Корректировка времени"

Для настройки параметров обогащения выполните следующие действия:

1. В поле **Поле события** из выпадающего списка выберите поле, к которому будет применена корректировка времени.
2. В поле **Смещение (секунд)** укажите смещение времени.

3. Лог-коллектор

3.1 Общие сведения

Лог-коллектор (RADAR LOG-COLLECTOR) предназначен для организации сбора событий от источников событий ИБ. Лог-коллектор позволяет организовать различные схемы сбора событий от любых источников, участвующих в сетевом взаимодействии и создающих журналы событий.

Основные функции лог-коллектора:

- сбор событий, локально и удалённо;
- отправка событий в другие системы;
- обработка событий перед отправкой;
- пересылка событий в зашифрованном виде и со сжатием;
- накопление событий при разрыве соединения и отправка после восстановления.

Варианты развертывания:

- установка на источнике для организации локального сбора событий с последующей передачей в **Платформу Радар** или в промежуточный лог-коллектор.
- установка на выделенный сервер для организации удаленного сбора и пересылки событий.
- установка цепочки лог-коллекторов для передачи событий в зашифрованном виде.

Работа с лог-коллектором включает в себя следующие процессы:

1. **«**Установка лог-коллектора**».**
2. **«**Настройка лог-коллектора**».**
3. «Настройка сервиса Log-proxy».

3.2 Установка лог-коллектора

3.2.1 Системные требования

Работа лог-коллектора возможна на следующих ОС:

- Windows Vista, Windows 10, Windows 11;
- Windows Server 2008, Windows Server 2011, Windows Server 2016, Windows Server 2019, Windows Server 2022;
- Linux Debian;
- Linux CentOS;
- Linux RedHat;
- Astra Linux.

Варианты конфигурации оборудования приведены в таблице:

	CPU (cores)	RAM	HDD (GB)
Минимальные аппаратные требования	4	4	50
Требования при установке с Windows Event Collector	4	8	500

На приведенных выше минимальных требованиях к ресурсам, лог-коллектор обеспечивает обработку потока 5000 событий в секунду.

Должны быть выполнены требования раздела «Межсетевое взаимодействие».

3.2.2 ОС Windows

В настоящем разделе подробно описана процедура установки и обновления лог-коллектора на ОС Windows.

3.2.2.1 Установка

Внимание! *Установка лог-коллектора осуществляется под учетной записью с правами администратора.*

Перед началом установки необходимо выполнить следующие действия:

- получить msi-пакет, который находится в каталоге `/opt/pangeoradar/repository/pangeoradar-logcollector/;`
- открыть порт `8080/tcp`.

Для запуска процесса установки запустите полученный файл. Откроется мастер установки лог-коллектора (см. «Рис. 71»).

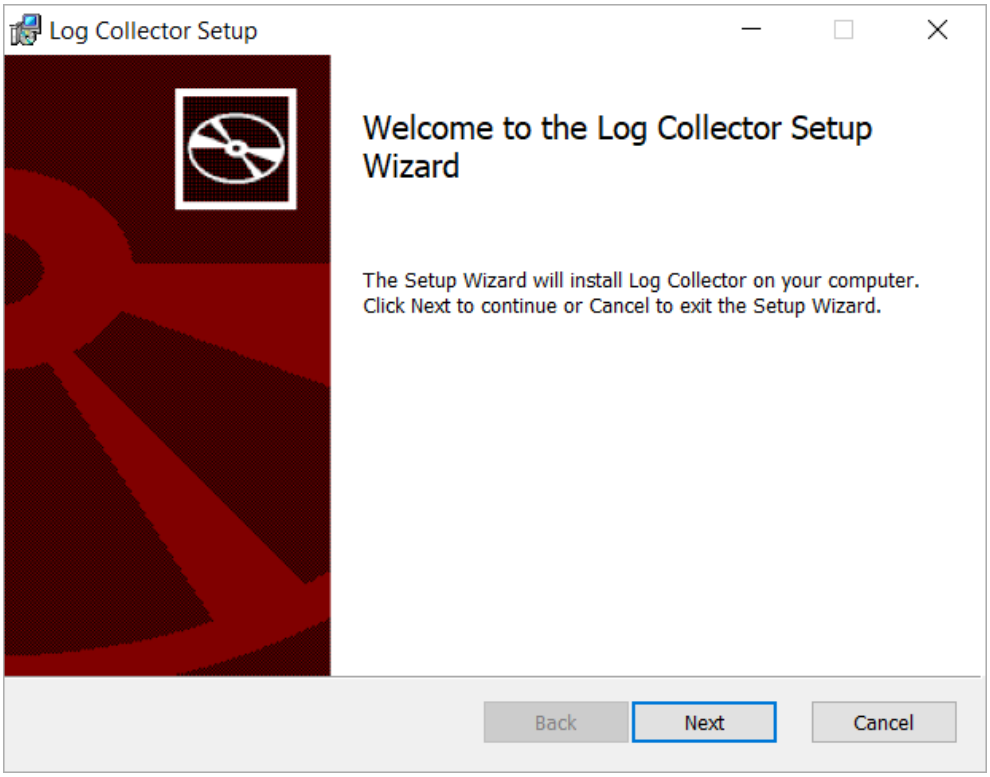


Рис. 71 – Запуск установки

Для перехода к началу установки нажмите кнопку **Next**.

3.2.2.1.1 Шаг 1. Путь установки

Укажите каталог, в который необходимо установить лог-коллектор (см. «Рис. 72»).

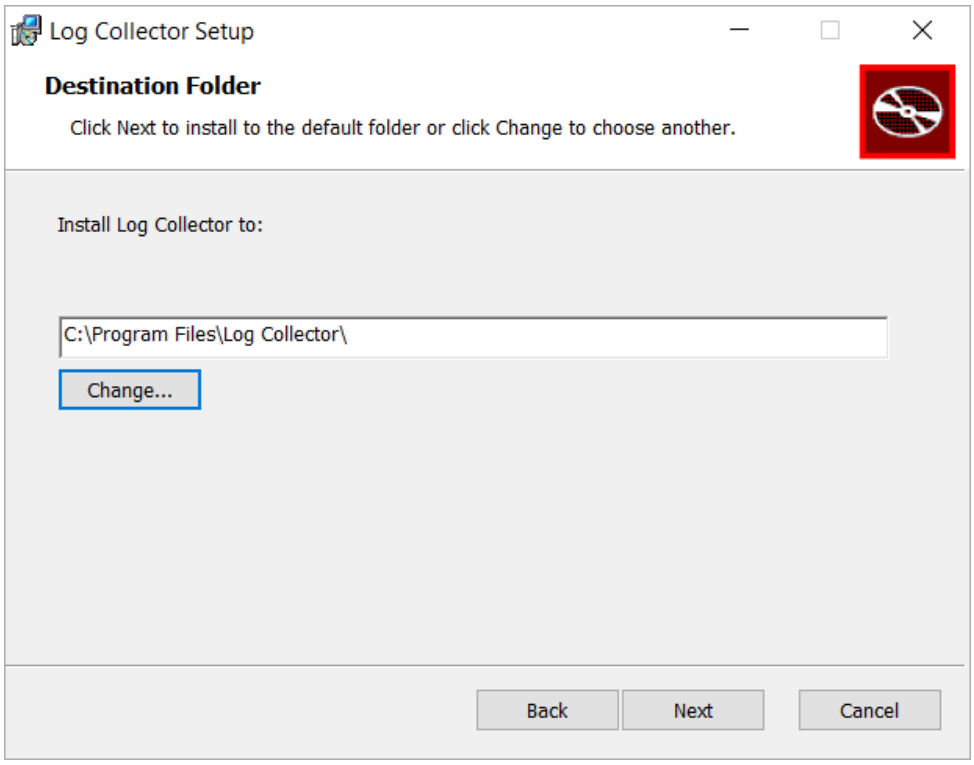


Рис. 72 – Путь установки программы

Для перехода к следующему шагу нажмите кнопку **Next**.

3.2.2.1.2 Шаг 2. Конфигурация подключения к платформе

Укажите параметры для подключения лог-коллектора к платформе (см. «Рис. 73»).

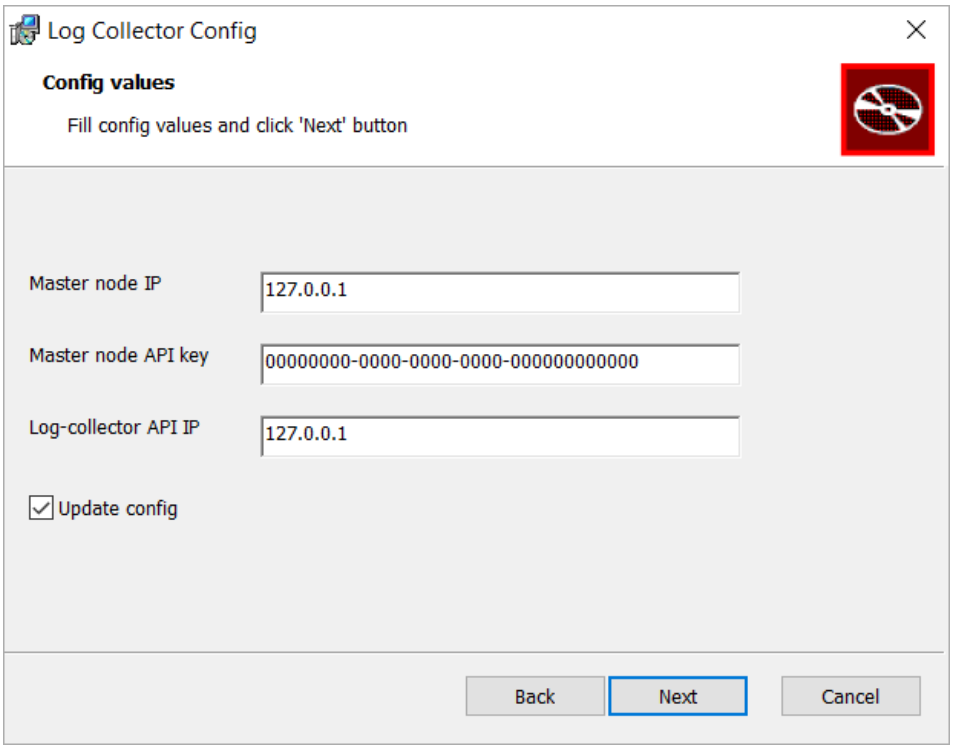


Рис. 73 – Параметры подключения к платформе

Если установка лог-коллектора уже выполнялась, то на данном шаге будет отображена прошлая конфигурация.

Для изменения конфигурации установите флаг **Update config** и укажите следующие данные:

- в поле **Master node IP** укажите IP-адрес платформы или IP-адрес узла на котором развернута роль **master**;
- в поле **Master node API key** укажите ваш ключ API, который можно получить в разделе **Администрирование** → **Кластер** → вкладка **API ключи**;
- в поле **Log-collector API IP** укажите IP-адрес сетевого интерфейса, который будет использоваться лог-коллектором.

Для перехода к следующему шагу нажмите кнопку **Next**.

3.2.2.1.3 Шаг 3. Завершение установки

Нажмите кнопку **Install** (см. «Рис. 74»).

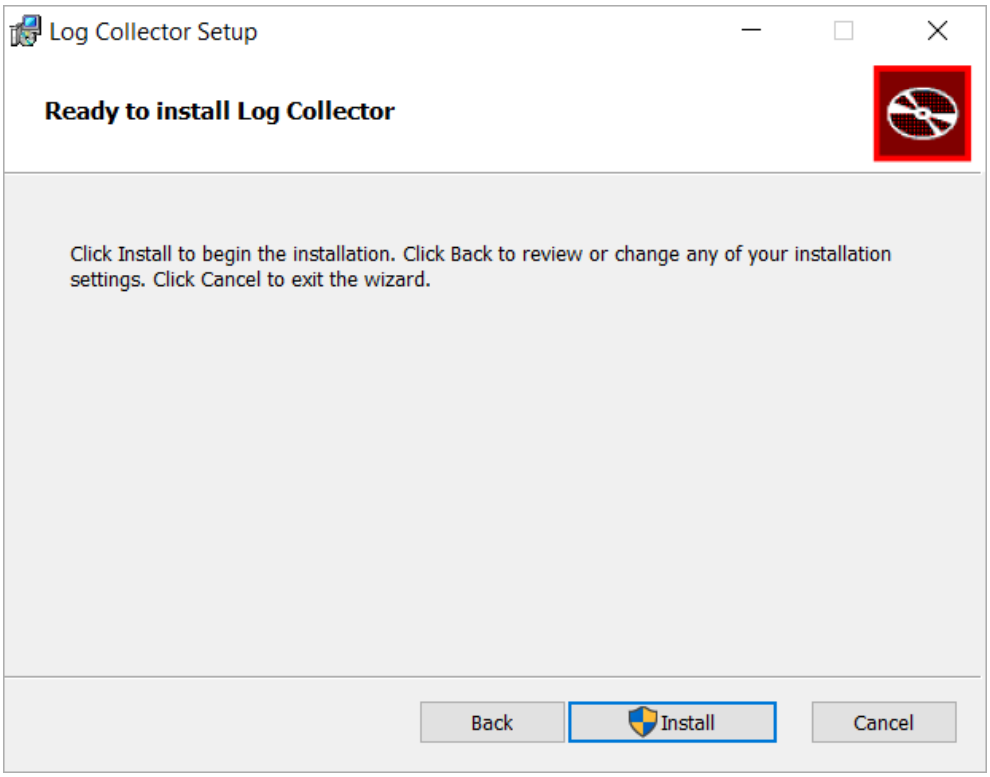


Рис. 74 – Установка платформы

Начнется процесс установки лог-коллектора (см. «Рис. 75»).

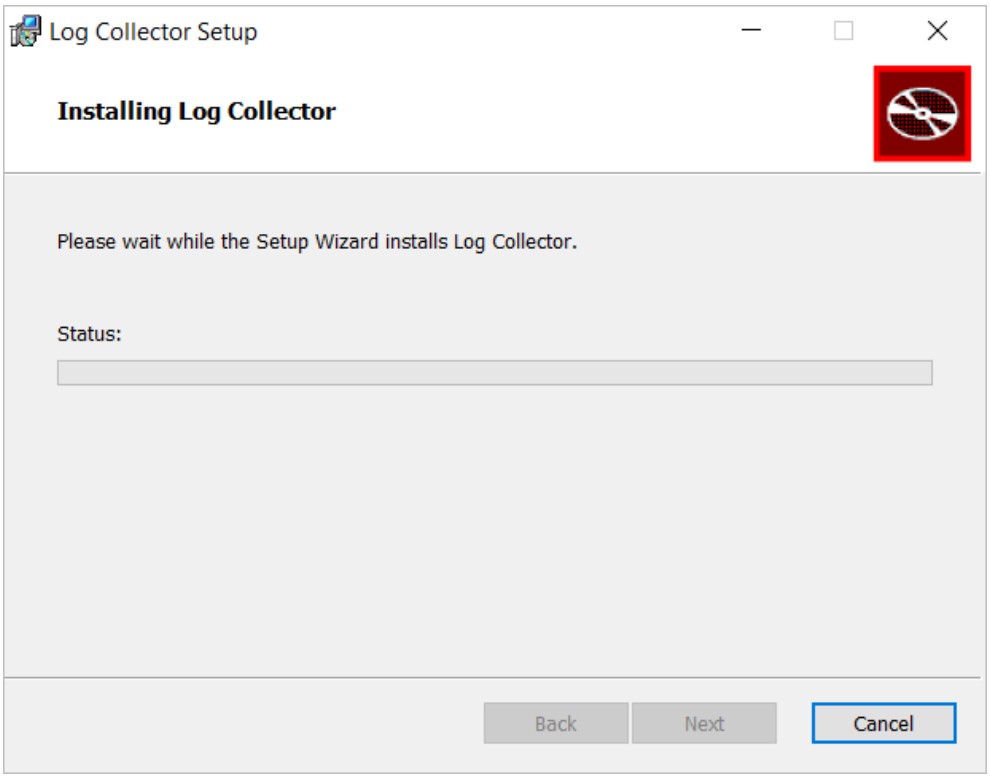


Рис. 75 – Процесс установки

По завершению процесса установки нажмите кнопку **Finish** (см. «Рис. 76»).

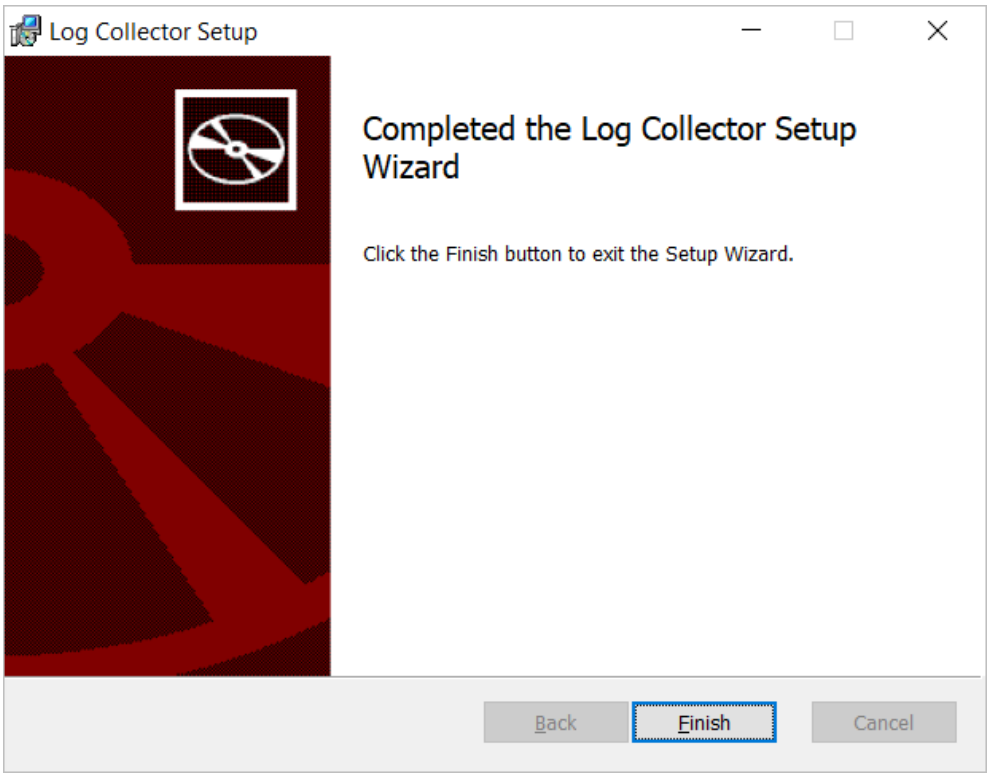


Рис. 76 – Завершение установки

3.2.2.1.4 Шаг 4. Установка сертификата для API взаимодействия

Для корректной работы API взаимодействия лог-коллектора с платформой, необходимо добавить сертификат платформы `pgr.srt` в доверенные сертификаты для учетной записи компьютера, на котором установлен лог-коллектор:

1. Получите сертификат `pgr.srt` по следующему пути: `/opt/pangeoradar/certs`.
2. Поместите его на нужный компьютер, вызовите контекстное меню и выберите пункт **Установить сертификат**.
3. Следуя инструкциям мастера импорта сертификатов, добавьте сертификат в доверенные (см. «Рис. 77»).

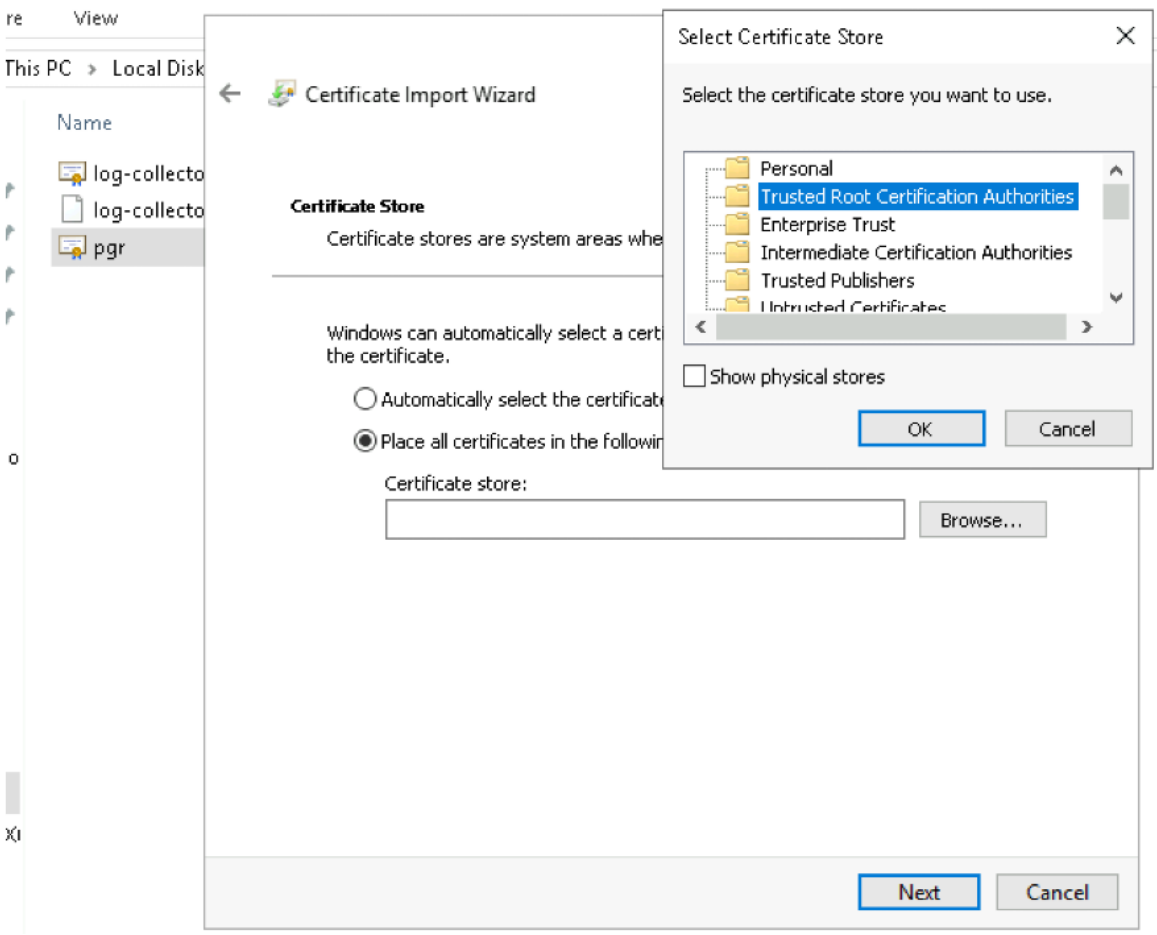


Рис. 77 – Импорт сертификата

3.2.2.1.5 Шаг 5. Запуск и Остановка лог-коллектора

Через службы (см. «Рис. 78»):

1. Запустите приложение **Службы/Services**.
2. Найдите в списке службу лог-коллектора Pangeo Radar Log Collector Service.
3. Нажмите кнопку **Запустить/Start** для запуска лог-коллектора или **Остановить/Stop** для остановки.

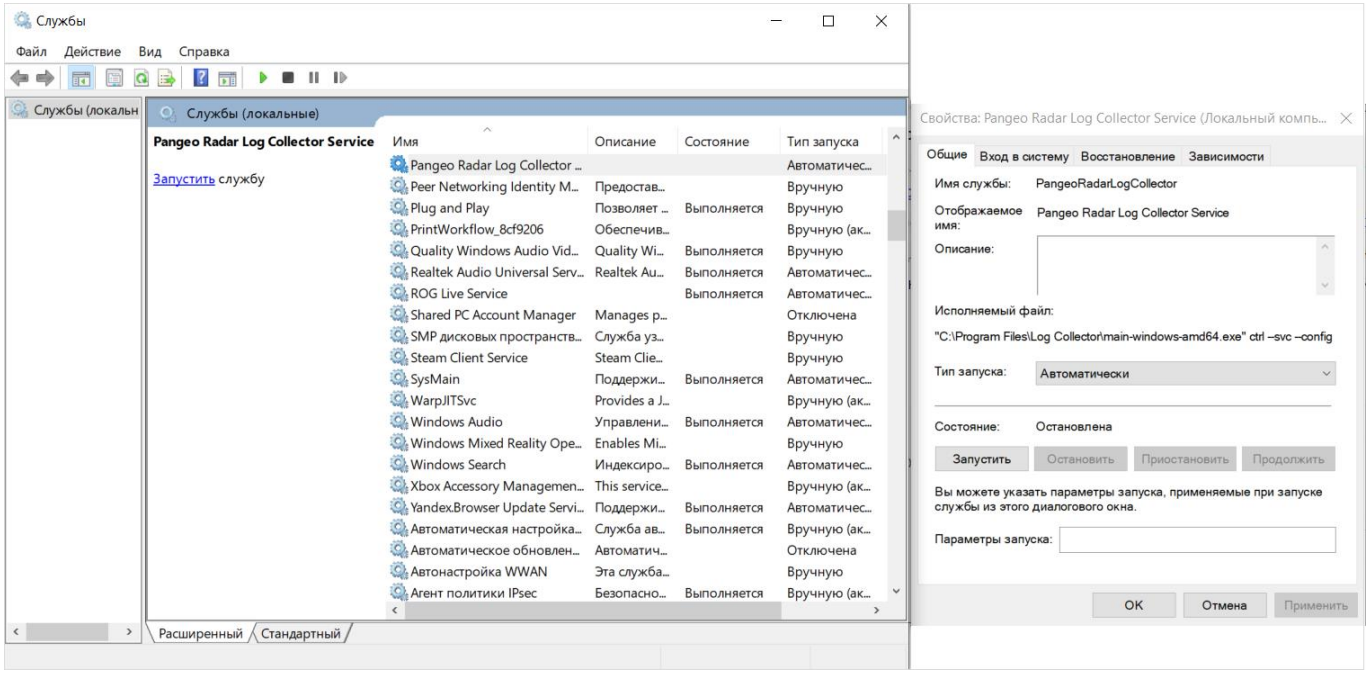


Рис. 78 – Запуск/Остановка службы лог-коллектора

Через терминал:

1. Запустите терминал/командную строку.
2. Перейдите в каталог с установленным лог-коллектором:

   ```
   # cd C:\Program Files\Log Collector
   ```

3. Для запуска лог-коллектора укажите следующую команду:

   ```
   # main-windows-amd64.exe ctrl
   ```

4. Для остановки работы лог-коллектора используйте сочетание клавиш `ctrl-c`.

3.2.2.1.6 Шаг 6. Проверка работы лог-коллектора

При первом подключении коллектора к платформе в разделе **Администрирование** → **Кластер** → вкладка **Узлы** появится узел с Windows-коллектором, которому будет присвоена роль `agent`. Данному узлу необходимо добавить роль `agent_win`.

При необходимости проверьте журнал работы лог-коллектора. Для этого в разделе **Администрирование** → **Кластер** → вкладка **Узлы** откройте узел с ролью `agent_win` и в блоке **Информация об агенте** нажмите кнопку **Показать логи**.

При наличии включенного локального брандмауэра необходимо открыть порты для межсетевого взаимодействия (см. раздел «Межсетевое взаимодействие»).

Выполните настройку лог-коллектора на прием и отправку событий (см. раздел «Настройка лог-коллектора»).

3.2.2.2 Переустановка и Обновление

Перед переустановкой или обновлением лог-коллектора выполните следующие действия:

- в случае обновления лог-коллектора, получите msi-пакет с обновленной версией лог-коллектора у службы технического сопровождения по электронному адресу support@pangeoradar.ru;
- в случае переустановки лог-коллектора, получите msi-пакет, который находится в каталоге `/opt/pangeoradar/repository/pangeoradar-logcollector/`;
- сделайте резервную копию профилей сбора (для этого можно выполнить операцию экспорта);
- удалите установленную версию лог-коллектора через механизм ОС Windows **Установка и удаление программ → Удалить**.

Запустите полученный msi-пакет и следуйте инструкциям мастера установка. Действия будут аналогичны следующим шагам по установке: «Шаг 1. Путь установки» - «Шаг 3. Завершение установки».

Проверьте корректность профилей сбора после обновления. При необходимости выполните импорт ранее сохраненных профилей сбора.

Для устранения проблем, возникших в ходе установки лог-коллектора, воспользуйтесь функцией восстановления целостности файлов. Для этого воспользуйтесь функцией **Установка и удаление программ → Изменить**. Откроется мастер установки лог-коллектора (см. «Рис. 79»).

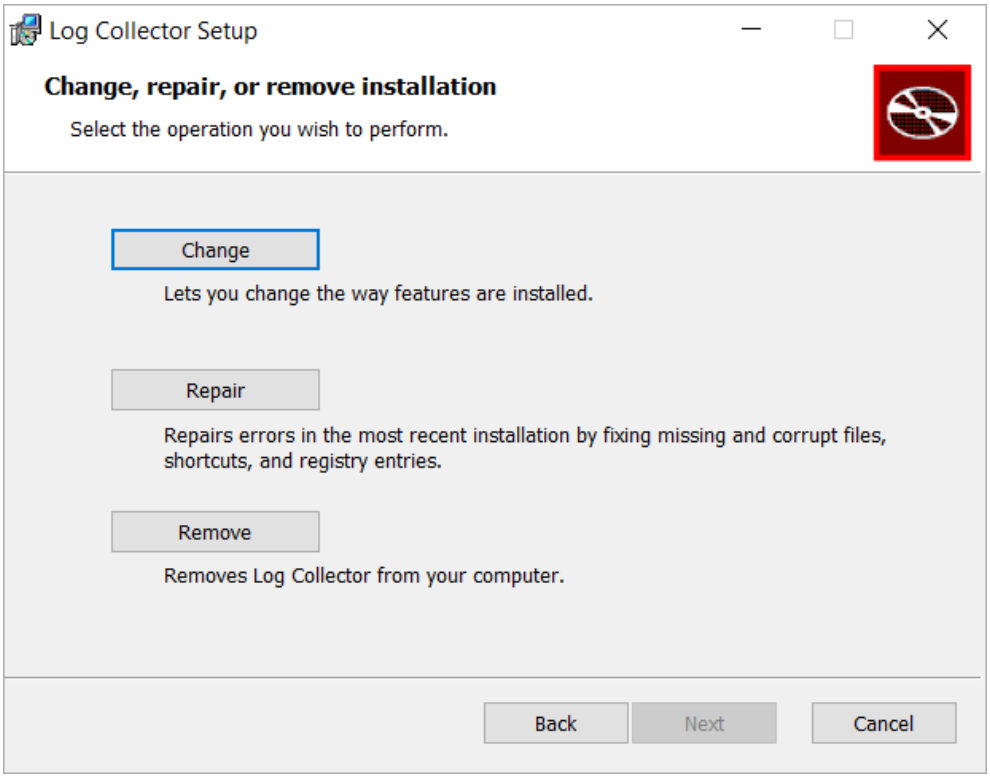


Рис. 79 – Обновление/переустановка лог-коллектора

Нажмите кнопку **Repair**. Начнется процесс восстановления (см. рисунок 10).

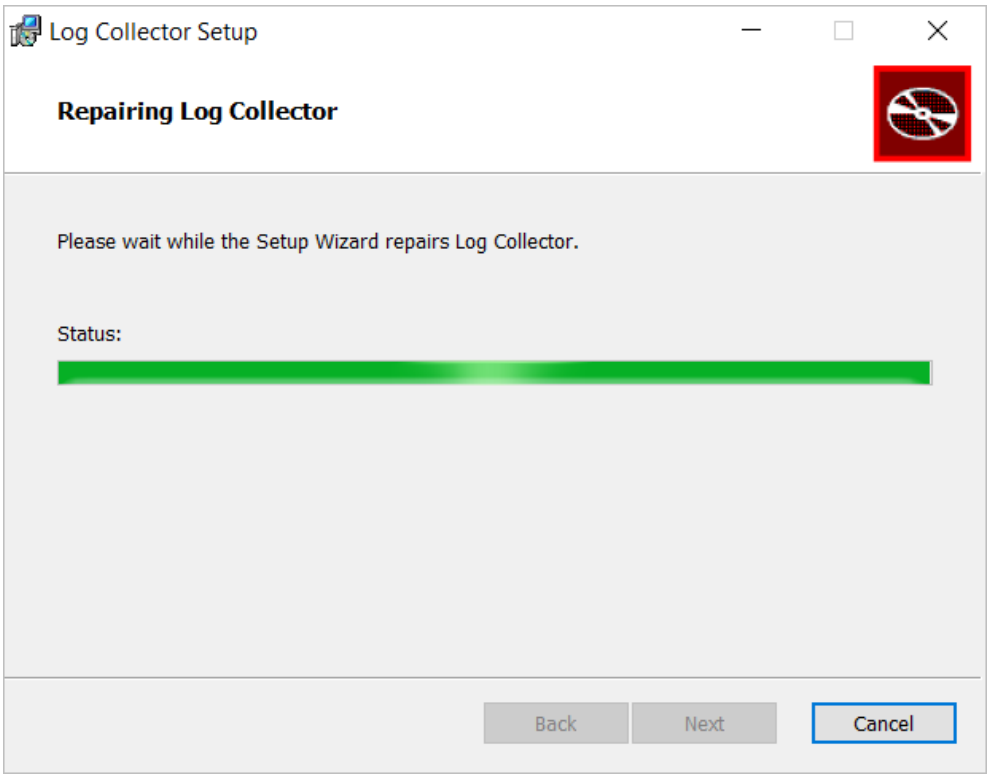


Рис. 80 – Восстановление целостности файлов лог-коллектора

3.2.3 ОС Linux

В настоящем разделе подробно описана процедура установки и обновления лог-коллектора на ОС Linux.

3.2.3.1 Автоматическая установка

Во время установки **Платформы Радар** на один сервер, лог-коллектор автоматически устанавливается на платформу и подключается по защищенному протоколу.

Во время распределенной установки, лог-коллектор автоматически устанавливается на узле с ролью **agent**.

Для проверки установки лог-коллектора в веб интерфейсе платформы перейдите в раздел **Администрирование** → **Кластер** → вкладка **Узлы** и удостоверьтесь что сервис **logcollector** работает в штатном режиме (индикатор – ●).

Для установки лог-коллектора на выделенный узел выполните следующие действия:

1. Добавьте узел со следующими параметрами:
   - в поле **Название** укажите наименование узла;
   - в полях **Логин** и **Пароль** укажите данные для подключения привилегированного пользователя root к узлу;
   - в полях **IP** и **Порт** укажите IP-адрес и порт подключения к узлу, на котором будет установлен лог-коллектор.
2. Начнётся процесс добавления узла в кластер с установкой и настройкой необходимых компонентов.

3. После успешного добавления узла ему необходимо добавить роль **agent**. После добавления роли на форме просмотра узла появятся следующие блоки для управления параметрами лог-коллектора: **Управление агентом**, **Секреты агента**, **Информация об агенте** (см. «Рис. 81»).

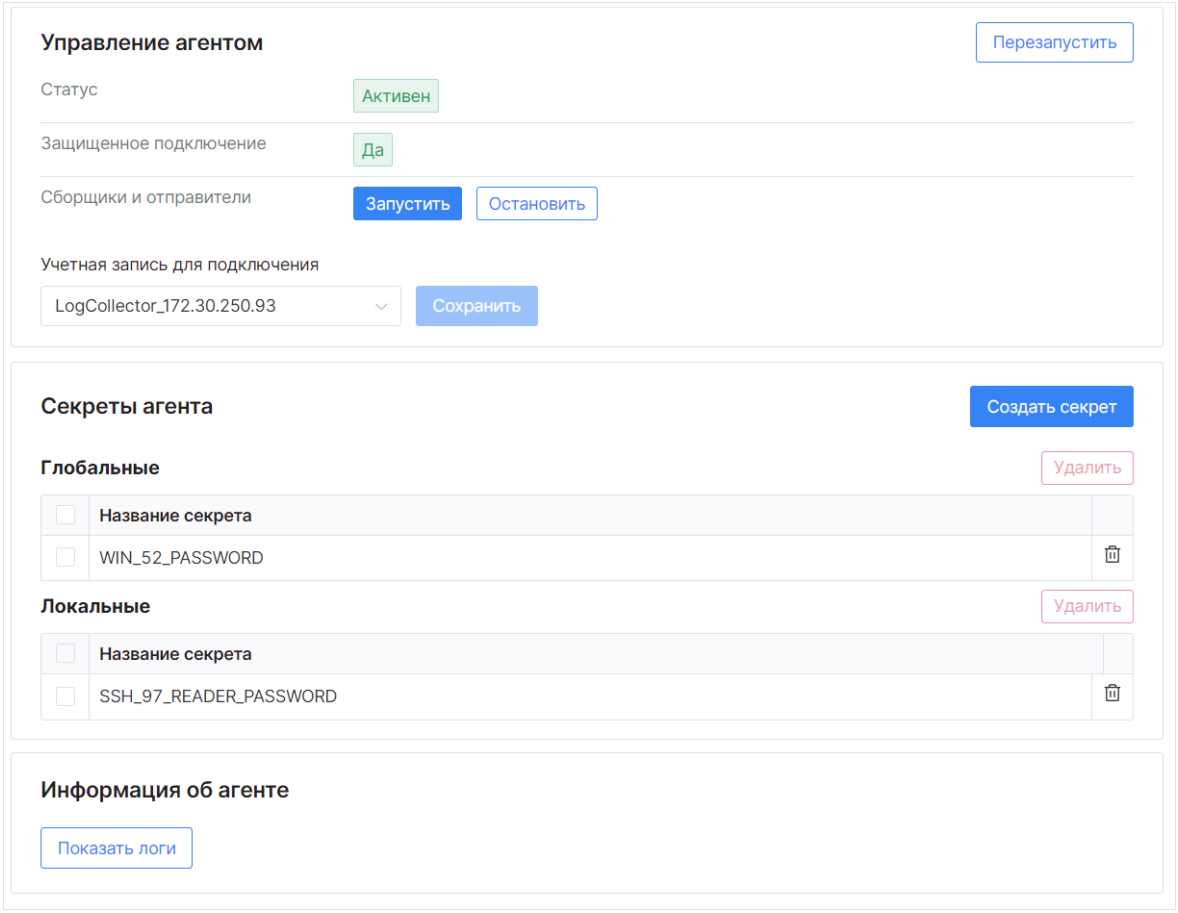


Рис. 81 – Форма просмотра узла. Блоки управления агентом

4. По установки роли **agent** на узле будет развернут агент сбора. Проверьте параметры агента сбора и выполните настройку профилей сбора на данном агенте (см. раздел «Настройка лог-коллектора»).

5. На узле лог-коллектора выполните команду для разрешения взаимодействия по порту API (например, 8080):

   ```
   # ufw allow 8080
   ```

   Этой же командой выполните открытие портов, необходимых для приема событий на лог-коллекторе.

6. Проверить журнал на предмет наличия или отсутствия ошибок. Для этого на форме просмотра узла с ролью **agent** в блоке **Информация об агенте** нажмите кнопку **Показать логи**. Откроется окно **Просмотр логов** (см. «Рис. 82»).

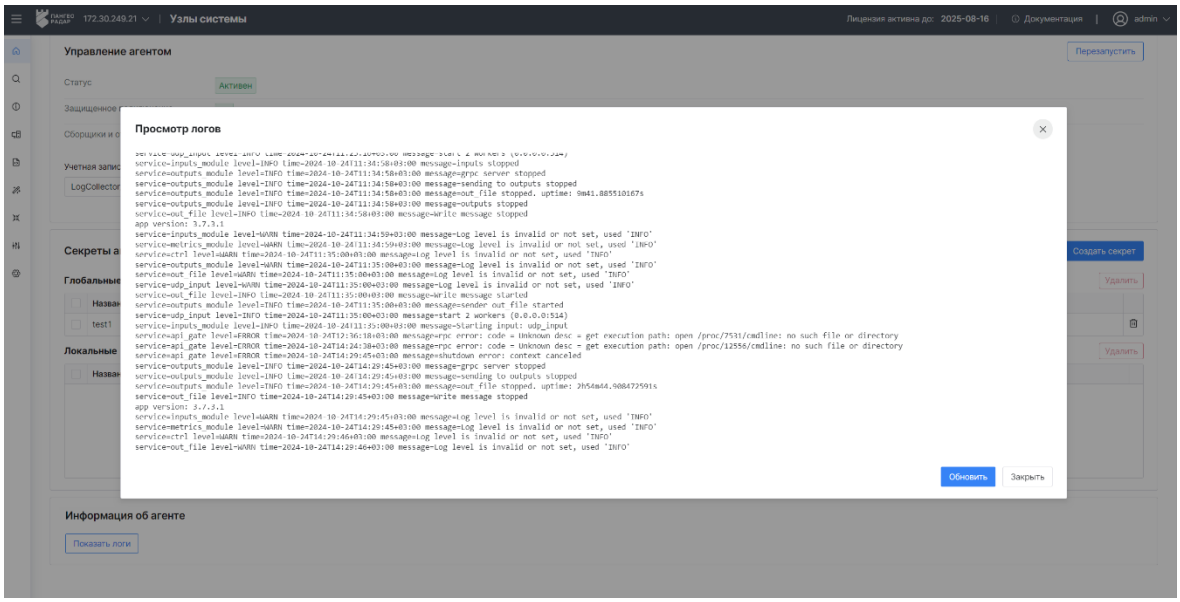


Рис. 82 – Окно "Просмотр логов"

7. Проверить наличие сертификата `pgr.crt` для API-взаимодействия в каталоге `/opt/pangeoradar/certs/`. Если сертификат отсутствует, то выполните следующие действия:

   - при необходимости создайте каталог для хранения сертификата:

     ```
     # mkdir -p /opt/pangeoradar/certs/
     ```

   - получите сертификат для доступа к узлу с ролью **MASTER**:

     ```
     # echo | openssl s_client -servername <ip/fqdn адрес узла с ролью мастер> -connect <ip/fqdn адрес узла с ролью мастер>:443 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /opt/pangeoradar/certs/pgr.crt
     ```

   - выполните установку сертификата:

     ```
     # mkdir -p /usr/local/share/ca-certificates/pangeoradar

     # cp /opt/pangeoradar/certs/pgr.crt /usr/local/share/ca-certificates/pangeoradar/

     # chmod 755 /usr/local/share/ca-certificates/pangeoradar

     # chmod 644 /usr/local/share/ca-certificates/pangeoradar/pgr.crt

     # update-ca-certificates
     ```

8. При наличии включенного локального файрволла откройте порты для межсетевого взаимодействия (см. раздел «Межсетевое взаимодействие»).

3.2.3.2 Ручная установка, обновление и переустановка

Внимание! *Все действия в разделе осуществляются под учетной записью с правами администратора.*

По умолчанию лог-коллектор обновляется автоматически с обновлением платформы.

Перед ручной установкой, обновлением или переустановкой лог-коллектора выполните следующие действия:

- получите deb-пакет для Linux с нужной версией лог-коллектора у службы технического сопровождения по электронному адресу support@pangeoradar.ru.

  Например, `log-collector_amd64_<номер версии>.deb`;

- сделайте резервную копию профилей сбора (для этого можно выполнить операцию экспорта в соответствующем разделе).

Выполните следующие действия:

1. Посмотрите название установленного пакета лог-коллектора:

   ```
   # dpkg -s | grep pangeoradar-logcollector
   ```

2. Проверьте запущен ли сервис лог-коллектора:

   ```
   # systemctl status pangeoradar-logcollector.service
   ```

   Если сервис имеет статус `active (running)`, то остановите сервис:

   ```
   # systemctl stop pangeoradar-logcollector.service
   ```

3. Удалите предыдущую версию лог-коллектора:

   ```
   # dpkg -r <название установленного пакета лог-коллектора>
   ```

   При выполнении команды у вас запросит подтверждение выполняемой операции, внимательно ознакомьтесь с данным сообщением.

   Если все указано верно, введите **Y**.

4. Проверьте удаление пакета:

   ```
   # dpkg -s | grep pangeoradar-l
   ```

5. Установите новый пакет лог-коллектора:

   ```
   # dpkg -i <наименование нового пакета лог-коллектора>.deb
   ```

6. После установки проверьте корректность профилей сбора. При необходимости импортируйте актуальные профили сбора.

7. Выполните перезагрузку сервиса лог-коллектора:

   ```
   # systemctl restart pangeoradar-logcollector.service
   ```

8. Для проверки правильности установки пакета и правильности работы сервиса выполните следующие команды:

   ```
   # dpkg -s pangeoradar-log-collector
   # systemctl status pangeoradar-logcollector.service
   ```

3.2.4 Межсетевое взаимодействие

Внимание! *Для корректной работы лог-коллектора должно быть обеспечено двухстороннее взаимодействие с подсистемой управления* ***Платформой Радар*** *(узлом с ролью MASTER). Это необходимо для того, чтобы лог-коллектор мог беспрепятственно слать и получать запросы от ядра платформы.*

В таблице ниже представлено межсетевое взаимодействие лог-коллектора с платформой и источниками.

Табл. 2 – Межсетевое взаимодействие лог-коллектора с платформой и источниками

Исходящий	Входящий	Порты	Описание
Log-Collector	Master	9009	Взаимодействие с Мастером
Master	Log-Collector	8080/tcp (Windows-версия), 8085/tcp, 22/tcp (Linux-версия), 6677/tcp (Linux-версия), 9100/tcp (Linux-версия)	Управление коллектором с мастера и сбор статистики
Источники событий	Log-Collector	1500-5000/tcp, 500-5000/udp	Пассивный сбор событий
Log-Collector	Источники событий	22/tcp 135/tcp, 135/udp, 445/tcp 1433/tcp, Динамический диапазон портов Microsoft RPC (49152-65535/tcp)	Активный сбор событий
АРМ администратора	IP-адрес лог-коллектора	22/tcp (Linux-версия), 3389/tcp (Windows-версия), 3389/udp (Windows-версия)	Администрирование
Log-Collector	Log-proxy	1100/tcp 1100/udp	Отправка событий в сервис **Kafka**

3.2.5 Включение API взаимодействия

Сгенерируйте сертификат agent.crt для узла с ролью AGENT:

```
# openssl req -newkey rsa:4096 -nodes -keyout agent.key -x509 -days 365 -out agent.crt -addext 'subjectAltName=IP:<log-collector's ip>' -subj '/C=RU/ST=RU/L=<location>/O=<organization>/OU=<department>/CN=<log-collector's ip>/'
```

Где:

- **log-collector's ip** – IP-адресс лог-коллектора;
- **location** – расположение (например: Moscow);
- **organization** – наименование организации;
- **department** – наименование подразделения.

Проверьте сгенерированный сертификат:

```
# openssl x509 -in agent.crt -text
```

Пример выполнения команды

```
-----BEGIN CERTIFICATE-----
MIIFtTCCA52gAwIBAgIUSg8zcrBo9qojzqo8/0B+xzgkwvcwDQYJKoZIhvcNAQEL
BQAwWTELMAkGA1UEBhMCUlUxCzAJBgNVBAgMAlJVMQ8wDQYDVQQHDAZNb3Njb3cx
CzAJBgNVBAoMAlREMQswCQYDVQQLDAJURDESMBAGA1UEAwwJMTAuMC4xLjI3MB4X
DTIxMTIwMTE3MTI1MloXDTIyMTIwMTE3MTI1MlowWTELMAkGA1UEBhMCUlUxCzAJ
BgNVBAgMAlJVMQ8wDQYDVQQHDAZNb3Njb3cxCzAJBgNVBAoMAlREMQswCQYDVQQL
DAJURDESMBAGA1UEAwwJMTAuMC4xLjI3MIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAwy2II3egewxF13uspu4zi2G6O1VAxILaBKvmkaADcRnqTOii51w3
ltBHkij1PF4rJKKnz04g74SBhjAvs7MPvFcbNt+A22cDJoL3rUgPhcoOTFTkDQQw
q2AEfJ0r9Ojc5quG9djbnhf5XjUxeCklBIHWbhrJdpuJ7QLKgCHebiC8Z8JL0GUh
WM0NK/KPrf+LxJPyz7ItmCI/ORvB7bwE6XQ7lG+6pIHCvY0MZL5Du3H4yKOfSutw
v05q+/ELQSQGDRJK38uaU8G6r7BO2XA+9XpH0g8v3wcQwq7a/l9/64ORx0HWescc
cubxYnnjZswNyuw7eb28TwSEAGH0YyDtouN8OTb5CLVo+MD88q12L6oENwbXZG4C
SJrH29GoFlbxVSGeX879y6dWWUZM7c5JolaCwrHh6iJgkNBIRsX8hYmsQ2HylhEJ
2xVzwbETAXcFAwNbX0vHRLcoKG/+2EYA+xT+xj3LBVFkV9ws0Ue8EVpGXNHfKdy4
DH3BmWMtRYdThWIVLIfZP7Wl9SDD1vC6XiwO0znmkp+nslFhmE7m+fWdNIOE3XJR
Dv//OEraSbYHTdzEhOESssonLaGt2IC07FPoqJAMp6rz7Q26xzLb1UOcWUGiai9s
4fBCVG9gC3EkKRc2HoIoPd9opTsaBwJP1DXPX2W4U63lV4B+Z0sy3hUCAwEAAaN1
MHMwHQYDVR0OBBYEFPfi3rgrI0eZ0DYi8SEylx/Qa00IMA8GA1UdEQQIMAaHBAqq
CRUwHwYDVR0jBBgwFoAU9+LeuCsjR5nQNiLxITKXH9BrTQgwDwYDVR0TAQH/BAUw
AwEB/zAPBgNVHREECDAGhwQKAAEbMA0GCSqGSIb3DQEBCwUAA4ICAQCFMNG0eR9Q
+txzRY7B4daGMiE7jcUi+YanactTeivZLmND+6aCi/SuEEWU9fR+A82qMoOLhUb2
mAOir2uT0twligvmTsRSABFS0aDIlEQXIgmp2fAq/BtorRDLNDSs8aCVzuh6aWl/
0M2tM2lEDOo1CutK1b9CLGnQQgT3J0Xmmh32tLyblXyn3arrpHTnOJpUjeoj2b5R
wZC/TZlcgs3WBN21fC4a2waVa/he1C/1cJILSH0N2zoeAgRjZz8zV4IYRpuldM3/
pdZctdbozN3L846n5jasmTNs4cDrcBmbkNVJlEFaNo33hwo9NY//u09UPEh4q/Gi
RHRk5f7JxZlGOd/VEuYzEY+yNM2wxwCJNLhvJ/0j4LaKVuD/TmnrK4QGIcdDDga7
ZVT2/1aV4pHthZDv0mosvLY4OhXKi93aXsZxa8O25qHQJC8MQ852UKDvhsZ4Uvrf
kAGQxe9MgqccOs/vngZMwQdMPzXVsjtUDaX5hDRUYBZmnrDZY7Yzlp2F43aqyC/A
aO5np4qOSlsaHIZw3nSongpv+xIk97/jrPaaWBAFNAsqBSvBSqCFhTSY3o9W4UZk
9pI5HVbXdPOb1S2uEGqL5OGnbMwVAFXj1gidmunXkZSzrKgkJPjMUg7q/+PoVzrU
vpOnAxWtryPrBp9yZcyFBdH1nKOB79uFRg==
-----END CERTIFICATE-----
```

Добавьте сертификат на узел с ролью **AGENT** или **AGENT WIN**:

1. Скопируйте тело сертификата.
2. В веб интерфейсе платформы перейдите в раздел **Администрирование** → **Кластер** → вкладка **Учетные записи для сбора данных**.
3. Добавьте учетную запись для сбора данных с типом авторизации **Сертификат**, в поле **Сертификат** укажите скопированное тело сертификата и в поле **Транспорты** добавьте протоколы `wmi`, `rpc`, `ssh` (см. «Рис. 83»).

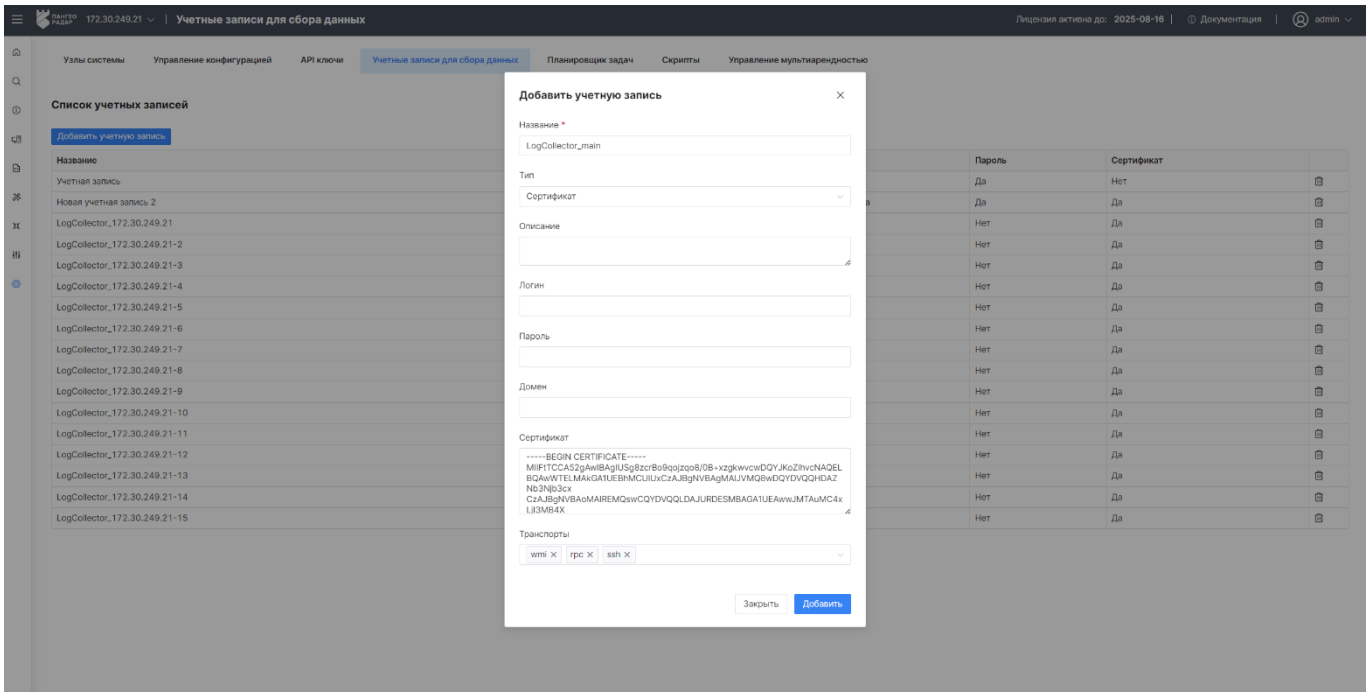


Рис. 83 – Добавление учетной записи для сбора данных

4. Перейдите в раздел **Администрирование → Кластер →** вкладка **Узлы системы**.
5. Откройте форму просмотра узла с ролью **AGENT** или **AGENT WIN** и перейдите к блоку **Управление агентом** (см. «Рис. 84»).

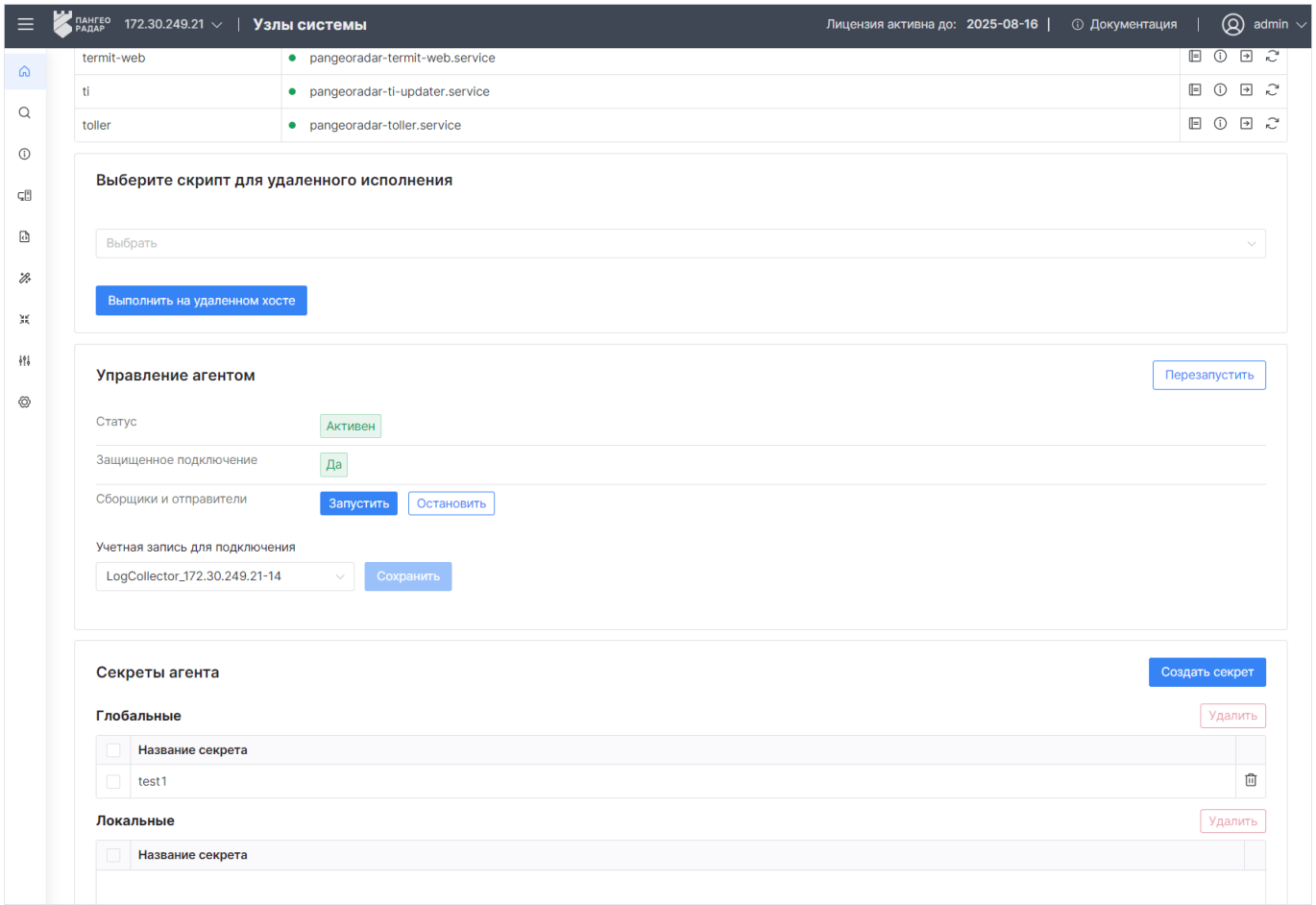


Рис. 84 – Форма просмотра узла. Блок "Управление агентом"

6. В блоке **Управление агентом** выполните следующие действия:
    - в поле **Учетная запись для подключения** из выпадающего списка выберите учетную запись для сбора данных;
    - в поле **Сборщики и отправители** при необходимости запустите компоненты сбора и отправки событий.

      Примечание: *перед запуском, соответствующие компоненты сбора и отправки событий должны быть настроены в конфигурационном файле лог-коллектора*.
    - нажмите кнопку **Перезапустить**.

3.3 Настройка лог-коллектора

3.3.1 Описание

Настройка лог-коллектора заключается в конфигурировании **Агентов сбора** и **Профилей сбора** под особенности инфраструктуры организации.

Агент сбора – это компонент лог-коллектора, отвечающий за сбор событий от источников. Агент сбора создается автоматически при назначении узлу кластера соответствующей роли:

- **agent** – на узле будет установлена версия агента сбора для ОС Linux;
- **agent win** – на узле будет установлена версия агента сбора для ОС Windows.

Примечание: *перед началом настройки лог-коллектора добавьте и установите (раскатите) соответствующие роли на нужных узлах*.

В агент сбора входят следующие компоненты:

- **Контроллер** – общие параметры управления лог-коллектором и настройка поведения лог коллектора при достижении предела занятого места на диске;
- **API Server** – предоставляет возможность удаленного управления лог-коллектором и мониторинга;
- **Сбор метрик** – осуществляет сбор статистики по работе лог-коллектора;
- **Журналирование** – осуществляет ведение журнала работы лог-коллектора.

Управление агентами сбора описано в разделе «Агенты сбора».

Профиль сбора – это набор настроек, отвечающий за сбор событий ИБ с конкретных источников. Принцип настройки лог-коллектора подразумевает что для одного агента сбора может быть настроено произвольное количество профилей сбора. Необходимое количество профилей сбора определяется количеством источников, с которых будет осуществляться сбор.

В зависимости от типа сбора событий компонент может работать в следующих режимах:

- **Активный** – лог-коллектор, согласно настройкам профиля сбора событий, будет обращаться к источнику для сбора событий;
- **Пассивный** – источник самостоятельно отправляет события в лог-коллектор.

Режимы работы профилей сбора также определяются по способу сетевого взаимодействия с источником:

- **Локальный** – лог-коллектор располагается на источнике, а именно лог-коллектор устанавливается в системе в виде агента и производит чтение файлов журналов;
- **Удаленный** – взаимодействие между лог-коллектором и источником выполняется по сети. Лог-коллектор устанавливается на выделенный сервер и осуществляет удаленный сбор событий. Также может быть установлен на конечном источнике событий, и осуществлять сбор не только с этого источника событий, но и с других систем.

За параметры сбора по различным протоколам и типам источников отвечают модули сбора, которые входят в состав профиля сбора. В зависимости от ОС, на которой функционирует агент сбора, поддерживаются следующие модули сбора:

Табл. 3 – Перечень поддерживаемых модулей сбора

№	Модуль сбора	Windows	Linux	Описание
1	etw_input	+	–	Сбор событий через Event Tracing for Windows
2	eventlog_input_local	+	–	Сбор событий через Windows EventLog (механизм RPC)
3	eventlog_input_remote	+	–	Сбор событий через Windows EventLog (механизм RPC)
4	external_command_input	+	+	Выполнение внешней команды в ОС
5	file_input	+	+	Чтение локального файла
6	ftp_input	+	+	Чтение файла, доступного через FTP
7	http_collector_input	+	+	Чтение файла, доступного через HTTP/HTTPs
8	http_request_input	+	+	Приём HTTP/HTTPs-запросов
9	kafka_input	–	+	Компонент отправляет получаемый поток событий в сервис Kafka.
10	mseven6_input	–	+	Сбор событий через Windows EventLog (механизм RPC)
11	netflow (nf_input)	+	+	Прием NetFlow трафика
12	odbc_input	+	+	Чтение данных из СУБД (MySQL, Oracle, MS SQL, PostgreSQL)
13	opsec_lea_input	–	+	Сбор событий с источников Checkpoint
14	sftp_input	+	+	Чтение файла, доступного через SFTP
15	smb_input	+	+	Чтение файла, доступного через SMB
16	snmp_input	+	+	Приём SNMP Traps
17	ssh (ssh_collector_input)	+	+	Выполнение внешней команды через SSH

№	Модуль сбора	Windows	Linux	Описание
18	tcp_input	+	+	Приём TCP трафика
19	udp_input	+	+	Приём UDP трафика
20	wmi_input	+	–	Сбор событий через механизм WMI

После сбора и обработки событий профилем сбора, они отправляются в очередь на отправку. В зависимости от типа данных (структурированные/неструктурированные), получаемых от источника, к ним можно применить фильтр для формирования очереди. Фильтры используют механизм черных и белых списков. Подробнее см. раздел «Фильтрация».

Управление профилями сбора описано в разделе «Профили сбора».

3.3.2 Агенты сбора

Работа с агентами сбора включает в себя следующие процессы:

1. «Просмотр агента сбора».
2. «Настройка агента сбора».
3. «Публикация изменений».
4. «Изменение состояния профиля сбора».

Для работы с агентами сбора перейдите в раздел **Источники → Агенты сбора** (см. «Рис. 85»).

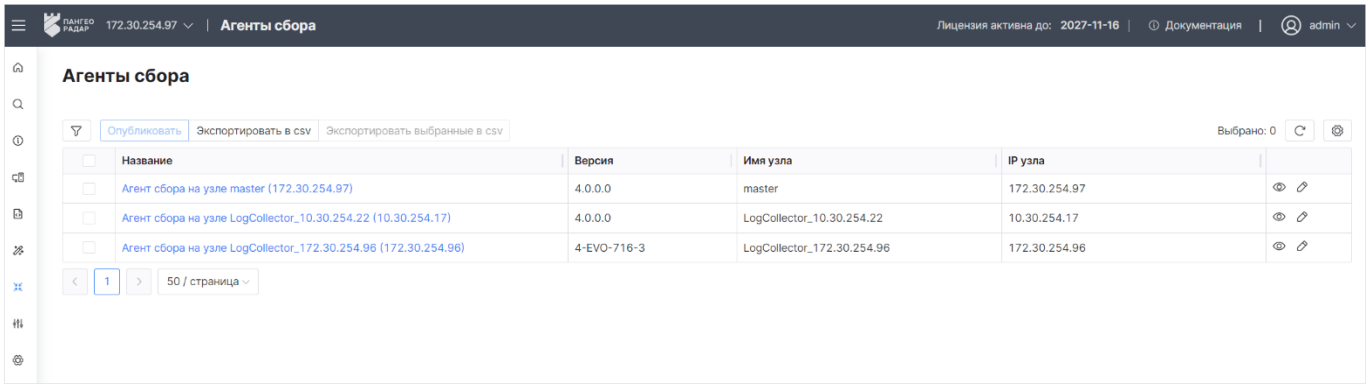


Рис. 85 – Раздел "Агенты сбора"

В разделе отображается следующая информация:

- **Название** – наименование агента сбора;
- **Версия** – версия агента сбора, установленного на узле;
- **Имя узла** – наименование узла, на котором установлен агент сбора;
- **IP узла** – IP-адрес узла, на котором установлен агент сбора.

При работе над агентами сбора доступны следующие элементы управления:

Кнопка	Действие

Кнопка	Действие
	просмотр поля события
	редактирование информации о поле события

3.3.2.1 Просмотр агента сбора

Открыть агент сбора на просмотр можно двумя способами:

- нажмите кнопку  в строке нужного агента сбора;
- нажмите по ссылке в графе "Название".

Откроется форма просмотра агента сбора (см. «Рис. 86»).

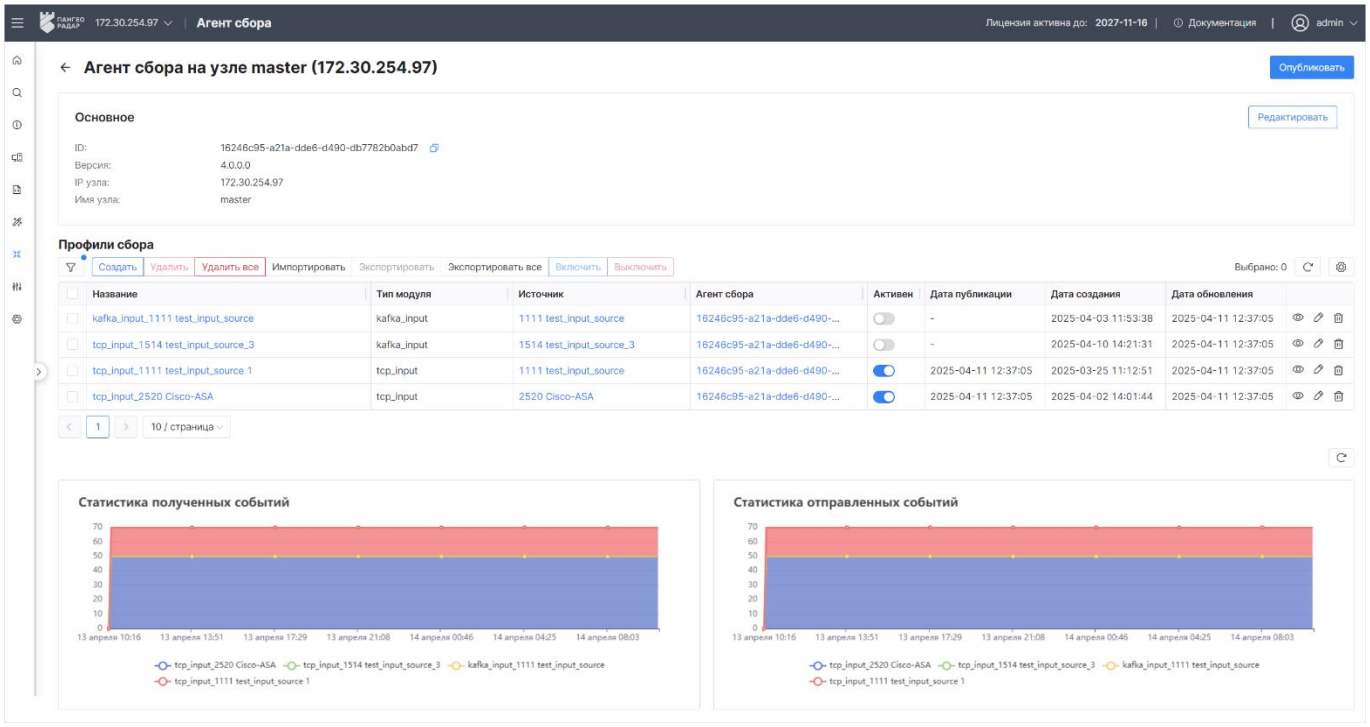


Рис. 86 – Форма "Просмотр агента сбора"

На форме отображается следующая информация:

- Блок **Основное** – содержит следующую информацию:
  - Наименование агента сбора;
  - **ID** – идентификатор агента сбора;
  - **Версия** – версия лог-коллектора, установленного на узле;
  - **Имя узла** – наименование узла, на котором установлен агент сбора лог-коллектора;
  - **IP узла** – IP-адрес узла, на котором установлен лог-коллектор.
- Блок **Профили сбора** – содержит информация о профилях сбора, настроенных для данного агента сбора:

- **Название** – наименование профиля сбора;
- **Тип модуля** – тип модуля сбора, по которому работает профиль сбора;
- **Источник** – наименование источника, для которого настроен профиль сбора;
- **Агент сбора** – наименование агента сбора, на котором установлен профиль сбора;
- **Активен** – состояние профиля сбора;
- **Дата публикации** – дата и время публикации информации о профиле сбора в платформе;
- **Дата создания** – дата и время создания профиля сбора;
- **Дата обновления** – дата и время изменения информации о профиле сбора.

- Блок **Статистика полученных событий** – содержит графическое представление количества полученных событий от источников за период времени по каждому профилю сбора;
- Блок **Статистика отправленных событий** – содержит графическое представление количества отправленных событий в сервис **Log-proxy** за период времени по каждому профилю сбора.

3.3.2.2 Настройка агента сбора

Для настройки агента сбора необходимо открыть его на редактирование, внести необходимые изменения и нажать кнопку **Сохранить**.

Открыть агент сбора на редактирование можно следующими способами:

- Перейдите в раздел **Источники → Агенты сбора** и нажмите кнопку  в строке нужного агента сбора.
- Перейдите на форму просмотра агента сбора (см. «Рис. 86»). и нажмите кнопку **Редактировать**.

Настройка агента сбора выполняется в следующих блоках:

- **Настройки контроллера** – управление общими параметрами и настройка поведения лог коллектора при достижении предела занятого места на диске;
- **Настройки api_server** – настройка удаленного управления лог-коллектором;
- **Настройки metric_server** – настройка параметров сбора статистики по работе лог-коллектора;
- **Настройки журнала** – настройка журналирования работы лог-коллектора.

3.3.2.2.1 Настройки контроллера

Контроллер отвечает за управление секретами лог-коллектора и отслеживает потребляемую нагрузку на систему.

Пример блока **Настройки контроллера** приведен на «Рис. 87».

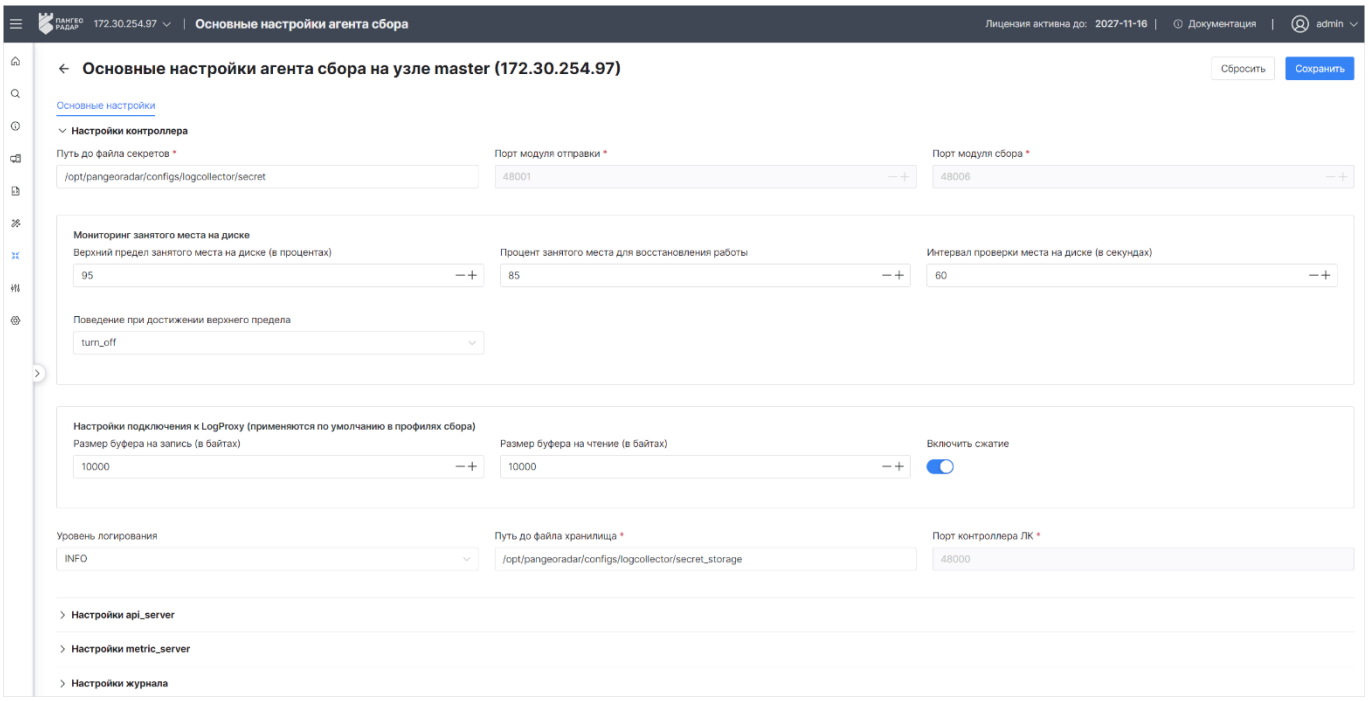


Рис. 87 – Настройка агента сбора. Блок "Настройки контроллера"

Укажите в блоке информацию о контроллере:

- **Порт контроллера ЛК** – порт контроллера лог-коллектора. Параметр нельзя изменить;
- **Порт модуля приемки** – порт модуля, на который приходят события от источника. Параметр нельзя изменить;
- **Порт модуля отправки** – порт модуля, с которого выполняется отправка событий в платформу. Параметр нельзя изменить;
- **Путь до файла секретов** – укажите путь до файла с секретами. Подробнее о секретах см. раздел «Секреты»;
- **Путь до файла хранилища** – укажите путь до хранилища секретов;
- **Верхний предел занятого места на диске (в процентах)** – укажите значение занятого диска в "%", при достижении которого будет выполнена команда, указанная в поле **Поведение при достижении верхнего предела**. Значение по умолчанию: "95";
- **Процент занятого места для восстановления работы** – укажите значение занятого диска в "%", при достижении которого будет восстановлена работа агента сбора. Значение по умолчанию: "80";
- **Интервал проверки места на диске (в секундах)** – укажите интервал проверки места на диске (в секундах). Значение по умолчанию: "60";
- **Поведение при достижении верхнего предела** – из выпадающего списка выберите действие, которое необходимо выполнить при достижении предела занятого места на диске. Возможные действия:
  - `turn_off` – выключить агент сбора;
  - `skip` – включить пропуск событий, при котором агент сбора будет читать события, но не будет пересылать в платформу.

Особенности работы лог-коллектора при достижении предела места на диске:

- активный сбор – когда место заканчивается, лог-коллектор перестает собирать события, но продолжает их отправку в сервис **Log-proxy**, чтобы освободить место;
- пассивный сбор – если источник может продолжать работать в штатном режиме, а лог-коллектор не доступен, то рекомендуется остановить прием событий (`turn_off`), при этом лог-коллектор продолжит их отправку в сервис **Log-proxy**, чтобы освободить место;
- пассивный сбор – если источник не может нормально продолжать работать и лог-коллектор не доступен. В этом случае лог-коллектор будет пропускать события (`skip`), но продолжит их отправку в сервис **Log-proxy**, чтобы освободить место.

Также подобная логика будет работать и в следующих случаях:

- когда есть проблемы с сетью и лог-коллектор не доступен;
- когда применяются новые параметры конфигурации лог-коллектора, возможна ситуация, что профили сбора есть, а с агентом сбора еще нет соединения;
- восстановление связи с источником, когда на стороне источника большая очередь и она массово разгружается без ограничителей.

В блоке **Настройки подключения к LogProxy** при необходимости выполните тонкую настройку подключения к сервису **Log-proxy**:

- **Размер буфера на запись** – укажите размер буфера, который используется при записи событий;
- **Размер буфера на чтение** – укажите размер буфера, который используется при чтении событий;
- **Включить сжатие** – при необходимости включите компрессию событий.

Настройки будут применены для всех профилей сбора, установленных на агенте. При необходимости в настройках профиля сбора их можно переопределить для конкретного модуля сбора (см. раздел «Настройка подключения к сервису Log-proxy»).

В поле **Уровень логирования** настройте параметры журналирования работы контроллера:

- ERROR – записывать сообщения об ошибках;
- WARN – записывать предупреждающие сообщения, которые указывают на потенциальные проблемы или ситуации, которые могут привести к ошибкам в будущем;
- INFO – записывать информационные сообщения, которые сообщают о нормальном функционировании приложения;
- DEBUG – записывать отладочную информацию.

3.3.2.2.2 Настройки api_server

API Server отвечает за возможность удаленного управления агентом сбора.

Пример блока **Настройки api_server** приведены на «Рис. 88».

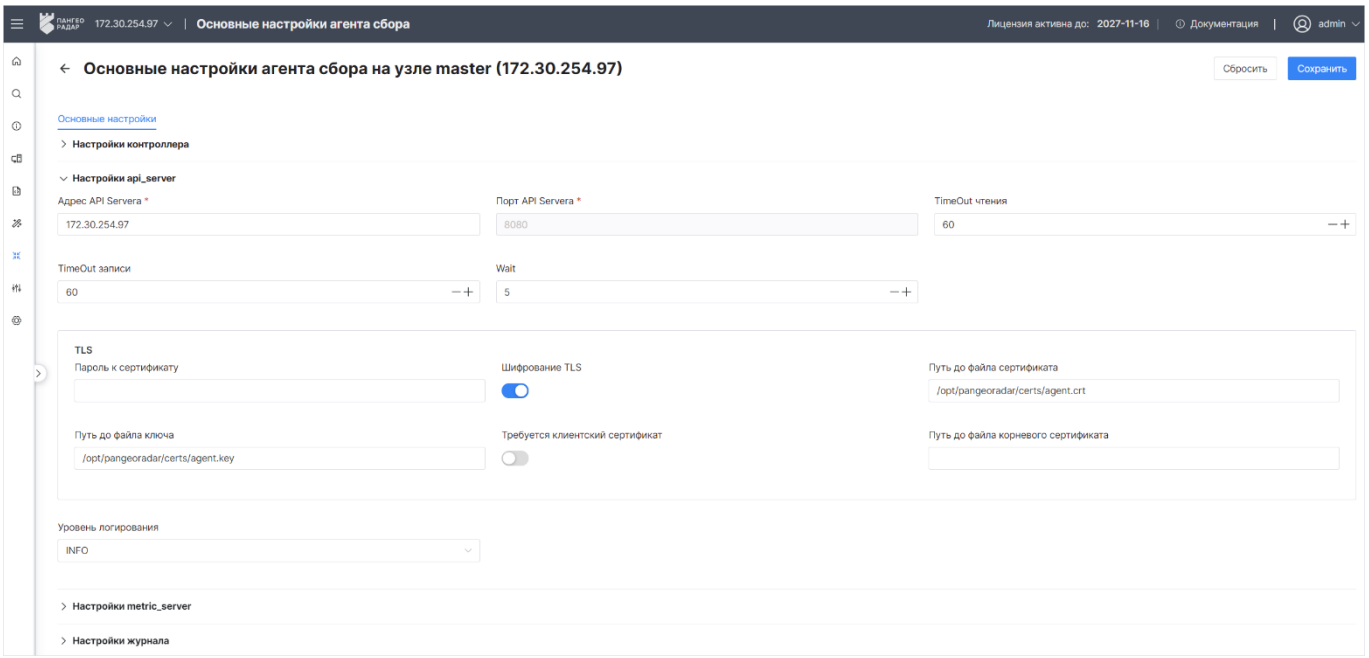


Рис. 88 – Настройка агента сбора. Блок "Настройки api_server"

Укажите в блоке информацию об API сервере:

- **Адрес API сервера** – укажите адрес сетевого интерфейса, используемого агентом сбора;
- **Порт API сервера** – порт, по которому выполняется API-взаимодействие. Параметр нельзя изменить;
- **TimeOut чтения** – укажите максимальное время ожидания получения запроса в секундах;
- **TimeOut записи** – укажите максимальное время ожидания отправки запроса в секундах;
- **Ожидание (Wait)** – укажите время ожидания окончания обработки запроса при получении сигнала на остановку приложения в секундах;
- **Шифрование TLS** – при необходимости включите опцию, которая позволяет включить использование протокола Transport Layer Security (TLS) для обеспечения безопасной передачи данных;
- **Путь до файла сертификата** – укажите путь до файла сертификата, используемого при TLS шифровании;
- **Путь до файла ключа** – укажите путь до файла ключей, используемых при TLS шифровании;
- **Пароль к сертификату** – пароль для расшифровки файла ключей. Если поле не задано, считается, что файл не зашифрован;
- **Требуется клиентский сертификат** – при необходимости включите проверку клиентского сертификата;
- **Путь до файла корневого сертификата** – путь до корневого сертификата. Поле заполняется при включенной проверке клиентского сертификата;
- **Уровень логирования** – из выпадающего списка выберите уровень журналирования работы API сервера. Возможные значения:
    - ERROR – записывать сообщения об ошибках;

- WARN – записывать предупреждающие сообщения, которые указывают на потенциальные проблемы или ситуации, которые могут привести к ошибкам в будущем;
- INFO – записывать информационные сообщения, которые сообщают о нормальном функционировании приложения;
- DEBUG – записывать отладочную информацию;
- TRACE – записывает всю информацию о работе сервиса;
- ALL – записывать все сообщения.

3.3.2.2.3 Настройки metric_server

Metric_server осуществляет сбор статистики работы агентов сбора лог-коллектора.

Пример блока **Настройки metric_server** приведены на «Рис. 89».

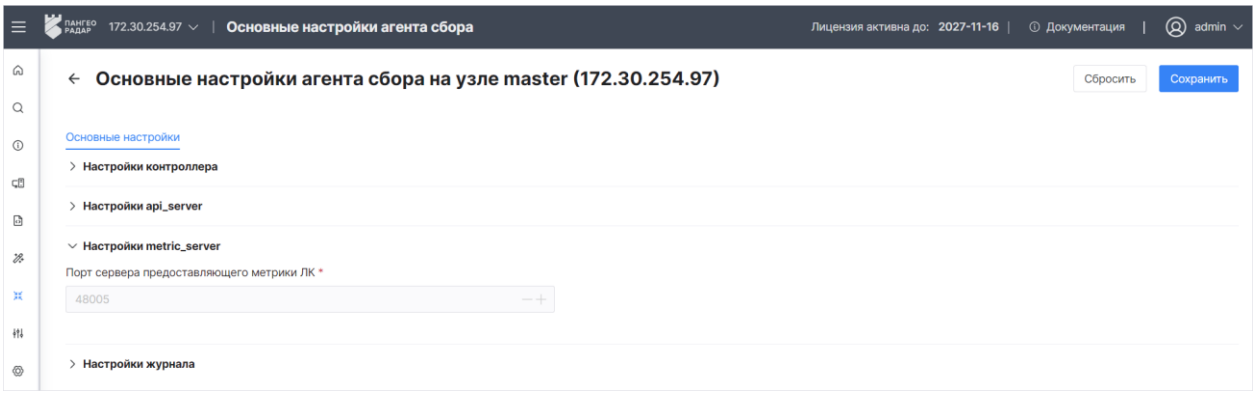


Рис. 89 – Настройка агента сбора. Блок "Настройки metric_server"

В блоке отображается информация об используемом порте сервера, предоставляющим метрики лог-коллектора.

Просмотр метрик:

1. Перейдите в веб-интерфейс платформы через который может выполняться централизованное управление лог-коллектором.
2. Перейдите в раздел **Администрирование** → **Мониторинг** и из выпадающего списка выберите рабочий стол **Лог коллектор**.

   Перечень виджетов рабочего стола **Лог коллектор** приведен в документе «Перечень метрик мониторинга».

3.3.2.2.4 Настройки журнала

Компонент отвечает за ведение журналов работы агента сбора. Поддерживаются следующие уровни журналирования:

- **ERROR** – записывать сообщения об ошибках;
- **WARN** – записывать предупреждающие сообщения, которые указывают на потенциальные проблемы или ситуации, которые могут привести к ошибкам в будущем;
- **INFO** – записывать информационные сообщения, которые сообщают о нормальном функционировании приложения;

- **DEBUG** – записывать отладочную информацию;
- **TRACE** – записывает всю информацию о работе сервиса;
- **ALL** – записывать все сообщения.

Пример блока **Настройки журнала** приведены на «Рис. 90».

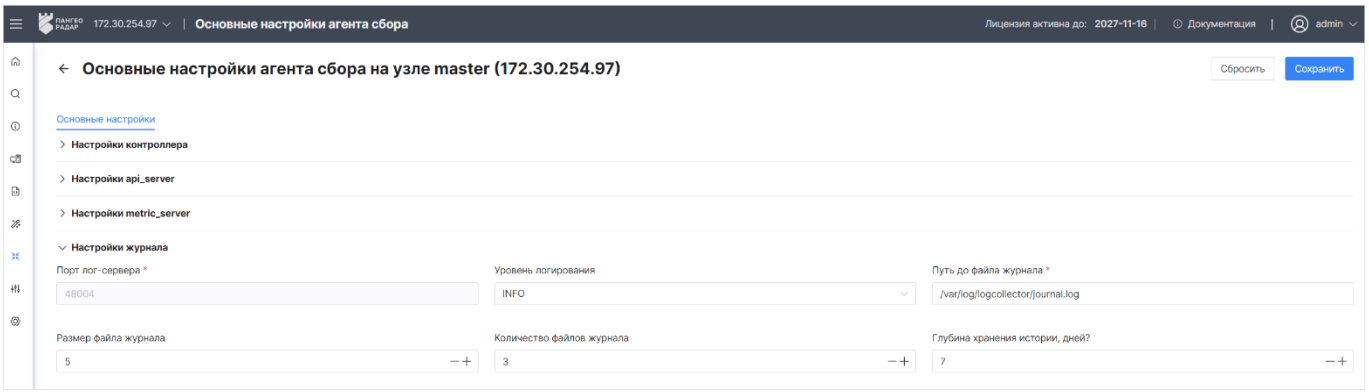


Рис. 90 – Настройка агента сбора. Блок "Настройки журнала"

Укажите в блоке следующую информацию:

- **Порт log_server** – порт сервера журналирования. Параметр нельзя изменить;
- **Уровень логирования** – общий уровень журналирования для всех компонентов агента сбора;
- **Путь до файла журнала** – путь до файла журнала;
- **Размер файла журнала** – параметр, который определяет максимальный размер файла журнала в мегабайтах, при достижении которого будет выполнена ротация журналов;
- **Количество файлов журнала** – порог количества файлов журнала, при достижении которого будут удалены устаревшие файлы журнала. Если параметр не указан, то файлы удаляться не будут;
- **Глубина хранения истории, дней** – укажите максимальное количество дней для хранения старых файлов журнала. Отсчет ведется по метке времени создания файла журнала. Если параметр не указан файлы удаляться не будут.

3.3.2.3 Публикация изменений

Чтобы настройки агента сбора вступили в силу, их необходимо **опубликовать** в платформе.

Публикацию изменений можно выполнить следующими способами:

Способ 1:

1. Выберите агенты сбора, в которые были внесены изменения. Для этого установите соответствующие флаги.
2. Нажмите кнопку **Опубликовать**.

Способ 2:

1. Перейдите на форму просмотра агента сбора.
2. Нажмите кнопку **Опубликовать**.

3.3.2.4 Изменение состояния профиля сбора

Профиль сбора на выбранном агенте может находиться в следующих состояниях:

- **Включен** – по профилю сбора выполняется сбор событий от источника;
- **Выключен** – профиль сбор добавлен в платформу, но по нему не выполняется сбор событий.

Изменить состояние профиля сбора на агенте можно следующими способами:

Способ 1:

1. Откройте агент сбора на просмотр.
2. Перейдите к блоку **Профили сбора**.
3. В графе **Активен** измените состояние нужного профиля сбора, установив переключатель в соответствующее положение.

Способ 2:

1. Откройте агент сбора на просмотр.
2. Перейдите к блоку **Профили сбора** и выберите профили сбора, установив соответствующие флаги.
3. Используйте кнопку **Включить**/**Выключить** для изменения состояния выбранных профилей сбора

Способ 3:

1. Откройте агент сбора на просмотр и перейдите к блоку **Профили сбора**.
2. Откройте профиль сбора на просмотр, нажав по ссылке в графе **Название** или по кнопке  в нужной строке.
3. На форме просмотра профиля сбора нажмите кнопку **Редактировать**.
4. В поле **Активен** установите переключатель в соответствующее положение.
5. Нажмите кнопку **Сохранить**.

Подробнее о работе с профилями сбора см. раздел «Профили сбора».

3.3.3 Профили сбора

Работа с профилями сбора включает в себя следующие процессы:

1. «Настройка профиля сбора».
2. «Просмотр профиля сбора».
3. «Редактирование профиля сбора».
4. «Экспорт профилей сбора».
5. «Импорт профилей сбора».
6. «Удаление профилей сбора».

Для работы с профилями сбора перейдите в раздел **Источники → Профили сбора** (см. «Рис. 91»).

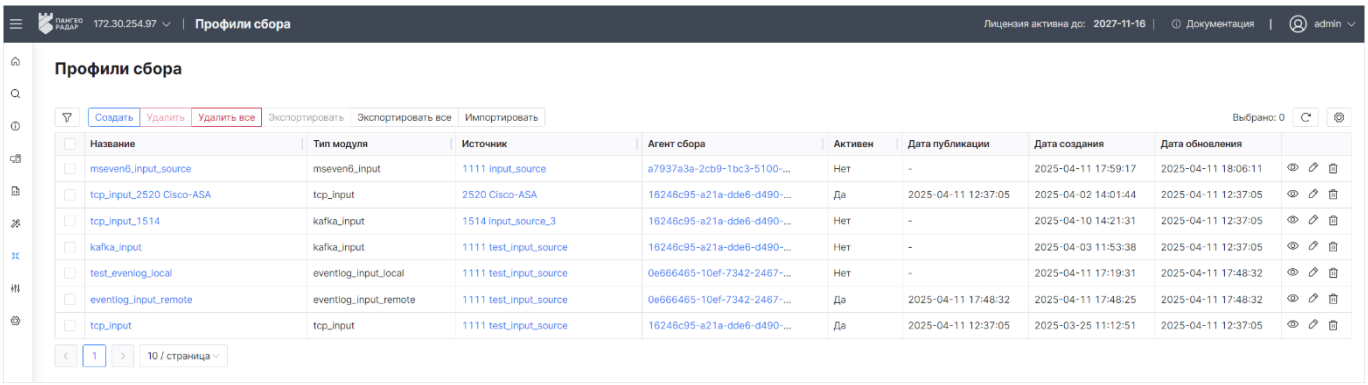


Рис. 91 – Раздел "Профили сбора"

В разделе отображается следующая информация:

- **Название** – наименование профиля сбора;
- **Тип модуля** – тип модуля сбора, по которому работает профиль сбора;
- **Источник** – наименование источника, для которого настроен профиль сбора;
- **Агент сбора** – наименование агента сбора, на котором установлен профиль сбора;
- **Активен** – состояние профиля сбора;
- **Дата публикации** – дата и время публикации информации о профиле сбора в платформе;
- **Дата создания** – дата и время создания профиля сбора;
- **Дата обновления** – дата и время изменения информации о профиле сбора.

3.3.3.1 Настройка профиля сбора

Настройка профиля сбора заключается в конфигурировании модуля сбора, по которому будет работать профиль.

Внимание! *Модуль сбора должен поддерживать ОС, на которой работает агент сбора, иначе профиль сбора работать не будет. Соответствие модулей сбора и ОС приведено в разделе «Описание».*

Порядок действий для настройки профиля сбора в общем случае выглядит следующим образом:

1. Нажмите кнопку **Создать**. Откроется форма "Создание профиля сбора" (см. «Рис. 92»).

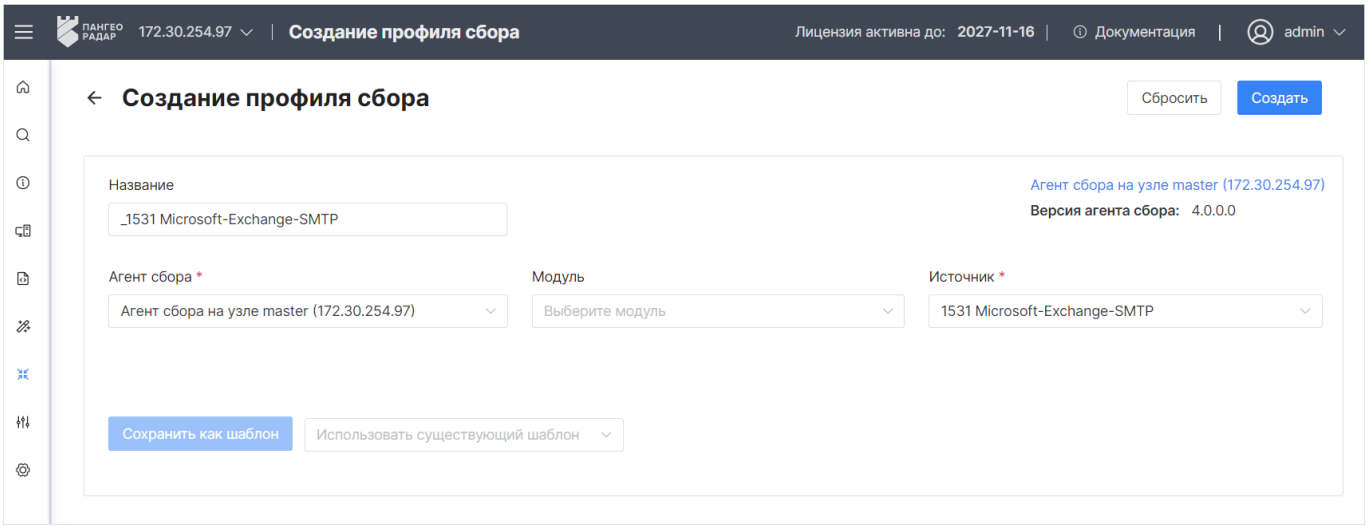


Рис. 92 – Форма "Создание профиля сбора"

2. С платформой поставляется набор заранее подготовленных шаблонов профилей сбора. Шаблон выбирается в поле **Использовать существующий шаблон**. При необходимости вы можете настроить профиль сбора вручную. Для этого укажите на форме следующую информацию:

   - **Название** – наименование профиля сбора формируется автоматически из двух частей: <Наименование модуля>_<Наименование источника>. При необходимости вы можете указать название самостоятельно;
   - **Агент сбора** – из выпадающего списка выберите агент сбора, на котором будет функционировать профиль;
   - **Источник** – из выпадающего списка выберите источник, с которого будут собираться события профилем сбора;
   - **Модуль сбора** –из выпадающего списка выберите модуль сбора, по которому будет работать профиль сбора. Поля формы будут автоматически сформированы для настройки выбранного модуля (см. «Рис. 93»).

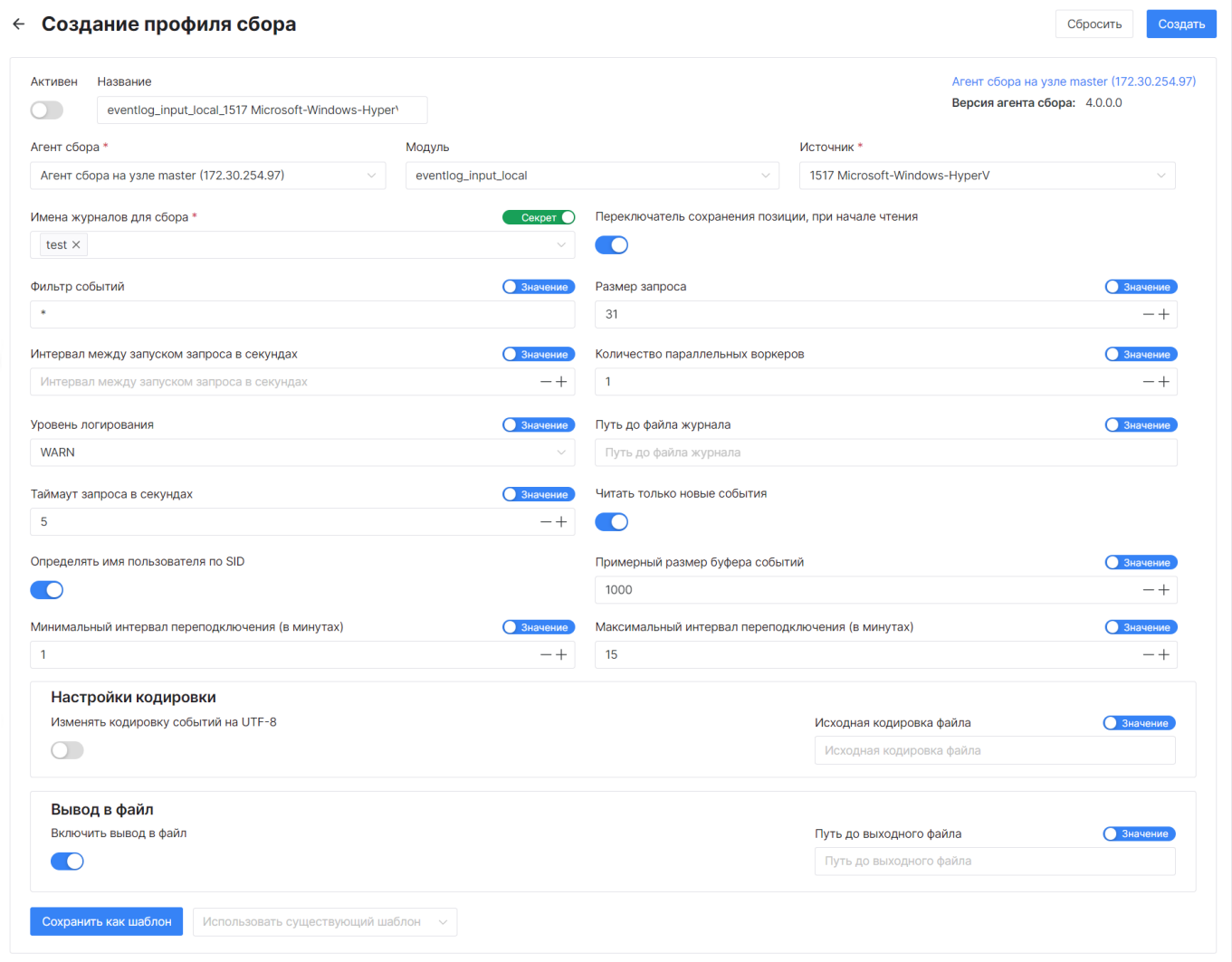


Рис. 93 – Форма "Создание профиля сбора". Пример настроек модуля

3. Настройте выбранный модуль сбора. Настройку модуля можно условно поделить на следующие действия:
    - Настройка основных параметров модуля (подробно описаны в соответствующих разделах ниже). При необходимости для части настроек вы можете использовать секреты (подробнее см. раздел «Секреты»):
    - Настройка журналирования.
    - Настройка кодировки.
    - Настройка вывода в файл.
4. После выбора и настройки модуля сбора, станет доступна возможность активировать профиль сбора на выбранном агенте. Для этого в поле **Активен** установите переключатель в положение "Включен".
5. Для сохранения изменений нажмите кнопку **Сохранить**.
6. **Опубликуйте** изменения на выбранном агенте сбора, чтобы изменения вступили в силу (см. раздел «Публикация изменений»).

3.3.3.1.1 Секреты

Секреты лог-коллектора – это необходимые для работы/настройки значения, которые будут зашифрованы и вставлены в нужные места в профиле сбора для сокрытия информации.

Секреты бывают двух видов:

- **Глобальные** – по умолчанию применяются ко всем коллекторам для удобства работы с ними;
- **Локальные** – переопределяют параметры глобальных секретов для конкретного экземпляра лог-коллектора.

Локальные секреты всегда имеют приоритет выше глобальных.

Создание секретов должно выполняться через веб-интерфейс платформы:

1. Перейдите в раздел **Администрирование** → **Кластер** → вкладка **Узлы**.
2. Откройте форму просмотра узла с ролью **agent** или **agent win**.
3. В блоке секреты агента нажмите кнопку **Создать секрет** (см. «Рис. 94»).

Рис. 94 – Форма просмотра узла. Блок "Секреты агента"

4. Откроется окно "Создать секрет" (см. «Рис. 95»).

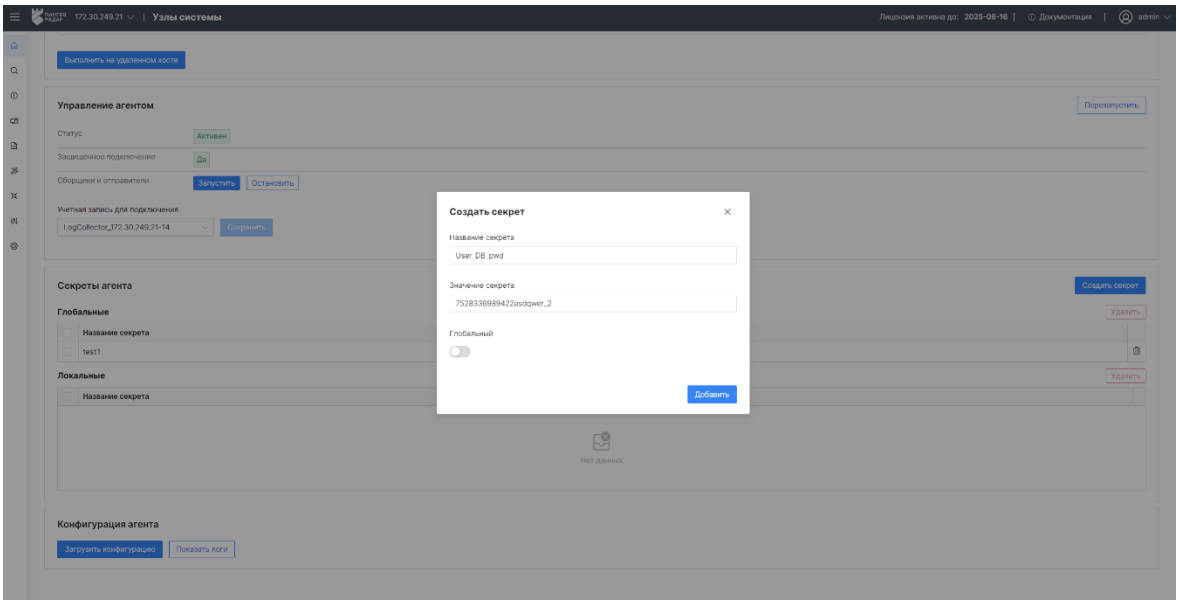


Рис. 95 – Окно "Создать секрет"

5. Укажите в окне следующую информацию:
    - в поле **Название секрета** укажите наименование секрета;
    - в поле **Значение секрета** укажите данные, которые необходимо зашифровать;
    - если необходимо применить секрет ко всем лог-коллекторам, то включите параметр **Глобальный**.

Использование секретов в профиле сбора: При настройке модуля профиля сбора, можно в качестве значения параметра указать конкретное значение или секрет. Для переключения между режимами ввода информации используйте соответствующий переключатель (см. «Рис. 96»).

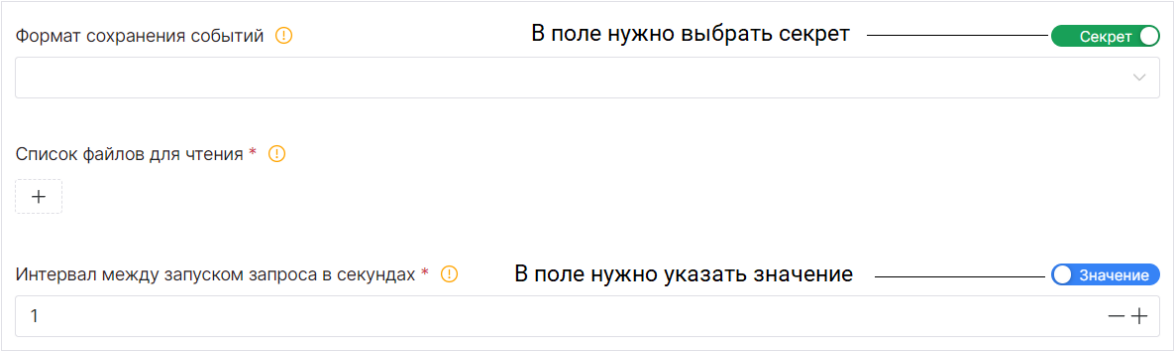


Рис. 96 – Способы указания параметров модуля сбора

3.3.3.1.2 Журналирование

Для большинства модулей сбора можно настроить уровень журналирования работы модуля. Поддерживаются следующие уровни журналирования:

- **ERROR** – записывать сообщения об ошибках;
- **WARN** – записывать предупреждающие сообщения, которые указывают на потенциальные проблемы или ситуации, которые могут привести к ошибкам в будущем;
- **INFO** – записывать информационные сообщения, которые сообщают о нормальном функционировании приложения;
- **DEBUG** – записывать отладочную информацию;
- **TRACE** – записывает всю информацию о работе сервиса;
- **ALL** – записывать все сообщения.

Настройка выполняется в поле **Уровень логирования**.

3.3.3.1.3 Фильтрация

Фильтры применяются к собранным событиям от источников перед формированием очереди на отправку. Фильтр представляет из себя массив регулярных выражений, которые реализуют механизм черных и белых списков:

- Белый список – события, которые соответствуют регулярному выражению, попадают в очередь на отправку.
- Черный список – события, которые соответствуют регулярному выражению, блокируются и не попадают в очередь на отправку.

Сначала проверяется белый список, а затем черный.

Фильтры задаются в блоке **Настройки фильтрации** (см. «Рис. 97»).

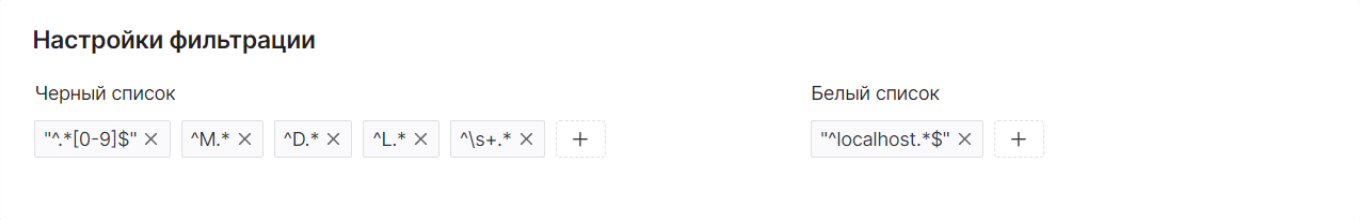


Рис. 97 – Форма "Создание профиля сбора". Блок настройки фильтрации

В блоке доступны следующие настройки:

- Белый список – укажите массив регулярных выражений, формирующий белый список;
- Черный список – укажите массив регулярных выражений, формирующий черный список.

Возможность применения фильтра к компоненту сбора обуславливается типом собираемых данных: структурированные или неструктурированные. Например, данные, собираемые от источников **wmi**, **eventlog**, **odbc**, **etw** являются структурированными, а от остальных источников – неструктурированные.

3.3.3.1.4 Кодировка собираемых данных

Профиль сбора позволяет настроить кодировку данных, собираемых от источников. Для этого в параметрах выбранного модуля сбора используется блок **Настройки кодировки** (см. «Рис. 98»).

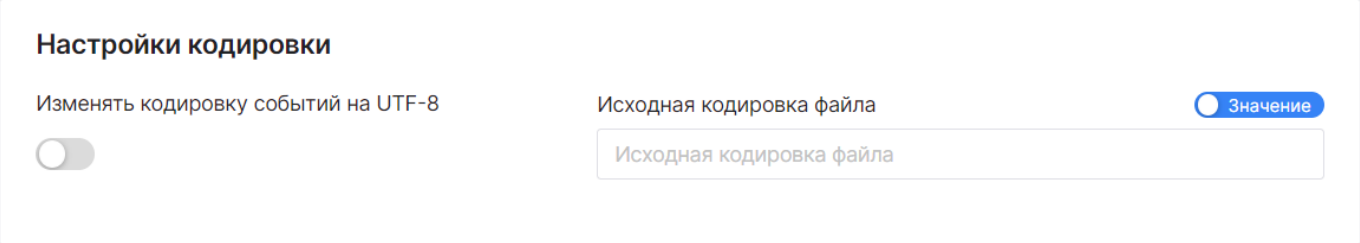


Рис. 98 – Форма "Создание профиля сбора". Блок "Настройки кодировки"

В блоке доступны следующие настройки:

- **Исходная кодировка** – укажите кодировку событий источника. Если значение не указано, то профиль сбора попытается определить кодировку самостоятельно;
- **Изменить кодировку событий на UTF-8** – опция, позволяющая изменить кодировку исходника в `utf8`.

3.3.3.1.5 Запись потока событий в файл

Для профиля сбора можно настроить отправку получаемого потока событий в локальный файл. Для этого в параметрах выбранного модуля сбора используется блок Вывод в файл (см. «Рис. 99»).

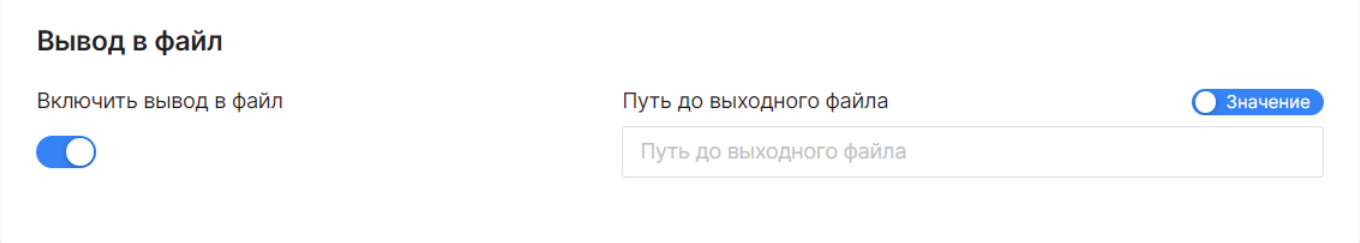


Рис. 99 – Форма "Создание профиля сбора". Блок "Вывод в файл"

В блоке доступны следующие настройки:

- **Путь до файла** – укажите путь до локального файла, в который будут выводиться события;
- **Включить вывод в файл** – опция, позволяющая включить вывод потока событий в файл.

3.3.3.1.6 Формат сохранения событий

Лог-коллектор позволяет настроить для компонентов сбора формат сохранения событий. Для этого в параметрах компонентов сбора используется поле **Формат сохранения событий**, которое может иметь следующие значения:

- **raw** – данные сохраняются в том виде, в котором пришли;
- **json** – пришедшие данные обогащаются дополнительной технической информацией и упаковываются в пакет json.

Данная настройка применима только к неструктурированным данным (кроме **eventlog_input**, **wmi_input**, **odbc_input**, **etw_input**).

3.3.3.1.7 Параметры чтения многострочных событий

В модули сбора **file_input**, **sftp_input**, **smb_input**, **ftp_input** добавлены параметры чтения из событий следующих форматов: RAW, JSON, XML (по умолчанию RAW). Параметр настраивается в поле **Формат событий в файлах**.

При этом для этих модулей можно настроить параметры чтения многострочных событий:

- **Разделитель событий в файле для многострочных событий**. В поле указывается символ для разделения событий. Поддерживаются любые строки (один и несколько символов), также поддерживаются файлы в не utf-8 кодировке. Если поле не указано, то файлы будут читаться построчно.
- **Удалять разделитель событий**. В поле включается опция, удаляющая разделитель. При включенной опции строка разделителя удаляется из прочитанных событий.
- **Отсутствие разделителя событий в файле, используется для чтения событий в форматах JSON и XML без явного разделителя**. Если указан разделитель, конец файла не считается концом события. Т.е. Если указан ';' прочитаны будут все события до последнего ';'. Остаток файла после него читаться не будет, т.к. событие получается неполное. Для того, чтобы этого избежать, в данном поле можно включить отсутствие разделителя. Опция применима только для чтения событий в форматах JSON и XML без явного разделителя. При всех других сочетаниях параметров файлы будут читаться как RAW построчно или с указанным разделителем.

При использовании разделителя автоматическое определение кодировки может срабатывать неправильно и разделение событий по разделителю не будет работать. Поэтому для файлов в кодировке отличной от utf-8 не рекомендуется изменять кодировку событий (см. «Кодировка собираемых данных»).

3.3.3.1.8 Настройка подключения к сервису Log-proxy

Для профиля сбора можно выполнить тонкую настройку **подключения к сервису Log-proxy**. Для этого в параметрах выбранного модуля сбора используется блок **Настройки подключения к LogProxy** (см. «Рис. 100»).

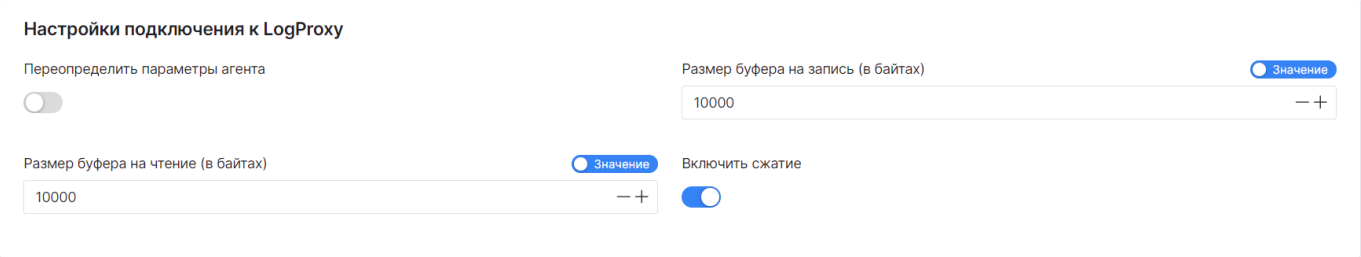


Рис. 100 – Форма "Создание профиля сбора". Блок "Настройки подключения к LogProxy"

В блоке доступны следующие настройки:

- **Переопределить параметры агента** – при необходимости включите для выбранного модуля сбора переопределение параметров, выставленных для агента сбора (см. раздел «Настройки контроллера»);
- **Размер буфера на запись** – укажите размер буфера, который используется при записи событий;
- **Размер буфера на чтение** – укажите размер буфера, который используется при чтении событий;
- **Включить сжатие** – при необходимости включите компрессию событий.

Настройки будут применены для всех профилей сбора, установленных на агенте. При необходимости в настройках профиля сбора их можно переопределить для конкретного модуля сбора.

3.3.3.1.9 Настройки фильтрации (исключения) событий

Для модулей `eventlog_input_local`, `eventlog_input_remote`, `mseven6_input`, `wmi_input` можно задать фильтры по полям событий с помощью регулярных выражений. Для этого в параметрах выбранного модуля сбора используется блок **Настройки фильтрации (исключения) событий** (см. «Рис. 101»).

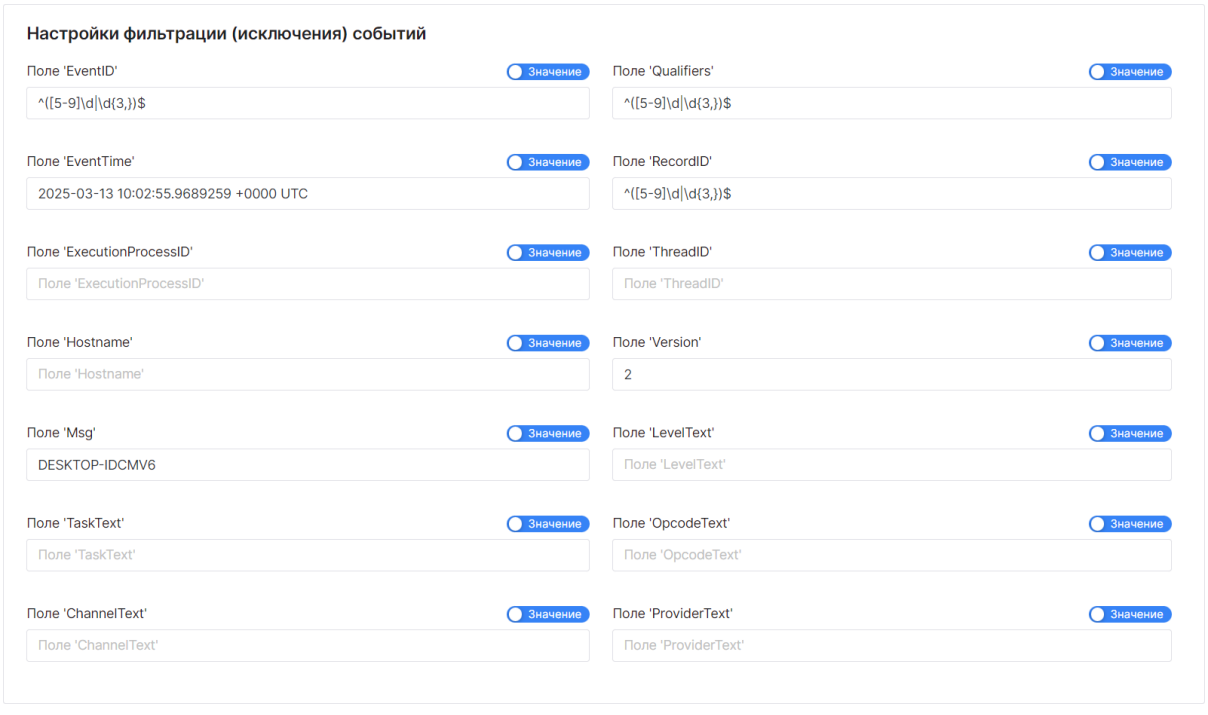


Рис. 101 – Форма "Создание профиля сбора". Блок "Настройки фильтрации (исключения) событий"

В данном блоке можно указать для полей следующие типы фильтров:

- Фильтры по времени, пример: `2025-03-13 10:02:55.9689259 +0000 UTC`. Используется для следующих полей:
    - Created;
    - EventTime.
- Числовые фильтры, пример: `^([5-9]\d|\d{3,})$`. Используется для следующих полей:
    - EventID;
    - Qualifiers;
    - RecordID;
    - ExecutionProcessID;
    - ThreadID;
    - Version.
- Строковые фильтры, пример: `DESKTOP-IDCMV6G`. Используется для следующих полей:
    - Hostname;
    - Msg.
- Возможные значения:
    - Пример для поля LevelText: `Information, Warning, Error`;
    - Пример для поля TaskText: `Service, State, Event`;
    - Пример для поля OpcodeText: `ServiceShutdown`;
    - Пример для поля ChannelText: `System`;
    - Пример для поля ProviderTex: `System`.

3.3.3.1.10 Модуль etw_input

Описание: Локальный сбор событий через технологию Event Tracing for Windows (ETW).

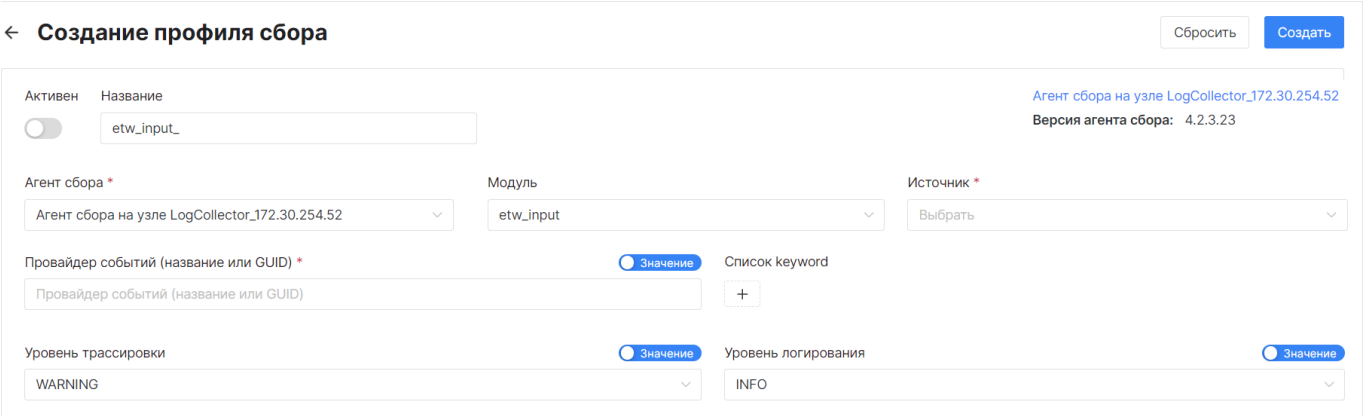
Поддержка ОС: Только Windows.

Поддержка фильтрации: нет.

Поддержка настройки кодировки: нет.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:



Параметры модуля:

- **Провайдер событий (название или GUID)** – укажите наименование элемента системы, который генерирует события и отправляет их коннектору ETW. Например Microsoft-Windows-Networking-Correlation;
- **Список keyword** – укажите ключевые слова для фильтрации событий. Например, 0xFFFFFFFFFFFFFFFF.Подробнее о ключевых словах см. на сайте;
- **Уровень трассировки** – из выпадающего списка выберите уровень важности для фильтрации событий. Доступны следующие значения:
  - VERBOSE – передавать подробные сообщения, которые предоставляет более подробную информацию, чем уровень **information**;
  - INFORMATION – передавать информационные сообщения, которые сообщают о нормальном функционировании приложения;
  - WARNING – передавать предупреждающие сообщения, которые указывают на потенциальные проблемы или ситуации, которые могут привести к ошибкам в будущем;
  - ERROR – передавать сообщения об ошибках;
  - CRITICAL – передавать сообщения об ошибках, которые указывает на серьёзную проблему, способную повлиять на стабильность или производительность.
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.11 Модуль eventlog_input_local

Описание: Локальный сбор событий через Windows EventLog по механизму RPC.

Поддержка ОС: Только Windows.

Поддержка фильтрации: нет.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Настройки фильтрации (исключения) событий: есть.

Пример формы настройки модуля:

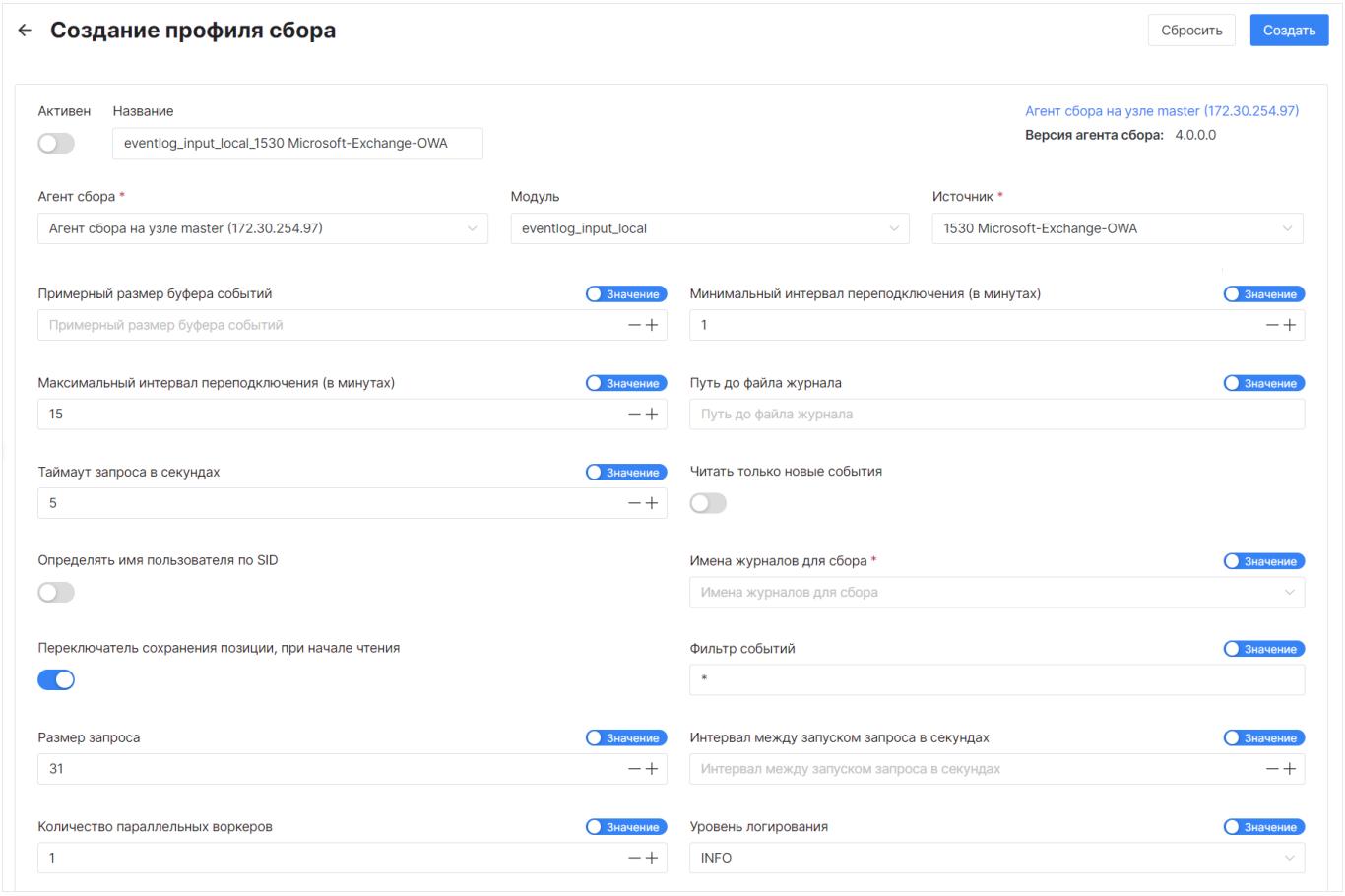


Рис. 102 – Пример формы для модуля eventlog_input_local

Параметры модуля:

- **Примерный размер буфера событий** – укажите размер буфера, который используется при получении событий. Значение по умолчанию: **1000**. Для определения оптимального размера буфера используется следующая формула*: Размер запроса * Количество параллельных воркеров*, где результат корректируется до ближайшего значения, кратного результатам умножения;
- **Минимальный интервал переподключения (в минутах)** – укажите минимальное время ожидания переподключения к источнику в минутах (при недоступности источника). Значение по умолчанию: **1**;
- **Максимальный интервал переподключения (в минутах)** – укажите максимальное время ожидания переподключения к источнику в минутах (при недоступности источника). Значение по умолчанию **15**. Максимальное значение: **30**;
- **Путь до файла журнала** – укажите путь к файлу журнала для сбора событий от источника. Поддерживаемые форматы .evt, .evtx, .etl;
- **Таймаут запроса в секундах** – укажите таймаут отправки запроса в секундах;
- **Читать только новые события** – при необходимости включите опцию, которая позволяет забирать из журнала только новые события;
- **Определять имя пользователя по SID** – при необходимости включите опцию, которая позволяет конвертировать значения SID в имена пользователей;

- **Имена журналов для сбора** – из выпадающего списка выберите один или несколько каналов, из которых нужно собирать события. Поле указывается в случае, если не указано поле **Путь до файла журнала**. Возможные значения:
    - Application;
    - Microsoft-Windows-PowerShell/Operational;
    - Security;
    - System.
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Фильтр событий** – укажите запрос для фильтрации событий для чтения с помощью выражения XPath. Возможные значения:
    - структурированный XML запрос, например

      `<QueryList><Query><Select Path=\"Security\">*[System[(EventID=42) and (Level=2)]]</Select></Query></QueryList>`;
    - * - все параметры.
- **Размер запроса** – укажите количество событий, загружаемых за один запрос;
- **Интервал между запуском запроса в секундах** – укажите интервал, через который файл (или канал) проверяется на наличие новых записей лога;
- **Количество параллельных воркеров** – укажите количество воркеров, которое будет задействовано для обработки событий;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.12 Модуль eventlog_input_remote

Описание: Удаленный сбор событий через Windows EventLog по механизму RPC.

Поддержка ОС: Только Windows.

Поддержка фильтрации: нет.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Настройки фильтрации (исключения) событий: есть.

Пример формы настройки модуля:

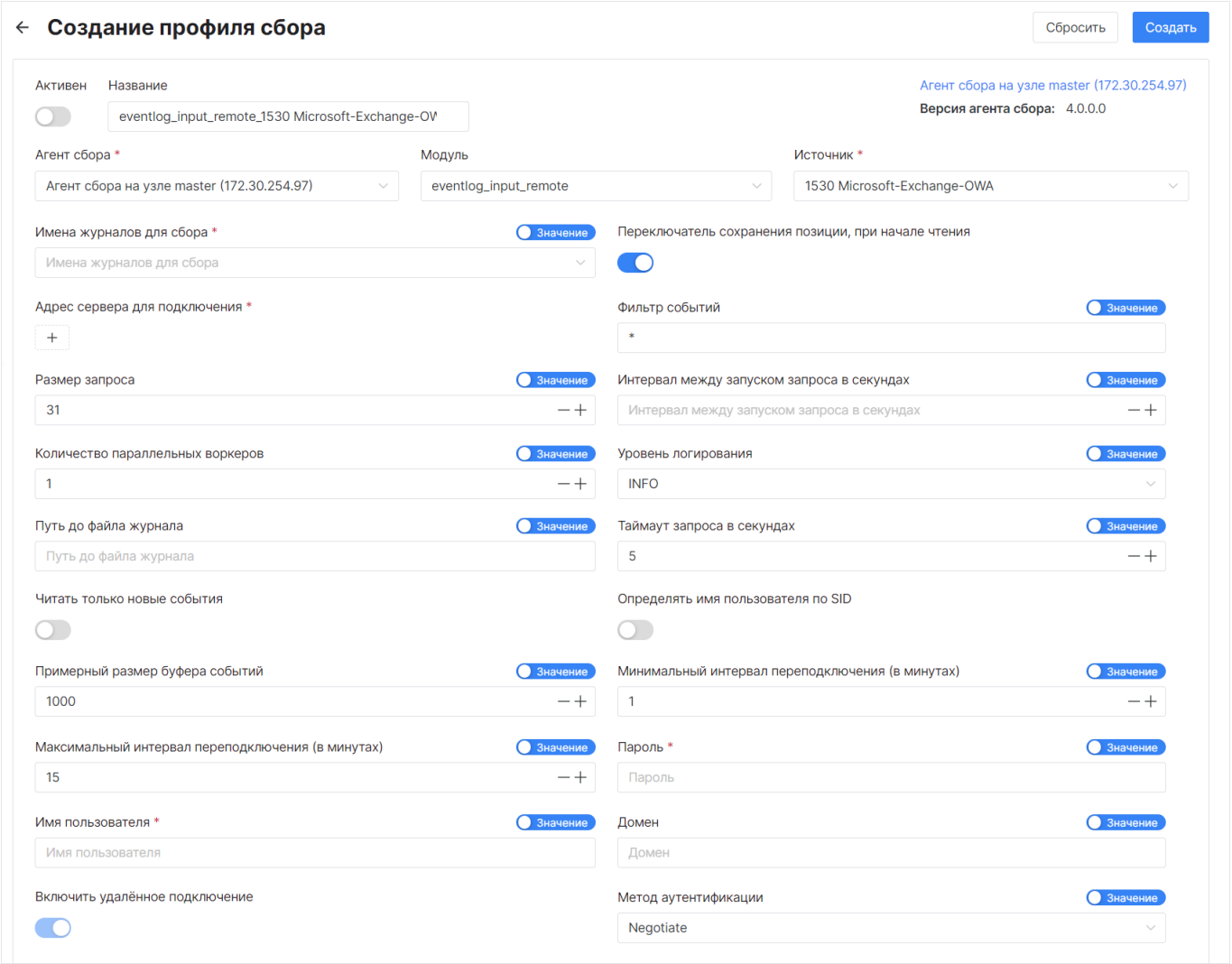


Рис. 103 – Пример формы для модуля eventlog_input_remote

Параметры модуля:

- **Имена журналов для сбора** – из выпадающего списка выберите один или несколько каналов, из которых нужно собирать события. Поле указывается в случае, если не указано поле **Путь до файла журнала**. Возможные значения:
    - Application;
    - Microsoft-Windows-PowerShell/Operational;
    - Security;
    - System.
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Адрес сервера для подключения** – укажите адрес удаленного сервера;
- **Фильтр событий** – укажите запрос для фильтрации событий для чтения с помощью выражения XPath. Возможные значения:
    - структурированный XML запрос, например

```
<QueryList><Query><Select Path=\"Security\">*[System[(EventID=42) and (Level=2)]]</Select></Query></QueryList>
```
;

- * - все параметры.

- **Размер запроса** – укажите количество событий, загружаемых за один запрос;
- **Интервал между запуском запроса в секундах** – укажите интервал, через который файл (или канал) проверяется на наличие новых записей лога;
- **Количество параллельных воркеров** – укажите количество воркеров, которое будет задействовано для обработки событий;
- **Путь до файла журнала** – укажите путь к файлу журнала для сбора событий от источника. Поддерживаемые форматы .evt, .evtx, .etl;
- **Таймаут запроса в секундах** – укажите таймаут отправки запроса в секундах;
- **Читать только новые события** – при необходимости включите опцию, которая позволяет забирать из журнала только новые события;
- **Определять имя пользователя по SID** – при необходимости включите опцию, которая позволяет конвертировать значения SID в имена пользователей;
- **Примерный размер буфера событий** – укажите размер буфера, который используется при получении событий. Значение по умолчанию: **1000**. Для определения оптимального размера буфера используется следующая формула: *Размер запроса * Количество параллельных воркеров*, где результат корректируется до ближайшего значения, кратного результатам умножения;
- **Минимальный интервал переподключения (в минутах)** – укажите минимальное время ожидания переподключения к источнику в минутах (при недоступности источника). Значение по умолчанию: **1**;
- **Максимальный интервал переподключения (в минутах)** – укажите максимальное время ожидания переподключения к источнику в минутах (при недоступности источника). Значение по умолчанию **15**. Максимальное значение: **30**;
- **Уровень логирования** – выберите уровень журналирования модуля;
- **Параметры удаленного подключения** – укажите в следующих полях параметры для удаленного подключения к серверу, указанному в поле **Адрес сервера для подключения**:
    - **Включить удалённое подключение** – для данного модуля удаленное подключение используется по умолчанию. Параметр нельзя изменить;
    - **Имя пользователя** – укажите имя пользователя для удаленного подключения;
    - **Пароль** – укажите пароль пользователя;
    - **Домен** – укажите домен пользователя;
    - **Метод аутентификации** – выберите метод аутентификации. Доступные значения:
        - Negotiate,
        - Kerberos,
        - NTLM.

3.3.3.1.13 Модуль external_command_input

Описание: Выполнение внешней команды в ОС.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

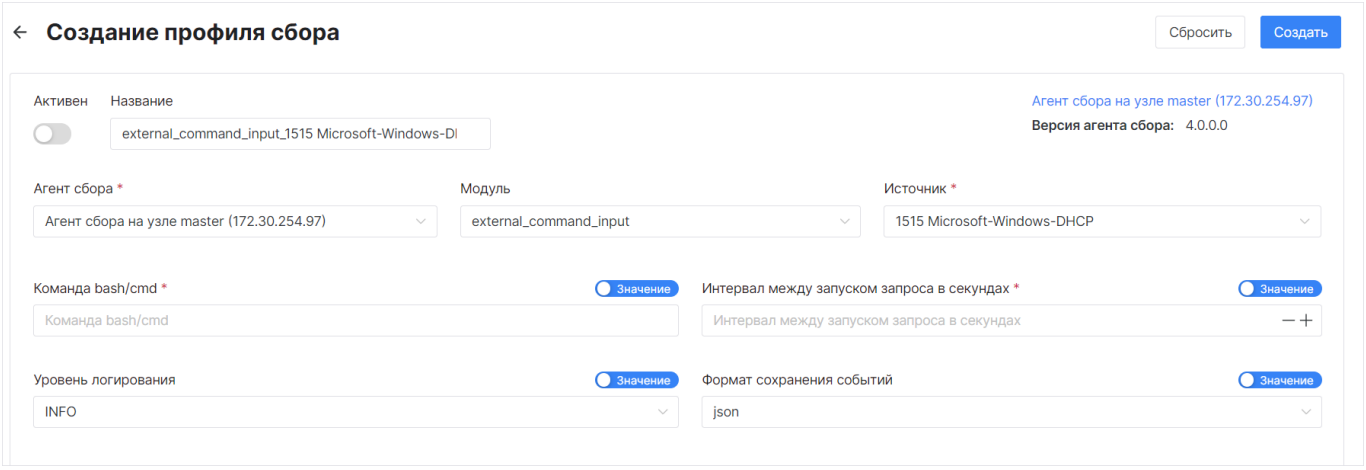


Рис. 104 – Пример формы для модуля external_command_input

Параметры модуля:

- **Команда bash/cmd** – укажите исполняемую команду в формате `bash/cmd` для ОС Linux/Windows соответственно;
- **Интервал между запуском запроса в секундах** – укажите интервал между выполнением команд в секундах;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.14 Модуль file_input

Описание: Сбор событий из локального файла.

Предварительно необходимо создать файл, из которого будет идти чтение, например `/var/log/logcollector/test_logs.txt`.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть. Настройка блока имеет следующие особенности:

- **Исходная кодировка** – укажите кодировку событий источника. Если значение не указано, то профиль сбора попытается определить кодировку самостоятельно;
- **Изменить кодировку событий на UTF-8** – опция, позволяющая изменить кодировку исходника в utf8;

- **Размер буфера для определения исходной кодировки** – укажите размер буфера, который будет использоваться для определения кодировки (в байтах).

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

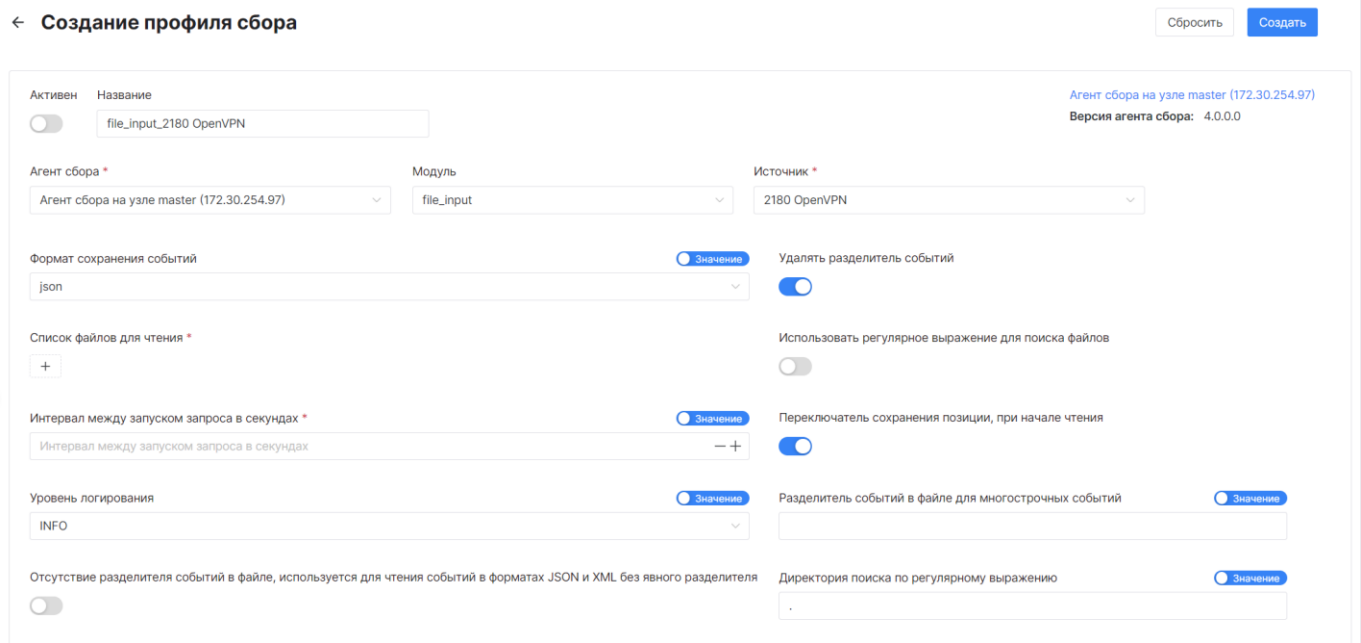


Рис. 105 – Пример формы для модуля file_input

Параметры модуля:

- **Формат сохранения событий** – выберите формат сохранения событий;
- **Удалять разделитель событий** – настройте параметры чтения многострочных событий;
- **Список файлов для чтения** – укажите путь к файлам журналов;
- **Использовать регулярное выражение для поиска файлов** – при необходимости включите опцию, позволяющую использовать **regexp** (регулярные выражения) для поиска файлов журналов;
- **Директория поиска по регулярному выражению** – укажите начальный каталог для поиска файлов;
- **Интервал между запуском запроса в секундах** – укажите интервал между чтением файлов, в секундах;
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Разделитель событий в файле для многострочных событий** – настройте параметры чтения многострочных событий;
- **Отсутствие разделителя событий в файле, используется для чтения событий в форматах JSON и XML без явного разделителя** – настройте параметры чтения многострочных событий;

- **Регулярное выражение для поиска файлов** – укажите регулярное выражение для поиска файлов журнала;
- **Читать только новые события** – при необходимости включите опцию, которая позволяет забирать из журнала только новые события;
- **Отслеживать переименование файлов** – при необходимости включите опцию, которая позволяет использовать мониторинг наименований всех файлов журналов с помощью **file watchers**;
- **Формат событий в файлах** – настройте параметры чтения многострочных событий;
- **Интервал проверки директории на наличие новых файлов (в секундах)** – укажите интервал поиска новых файлов в указанных каталогах. Значение указывается в секундах;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.15 Модуль ftp_input

Описание: Чтение файла, доступного через FTP сервер. Предварительно необходимо создать файл, из которого будет идти чтение.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть. Настройка блока имеет следующие особенности:

- **Исходная кодировка** – укажите кодировку событий источника. Если значение не указано, то профиль сбора попытается определить кодировку самостоятельно;
- **Изменить кодировку событий на UTF-8** – опция, позволяющая изменить кодировку исходника в utf8;
- **Размер буфера для определения исходной кодировки** – укажите размер буфера, который будет использоваться для определения кодировки (в байтах).

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

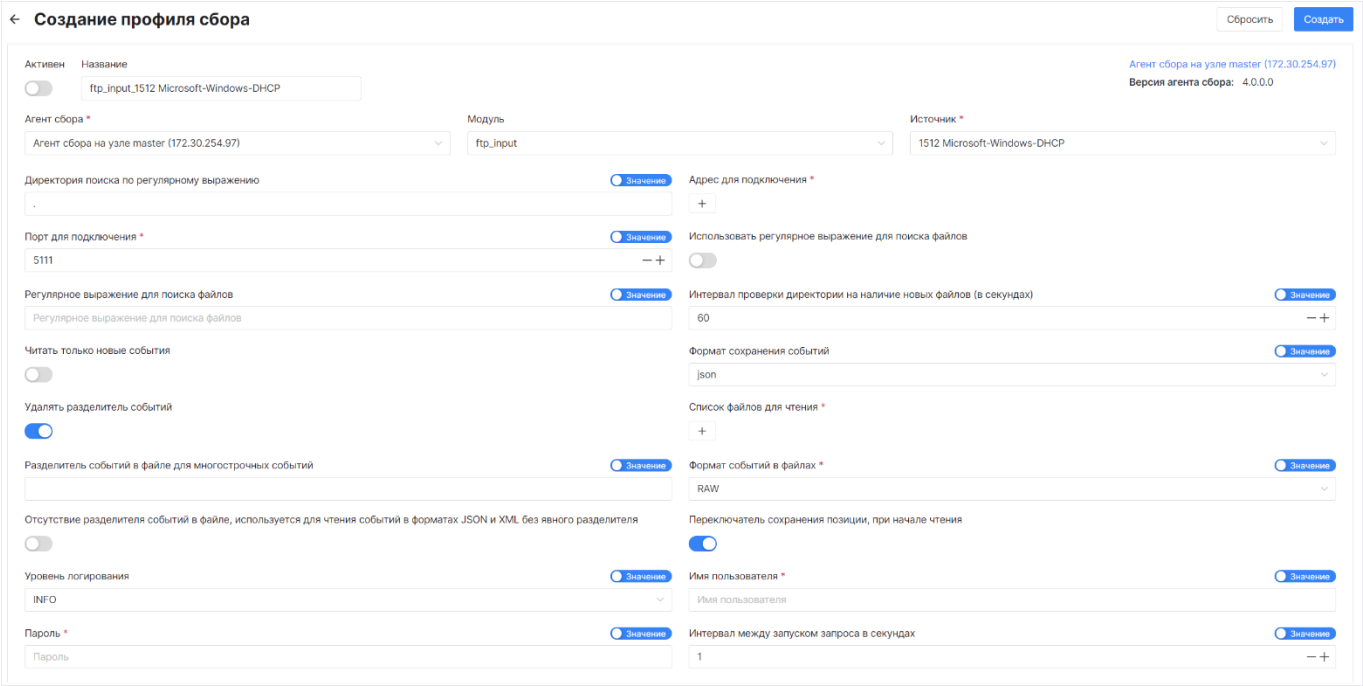


Рис. 106 – Пример формы для модуля ftp_input

Параметры модуля:

- **Директория поиска по регулярному выражению** – укажите каталог для поиска файлов по регулярному выражению;
- **Адрес для подключения** – укажите адреса для подключения к ftp-серверу;
- **Порт для подключения** – укажите порт для подключения к ftp-серверу;
- **Использовать регулярное выражение для поиска файлов** – при необходимости включите опцию, позволяющую использовать **regexp** (регулярные выражения) для поиска файлов журналов;
- **Регулярное выражение для поиска файлов** – укажите регулярное выражение для поиска файлов журнала;
- **Интервал проверки директории на наличие новых файлов (в секундах)** – укажите интервал поиска новых файлов в указанных каталогах. Значение указывается в секундах;
- **Читать только новые события** – при необходимости включите опцию, которая позволяет забирать из журнала только новые события;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Удалять разделитель событий** – настройте параметры чтения многострочных событий;
- **Список файлов для чтения** – укажите путь к файлам журналов;
- **Разделитель событий в файле для многострочных событий** – настройте параметры чтения многострочных событий;
- **Формат событий в файлах** – настройте параметры чтения многострочных событий;

- **Отсутствие разделителя событий в файле, используется для чтения событий в форматах JSON и XML без явного разделителя** – настройте параметры чтения многострочных событий;
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Имя пользователя** – укажите имя пользователя для доступа к ftp-серверу;
- **Пароль** – укажите пароль пользователя;
- **Интервал между запуском запроса в секундах** – укажите интервал между чтением файлов. Значение указывается в секундах;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.16 Модуль http_collector_input

Описание: Чтение файла, доступного через HTTP/HTTPs. Предварительно необходимо создать файл, из которого будет идти чтение.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

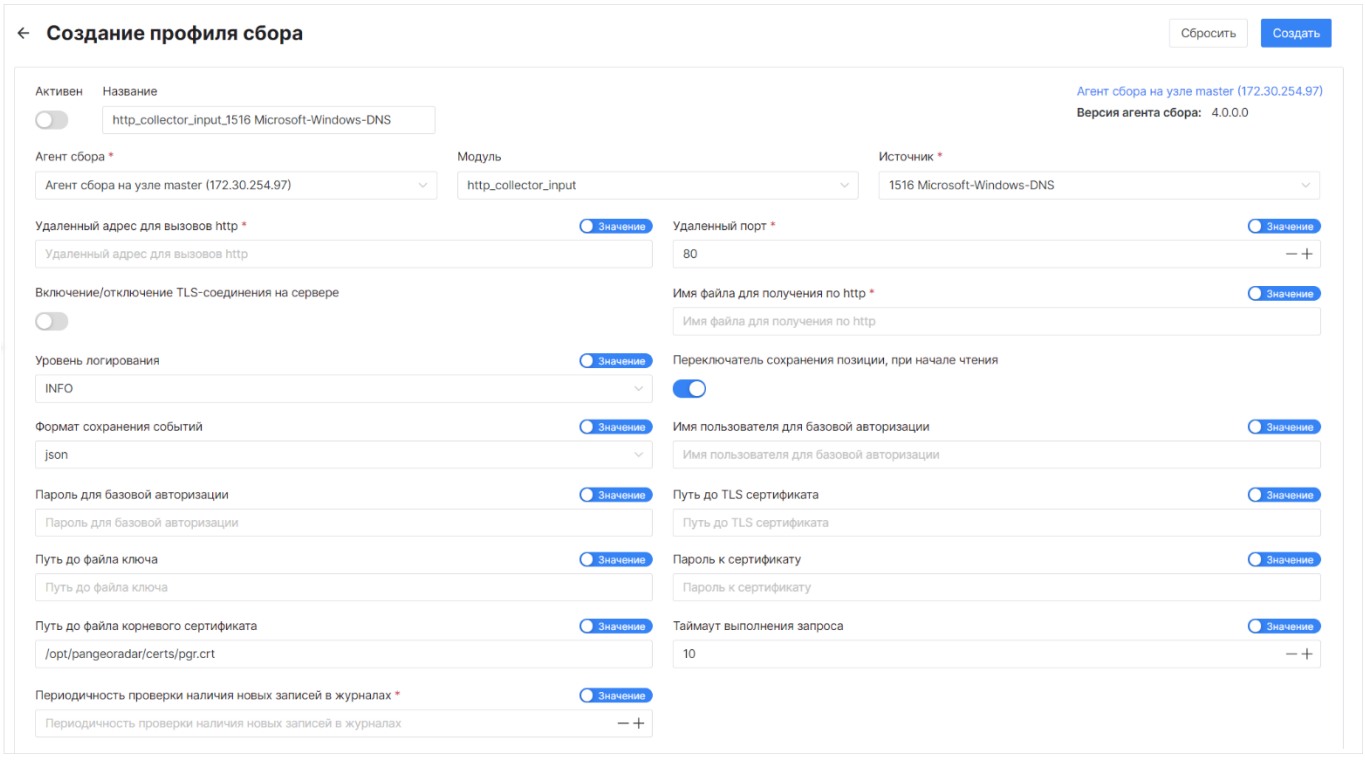


Рис. 107 – Пример формы для модуля http_collector_input

Параметры модуля:

- **Удаленный адрес для вызовов http** – укажите адрес сервера для http запросов;

- **Удаленный порт** – укажите порт сервера для http запросов;
- **Включение/отключение TLS-соединения на сервере** – при необходимости включите использование протокола Transport Layer Security (TLS) для обеспечения безопасной передачи данных;
- **Имя файла для получения по http** – укажите наименование файла для получения по HTTP;
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Имя пользователя для базовой авторизации** – укажите имя пользователя для базовой авторизации на http сервере. Если значение не указано, то считается, что авторизация выключена;
- **Пароль для базовой авторизации** – укажите пароль пользователя;
- **Путь до TLS сертификата** – укажите путь для файла сертификата, используемого при включенном TLS соединении;
- **Путь до файла ключа** – укажите путь для файла ключей, используемых при включенном TLS соединении;
- **Пароль к сертификату** – укажите пароль к TLS сертификату;
- **Путь до файла корневого сертификата** – укажите путь до корневого сертификата;
- **Таймаут выполнения запроса** – укажите ограничение времени обработки запросов, сделанных http клиентом. Значение указывается в секундах;
- **Периодичность проверки наличия новых записей в журналах** – укажите интервал между чтением файлов, в секундах;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.17 Модуль http_request_input

Описание: Приём HTTP/HTTPs-запросов.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

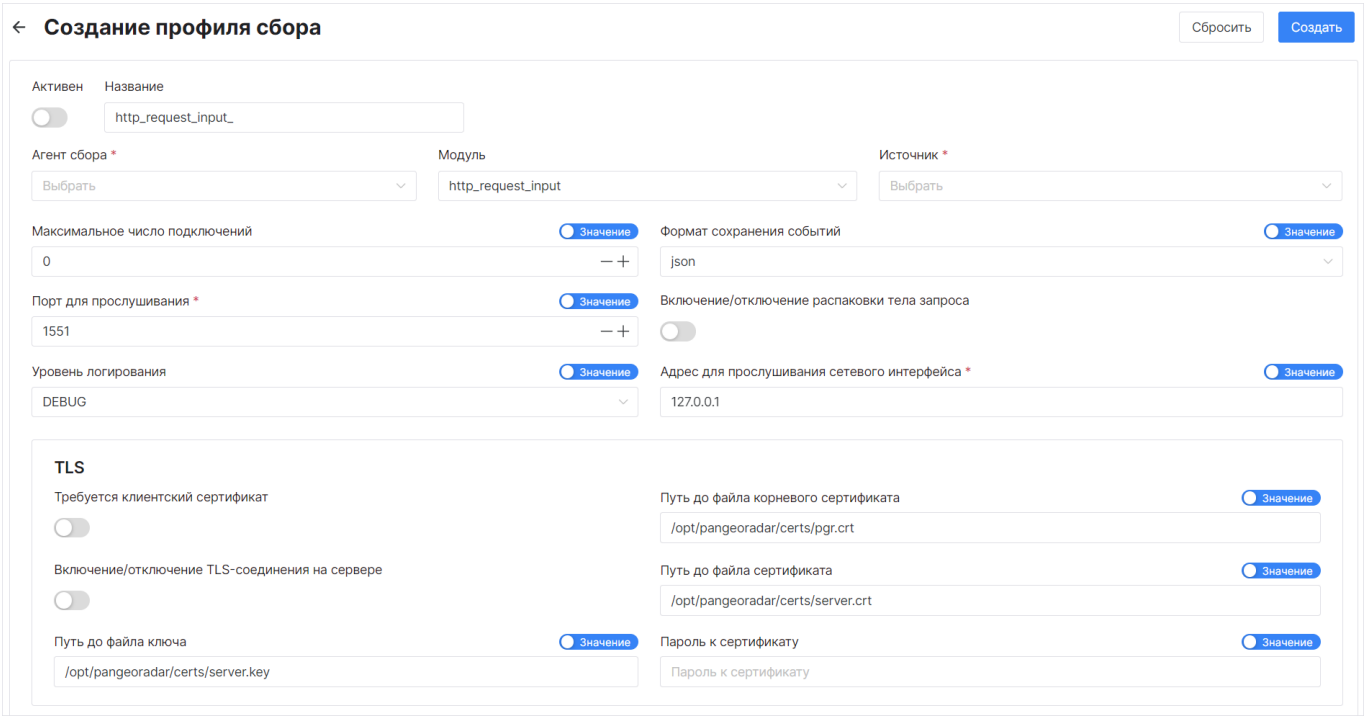


Рис. 108 – Пример формы для модуля http_request_input

Параметры модуля:

- **Максимальное число подключений** – укажите лимит соединений с сервером;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Порт для прослушивания** – укажите порт сервера;
- **Включение/отключение распаковки тела запроса** – при необходимости включите автоматическую распаковку тела запроса;
- **Адрес для прослушивания сетевого интерфейса** – укажите адрес сервера;
- **Уровень логирования** – выберите уровень журналирования модуля;
- **TLS**. В блоке указываются параметры использования протокола Transport Layer Security (TLS) для обеспечения безопасной передачи данных:
    - **Требуется клиентский сертификат** – при необходимости включите необходимость использования клиентского сертификата для подключения к серверу;
    - **Путь до файла корневого сертификата** – укажите путь до корневого сертификата;
    - **Включение/отключение TLS-соединения на сервере** – при необходимости включите использование протокола TLS;
    - **Путь до файла сертификата** – укажите путь для файла сертификата, используемого при включенном TLS соединении;
    - **Путь до файла ключа** – укажите путь для файла ключей, используемых при включенном TLS соединении;
    - **Пароль к сертификату** – укажите пароль к TLS сертификату.

3.3.3.1.18 Модуль kafka_input

Описание: Приём HTTP/HTTPs-запросов.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: нет.

Поддержка настройки кодировки: нет.

Поддержка вывода в файл: нет.

Пример формы настройки модуля:

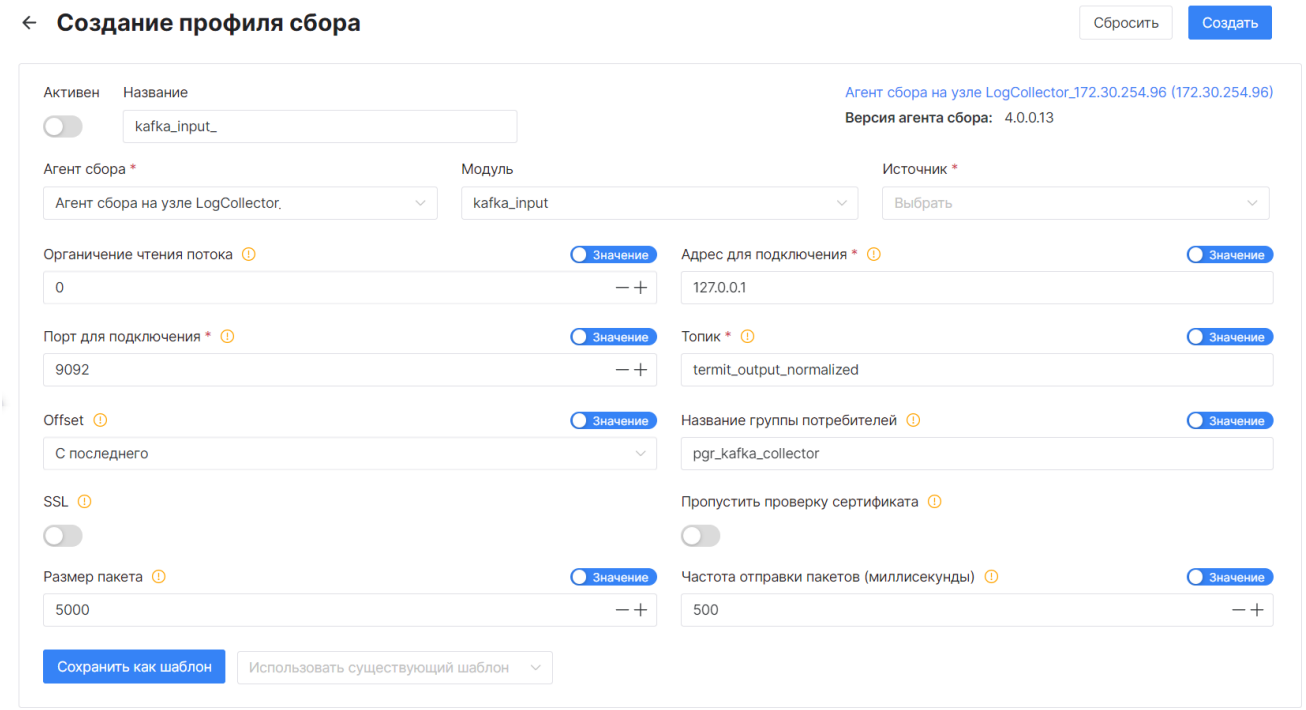


Рис. 109 – Пример формы для модуля kafka_input

Параметры модуля:

- **Ограничение чтения потока** – укажите ограничение чтения потока. Параметр **0** – без ограничений;
- **Адрес для подключения** – укажите адрес для подключения к сервису **Kafka**;
- **Порт для подключения** – укажите порт для подключения к сервису **Kafka**;
- **Топик** – укажите заголовок, по которому будет выполняться чтение. Допустимые значения:
  - `termit_output_normalized` – нормализованные события;
  - `termit_output_parsing` – разобранные события;
  - `termit_output_error` – неразобранные события;
- **Offset** – выберите из выпадающего списка способ смещения событий: с самого раннего, с последнего;
- **Название группы потребителей** – укажите группу потребителей (consumer) в сервисе которая будет читать сообщения из сервиса **Kafka**;

- **SSL** – при необходимости включите использование протокола SSL;
- **Пропустить проверку сертификата** – при необходимости включите опцию, которая позволяет пропустить проверку сертификата при обращении к сервису **Kafka**;
- **Размер пакета** – укажите количество событий, которое будет передано в одном пакете;
- **Частота отправки пакетов (миллисекунды)** – укажите интервал отправки пакетов. Значение указывается в миллисекундах.

3.3.3.1.19 Модуль mseven6_input

Описание: модуль для сбора событий по протоколу MS-EVEN6 с Windows Vista и выше.

Поддержка ОС: Linux.

Поддержка фильтрации: нет.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Настройки фильтрации (исключения) событий: есть.

Пример формы настройки модуля:

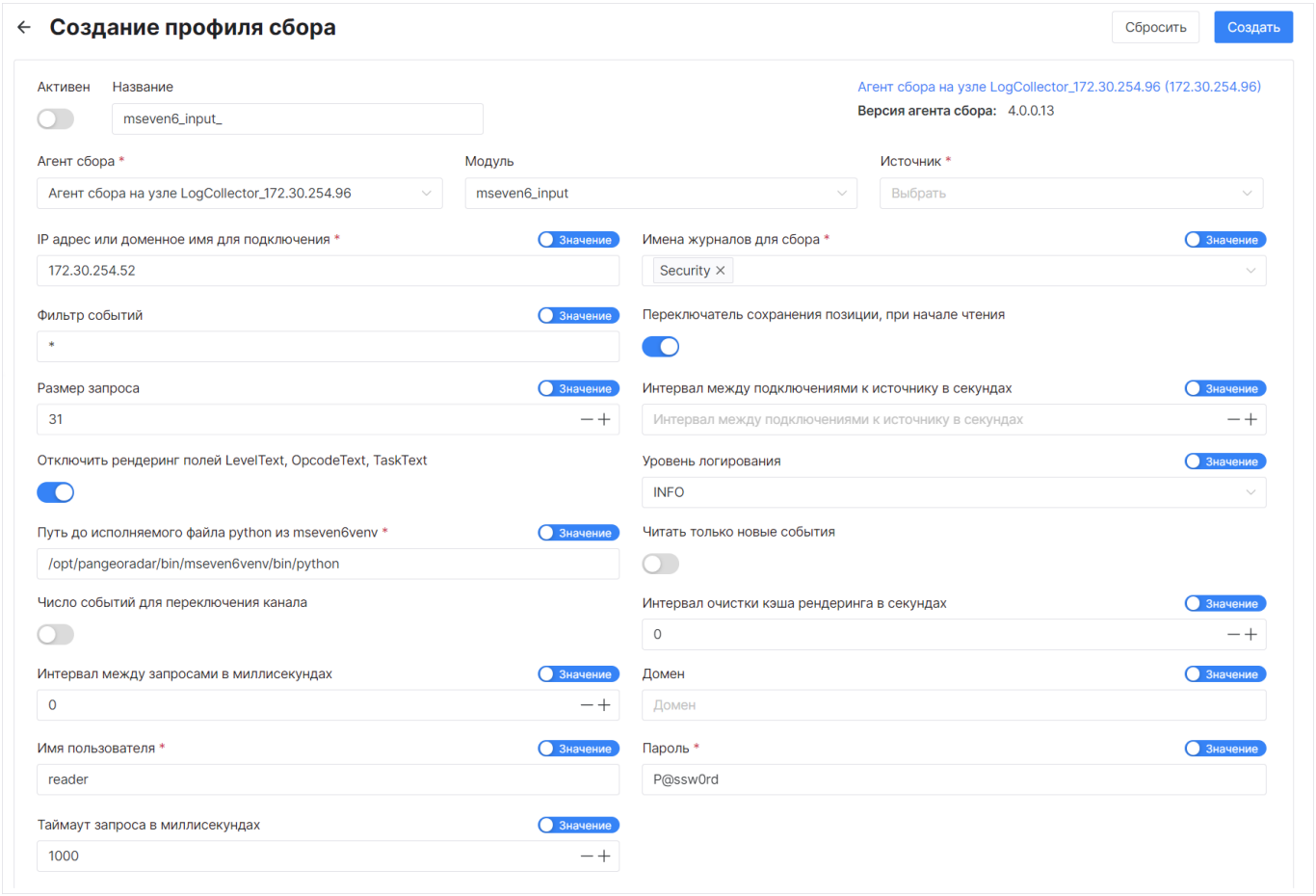


Рис. 110 – Пример формы для модуля mseven6_input

Параметры модуля:

- **IP адрес или доменное имя для подключения** – укажите адрес удаленного сервера, с которого будут собираться события;

- **Имена журналов для сбора** – из выпадающего списка выберите один или несколько каналов, из которых нужно собирать события. Поле указывается в случае, если не указано поле **Путь до файла журнала**. Возможные значения:
    - Application;
    - Microsoft-Windows-PowerShell/Operational;
    - Security;
    - System.
- **Фильтр событий** – укажите запрос для фильтрации событий для чтения с помощью выражения XPath. Возможные значения:
    - структурированный XML запрос, например
      `<QueryList><Query><Select Path=\"Security\">*[System[(EventID=42) and (Level=2)]]</Select></Query></QueryList>`;
    - * - все параметры.
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Размер запроса** – укажите количество событий, загружаемых за один запрос;
- **Интервал между подключениями к источнику в секундах** – укажите интервал между подключениями к источнику;
- **Отключить рендеринг полей LevelText, OpcodeText, TaskText** – при необходимости включите опцию, которая отключит рендеринг полей LevelText, OpcodeText, TaskText;
- **Путь до исполняемого файла python из mseven6venv** – укажите путь до исполняемого файла;
- **Читать только новые события** – при необходимости включите опцию, которая позволяет забирать из журнала только новые события;
- **Число событий для переключения канала** – в случае, если указано несколько источников или каналов, опция считает число событий и при достижении указанного значения, переключается на чтение следующего источника
- **Интервал очистки кэша рендеринга в секундах** – укажите интервал очистки кэша;
- **Интервал между запросами в миллисекундах** – укажите интервал, через который файл (или канал) проверяется на наличие новых записей лога;
- **Имя пользователя** – укажите имя пользователя для доступа к удаленному серверу;
- **Пароль** – укажите пароль пользователя;
- **Домен** – укажите наименование домена источника;
- **Таймаут запроса в миллисекундах** – укажите таймаут отправки запроса;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.20 Модуль nf_input

Описание: Прием NetFlow трафика.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

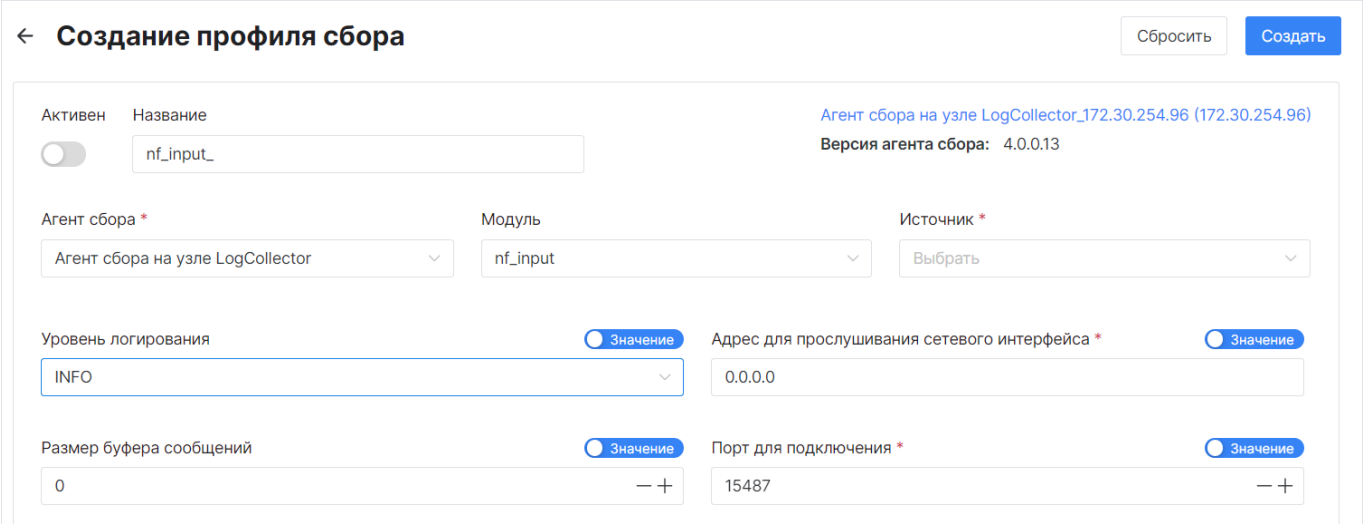


Рис. 111 – Пример формы для модуля nf_input

Параметры модуля:

- **Адрес для прослушивания сетевого интерфейса** – укажите адрес Netflow сервера;
- **Размер буфера сообщений** – укажите размер буфера сообщений. Если параметр не задан, то значение берется из параметра Netflow сервера SO_RCVBUF. Значение указывается в байтах;
- **Порт для подключения** – укажите порт Netflow сервера;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.21 Модуль odbc_input

Описание: Чтение данных из СУБД (MySQL, Oracle, MS SQL, PostgreSQL).

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: нет.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

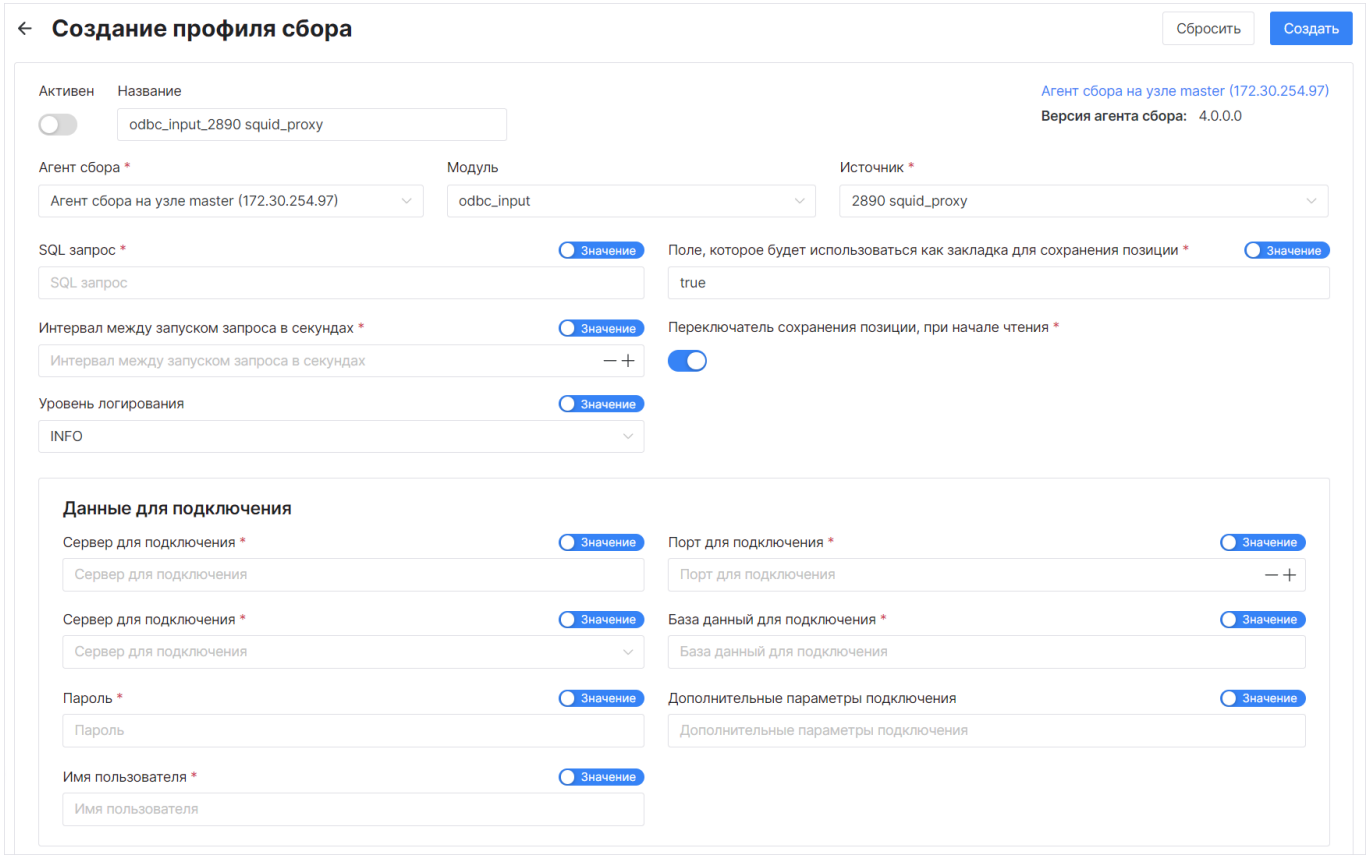


Рис. 112 – Пример формы для модуля odbc_input

Параметры модуля:

- **SQL запрос** – укажите SQL запрос к базе данных;
- **Поле, которое будет использоваться как закладка для сохранения позиции** – укажите поле, которое будет использоваться как закладка для сохранения позиции. Поле должно быть указано в операторе SELECT sql-запроса;
- **Интервал между запуском запроса в секундах** – укажите интервал, через который будет выполняться проверка новых записей в журнале. Значение указывается секундах;
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Уровень логирования** – выберите уровень журналирования модуля;
- **Данные для подключения**. В блоке указываются параметры подключения к БД:
  - **Сервер для подключения** – укажите адрес сервера БД;
  - **Порт для подключения** – укажите порт сервера БД;
  - **Драйвер для подключения** – укажите драйвер для подключения к БД, например MySQL ODBC 8.0 Driver;
  - **База данных для подключения** – укажите наименование БД;
  - **Имя пользователя** – укажите имя пользователя БД;
  - **Пароль** – укажите пароль пользователя для подключения к БД;

- **Дополнительные параметры подключения** – при необходимости укажите дополнительные параметры подключения к БД**.**

3.3.3.1.22 Модуль opsec_lea_input

Описание: Сбор событий с источников «Checkpoint Firewall (opsec)».

Поддержка ОС: Linux.

Поддержка фильтрации: нет.

Поддержка настройки кодировки: нет.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

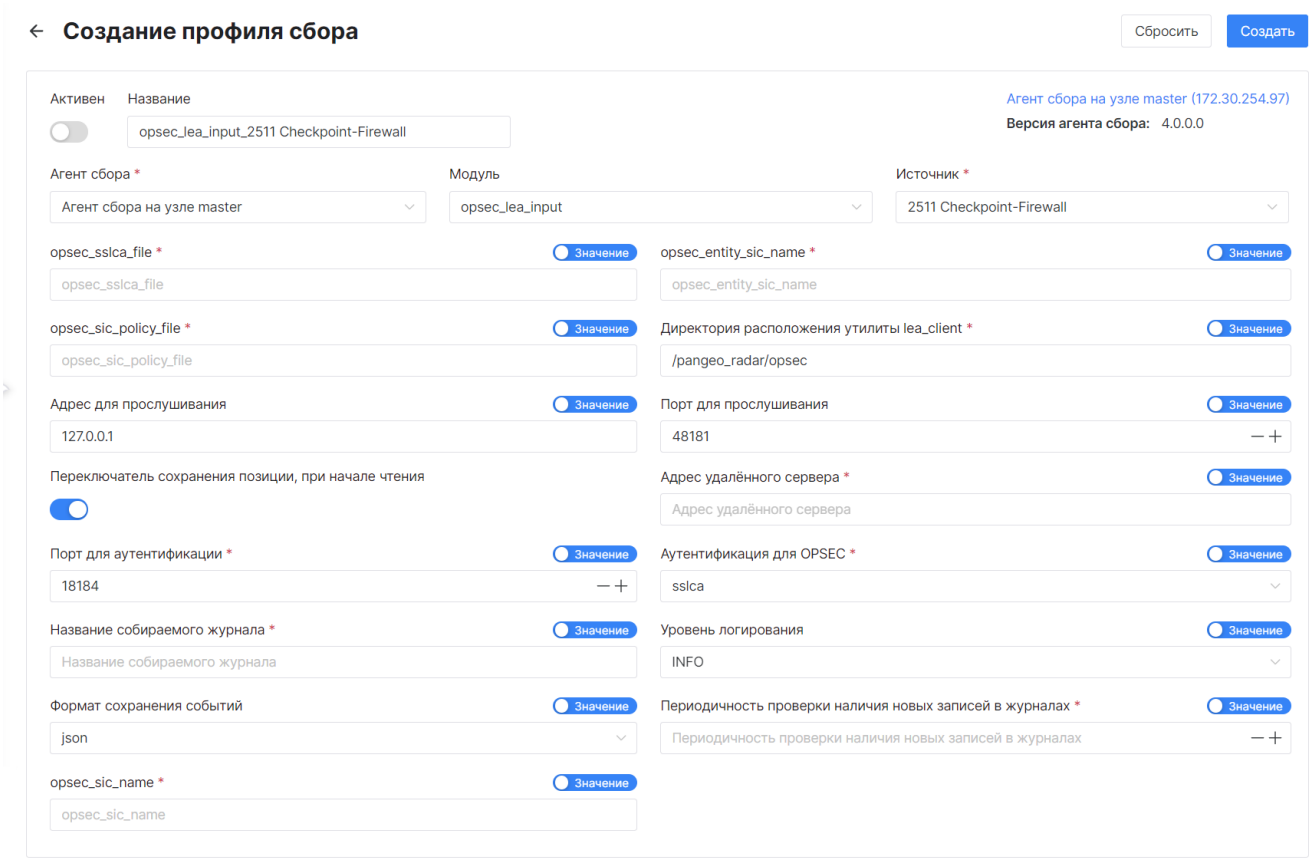


Рис. 113 – Пример формы для модуля opsec_lea_input

Параметры модуля:

- **opsec_sslca_file** – укажите путь к файлу, который содержит цифровой сертификат приложения OPSEC;
- **opsec_entity_sic_name** – укажите официальное имя приложения OPSEC, которое является полным именем приложения, определённым сервером;
- **opsec_sic_policy_file** – укажите путь к файлу политики SIC;
- **Директория расположения утилиты lea_client** – укажите путь к директории расположения утилиты lea_client;
- **Адрес для прослушивания** – укажите IP-адрес расположения утилиты lea_client;

- **Порт для прослушивания** – укажите порт для подключения к утилите lea_client;
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Адрес удалённого сервера** – укажите IP-адрес агента сбора;
- **Порт для аутентификации** – укажите порт для аутентификации на агенте сбора;
- **Аутентификация для OPSEC** – выберите способ аутентификации для OPSEC: sslca, fwn1;
- **Название собираемого журнала** – укажите наименование файла журнала;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Периодичность проверки наличия новых записей в журналах** – укажите интервал проверки наличия новых записей в журналах. Значение задается в секундах;
- **opsec_sic_name** –укажите DN сервера Checkpoint;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.23 Модуль sftp_input

Описание: Чтение файла, доступного через SFTP.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть. Настройка блока имеет следующие особенности:

- **Исходная кодировка** – укажите кодировку событий источника. Если значение не указано, то профиль сбора попытается определить кодировку самостоятельно;
- **Изменить кодировку событий на UTF-8** – опция, позволяющая изменить кодировку исходника в utf8;
- **Размер буфера для определения исходной кодировки** – укажите размер буфера, который будет использоваться для определения кодировки (в байтах).

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

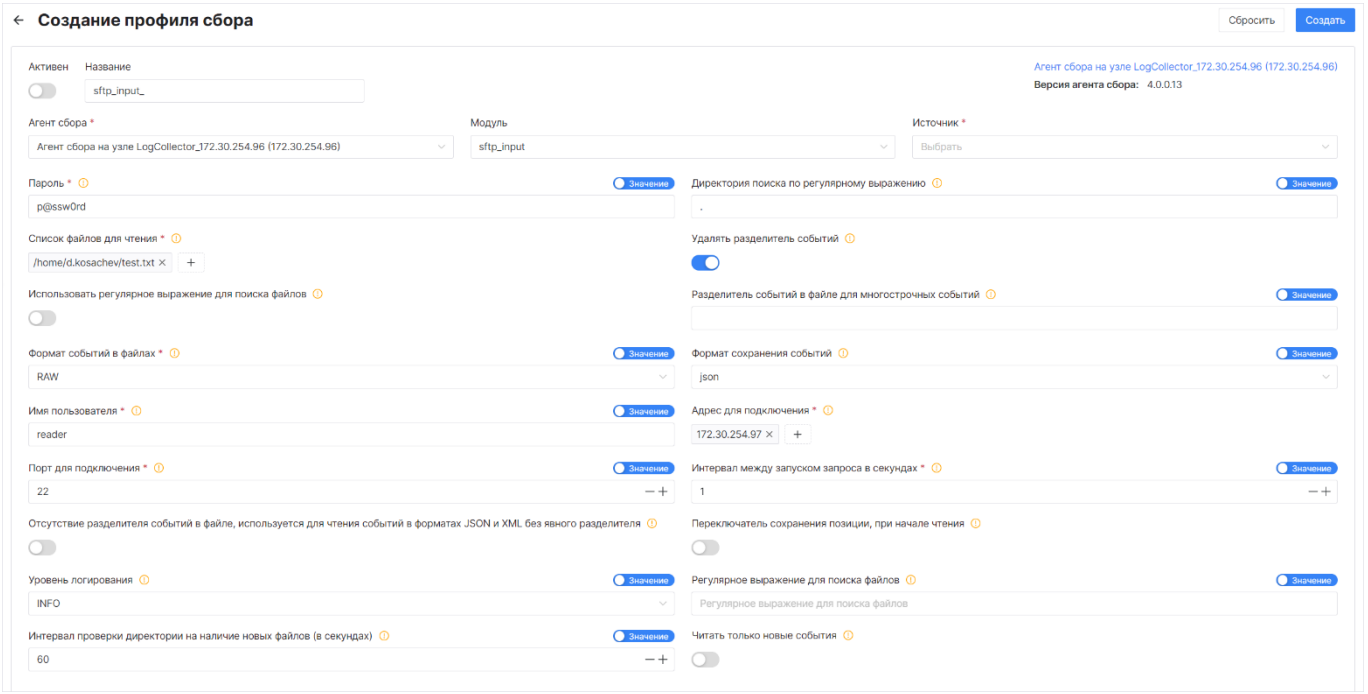


Рис. 114 – Пример формы для модуля sftp_input

Параметры модуля:

- **Пароль** – укажите пароль пользователя ssh;
- **Директория поиска по регулярному выражению** – укажите каталог для поиска файлов по регулярному выражению;
- **Список файлов для чтения** – укажите список файлов журналов;
- **Удалять разделитель событий** – настройте параметры чтения многострочных событий;
- **Использовать регулярное выражение для поиска файлов** – при необходимости включите опцию, позволяющую использовать **regexp** (регулярные выражения) для поиска файлов журналов;
- **Разделитель событий в файле для многострочных событий** – настройте параметры чтения многострочных событий;
- **Формат событий в файлах** – настройте параметры чтения многострочных событий;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Имя пользователя** – укажите имя пользователя ssh;
- **Адрес для подключения** – укажите адрес sftp сервера;
- **Порт для подключения** – укажите порт sftp сервера;
- **Интервал между запуском запроса в секундах** – укажите интервал между чтением файлов, в секундах;
- **Отсутствие разделителя событий в файле, используется для чтения событий в форматах JSON и XML без явного разделителя** – настройте параметры чтения многострочных событий;

- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Регулярное выражение для поиска файлов** – укажите регулярное выражение для поиска файлов журнала;
- **Интервал проверки директории на наличие новых файлов (в секундах)** – укажите интервал поиска новых файлов в указанных каталогах. Значение указывается в секундах;
- **Читать только новые события** – при необходимости включите опцию, которая позволяет забирать из журнала только новые события;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.24 Модуль smb_input

Описание: Чтение файла, доступного через SMB.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть. Настройка блока имеет следующие особенности:

- **Исходная кодировка** – укажите кодировку событий источника. Если значение не указано, то профиль сбора попытается определить кодировку самостоятельно;
- **Изменить кодировку событий на UTF-8** – опция, позволяющая изменить кодировку исходника в utf8;
- **Размер буфера для определения исходной кодировки** – укажите размер буфера, который будет использоваться для определения кодировки (в байтах).

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

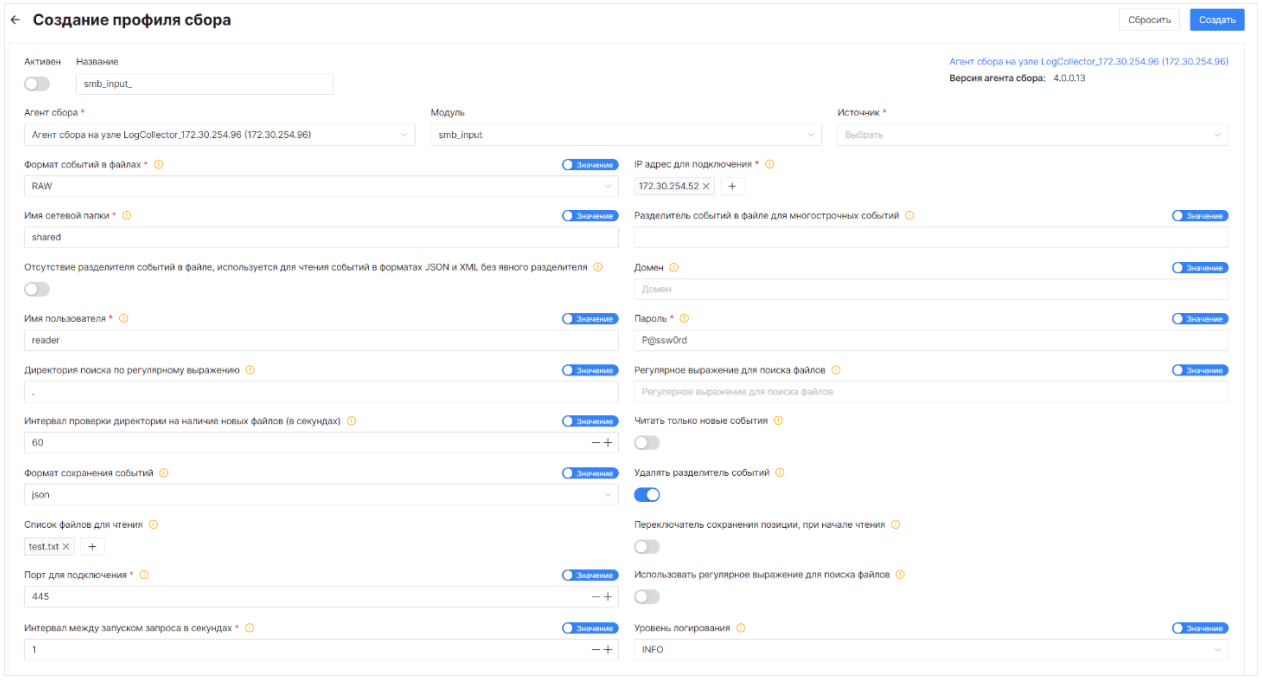


Рис. 115 – Пример формы для модуля smb_input

Параметры модуля:

- **Формат событий в файлах** – настройте параметры чтения многострочных событий;
- **IP адрес для подключения** – укажите адрес SMB сервера;
- **Имя сетевой папки** – укажите путь к папкам и файлам, открытым к свободному доступу на сервере, использующем протокол SMB. должен соответствовать формату <share> или \\<server>\<share>;
- **Разделитель событий в файле для многострочных событий** – настройте параметры чтения многострочных событий;
- **Отсутствие разделителя событий в файле, используется для чтения событий в форматах JSON и XML без явного разделителя** – настройте параметры чтения многострочных событий;
- **Домен** – укажите домен SMB сервера;
- **Имя пользователя** – укажите имя пользователя для подключения к SMB серверу;
- **Пароль** – укажите пароль пользователя;
- **Директория поиска по регулярному выражению** – укажите каталог для поиска файлов по регулярному выражению;
- **Регулярное выражение для поиска файлов** – укажите регулярное выражение для поиска файлов журнала;
- **Интервал проверки директории на наличие новых файлов (в секундах)** – укажите интервал поиска новых файлов в указанных каталогах. Значение указывается в секундах;
- **Читать только новые события** – при необходимости включите опцию, которая позволяет забирать из журнала только новые события;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Удалять разделитель событий** – настройте параметры чтения многострочных событий;
- **Список файлов для чтения** – укажите список файлов журналов;
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Порт для подключения** – укажите порт SMB сервера;
- **Использовать регулярное выражение для поиска файлов** – при необходимости включите опцию, позволяющую использовать **regexp** (регулярные выражения) для поиска файлов журналов;
- **Интервал между запуском запроса в секундах** – укажите интервал между запуском сканирования файлов. Значение указывается в секундах;
- **Уровень логирования** – выберите уровень журналирования модуля;
- **Настройки аутентификации по Kerberos**. В блоке указываются настройки аутентификации по kerberos:

- **Включить аутентификацию по Kerberos** – при необходимости включите опцию, которая позволяет использовать для подключения к SMB серверу аутентификацию с помощью kerberos;
- **Имя целевого сервиса** – укажите имя целевого сервиса (service principal name);
- **Область (realm)** – укажите область сети, используемая kerberos. Параметр регистрозависимый, обычно пишется в верхнем регистре и совпадает с именем домена;
- **Путь до конфигурации Kerberos** – укажите путь до конфигурации kerberos;

3.3.3.1.25 Модуль snmp_traps_input

Описание: Приём SNMP Traps.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть. Настройка блока имеет следующие особенности:

- **Исходная кодировка** – укажите кодировку событий источника. Если значение не указано, то профиль сбора попытается определить кодировку самостоятельно;
- **Изменить кодировку событий на UTF-8** – опция, позволяющая изменить кодировку исходника в utf8;
- **Размер буфера для определения исходной кодировки** – укажите размер буфера, который будет использоваться для определения кодировки (в байтах).

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

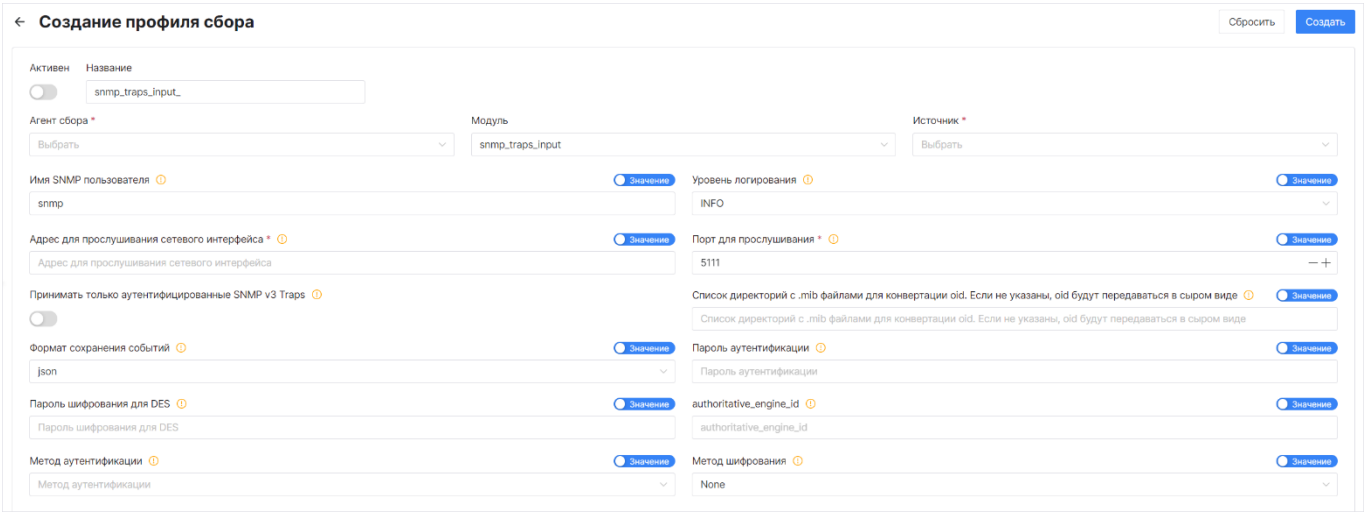


Рис. 116 – Пример формы для модуля snmp_traps_input

Параметры модуля:

- **Имя SNMP пользователя** – укажите имя SNMP пользователя;
- **Адрес для прослушивания сетевого интерфейса** – укажите адрес SNMP сервера;
- **Порт для прослушивания** – укажите порт SNMP сервера;

- **Принимать только аутентифицированные SNMP v3 Traps** – при необходимости включите опцию, которая включает прием только аутентифицированных SNMP v3 Traps;
- **Список директорий с .mib файлами для конвертации oid. Если не указаны, oid будут передаваться в сыром виде** – укажите список директорий с .mib файлами для конвертации oid. Если не указаны, oid будут передаваться в сыром виде;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Пароль аутентификации** – укажите пароль пользователя. Используется с MD5 или SHA;
- **Пароль шифрования для DES** – укажите пароль шифрования для DES;
- **authoritative_engine_id** – укажите движок, который используется в SNMPv3 для идентификации сущностей;
- **Метод аутентификации** – выберите метод аутентификации на SNMP сервере: MD5, SHA;
- **Метод шифрования** – выберите метод шифрования. Поддерживается только DES;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.26 Модуль ssh_collector_input

Описание: Выполнение внешней команды через SSH.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

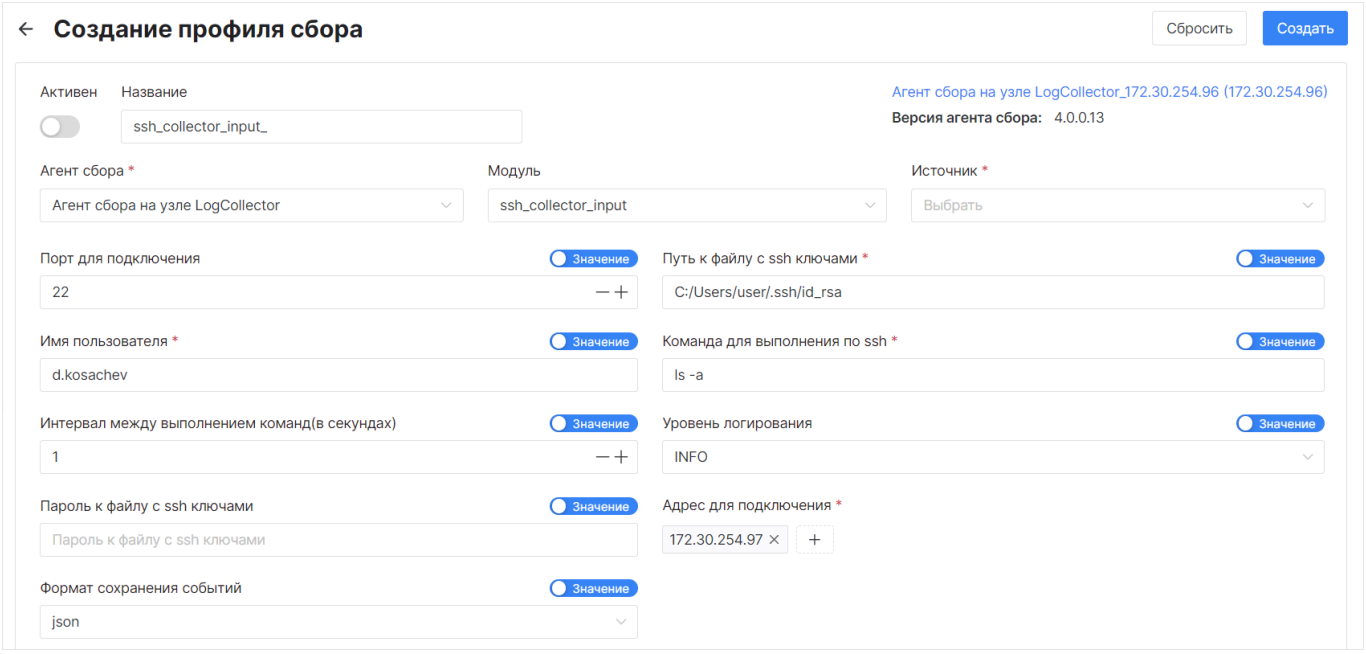


Рис. 117 – Пример формы для модуля ssh_collector_input

Параметры модуля:

- **Порт для подключения** – укажите порт для подключения к хосту;

- **Путь к файлу с ssh ключам** – укажите путь к файлу с ssh ключами;
- **Имя пользователя** – укажите имя пользователя для удаленного подключения;
- **Команда для выполнения по ssh** – укажите команду для выполнения по ssh;
- **Интервал между выполнением команд (в секундах)** – укажите интервал между выполнением команд. Значение указывается в секундах;
- **Пароль к файлу с ssh ключами** – укажите пароль от файла с ключами;
- **Адрес для подключения** – укажите список хостов для подключения;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.27 Модуль tcp_input

Описание: Приём TCP трафика.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

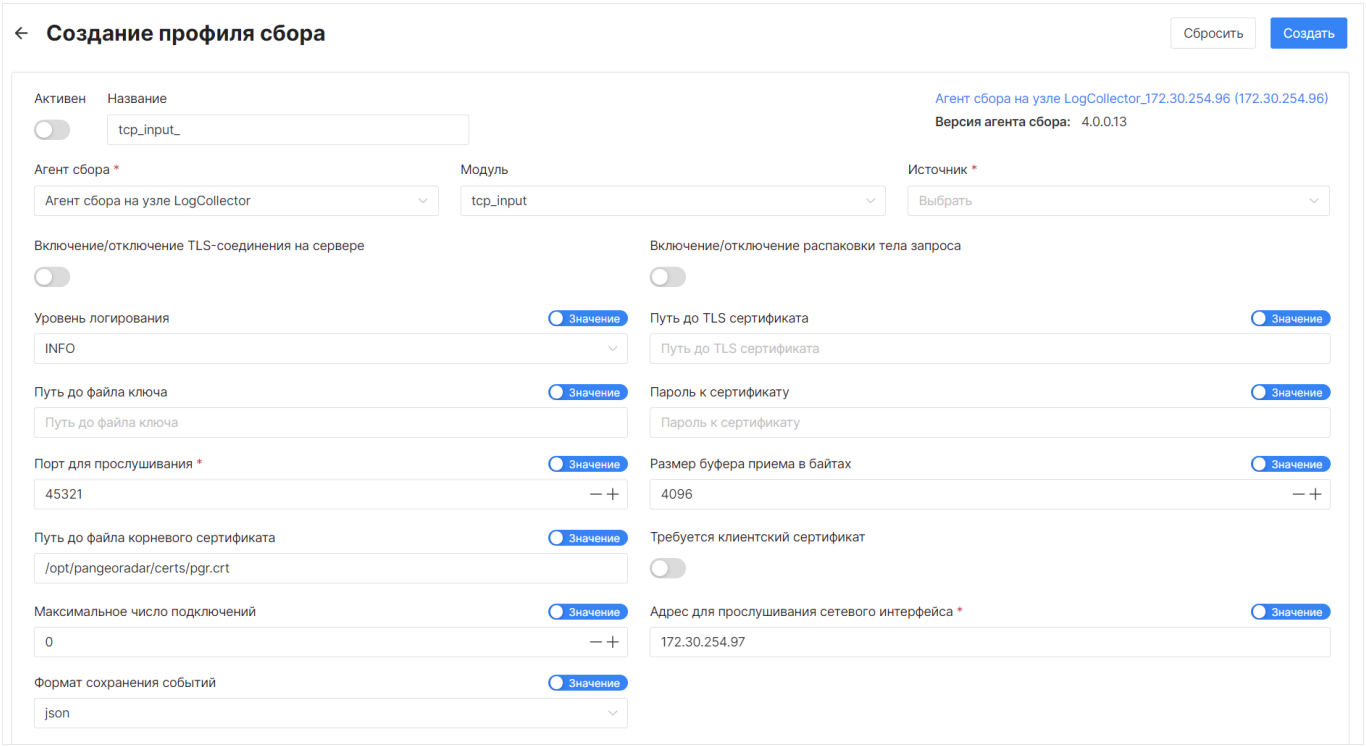


Рис. 118 – Пример формы для модуля tcp_input

Параметры модуля:

- **Включение/отключение TLS-соединения на сервере** – при необходимости включите использование протокола TLS;

- **Включение/отключение распаковки тела запроса** – опция, которая включает распаковку тела запроса. Ожидается, что тело запроса упаковано в архив;
- **Путь до TLS сертификата** – укажите путь для файла сертификата, используемого при включенном TLS соединении;
- **Путь до файла ключа** – укажите путь для файла ключей, используемых при включенном TLS соединении;
- **Пароль к сертификату** – укажите пароль к TLS сертификату;
- **Порт для прослушивания** – укажите порт сервера;
- **Размер буфера приема в байтах** – укажите размер буфера сообщений. Значение указывается в байтах;
- **Путь до файла корневого сертификата** – укажите путь до корневого сертификата;
- **Требуется клиентский сертификат** – при необходимости включите необходимость использования клиентского сертификата для подключения к серверу;
- **Максимальное число подключений** – укажите лимит соединений с сервером;
- **Адрес для прослушивания сетевого интерфейса** – укажите адрес сервера;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.28 Модуль udp_input

Описание: Приём UDP трафика.

Поддержка ОС: Windows, Linux.

Поддержка фильтрации: есть.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

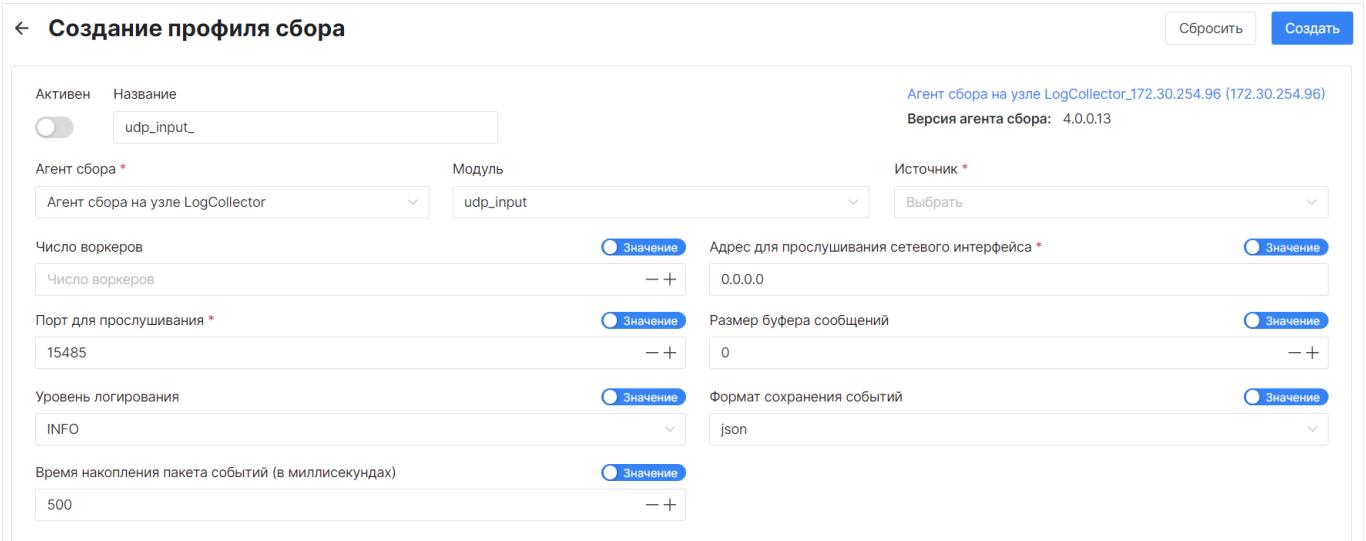


Рис. 119 – Пример формы для модуля udp_input

Параметры модуля:

- **Число воркеров** – укажите количество воркеров, которое будет задействовано для обработки событий;
- **Адрес для прослушивания сетевого интерфейса** – укажите адрес сервера;
- **Порт для прослушивания** – укажите порт сервера;
- **Размер буфера сообщений** – укажите размер буфера сообщений. Значение указывается в байтах;
- **Время накопления пакета событий (в миллисекундах)** – укажите интервал формирования пакета событий;
- **Формат сохранения событий** – выберите формат сохранения событий;
- **Уровень логирования** – выберите уровень журналирования модуля.

3.3.3.1.29 Модуль wmi_input

Описание: Сбор событий через механизм WMI.

Поддержка ОС: Windows.

Поддержка фильтрации: нет.

Поддержка настройки кодировки: есть.

Поддержка вывода в файл: есть.

Пример формы настройки модуля:

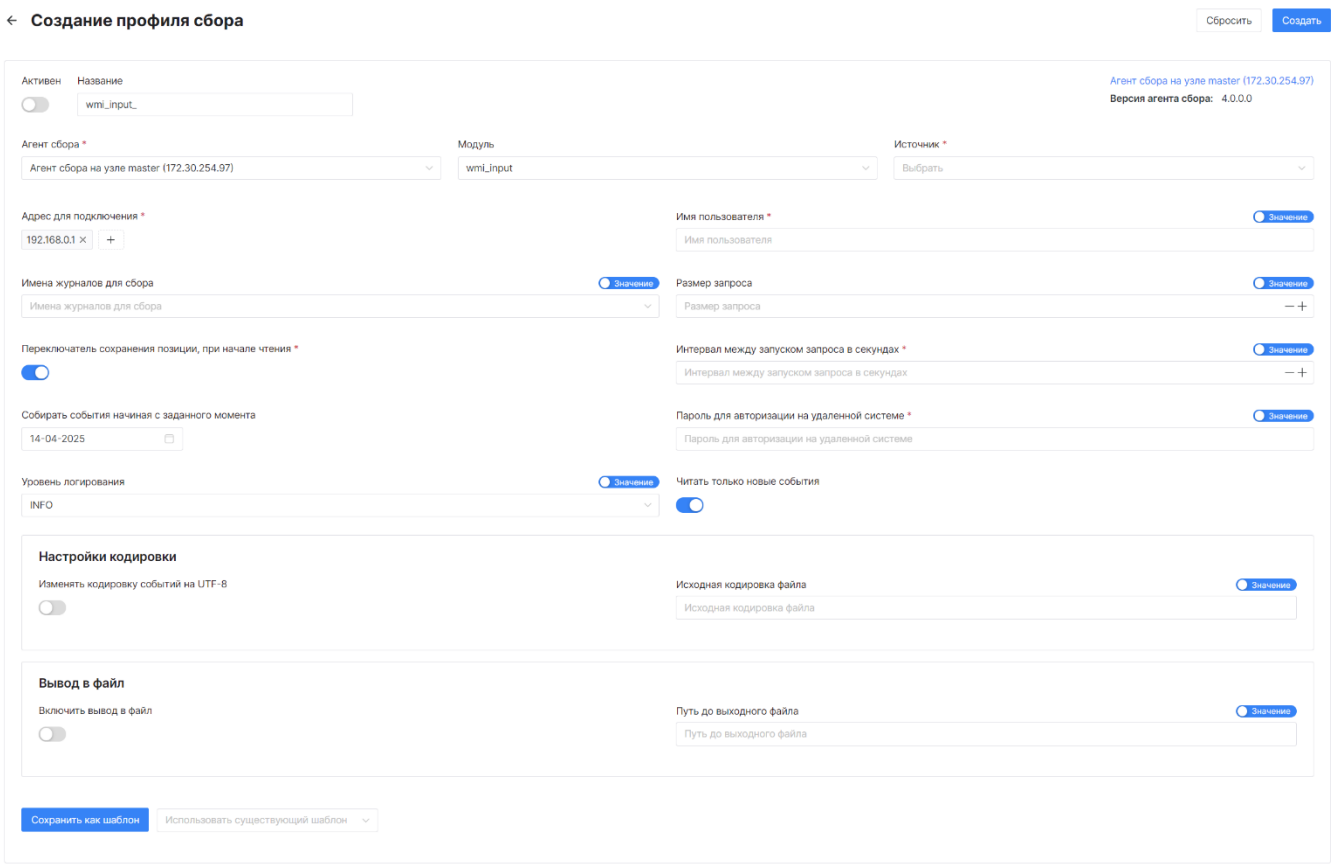


Рис. 120 – Пример формы для модуля wmi_input

Параметры модуля:

- **Адрес для подключения** – укажите адрес удаленного сервера;
- **Имя пользователя** – укажите имя пользователя для удаленного подключения;
- **Имена журналов для сбора** – из выпадающего списка выберите один или несколько каналов, из которых нужно собирать события. Поле указывается в случае, если не указано поле **Путь до файла журнала**. Возможные значения:
  - Application;
  - Microsoft-Windows-PowerShell/Operational;
  - Security;
  - System.
- **Размер запроса** – укажите количество событий, загружаемых за один запрос;
- **Переключатель сохранения позиции, при начале чтения** – при необходимости включите опцию, которая позволяет продолжить чтение журнала с последней сохраненной позиции после перезапуска;
- **Интервал между запуском запроса в секундах** – укажите интервал, через который файл (или канал) проверяется на наличие новых записей лога;
- **Собирать события начиная с заданного момента** – укажите дату и время, с которого необходимо начать собирать события;
- **Пароль для авторизации на удаленной системе** – укажите пароль пользователя;
- **Читать только новые события** – при необходимости включите опцию, которая позволяет забирать из журнала только новые события;
- **Уровень логирования** – выберите уровень журналирования модуля;
- **Настройки фильтрации (исключения) событий** – в блоке указываются фильтры по полям событий с помощью регулярных выражений. В данном блоке можно указать для полей следующие типы фильтров:
  - Фильтры по времени, пример: `2025-03-13 10:02:55.9689259 +0000 UTC`. Используется для следующих полей:
    - Created;
    - EventTime;
  - Числовые фильтры, пример: `^([5-9]\d|\d{3,})$`. Используется для следующих полей:
    - EventID;
    - Qualifiers;
    - RecordID;
    - ExecutionProcessID;
    - ThreadID;

- Version.

- Строковые фильтры, пример: `DESKTOP-IDCMV6G`. Используется для следующих полей:
  - Hostname;
  - Msg.
- Возможные значения:
  - Пример для поля LevelText: `Information, Warning, Error`;
  - Пример для поля TaskText: `Service, State, Event`;
  - Пример для поля OpcodeText: `ServiceShutdown`;
  - Пример для поля ChannelText: `System`;
  - Пример для поля ProviderTex: `System`.

3.3.3.2 Просмотр профиля сбора

Открыть профиль сбора на просмотр можно двумя способами:

- нажмите кнопку в строке нужного профиля сбора;
- нажмите по ссылке в колонке "Название".

Откроется форма просмотра агента сбора. Поля формы формируются в зависимости от выбранного модуля сбора.

На форме просмотра профиля сбора доступно три общих блока: **Статистика**, **Полученные события** и **Отправленные события** (см. «Рис. 121»).

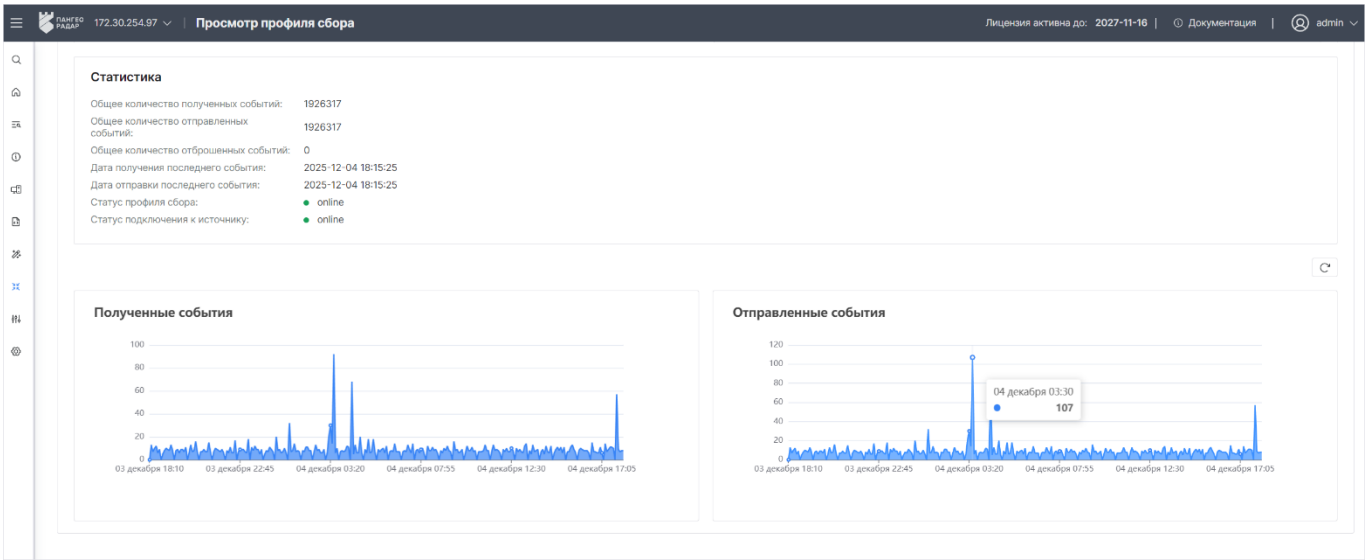


Рис. 121 – Форма "Просмотр профиля сбора". Общие блоки

В общих блоках отображается следующая информация:

- Блок **Статистика** содержит сводную информацию о потоке событий, собранных профилем:
  - Общее количество полученных событий;

    - Общее количество отправленных событий;
    - Общее количество отброшенных событий;
    - Дата получения последнего события;
    - Дата отправки последнего события;
    - Статус профиля сбора;
    - Статус подключения к источнику.
- Блок **Статистика полученных событий** – содержит графическое представление количества полученных событий от источников за период времени;
- Блок **Статистика отправленных событий** – содержит графическое представление количества отправленных событий в сервис **Log-proxy** за период времени.

3.3.3.3 Редактирование профиля сбора

Открыть профиль сбора на редактирование можно следующими способами:

- Перейдите в раздел **Источники → Профили сбора** и нажмите кнопку  в строке нужного профиля сбора.
- Перейдите на форму просмотра профиля сбора и нажмите кнопку **Редактировать**.

Внесите необходимые изменения и нажмите кнопку **Сохранить**.

3.3.3.4 Экспорт профилей сбора

Для массового экспорта профилей сбора установите нужные флаги и нажмите кнопку **Экспортировать**. Будет сформирован архив с профилями в формате `.zip`.

Для экспорта всех профилей сбора нажмите кнопку **Экспортировать все**.

3.3.3.5 Импорт профилей сбора

1. Нажмите кнопку **Импортировать**.
2. В открывшемся окне укажите путь к архиву с профилями сбора.
3. Нажмите кнопку **Открыть**.
4. Чтобы все изменения вступили в силу нажмите кнопку **Синхронизировать**.

3.3.3.6 Удаление профилей сбора

Для удаления профиля сбора нажмите кнопку  в соответствующей строке.

Для массового удаления профилей сбора установите нужные флаги и нажмите кнопку **Удалить**.

Для удаление всех профилей сбора нажмите кнопку **Удалить все**.

Чтобы все изменения вступили в силу перейдите в раздел **Источники → Агенты сбора**, выберите агенты сбора, на которых были выполнены изменения и нажмите кнопку **Опубликовать**.

3.4 Настройка сервиса Log-proxy

3.4.1 Описание

Log-proxy – сервис, который отвечает за быструю пересылку событий, пришедших от лог-коллектора в сервис **Kafka**.

Основные характеристики сервиса:

- используется только один порт для приема сообщений от всех лог-коллекторов (по умолчанию 1100);
- реализовано сжатие данных при передаче от лог-коллекторов.

Начиная с версии 3.7.2 **Платформы Радар** сервис **Log-proxy** используется в качестве замены сервиса **Rsyslog.**

При включенном сервисе все события от лог-коллектора будут заворачиваться в **websocket**, который работает по аналогии с компонентами отправки событий (секция output), но в один порт. События будут отправляться по указанному URL из включенных TCP/UDP компонентов отправки событий (секция senders). К нормализованным и разобранным событиям будет добавляться поле с соответствующим id, который задается в конфигурации сервиса **Log-proxy** через веб-интерфейс платформы (см. раздел «Включение пересылки событий через сервис Log-proxy»).

3.4.2 Включение пересылки событий через сервис Log-proxy

Если **Платформа Радар** работает в обычной инфраструктуре, то сервис **Log-proxy** включен по умолчанию и не требует дополнительных настроек.

Если **Платформа радар** работает в инфраструктуре мультитенант или мультиарендность, необходимо настроить пересылку событий из подчиненных инстансов.

Для включения пересылки событий через сервис **Log-proxy** выполните следующие действия:

1. В веб-интерфейсе платформы перейдите в раздел **Администрирование → Кластер →** вкладка **Управление конфигурацией**.
2. Проверьте настройки сервиса **Log-proxy**. Для этого в древовидном списке параметров сервисов выберите **Logproxy** (см. «Рис. 122»).

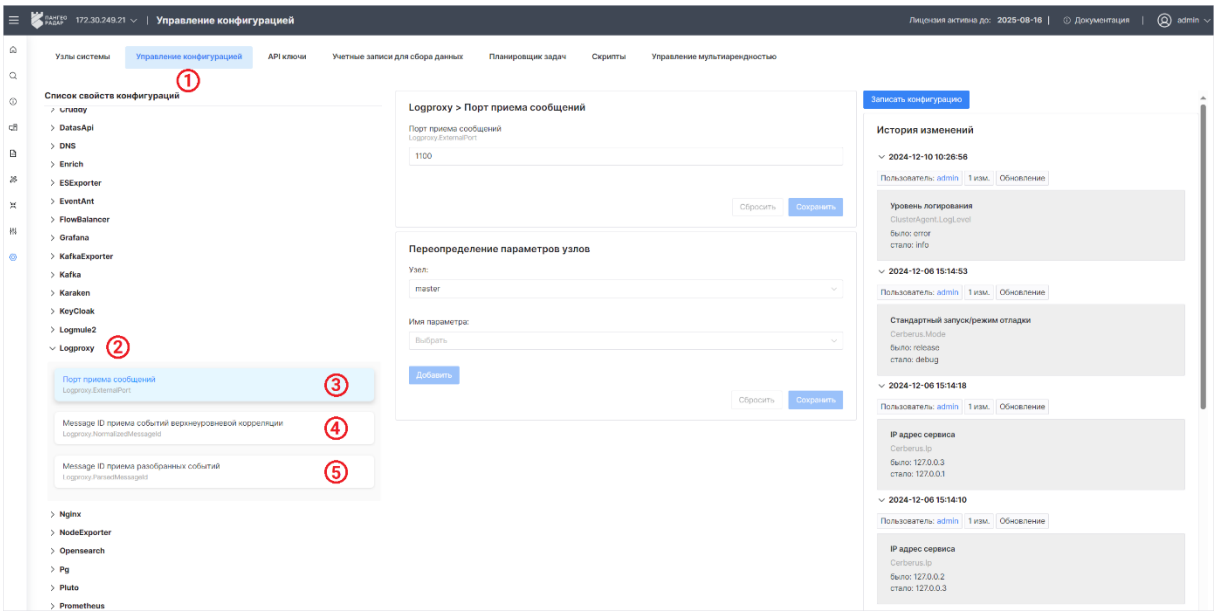


Рис. 122 – Управление конфигурацией сервиса Log-proxy

При необходимости переопределите следующие параметры:

- **Порт приема сообщений** – параметр определяет порт, который слушает сервис для приема сообщений от лог-коллектора. По умолчанию `1100`;
- **Message ID приема событий верхнеуровневой корреляции** – параметр определяет идентификатор (id) сообщения, которое отправляется в очередь нормализованных событий. По умолчанию `9999`;
- **Message ID приема разобранных событий** – параметр определяет идентификатор (id) сообщения, которое отправляется в очередь разобранных событий. По умолчанию `9998`.

3. Включите пересылку событий. Для этого в древовидном списке параметров сервисов выберите **FlowBalancer** → **Head** и установите параметр **Пересылать события** в значение `true` (см. «Рис. 123»).

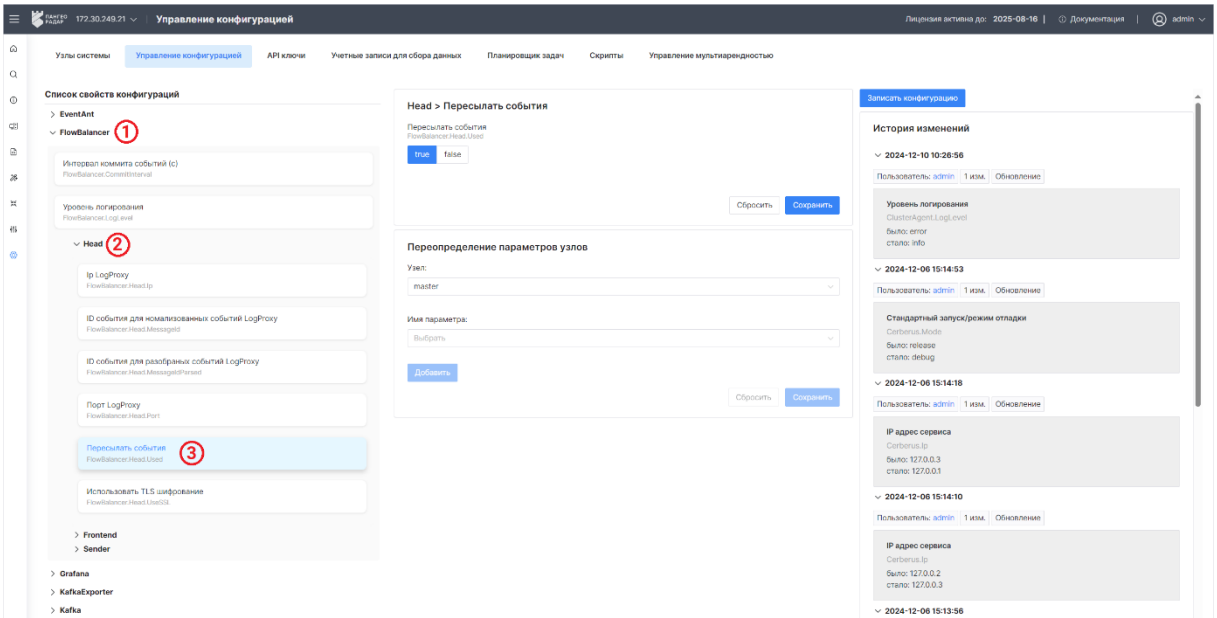


Рис. 123 – Управление конфигурацией сервиса FlowBalancer

При необходимости переопределите следующие параметры:

- **Ip LogProxy** – внешний IP-адрес сервиса **Log-proxy**;
- **Порт LogProxy** – внешний порт сервиса **Log-proxy**;
- **ID события для нормализованных событий LogProxy** – идентификатор (id) нормализованного события, пришедшего от сервиса (`Logproxy.NormalizedMessageId`);
- **ID события для разобранных событий LogProxy** – идентификатор (id) разобранного события, пришедшего от сервиса (`Logproxy.ParsedMessageId`).

4. После внесения изменений нажмите кнопку **Записать конфигурацию**.
5. В разделе **Коррелятор → Пересылка событий** создайте фильтры для пересылки событий.

   Внимание! Необходимо настроить фильтры для максимальной фильтрации событий. Чем больше событий будет отфильтровано, тем меньше будет нагрузка на устройство и тем больший поток сможет пройти.

3.4.3 Маршрутизация событий

Настройка выполняется в конфигурационном файле сервиса **Log-proxy** – `config.json`.

Расположение файла: `opt/pangeoradar/configs/logproxy/config.json`.

Необходимо переопределить параметры маршрутизации событий (секция router) следующим образом:

```
router:
    {"log_collector_id":
        {
        "name":"input_name",
        "template":"template_name",
        "broker":"URL KAFKA",
        "topic": "topic_name"
        }
    }
```

Где:

- `log_collector_id` – значение id от лог-коллектора;
- `name` – наименование источника событий;
- `template` – наименование шаблона для обработки сообщений;
- `broker` – IP-адрес и порт сервиса **Kafka**;
- `topic` – наименование топика, в который будет выполняться запись.

Для включения шаблона для обработки сообщений необходимо добавить секцию `templates`:

```
templates:
    {"template_name": "output_template"},
```

Где:

- `template_name` – наименование шаблона для обработки сообщений, которое указывается в параметрах секции `router`;
- `output_template` – результирующая строка, в которую надо подставить значения от лог-коллектора с соответствующим преобразованием. В параметре используются следующие переменные:
  - `%FROMHOST-IP%` – IP-адрес лог-коллектора, отправившего запрос;
  - `%timegenerated:::date-rfc3339%` – дата приема сообщения в формате `rfc3339`;
  - `%inputname%` – имя источника из секции `router`.

Примечание: в настройках шаблона доступен для ввода только тип данных `json` и соответствующее преобразование: `json-json`.

Пример настройки:

```
router:
    {"1519":
        {
        "name": "1514-Microsoft-Windows-Eventlog",
        "template": "json-json",
        "broker": "127.0.0.1:9092",
        "topic": "1514-Microsoft-Windows-Eventlog"
        }
    }

templates: {
    "json-json":"{\"rs_relay_ip\":\"%FROMHOST-
IP%\",\"rs_collector_ts\":\"%timegenerated:::date-
rfc3339%\",\"__rs_module\":\"%inputname%\",%rawmsg:2:$:%",
    }
```

3.4.4 Настройка журналирования сервиса Log-proxy

Уровень детализации ведения журналов работы сервиса **Log-proxy** (pangeoradar-logproxy.service) настраивается параметром `logLevel` при запуске сервиса. Возможные значения:

- 0 – журналирование отключено;
- 1 – выводить только информационные сообщения;
- 2 – выводить только предупреждения;
- 3 – выводить только критические ошибки;
- 4 – выводить информационные сообщения и предупреждения;
- 5 – выводить информационные сообщения и критические ошибки;
- 6 – выводить предупреждения и критические ошибки;
- 7 – выводить все сообщения.

Значение по умолчанию: 3 – выводить только критические ошибки.

Примечание: *аналогичные настройки журналирования используются в параметрах запуска сервиса* ***Termite***.

4. Подключение источников

4.1 Перечень поддерживаемых источников

Данный раздел содержит перечень систем, которые могут быть подключены к **Платформе Радар** в качестве источников событий

4.1.1 Операционные системы

Наименование	**Версия**
Alt Linux	10
Astra Linux	1.7.x, 1.8
CentOS Linux	6, 7, 8, 9
Debian Linux	8, 9, 10, 12
Fedora Linux	30, 31
FreeBSD	13.2, 14.0
IBM AIX	7.1, 7.2
Linux Auditd	
Microsoft Windows	XP, 7+
Microsoft Windows Event Forwarding	7+, 2008+
Microsoft Windows Server	2003, 2008+
Oracle Solaris	10, 11
Red Hat Enterprise Linux (RHEL)	6, 7, 8
SUSE Linux Enterprise	11.3, 12, 15
Ubuntu Linux	16.04+

4.1.2 Решения Network Security

Наименование	**Версия**
Barracuda Firewall	

Наименование	Версия
Bluecoat Proxysg	6, 7
CheckPoint Firewall-Netflow	
Checkpoint Firewall (NGFW)	77, 80
Checkpoint Firewall (opsec)	77, 80
Cisco ASA	
Cisco Firepower	
Fortinet FortiAnalyzer	
Fortinet Fortigate	5, 6
Fortinet FortiSandbox	
Fortinet FortiWeb	
HAProxy	2+
Ideco UTM-CEF	
Ideco UTM-Syslog	
Kaspersky Web Traffic Security	
Linux-Iptables	
Microsoft Forefront TMG	2010+
McAfee Web Gateway	
NGate CryptoPro VPNGate	
OpenVPN	
OPSEC LEA	
PaloAlto NGFW	7, 8
PfSense Firewall Netgate	
Radware DefencePro	
SecurityCode Continent	3.7, 3.9

Наименование	Версия
SecurityCode Continent IDS	
Snort	2.9+
Solar WebProxy	3.8.x
Squid Proxy	3.5+
Suricata	
Suricata IDS	
Teleport (Gravitational inc)	
Trend Micro TippingPoint	
Usergate UTM Firewall	6
VipNet Coordinator	3+, 4+
ViPNet IDS infotecs	
Wireguard EdgeSecurity	
Zabbix Monitoring	
Zeek (IDS Bro-ids)	

4.1.3 Решения System Security

Наименование	Версия
Confident Dallaslock	8.0-K
F5 BIG-IP	15
Kaspersky Anti Targeted Attack	
Kaspersky Secure Mail Gateway	2.x
Keycloack	
Papercut-NG	
Sysmon Windows	

Наименование	Версия
Бастион СКДПУ НТ	
Бастион СКДПУ НТ модуль UEBA	

4.1.4 Решения Endpoint Security

Наименование	Версия
DrWeb-Syslog	
DrWeb-Windows logs	
ESET Security Management Center	10.x
FireEye HX	
Kaspersky Security Center	10, 11
McAfee ePolicy Orchestrator	5.9, 5.10
Microsoft Windows AppLocker	
Microsoft Windows Defender	
Microsoft Windows Firewall	
PaloAlto Traps	
Symantec Endpoint Protection	14

4.1.5 Сетевые устройства

Наименование	Версия
Cisco Aironet	
Cisco ASR	
Cisco IOS Netflow	5, 9
Cisco IOS Switch	
Cisco IOS Router	
Cisco Nexus Switch	3064 (NS-OS 2.8.0)

Наименование	Версия
Cisco SG200 Switch	
D-link xStack	
Eltex Switch	
HP Switch	
Huawei Switch	
Infoblox Trinzic	
Keenetic Router	
MikroTik Router	Mikrotik-hEX-S, Mikrotik-hAP-ac2
Ubiquiti Switch	

4.1.6 Инфраструктурные системы

Наименование	Версия
ALD-pro	
Citrix ADC (Netscaler)	
CommuniGate	
Dell IDRAC	
FreeIpa	4.9.10+
FreeRADIUS	
Gitlab	
ISC Bind DNS	9
Linux NFS Server	
Microsoft DHCP	2008+
Microsoft Windows DNS	2008+
Microsoft Windows RDS-GW	

Наименование	Версия
OpenStack	
Simon Kelley DNSmasq	
Unbound_DNS	

4.1.7 Системы виртуализации

Наименование	Версия
KVM Hypervisor. Libvirt	4.1
Microsoft Windows HyperV	
Proxmox	
vGate	
VMware ESXi	
VMware vCenter	

4.1.8 Системы управления базами данных

Наименование	Версия
Microsoft SQL Server. Event Log	2014+
Microsoft SQL Server. ODBC	2014+
Oracle Database. Audit	
Oracle Database. NetListener	
Oracle MySQL	
PostgreSQL	9+

4.1.9 Web-серверы

Наименование	Версия
Apache HTTP Server	

Наименование	Версия
Apache HTTP Server. Windows	
Apache Tomcat	
Lighttpd	
Mantis Bug Tracker	
Microsoft IIS	
Microsoft Sharepoint	2019+
Nginx	

4.1.10 Системы контроля привилегированного доступа

Наименование	Версия
CyberArk PAM	
RSA SecurID	
SearchInform DLP	
Solar Dozor	7.9
SmartLine DeviceLock DLP	8x
Staffcop Enterprise	

4.1.11 Системы Enterprise Resource Planning (ERP)

Наименование	Версия
1C:Enterprise	

4.1.12 Системы электронной почты

Наименование	Версия
IBM Postfix	
Microsoft Exchange Server. Audit	2013/2016/2019

Наименование	Версия
Microsoft Exchange Server. Message Tracking	2013/2016/2019
Microsoft Exchange Server. OWA	2013/2016/2019
Microsoft Exchange Server. SMTP	2013/2016/2019
Zimbra	
МойОфис Почта	

4.1.13 Системы защиты электронной почты

Наименование	Версия
SEPPmail Secure Email	9

4.2 Операционные системы

4.2.1 Alt Linux

4.2.1.1 Описание

Платформа Радар поддерживает сбор событий с версии "Альт Рабочая станция 10.0" и выше.

Для журналирования событий используются следующие службы:

- `rsyslog` - служба журналирования для отправки событий в платформу;
- `auditd` - отвечает за запись сообщений аудита вызванных активностью приложений или системы.

Примечание: *по умолчанию управление журналами в ОС осуществляется службами systemd-journald и journalct.*

В целях организации безопасной передачи данных на агент сбора лог-коллектора по протоколу TCP, а также обеспечения возможности фильтрации сообщений по источникам и их содержимому предлагается установить пакет rsyslog (см. раздел «Настройка службы rsyslog»).

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Linux-Alt
Номер (Порт)	2692
Вендор	BaseAltSPO
Тип	Linux

Характеристика	Значение
Профиль сбора	«Модуль tcp_input»

Настройка источника включает в себя следующие процессы:

1. «Настройка службы rsyslog».
2. «Настройка службы auditd».
3. «Включение источника на платформе».

4.2.1.2 Настройка службы rsyslog

В файле `/etc/systemd/journald.conf` включите пересылку записи журналов в `syslog`:

Storage=none

`ForwardToSyslog=yes`

`Установите службу rsyslog:`

`# apt-get install rsyslog-classic`

В конфигурационном файле `/etc/rsyslog.d/00_common.conf` укажите адрес лог-коллектора, добавив следующую строку:

`auth,authpriv.* @@<IP-адрес агента сбора лог-коллектора>:port`

Где:

- `<ip-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

Чтобы служба `rsyslog` принимала и отправляла поток событий от службы `auditd`, необходимо создать файл `/etc/rsyslog.d/30-auditd.conf` и указать в нем следующие параметры:

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

input(type="imfile" File="/var/log/audit/audit.log"
    Severity="info"
    Facility="local6")

local6.*  @@<IP-адрес агента сбора лог-коллектора>:port
```

Где:

- `<ip-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

Перезапустите службу:

`# service rsyslogd restart`

4.2.1.3 Настройка службы auditd

Службы `auditd` и `audispd-plugins` установлены в системе по умолчанию.

Выполните настройку файла `/etc/audit/rules.d/extended.rules` в соответствии с рекомендациями раздела «Настройка правил расширенного аудита».

В конфигурационном файле `/etc/audit/plugins.d/syslog.conf` укажите следующие параметры:

```
active = yes
direction = out
path = /sbin/audisp-syslog
type = always
args = LOG_LOCAL6
format = string
```

Перезапустите службу.

4.2.1.4 Включение источника на платформе

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Linux-Alt**.

4.2.2 FreeBSD

4.2.2.1 Описание

Платформа Радар поддерживает сбор событий со следующих версий операционной системы:

- FreeBSD 14.0-RELEASE;
- FreeBSD 13.2-RELEASE.

Для журналирования событий используются следующие службы:

- `syslog-ng` - служба журналирования для отправки событий в платформу;
- `auditd` - отвечает за запись сообщений аудита вызванных активностью приложений или системы.

Примечание: *в стандартной конфигурации FreeBSD управление журналами осуществляется службой* `syslogd`*, которая поддерживает передачу данных исключительно по протоколу UDP*.

*Для обеспечения безопасной передачи журналов по протоколу **TCP**, а также реализации механизмов фильтрации событий по источникам и их содержимому, рекомендуется использовать пакет **syslog-ng***.

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	FreeBSD
Номер (Порт)	2722
Вендор	The-FreeBSD-Project
Тип	OS
Профиль сбора	«Модуль tcp_input»

Настройка источника включает в себя следующие процессы:

1. «Настройка службы syslog-ng».
2. «Настройка журналирования ZFS».
3. «Настройка службы auditd».
4. «Включение источника на платформе».

4.2.2.2 Настройка службы syslog-ng

Шаг 1. Установка и активация службы

Установите пакет `syslog-ng` и включите автозагрузку:

```
# pkg install syslog-ng
# sysrc syslog_ng_enable="YES"
```

Шаг 2. Базовая конфигурация

Пример полной конфигурации `syslog-ng (/usr/local/etc/syslog-ng.conf)`:

```
@version:4.8
@include "scl.conf"

# ============================================================
# Глобальные настройки
# ============================================================

options {
    chain_hostnames(off);
    flush_lines(0);
    threaded(yes);
};

# chain_hostnames - управляет записью имён хостов в логе (в текущем виде не будет
добавлять предыдущие имена хоста к сообщениям при пересылке события)
# flush_lines - Определяет, после скольких сообщений syslog-ng будет записывать
данные на диск.
# При необходимости выставить определенное значение (например 100) для сокращения
количества операций записи на диск
# threaded - управляет многопоточностью обработки сообщений


# ============================================================
# Источники
# ============================================================

# Системные источники:
source src { system(); udp(); internal(); file("/var/log/uucp/Log" follow_freq(1));
};

# Источник для сбора событий ZFS:

# source s_zfs_events {
#     file("/var/log/zfs_events.log"  # Читает логи из указанного файла
#          flags(no-multi-line, no-parse) # Отключает разбор многострочных сообщений
и парсинг формата
#          multi-line-mode(indented) # При наличии многострочных событий, объединяет
их по отступам
#          follow_freq(1)); # Управляет частотой проверки обновления файла (секунды)
```

```
# };


# ========================================================
# Назначения
# ========================================================

# Базовое унифицированное назначение для отправки событий в SIEM (тут требуется
указать данные для подключения к узлу с установленным лог-коллектором):

destination d_siem       { tcp("<ip адрес лог-коллектора>" port(<порт лог-
коллектора>) log_fifo_size(1000)); };

# Стандартные назначения для записи системных журналов:

# Основные destination (без изменений имен файлов)
destination d_messages   { file("/var/log/messages"); };   # Общие системные
сообщения
destination d_security   { file("/var/log/security"); };   # События безопасности
destination d_auth       { file("/var/log/auth.log"); };   # Аутентификация и
авторизация
# destination d_mail      { file("/var/log/maillog"); };    # Почтовый сервис
# destination d_lpd_errs  { file("/var/log/lpd-errs"); };   # Система печати LPD
destination d_xfer       { file("/var/log/xferlog"); };    # FTP-транзакции
destination d_cron       { file("/var/log/cron"); };       # Задачи планировщика
# destination d_debug     { file("/var/log/debug.log"); };  # Отладочная информация
destination d_slip       { file("/var/log/slip.log"); };   # SLIP-соединения
destination d_ppp        { file("/var/log/ppp.log"); };    # PPP-соединения
destination d_kern       { file("/var/log/kern.log"); };   # Сообщения ядра
destination d_firewall   { file("/var/log/firewall.log"); }; # Фаервол/фильтрация
пакетов
destination d_devd   { file("/var/log/devd.log"); }; # События демона devd

# ========================================================
# Фильтры
# ========================================================

# Фильтры по уровню важности:
filter f_emerg     { level(emerg); };         # 0: Emergency - система
неработоспособна
filter f_alert     { level(alert..emerg); };  # 1: Alert - требуется немедленное
действие
filter f_crit      { level(crit..emerg); };   # 2: Critical - критические состояния
filter f_err       { level(err..emerg); };    # 3: Error - ошибки приложений
filter f_warning   { level(warning..emerg); }; # 4: Warning - предупреждения
# filter f_notice    { level(notice..emerg); };  # 5: Notice - важные штатные события
# filter f_info      { level(info..emerg); };    # 6: Informational - информационные
сообщения
# filter f_debug     { level(debug..emerg); };   # 7: Debug - отладочная информация

# Фильтры по facility:
filter f_auth      { facility(auth); };       # Аутентификация
filter f_authpriv  { facility(authpriv); };   # Привилегированная авторизация
filter f_cron      { facility(cron); };       # Планировщик задач
filter f_kern      { facility(kern); };       # Ядро системы
filter f_ftp       { facility(ftp); };        # FTP-сервис
filter f_ppp { program("ppp"); };             # PPP-соединения (добавлен)
filter f_slip { program("slattach"); };       # SLIP-соединения
# filter f_daemon    { facility(daemon); };     # Фоновые демоны
# filter f_mail      { facility(mail); };       # Почтовый сервис
# filter f_security  { facility(security); };   # Сообщения безопасности (устаревшее)
# filter f_uucp      { facility(uucp); };       # UUCP
# filter f_news      { facility(news); };       # Сервер новостей
# filter f_local0    { facility(local0); };     # Локальные facility
```

```
# filter f_local1    { facility(local1); };
# filter f_local2    { facility(local2); };
# filter f_local3    { facility(local3); };
# filter f_local4    { facility(local4); };
# filter f_local5    { facility(local5); };
# filter f_local6    { facility(local6); };
# filter f_local7    { facility(local7); };

# Специальные фильтры:

filter f_firewall  { program("ipfw|pf|ipfilter"); }; # Фильтрация пакетов
filter f_devd { not (program("devd") and level(info)); };  # Исключение спама devd
# filter f_zfs_events { tags("zfs_events"); };               # ZFS события
(стандартный фильтр)

# Опциональный фильтр для devd (не производительный)
# filter f_devd_important {
#     program("devd") and (
#         match("usb|umass|da[0-9]|ugen|iface" value("MESSAGE"))  # USB, диски,
сетевые интерфейсы
#         or level(warning..emerg)  # Только предупреждения и выше
#     );
# };

# =========================================================
# Дополнительные действия
# =========================================================

# Перезапись program для событий zfs (необходимо корректной нормализации)
rewrite r_set_program { set("zfs_events", value("PROGRAM")); };

# Правила маршрутизации для отправки в SIEM:

# log { source(s_zfs_events); rewrite(r_set_program); destination(d_siem); }; # ZFS в
SIEM
log { source(src); filter(f_devd); destination(d_siem); };             # Системные
логи (без devd) в SIEM

# Запись основных системных событий в файл:

log { source(src); filter(f_devd); destination(d_devd); flags(final); }; # События
демона devd (управление устройствами)
log { source(src); destination(d_messages); };                          # Все
сообщения → /var/log/messages
log { source(src); filter(f_auth); destination(d_auth); };              #
Аутентификация → auth.log
log { source(src); filter(f_authpriv); destination(d_security); };      #
Привилегированные операции → security
log { source(src); filter(f_kern); destination(d_kern); };              # Ядро →
kern.log
log { source(src); filter(f_cron); destination(d_cron); };              # Cron-задачи
→ cron
log { source(src); filter(f_ftp); destination(d_xfer); };               # FTP →
xferlog
log { source(src); filter(f_firewall); destination(d_firewall); };      # Фаервол →
firewall.log
# log { source(src); filter(f_mail); destination(d_mail); };            # Почта →
maillog
# log { source(src); filter(f_debug); destination(d_debug); };          # Отладка →
debug.log


# Критические события (дублирование в отдельные файлы):
```

```
log { source(src); filter(f_emerg); destination(d_security); flags(final); };    # Emergency → security
log { source(src); filter(f_alert); destination(d_security); flags(final); };    # Alert → security
log { source(src); filter(f_crit); destination(d_security); flags(final); };     # Critical → security

# Сетевые подключения (PPP/SLIP):

log { source(src); filter(f_ppp); destination(d_ppp); };                 # PPP → ppp.log
log { source(src); filter(f_slip); destination(d_slip); };                  # SLIP → slip.log
```

Где:

- `src` - стандартный источник syslog (определен в конфигурационном файле по умолчанию;
- `d_siem` - назначение отправки на удаленный хост SIEM-платформы;
- `<ip-адрес лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `порт лог-коллектора` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
- `f_devd` - фильтр, который позволяет исключить частые сообщения от процесса `devd`;
- `log_fifo_size(1000)` - буферизация для предотвращения потери событий при сетевых сбоях.

Примечание: более подробное описание настройки `syslog-ng` приведено в разделе «Настройка syslog-ng».

Шаг 3. Настройка шифрования (опционально)

Для включения **Шифрования TLS** в базовой конфигурации замените параметр `tcp()` на `tls()` и укажите параметры сертификатов.

Шаг 4. Перезапуск службы

Для перезапуска службы `syslog-ng` выполните команду:

```
# service syslog-ng restart && pgrep syslog-ng
```

Проверьте подключение к агенту сбора лог-коллектора командой:

```
# nc -zv <ip адрес лог-коллектора> <порт лог-коллектора>
```

Шаг5. Проверка событий

Пример событий ОС FreeBSD записанных `syslog-ng`:

```
Aug 13 20:20:00 freebsd_content /usr/sbin/cron[1115]: (root) CMD (/usr/libexec/atrun)

Aug 13 20:20:55 freebsd_content syslog-ng[1049]: syslog-ng shutting down; version='4.8.1'

Aug 13 22:20:50 freebsd_content devd[460]: Processing event '!system=DEVFS subsystem=CDEV type=CREATE cdev=pts/2'
```

4.2.2.3 Настройка журналирования ZFS

1. Создайте файл для исполнения сервисного скрипта `/usr/local/etc/rc.d/zfs_events`.
2. Укажите в файле следующие параметры:

```
#!/bin/sh

# PROVIDE: zfs_events
# REQUIRE: DAEMON
# KEYWORD: shutdown

. /etc/rc.subr

name="zfs_events"
rcvar=zfs_events_enable

load_rc_config $name

: ${zfs_events_enable="NO"}
: ${zfs_events_output="/var/log/zfs_events.log"}

pidfile="/var/run/${name}.pid"
command="/sbin/zpool"
command_args="events -H -v -f"

start_cmd="zfs_events_start"
stop_cmd="zfs_events_stop"

zfs_events_start() {
    if [ -f "$pidfile" ] && kill -0 $(cat "$pidfile") 2>/dev/null; then
        echo "$name is already running."
        return 1
    fi
    echo "Starting $name..."
    /usr/sbin/daemon -p "$pidfile" /bin/sh -c "$command $command_args >
$zfs_events_output 2>&1" &
}

zfs_events_stop() {
    if [ -f "$pidfile" ] && kill -0 $(cat "$pidfile") 2>/dev/null; then
        echo "Stopping $name..."
        kill $(cat "$pidfile")
        rm -f "$pidfile"
    else
        echo "$name is not running."
    fi
}


run_rc_command "$1"
```

3. Определите рекомендуемые разрешения для необходимых файлов:

   Права и владелец основного файла скрипта:

```
# sudo chown root:wheel /usr/local/etc/rc.d/zfs_events  # Владелец: root,
группа: wheel
# sudo chmod 755 /usr/local/etc/rc.d/zfs_events         # Права: rwxr-xr-x
```

   Права для файла логов:

```
# sudo touch /var/log/zfs_events.log # файл лучше создать самостоятельно, чтобы
сразу выдать необходимые разрешения
```

```
# sudo chown root:wheel /var/log/zfs_events.log  # Владелец: root, группа:
wheel
# sudo chmod 640 /var/log/zfs_events.log         # Права: rw-r-----
```

Права для PID-файла:

```
# sudo touch /var/run/zfs_events.pid
# sudo chown root:wheel /var/run/zfs_events.pid  # Владелец: root, группа:
wheel
# sudo chmod 644 /var/run/zfs_events.pid         # Права: rw-r--r--
```

4. Настройте автозапуск при загрузке системы. Для этого в конфигурационный файл `/etc/rc.conf` добавьте параметр `zfs_events_enable="YES"`.

5. Запустите скрипт:

   ```
   # service zfs_events start
   ```

4.2.2.4 Настройка службы auditd

Шаг 1. Общая настройка

Включите и настройте автозапуск службы при загрузке системы:

- включите автозапуск службы в конфигурационном файле `/etc/rc.conf`:

  ```
  echo 'auditd_enable="YES"' >> /etc/rc.conf
  ```

- запустите службу в текущем сеансе:

  ```
  # service auditd start && pgrep auditd
  ```

Конфигурационные файлы `auditd` расположены в директории `/etc/security`:

```
audit_class     audit_control~     audit_user     audit_warn     auditdistd.conf~
audit_control   audit_event        audit_user~    auditdistd.conf
```

Примечание: изменения следует вносить в следующие конфигурационные файлы: `/etc/security/audit_control` (глобальные параметры аудита) и `/etc/security/audit_user` (параметры аудита для конкретных пользователей). Подробнее см. в руководстве auditd для FreeBSD.

Настройте конфигурационный файл `/etc/security/audit_control` следующим образом:

```
# Основные параметры системы аудита
dir:/var/audit           # Директория хранения журналов
dist:off                 # Отключение создания жестких ссылок
flags:lo,aa,ad,ap        # Классы аудируемых событий
minfree:5                # Минимальный процент свободного места
naflags:lo,aa            # Флаги для событий без атрибутов
policy:cnt,argv          # Политика обработки событий
filesz:2M                # Максимальный размер файла журнала
expire-after:10M         # Максимальный объем хранилища
```

Ключевые классы аудируемых событий:

- `lo`: события входа/выхода;
- `aa`: административные действия;
- `ad`: изменения прав доступа;
- `ap`: операции с атрибутами.

Полный список классов: FreeBSD Audit Documentation.

Настройте параметры аудита по пользователям в файле `/etc/security/audit_user`:

```
# Формат: пользователь:включаемые_классы:исключаемые_классы
root:lo,ad:no           # Аудит всех действий root
user:-fc,ad:+fw         # Для обычного пользователя:
                        # - исключить успешные операции с файлами (-fc)
                       # - включить неудачные попытки записи (+fw)
```

Работа с журналами аудита:

- просмотр журнала:

  ```
  # praudit -xl /var/audit/20231129122235.20231129122958
  ```

- мониторинг событий в реальном времени:

  ```
  # praudit -xl /dev/auditpipe
  ```

Примечание: *журналы хранятся в* `/var/audit`.

Шаг 2. Настройка интеграции с платформой

1. Создайте файл для исполнения сервисного скрипта `/usr/local/etc/rc.d/audit2syslog`.
2. Укажите в файле следующие параметры:

```
#!/bin/sh

# Скрипт запуска службы audit2syslog, которая перенаправляет логи аудита
FreeBSD
# из /dev/auditpipe через утилиту praudit в системный журнал (syslog).
# Используется в системе FreeBSD и интегрируется с rc-системой через rc.subr.

# Подключаем библиотеку rc.subr для использования стандартных функций
управления службой
. /etc/rc.subr

# Определение полных путей к утилитам, чтобы не зависеть от переменной PATH
pgrep_cmd="/usr/bin/pgrep"
kill_cmd="/bin/kill"
stat_cmd="/usr/bin/stat"
logger_cmd="/usr/bin/logger"

# Определение путей для служебных файлов
pidfile="/var/run/audit2syslog.pid"    # PID-файл процесса praudit
script_log="/var/log/audit2syslog.log" # Файл логов

# Функция запуска службы:
audit2syslog_start()
{
    # Проверяем, запущен ли auditd
    if ! ${pgrep_cmd} -x auditd > /dev/null 2>&1; then
        echo "$(date '+%F %T') audit2syslog: auditd не запущен" >>
"${script_log}"
        return 1  # Возвращаем ошибку, если auditd не включен
    fi

    # Проверяем наличие устройства /dev/auditpipe, из которого praudit читает
логи аудита
    if [ ! -e /dev/auditpipe ]; then
        echo "$(date '+%F %T') audit2syslog: /dev/auditpipe отсутствует" >>
"${script_log}"
```

```
        return 1  # Возвращаем ошибку, если устройство недоступно
    fi

    # Опционально! Проверяем права доступа к /dev/auditpipe (должны быть 600,
владелец root, группа wheel)
    mode=$(${stat_cmd} -f "%OLp" /dev/auditpipe)  # Права в числовом формате
    owner=$(${stat_cmd} -f "%Su" /dev/auditpipe)  # Владелец
    group=$(${stat_cmd} -f "%Sg" /dev/auditpipe)  # Группа
    if [ "${mode}" != "0600" ] && [ "${mode}" != "600" ] || [ "${owner}" !=
"root" ] || [ "${group}" != "wheel" ]; then
        echo "$(date '+%F %T') audit2syslog: неверные права на /dev/auditpipe
(${owner}:${group} ${mode})" >> "${script_log}"
        [ -t 0 ] && echo "audit2syslog: служба не запущена, неверные права на
/dev/auditpipe (${owner}:${group} ${mode})" # Вывод в stdout
        return 1  # Возвращаем ошибку, если права неверные
    fi

    # Проверяем, существует ли pidfile и запущен ли процесс связанный с PID
содержащемся в файле
    if [ -r "${pidfile}" ]; then
        PID=$(cat "${pidfile}")
        # Проверяем, существует ли процесс с указанным PID
        if kill -0 "${PID}" 2>/dev/null; then  # kill -0 проверяет процесс без
его завершения, ошибки подавляем
            echo "$(date '+%F %T') audit2syslog: служба не запущена повторно,
процесс уже работает (PID=${PID})" >> "${script_log}"
            [ -t 0 ] && echo "audit2syslog: служба не запущена повторно,
процесс уже работает (PID=${PID})" # Вывод в stdout
            return 0  # Упешно завершаем скрипт, так как служба уже работает
(чтобы не задублироваться)
        else
            # Удаляем устаревший pidfile, если процесс не существует
            echo "$(date '+%F %T') audit2syslog: устаревший pidfile найден
(PID=${PID}), удаляем" >> "${script_log}"
            [ -t 0 ] && echo "audit2syslog: устаревший pidfile найден
(PID=${PID}), удаляем" >&2 # Выводим в stderr
            rm -f "${pidfile}"  # Удаляем pidfile
        fi
    fi

    # Проверяем, запущен ли процесс praudit с /dev/auditpipe
    if PIDS=$(${pgrep_cmd} -f "${command} -xl /dev/auditpipe" 2>/dev/null);
then
        # Логируем, что процесс praudit уже работает, и выводим сообщение в
терминал, если скрипт запущен в интерактивном режиме
        echo "$(date '+%F %T') audit2syslog: служба не запущена повторно,
обнаружен процесс praudit с /dev/auditpipe (PID(s)=${PIDS})" >> "${script_log}"
        [ -t 0 ] && echo "audit2syslog: служба не запущена повторно, обнаружен
процесс praudit с /dev/auditpipe (PID(s)=${PIDS})"
        return 1  # Завершаем с ошибкой, чтобы исключить дублирование
    fi

    # Запускаем praudit в фоновом режиме для чтения логов из /dev/auditpipe и
перенаправления в syslog
    ${command} -xl /dev/auditpipe | ${logger_cmd} ${audit2syslog_flags} 2>>
"${script_log}" &
    # Сохраняем PID запущенного процесса в pidfile
    echo $! > "${pidfile}"
    # Логируем успешный запуск с указанием PID
    echo "$(date '+%F %T') audit2syslog: запущен praudit (PID=$(cat
"${pidfile}"))" >> "${script_log}"
    [ -t 0 ] && echo "audit2syslog: запущен praudit (PID=$(cat "${pidfile}"))"
>&2
}
```

```
# Функция остановки службы: завершает процесс praudit, связанный с этой службой
audit2syslog_stop()
{
    # Проверяем наличие pidfile, чтобы определить, какой процесс останавливать
    if [ -r "${pidfile}" ]; then
        PID=$(cat "${pidfile}")
        if kill -0 "${PID}" 2>/dev/null; then
            ${kill_cmd} -TERM "${PID}"
            sleep 1
            if kill -0 "${PID}" 2>/dev/null; then
                echo "$(date '+%F %T') audit2syslog: praudit не ответил на
TERM, посылаем KILL" >> "${script_log}"
                ${kill_cmd} -KILL "${PID}"
            fi
            echo "$(date '+%F %T') audit2syslog: остановлен praudit
(PID=${PID})" >> "${script_log}"
            [ -t 0 ] && echo "audit2syslog: остановлен praudit (PID=${PID})"
            rm -f "${pidfile}"
        else
            echo "$(date '+%F %T') audit2syslog: pidfile содержит некорректный
PID (${PID})" >> "${script_log}"
            [ -t 0 ] && echo "audit2syslog: pidfile содержит некорректный PID
(${PID})" >&2
        fi
    else
        if PIDS=$(${pgrep_cmd} -f "${command} -xl /dev/auditpipe" 2>/dev/null);
then
            echo "$(date '+%F %T') audit2syslog: невозможно корректно завершить
службу, pidfile отсутствует, но найден praudit с /dev/auditpipe
(PID(s)=${PIDS})" >> "${script_log}"
            [ -t 0 ] && echo "audit2syslog: невозможно корректно завершить
службу, pidfile отсутствует, но найден praudit с /dev/auditpipe
(PID(s)=${PIDS})" >&2
            return 1
        else
            echo "$(date '+%F %T') audit2syslog: pidfile не найден, процесс
praudit для /dev/auditpipe не запущен" >> "${script_log}"
            [ -t 0 ] && echo "audit2syslog: pidfile не найден, процесс praudit
для /dev/auditpipe не запущен" >&2
            return 1
        fi
    fi
}

# Определяем основные переменные для работы с rc.subr
name=audit2syslog                    # Имя службы, используется в /etc/rc.conf
rcvar=audit2syslog_enable            # Переменная в /etc/rc.conf для
включения/выключения службы
command=/usr/sbin/praudit            # Команда для чтения логов аудита
audit2syslog_flags="-t audit_trail"       # Флаги для logger, указывающие тег
сообщений в syslog

# Указываем функции для выполнения команд start и stop
start_cmd=${name}_start
stop_cmd=${name}_stop

# Загружаем конфигурацию службы из /etc/rc.conf (например, audit2syslog_enable,
audit2syslog_flags)
load_rc_config $name

# Выполнение команды, переданной скрипту (start, stop, restart и т.д.)
run_rc_command "$1"
```

3. Определите рекомендуемые права и владельца файла:

   Права для основного файла скрипта:

   ```
   chown root:wheel /usr/local/etc/rc.d/audit2syslog  # Владелец и группа
   chmod 755 /usr/local/etc/rc.d/audit2syslog         # Права: rwxr-xr-x
   ```

   Права для PID-файла и логов:

   ```
   touch /var/run/audit2syslog.pid /var/log/audit2syslog.log
   chown root:wheel /var/run/audit2syslog.pid /var/log/audit2syslog.log
   chmod 644 /var/run/audit2syslog.pid /var/log/audit2syslog.log  # rw-r--r--
   ```

   Права для `/dev/auditpipe`:

   ```
   chown root:wheel /dev/auditpipe
   chmod 600 /dev/auditpipe  # rw-------
   ```

4. Настройте автозапуск при загрузке системы. Для этого в конфигурационный файл `/etc/rc.conf` добавьте параметр `audit2syslog_enable="YES"`.

5. Запустите сервис:

   ```
   # service audit2syslog start
   ```

Шаг 3. Проверка событий

Пример событий auditd:

```
<?xml version='1.0' ?>
<audit>
<record version="11" event="getaudit_addr(2)" modifier="0" time="Wed Aug 13 19:26:45
2025" msec=" + 612 msec" ><subject audit-uid="testuser" uid="root" gid="testuser"
ruid="testuser" rgid="testuser" pid="1368" sid="1323" tid="0 0.0.0.0" /><return
errval="success" retval="0" /></record>
<record version="11" event="auditon(2)" modifier="0" time="Wed Aug 13 19:26:45 2025"
msec=" + 612 msec" ><argument arg-num="1" value="0x1d" desc="cmd" /><subject audit-
uid="testuser" uid="root" gid="testuser" ruid="testuser" rgid="testuser" pid="1368"
sid="1323" tid="0 0.0.0.0" /><return errval="success" retval="0" /></record>
<record version="11" event="su(1)" modifier="0" time="Wed Aug 13 19:26:45 2025"
msec=" + 612 msec" ><subject audit-uid="testuser" uid="root" gid="testuser"
ruid="testuser" rgid="testuser" pid="1368" sid="1368" tid="0 0.0.0.0"
/><text>successful authentication</text><return errval="success" retval="0"
/></record>
</audit>
```

4.2.2.5 Включение источника на платформе

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **FreeBSD**.

4.2.3 IBM AIX

Платформа Радар поддерживает сбор событий со следующих версий операционной системы:

- AIX 7.1;
- AIX 7.2;
- AIX 7.3.

Характеристики источника в **Платформе Радар**:

Характеристика	Значение

Характеристика	Значение
Название	IBM-AIX
Номер (Порт)	2641
Вендор	IBM
Тип	AIX
Профиль сбора	«Модуль udp_input»

Для настройки источника на отправку событий в **Платформу Радар** выполните следующие действия:

1. Подключитесь к вашему устройству под пользователем `root`.
2. Откройте файл `/etc/syslog.conf`.
3. Настройте отправку событий на агент сбора лог-коллектора: `auth.info @@<IP_address агента сбора лог-коллектора>`, где укажите соответствующий IP-адрес. Например:

```
#####
begin
/etc/syslog.conf
mail.debug
/var/adm/maillogmail.none
/var/adm/maillogauth.notice
/var/adm/authloglpr.debug
/var/adm/lpd-errskern.debug
/var/adm/messages*.emerg;*.alert;*.crit;*.warning;*.err;*.notice;*.info
/var/adm/messages  auth.info @@<IP_address агента сбора лог-коллектора>
#####
end
/etc/syslog.conf
```

4. Сохраните изменения.
5. Перезапустите службу `syslog` командой:

   ```
   # refresh -s syslogd
   ```

6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **IBM-AIX**.

4.2.4 UFW и firewalld

Для получения событий с межсетевого экрана `uncomplicated firewall` (UFW) или `firewalld` его необходимо подключить как отдельный источник.

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Uncomplicated-Firewall-UFW

Характеристика	Значение
Номер (Порт)	2673
Вендор	Linux
Тип	Firewall
Профиль сбора	«Модуль tcp_input»

Настройка источника включает в себя следующие процессы:

1. «Настройка firewalld».
2. «Настройка UFW».
3. «Включение источника на платформе».

4.2.4.1 Настройка firewalld

По умолчанию firewalld используется в следующих ОС:

- RHEL 7 и более новые версии;
- CentOS 7 и более новые версии;
- Fedora 18 и более новые версии;
- SUSE 15 и более новые версии;
- openSUSE 15 и более новые версии.

4.2.4.1.1 Настройка для rsyslog

Запустите сервис:

```
# service firewalld start
```

Выберите тип передачи данных:

```
# firewall-cmd --set-log-denied=all | unicast | broadcast | multicast
```

Где:

- `unicast` – процесс отправки пакета от одного хоста к другому хосту;
- `multicast` – процесс отправки пакета от одного хоста к некоторой ограниченной группе хостов;
- `broadcast` – процесс отправки пакета от одного хоста ко всем хостам в сети.

Перезапустите службу:

```
# service firewalld restart
```

Чтобы журналирование пакетов было в отдельном файле, создайте файл `/etc/rsyslog.d/10-fw_log.conf` и укажите следующее содержимое:

```
:msg,contains,"_DROP" /var/log/firewalld.log
:msg,contains,"_REJECT" /var/log/firewalld.log
& stop
```

Для отправки событий `firewalld` на агент сбора лог-коллектора, создайте файл `/etc/rsyslog.d/11-fw_lc.conf` и укажите следующее содержимое:

```
module(load="imfile" PollingInterval="5")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/firewalld.log"
      Tag="firewalld"
      ruleset="sendlc")
template(
    name = "logtemplate"
    type = "string"
    string = "<%PRI%> %msg%\n"
)
ruleset(name="sendlc")
{
    action(type = "omfwd"
        Template = "logtemplate"
        Target="<IP-адрес агент сбора лог-коллектора>"
        Port="<порт>"
        Protocol="tcp"
        ResendLastMSGOnReconnect="on"
        action.resumeRetryCount="100"
        queue.type="linkedList"
        queue.size="10000")
    stop
}
```

Где:

- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `<порт>` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

Перезапустите службу `rsyslog`:

```
# service rsyslog start
```

Откройте соответствующий порт:

```
# firewall-cmd --permanent --add-port=<номер порта>/tcp
```

4.2.4.1.2 Настройка для syslog-ng

Настроите перенаправление событий службы в файл `/var/log/firewalld`.

В директории `/etc/syslog-ng/conf.d` добавьте файл `firewalld_messages.conf` со следующими параметрами:

```
destination d_firewalld_net {
  tcp (
      "<IP-адрес агента сбора лог-коллектора>"
```

```
      port (<номер порта>)
      persist-name(d_firewalld_for_siem)
  );
};
destination d_firewalld_file {
    file(
      "/var/log/firewalld.log"
    );
};

filter f_firewalld {
    message("^.*_REJECT:.*$")
};

log {
    source(s_sys);
    filter(f_firewalld);
    destination(d_firewalld_file);
};
log {
    source(s_sys);
    filter(f_firewalld);
    destination(d_firewalld_net);
};
```

Где, укажите следующие параметры:

- В параметре `destination d_firewalld_net` укажите:
  - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
  - `<номер порта>` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.
- В параметре `destination d_firewalld_file` укажите следующий путь к файлу: `/var/log/firewalld.log`.

Для включения отправки журналов службой `firewalld` выполните команду:

```
# firewall-cmd --set-log-denied=all
```

Для завершения настройки необходимо перезапустить службу `firewalld` и `syslog-ng`.

4.2.4.2 Настройка UFW

4.2.4.2.1 Настройка rsyslog

Проверьте статус службы UFW:

```
# ufw status
```

Если не служба не запущена, то включите ее

ufw enable

Включите журналирование событий:

```
# ufw logging low | medium | high | full
```

Где:

- `low` — регистрирует все заблокированные пакеты, не соответствующие заданной политике (с ограничением скорости), а также пакеты, соответствующие зарегистрированным правилам;
- `medium` — все то, что при значении low, а также все разрешенные пакеты, не соответствующие заданной политике, все недопустимые пакеты, и все новые соединения. Все записи ведутся с ограничением скорости;
- `high` — работает также как и medium. Плюс все пакеты с ограничением скорости;
- `full` — также как и `high`, но без ограничения скорости.

Примечание: рекомендуется использовать уровень логирования medium.

Перезапустите службу:

```
# ufw reload
```

В конфигурационный файл `/etc/rsyslog.conf` добавьте строку, указав IP-адрес агента сбора лог-коллектора:

```
if $msg contains '[UFW ' then {
    action(type="omfwd" target="IP-адрес агента сбора лог-коллектора" port="номер порта" protocol="протокол")
    stop
}
```

Где:

- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `<номер порта>` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
- `<протокол>` - протокол (tcp или udp), по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

Перезапустите службу журналирования:

```
# systemctl restart rsyslog
```

Откройте соответствующий порт:

```
# ufw allow <номер порта>
```

4.2.4.2.2 Настройка syslog-ng

Перед настройкой службы `syslog-ng` задайте фильтр `f_ufw` в файле:

```
/etc/syslog-ng/conf.d/20-ufw.conf
```

Примечание: в ОС Astra Linux фильтр создан по умолчанию.

Содержимое файла:

```
filter f_ufw {
    message("^.*UFW.*$")
```

```
};

destination d_ufw {
    file("/var/log/ufw.log");
};

log {
    source(s_src);
    filter(f_ufw);
    destination(d_ufw);
};
```

Для настройки службы `syslog-ng` добавьте в конфигурационный файл службы `/usr/local/etc/syslog-ng.conf` следующие параметры:

В блоке `Destinations` укажите пути для отправки сообщений в агент сбора лог-коллектора:

```
# Send the messages to an other host
#
destination d_net { tcp("<ip агента сбора лог-коллектора>" port(<номер порта>)
log_fifo_size(1000)); };

destination d_ufw_net { tcp("<ip агента сбора лог-коллектора, на котором подключен
ufw как источник>" port(<номер порта>) log_fifo_size(1000)); };
```

Где, укажите следующие параметры:

- В параметре `destination d_net` укажите:
    - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора, на котором подключена «ОС семейства Unix» как источник;
    - `<номер порта>` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.
- В параметре `destination d_ufw_net` укажите:
    - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора, на котором подключен UFW как источник;
    - `<номер порта>` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

В блоке `Log path` настройте фильтр для журналов от UFW:

```
log { source(s_src);
        if {
                filter(f_ufw);
                destination(d_ufw_net);
        } else {
                destination(d_net);
        };
};
```

Проверьте настройки UFW, выполнив следующие команды:

```
# sudo ufw enable
# sudo ufw logging on
# sudo ufw logging low | medium | high | full
```

Перезапустите службу `syslog-ng`:

```
# sudo service syslod-ng restart
```

4.2.4.3 Включение источника на платформе

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Uncomplicated-Firewall-UFW**.

4.2.5 Windows

Платформа Радар поддерживает сбор событий со следующих версий Windows:

- версии для персональных компьютеров:
  - Windows XP;
  - Windows 7;
  - Windows 8, 8.1;
  - Windows 10;
  - Windows 11.
- серверные версии:
  - Windows Server 2008;
  - Windows Server 2012;
  - Windows Server 2016;
  - Windows Server 2019;
  - Windows Server 2022.

Для журналирования событий используются следующие сервисы:

- **Windows Eventlog** - журнал событий Windows 7 и последующих версий;
- **Windows XP Eventlog** - журнал событий Windows XP;
- **Windows Event Collector (WEC)** - сервер, который на основании создаваемых подписок на события получает события от источников и обеспечивает их локальное хранение.

4.2.5.1 Настройка источника Windows Eventlog

Характеристики источника **Windows Eventlog** в **Платформе Радар**:

Характеристика	Значение

Характеристика	Значение
Название	Microsoft-Windows-Eventlog
Номер (Порт)	1514
Вендор	Microsoft
Тип	Eventlog
Профиль сбора	«Модуль eventlog_input_local» «Модуль eventlog_input_remote»

Характеристики источника **Windows XP Eventlog** в **Платформе Радар**:

Характеристика	Значение
Название	Microsoft-Windows-XP
Номер (Порт)	1523
Вендор	Microsoft
Тип	XP
Профиль сбора	«Модуль eventlog_input_local» «Модуль eventlog_input_remote»

Настройка источника включает в себя следующие процессы:

1. «Создание учетной записи для сбора событий».
2. «Предоставление пользователю прав доступа к журналу событий».
3. «Настройка расширенных политик аудита Windows».
4. «Включение источника на платформе».

4.2.5.1.1 Создание учетной записи для сбора событий

Создание учетной записи для сбора событий имеет следующие особенности:

- если источник находится в домене, то на контроллере домена необходимо создать учетную запись и предоставить ей права доступа к журналу событий;
- если источник не находится в домене, то необходимо создать локальную учетную запись с аналогичным набором прав.

Для создания учетной записи выполните следующие действия:

1. В панели управления Windows откройте консоль **Управление компьютером**.
2. Перейдите в раздел: **Служебные программы → Local Users and Groups (Локальные пользователи и группы) → Users (Пользователи)**.
3. Вызовите контекстное меню и выберите пункт **New User (Новый пользователь)**. Откроется окно "New User (Новый пользователь)" (см. «Рис. 124»).

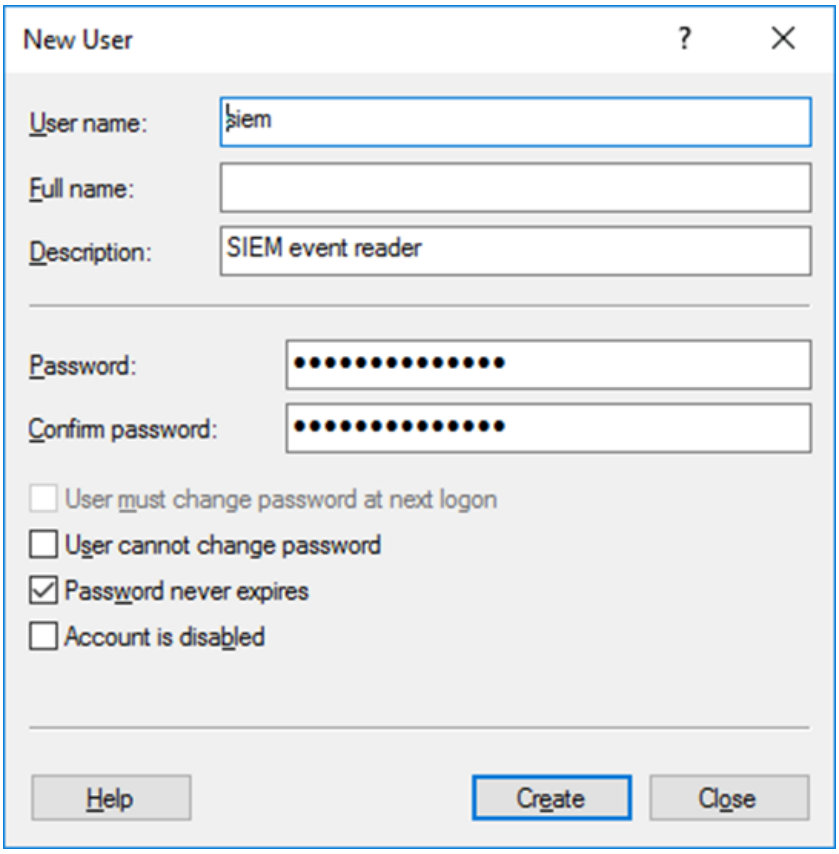


Рис. 124 -- Окно "New User (Новый пользователь)"

4. Укажите следующие данные:
    - в поле Name укажите имя нового пользователя;
    - в полях Password и Confirm Password укажите пароль;
    - если вы не хотите, чтобы пользователь мог изменить пароль, то установите соответствующий флаг;
    - для включения неограниченного срока действия пароля установите соответствующий флаг
5. Нажмите кнопку **Создать**. Откроется страница с отчетом.

4.2.5.1.2 Предоставление пользователю прав доступа к журналу событий

Для предоставления пользователю прав доступа к журналу событий, его необходимо добавить в группу Event Log Readers.

Для добавления пользователя в группу Event Log Readers (с правом доступа к журналам событий) необходимо выполнить следующие действия:

1. В консоли Computer Management (Управление компьютером) открыть раздел:

    System Tools (Служебные программы) → Local Users and Groups (Локальные пользователи и группы) → Groups (Группы)
2. Выбрать в списке группу Event Log Readers (Читатели журнала событий) (см. «Рис. 125»).

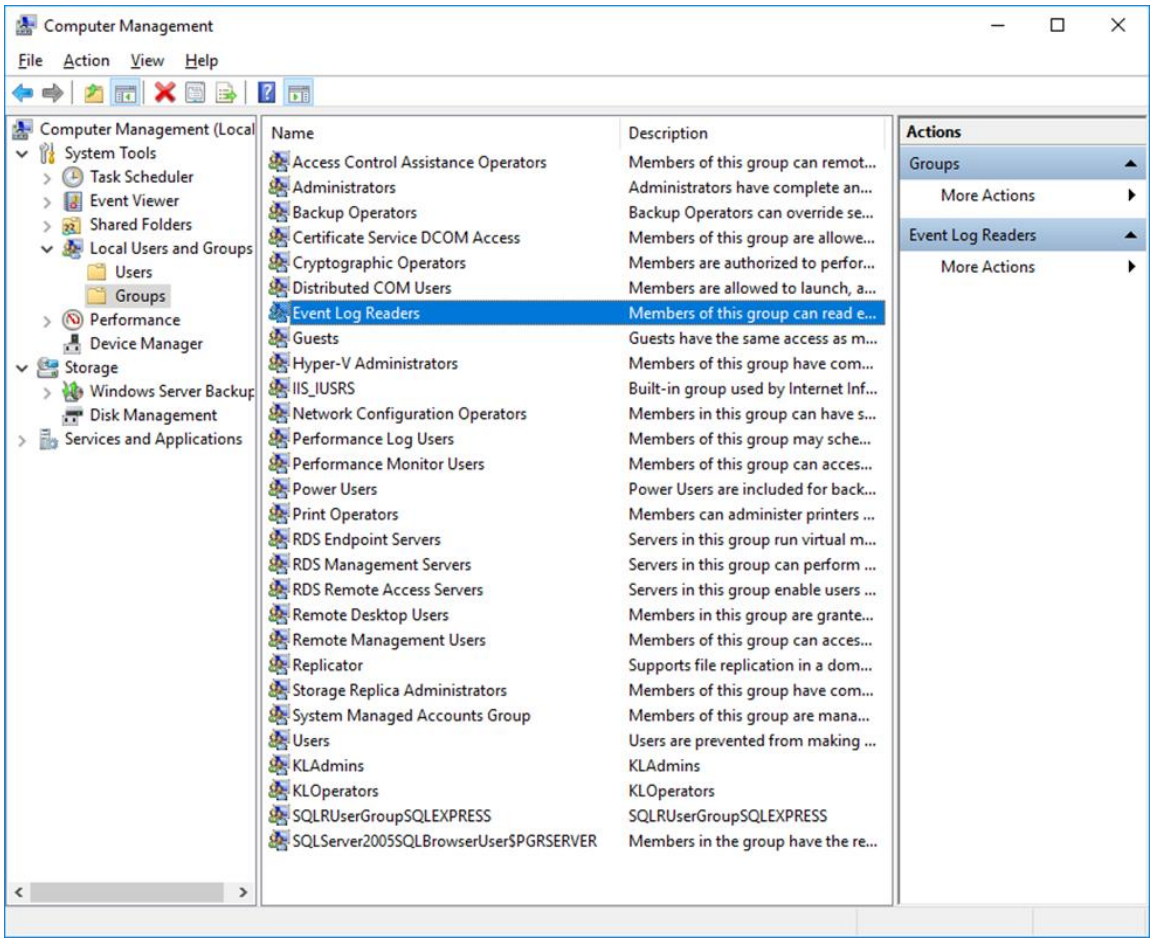


Рис. 125 -- Выбор группы Event Log Readers для включения учетной записи.

3. Открыть правой кнопкой мыши контекстное меню группы Event Log Readers (Читатели журнала событий) и выбрать пункт Add To Group (Добавить в группу). Откроется окно Event Log Readers Properties (Свойства: Читатели журнала событий) (см. «Рис. 126»).
4. Для добавления пользователя в группу:
   - Нажать кнопку Add (Добавить).
   - В открывшемся окне Select Users (Выбор: Пользователи) выбрать в списке пользователя, созданного ранее, и добавить его в группу, нажав кнопку OK.
5. Для сохранения введенных настроек в окне Event Log Readers Properties (Свойства: Читатели журнала событий) нажать кнопку OK (см. «Рис. 126»).

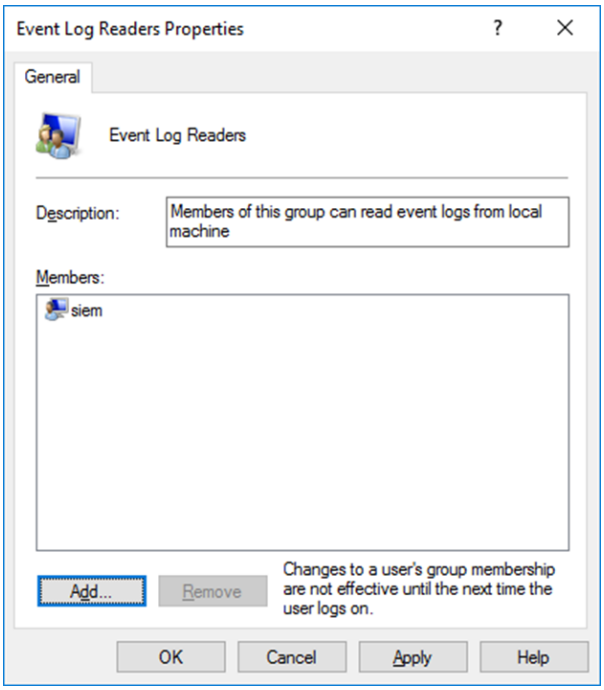


Рис. 126 -- Добавление пользователя в группу Event Log Readers.

Внесенные изменения вступают в действие при следующем входе нового пользователя в систему.

4.2.5.1.3 Настройка расширенных политик аудита Windows

Для настройки политик аудита на контроллерах домена используются групповые политики домена.

В групповой политике, применяемой для контроллеров домена, включите политику использования расширенной конфигурации политики аудита «Audit: Force audit policy subcategory settings (Windows Vista or later) (Аудит: принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (Windows Visa или следующие версии))».

Данную политику необходимо включить в разделе «Computer Configuration (Конфигурация компьютера)» → «Windows Settings (Конфигурация Windows)» → «Security Settings (Параметры безопасности)» → «Local Policies (Локальные политики)» → «Security Options (Параметры безопасности)» (см. «Рис. 127»).

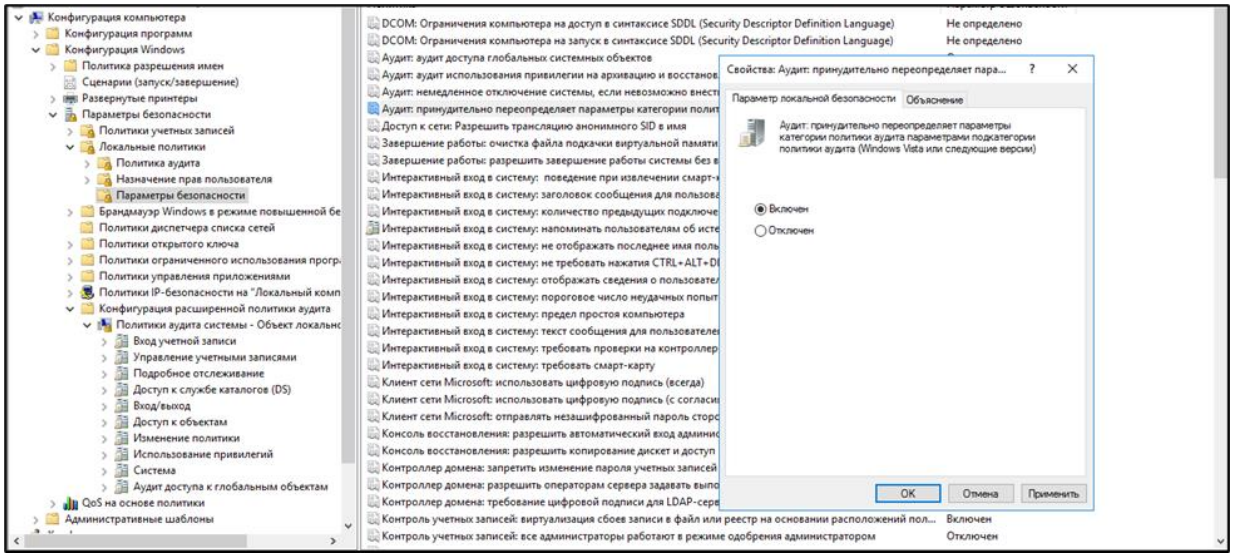


Рис. 127 -- Добавление Audit: Force audit policy subcategory settings

Для активации аудита для контроллеров домена необходимо настроить групповую политику, которая распространяется на контейнер, содержащий DC (Контроллеры домена), в соответствии с таблицей 1. (см. «Рис. 128»).

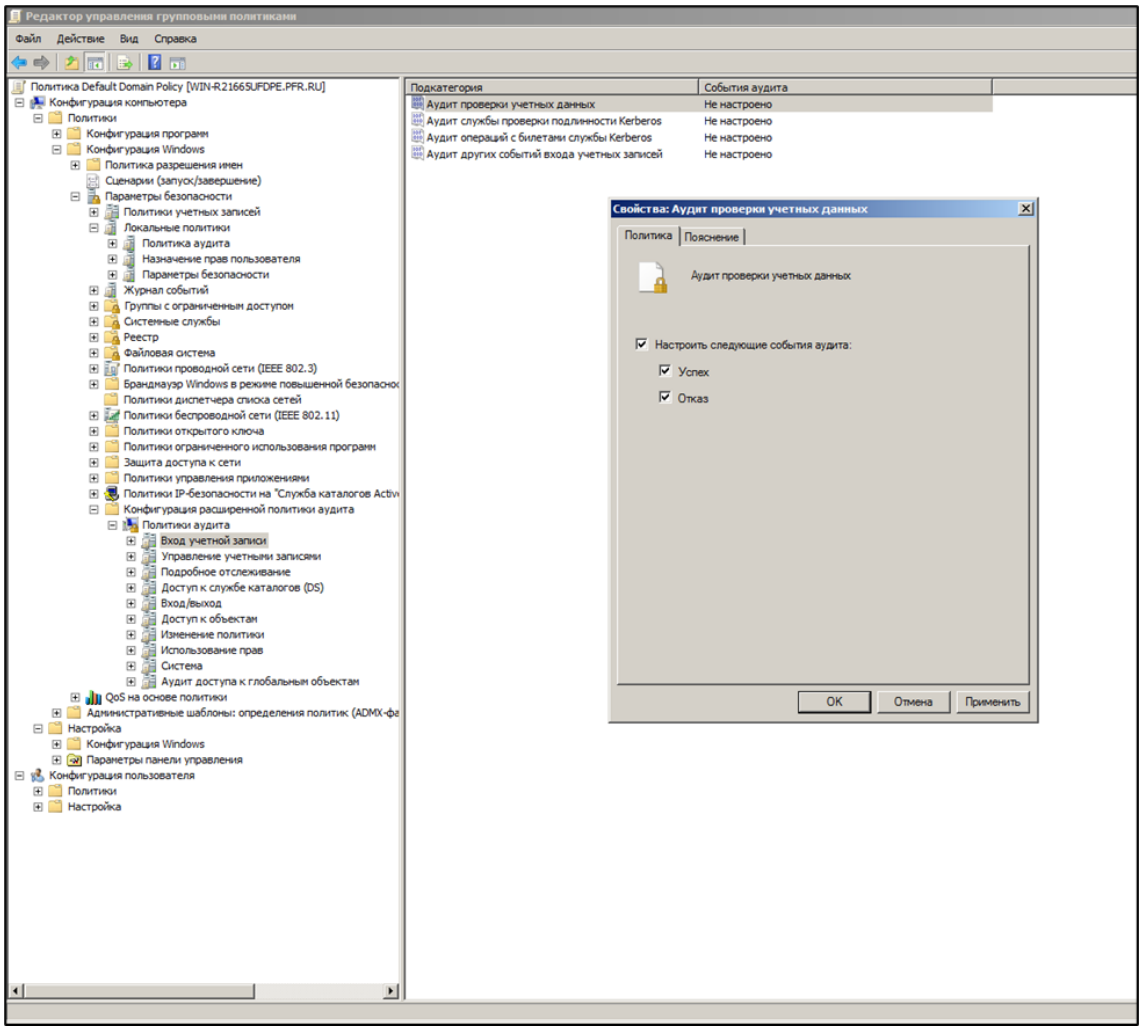


Рис. 128 -- Изменение политик аудита.

Таблица 1 -- Политики аудита ОС Windows 2008/2012

Политика аудита	**Тип событий**
Аудит проверки учетных данных (Account Logon → Audit Credential Validation)	Успех и Отказ
Аудит службы проверки подлинности Kerberos (Account Logon → Audit Kerberos Authentication Service)	Успех и Отказ
Аудит операций с билетами службы Kerberos (Account Logon → Audit Kerberos Service Ticket Operations)	Успех и Отказ
Аудит других событий входа учетных записей (Account Logon → Audit Other Account Logon Events)	Успех и Отказ
Аудит управления группами приложений (Account Management → Audit Application Group Management)	Успех и Отказ
Аудит управления учетными записями компьютеров (Account Management → Audit Computer Account Management)	Успех и Отказ
Аудит управления группами распространения (Account Management → Audit Distribution Group Management)	Успех и Отказ

Политика аудита	Тип событий
Аудит других событий управления учетными записями (Account Management → Audit Other Account Management Events)	Успех и Отказ
Аудит управления группами безопасности (Account Management → Audit Security Group Management)	Успех и Отказ
Аудит управления учетными записями (Account Management → Audit User Account Management)	Успех и Отказ
Аудит активности DPAPI (Detailed Tracking → Audit DPAPI Activity)	Не фиксируются
Аудит создания процессов (Detailed Tracking → Audit Process Creation)	Успех и Отказ
Включать командную строку в события создания процессов (Computer Configuration → Administrative Templates → System → Audit Process Creation → Include command line in process creation events)	Включено
Аудит завершения процессов (Detailed Tracking → Audit Process Termination)	Успех и Отказ
Аудит событий RPC (Detailed Tracking → Audit RPC Events)	Не фиксируются
Аудит подробной репликации службы каталогов (DS Access → Audit Detailed Directory Service Replication)	Не фиксируются
Аудит доступа к службе каталогов (DS Access → Audit Directory Service Access)	Успех и Отказ
Аудит изменения службы каталогов (DS Access → Audit Directory Service Changes)	Успех и Отказ
Аудит репликации службы каталогов (DS Access → Audit Directory Service Replication)	Не фиксируются
Аудит блокировки учетных записей (Logon/Logoff → Audit Account Lockout)	Успех и Отказ
Аудит расширенного режима IPsec (Logon/Logoff → Audit IPsec Extended Mode)	Не фиксируются
Аудит основного режима IPsec (Logon/Logoff → Audit IPsec Main Mode)	Не фиксируются
Аудит быстрого режима IPsec (Logon/Logoff → Audit IPsec Quick Mode)	Не фиксируются
Аудит выхода из системы (Logon/Logoff → Audit Logoff)	Успех
Аудит входа в систему (Logon/Logoff → Audit Logon)	Успех и Отказ
Аудит сервера политики сети (Logon/Logoff → Audit Network Policy Server)	Не фиксируются
Аудит других событий входа/выхода (Logon/Logoff → Audit Other Logon/Logoff Events)	Успех и Отказ
Аудит специального входа (Logon/Logoff → Audit Special Logon)	Успех и Отказ
Аудит событий, создаваемых приложениями (Object Access → Audit Application Generated)	Не фиксируются
Аудит сведений об общем файловом ресурсе (Object Access → Audit Detailed File Share)	Не фиксируются

Политика аудита	Тип событий
Аудит общего файлового ресурса (Object Access→ Audit File Share)	Успех и Отказ
Аудит файловой системы (Object Access→ Audit File System)	Успех и Отказ
Аудит подключения фильтрации (Object Access→ Audit Filtering Platform Connection)	Не фиксируются
Аудит отбрасывания пакетов фильтрации (Object Access→ Audit Filtering Platform Packet Drop)	Не фиксируются
Аудит работы с дискрипторами(Object Access→ Audit Handle Manipulation)	Не фиксируются
Аудит объектов ядра (Object Access→ Audit Kernel Object)	Не фиксируются
Аудит других событий доступа к объектам(Object Access→ Audit Other Object Access Events)	Не фиксируются
Аудит реестра (Object Access → Audit Registry)	Успех и Отказ
Аудит диспетчера учетных записей безопасности (Object Access → Audit SAM)	Не фиксируются
Аудит изменения политики аудита (Policy Change→ Audit Policy Change)	Успех и отказ
Аудит изменения политики проверки подлинности (Policy Change→Audit Audit Authorization Policy Change)	Успех и Отказ
Аудит изменения политики авторизации (Policy Change→Audit Authorization Policy Change)	Успех и Отказ
Аудит изменения политики фильтрации (Policy Change→Audit Filtering Platform Policy Change)	Не фиксируются
Аудит изменения политики на уровне правил MPSSVC (Policy Change→Audit MPSSVC Rule-Level Policy Change)	Успех и Отказ
Аудит других событий изменения политики (Policy Change→Audit Other Policy Change Events)	Успех и Отказ
Аудит использования привилегий, затрагивающих конфиденциальные данные (Privilege Use→Audit Sensitive Privilege Use)	Успех и Отказ
Аудит использования привилегий, не затрагивающих конфиденциальные данные (Privilege Use→Audit Non-Sensitive Privilege Use)	Успех и Отказ
Аудит драйвера IPsec (System→Audit IPsec Driver)	Не фиксируются
Аудит других системных событий (System→Audit Other System Events)	Не фиксируются
Аудит изменения состояния безопасности (System→Audit Security State Change)	Успех и Отказ
Аудит расширения системы безопасности (System→Audit Security System Extension)	Успех и Отказ
Аудит целостности системы (System→Audit System Integrity)	Успех и Отказ

4.2.5.1.4 Включение источника на платформе

Перейдите в веб-интерфейс платформы и выполните следующие действия:

1. Перейдите в раздел **Источники → Источники**.
2. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Windows-Eventlog** или **Microsoft-Windows-XP**.

4.2.5.2 Настройка источника WEC

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Microsoft-Windows-WEC
Номер (Порт)	1524
Вендор	Microsoft
Тип	WEC
Профиль сбора	«Модуль eventlog_input_local» «Модуль eventlog_input_remote»

В зависимости от конфигурации сети настройка источника выполняется одним из следующих способов:

- «Настройка WEC вне домена»;
- «Настройка WEC в домене с использованием групповых политик».

4.2.5.2.1 Настройка WEC вне домена

Настройка пересылки событий, инициированной сборщиком

Перед настройкой необходимо:

- разрешить между источником и сборщиком сетевое взаимодействие по портам 5985/TCP и 5986/TCP;
- на источнике добавить «Network Service» и используемого пользователя в «Local Computer Policy/Computer Configuration/Windows Settings/Security Settings/Local Policy/User Rights Assignment/Manage auditing and security log»;

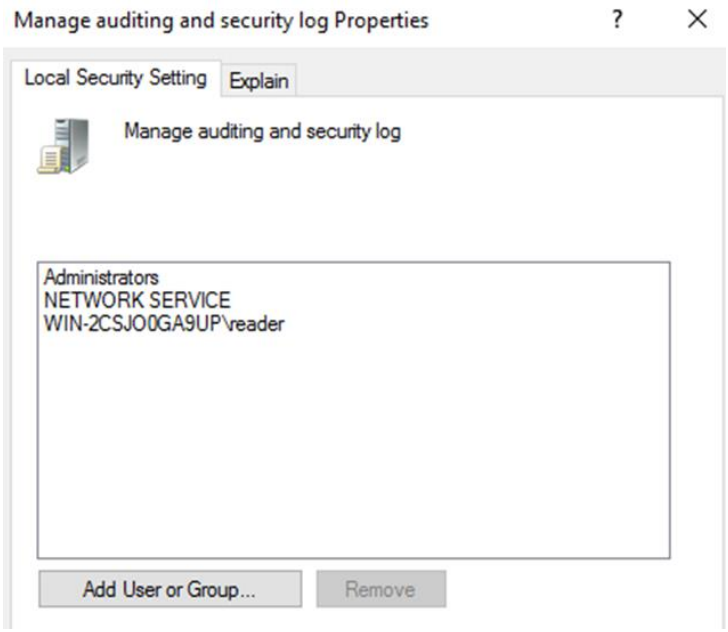


Рис. 129 – Добавление Network Service

- выключить на источнике и сборщике проверку подлинности NTLM в «Local Computer Policy/Computer Configuration/Windows Settings/Security Settings/Local Policy/Security Option»(опционально);
- на источнике добавить «Network Service» и используемого пользователя в группу «Event Log Readers»;
- установить последние обновления для операционной системы и перезагрузить (исправляют известные проблемы с WinRM и .Net).

Настройка источника событий:

1. Открыть командную строку с правами администратора системы и в ней последовательно выполнить следующие команды:

```
winrm qc –q
wecutil qc /q
winrm set winrm/config/client @{TrustedHosts="ip_адрес_сборщика"}
```

2. Создать учетную запись и добавить ее в группу «Читатели журнала событий».

Настройка сборщика событий:

1. Открыть командную строку с правами администратора системы и в ней последовательно выполнить следующие команды:

```
winrm qc –q
wecutil qc /q
winrm set winrm/config/client @{TrustedHosts="ip_адрес_источника"}
```

2. Зайти в «Просмотр событий» и создать подписку:
    - Нажать правой кнопкой по пункту «Подписки» и выбрать «Создать подписку».

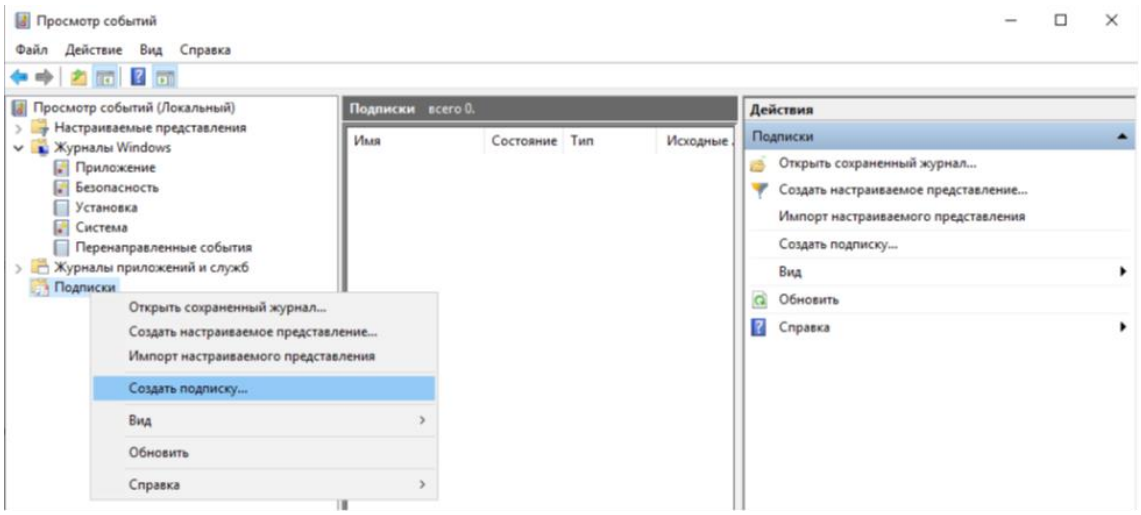


Рис. 130 – Просмотр событий. Создание подписки

- В открывшемся окне ввести имя подписки, выбрать конечный журнал для получаемых событий и тип подписки «Инициировано сборщиком» и нажать «Выбрать компьютеры».

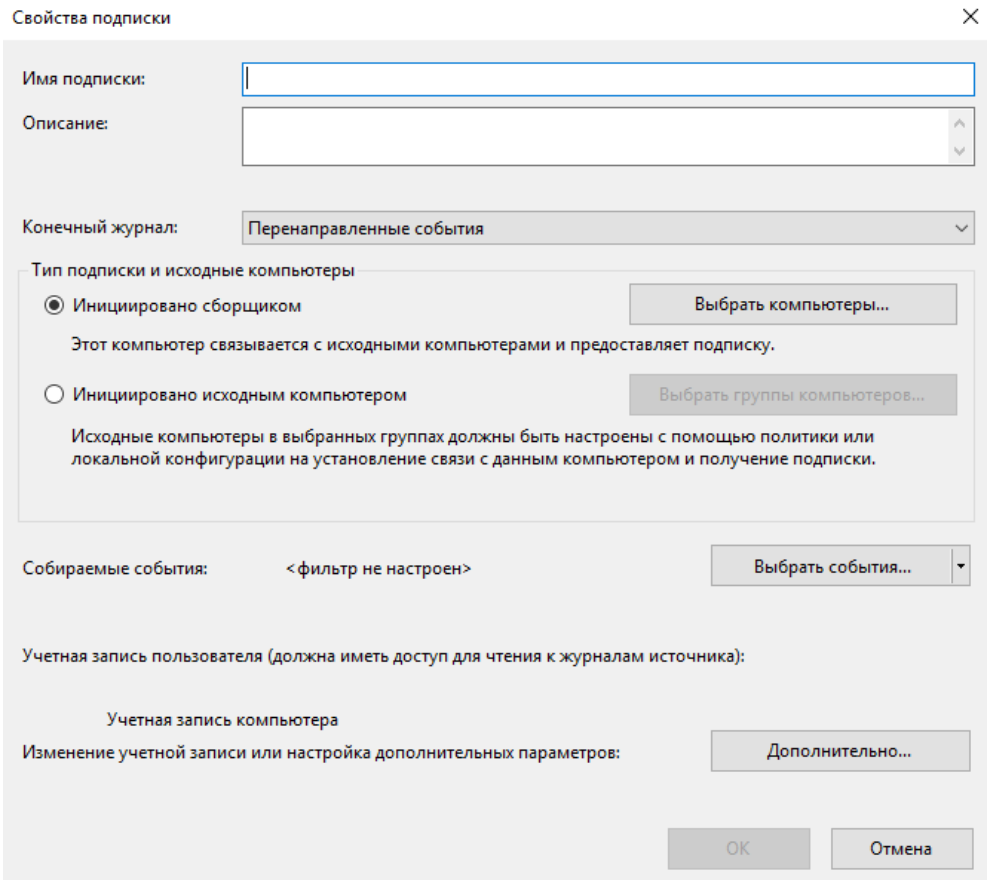


Рис. 131 – Свойства подписки

- Нажать «Добавить доменный компьютер».

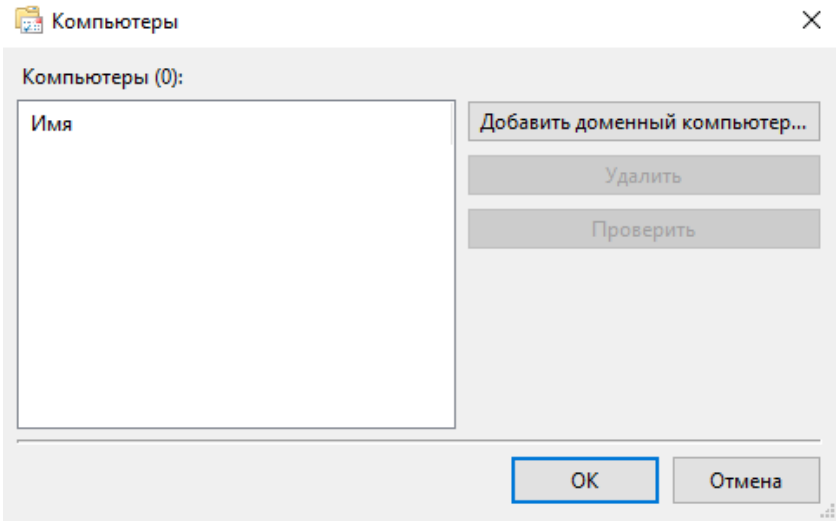


Рис. 132 – Добавление комментария

- Ввести IP-адрес или DNS-имя источника и нажать «OK».

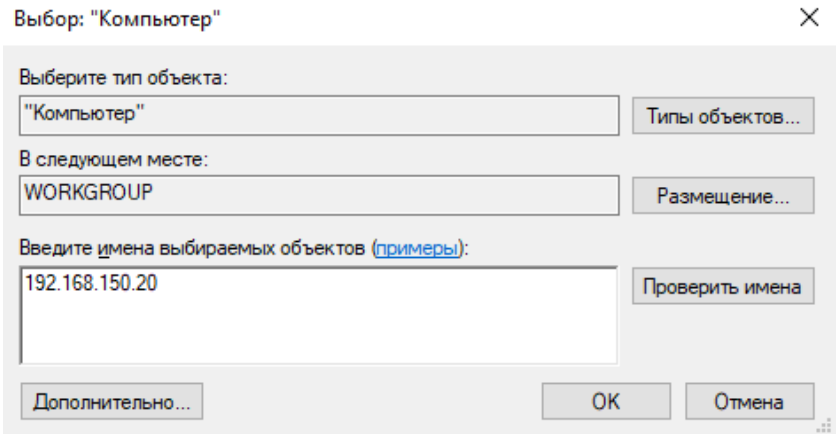


Рис. 133 – Заполнение сведений об IP-адресе или DNS источника

- Нажать «Выбрать события», настроить фильтр для запроса необходимых событий и нажать «OK».

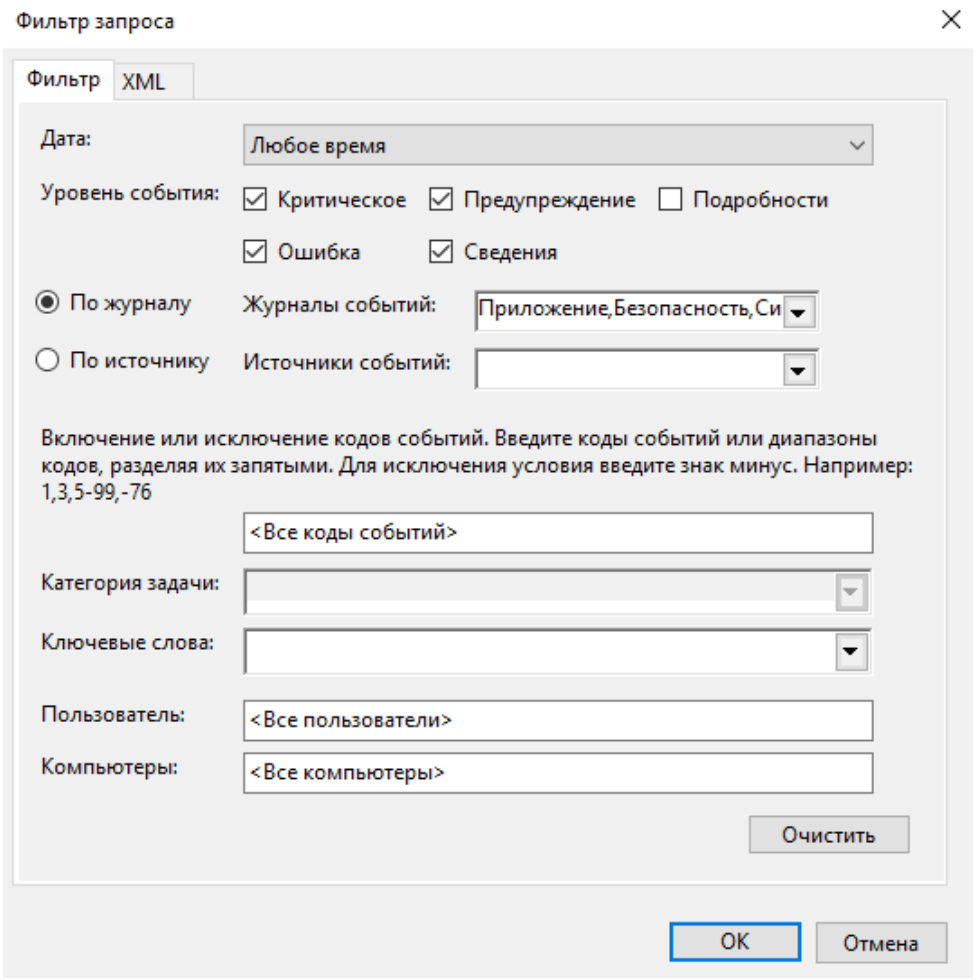


Рис. 134 – Фильтр запроса

- Нажать «Дополнительно» и выбрать «Определенный пользователь», остальные параметры оставить по умолчанию.

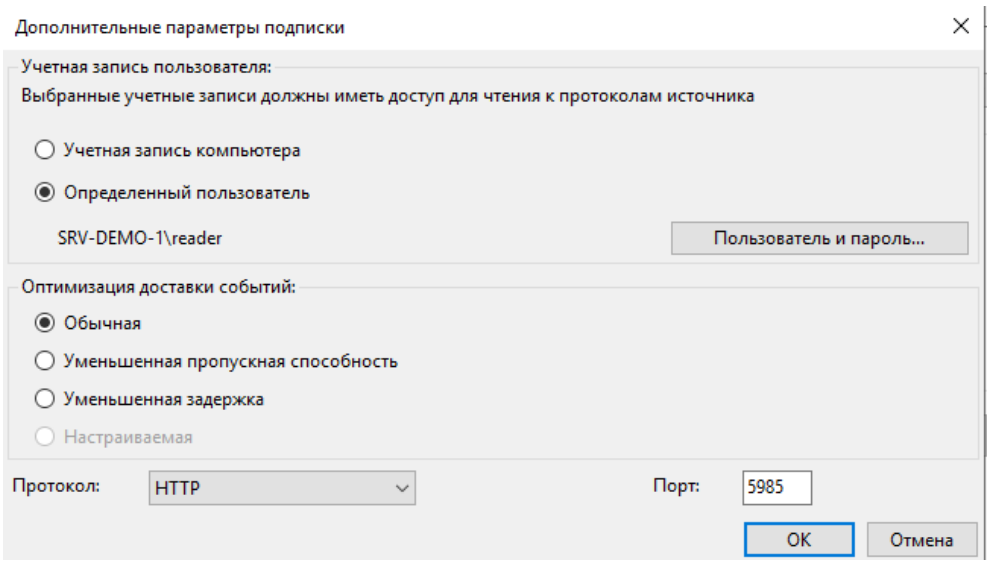


Рис. 135 – Дополнительные параметры подписки

3. Нажать «Пользователь и пароль», внести учетные данные пользователя, созданного на сервере-источнике событий, и затем сохранить изменения.

4. После создания подписки проверить её статус, нажав по ней правой кнопкой и выбрав «Состояние выполнения».

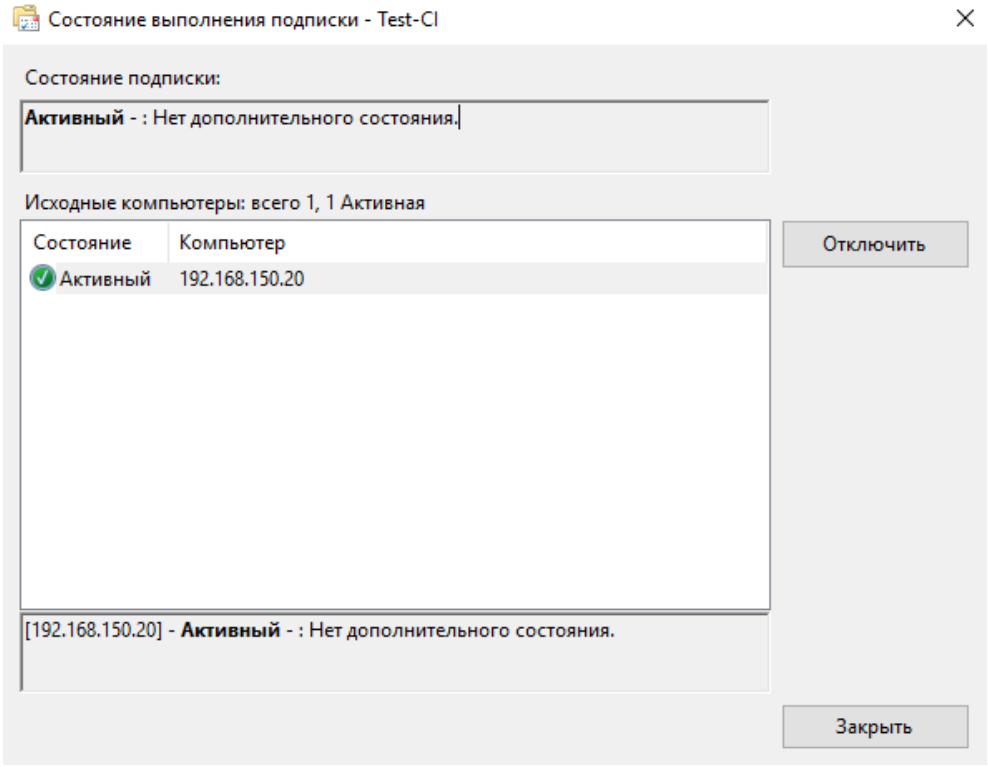


Рис. 136 – Состояние выполнения подписки

5. Проверить поступление событий в указанный в подписке журнал.

Настройка пересылки событий, инициированной источником

Перед настройкой необходимо разрешить на файерволе сборщика сетевое взаимодействие по порту 5986/tcp.

Также необходимо выпустить и установить сертификаты проверки подлинности клиента и сервера в соответствии со следующими требованиями:

- сертификат проверки подлинности сервера должен быть установлен на компьютере сборщика событий в личном хранилище локального компьютера, субъект этого сертификата должен соответствовать полному доменному имени сборщика;
- сертификат проверки подлинности клиента должен быть установлен на компьютерах источника событий в личном хранилище локального компьютера, субъект этого сертификата должен соответствовать полному доменному имени источника;
- сертификат удостоверяющего центра должен быть установлен на всех компьютерах в «Доверенные корневые центры сертификации»; если сертификат клиента выдан центром сертификации, отличным от одного из сборщиков событий, эти корневые и промежуточные сертификаты также должны быть установлены на сборщике событий;
- проверить у сертификата проверки подлинности клиента наличие разрешения на чтение для пользователя NETWORK SERVICE:

  `Консоль управления сертификатами\правой кнопкой по сертификату\Управление закрытыми ключами`

- если сертификат клиента был выдан промежуточным центром сертификации, а сборщик работает на Windows 2012 или более поздней версии, необходимо настроить следующий раздел реестра:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\
  ClientAuthTrustMode (DWORD) = 2
  ```

Проверить состояние отзыва сертификатов можно следующим образом:

```
certutil -verify -urlfetch <путь до файла сертификата>
```

Настройка источника событий

1. Открыть командную строку с правами администратора системы и в ней выполнить следующую команду:

   ```
   winrm qc –q
   ```

2. Открыть редактор локальной групповой политики (gpedit.msc) и перейти в раздел: Политика локального компьютера\Конфигурация компьютера\Административные шаблоны\Windows Компоненты\Пересылка событий.

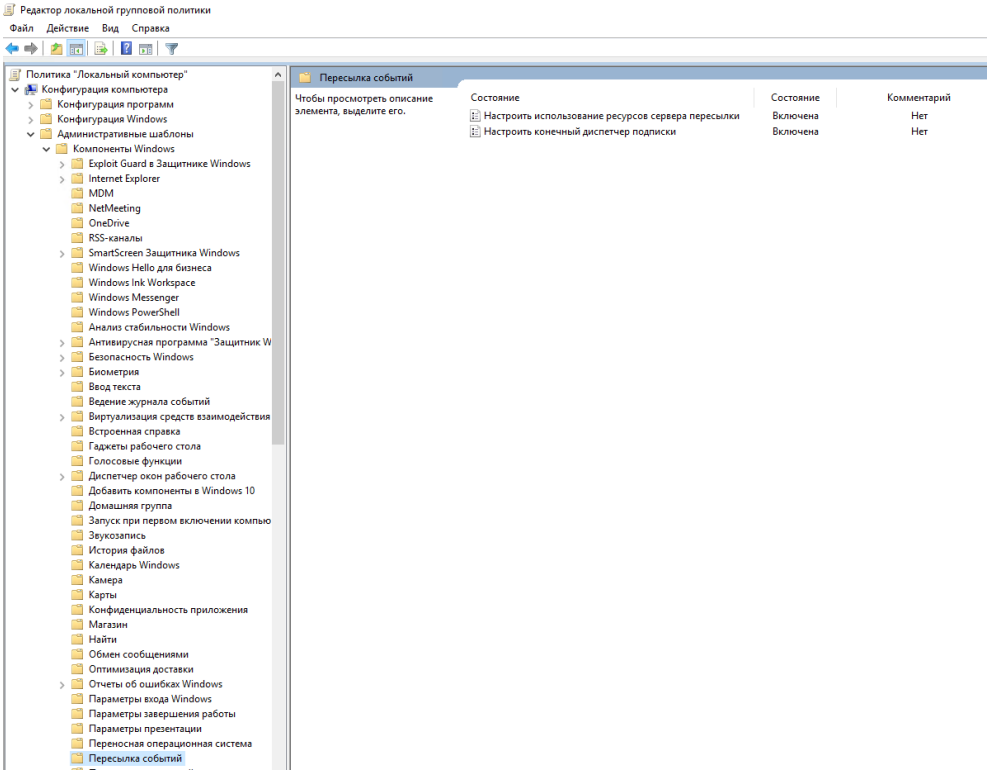


Рис. 137 – Редактор локальной групповой политики

3. Открыть элемент «Настроить конечный диспетчер подписки», включить его и нажать кнопку «Показать».

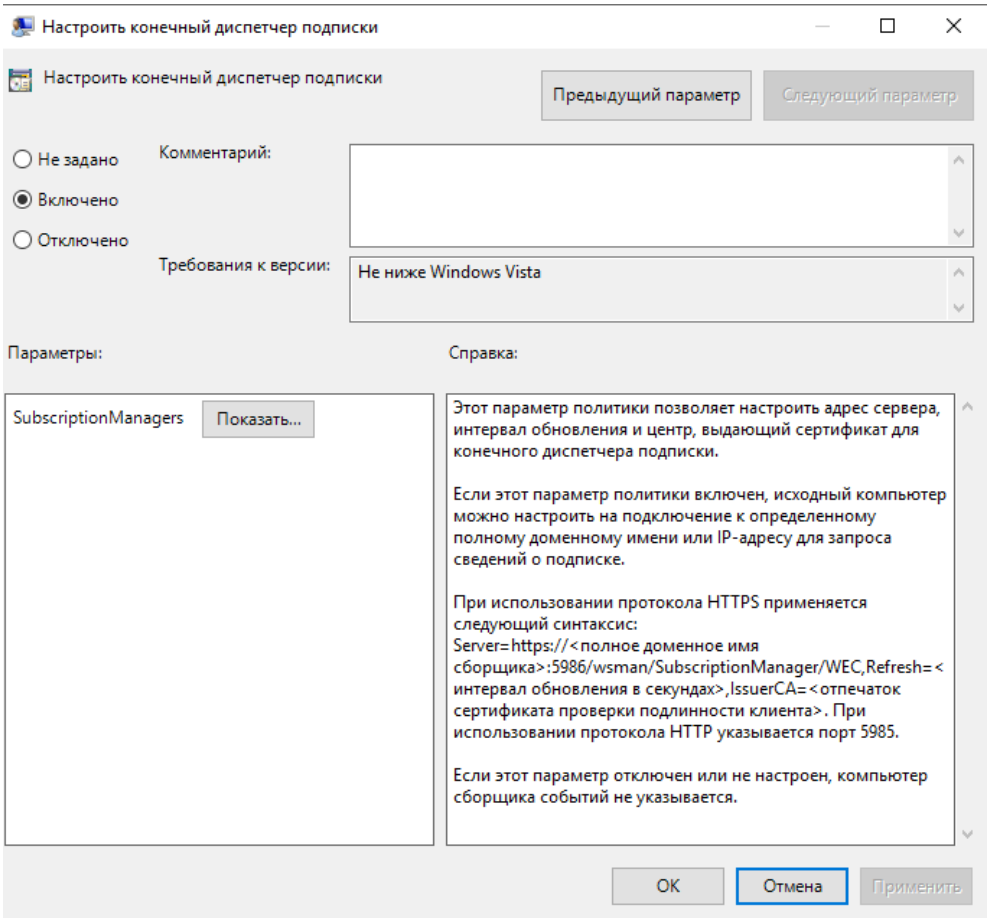


Рис. 138 – Настроить конечный диспетчер подписки

4. В открывшемся окне ввести следующий параметр и нажать «OK»:

```
Server=https://<FQDN сборщика>:5986/wsman/SubscriptionManager/WEC,Refresh=60,IssuerCA=<Отпечаток сертификата CA>
```

5. В открытой командной строке с правами администратора системы выполнить следующую команду:

```
gpupdate /force
```

Настройка сборщика событий

1. Открыть командную строку с правами администратора системы и в ней последовательно выполнить следующие команды:

```
winrm qc -q
```

```
wecutil qc /q
```

```
winrm set winrm/config/service/auth @{Certificate=”true”}
```

2. Ввести указанную ниже команду и проверить, что параметру «AllowUnencrypted» в разделах «Service» и «Client» присвоено значение «false»:

```
winrm get winrm/config
```

Если присвоено значение «true», то ввести следующие команды:

```
winrm set winrm/config/service @{AllowUnencrypted="false"}
```

```
winrm set winrm/config/client @{AllowUnencrypted="false"}
```

3. Проверить настройки прослушивателя WinRM:

   ```
   winrm e winrm/config/listener
   ```

   Если в выводе команды «Transport=HTTP» и «Port=5985», то необходимо выполнить переключение на HTTPS и 5986.

4. Выполнить переключение прослушивателя WinRM на HTTPS, введя последовательно следующие команды:

   ```
   winrm delete winrm/config/Listener?Address=*+Transport=HTTP
   ```

   ```
   winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<FQDN сборщика>"; CertificateThumbprint="<Отпечаток сертификата проверки подлинности сервера>”}
   ```

5. Создать локального пользователя и добавить его в локальную группу администраторов.

6. Создать сопоставление сертификата, который присутствует в доверенных корневых центрах сертификации компьютера или промежуточных центрах сертификации, с созданным ранее пользователем:

   ```
   winrm create winrm/config/service/certmapping?Issuer=<Отпечаток сертификата CA>+Subject=*+URI=* @{UserName=”<username>”;Password=”<password>”}
   ```

7. Проверить прослушиватель и сопоставление сертификатов можно следующими командами:

   - С клиента:

     ```
     winrm get winrm/config -r:https://<Полное_имя_сборщика>:5986 -a:certificate -certificate:”<Отпечаток сертификата проверки подлинности клиента>”
     ```

   - С сервера:

     ```
     winrm enum winrm/config/service/certmapping
     ```

8. Зайти в «Просмотр событий» и создать подписку:

   - Нажать правой кнопкой по пункту «Подписки» и выбрать «Создать подписку».

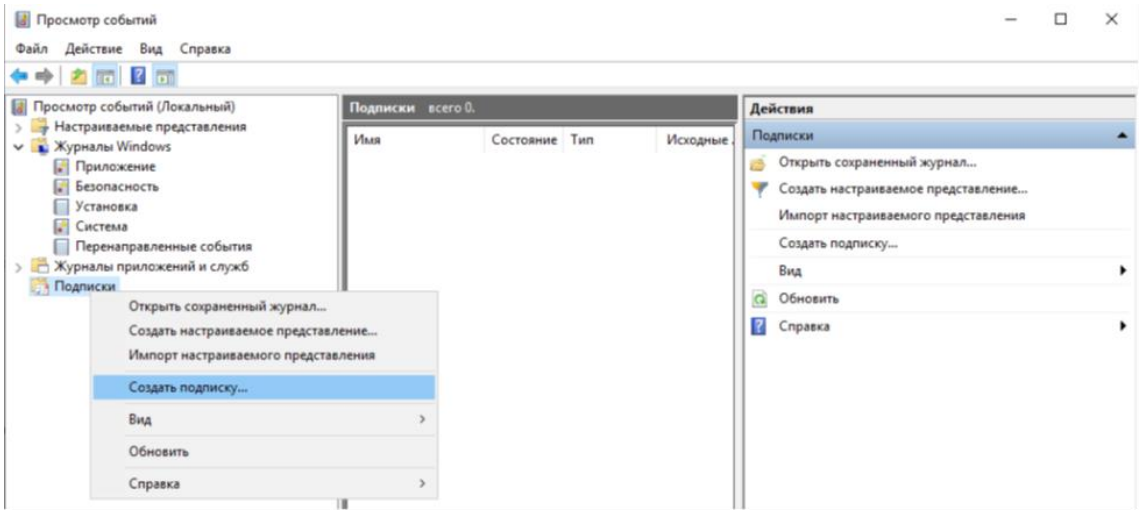


Рис. 139 – Просмотр событий

   - В открывшемся окне ввести имя подписки, выбрать конечный журнал для получаемых событий и тип подписки «Инициировано исходным компьютером» и нажать «Выбрать группы компьютеров».

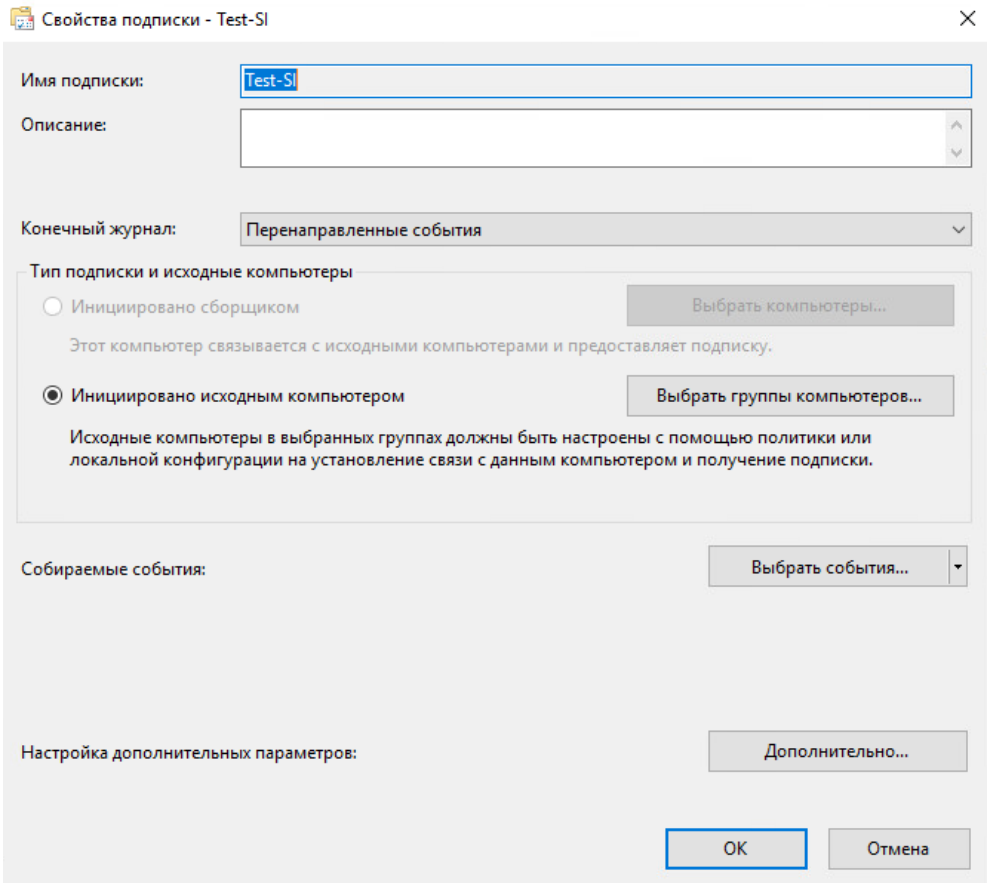


Рис. 140 – Свойства подписки

- Нажать «Добавить не доменный компьютер».

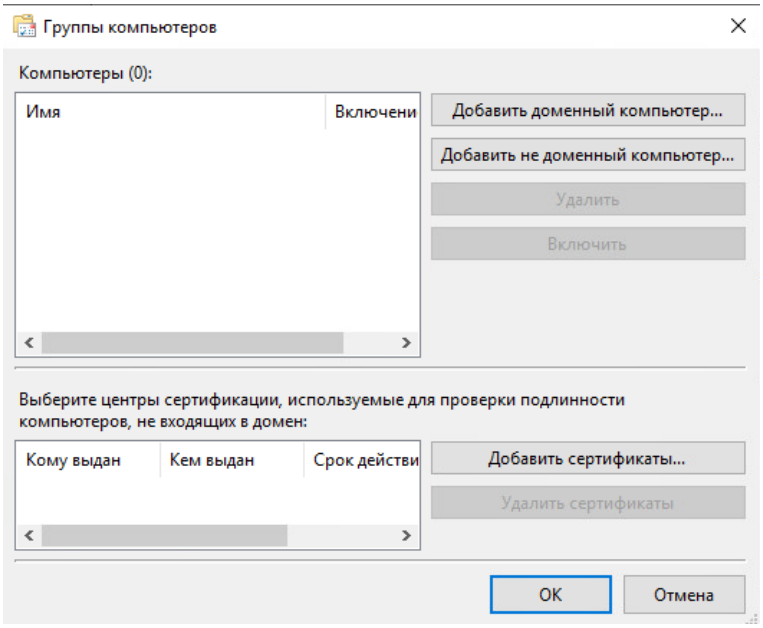
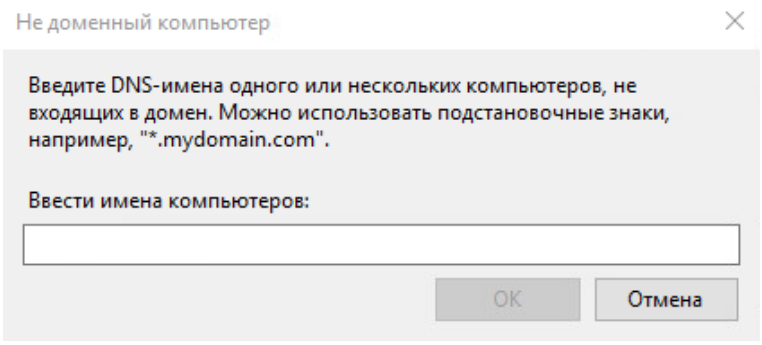


Рис. 141 – Группы компьютеров

- В открывшемся окне ввести имя источника событий и нажать «ОК».



- Нажать «Добавить сертификаты».

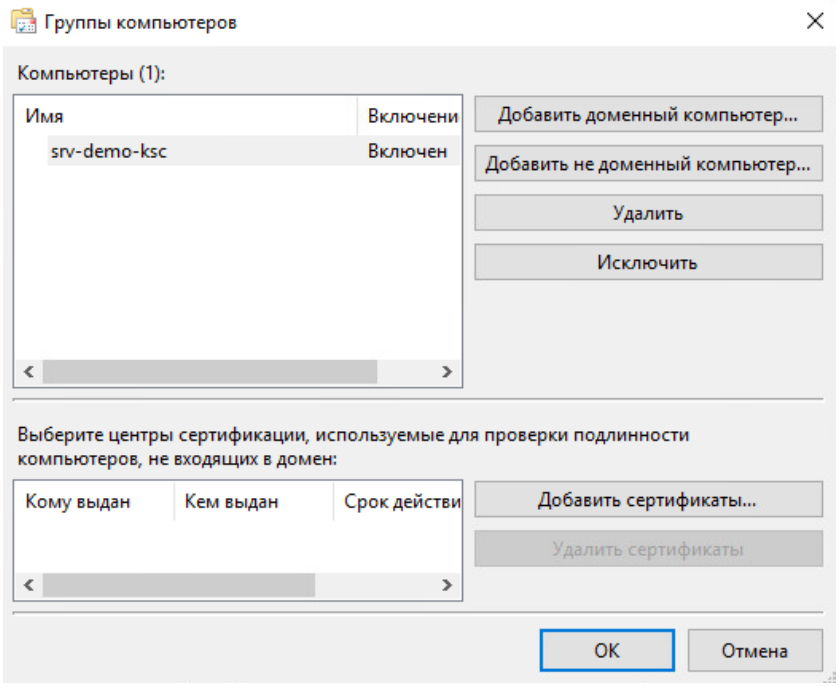


Рис. 142 – Группы компьютеров. Добавление сертификата

- В открывшемся окне выбрать сертификат центра сертификации, выпустившего сертификаты проверки подлинности клиента и сервера, и нажать «OK».

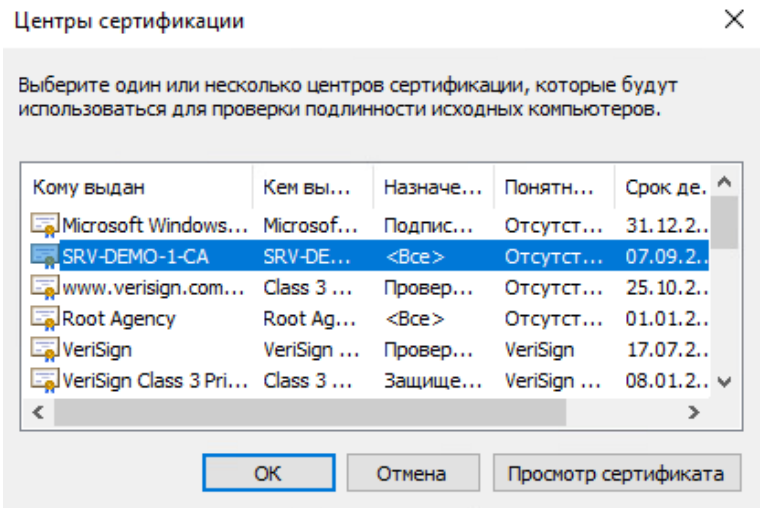


Рис. 143 – Центры сертификации

- Добавить при необходимости другие источники событий и сертификаты центров сертификации и нажать «OK».

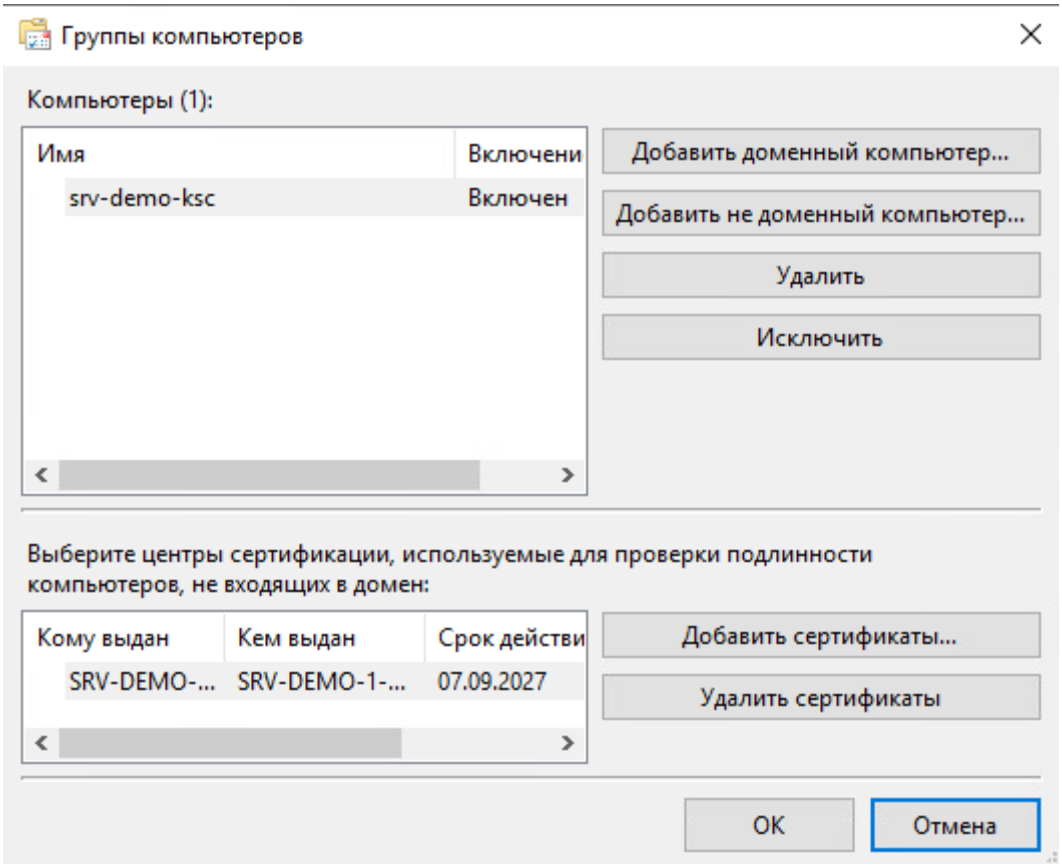


Рис. 144 – Группы компьютеров

- Нажать «Выбрать события», настроить фильтр для запроса необходимых событий и нажать «ОК».

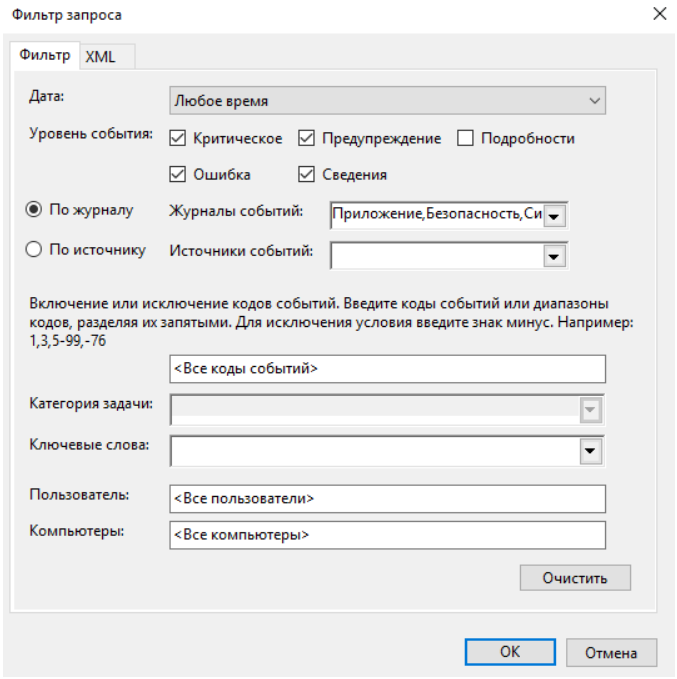


Рис. 145 – Фильтр запроса

- Нажать «Дополнительно», выбрать протокол «HTTPS» и сохранить изменения.

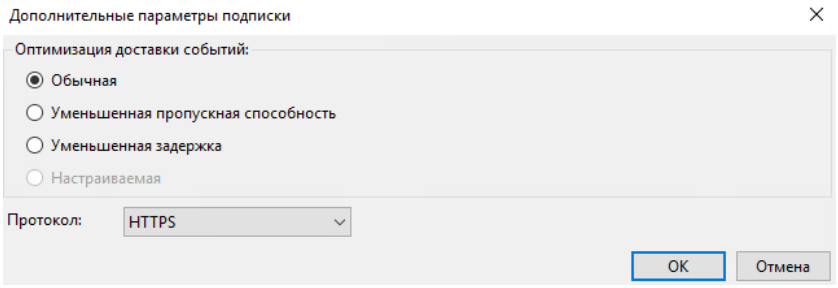


Рис. 146 – Дополнительные параметры подписки

9. После создания подписки проверить её статус, нажав по ней правой кнопкой и выбрав «Состояние выполнения». Должен появиться источник событий с состоянием «Активный».

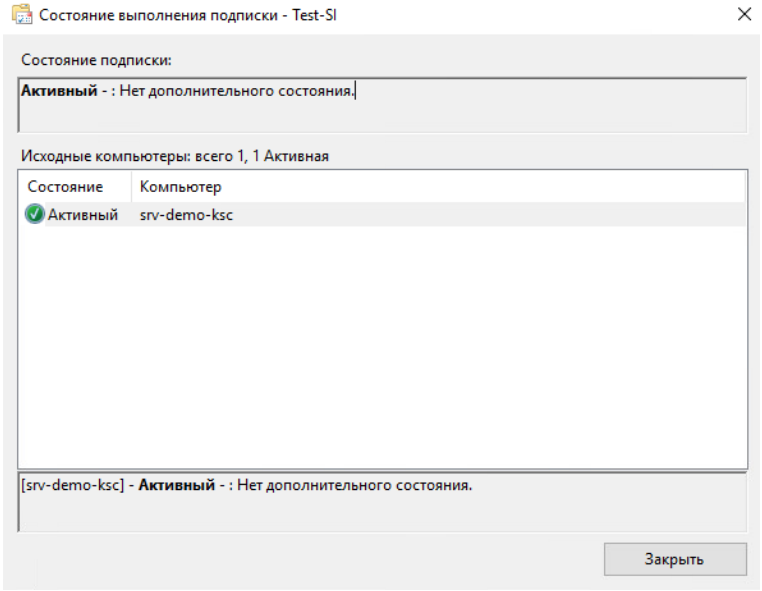


Рис. 147 – Состояние выполнения подписки

10. Проверить в конечном журнале сборщика поступление событий с источника. В случае непоступления событий просмотреть следующие журналы событий источника и сборщика на предмет наличия ошибок:

    `Microsoft-Windows-Windows Remote Management/Operational`

    `Microsoft-Windows-Eventlog-ForwardingPlugin/Operational`

    `Microsoft-Windows-CAPI2/Operational`

    `Microsoft-Windows-EventCollector/Operational`

4.2.5.2.2 Настройка WEC в домене с использованием групповых политик

Данная инструкция применяется в случае, если серверы-источники и сервер WEC расположены в одном домене. Используется метод сбора, инициированный источником.

Настройка сервера WEC

Для настройки сервера WEC необходимо:

1. Открыть командную строку.
2. Запустить службу удаленного управления Windows: winrm qc –q.
3. Запустите службу сборщика событий Windows: wecutil qc /q.

Сервер-сборщик настроен.

Настройка подписки с типом «Инициировано источником»

Для настройки подписки на сервере WEC необходимо:

1. Открыть панель управления Windows.
2. Выбрать «Administrative Tools» → «Event Viewer».
3. В левой части окна выбрать «Subscriptions».
4. В главном меню выбрать «Action» → «Create Subscription…».
5. В открывшемся окне в поле «Subscription name» введите название подписки.

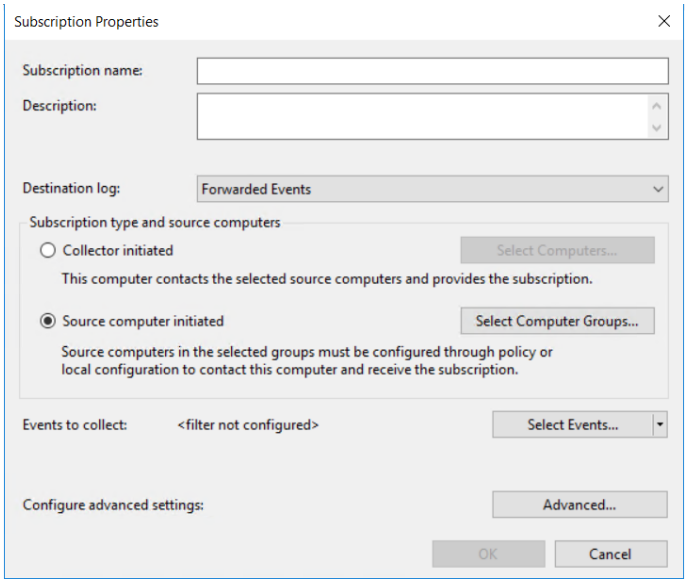


Рис. 148 – Create Subscription

6. В раскрывающемся списке «Destination log» выбрать «Forwarded Events».
7. В блоке параметров «Subscription type and source computers» выбрать вариант «Source computer initiated».
8. Нажать кнопку «Select Computers…»
9. В открывшемся окне нажать кнопку «Add Domain Computers…».
10. В открывшемся окне в поле «Enter the object name to select» ввести имя компьютера и нажать кнопку «Check Names».
11. Нажать кнопку «OK».
12. В окне «Computer Groups» нажать кнопку «OK».
13. В окне «Subscription Properties» нажать кнопку «Select Events…».

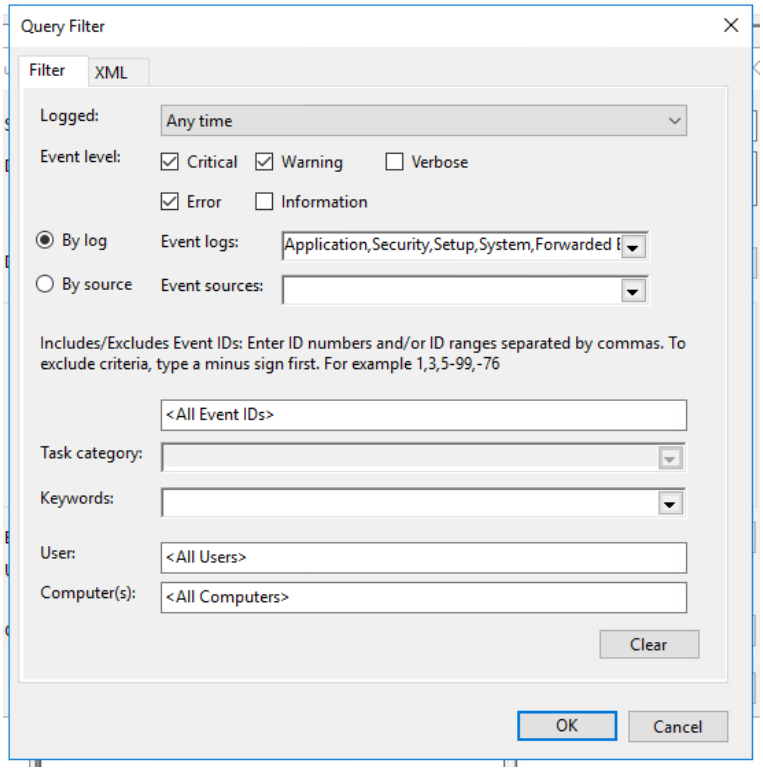


Рис. 149 – Query Filter

14. В открывшемся окне настроить фильтр событий и нажать кнопку «OK».
15. В окне «Subscription Properties» нажать кнопку «Advanced…».

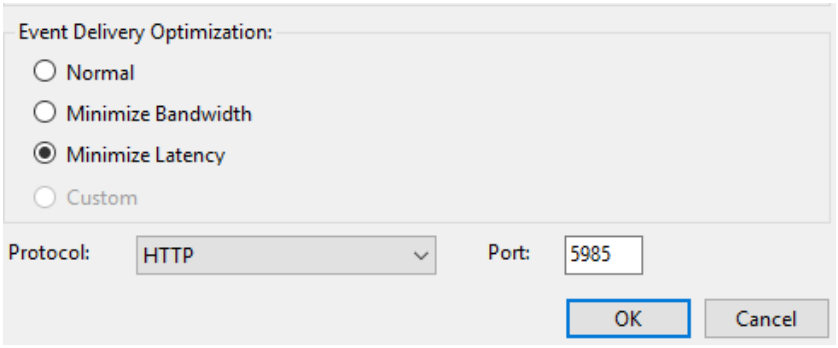


Рис. 150 – Event Delivery Optimization

16. В открывшемся окне в блоке параметров «Event Delivery Optimization» выбрать вариант «Minimize Latency».
17. Нажать кнопку «OK».
18. Снова нажать кнопку «OK».

Настройка групповой политики для межсетевого экранирования

Для настройки групповой политики для межсетевого экранирования на контроллере домена необходимо:

1. Открыть панель управления Windows.
2. Выбрать «Administrative Tools» → «Group Policy Management».
3. В левой части окна выбрать групповую политику и нажать правую кнопку мыши.

4. В выпадающем списке нажать «Edit…».

   Откроется окно «Group Policy Management Editor».

5. В левой части окна выбрать узел «<Имя политики> Policy» → «Computer Configuration» → «Policies» → «Windows Settings» → «Security Settings» → «Windows Firewall with Advanced Security» → «Windows Firewall with Advanced Security» → «Inbound Rules».

6. В главном меню выбрать «Action» → «New Rule».

   Откроется мастер создания правила для нового входящего подключения.

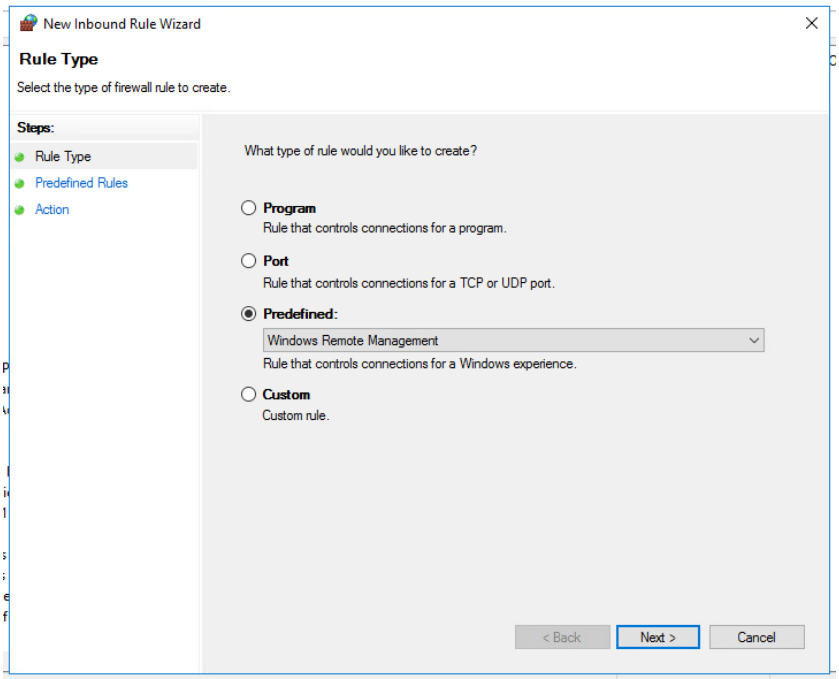


Рис. 151 – Мастер создания правила для нового входящего подключения

7. На первом шаге выбрать вариант «Predefined».

8. В раскрывающемся списке выбрать «Windows Remote Management» и нажать кнопку «Next».

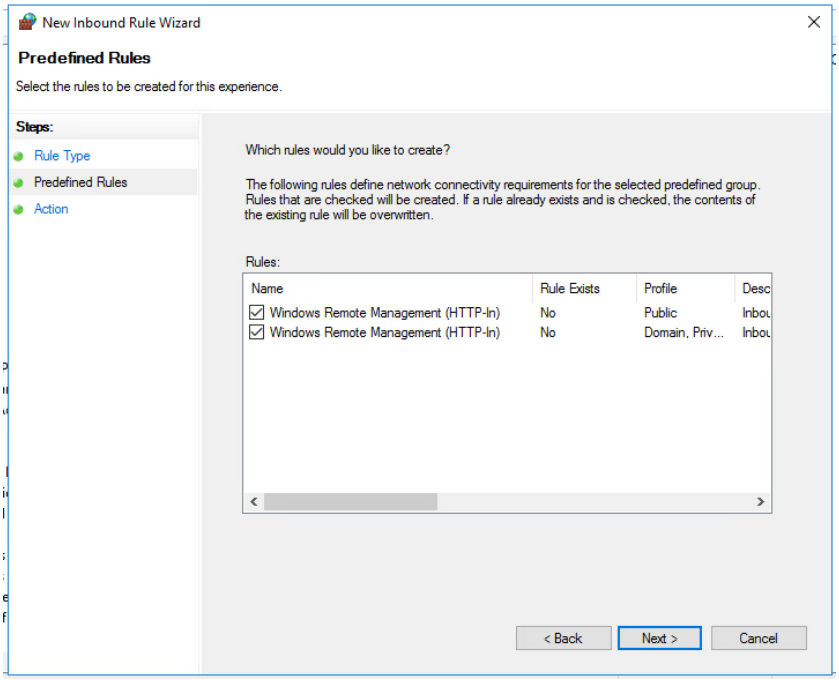


Рис. 152 – Мастер создания правила для нового входящего подключения. Шаг 1

9. На следующем шаге нажать кнопку «Next».

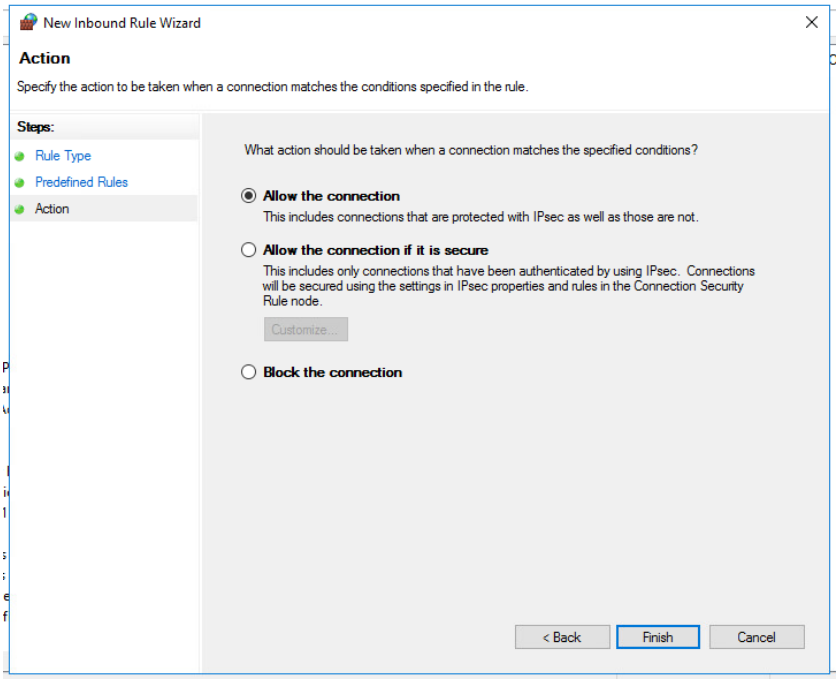


Рис. 153 – Мастер создания правила для нового входящего подключения. Шаг 2

10. На следующем шаге выбрать вариант «Allow the connection» и нажать кнопку «Finish».
11. В левой части окна выбрать узел «<Имя политики> Policy» → «Computer Configuration» → «Policies» → «Windows Settings» → «Security Settings» → «System Services».
12. В правой части окна выбрать «Windows Firewall».

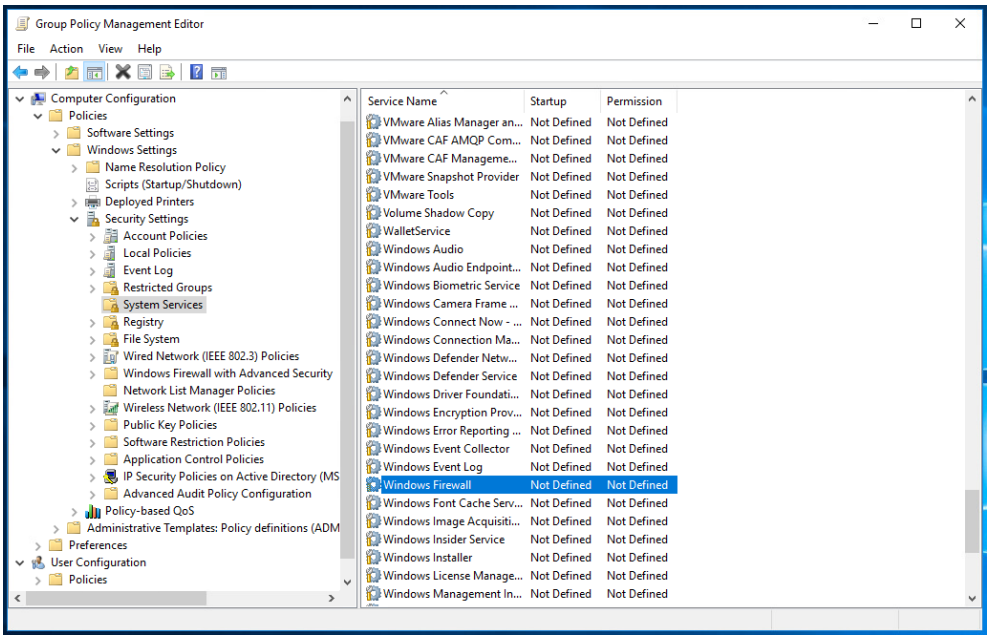


Рис. 154 – Настройка групповых политик

13. В главном меню выбрать «Action» → «Properties».
14. В открывшемся окне установить флажок «Define this policy setting».
15. Выбрать автоматический режим запуска службы.

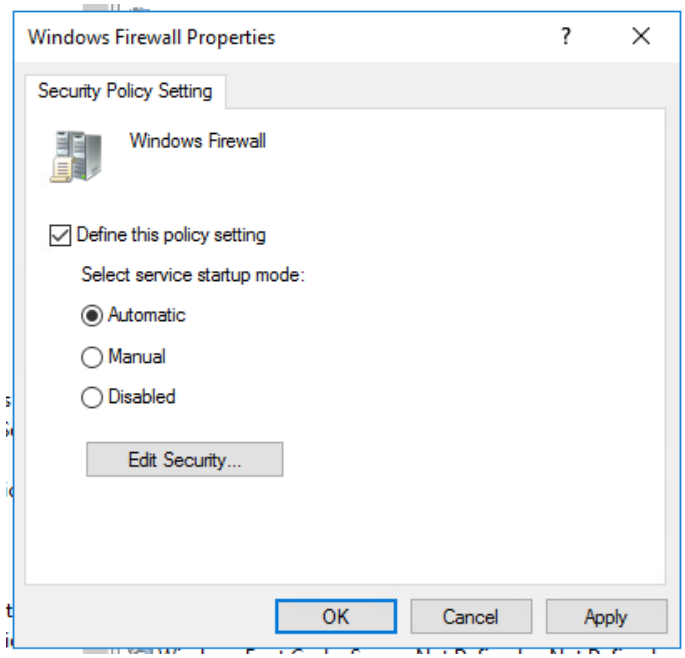


Рис. 155 – Настройки Windows Firewall

16. Нажать кнопку «ОК».

Групповая политика настроена.

Настройка групповой политики для учетной записи Сервера Сборщика

Для настройки групповой политики для учетной записи «Network Service» на контроллере домена необходимо:

1. Открыть панель управления Windows.

2. Выбрать «Administrative Tools» → «Group Policy Management»
3. В левой части окна выбрать групповую политику и нажать правую кнопку мыши.
4. В выпадающем списке нажать «Edit…».

   Откроется окно «Group Policy Management Editor».
5. В левой части окна в контекстном меню узла «<Имя политики> Policy» → «Computer Configuration» → «Policies» → «Windows Settings» → «Security Settings» → «Restricted Groups» выбрать узел «Add Group».
6. В открывшемся окне в поле «Group» ввести «Event Log Readers» и нажать кнопку «OK».
7. В открывшемся окне справа от поля «Members of this groupы» нажать кнопку «Add…».

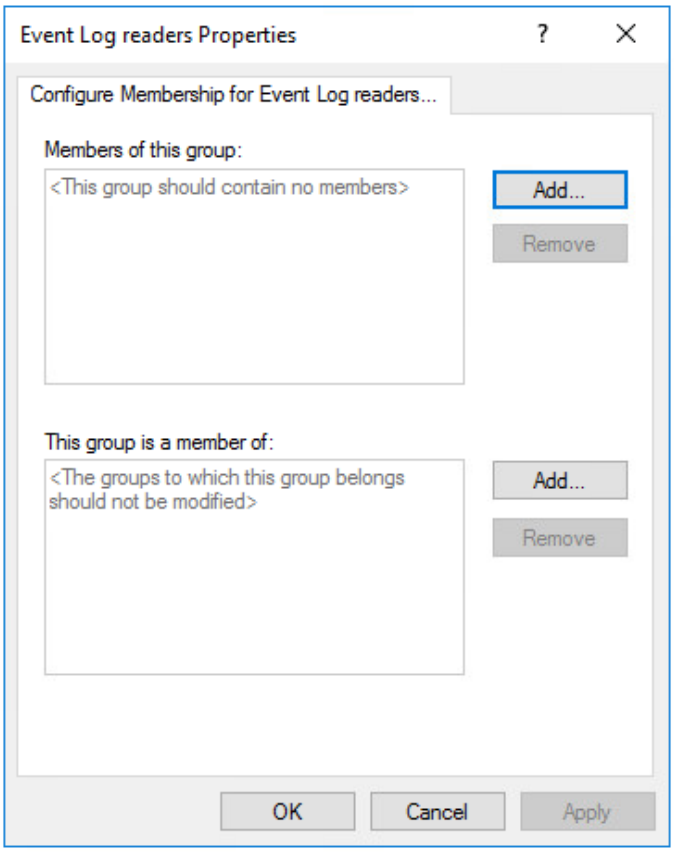


Рис. 156 - Event Log Readers Properties

8. В открывшемся окне в поле «Members of this group» ввести «Network Service» и нажать кнопку «OK».
9. Нажать кнопку «OK».

Групповая политика настроена.

Настройка групповой политики для сервера WEC

Для настройки групповой политики для сервера WEC на контроллере домена необходимо:

1. Открыть панель управления Windows.
2. Выбрать «Administrative Tools» → «Group Policy Management»
3. В левой части окна выбрать групповую политику и нажать правую кнопку мыши.

4. В выпадающем списке нажать «Edit…».

   Откроется окно «Group Policy Management Editor».

5. В левой части окна выбрать узел «<Имя политики> Policy» → «Computer Configuration» → «Policies» → «Administrative Templates…» → «Windows Components» → «Event Forwarding».

6. Выбрать параметр «Configure target Subscription Manager».

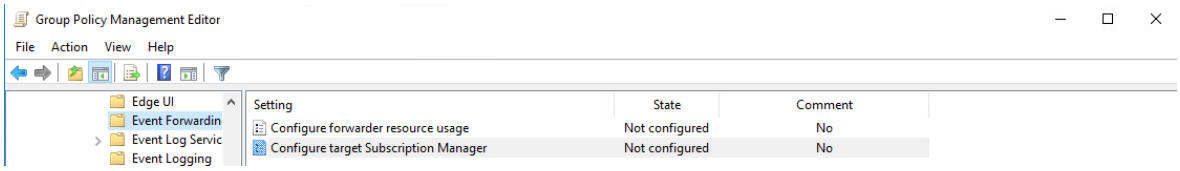


Рис. 157 - Group Policy Management Editor

7. В главном меню выбрать «Action» → «Edit».

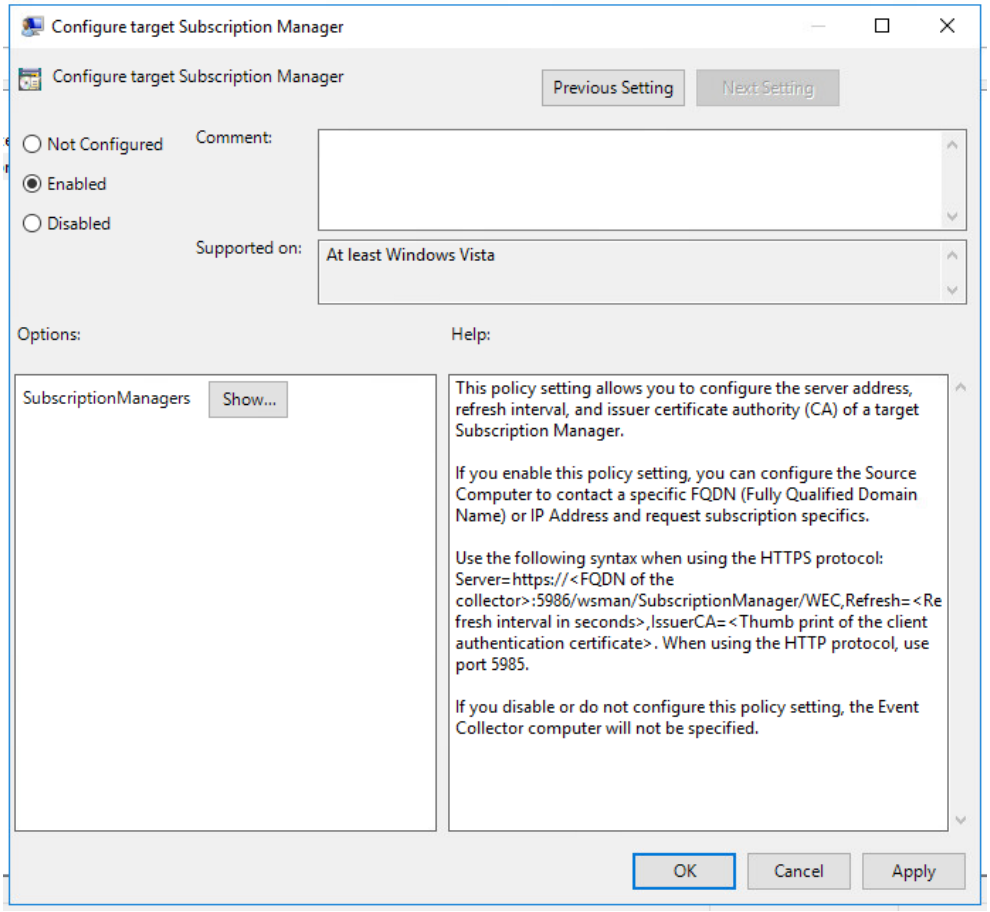


Рис. 158 – Настройка подписи

8. В открывшемся окне выбрать вариант «Enabled».

9. Нажать кнопку «Show».

10. В открывшемся окне ввести имя сервера WEC в формате FQDN, в зависимости от используемого протокола:

    - если используется протокол HTTP:

      `Server=http://<Имя сервера WEC>:5985/wsman/SubscriptionManager/WEC`

- если используется протокол HTTPS:

  ```
  Server=https://<Имя сервера WEC>:5986/wsman/SubscriptionManager/WEC
  ```

11. Нажать кнопку «OK».
12. Снова нажать кнопку «OK».
13. Выбрать параметр «Configure forwarder resource usage».
14. В главном меню выбрать «Action» → «Edit».

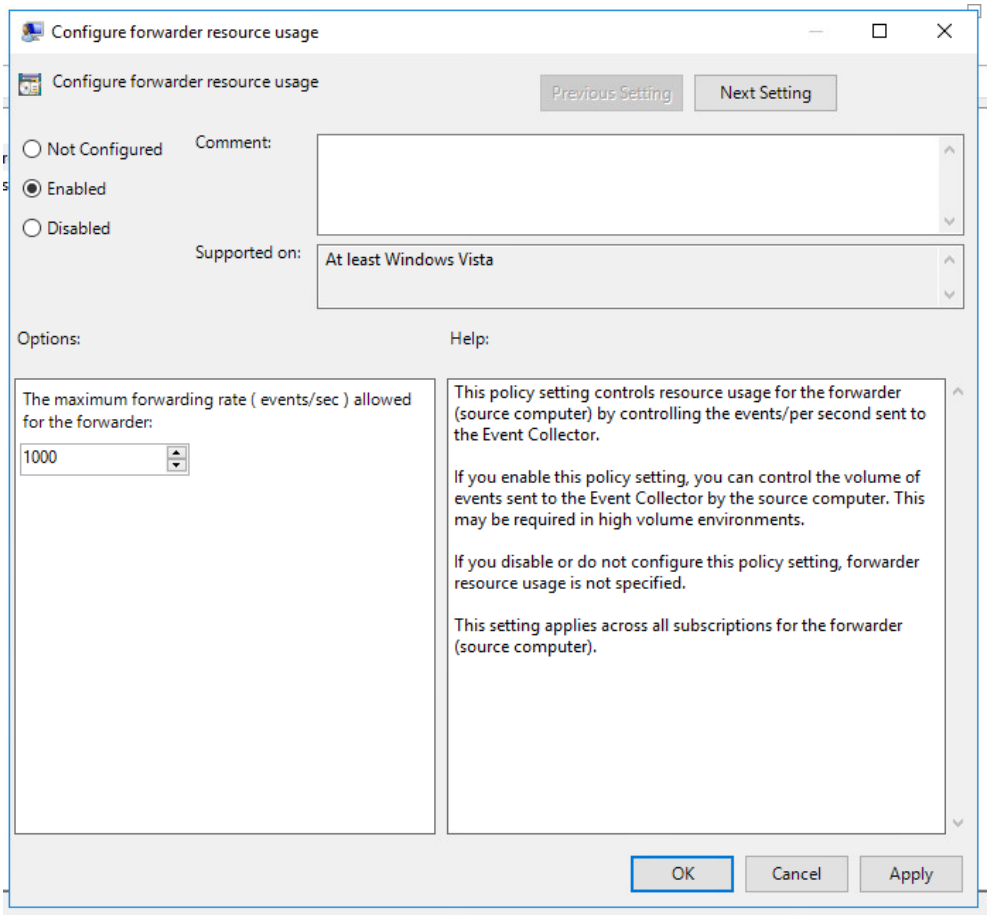


Рис. 159 – Configure forwarder resource usage

15. В открывшемся окне выбрать вариант «Включено».
16. В поле «The maximum forwarding rate (events/sec) allowed for the forwarder» ввести максимальное число событий, передаваемых за секунду.

    Среднее число событий, сохраняемое за сутки в журнале безопасности ОС (Security), можно узнать выполнив в Windows PowerShell команду:

    ```
    (Get-WinEvent -FilterXML "<QueryList><Query><Select Path='Security'>*[System[TimeCreated[timediff() @SystemTime )<=86400000]]]</Select></Query></QueryList>").count.count`
    ```

17. Нажать кнопку «OK».
18. В левой части окна выбрать узел «<Имя политики> Policy» → «Computer Configuration» → «Policies» → «Windows Settings» → «Security Settings» → «System Services».
19. Выбрать «Windows Remote Management (WS-Management)».

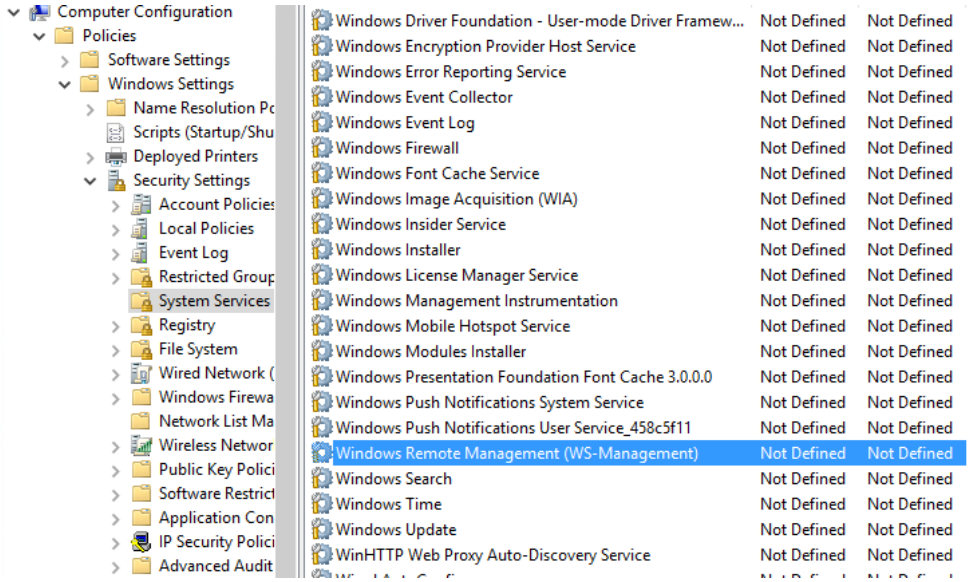


Рис. 160 - Windows Remote Management (WS-Management)

20. В главном меню выбрать «Action» → «Properties».
21. В открывшемся окне установить флажок «Define this policy setting».
22. Выбрать автоматический режим запуска службы.

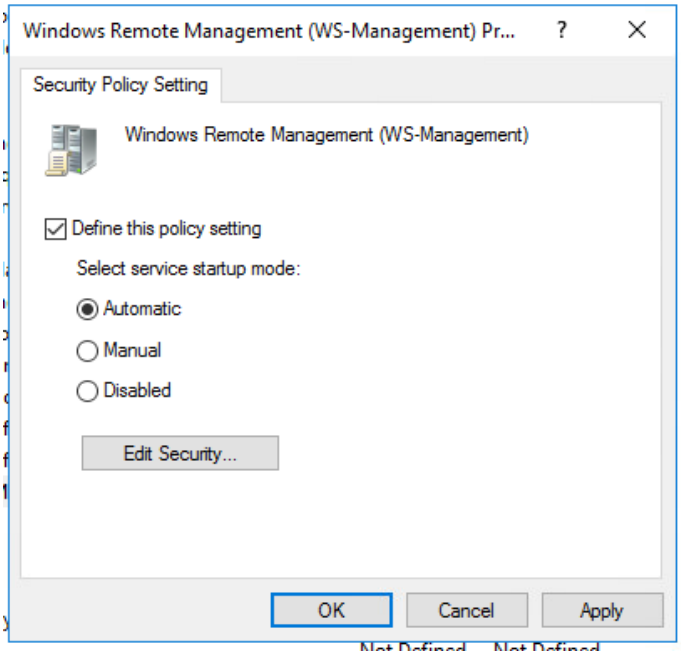


Рис. 161 – Windows Remote Management (WS-Management) Settings

23. Нажать кнопку «OK».

Групповая политика настроена.

Подготовка форвардеров к отправке

Для подготовки необходимо:

1. Открыть командную строку.
2. Выполнить в интерфейсе командной строки команду gpupdate /force (для обновления групповых политик на форвардерах).

3. Перезапуск службы «Служба удаленного управления Windows (WS-Management)» («Windows Remote Management (WS-Management)».

Создание групповой политики

Для настройки групповой политики на контроллере домена необходимо:

1. Открыть панель управления Windows.
2. Выбрать «Administrative Tools» → «Group Policy Management».
3. В левой части окна выбрать объект, для которого нужно создать групповую политику.

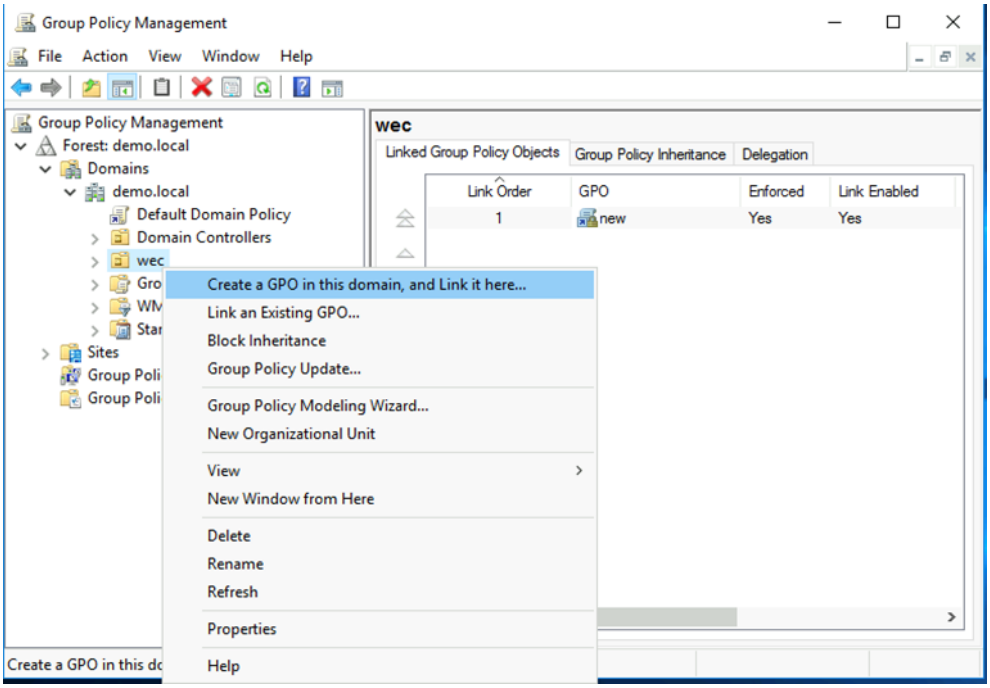


Рис. 162 – Group Policy Management

4. В главном меню выбрать «Action» → «Create a GPO in this domain, and Link it here…».
5. В открывшемся окне в поле «Имя» ввести имя групповой политики.
6. Нажать кнопку «OK».

Групповая политика создана.

Решение возникновения возможных проблем

В случае возникновения проблем с настройкой WEC – журналы с ошибками можно найти в Event Viewer, в разделе «Applications and Services Logs» → «Microsoft» → «Windows» → «Eventlog-ForwardingPlugin» → «Operational».

Если в журнале следующая ошибка:

```
The forwarder is having a problem communicating with subscription manager at address http://<FQDN_of_WEC_Server>:5985/wsman/SubscriptionManager/WEC. Error code is 2150859027 and Error Message is <f:WSManFault xmlns:f="http://schemas.microsoft.com/wbem/wsman/1/wsmanfault " Code="2150859027" Machine="demo-server2012.demo.local"><f:Message>The WinRM client sent a request to an HTTP server and got a response saying the requested HTTP URL was not available. This is usually returned by a HTTP server that does not support the WS-Management protocol. </f:Message></f:WSManFault>.
```

На WEC сервере необходимо выполнить следующие команды:

```
# netsh http delete urlacl url=http://+:5985/wsman/
```

```
# netsh http add urlacl url=http://+:5985/wsman/ sddl=D:(A;;GX;;;S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970)(A;;GX;;;S-1-5-80-4059739203-877974739-1245631912-527174227-2996563517)
```

После чего перезапустить службу «Служба удаленного управления Windows (WS-Management)» («Windows Remote Management (WS-Management)» на сервере WEC и компьютере-форвардере.

4.2.5.2.3 Включение источника на платформе

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Windows-WEC**.

4.2.6 ОС семейства Unix

4.2.6.1 Описание

Примечание: *начиная с версии 3.7.2 в **Платформе Радар** все источники, которые являются операционными системами семейства Unix, объединены в один источник **Linux-Unix**.*

Платформа Радар поддерживает сбор событий со следующих ОС семейства Unix:

- Astra Linux Special Edition 1.7 и выше;
- Ubuntu 16.04, 18.04, 20.04, 22.04;
- CentOS 6, 7, 8, 9;
- Debian 8, 9, 10, 12;
- Oracle Solaris 10, 11;
- Red Hat Enterprise Linux 6, 7, 8;
- SUSE Linux Enterprise Server 11.3, 12, 15;
- Fedora 30, 31.

Для журналирования событий используются следующие службы:

- `rsyslog` или `syslog-ng` - служба журналирования для отправки событий в платформу;
- `auditd` - отвечает за запись сообщений аудита вызванных активностью приложений или системы.

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Linux-Unix
Номер (Порт)	2671
Вендор	Unix
Тип	Linux

Характеристика	Значение
Профиль сбора	«Модуль tcp_input» «Модуль udp_input»

Примечание: *если источник будет отдавать большой поток событий, и если таких источников будет много, то рекомендуется передавать события по протоколу UDP. Так как при использовании протокола TCP может образоваться большая очередь на агенте сбора лог-коллектора. Но при использовании протокола UDP могут происходить потери. Для выбора оптимальных настроек для вашей системы, рекомендуется обратиться в службу технического сопровождения* ***Платформы Радар***.

Настройка источника включает в себя следующие процессы:

1. Настройка службы журналирования.
2. Настройка службы `auditd`.
3. Настройка журналирования bash-команд.
4. Проверка настроенной конфигурации.
5. Включение источника на платформе.

Примечание: *все действия при настройке источника должны выполняться от имени суперпользователя*.

4.2.6.2 Настройка службы журналирования

Для отправки событий стандарта syslog в **Платформу Радар** на источнике необходимо настроить службу журналирования и отправку событий.

В целях организации безопасной передачи данных на агент сбора лог-коллектора по протоколу TCP, а также обеспечения возможности фильтрации сообщений по источникам и их содержимому предлагается использовать службы `rsyslog` или `syslog-ng`.

Службы реализуют механизм централизованного протоколирования событий в ОС семейства Unix. Все части системы (включая ядро и системные службы) передают происходящие в них события службе журналирования. В свою очередь, служба журналирования добавляет к телу события информацию о *важности* (severity), *категории* (facility), времени происшествия события, hostname или IP-адрес хоста, имя и PID службы, сгенерировавшей лог.

Служба журналирования, согласно настройкам в файле конфигурации, классифицирует все события в несколько выходных потоков, согласно *категории* (facility) и *важности* (severity). Например, события ядра системы будут иметь категорию kern, а события почтового сервера - категорию mail. Если уровень важности не имеет значения, но необходимо, чтобы в одном файле были собраны события только одного демона, в файле конфигурации службы журналирования указывается запись `kern.* -/var/log/kern.log`, где * - любой уровень важности события. Но если необходимо, например, сохранять в файл события ошибок почтового сервера, указывается строка `mail.err /var/log/mail.err`. Таким образом, можно распределить события разных категорий и уровней важности по разным файлам.

Перед началом работы с платформой мы рекомендуем вам настроить параметры *категории* (facility) и *важности* (severity) события для оптимизации передаваемого в платформу потока.

Подробнее о механизме централизованного протоколирования событий вы можете ознакомиться в соответствующих руководствах для вашей ОС.

4.2.6.2.1 Определение используемой службы журналирования

Если установлена ОС Astra Linux, Debian или Ubuntu, то выполните команду:

```
# dpkg --list | grep syslog
```

Если ALT Linux, CentOS или Red Hat Enterprise Linux, то выполните команду:

```
# rpm -qa *syslog*
```

Если SUSE Linux Enterprise Server, то выполните команду:

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

На экран будет выведено название используемой службы. Если результат отличается от `rsyslog` или `syslog-ng`, то рекомендуется выполнить установку соответствующей службы.

4.2.6.2.2 Настройка rsyslog

Если служба не установлена, то вы можете ее установить. Для этого выполните соответствующую команду:

ОС	**Команда**
для систем на базе deb (Debian / Ubuntu)	`# apt-get update` `# apt-get install rsyslog`
для систем на базе RPM (Red Hat / CentOS)	`# yum -y install rsyslog`

Добавьте службу `rsyslog` в автозагрузку и запустите:

```
# systemctl enable rsyslog
# systemctl start rsyslog
```

Конфигурационный файл службы `/etc/rsyslog.conf` по умолчанию имеет следующую структуру:

Первой идет секция модулей:

- Модули ввода — можно рассматривать как способ сбора информации из различных источников, начинаются с `im`;
- Модули вывода — позволяют отправлять сообщения в файлы, по сети или в базу данных, имя начинается на `om`;
- Модули фильтрации — позволяют фильтровать поступающие сообщения по различным критериям, начинаются с `fm`;
- Модули парсинга — предоставляют расширенные возможности для синтаксического анализа сообщения, начинаются с `pm`.

Далее идет секция глобальных директив:

- `$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat` предписывает записывать события в формате `<PRI> TIMESTAMP HOSTNAME TAG MSG`;
- `$RepeatedMsgReduction on` предписывает отбрасывать дубликаты сообщений;
- `$WorkDirectory /var/spool/rsyslog` — задает директорию для рабочих файлов службы;
- `$IncludeConfig /etc/rsyslog.d/*.conf` — задает директорию дополнительных файлов конфигурации.

Директивы `$FileOwner, $FileGroup` и прочие — устанавливают права доступа, владельца и группу по умолчанию для лог-файлов.

Для настройки пересылки событий в агент сбора лог-коллектора необходимо в конец конфигурационного файла `rsyslog.conf` добавить следующую строку:

```
auth,authpriv.* @@<адрес агента сбора лог-коллектора>:port
```

Где:

- `<ip-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
- `@@` - указывается в случае, если используется протокол TCP;
- `@` - указывается в случае, если используется протокол UDP.

Для завершения настройки необходимо перезапустить службу `rsyslog`.

Настройка отправки событий от службы auditd

Чтобы служба rsyslog принимала и отправляла поток событий от службы auditd, необходимо создать файл /etc/rsyslog.d/30-auditd.conf и указать в нем следующие параметры:

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

input(type="imfile" File="/var/log/audit/audit.log"
    Severity="info"
    Facility="local6"
    tag="audit:")

local6.*  @@<IP-адрес агента сбора лог-коллектора>:port
```

Где:

- `<ip-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
- `@@` - указывается в случае, если используется протокол TCP;
- `@` - указывается в случае, если используется протокол UDP.

Настройка отправки событий от службы UFW и firewalld

Служба `rsyslog` может самостоятельно передавать события от служб `firewalld` и `UFW`.

При необходимости вы можете подключить службы как отдельный источник.

Описание настройки служб описано в разделе «UFW и firewalld».

4.2.6.2.3 Настройка syslog-ng

Если служба не установлена, то вы можете ее установить. Для этого выполните соответствующую команду:

ОС	Команда
для систем на базе deb (Debian / Ubuntu)	`# apt-get update` `# apt-get install syslog-ng`
для систем на базе RPM (Red Hat / CentOS)	`# yum -y install syslog-ng`

Добавьте службу `syslog-ng` в автозагрузку и запустите:

```
# systemctl enable syslog-ng
```

```
# systemctl start syslog-ng
```

В конфигурационном файле `/etc/syslog-ng/syslog-ng.conf` настройте службу на сбор необходимых событий (пример файла приведен в разделе «Пример файла конфигурации службы syslog-ng»).

В начале файла укажите версию службы (если она не указана) и включенные конфигурационные файлы:

```
@version: 3.35
```

```
@include "scl.conf"
```

```
@include "/etc/syslog-ng/conf.d/*.conf"
```

В блоке `options` установите следующие глобальные переменные:

```
options {
    flush_lines (0);
    time_reopen (10);
    log_fifo_size (1000);
    chain_hostnames (off);
    use_dns (no);
    dns-cache(no);
    use_fqdn (no);
    create_dirs (no);
    keep_hostname (yes);
    stats-freq(0);
    mark-freq(0);
};
```

В блоке `Sources` укажите источники получения логов, например:

```
source s_sys {
       system();
       internal();
};
```

В блоке `Destinations` укажите пути к файлам, собираемых журналов:

```
# стандартные файлы журналов.
#
destination d_auth { file("/var/log/auth.log"); };
destination d_auth { file("/var/log/auth.log"); };
destination d_daemon { file("/var/log/daemon.log"); };
destination d_kern { file("/var/log/kern.log"); };
destination d_lpr { file("/var/log/lpr.log"); };
destination d_mail { file("/var/log/mail.log"); };
destination d_syslog { file("/var/log/syslog"); };
destination d_user { file("/var/log/user.log"); };
destination d_uucp { file("/var/log/uucp.log"); };

# журналы, поступающие от почтовых подсистем.
#
destination d_mailinfo { file("/var/log/mail.info"); };
destination d_mailwarn { file("/var/log/mail.warn"); };
destination d_mailerr { file("/var/log/mail.err"); };

# универсальные файлы журналов.
#
destination d_debug { file("/var/log/debug"); };
destination d_error { file("/var/log/error"); };
destination d_messages { file("/var/log/messages"); };

# root's консоль.
#
destination d_mlal { usertty("*"); };

# virtual консоль.
#
destination d_cons { file("/dev/console"); };

# отптравка сообщений в агент сбора лог-коллектора
#
destination d_net { tcp("<IP-адрес агента сбора лог-коллектора>" port
log_fifo_size(1000)); };
```

Где, в параметре `destination d_net` укажите следующие данные:

- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

В блоке `Filters` настройте правила и уровни журналирования, чтобы установить какие именно сообщения будут отправляться. Рекомендуются следующие настройки:

```
filter f_dbg { level(debug); };
filter f_info { level(info); };
filter f_notice { level(notice); };
filter f_warn { level(warn); };
filter f_err { level(err); };
filter f_crit { level(crit .. emerg); };

filter f_debug { level(debug) and not facility(auth, authpriv, news, mail); };
filter f_error { level(err .. emerg) ; };
filter f_messages { level(info,notice,warn) and
                    not facility(auth,authpriv,cron,daemon,mail,news); };
```

```
filter f_audit { program("audit"); };
filter f_auth { facility(auth, authpriv); };
filter f_daemon { facility(daemon) and not filter(f_debug); };
filter f_kern { facility(kern) and not filter(f_debug); };
filter f_lpr { facility(lpr) and not filter(f_debug); };
filter f_local { facility(local0, local1, local3, local4, local5,
                      local6, local7) and not filter(f_debug); };

filter f_mail { facility(mail) and not filter(f_debug); };
filter f_syslog3 { not facility(auth, authpriv, mail) and not filter(f_debug); };
filter f_user { facility(user) and not filter(f_debug); };
filter f_uucp { facility(uucp) and not filter(f_debug); };

filter f_cnews { level(notice, err, crit) and facility(news); };
filter f_cother { level(debug, info, notice, warn) or facility(daemon, mail); };


filter f_console { level(warn .. emerg); };
```

В блоке `Log path` укажите маршрутизацию принятого службой логирования потока событий (блок `Source`) в указанные файлы логов (блока `Destination`) в соответствии с заданными фильтрами:

```
log { source(s_sys); filter(f_auth); destination(d_auth); };
log { source(s_sys); filter(f_daemon); destination(d_daemon); };
log { source(s_sys); filter(f_kern); destination(d_kern); };
log { source(s_sys); filter(f_lpr); destination(d_lpr); };
log { source(s_sys); filter(f_syslog3); destination(d_syslog); };
log { source(s_sys); filter(f_user); destination(d_user); };
log { source(s_sys); filter(f_uucp); destination(d_uucp); };

log { source(s_sys); filter(f_mail); destination(d_mail); };

log { source(s_sys); filter(f_debug); destination(d_debug); };
log { source(s_sys); filter(f_error); destination(d_error); };
log { source(s_sys); filter(f_messages); destination(d_messages); };

log { source(s_sys); filter(f_console); destination(d_cons); };
log { source(s_sys); filter(f_crit); destination(d_mlal); };

# для отправки сообщений на удаленный сайт
# убедитесь, что строка ниже не закомментирована
log { source(s_sys); filter(f_auth); destination(d_net); };
```

Внимание! *убедитесь, что не закомментирована строка* `log { source(s_sys); filter(f_auth); destination(d_net); }`

Для завершения настройки необходимо перезапустить службу `syslog-ng`.

Настройка отправки событий от службы auditd

Для отправки событий собираемых службой auditd на агент сбора лог-коллектора, в директории `/etc/syslog-ng/conf.d` добавьте файл `audit_messages.conf` со следующими параметрами:

```
source s_audit {
```

```
    file (/var/log/audit/audit.log persist-name (s_auditd_for_siem)
program_override("auditd"));
};

destination d_auditd {
    tcp (
        "<IP-адрес агента сбора лог-коллектора>"
        port
        persist-name(d_auditd_for_siem)
        );
};

log {
    source(s_audit); destination(d_auditd);
};
```

Где, в параметре `destination d_auditd` укажите следующие параметры:

- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

Настройка отправки событий от службы UFW и firewalld

Служба `syslog-ng` может самостоятельно передавать события от служб `firewalld` и `UFW`.

При необходимости вы можете подключить службы как отдельный источник.

Описание настройки служб описано в разделе «UFW и firewalld».

4.2.6.3 Настройка службы auditd

Служба `auditd` предназначена для мониторинга событий операционной системы и записи их в журналы событий.

Настройка службы включает в себя установку и подключение службы в качестве источника событий для **Платформы Радар**.

Если служба не установлена, то вы можете ее установить. Для этого выполните соответствующую команду:

ОС	Команда
для систем на базе deb (Debian / Ubuntu)	`# sudo apt-get install auditd` `# sudo apt-get install audispd-plugins`
для систем на базе RPM (Red Hat / CentOS)	`# yum -y install auditd` `# yum -y install audispd-plugins`

4.2.6.3.1 Настройка конфигурационного файла службы auditd

Конфигурационный файл службы - `/etc/audit/auditd.conf` - содержит информацию о конфигурации, специфичную для аудита. Структура файла: одно ключевое слово конфигурации в каждой строке, знак равенства, а затем следует соответствующая информация о конфигурации.

Если у вас ОС на базе deb (Debian / Ubuntu), то в `/etc/audit/auditd.conf` укажите следующее содержимое:

```
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NUMERIC
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
```

Если у вас ОС на базе RPM (Red Hat / CentOS), то в /etc/audit/auditd.conf укажите следующее содержимое:

```
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 6
name_format = HOSTNAME
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
```

```
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
transport = TCP
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
q_depth = 1200
overflow_action = SYSLOG
max_restarts = 10
plugin_dir = /etc/audit/plugins.d
end_of_event_timeout = 2
```

Описание параметров конфигурационного файла `/etc/audit/auditd.conf` приведено в разделе «Описание параметров файла auditd.conf».

4.2.6.3.2 Настройка правил расширенного аудита

Если у вас ОС на базе deb (Debian / Ubuntu), то создайте файл с правилами расширенного аудита `/etc/audit/rules.d/extended.rules` и добавьте туда следующие правила:

```
-D
-b 8192
-f 1

-a exclude,always -F msgtype=BPRM_FCAPS
-a exclude,always -F msgtype=BPF


# ===== EXECVE (ВСЕ КОМАНДЫ) =====
-a always,exit -F arch=b64 -S execve,execveat -k exec_all_commands
-a always,exit -F arch=b32 -S execve,execveat -k exec_all_commands

# ===== PRIVILEGE ESCALATION =====
-a always,exit -F arch=b64 -S
setuid,setgid,setreuid,setregid,setresuid,setresgid,setfsuid,setfsgid -k
privilege_escalation
-a always,exit -F arch=b32 -S
setuid,setgid,setreuid,setregid,setresuid,setresgid,setfsuid,setfsgid -k
privilege_escalation

# ===== SENSITIVE FILES =====
-a always,exit -F arch=b64 -S open,openat,openat2 -F path=/etc/shadow -F auid!=-1 -k
shadow_read
-a always,exit -F arch=b32 -S open,openat -F path=/etc/shadow -F auid!=-1 -k
shadow_read

-a always,exit -F arch=b64 -S open,openat,openat2 -F path=/etc/passwd -F auid!=-1 -k
passwd_read
-a always,exit -F arch=b32 -S open,openat -F path=/etc/passwd -F auid!=-1 -k
passwd_read

# ===== MOUNT OPERATIONS =====
-a always,exit -F arch=b64 -S mount,umount2 -k mount_operations
-a always,exit -F arch=b32 -S mount,umount2 -k mount_operations
```

```
# ===== PTRACE (Process Tracing) =====
-a always,exit -F arch=b64 -S ptrace -k ptrace_usage
-a always,exit -F arch=b32 -S ptrace -k ptrace_usage

# ===== SOCKET OPERATIONS =====
-a always,exit -F arch=b64 -S socket -F a0=2 -k socket_ipv4
-a always,exit -F arch=b32 -S socket -F a0=2 -k socket_ipv4

-a always,exit -F arch=b64 -S socket -F a0=0xa -k socket_ipv6
-a always,exit -F arch=b32 -S socket -F a0=0xa -k socket_ipv6

-a always,exit -F arch=b64 -S bind -k network_bind
-a always,exit -F arch=b32 -S bind -k network_bind

# ===== TIME MANIPULATION =====
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time_changes
-a always,exit -F arch=b32 -S adjtimex,settimeofday,stime,clock_settime -k
time_changes

# ===== NETWORK CONFIG =====
-a always,exit -F arch=b64 -S sethostname,setdomainname -k network_modifications
-a always,exit -F arch=b32 -S sethostname,setdomainname -k network_modifications

# ===== PROCESS TRACKING =====
-a always,exit -F arch=b64 -S fork,vfork,clone,clone3 -F auid!=-1 -k process_creation
-a always,exit -F arch=b32 -S fork,vfork,clone,clone3 -F auid!=-1 -k process_creation

-a always,exit -F arch=b64 -S exit,exit_group -k process_exit
-a always,exit -F arch=b32 -S exit,exit_group -k process_exit

# ===== FILE OPERATIONS =====
# Статистика файлов (базовая информация)
-a always,exit -F arch=b64 -S stat,lstat,statx -k file_stat
-a always,exit -F arch=b32 -S lstat,stat -k file_stat

# fstat - информация о открытом файле
-a always,exit -F arch=b64 -S fstat -k fstat_usage
-a always,exit -F arch=b32 -S fstat -k fstat_usage

# mknod - создание специальных файлов
-a always,exit -F arch=b64 -S mknod,mknodat -k mknod_usage
-a always,exit -F arch=b32 -S mknod,mknodat -k mknod_usage

# chown - изменение владельца
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid!=-1 -k chown_usage
-a always,exit -F arch=b32 -S chown,fchown,lchown,fchownat -F auid!=-1 -k chown_usage

# link операции - создание жестких и символических ссылок
-a always,exit -F arch=b64 -S link,linkat,symlink,symlinkat -F auid!=-1 -k link_usage
-a always,exit -F arch=b32 -S link,linkat,symlink,symlinkat -F auid!=-1 -k link_usage


# ===== SOCKET OPTIONS =====
-a always,exit -F arch=b64 -S setsockopt -F auid!=-1 -k setsockopt_usage
-a always,exit -F arch=b32 -S setsockopt -F auid!=-1 -k setsockopt_usage

-a always,exit -F arch=b64 -S getsockopt -F auid!=-1 -k getsockopt_usage
-a always,exit -F arch=b32 -S getsockopt -F auid!=-1 -k getsockopt_usage

-a always,exit -F arch=b64 -S listen -k listen_usage
-a always,exit -F arch=b32 -S listen -k listen_usage

-a always,exit -F arch=b64 -S accept,accept4 -k accept_usage
-a always,exit -F arch=b32 -S accept4 -k accept_usage
```

```
-a always,exit -F arch=b64 -S shutdown -k shutdown_usage
-a always,exit -F arch=b32 -S shutdown -k shutdown_usage

-a always,exit -F arch=b64 -S getpeername -k getpeername_usage
-a always,exit -F arch=b32 -S getpeername -k getpeername_usage

-a always,exit -F arch=b64 -S getsockname -k getsockname_usage
-a always,exit -F arch=b32 -S getsockname -k getsockname_usage

# ===== SIGNALS & IPC =====
-a always,exit -F arch=b64 -S getgroups -k groups_query
-a always,exit -F arch=b32 -S getgroups -k groups_query

-a always,exit -F arch=b64 -S kill,rt_sigqueueinfo,tgkill -k kill_signal_usage
-a always,exit -F arch=b32 -S kill,rt_sigqueueinfo,tgkill -k kill_signal_usage

-a always,exit -F arch=b64 -S futex -F auid!=-1 -k futex_usage
-a always,exit -F arch=b32 -S futex -F auid!=-1 -k futex_usage

-a always,exit -F arch=b64 -S shmget,shmctl,shmdt,shmat -k ipc_shm_usage
-a always,exit -F arch=b32 -S shmget,shmctl,shmdt,shmat -k ipc_shm_usage

-a always,exit -F arch=b64 -S semget,semctl,semop,semtimedop -k ipc_sem_usage
-a always,exit -F arch=b32 -S semget -k ipc_sem_usage

-a always,exit -F arch=b64 -S msgget,msgctl,msgsnd,msgrcv -k ipc_msg_usage
-a always,exit -F arch=b32 -S msgget,msgctl,msgsnd,msgrcv -k ipc_msg_usage

-a always,exit -F arch=b64 -S
inotify_init,inotify_init1,inotify_add_watch,inotify_rm_watch -k inotify_usage
-a always,exit -F arch=b32 -S
inotify_init,inotify_init1,inotify_add_watch,inotify_rm_watch -k inotify_usage

-a always,exit -F arch=b64 -S splice,tee,vmsplice -k splice_usage
-a always,exit -F arch=b32 -S splice,tee,vmsplice -k splice_usage

-a always,exit -F arch=b64 -S pipe,pipe2 -k pipe_usage
-a always,exit -F arch=b32 -S pipe,pipe2 -k pipe_usage

-a always,exit -F arch=b64 -S flock -F auid!=-1 -k flock_usage
-a always,exit -F arch=b32 -S flock -F auid!=-1 -k flock_usage

-a always,exit -F arch=b64 -S mlock,mlock2,munlock,mlockall,munlockall -k mlock_usage
-a always,exit -F arch=b32 -S mlock,mlock2,munlock,mlockall,munlockall -k mlock_usage

-a always,exit -F arch=b64 -S mremap -F auid!=-1 -k mremap_usage
-a always,exit -F arch=b32 -S mremap -F auid!=-1 -k mremap_usage

-a always,exit -F arch=b64 -S mincore -F auid!=-1 -k mincore_usage
-a always,exit -F arch=b32 -S mincore -F auid!=-1 -k mincore_usage

-a always,exit -F arch=b64 -S madvise -F auid!=-1 -k madvise_usage
-a always,exit -F arch=b32 -S madvise -F auid!=-1 -k madvise_usage

# ===== WATCH RULES (Конфигурационные файлы) =====
-w /etc/passwd -p wa -k passwd_changes
-w /etc/group -p wa -k group_changes
-w /etc/shadow -p wa -k shadow_changes
-w /etc/gshadow -p wa -k gshadow_changes
-w /etc/security/opasswd -p wa -k opasswd_changes

-w /etc/ssh/sshd_config -p wa -k sshd_config_changes
-w /etc/ssh/ssh_config -p wa -k ssh_config_changes
```

```
-w /root/.ssh -p wa -k root_ssh_changes
-w /home -p wa -k home_changes

-w /etc/pam.d/ -p wa -k pam_changes
-w /etc/security/pwquality.conf -p wa -k pwquality_changes
-w /etc/security/ -p wa -k security_config_changes

-w /etc/sudoers -p wa -k sudoers_changes
-w /etc/sudoers.d/ -p wa -k sudoers_d_changes

-w /etc/cron.d/ -p wa -k cron_d_changes
-w /etc/cron.daily/ -p wa -k cron_daily_changes
-w /etc/cron.hourly/ -p wa -k cron_hourly_changes
-w /etc/cron.monthly/ -p wa -k cron_monthly_changes
-w /etc/cron.weekly/ -p wa -k cron_weekly_changes
-w /etc/crontab -p wa -k crontab_changes
-w /var/spool/cron/ -p wa -k cron_spool_changes

-w /etc/systemd/ -p wa -k systemd_changes
-w /usr/lib/systemd/system/ -p wa -k systemd_system_changes
-w /lib/systemd/system/ -p wa -k systemd_lib_changes

-w /etc/init.d/ -p wa -k init_d_changes
-w /etc/rc.local -p wa -k rc_local_changes

-w /etc/profile -p wa -k profile_changes
-w /etc/profile.d/ -p wa -k profile_d_changes
-w /etc/bash.bashrc -p wa -k bashrc_changes
-w /etc/zsh/ -p wa -k zsh_changes

-w /etc/hosts -p wa -k hosts_changes
-w /etc/hostname -p wa -k hostname_changes
-w /etc/network -p wa -k network_config_changes
-w /etc/resolv.conf -p wa -k resolv_conf_changes

-w /sbin/insmod -p x -k insmod_execution
-w /sbin/rmmod -p x -k rmmod_execution
-w /sbin/modprobe -p x -k modprobe_execution
-a always,exit -F arch=b64 -S init_module,delete_module,finit_module -k
kernel_module_operations
-a always,exit -F arch=b32 -S init_module,delete_module,finit_module -k
kernel_module_operations

-w /etc/modprobe.conf -p wa -k modprobe_conf_changes
-w /etc/modprobe.d/ -p wa -k modprobe_d_changes

-w /boot -p wa -k boot_changes
-w /boot/grub -p wa -k grub_changes
-w /boot/grub2 -p wa -k grub2_changes

-w /etc/ld.so.preload -p wa -k ld_preload_changes
-w /etc/ld.so.conf -p wa -k ld_so_conf_changes
-w /etc/ld.so.conf.d/ -p wa -k ld_so_conf_d_changes

-a always,exit -F arch=b64 -S open,openat,openat2 -F dir=/tmp -k tmp_library_load
-a always,exit -F arch=b32 -S open,openat -F dir=/tmp -k tmp_library_load

-a always,exit -F arch=b64 -S open,openat,openat2 -F dir=/dev/shm -k shm_library_load
-a always,exit -F arch=b32 -S open,openat -F dir=/dev/shm -k shm_library_load

-w /etc/selinux -p wa -k selinux_changes
-w /usr/sbin/setenforce -p x -k setenforce_execution
-w /usr/sbin/semodule -p x -k semodule_execution
```

```
-w /etc/apparmor -p wa -k apparmor_changes
-w /etc/apparmor.d/ -p wa -k apparmor_d_changes

-w /etc/audit/ -p wa -k audit_config_changes
-w /etc/libaudit.conf -p wa -k libaudit_conf_changes
-w /sbin/auditctl -p x -k auditctl_execution
-w /sbin/auditd -p x -k auditd_execution
-w /var/log/audit/ -p wa -k audit_log_changes

-w /etc/locale.conf -p wa -k locale_changes
-w /etc/localtime -p wa -k localtime_changes

# ===== DANGEROUS TOOLS =====
-w /usr/bin/docker -p x -k docker_execution
-w /var/lib/docker/ -p wa -k docker_data_changes
-w /etc/docker/ -p wa -k docker_config_changes

-w /usr/bin/nc -p x -k nc_execution
-w /usr/bin/ncat -p x -k ncat_execution
-w /usr/bin/socat -p x -k socat_execution
-w /usr/bin/netcat -p x -k netcat_execution

-w /usr/bin/tcpdump -p x -k tcpdump_execution
-w /usr/sbin/tcpdump -p x -k tcpdump_sbin_execution

-w /usr/bin/ssh -p x -k ssh_execution
-w /usr/bin/scp -p x -k scp_execution

-w /usr/bin/sudo -p x -k sudo_execution
-w /usr/bin/su -p x -k su_execution

-w /usr/bin/python3 -p x -k python3_execution
-w /usr/bin/perl -p x -k perl_execution


-e 1
```

Если у вас ОС на базе RPM (Red Hat / CentOS), то в /etc/audit/rules.d/extended.rules помимо правил выше, укажите следующее содержимое:

```
-i
--reset-lost
-a always,exclude -F msgtype=CRYPTO_KEY_USER
-a always,exclude -F msgtype=CRYPTO_SESSION
-a always,exclude -F msgtype=NETFILTER_CFG
-a always,exclude -F msgtype=SYSTEM_RUNLEVEL
-a always,exclude -F msgtype=BPF
-e 1
```

4.2.6.3.3 Настройка плагина syslog для записи логов auditd

В файл `/etc/audit/plugins.d/syslog.conf` внесите следующие изменения:

Для Debian 10, CentOS, Fedora и Ubuntu:

```
# This file controls the configuration of the syslog plugin.
```

```
# It simply takes events and writes them to syslog. The
# arguments provided can be the default priority that you
# want the events written with. And optionally, you can give
# a second argument indicating the facility that you want events
# logged to. Valid options are LOG_LOCAL0 through 7, LOG_AUTH,
# LOG_AUTHPRIV, LOG_DAEMON, LOG_SYSLOG, and LOG_USER.

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

Для Debian 11 и выше:

```
# This file controls the configuration of the syslog plugin.
# It simply takes events and writes them to syslog. The
# arguments provided can be the default priority that you
# want the events written with. And optionally, you can give
# a second argument indicating the facility that you want events
# logged to. Valid options are LOG_LOCAL0 through 7, LOG_AUTH,
# LOG_AUTHPRIV, LOG_DAEMON, LOG_SYSLOG, and LOG_USER.

active = yes
direction = out
path = /sbin/audisp-syslog
type = always
args = LOG_LOCAL6
format = string
```

4.2.6.4 Настройка журналирования bash-команд

Для реализации механизма журналирования может использоваться встроенная переменная `bash PROMPT_COMMAND`, которая выполняется перед выводом приглашения командной строки. Переменная записывает предыдущую выполненную команду в формате `syslog key-value`.

4.2.6.4.1 Подготовка к настройке журналирования bash-команд

Перед выполнением настройки журналирования bash-команд убедитесь, что соблюдены следующие условия:

- получен доступ **root** или права `sudo` для записи в `/etc/profile.d/` ;

- установлен `logger`;
- установлен **Bash** (не zsh, fish и др.) версии 4.3 или выше.

4.2.6.4.2 Шаги по настройке журналирования bash-команд

1. Создайте файл bash-syslog.sh в каталоге `/etc/profile.d`.
2. Укажите в файле следующие настройки:

```
#!/bin/bash

# Логирование всей введённой пользователем строки через syslog (key=value формат)
# Работает только в интерактивных сессиях bash

__audit_logger() {
    local RETVAL=$?
    local CMD="$(history 1 | sed 's/^ *[0-9]* *//')"
    [[ -z "$CMD" && $RETVAL -eq 0 ]] && return
    local ESCAPED_CMD=${CMD//\"/\\\"}

    # Получаем системные данные
    local TS=$(date -u +"%Y-%m-%dT%H:%M:%SZ")
    local USER=$(whoami)
    local LOGIN_USER=$LOGNAME
    local USER_ID=$(id -u)
    local GID=$(id -g)
    local GROUP=$(id -gn)
    local PID=$$
    local HOST=$(hostname)
    local IP=${SSH_CONNECTION%% *}
    IP=${IP:-"local"}
    local TTY=$(tty 2>/dev/null)
    local CWD=$(pwd)
    local SHELL_NAME=$0
    local BASH_VER=$BASH_VERSION

    # Формируем и отправляем лог
    logger -t logger -p user.debug \
        "logger: type=logger_audit_command timestamp=\"$TS\" UID=\"$USER\" AUID=\"$LOGIN_USER\" uid=$USER_ID gid=$GID GID=\"$GROUP\" cwd=\"$CWD\" tty=\"$TTY\" ip=\"$IP\" hostname=\"$HOST\" shell=\"$SHELL_NAME\" bash_version=\"$BASH_VER\" pid=$PID command=\"$ESCAPED_CMD\" exit_code=$RETVAL"
}

# Активируем только в интерактивных сессиях
if [[ $- == *i* ]]; then
    export PROMPT_COMMAND=__audit_logger
fi
```

Где:

- `RETRN_VAL=$?` — сохраняем код возврата предыдущей команды (на всякий случай, можно расширить);
- `logger` — отправляем сообщение в системный журнал;
- `-p user.debug` — используем syslog-фасилити user/debug (по умолчанию попадёт в /var/log/syslog);
- `$(whoami)` — кто выполнил команду.

3. Выдайте разрешение на исполнение этого файла:

```
# sudo chmod +x /etc/profile.d/bash-syslog.sh
```

4. Запустите скрипт:

```
# sudo bash /etc/profile.d/bash-syslog.sh
```

5. Перезапустите экземпляр **Bash**:

```
# exec bash -l
```

4.2.6.4.3 Проверка настройки журналирования bash-команд

Выполните команду:

```
# echo "Test command"
# tail -n 5 /var/log/syslog | grep "user.debug"
```

Ожидаемый результат:

```
<15>Aug 15 14:28:51 deb12-auditd logger: logger: type=logger_audit_command timestamp="2025-08-15T11:28:51Z" UID="root" AUID=\"root\" uid=0 gid=0 GID="root" cwd="/root" tty="/dev/pts/0" ip="172.30.253.1" hostname="deb12-auditd" shell="-bash" bash_version="5.2.15(1)-release" pid=6324 command="ls" exit_code=0
```

4.2.6.4.4 Откат изменений

1. Создайте файл скрипта в любой директории:

```
# nano /tmp/revert-bash-syslog.sh
```

2. Укажите в файле revert-bash-syslog.sh следующие параметры:

```
#!/bin/bash

set -e  # Завершить выполнение при любой ошибке

# Путь к скрипту, который мы создавали для журналирования
HOOK_FILE="/etc/profile.d/bash-syslog.sh"

echo "[!] Откат журналирования bash-команд через syslog..."

# Проверяем наличие файла
if [ -f "$HOOK_FILE" ]; then
    echo "[+] Найден скрипт журналирования: $HOOK_FILE"
    echo "[+] Удаляю..."
    rm -f "$HOOK_FILE"
    echo "Скрипт удалён."
else
    echo "[=] Файл $HOOK_FILE не найден — возможно, уже был удалён."
fi

# На всякий случай очищаем переменную окружения в текущей сессии
unset PROMPT_COMMAND

echo "PROMPT_COMMAND очищен из текущего окружения."

echo "  exec bash -l - выполнение"
echo "  echo \$PROMPT_COMMAND    # ← должно быть пусто"
echo "  Для проверки, что команды больше не журналируются после перезагрузки:"
echo "  tail -f /var/log/syslog | grep logger"
```

3. Установите права на выполнение:

```
# sudo chmod +x /tmp/revert-bash-syslog.sh
```

4. Запустите скрипт:

```
# sudo bash /tmp/revert-bash-syslog.sh
```

5. Перезапустите текущую оболочку:

```
# exec bash -l
```

4.2.6.5 Перезапуск служб

После настройки конфигурации любой службы, её необходимо перезапустить.

Если в ОС используется система инициализации `Upstart`, то выполните команду:

```
# service <Название службы> restart
```

Если System V, то выполните команду:

```
# /etc/init.d/<Название службы> restart
```

4.2.6.6 Настройка брандмауэра

Если используется брандмауэр, то необходимо открыть порт 2671/TCP.

Для этого выполните следующую команду:

- если используется служба `firewalld`:

```
# firewall-cmd --permanent --add-port=2671/tcp
```

- если используется служба `iptables`:

```
# iptables -A OUTPUT -p tcp --dport 2661 -j ACCEPT
```

- если в вашей ОС используется SElinux, то чтобы проверить активен ли он выполните команду

```
# getenforce
```

Если был получен ответ `Permissive`, то служба остановлена; если `Enforcing`, то служба запущена и ее необходимо настроить следующим образом:

```
# semanage port -a -t syslogd_port_t -p tcp 2661
# ausearch -c 'audisp-remote' --raw | audit2allow -M my-audispremote
# semodule -X 300 -i my-audispremote.pp
```

При необходимости можно отключить службу командой:

```
# setenforce 0
```

4.2.6.7 Включение источника на платформе

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Unix/Linux**.

4.2.6.8 Пример файла конфигурации службы syslog-ng

Пример файла `/etc/syslog-ng/syslog-ng.conf`:

```
@version: 3.35
@include "scl.conf"

# Syslog-ng configuration file, compatible with default Debian syslogd
# installation.

# First, set some global options.
#options { chain_hostnames(off); flush_lines(0); use_dns(no); use_fqdn(no);
#          dns_cache(no); owner("root"); group("adm"); perm(0640);
#          stats_freq(0); bad_hostname("^gconfd$"); mark-freq(0);
#};

options {
    flush_lines (0);
    time_reopen (10);
    log_fifo_size (1000);
    chain_hostnames (off);
    use_dns (no);
    dns-cache(no);
    use_fqdn (no);
    create_dirs (no);
    keep_hostname (yes);
    stats-freq(0);
    mark-freq(0);
};

########################
# Sources
########################
# This is the default behavior of sysklogd package
# Logs may come from unix stream, but not from another machine.
#
source s_sys {
       system();
       internal();
};

# If you wish to get logs from remote machine you should uncomment
# this and comment the above source line.
#
#source s_net { tcp(ip(127.0.0.1) port(1000)); };

########################
# Destinations
########################
# First some standard logfile
#
destination d_auth { file("/var/log/auth.log"); };
#destination d_cron { file("/var/log/cron.log"); };
destination d_daemon { file("/var/log/daemon.log"); };
destination d_kern { file("/var/log/kern.log"); };
destination d_lpr { file("/var/log/lpr.log"); };
destination d_mail { file("/var/log/mail.log"); };
destination d_syslog { file("/var/log/syslog"); };
destination d_user { file("/var/log/user.log"); };
destination d_uucp { file("/var/log/uucp.log"); };

# This files are the log come from the mail subsystem.
#
destination d_mailinfo { file("/var/log/mail.info"); };
destination d_mailwarn { file("/var/log/mail.warn"); };
destination d_mailerr { file("/var/log/mail.err"); };

# Logging for INN news system
```

```
#
#destination d_newscrit { file("/var/log/news/news.crit"); };
#destination d_newserr { file("/var/log/news/news.err"); };
#destination d_newsnotice { file("/var/log/news/news.notice"); };

# Some 'catch-all' logfiles.
#
destination d_debug { file("/var/log/debug"); };
destination d_error { file("/var/log/error"); };
destination d_messages { file("/var/log/messages"); };

# The root's console.
#
destination d_mlal { usertty("*"); };

# Virtual console.
#
destination d_cons { file("/dev/console"); };

# The named pipe /dev/xconsole is for the nsole' utility.  To use it,
# you must invoke nsole' with the -file' option:
#
#    $ xconsole -file /dev/xconsole [...]
#
#destination d_xconsole { pipe("/dev/xconsole"); };

# Send the messages to an other host
#
destination d_net { tcp("<IP-адрес агента сбора лог-коллектора>" port
log_fifo_size(1000)); };

# Debian only
#destination d_ppp { file("/var/log/ppp.log"); };

########################
# Filters
########################
# Here's come the filter options. With this rules, we can set which
# message go where.
filter f_dbg { level(debug); };
filter f_info { level(info); };
filter f_notice { level(notice); };
filter f_warn { level(warn); };
filter f_err { level(err); };
filter f_crit { level(crit .. emerg); };

filter f_debug { level(debug) and not facility(auth, authpriv, news, mail); };
filter f_error { level(err .. emerg) ; };
filter f_messages { level(info,notice,warn) and
                    not facility(auth,authpriv,cron,daemon,mail,news); };

filter f_audit { program("audit"); };
#filter f_auth { facility(auth, authpriv) and not filter(f_debug) and not
filter(f_audit); };
filter f_auth { facility(auth, authpriv); };
#filter f_cron { facility(cron) and not filter(f_debug); };
filter f_daemon { facility(daemon) and not filter(f_debug); };
filter f_kern { facility(kern) and not filter(f_debug); };
filter f_lpr { facility(lpr) and not filter(f_debug); };
filter f_local { facility(local0, local1, local3, local4, local5,
                        local6, local7) and not filter(f_debug); };
filter f_mail { facility(mail) and not filter(f_debug); };
#filter f_news { facility(news) and not filter(f_debug); };
filter f_syslog3 { not facility(auth, authpriv, mail) and not filter(f_debug); };
```

```
filter f_user { facility(user) and not filter(f_debug); };
filter f_uucp { facility(uucp) and not filter(f_debug); };

filter f_cnews { level(notice, err, crit) and facility(news); };
filter f_cother { level(debug, info, notice, warn) or facility(daemon, mail); };

#filter f_ppp { facility(local2) and not filter(f_debug); };
filter f_console { level(warn .. emerg); };

########################
# Log paths
########################
log { source(s_sys); filter(f_auth); destination(d_auth); };
#log { source(s_sys); filter(f_cron); destination(d_cron); };
log { source(s_sys); filter(f_daemon); destination(d_daemon); };
log { source(s_sys); filter(f_kern); destination(d_kern); };
log { source(s_sys); filter(f_lpr); destination(d_lpr); };
log { source(s_sys); filter(f_syslog3); destination(d_syslog); };
log { source(s_sys); filter(f_user); destination(d_user); };
log { source(s_sys); filter(f_uucp); destination(d_uucp); };

log { source(s_sys); filter(f_mail); destination(d_mail); };
#log { source(s_sys); filter(f_mail); filter(f_info); destination(d_mailinfo); };
#log { source(s_sys); filter(f_mail); filter(f_warn); destination(d_mailwarn); };
#log { source(s_sys); filter(f_mail); filter(f_err); destination(d_mailerr); };

#log { source(s_sys); filter(f_news); filter(f_crit); destination(d_newscrit); };
#log { source(s_sys); filter(f_news); filter(f_err); destination(d_newserr); };
#log { source(s_sys); filter(f_news); filter(f_notice); destination(d_newsnotice); };
#log { source(s_sys); filter(f_cnews); destination(d_console_all); };
#log { source(s_sys); filter(f_cother); destination(d_console_all); };

#log { source(s_sys); filter(f_ppp); destination(d_ppp); };

log { source(s_sys); filter(f_debug); destination(d_debug); };
log { source(s_sys); filter(f_error); destination(d_error); };
log { source(s_sys); filter(f_messages); destination(d_messages); };

log { source(s_sys); filter(f_console); destination(d_cons); };
log { source(s_sys); filter(f_crit); destination(d_mlal); };

# All messages send to a remote site
#
log { source(s_sys); filter(f_auth); destination(d_net); };

###
# Include all config files in /etc/syslog-ng/conf.d/
###
@include "/etc/syslog-ng/conf.d/*.conf"
```

4.2.6.9 Описание параметров файла auditd.conf

Перечень рекомендуемых параметров конфигурации приведен в таблице:

Ключевое слово	Описание	Debian / Ubuntu	Red Hat / CentOS
local_events	Параметр определяет, необходимо ли службе собирать локальные события	yes	yes
write_logs	Параметр определяет, необходимо ли службе записывать журналы	yes	yes

Ключевое слово	Описание	Debian / Ubuntu	Red Hat / CentOS
log_file	Полный путь к файлу журнала, в котором будут храниться записи аудита	/var/log/audit/audit.log	/var/log/audit/audit.log
log_group	Группа, которая применяется к разрешениям файла журнала	adm	adm
log_format	Формат журнала. Параметр описывает, как информация должна храниться. Доступные значения - RAW - запись аудита будут храниться точно так, как его отправляет ядро; - NOLOG - запись аудита храниться не будет; - ENRICHED - запись аудита будет храниться с обогащением: добавится информация о uid, gid, системных вызовах, архитектуре и адресе сокета перед записью события на диск.	ENRICHED	RAW
flush	Команда сброса данных на диск. Допустимые значения: - none - incremental - data - sync	INCREMENTAL_ASYNC	INCREMENTAL_ASYNC
freq	Сколько записей следует записать перед выполнением команды flush. Доступно только, если flush имеет значение incremental	50	50
max_log_file	Максимальный размер файла журнала, в мегабайтах	8	8
num_logs	Количество сохраняемых файлов журнала	5	5
priority_boost	Необходимое повышение приоритета	4	6
disp_qos	Поведение службы при потерях между службой и диспетчером. Допустимые значения - lossy - блокировать связь; - lossless - не блокировать связь	lossy	параметр не указывается
dispatcher	Это программа, которая запускается службой при запуске. Она будет передавать копии всех событий аудита на стандартный ввод этого приложения. Убедитесь, что вы доверяете приложению, которое вы добавляете в эту строку, поскольку оно запускается с правами root	/sbin/audispd	параметр не указывается
name_format	Формат наименования узлов (node) компьютеров, которые добавляются в поток событий аудита. Допустимые значения: - none - в событие аудита не указывается имя компьютера; - hostname - указывается имя, возвращаемое запросом gethostname - fqd - полное доменное имя компьютера - numeric - тоже что и fqd, но при этом определяется IP-адрес компьютера - user - наименование учетной записи пользователя компьютера	NUMERIC	HOSTNAME
max_log_file_action	Поведение службы при достижении максимального размера файла журнала. Допустимые значения: - ignore - ничего не делать; - syslog - выдать предупреждение в системный журнал; - suspend - прекратить запись; - rotate - последовательно менять журналы для записи; - keep_logs - аналогичен параметру Rotate, за исключением того, что он не использует параметр num_logs. Это предотвращает перезапись журналов аудита	ROTATE	ROTATE
space_left	Количество оставшихся на диске мегабайт, при достижении которых служба будет требовать выполнение параметра space_left_action, поскольку в системе начинает заканчиваться дисковое пространство	75	75
space_left_action	Поведение службы когда в системе начало заканчиваться дисковое пространство. Допустимые значения: - ignore - ничего не делать; - syslog - выдать предупреждение в системный журнал;	SYSLOG	SYSLOG

Ключевое слово	Описание	Debian / Ubuntu	Red Hat / CentOS
	- email - отправить предупреждение на адрес электронной почты, указанный в параметре action_mail_acct и в системный журнал; - exec - выполнить скрипт; - suspend - прекратить запись журналов - single - перевести компьютер в однопользовательский режим - halt - выключить компьютер.		
verify_email	Поведение службы для проверки адреса электронной почты	yes	yes
action_mail_acct	Адрес электронной почты или алиас. Значение по умолчанию - root	root	root
admin_space_left	Количество оставшихся на диске мегабайт, при достижении которых служба будет требовать выполнение параметра admin_space_left_action, поскольку в системе начинает критически не хватать дискового пространства	50	50
admin_space_left_action	Поведение службы, когда в системе начинает критически не хватать дискового пространства. Допустимые значения те же, что и для space_left_action	SUSPEND	SUSPEND
disk_full_action	Какое действие следует предпринять, если служба обнаружила что диск, на который записываются файлы журналов, заполнен. Допустимые значения те же, что и для space_left_action	SUSPEND	SUSPEND
disk_error_action	Какие действия следует предпринять при возникновении ошибки при записи событий аудита на диск или изменении последовательности журналов.	SUSPEND	SUSPEND
use_libwrap	Параметр определяет, следует ли использовать tcp_wrappers для обнаружения попыток подключения с разрешенных компьютеров	yes	yes
tcp_listen_queue	Параметр определяет количество допустимых ожидающих соединений в очереди	5	5
tcp_max_per_addr	Параметр определяет количество разрешенных одновременных подключений с одного IP-адреса	1	1
tcp_client_max_idle	Параметр определяет количество секунд, в течение которых допустимо бездействие клиента (не поступают данные), прежде чем служба подаст жалобу для закрытия неактивного подключения. Значение 0 отключает проверку.	0	0
enable_krb5	Параметр определяет, использовать ли Kerberos 5 для аутентификации и шифрования	no	параметр не указывается
krb5_principal	Это принципал для этого сервера. По умолчанию используется auditd. Учитывая это значение по умолчанию, сервер будет искать ключ с именем вида Auditd/hostname@EXAMPLE.COM, хранящийся в /etc/audit/audit.key, для аутентификации, где имя хоста — это имя хоста сервера, возвращаемое DNS	auditd	auditd
transport	Протокол передачи данных. Если установлено значение TCP, будут использоваться только TCP-соединения в виде открытого текста. Если установлено значение KRB5, для аутентификации и шифрования будет использоваться Kerberos 5	параметр не указывается	tcp
distribute_network	Параметр определяет, используется ли распределенная сеть	no	no
q_depth	Параметр определяет, насколько большой должна быть внутренняя очередь событий аудита	параметр не указывается	1200
overflow_action	Параметр определяет, какое действия нужно предпринять службе при переполнении внутренней очереди. Допустимые значения те же, что и для space_left_action	параметр не указывается	SYSLOG
max_restarts	Параметр определяет, сколько раз служба может попытаться перезапустить вышедший из строя плагин	параметр не указывается	10

Ключевое слово	Описание	Debian / Ubuntu	Red Hat / CentOS
plugin_dir	Параметр определяет путь, по которому установлены плагины.	параметр не указывается	/etc/audit/plugins.d
end_of_event_timeout	Параметр определяет количество секунд, используемое библиотечными процедурами пользовательского пространства auparse() и утилитами aureport(8), ausearch(8) для того, чтобы считать событие завершенным при анализе потока журнала событий.	параметр не указывается	2

4.3 Решения Network Security

При работе по подключению решений Network Security в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.3.1 Checkpoint Firewall (NGFW)

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Checkpoint-Firewall
Номер (Порт)	2511
Вендор	Checkpoint-Firewall
Тип	Log-Exporter
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Подключитесь к консоли Checkpoint Firewall.
2. Переключитесь в режим **expert**:

   ```
   > expert
   ```

3. Создайте конфигурацию отправки журналов:

   ```
   # cp_log_export add name <имя конфигурации> target-server <ip-адрес агента сбора лог-коллектора> target-port <порт, указанный ф профиле сбора> protocol tcp format <формат событий syslog | cef>
   ```

4. Запустите созданную конфигурацию:

   ```
   # cp_log_export restart name <имя конфигурации>r
   ```

5. Если в конфигурации была допущена ошибка, то измените ее:

   ```
   # cp_log_export set name <имя конфигурации> [параметры значения]
   ```

6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Checkpoint-Firewall**.

4.3.2 Checkpoint Firewall (opsec)

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Checkpoint-Firewall-opsec
Номер (Порт)	2510
Вендор	Checkpoint-Firewall
Тип	opsec
Профиль сбора	«Модуль opsec_lea_input»

Внимание! *Для настройки сервера CheckPoint необходим клиент SmartConsole.*

Внимание! *Для приема событий от источника Checkpoint-Firewall-OPSEC используется только агент сбора лог-коллектора для ОС Linux.*

Настройка источника включает в себя следующие шаги:

1. Подготовка объектов в системе "CheckPoint".
2. Настройка сервера "CheckPoint".
3. Включение источника в платформе.

Шаг 1. Подготовка объектов в системе CheckPoint

1. Войдите в веб-интерфейс системы **Checkpoint Firewall** и откройте окно "Object Explorer" (см. «Рис. 163»).

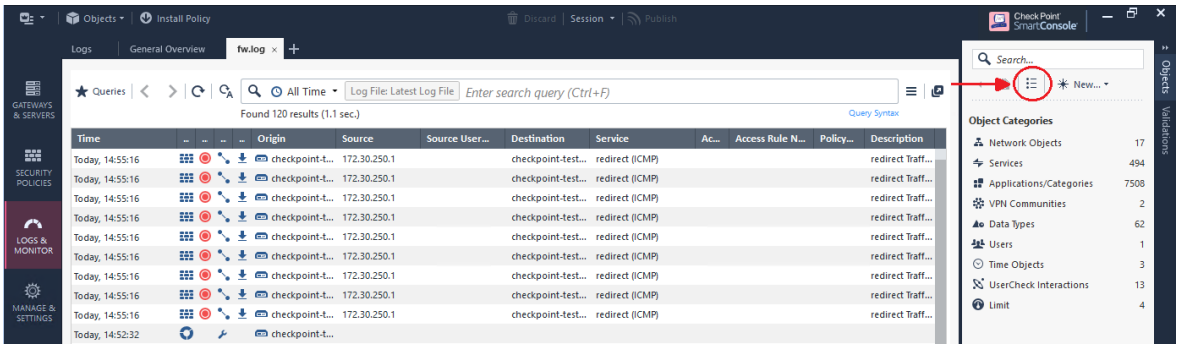


Рис. 163 – Переход в "Object Explorer"

2. В окне "Object Explorer" нажмите кнопку **New** и из категории "Network Object" выберите пункт **Host...**. (см. «Рис. 164»).

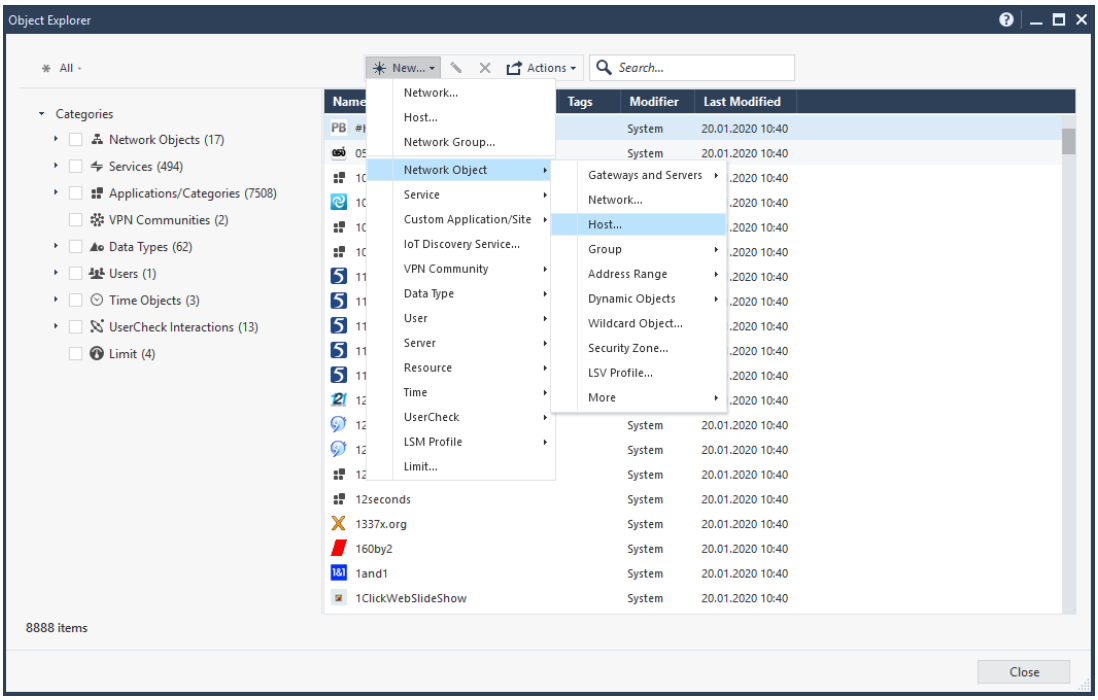


Рис. 164 – Окно "Object Explorer". Вызов окна "New Host"

3. Откроется окно "New Host" (см. «Рис. 165»).

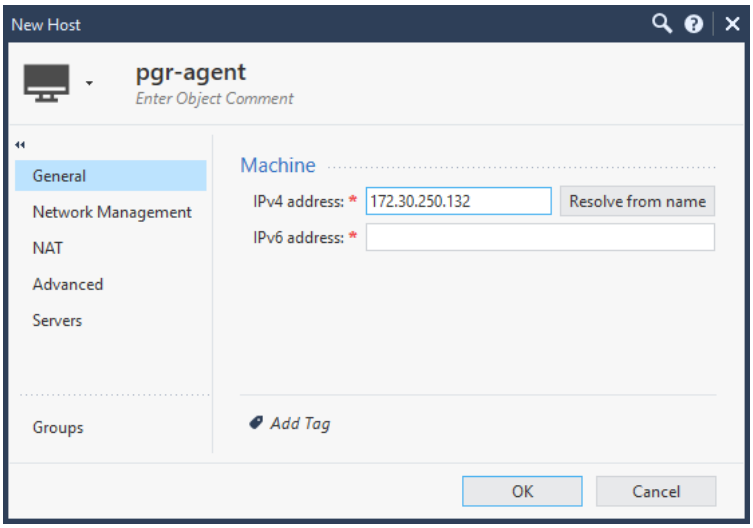


Рис. 165 – Окно "New Host"

4. В окне "New Host" выполните следующие действия:
   - укажите наименование хоста, например "*pgr-agent*";
   - в поле **IPv4 address** укажите IP-адрес агента сбора лог-коллектора;
   - нажмите кнопку **OK**. Хост появится в окне "Object Panel" в разделе **Network Objects – Hosts**.
5. В окне "Object Explorer" нажмите кнопку **New** и из категории "Server" выберите **OPSEC Application → Application** (см. «Рис. 166»).

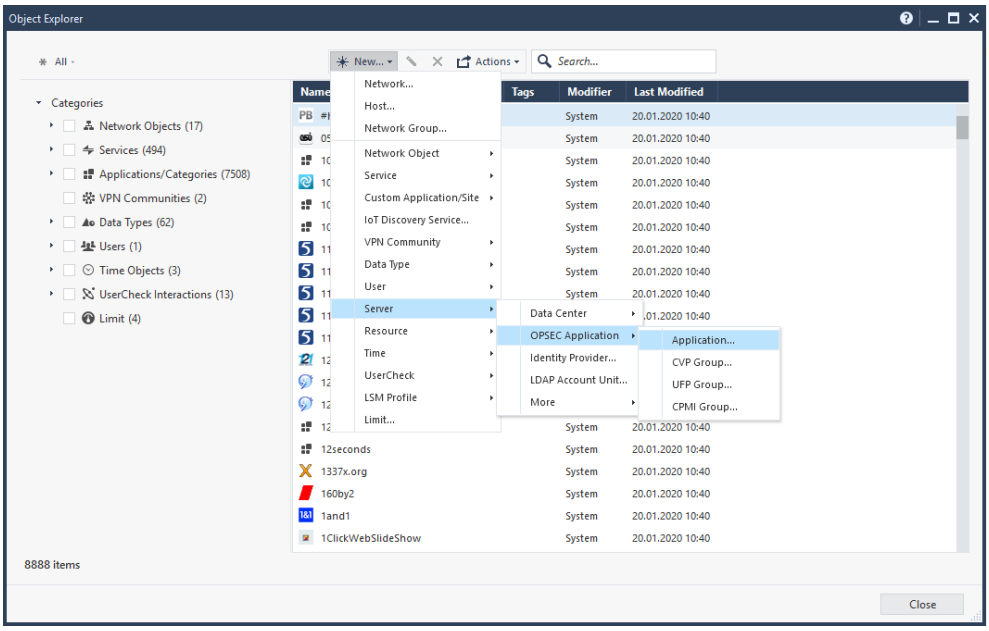


Рис. 166 – Окно "Object Explorer". Вызов окна "OPSEC Application"

6. Откроется окно"OPSEC Application Properties" (см. «Рис. 167»).

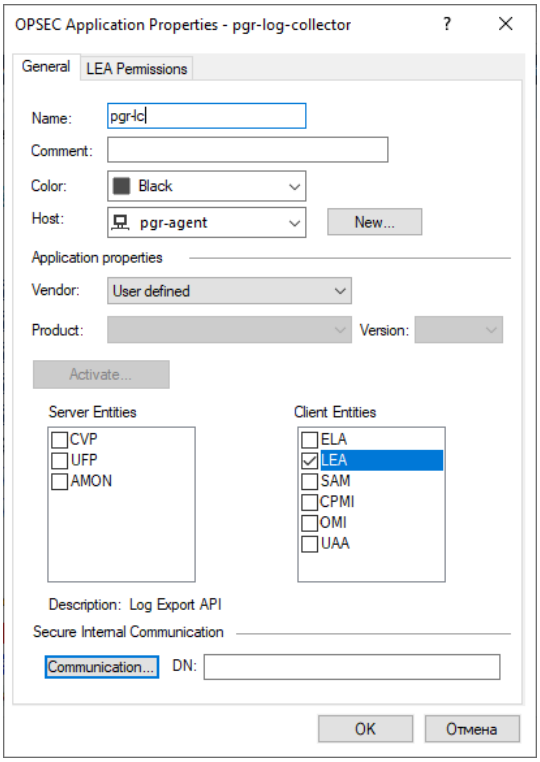


Рис. 167 – Окно "OPSEC Application Properties"

7. В окне выполните следующие действия:

   - в поле **Name** укажите название свойства, например "*pgr-lc*";
   - в поле **Host** из выпадающего списка выберите значение "*pgr-agent*";
   - в таблице **Client Entities** установите флаг "*LEA*";
   - нажмите на кнопку **Communication**. Откроется окно "Communication" (см. «Рис. 168»).

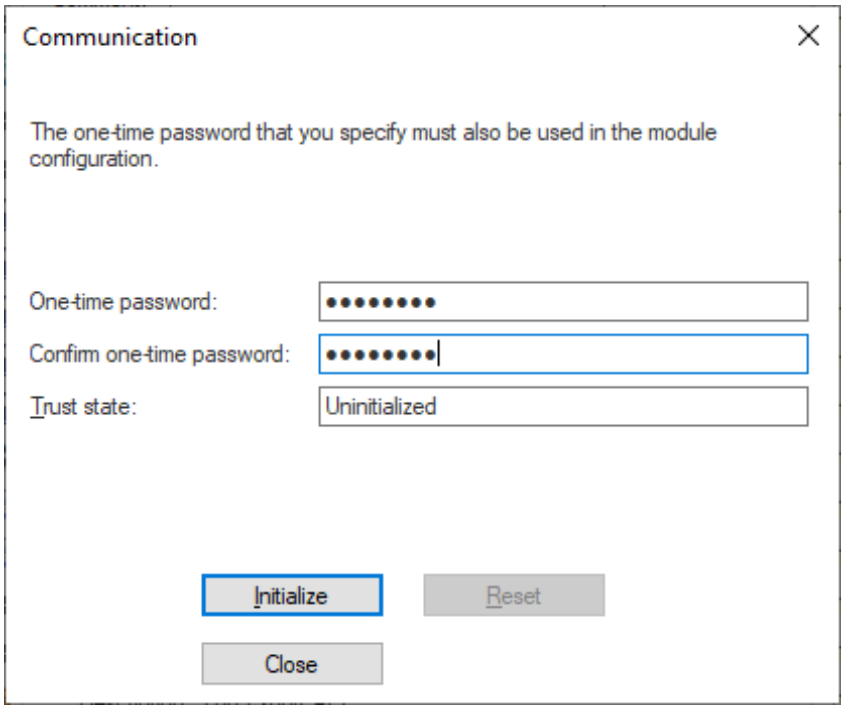


Рис. 168 – Окно "Communication"

- выполните в окне следующие действия:
  - укажите и подтвердите пароль в соответствующих полях;
  - нажмите кнопку **Initialize**.
- нажмите кнопку **OK** и закройте окно "OPSEC Application Properties".

8. Откройте на редактирование созданное ранее свойство **pgr-lc** (см. «Рис. 169») для копирования поля **DN**, так как оно будет использоваться при настройке профиля сбора.

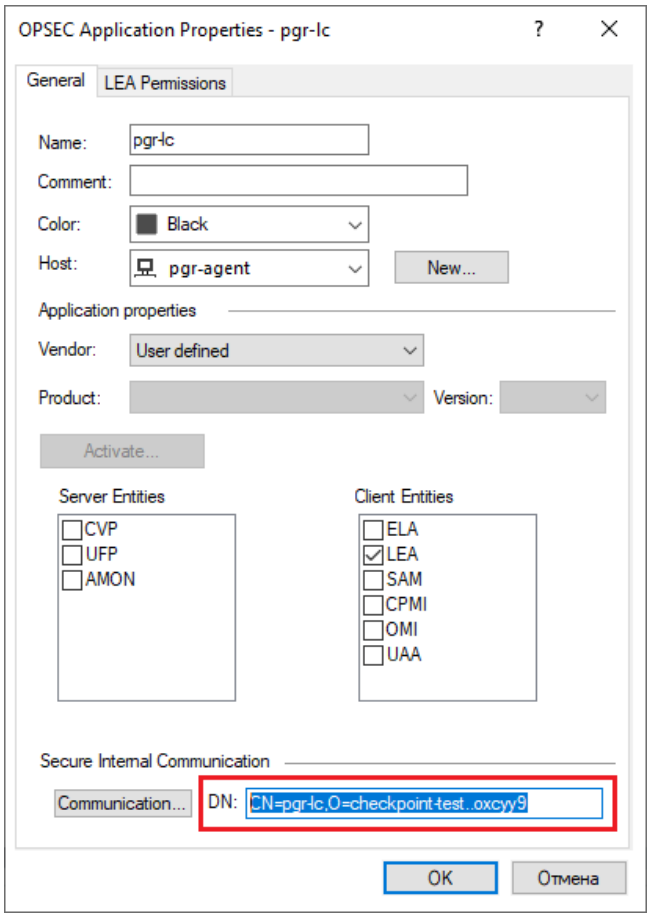


Рис. 169 – Окно "OPSEC Application Properties". Поле "DN" после инициализации

Например:

```
CN=pgr-lc,O=checkpoint-test..oxcyy9
```

9. Опубликуйте внесенные изменения нажав кнопку **Publish** (см. «Рис. 170»).

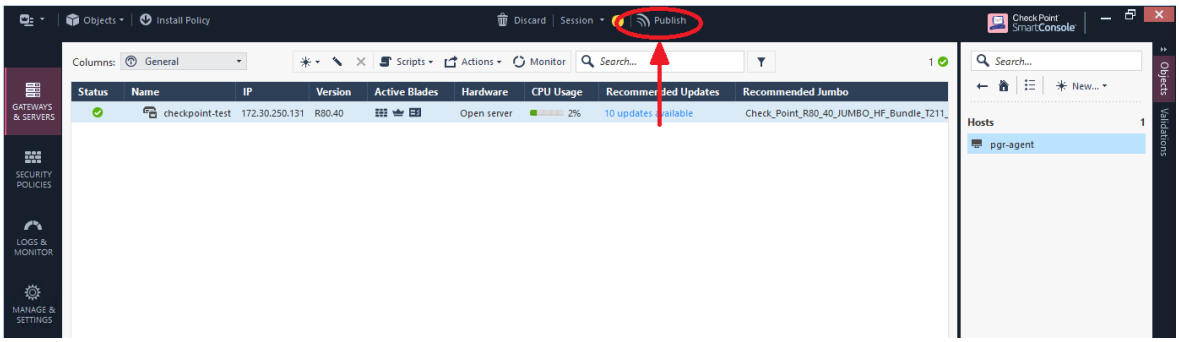


Рис. 170 – Веб-интерфейс системы "Checkpoint Firewall". Кнопка "Publish"

Шаг 2. Настройка сервера "CheckPoint"

При настройке профиля сбора (см. раздел «Модуль opsec_lea_input») потребуется указать значение **DN** сервера "CheckPoint".

Его можно получить, перейдя по пути **C:\Program Files (x86)\CheckPoint \SmartConsole\ R80.40\PROGRAM** и запустив приложение **GuiDBedit.exe**.

Далее перейдите в ветку **Table – Network Objects – network_objects** и выберите в столбце **Object Name** имя сервера "CheckPoint".

Откроется таблица объекта. В столбце **Field Name** найдите строку **sic_name** и скопируйте значение из столбца **Value** (см. «Рис. 171»).

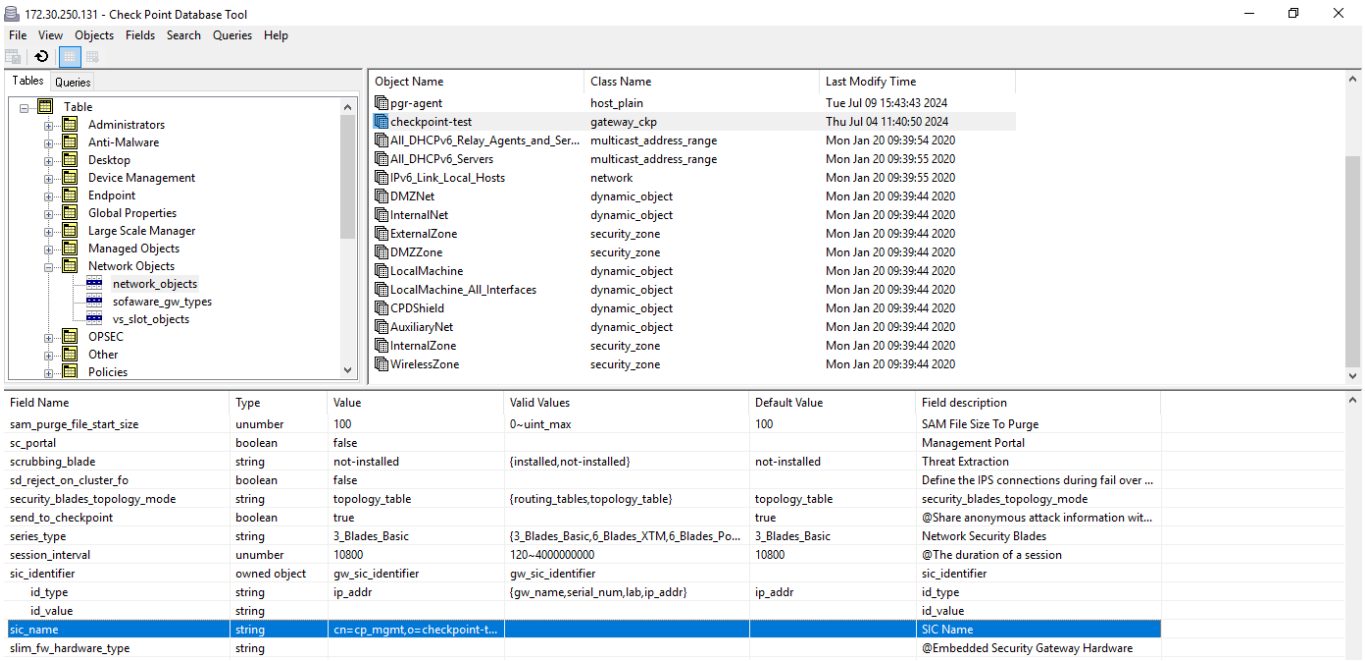


Рис. 171 – Получение "DN" сервера "CheckPoint"

Это значение и является DN сервера, например:

```
cn=cp_mgmt,o=checkpoint-test..oxcyy9
```

Выполните настройку подключения, межсетевого экранирования и журналирования:

1. Подключитесь по SSH к серверу, перейдите в режим **expert** и откройте файл `$FWDIR/conf/fwopsec.conf` на редактирование:

   ```
   > expert
   # vi $FWDIR/conf/fwopsec.conf
   ```

2. Укажите в файле следующие настройки:

   ```
   lea_server port 0
   lea server auth_port 18184
   lea server auth_type sslca
   ```

3. Сохраните изменения и перезапустите сервис:

   ```
   # cpstop
   # cpstart
   ```

4. Создайте правила межсетевого экранирования, разрешающие трафик по портам TCP/18184 и TCP/18210. По порту TCP/18210 происходит получение сертификата с сервера CheckPoint агентом сбора лог-коллектора. По порту TCP/18184 будет идти траффик в направлении от агента сбора лог-коллектора к серверу CheckPoint. После настройки правил нажмите кнопку **Install Policy** (см. «Рис. 172»).

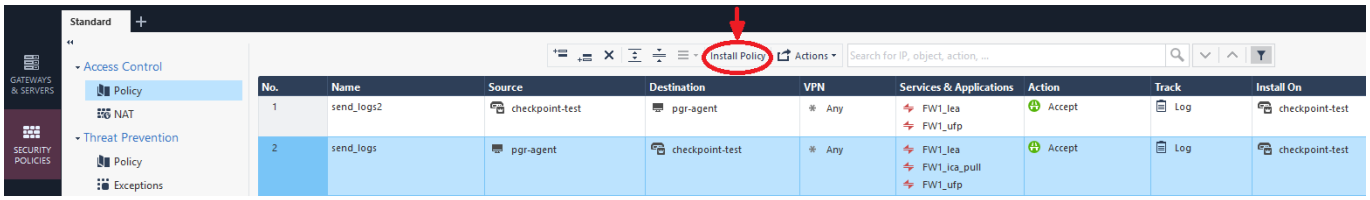


Рис. 172 – Получение "DN" сервера "CheckPoint"

5. Откройте политику на редактирование и в столбце **Track** установите значение "*Log*".

Шаг 3. Включение источника в платформе

Для установления соединения SIC между агентом сбора лог-коллектора и сервером CheckPoint необходимо скопировать сертификат ранее созданного объекта приложения **OPSEC pgr-lc** с сервера при помощи утилиты **opsec-tools** для ОС Linux.

Утилиту необходимо установить на узел, где расположен агент сбора лог-коллектора.

Получить утилиту можно по ссылке.

После установки утилиты выполните следующие действия:

1. Импортируйте сертификат:

   ```
   # ./opsec_pull_cert -h <IP-адрес сервера> -n <Название приложения OPSEC> -p <Пароль для входа в приложение OPSEC>
   ```

2. Сертификат `opsec.p12` появится в текущей директории.

   Внимание! *При попытке выполнить команду может возникнуть ошибка -bash: opsec_pull_cert: command not found или -bash: ./opsec_pull_cert: No such file or directory. Одним из возможных решений, может быть, установка недостающих библиотек: # dpkg --add-architecture i386 # apt-get update # apt-get install libstdc++6:i386 libgcc1:i386 libc6-i386 libpam-modules:i386*

3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Checkpoint-Firewall-opsec**.

4.3.3 Cisco ASA

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Cisco-ASA
Номер (Порт)	2520
Вендор	Cisco
Тип	ASA
Профиль сбора	«Модуль udp_input»

Внимание! *Все команды по настройке источника выполняются в* ***режиме глобальной конфигурации****. Для этого перейдите в привилегированный режим: введите enable и пароль администратора. В консольной строке знак > рядом с именем хоста сменится на #. Затем введите команду #configure terminal. В консольной строке знак # рядом с именем хоста сменится на (config)#.*

Для настройки источника выполните следующие действия:

1. Подключитесь к консоли устройства и перейдите в режим глобальной конфигурации.
2. Включите журналирование и экспорт событий с устройства:

```
(config)# logging enable
(config)# logging host <имя интерфейса> <IP-адрес агента сбора лог-коллектора>
(config)# logging trap <уровень логирования> (указать один из уровней важности
событий: alerts, critical, debugging, emergencies, errors, informational,
notifications, warnings)
(config)# logging console <уровень логирования> (указать один из уровней
важности событий: alerts, critical, debugging, emergencies, errors,
informational, notifications, warnings)
(config)# logging asdm <уровень логирования> (указать один из уровней важности
событий: alerts, critical, debugging, emergencies, errors, informational,
notifications, warnings)
(config)# logging device-id ipaddress <id устройства>
(config)# logging timestamp
```

3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Cisco-ASA**.

4.3.4 Fortinet FortiAnalyzer

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Fortinet-Fortianalyzer
Номер (Порт)	2572
Вендор	Fortinet
Тип	Analyzer
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс системы под учетной записью с правами администратора.
2. Перейдите в раздел **Advanced → Syslog Server** (см. «Рис. 173»).

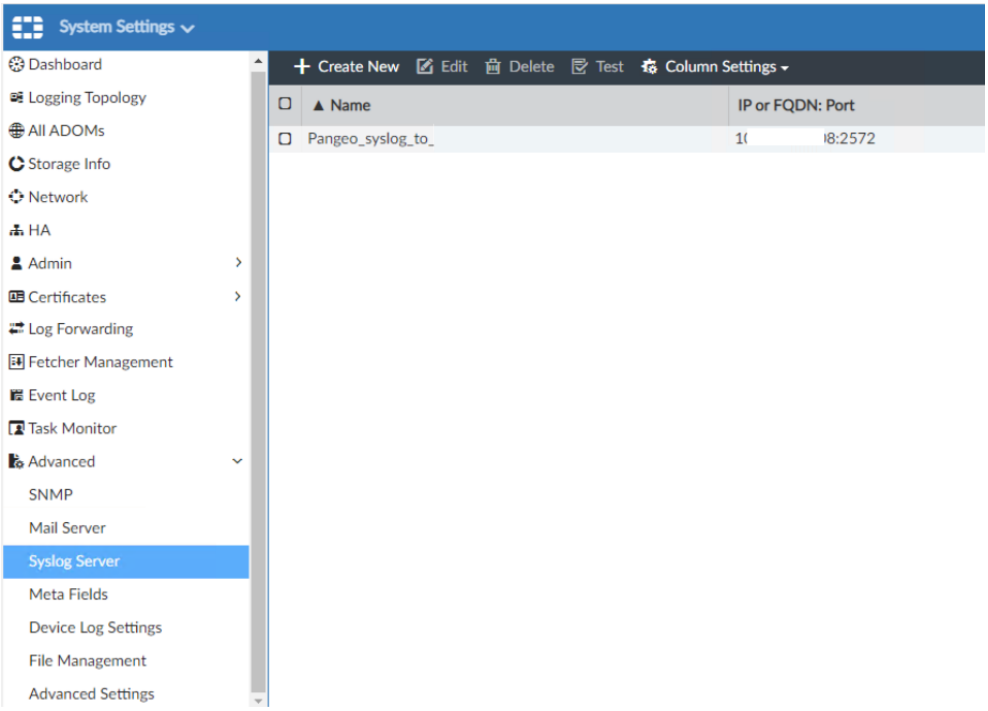


Рис. 173 – System Setting. Syslog Server

3. Нажмите кнопку **Create New**. Откроется окно "Create New Server Setting" (внешний вид окна аналогичен окну "Edit Syslog Server Setting" см. «Рис. 174»).

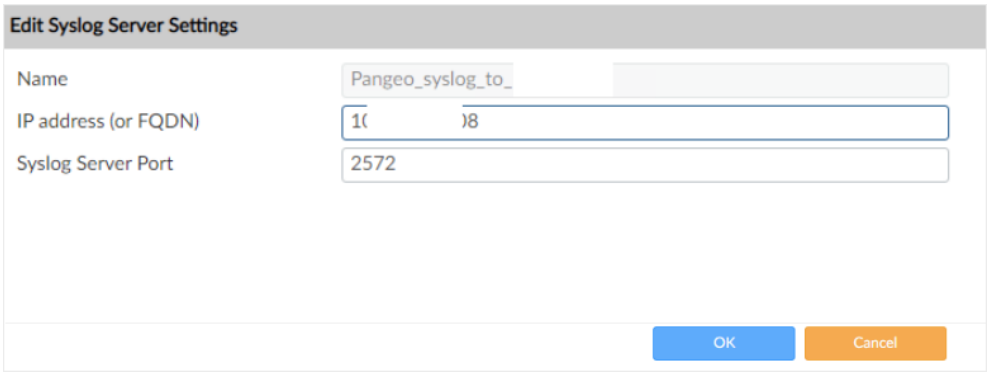


Рис. 174 – Окно "Edit Syslog Server Setting"

4. В открывшемся окне укажите следующие настройки:
   - в поле **Name** укажите название сервера;
   - в поле **IP-address (or FQDN)** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Syslog Server Port** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - нажмите кнопку **OK**.
5. Перейдите в раздел **Log Forwarding** и нажмите кнопку **Create New**. Откроется окно "Create New Log Forwarding" (см. «Рис. 175»).

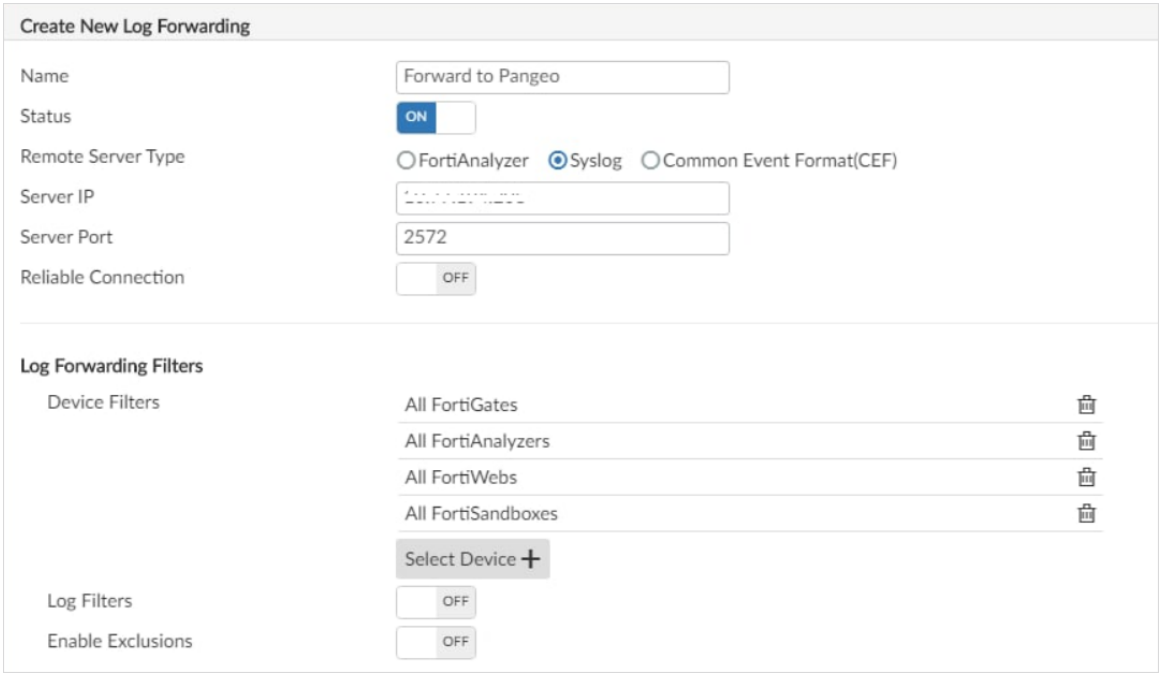


Рис. 175 – Окно "Create New Log Forwarding"

6. В открывшемся окне укажите следующие настройки:
   - в поле **Name** укажите наименование настройки;
   - в поле **Status** установите переключатель в положение **ON**;
   - в поле **Remote Server Type** выберите тип формата отправляемых журналов (рекомендуемое значение: "Syslog");
   - в поле **Server IP** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Server Port** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - в блоке **Device Filters** добавьте устройства, с которых будут пересылаться события;
   - нажмите кнопку **OK**.
7. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Fortinet-Fortianalyzer**.

4.3.5 Fortinet FortiSandbox

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Fortinet-Fortisandbox
Номер (Порт)	2574
Вендор	Fortinet

Характеристика	Значение
Тип	Sandbox
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс системы **FortiSandbox** под учетной записью с правами администратора.
2. Перейдите в раздел **Log&Report → Log Servers** (см. «Рис. 176»).

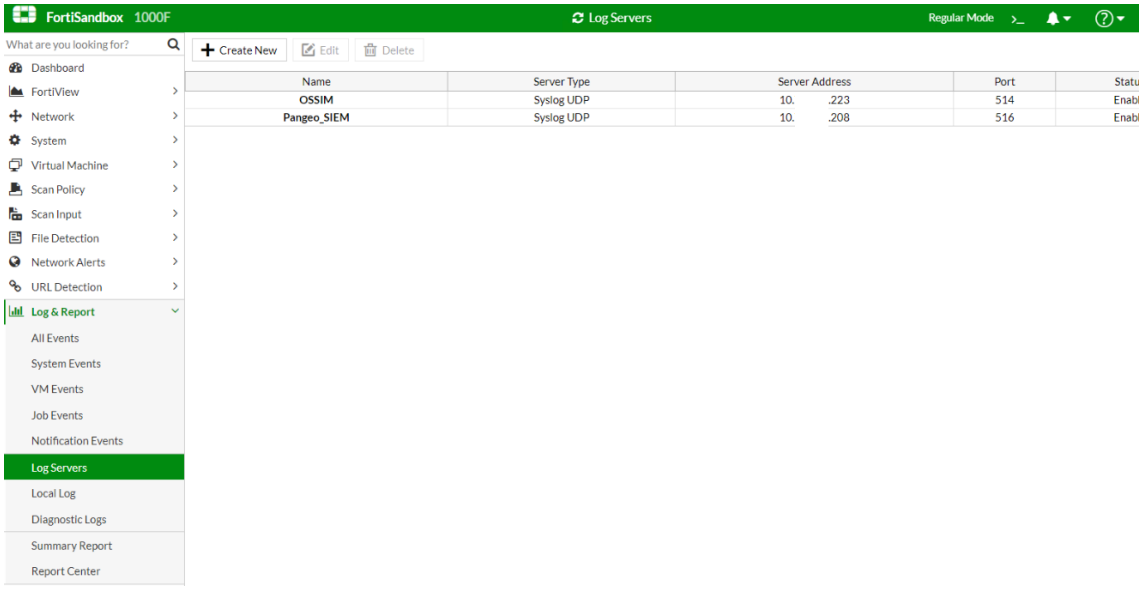


Рис. 176 – FortiSandbox. Раздел "Настройка журналов"

3. Нажмите кнопку **Create New** и в открывшемся окне (см. «Рис. 177») укажите следующие настройки:

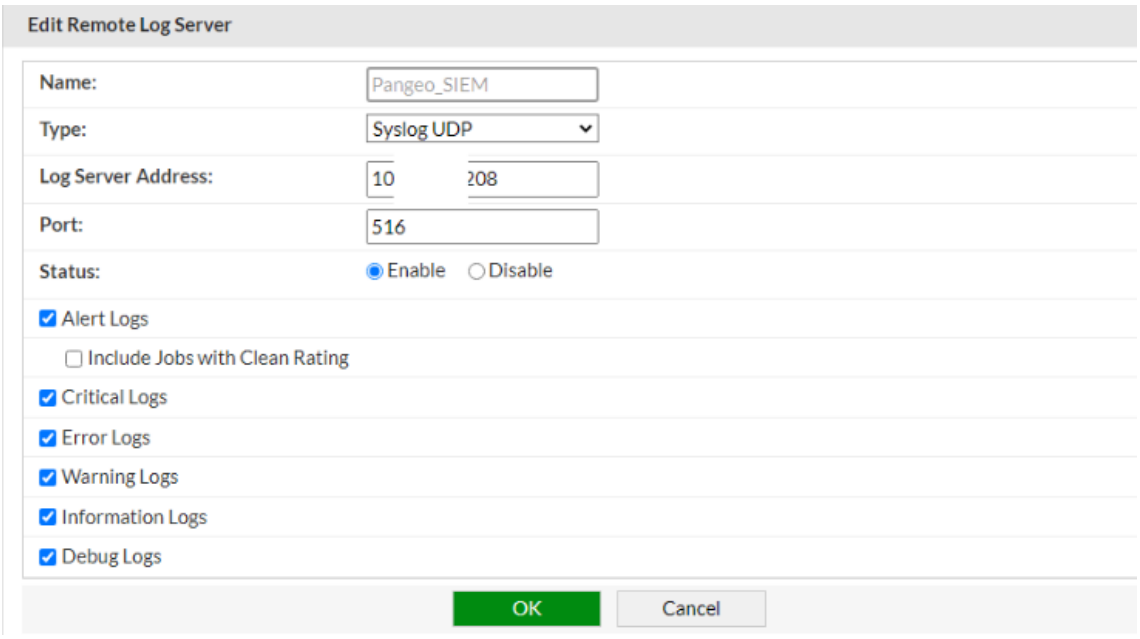


Рис. 177 – Окно "Edit Remote Log Server"

- в поле **Name** укажите наименование сервера;
- в поле **Type** выберите протокол взаимодействия и формат отправки событий;
- в поле **Log Server Address** укажите IP-адрес агента сбора лог-коллектора;
- в поле **Port** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
- в поле **Status** выберите значение Enable;
- выберите уровни логирования, установив соответствующие флаги;
- нажмите кнопку **OK**.

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Fortinet-Fortisandbox**.

4.3.6 Fortinet FortiWeb

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Fortinet-Fortisandbox
Номер (Порт)	2574
Вендор	Fortinet
Тип	Sandbox
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс системы **Fortiweb** и перейдите в раздел **Log&Report → Log Policy → SIEM Policy**.
2. Нажмите кнопку **Create New**.
3. При создании политики укажите следующие настройки:
   - в поле **Policy Type** выберите значение **ArcsSight CEF**;
   - в поле **IP Address(IPv4)** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Por**t укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - нажмите кнопку **OK**.
4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Fortinet-Fortiweb-WAF**.

4.3.7 HAProxy

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	HAProxy
Номер (Порт)	3020
Вендор	HAProxy
Тип	Proxy
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Откройте файл `/etc/haproxy/haproxy.cfg` и выполните следующие настройки:
   - в секцию `global` добавьте строку:

     ```
     log /dev/log local1 info
     ```

   - в секцию `default` добавьте следующие строки:

     ```
     log global
     mode    http
     option  httplog
     log-format "%ci:%cp %fi:%fp %bi:%bp [%tr] %ft %b/%s %TR/%Tw/%Tc/%Tr/%Ta ST=%ST %B %CC %CS %tsc %ac/%fc/%bc/%sc/%rc %sq/%bq URI=%HQ%{+Q}r"
     ```

2. Чтобы события HAProxy сохранялись в файл `/var/log/haproxy.log`, система автоматически создает файл `/etc/rsyslog.d/49-haproxy.conf`. Если файл не был создан, его необходимо создать вручную и наполнить следующим содержимым:

   ```
   $AddUnixListenSocket /var/lib/haproxy/dev/log
   :programname, startswith, "haproxy" {
     /var/log/haproxy.log
    stop
   }
   ```

3. Чтобы события HAProxy отправлялись на агент сбора лог-коллектора, необходимо создать файл `/etc/rsyslog.d/60-haproxy-siem.conf` и вставить следующие строки, указав IP-адрес агента сбора лог-коллектора и порт, указанный в соответствующем профиле сбора:

   ```
   module(load="imfile" PollingInterval="5")
   input(type="imfile"
         reopenOnTruncate="on"
         File="/var/log/haproxy.log"
         Tag="haproxy"
         ruleset="sendlc")
   template(
   ```

```
    name = "logtemplate"
    type = "string"
    string = "<%PRI%> %msg%\n"
)
ruleset(name="sendlc")
{
    action(type = "omfwd"
        Template = "logtemplate"
        Target="<IP-адрес агента сбора лог-коллектора>"
        Port="<порт, указанный в профиле сбора>"
        Protocol="tcp"
        ResendLastMSGOnReconnect="on"
        action.resumeRetryCount="100"
        queue.type="linkedList"
        queue.size="10000")
    stop
}
```

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **HAProxy**.

4.3.8 Kaspersky Web Traffic Security

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Kaspersky-Web-Traffic-Security
Номер (Порт)	2606
Вендор	Kaspersky
Тип	Proxy
Профиль сбора	«Модуль tcp_input»

Примечание: *данную инструкцию необходимо выполнить на каждом узле кластера Kaspersky Web Traffic Security*.

Для настройки источника выполните следующие действия:

1. Подключитесь к устройству Kaspersky Web Traffic Security с помощью интерфейса командной строки под пользователем root.
2. Создайте конфигурационный файл для службы rsyslog:

   ```
   vim /etc/rsyslog.d/kwts_to_siem.conf
   ```

3. Настройте отправку следующих объектов:

   ```
   local0.*,local1.*,local2.*,authpriv.*,local7.* @@<Ip-адрес агента сбора лог-коллектора>:<порт, указанный в профиле сбора>
   ```

4. Сохраните изменения и перезапустите службу `rsyslog`.

   ```
   # service rsyslog restart
   ```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Kaspersky-Web-Traffic-Security**.

4.3.9 McAfee Web Gateway

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Kaspersky-Web-Traffic-Security
Номер (Порт)	2606
Вендор	Kaspersky
Тип	Proxy
Профиль сбора	«Модуль tcp_input» «Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в интерфейс системы под учетной записью с правами администратора.
2. Перейдите в раздел **Policy**, затем выберите вкладку «Rule Sets» и пункт меню «Log Handler» (см. «Рис. 178»).

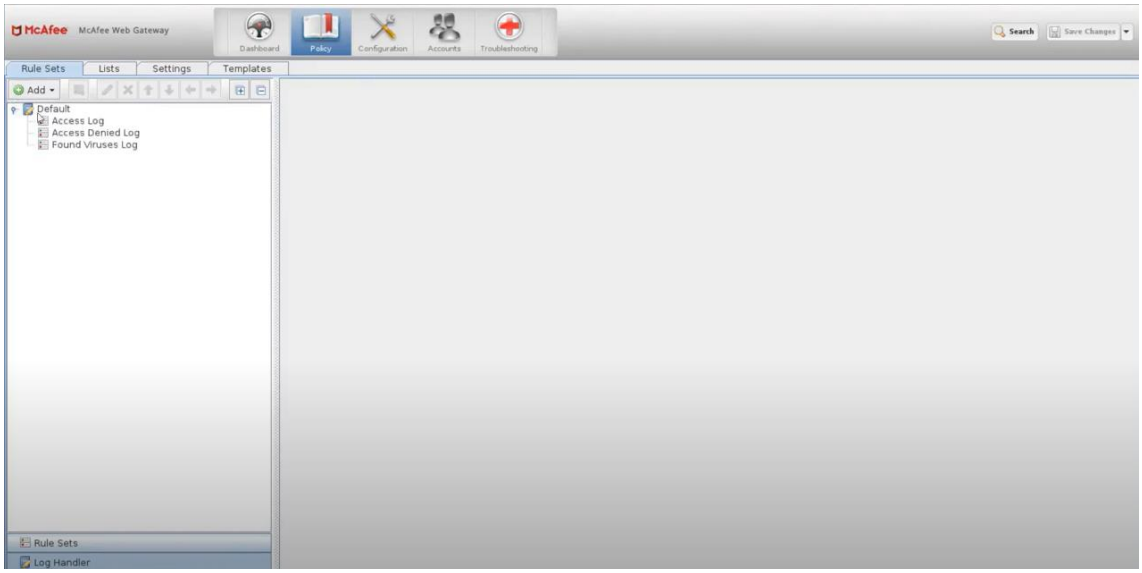


Рис. 178 – Выбор логов

3. Раскройте список «Default», выберите «Access Log», в правой части окна выделите правило и нажмите кнопку **Edit**.
4. В секции «Events» нажмите кнопку **Add**, а затем **Event**.
5. Выберите «Syslog (Number, String)» и нажмите кнопку **Parameters**.
6. Для параметра «1. Level (Number)» установите значение **6**, что указывает на уровень логирования «Informational». Для настройки параметра «2. Message (String)» нажмите **Use Property** и выберите «User-Defined.logLine».

7. Нажмите последовательно кнопки **OK → OK → Finish**.
8. Повторите действия п.п. 3-7 для других наборов правил.
9. Перейдите в раздел **Configuration** и выберите вкладку «File Editor».
10. Разверните список с именем соответствующего устройства и выберите файл rsyslog.conf (см. «Рис. 179»).

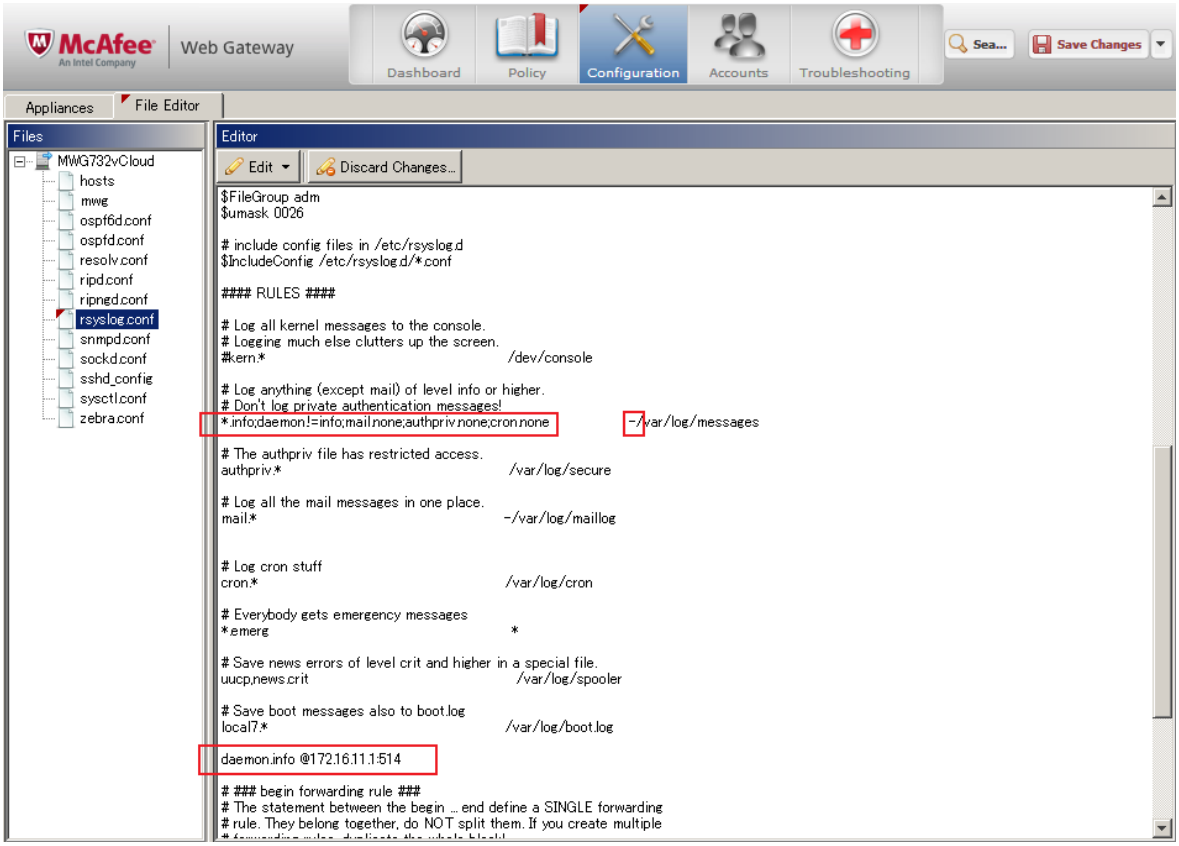


Рис. 179 – Редактирование rsyslog

11. Найдите в файле следующую строку:

    ```
    *.info;mail.none;authpriv.none;cron.none  /var/log/messages
    ```

    Добавьте в нее параметр «daemon.!=info»:

    ```
    *.info;daemon.!=info;mail.none;authpriv.none;cron.none  -/var/log/messages
    ```

    Также добавьте следующую строку для отправки событий на агент сбора лог-коллектора (@ - отправка по протоколу UDP, @@ - отправка по протоколу TCP):

    ```
    daemon.info @<ip-адрес агента сбора лог-коллектора>:<порт, указанный в профиле сбора>
    ```

12. Нажмите кнопку **Save Changes** для сохранения изменений.
13. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **McAfee-Web-Gateway**.

4.3.10 Microsoft Forefront TMG

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Microsoft-Forefront-Threat-Management-Gateway
Номер (Порт)	1540
Вендор	Microsoft
Тип	Firewall_Proxy
Профиль сбора	«Модуль smb_input»

Для настройки источника выполните следующие действия:

1. Войдите в интерфейс управления системой Forefront TMG Management.
2. Перейдите в раздел **Log & Reports** и откройте вкладку "Logging" (см. «Рис. 180»).

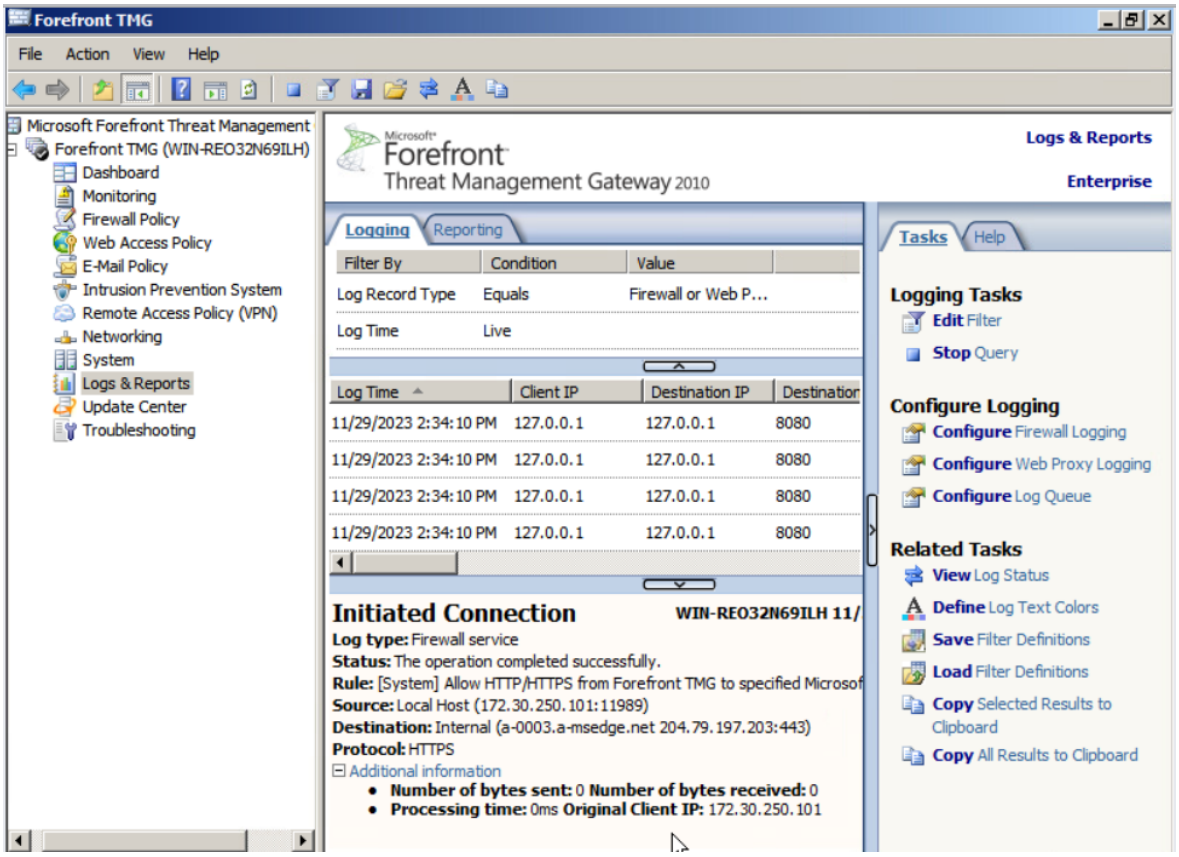


Рис. 180 – Forefront TMG. Раздел "Log & Reports"

3. В рабочей области справа перейдите на вкладку "Task" и нажмите кнопку **Configure Firewall Logging**. Откроется окно "Firewall Logging Properties" (см. «Рис. 181»).

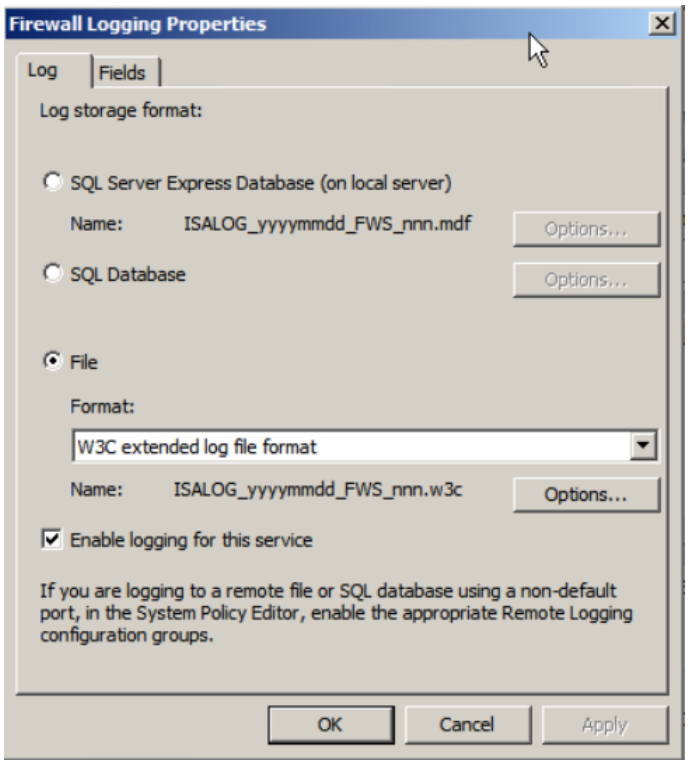


Рис. 181 – Окно "Firewall Logging Properties"

4. На вкладке "Log" выполните следующие действия:
   - в поле **Log storage format** выберите значение "*File*";
   - в поле **Format** из выпадающего списка выберите значение "*W3C*";
   - нажмите кнопку **Options**. Откроется окно "Options" (см. «Рис. 182»);

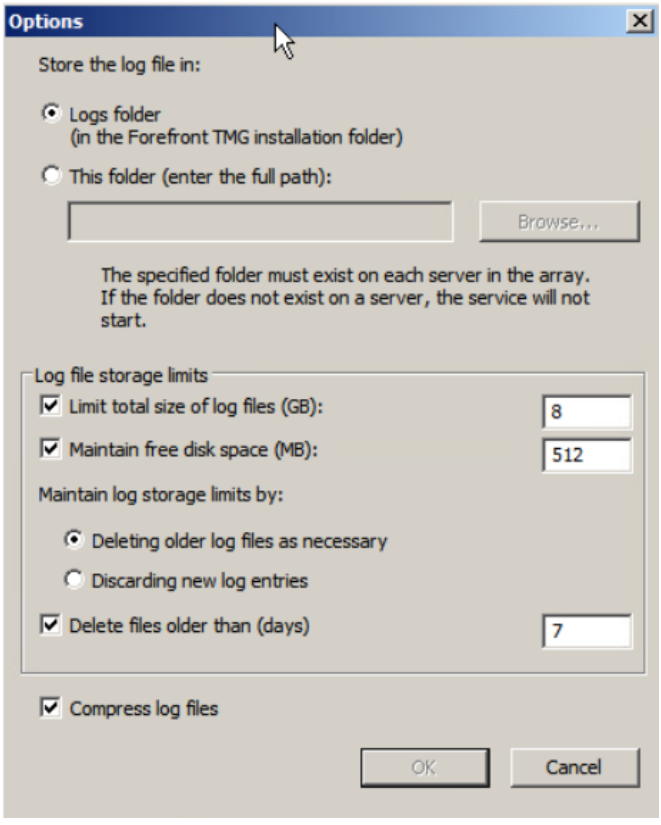


Рис. 182 – Firewall Logging Properties. Options

- в окне "Options" выполните следующие действия:
  - в поле **Store the log file in** выберите каталог хранения журнала;
  - в блоке **Log file storage limits** настройте необходимые лимиты для хранения файла с журналом;
  - нажмите кнопку **OK**.
- нажмите кнопку **OK**.

5. На вкладке "Task" нажмите кнопку **Configure Web Proxy Logging**. Откроется окно "Web Proxy Logging Properties" (см. «Рис. 183»).

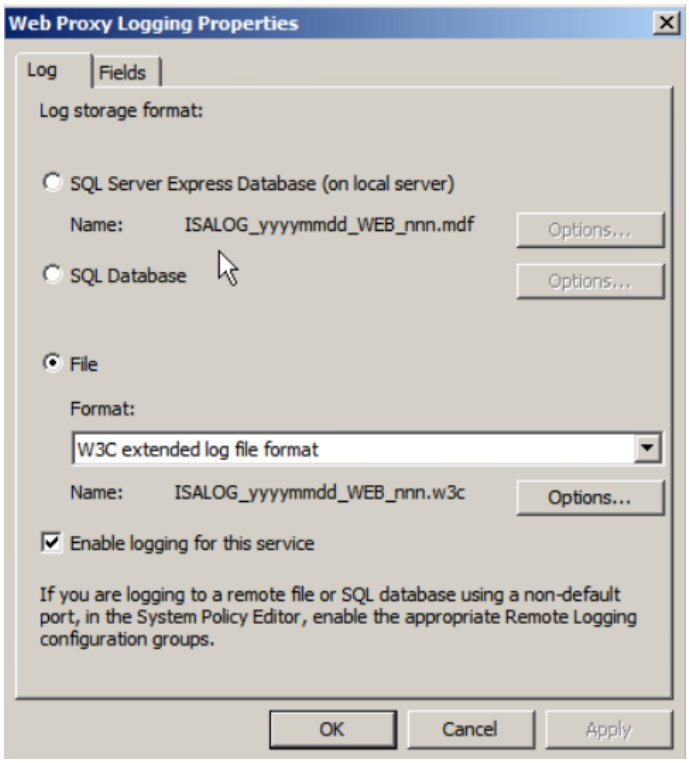


Рис. 183 – Окно "Web Proxy Logging Properties"

6. На вкладке "Log" выполните следующие действия:
   - в поле **Log storage format** выберите значение "*File*";
   - в поле **Format** из выпадающего списка выберите значение "*W3C*";
   - нажмите кнопку **Options**. Откроется окно "Options" (см. «Рис. 184»);

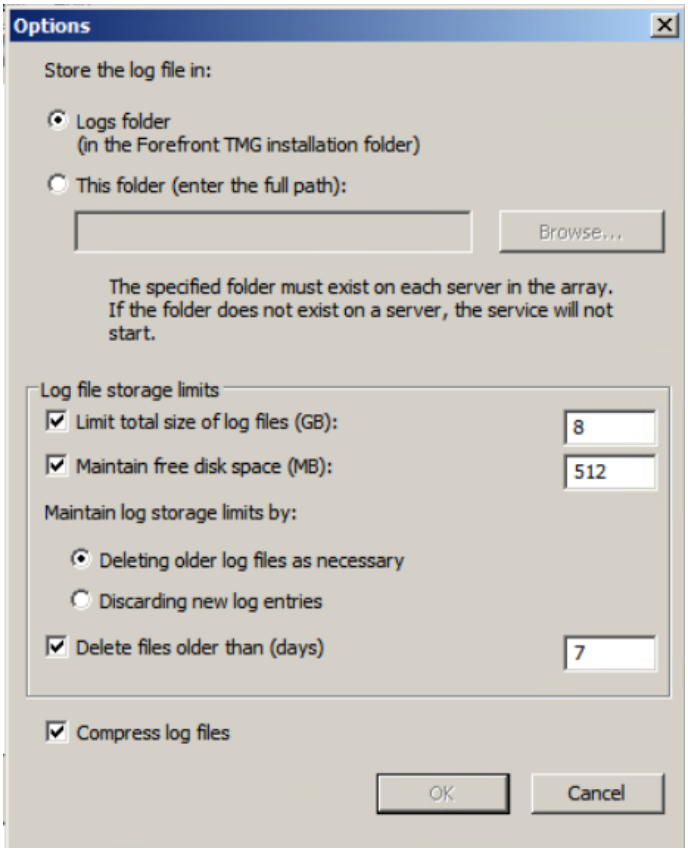


Рис. 184 – Web Proxy Logging Properties. Options

- в окне "Options" выполните следующие действия:
  - в поле **Store the log file in** выберите каталог хранения журнала;
  - в блоке **Log file storage limits** настройте необходимые лимиты для хранения файла с журналом;
  - нажмите кнопку **OK**.
- нажмите кнопку **OK**.

7. Нажмите кнопку **Apply** (см. «Рис. 185»).

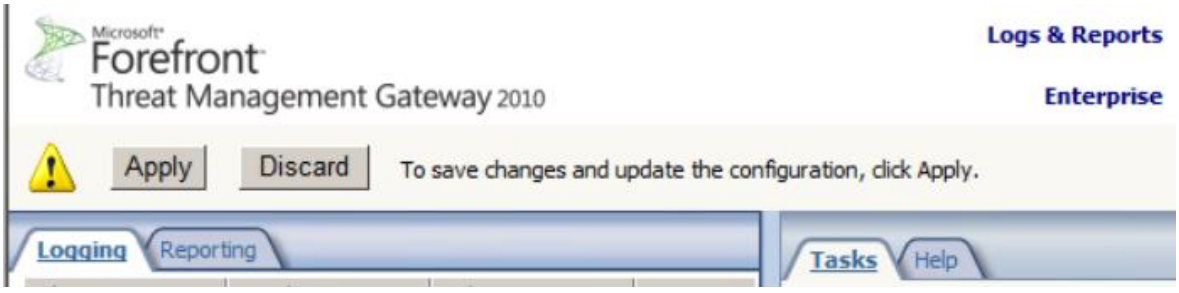


Рис. 185 – Forefront TMG. Кнопка "Apply"

8. Откройте сетевой доступ к каталогам, указанным в пп. 5 и 6.
9. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Forefront-Threat-Management-Gateway**.

4.3.11 Ngate CryptoPro VPNGate

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	CryptoPro-VPNGate-Ngate
Номер (Порт)	2562
Вендор	CryptoPro
Тип	VPNGate
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Настройте отправку журналов с помощью `rsyslog`:
   - перейдите в директорию `/etc/rsyslog.d/`;
   - откройте файл конфигурации `50-ng-manual-fwd.conf`;
   - закомментируйте содержимое и вставьте следующую информацию:

     ```
     module(load="imfile" PollingInterval="10")
     input(type="imfile"
           reopenOnTruncate="on"
           File="/var/log/ngate/ng-admin/ng-admin.log"
           Tag="ng-admin")
     if $syslogtag == 'ng-admin' then @<ip-адрес агента сбора лог коллектора>IP:<порт, указанный в профиле сбора>
     & stop
     ```

   - перезапустите службу `rsyslog`.
2. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **CryptoPro-VPNGate-Ngate**.

4.3.12 OpenVPN

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	OpenVPN
Номер (Порт)	2180
Вендор	Openvpn
Тип	VPN
Профиль сбора	«Модуль udp_input»

Файлы журналов источника содержат следующую информацию:

- /`var/log/openvpn/openvpn.log` - содержит информацию о подключениях к виртуальной частной сети (VPN);
- `/var/log/openvpn/status.log` - содержит информацию о каждом клиентском подключении, такую как IP-адрес клиента, используемый протокол, отправленные и полученные байты.

Для настройки источника выполните следующие действия:

1. В файл конфигурации OpenVPN (`/etc/openvpn/server.conf` или `/etc/openvpn/client.conf`) добавьте следующие настройки:

   ```
   status /var/log/openvpn/status.log
   log /var/log/openvpn.log
   log-append /var/log/openvpn.log
   verb 3
   ```

2. В каталоге `/etc/rsyslog.d/` создайте файл конфигурации для службы `rsyslog`:

   ```
   # sudo nano /etc/rsyslog.d/openvpn.conf
   ```

3. Настройте конфигурацию:

   ```
   module(load="imfile" PollingInterval="10")
   input(type="imfile"
         reopenOnTruncate="on"
         File="/var/log/openvpn/openvpn.log"
         Tag="standart_openvpn_log")
   if $syslogtag == 'standart_openvpn_log' then @<ip-адрес агента сбора лог-
   коллектора>:port
   & stop
   input(type="imfile"
         reopenOnTruncate="on"
         File="/var/log/openvpn/status.log"
         Tag="status_openvpn_log")
   if $syslogtag == 'status_openvpn_log' then @<ip-адрес агента сбора лог-
   коллектора>:port
         & stop
   ```

   Где:

   - `<ip-адрес агента сбора лог коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

4. Перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog
   ```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **OpenVPN**.

4.3.13 PaloAlto NGFW

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	PaloAlto-Firewall
Номер (Порт)	2580
Вендор	PaloAlto
Тип	Firewall
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в интерфейс устройства PaloAlto под учетной записью с правами администратора.
2. Перейдите в раздел **Device → Setup → Services → Service Route Configuration** (см. «Рис. 186»).

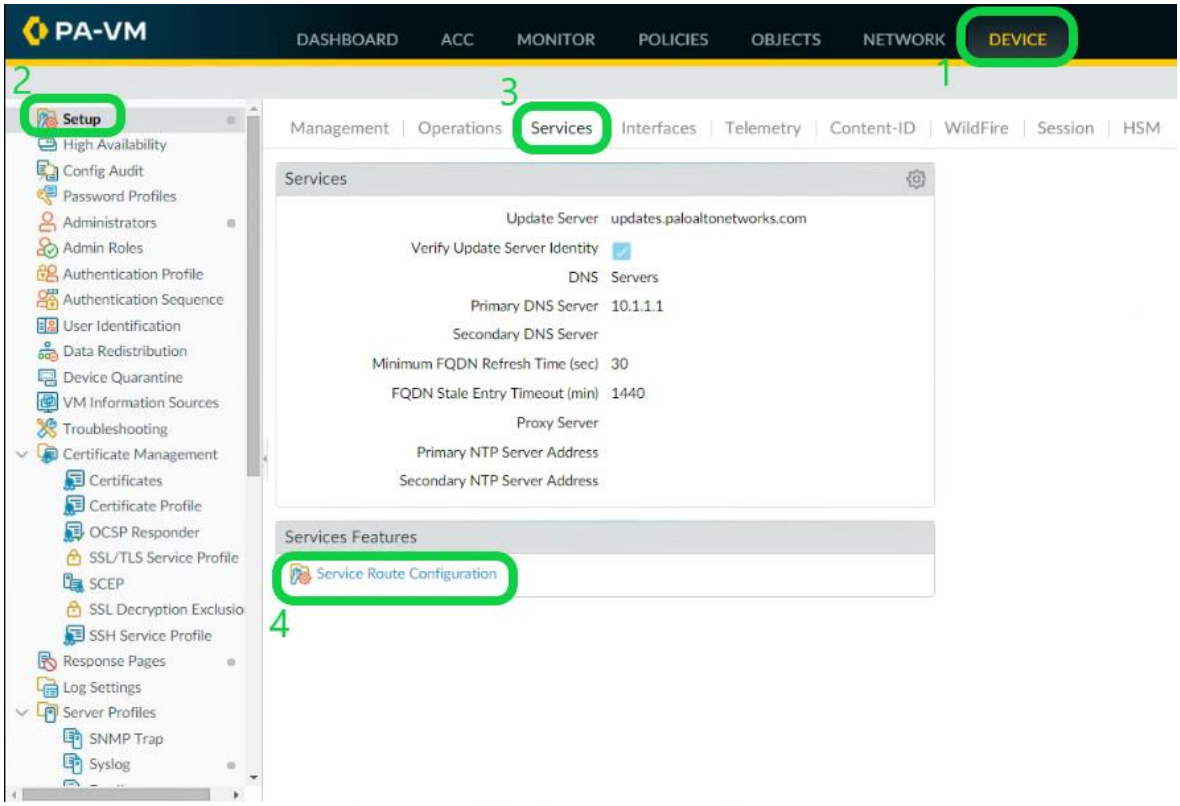


Рис. 186 – Интерфейс устройства PaloAlto. Переход в раздел "Service Route Configuration"

3. В открывшемся окне "Service Route Configuration" (см. «Рис. 187») выберите пункт **Customize** и на вкладке "IPv4" дважды нажмите на строку **Syslog**.

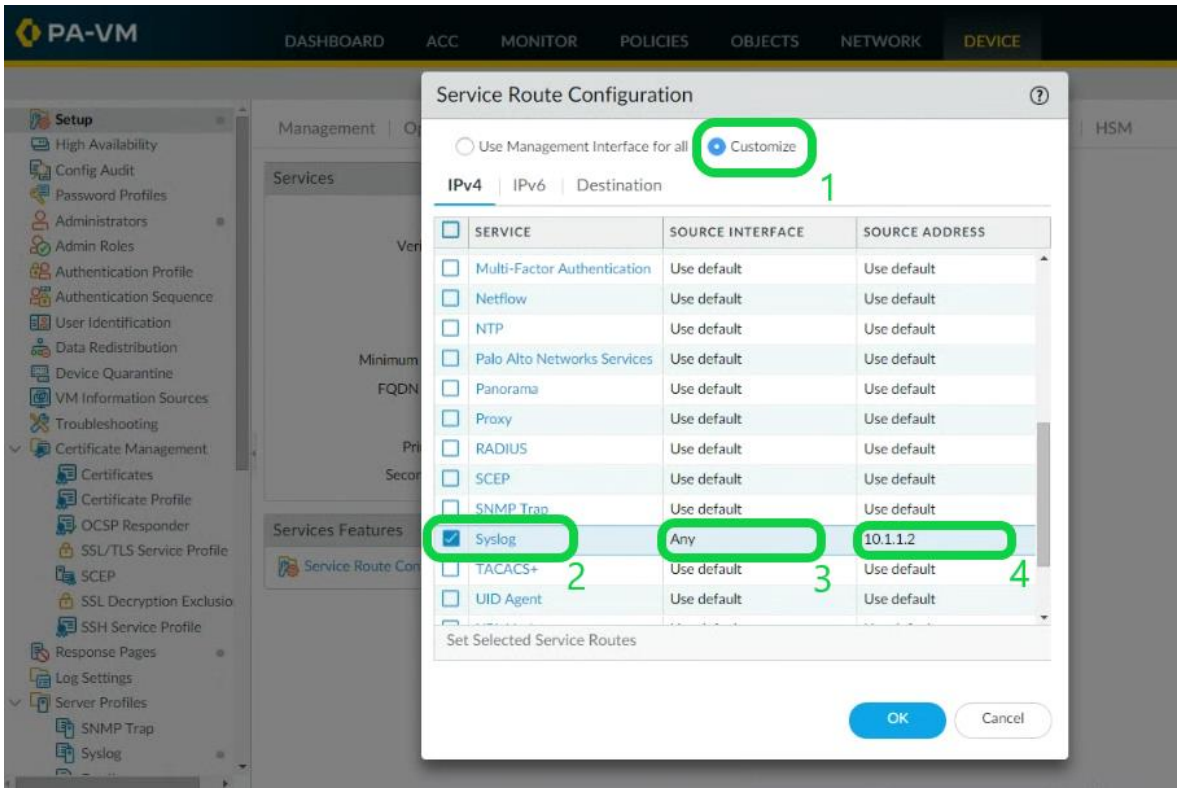


Рис. 187 – Окно "Service Route Configuration"

4. В открывшемся окне "Service Route Source" (см. «Рис. 188») выберите **Source Interface** и укажите **Source Address** с которого у вас будут отправляться события:

Рис. 188 – Окно "Service Route Source"

5. Нажмите кнопку **OK** в окнах "Service Route Source" и "Service Route Configuration".
6. Перейдите в раздел **Device → Server Profiles → Syslog** (см. «Рис. 189»).

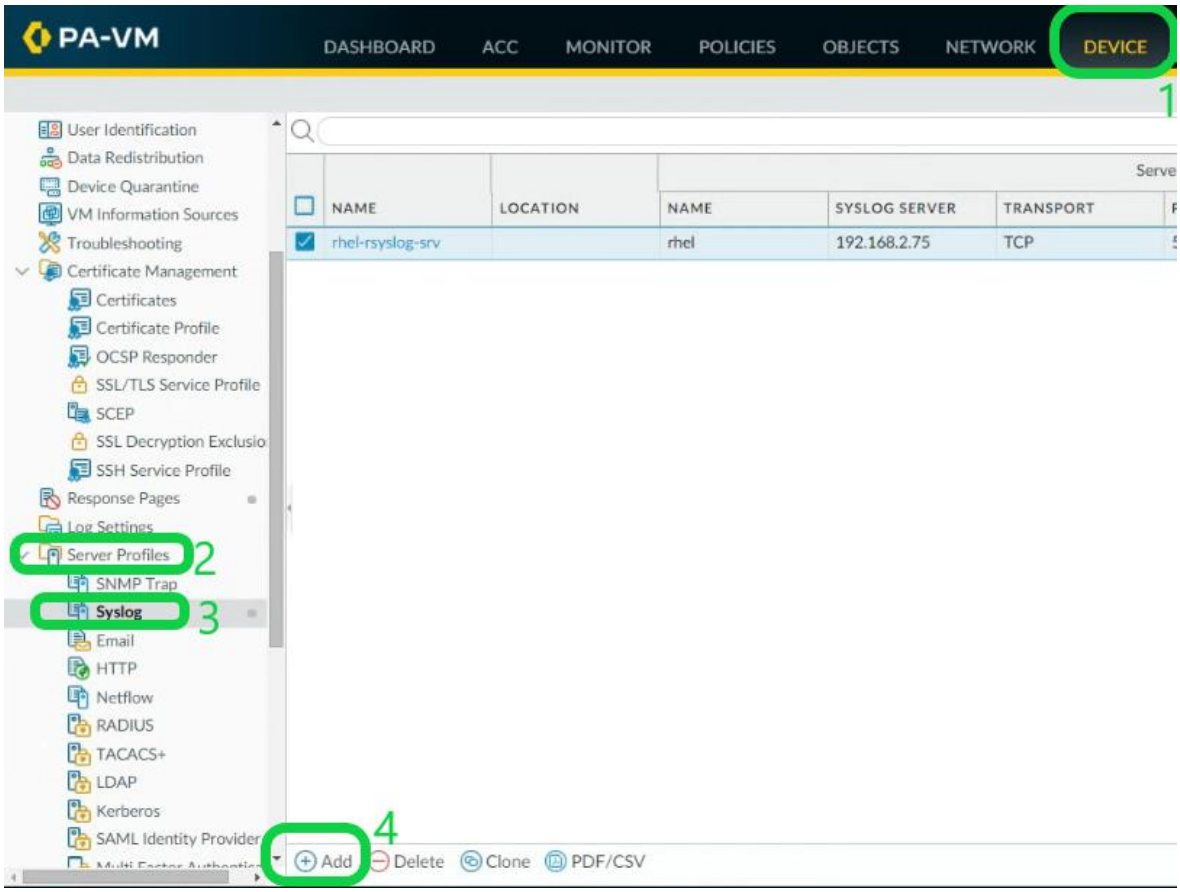


Рис. 189 – Интерфейс устройства PaloAlto. Переход в раздел "Syslog"

7. Нажмите кнопку **Add**. Откроется окно "Syslog Server Profile" (см. «Рис. 190»).

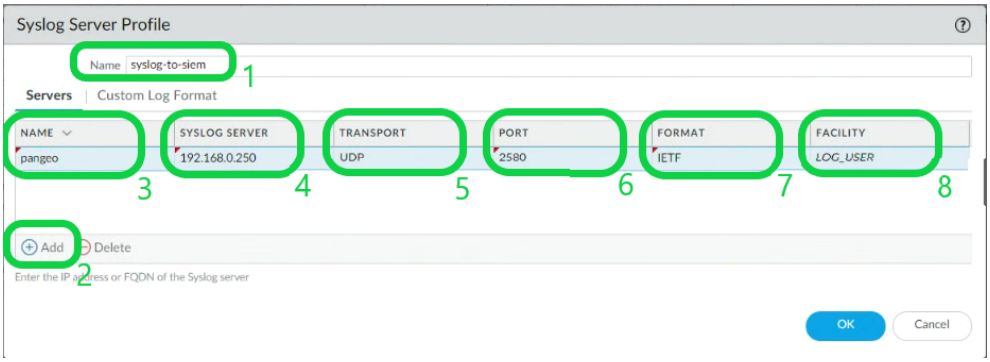


Рис. 190 – Окно "Syslog Server Profile"

8. В окне "Syslog Server Profile" в поле **Name** укажите наименование профиля и нажмите кнопку **Add**. В появившемся блоке полей укажите следующие настройки:

   - в поле **NAME** укажите наименование сервера;
   - в поле **SYSLOG SERVER** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **TRANSPORT** выберите протокол "*UDP*" для отправки событий;
   - в поле **PORT** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - в поле **FORMAT** выберите формат формирования syslog-сообщения "*IETF*";

- в поле **FACILITY** выберите значение facility для отправляемых сообщений "*LOG_USER*";
- нажмите кнопку **OK**.

9. Перейдите в раздел **Objects → Log Forwarding** (см. «Рис. 191»).

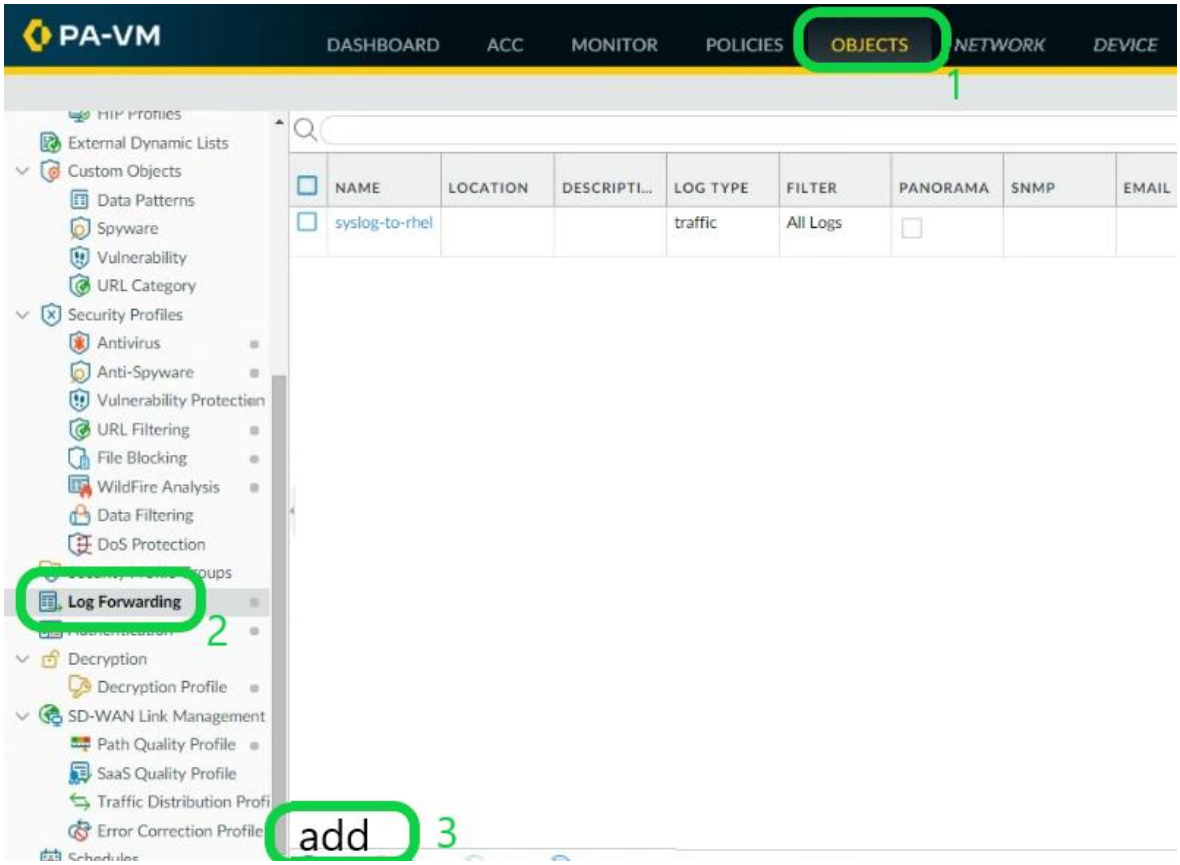


Рис. 191 – Интерфейс устройства PaloAlto. Переход в раздел "Log Forwarding"

10. Нажмите кнопку **Add**. Откроется окно "Log Forwarding Profile" (см. «Рис. 192»).

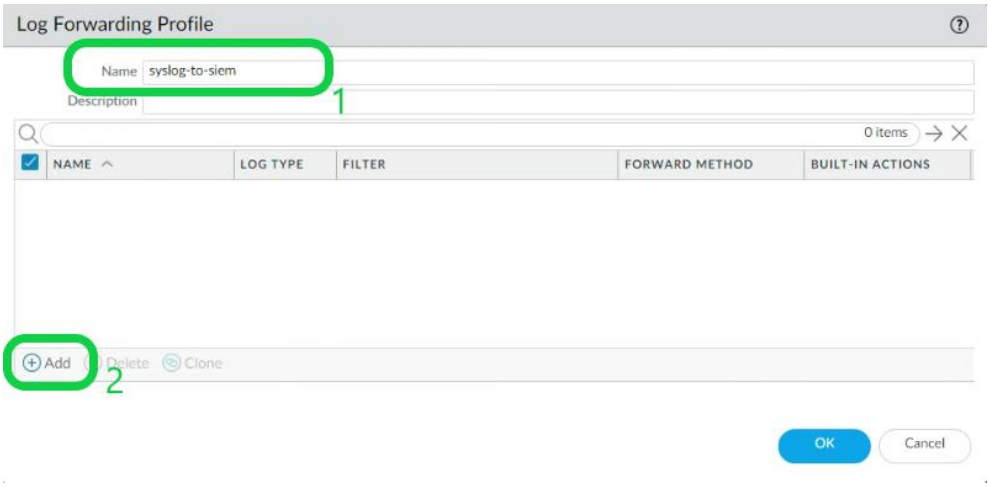


Рис. 192 – Окно "Log Forwarding Profile"

11. В окне "Log Forwarding Profile" в поле **Name** укажите наименование профиля и нажмите кнопку **Add**. Откроется окно "Log Forwarding Profile Match List" (см. «Рис. 193»).

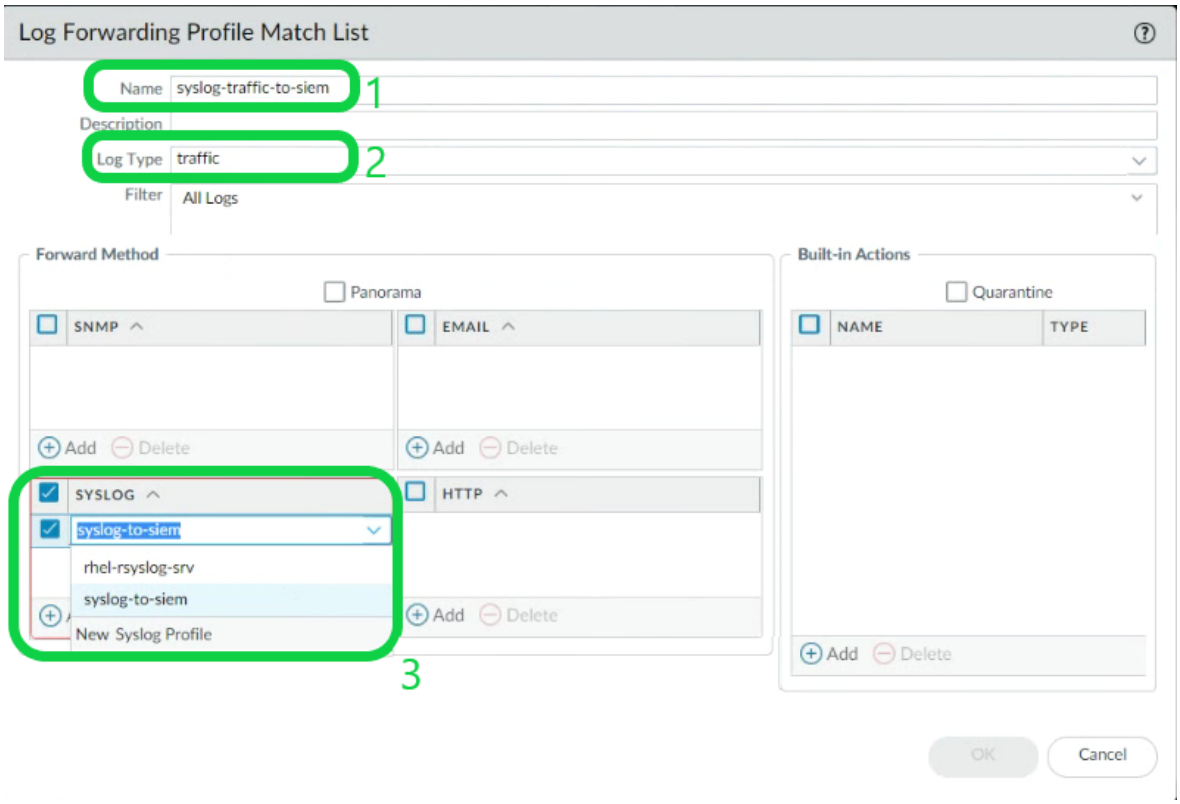


Рис. 193 – Настройка профиля отправки журналов. Шаг 1

12. В открывшемся окне укажите следующие настройки:

- в поле **Name** укажите наименование профиля;
- в поле **Log Type** выберите значение "*traffic*";
- в поле **Syslog** выберите созданный профиль для отправки событий syslog;
- повторите добавление созданных профилей указав в поле **Log Type** соответствующие значения "*threat*", "*auth*" и выбрав в поле **Syslog** соответствующий профиль (см. «Рис. 194»).

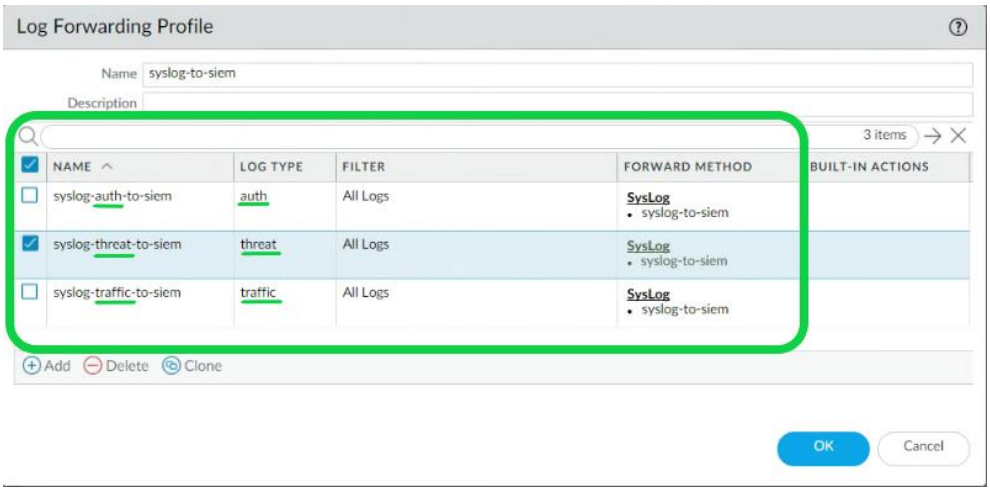


Рис. 194 – Настройка профиля отправки журналов. Шаг 2

- нажмите кнопку **OK**.

13. Перейдите в раздел **Device → Log Setting** (см. «Рис. 195»).

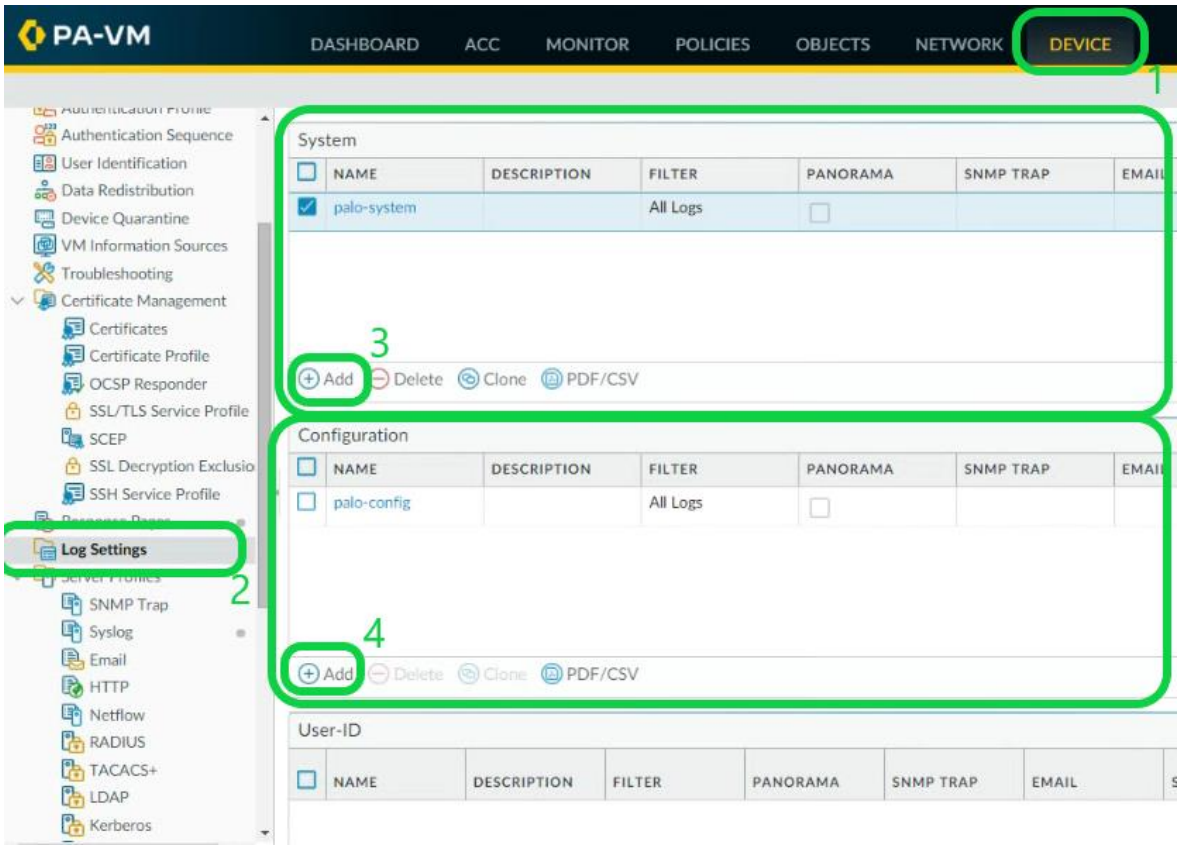


Рис. 195 – Интерфейс устройства PaloAlto. Переход в раздел "Log Setting"

14. В блоке **System** нажмите кнопку **Add**. Откроется окно "Log Setting - System" (см. «Рис. 196»).

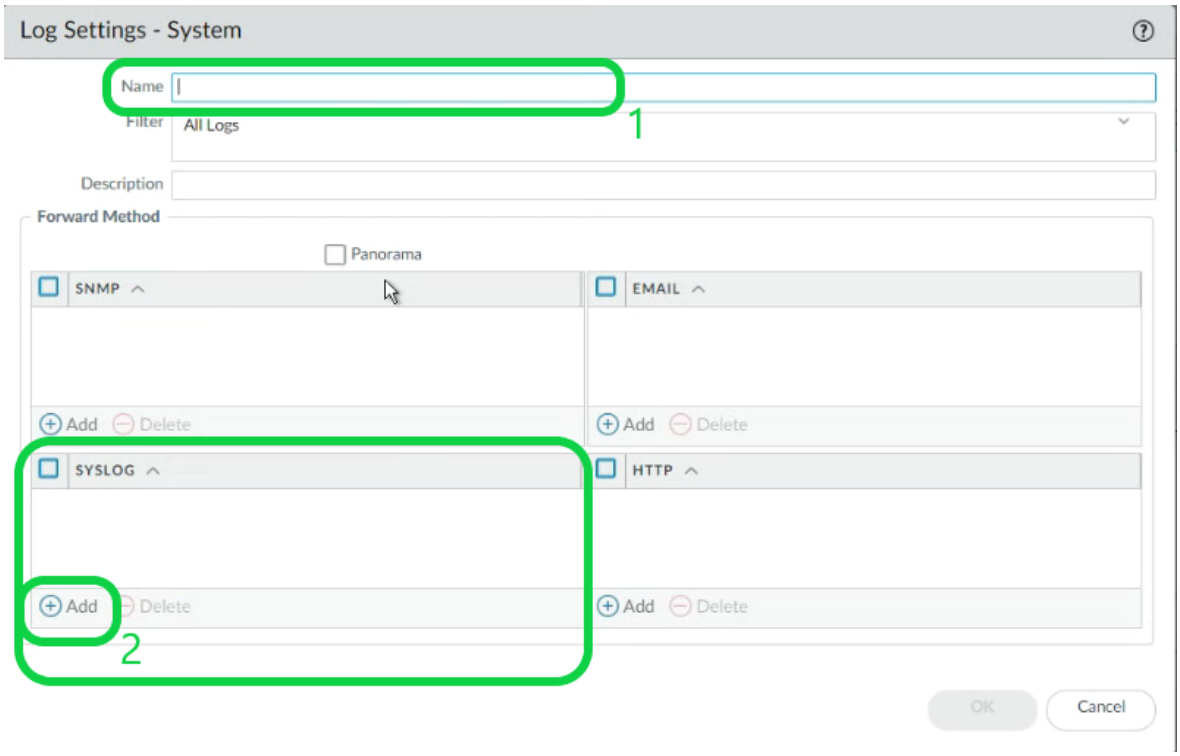


Рис. 196 – Окно "Log Setting - System"

15. В окне "Log Setting - System" в поле **Name** укажите наименование профиля, в блоке **Syslog** нажмите кнопку **Add**, выберите созданный профиль и нажмите кнопку **OK**.

16. Вернитесь в раздел **Device → Log Setting** (см. «Рис. 190»).и в блоке **Configuration** нажмите кнопку **Add**. Откроется окно "Log Setting - Configuration" (см. «Рис. 197»).

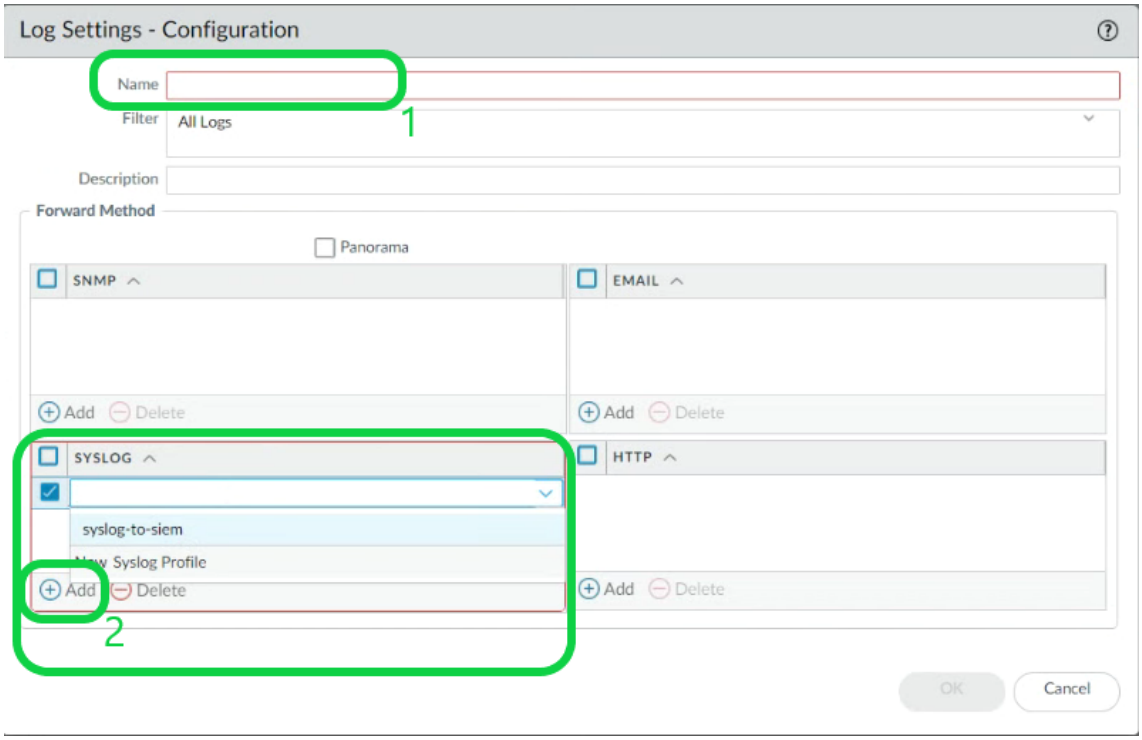


Рис. 197 – Окно "Log Setting - Configuration"

17. В окне "Log Setting - Configuration" в поле **Name** укажите наименование профиля, в блоке **Syslog** нажмите кнопку **Add**, выберите созданный профиль и нажмите кнопку **OK**.

18. Перейдите в раздел **Policies → Security** и нажмите кнопку **Add** (см. «Рис. 198»).

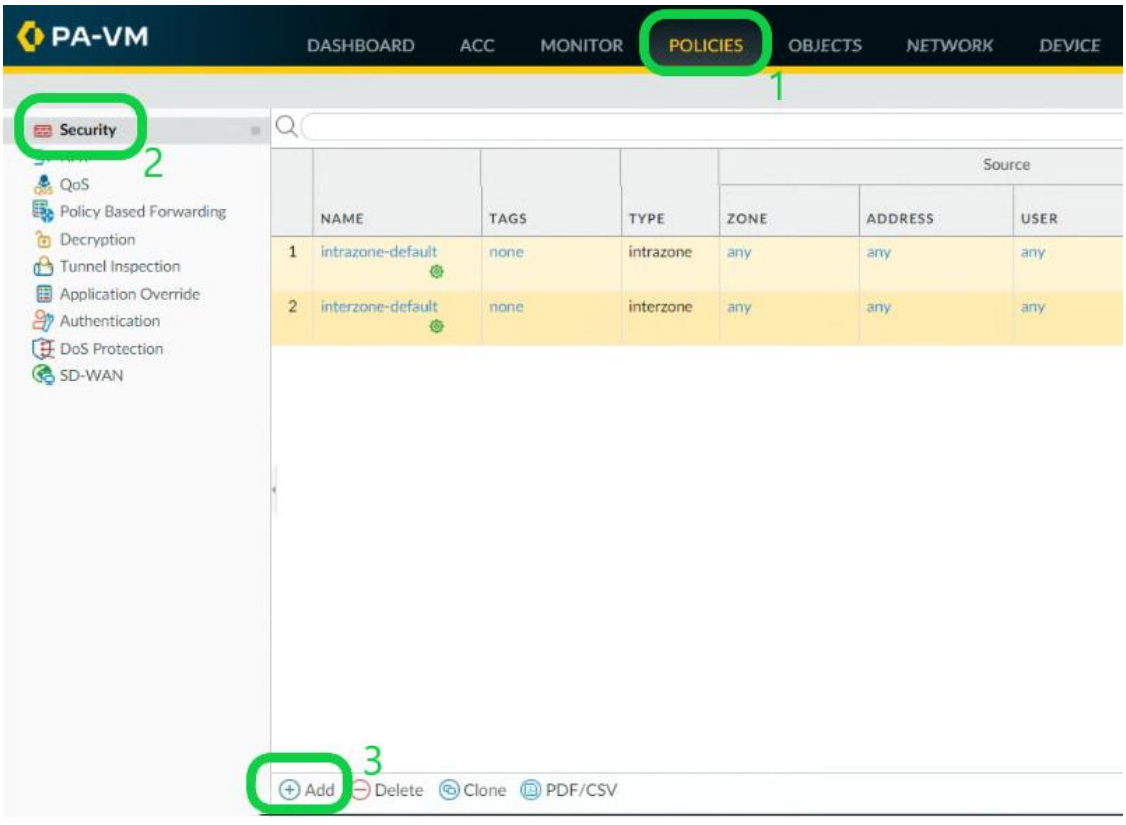


Рис. 198 – Интерфейс устройства PaloAlto. Переход в раздел "Security"

19. В открывшемся окне "Security Policy Rule" перейдите на вкладку "Source", выберите зону отправки **Source Zone**, если зона отсутствует, добавьте ее нажав кнопку **Add** (см. «Рис. 199»).

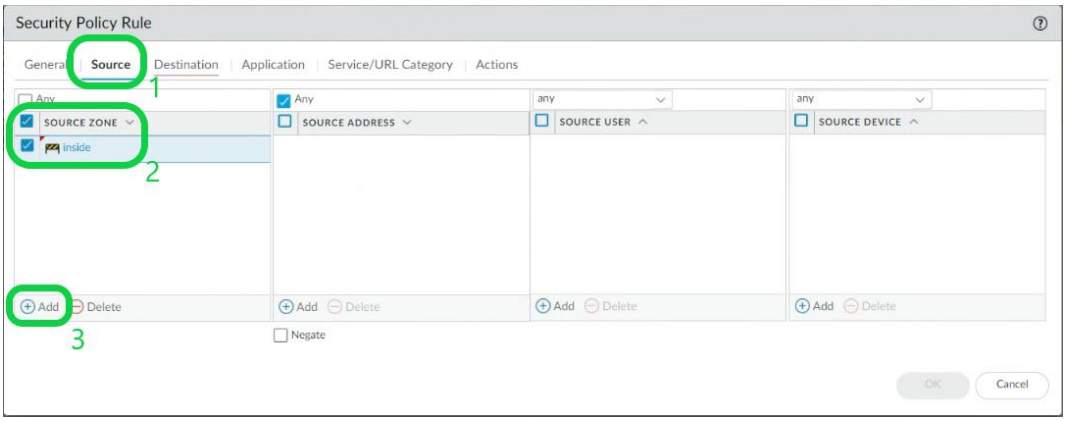


Рис. 199 – Окно "Security Policy Rule". Вкладка "Source

20. В окне "Security Policy Rule" перейдите на вкладку "Destination" выберите зону отправки **Destination Zone**, если зона отсутствует, добавьте ее нажав кнопку **Add** (см. «Рис. 200»).

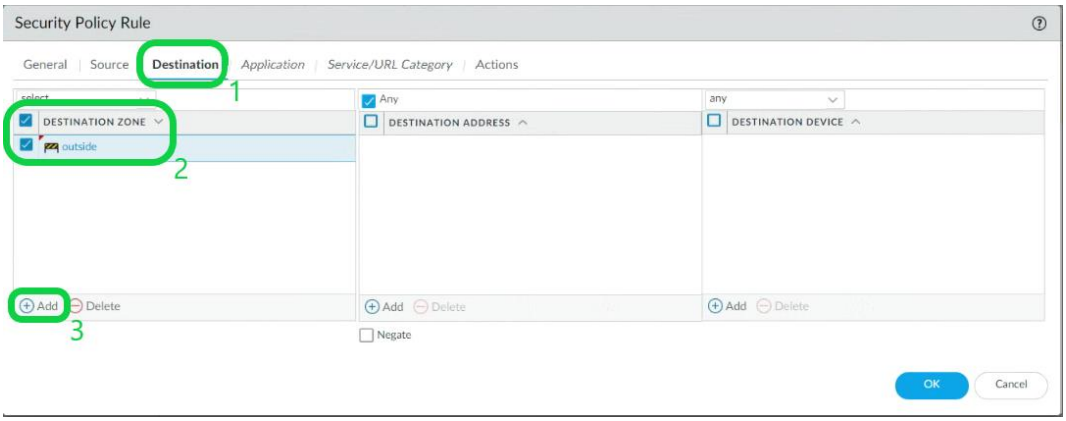


Рис. 200 – Окно "Security Policy Rule". Вкладка "Destination"

21. В окне "Security Policy Rule" перейдите на вкладку "Action" в блоке **Log Setting** установите флаги **Log at Session Start**, **Log at Session End**, в поле **Log Forwarding** выберите профиль отправки событий и нажмите кнопку **OK** (см. «Рис. 201»).

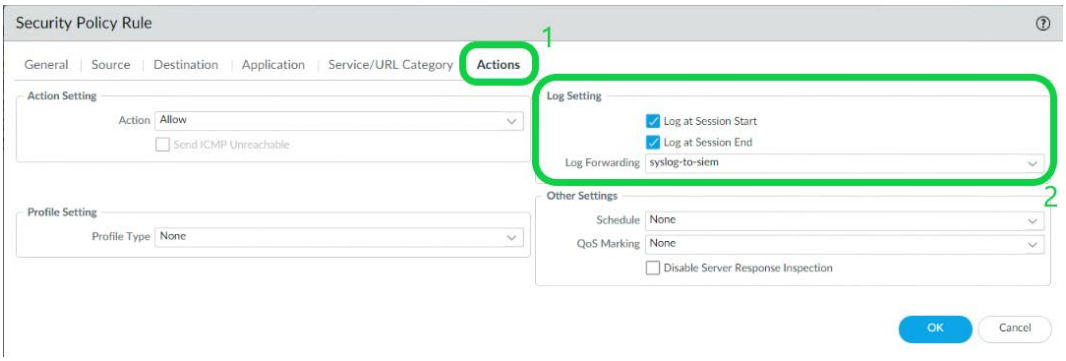


Рис. 201 – Окно "Security Policy Rule". Вкладка "Action"

22. Нажмите кнопку **Commit → Commit All Changes** и для просмотра введенных изменений нажмите кнопку **Change Summary** (см. «Рис. 202»).

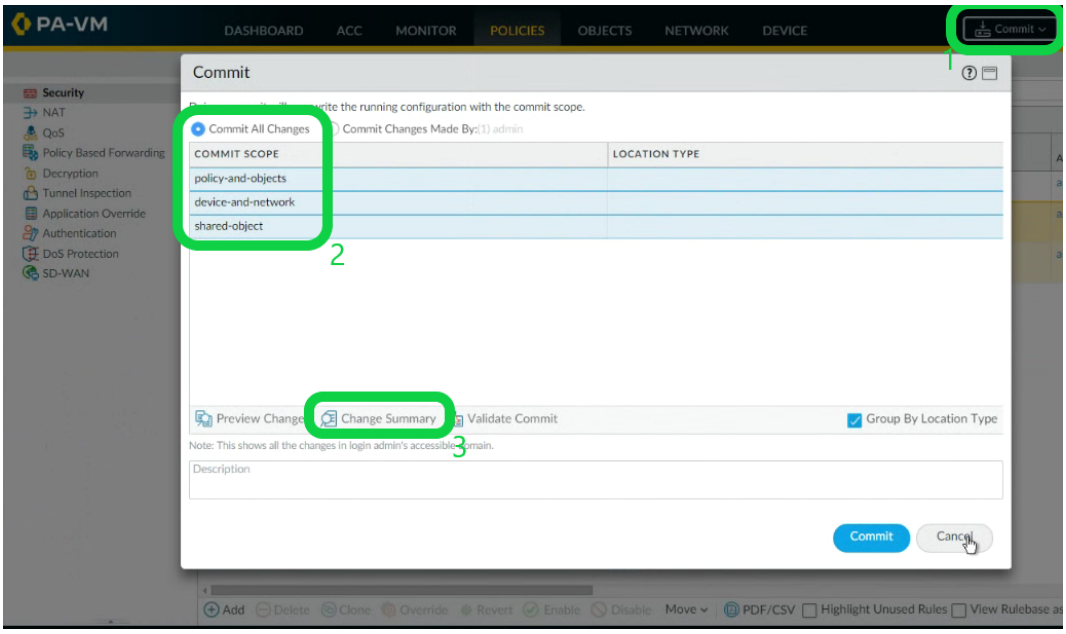


Рис. 202 -- Окно "Commit"

23. В открывшемся окне "Change Summary" - проверьте введенные изменения (см. «Рис. 203»).

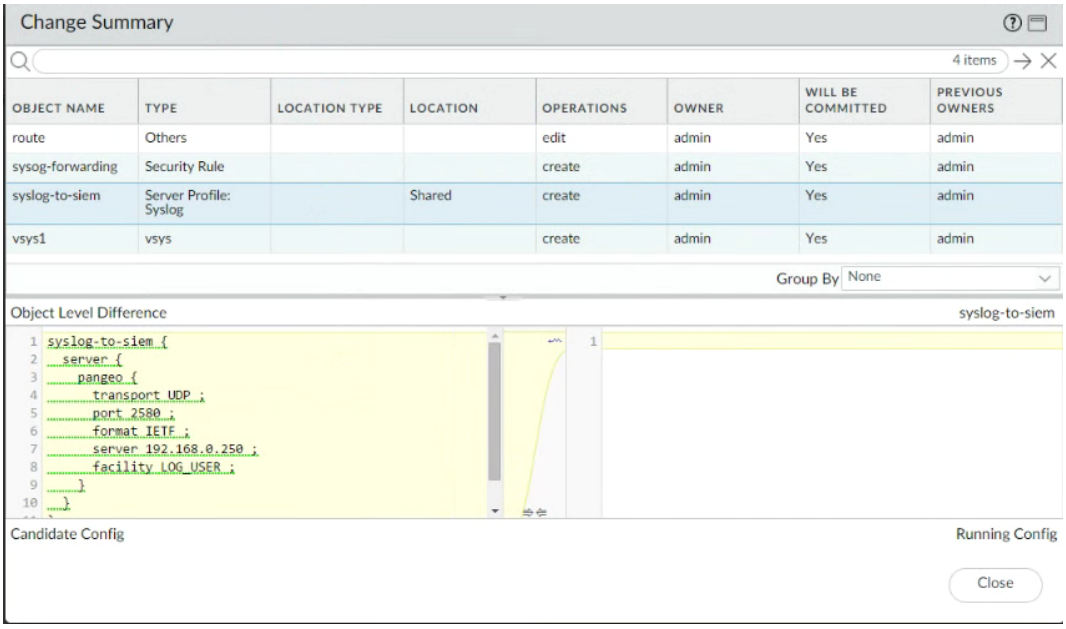


Рис. 203 – Окно " Change Summary "

24. После проверки корректности введенных изменений нажмите кнопку **Commit** и дождитесь результата **Successful** (см. «Рис. 204»).

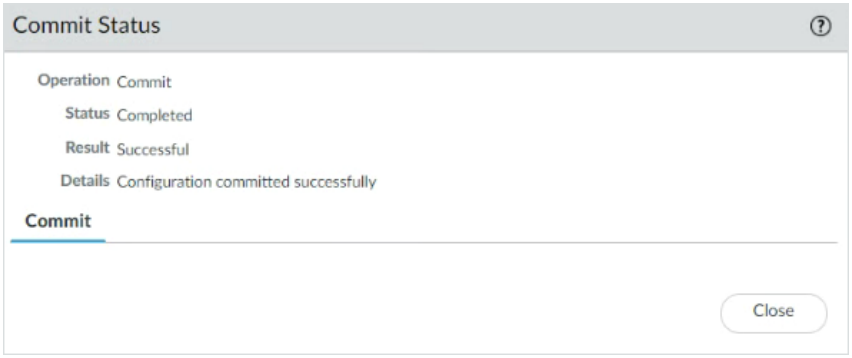


Рис. 204 – Окно "Commit Status"

25. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **PaloAlto-Firewall**.

4.3.14 Pfsense Firewall Netgate

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Pfsense-Firewall-Netgate
Номер (Порт)	2561
Вендор	Pfsense
Тип	Firewall
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс системы и перейдите в раздел **Status → System Log → Settings**.
2. Откройте блок **Remote Logging Options** (см. «Рис. 205»).

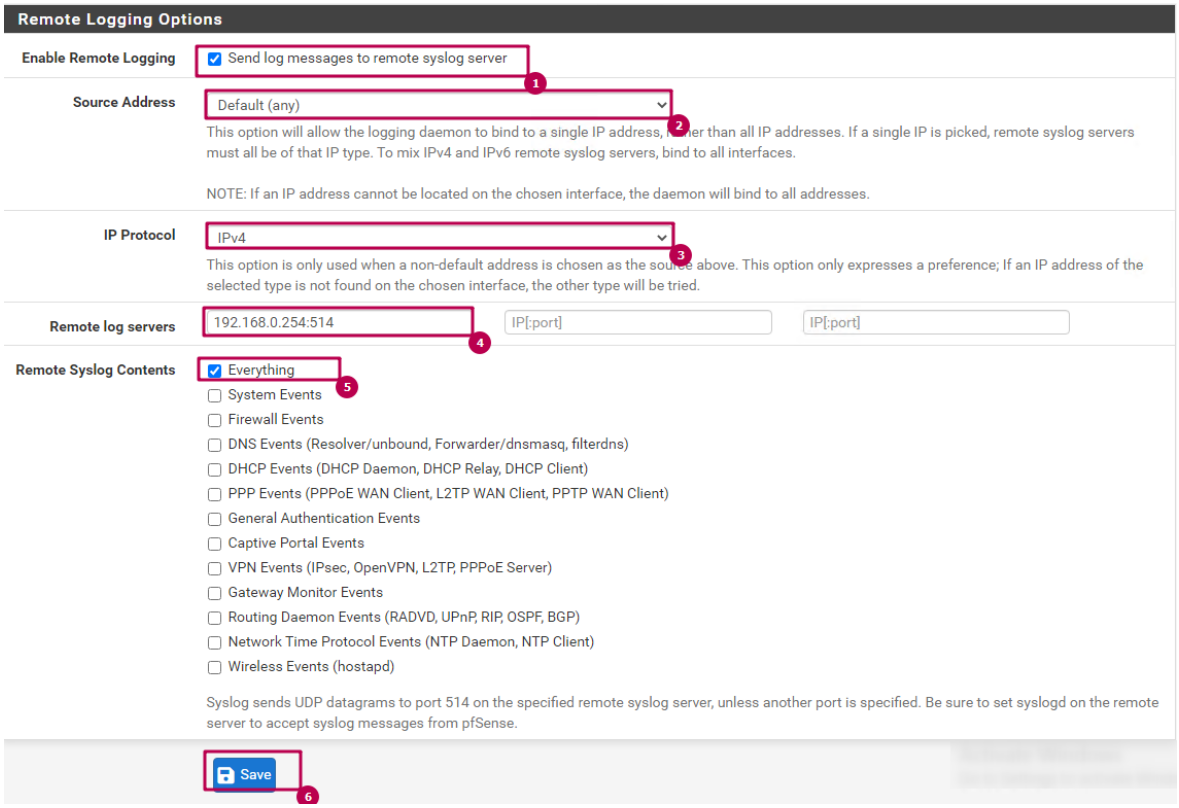


Рис. 205 – Настройка pfSense. Remote Logging Options

3. Укажите следующие настройки:
   - включите отправку журналов, установив флаг в поле **Enable Remote Logging**;
   - в поле **Source Address** из выпадающего списка выберите источник журналов;

- в поле **Remote log servers** укажите IP-адрес агента сбора лог-коллектора и порт, указанный в соответствующем профиле сбора;
- в поле **Remote Syslog Contents** выберите журналы для отправки, установив соответствующие флаги;
- нажмите кнопку **Save**.

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Pfsense-Firewall-Netgate**.

4.3.15 Snort

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Snort
Номер (Порт)	2517
Вендор	Cisco
Тип	NIDS
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. В каталоге `/etc/rsyslog.d/` создайте файл конфигурации для службы `rsyslog`:

   ```
   # sudo nano /etc/rsyslog.d/snort.conf
   ```

2. Настройте конфигурацию:

   ```
   If ($programname contains 'snort' and ($msg contains 'start' or $msg contains 'Start' or $msg contains 'Stop' or $msg contains 'stop' or $msg contains 'ERROR' or $msg contains 'fail' or $msg contains 'Fail')) or ($msg contains 'snort' and $msg contains 'exit') then @@x.x.x.x:port

   If $msg contains 'Classification' and $programname contains 'snort' then @@x.x.x.x:515
   ```

   Где:

   - `x.x.x.x:port` - IP-адрес агента сбора лог-коллектора и порт, указанный в соответствующем профиле сбора;
   - первая строка конфигурации позволяет отправлять в **Платформу Радар** системные журналы, исключая не информативные;
   - вторая строка включает пересылку предупреждений (alerts) в **Платформу Радар**.

3. Перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog
   ```

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Snort**.

4.3.16 Solar webProxy

Solar webProxy - продукт класса SWG (Secure Web Gateway) российской компании Ростелеком-Солар.

Перед настройкой источника рекомендуется ознакомиться с документом Руководство по установке и настройке Solar webProxy).

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Solar-WebProxy
Номер (Порт)	2592
Вендор	Solar
Тип	Proxy
Профиль сбора	«Модуль tcp_input» «Модуль udp_input»

Настройка источника включает в себя следующие шаги:

1. Настройка журналирования службы веб-интерфейса пользователя (smap-play-server).
2. Настройка журналирования веб-запросов пользователей прокси (skvt-wizor).
3. Настройка отправки событий в платформу.
4. Включение источника в платформе.

Шаг 1. Настройка журналирования службы веб-интерфейса пользователя (smap-play-server)

Данная настройка позволяет журналировать действия администраторов в веб-интерфейсе системы Solar webProxy.

События по умолчанию сохраняются в файл `/var/log/messages` на узле с ролью "Сервер управления".

Пример событий:

```
Mar 29 11:59:48 swp01-main java: webserver: admin@/192.168.11.2: get filter hosts
[swp01-filter.test.lab,swp01-reverse.test.lab]
Mar 29 12:00:06 swp01-main java: webserver: admin@/192.168.11.2: get list of all
categories
Mar 29 12:00:06 swp01-main java: webserver: admin@/192.168.11.2: Action: 'read
layer'; Layer: 'Вскрытие HTTPS'
Mar 29 12:00:10 swp01-main java: webserver: admin@/192.168.11.2: get list of all
categories
Mar 29 12:00:22 swp01-main java: webserver: admin@/192.168.11.2: get list of all
categories
```

Выполните следующие действия:

1. Войдите в веб-интерфейс системы и перейдите в раздел **Система → Основные настройки → Журналирование → Сервер веб-интерфейса**" (см. «Рис. 206»).

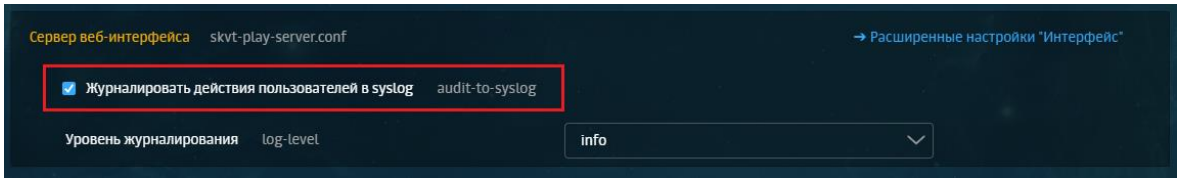


Рис. 206 – Журналирование действий пользователей

2. Установите флажок **Журналировать действия пользователей в syslog**.
3. Сохраните изменения и примените конфигурацию.
4. Откройте конфигурационный файл службы `rsyslog (/etc/rsyslog.conf)` и добавьте следующую настройку:

   ```
   local0.*                /var/log/messages
   ```

5. На узле с ролью **Сервер управления** создайте файл конфигурации `/etc/rsyslog.d/03-send_skvt_master.conf` и укажите следующие настройки:

   ```
   module(load="imfile" PollingInterval="10")
   input(type="imfile"
         reopenOnTruncate="on"
         File="/var/log/messages"
         )

   if $programname == 'java' and $msg contains 'webserver' then @@<ip-адрес агента сбора лог-коллектора>:port
   ```

   Где:

   - `<ip-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - `@@/@` - отправка будет выполняться по протоколу TCP/UDP.

6. Перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog
   ```

Шаг 2. Настройка журналирования веб-запросов пользователей прокси (skvt-wizor)

Пример событий:

```
Mar 29 15:24:11 swp01-filter java: [acc-domain:TEST.LAB] [acc-groups:] [acc-
ip:192.168.2.70] [acc-name:da] [acc-port:51380] [bytes-in:3147] [bytes-out:781] [flt-
categories:21004] [flt-codes:11,0,0,0,0] [flt-policy:Завершение обработки политики]
[flt-rules:Вскрывать HTTPS по умолчанию,Переход к слою Icap Request,Переход к слою
Запрет доступа к сайтам,Переход к слою Icap Response,Переход к слою Завершение
обработки политики] [flt-status:200] [flt-time:125] [req-
hostname:safebrowsing.googleapis.com] [req-method:GET] [req-
pathname:/v4/threatListUpdates:fetch] [req-protocol:https] [req-
query:$ct=application/x-
```

```
protobuf&key=AIzaSyC7jsptDS3am4tPx4r3nxis7IMjBc5Dovo&$httpMethod=POST&$req=ChUKE25hdm
NsaWVudC1hdXRvLWZmb3gaJwgFEAEaGwoNCAUQBhgBIgMwMDEwARC3nRAaAhgFyU6KeiICIAIoARonCAEQARo
bCg0IARAGGAEiAzAwMTABENWDDBoCGAUyxlEzIgIgAigBGicIAxABGhsKDQgDEAYYASIDMDAxMAEQ8_oLGgIY
BVB30G4iAiACKAEaJwgHEAEaGwoNCAcQBhgBIgMwMDEwARC81AwaAhgFLhmniCICIAIoARolCAkQARoZCg0IC
RAGGAEiAzAwMTABECAaAhgF-13fQCICIAIoAQ==] [req-referer:] [req-time:2023-03-
29T12:24:11.471Z] [res-datatype:application/x-protobuf] [res-ip:108.177.14.95] [traf-
mode:forward] [x-virus-id:] [req-port:443] [flt-reason:]

Mar 28 11:35:59 swp01-filter java: [acc-domain:] [acc-groups:] [acc-ip:192.168.2.70]
[acc-name:] [acc-port:55073] [bytes-in:0] [bytes-out:0] [flt-categories:] [flt-
codes:0] [flt-policy:policy.xml] [flt-rules:] [flt-status:407] [flt-time:1] [req-
hostname:secure.eicar.org] [req-method:CONNECT] [req-pathname:] [req-protocol:https]
[req-query:] [req-referer:] [req-time:2023-03-28T08:35:59.399Z] [res-
datatype:application/skvt-unchecked] [res-ip:] [traf-mode:forward] [x-virus-id:]
[req-port:443] [flt-reason:]
```

Выполните следующие действия:

1. Войдите в веб-интерфейс системы и перейдите в раздел **Система → Расширенные настройки → Фильтрация и кэширование трафика**.
2. Откройте настройки **Фильтрация и анализ трафика пользователей → Форматы записи в syslog** (см. «Рис. 207»).

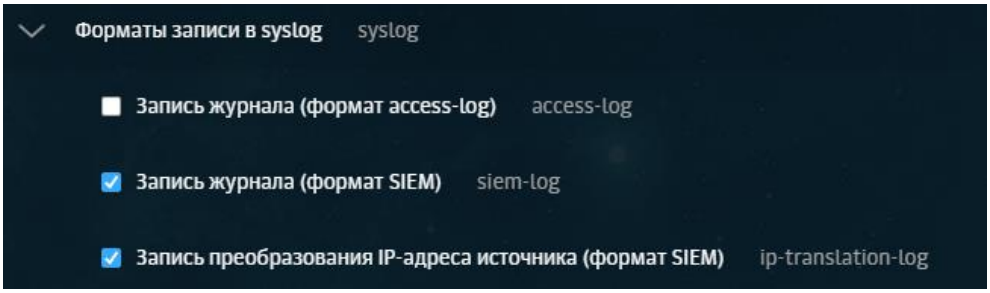


Рис. 207 – Форматы записи в syslog

3. Установите флаги **Запись журнала (формат SIEM)** и **Запись преобразования IP-адреса источника (формат SIEM)**.
4. Сохраните изменения и примените конфигурацию.
5. На узлах с ролью **Фильтр HTTP-трафика** и **Обратный прокси-сервер** настройте журналирование в отдельный файл:
   - создайте файл `/var/log/skvt.log`:
     ```
     # touch /var/log/skvt.log
     ```
   - настройте доступ к файлу:
     ```
     # chmod 600 /var/log/skvt.log
     ```

Шаг 3. Настройка отправки событий в платформу

1. Настройте перенаправление событий в файл `/var/log/skvt.log` внеся в файл `/etc/rsyslog.conf` соответствующую конфигурацию.
2. Во избежание дублирования отключите запись событий в файл `/var/log/messages` (оператор `stop`):

```
$template rawSkvt,"%syslogtag% %msg%\n"


local0.*                                        /var/log/skvt.log; rawSkvt
& stop
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
```

3. Сохраните изменения и перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog
```

4. Настройте ротацию файла `/var/log/skvt.log` с помощью `logrotate`. Для этого создайте файл `/etc/logrotate.d/skvt` со следующими настройками:

```
/var/log/skvt.log {
    weekly
    rotate 4
    missingok
    notifempty
    nomail
    compress
    create 0600 dozor dozor
    minsize 10M
}
```

5. Проверьте условия `logrotate`:

```
# logrotate -df /etc/logrotate.d/skvt
```

6. Запустите ротацию файла:

```
# logrotate -f /etc/logrotate.d/skv
```

7. Настройте отправку событий в **Платформу Радар**. Для этого создайте конфигурационный файл `/etc/rsyslog.d/03-send_skvt.conf` со следующими настройками:

```
module(load="imfile" PollingInterval="10")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/skvt.log"
      Tag="skvt_wizor_log"
     )

if $syslogtag == 'skvt_wizor_log' then @@<pangeo-log-collector>:<port>
& stop
```

8. Сохраните изменения и перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog
```

Шаг 4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Solar-WebProxy**.

4.3.17 Squid Proxy

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Squid-Proxy
Номер (Порт)	2890
Вендор	Squid
Тип	Proxy
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Откройте конфигурационный файл `squid.conf`:

   ```
   # sudo nano /etc/squid/squid.conf
   ```

2. Создайте шаблон формата журналов:

   ```
   logformat radar  %la:%lp %>a %[ui %[un [%tl] "%rm %ru / HTTP/%rv" %>Hs %<st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh
   ```

3. Укажите шаблон формата журналов в настройке журналирования `syslog`:

   ```
   access_log syslog:[local2.info](http://local2.info/ "Внешняя ссылка (откроется в новом окне)") radar
   ```

4. Сохраните файл и перезапустите службу:

   ```
   # sudo service squid restart
   ```

5. Откройте конфигурационный файл службы `rsyslog`:

   ```
   # sudo nano /etc/rsyslog.conf
   ```

6. Укажите IP-адрес агента сбора лог-коллектора, порт, указанный в соответствующем профиле сбора и отключите объединение сообщений:

   ```
   local2.* @<IP-адрес агента сбора лог-коллетора>:port

   $RepeatedMsgReduction off
   ```

7. Сохраните изменения и перезапустите службу:

   ```
    # sudo service rsyslog restart
   ```

8. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Squid-Proxy**.

4.3.18 Suricata

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Squid-Proxy
Номер (Порт)	2890
Вендор	Squid
Тип	Proxy
Профиль сбора (активный сбор)	«Модуль sftp_input» «Модуль ssh_collector_input»
Профиль сбора (пассивный сбор)	«Модуль tcp_input»

Перед настройкой источника проверьте и при необходимости внесите изменения в файл `/etc/suricata/suricata.yaml` на хосте, где установлена Suricata.

Ниже приведен пример данного файла в части логирования событий:

```
# Configure the type of alert (and other) logging you would like.
outputs:
  - eve-log:
      enabled: yes
      filetype: regular
      filename: eve.json
      # Enable for multi-threaded eve.json output; output files are amended with
      # an identifier, e.g., eve.9.json
      #threaded: false
      #prefix: "@cee: " # prefix to prepend to each log entry
      # the following are valid when type: syslog above
      #identity: "suricata"
      #facility: local5
      #level: Info ## possible levels: Emergency, Alert, Critical,
                   ## Error, Warning, Notice, Info, Debug
      #ethernet: no  # log ethernet header in events when available
      #compact: yes
      #ensure-ascii: yes
      #escape-slash: yes
      #redis:
      #  server: 127.0.0.1
      #  port: 6379
      #  async: true ## if redis replies are read asynchronously
      #  mode: list ## possible values: list|lpush (default), rpush, channel|publish
      #             ## lpush and rpush are using a Redis list. "list" is an alias for
lpush
      #             ## publish is using a Redis channel. "channel" is an alias for
publish
      #  key: suricata ## key or channel to use (default to suricata)
      # Redis pipelining set up. This will enable to only do a query every
      # 'batch-size' events. This should lower the latency induced by network
      # connection at the cost of some memory. There is no flushing implemented
      # so this setting should be reserved to high traffic Suricata deployments.
      #  pipelining:
      #    enabled: yes ## set enable to yes to enable query pipelining
      #    batch-size: 10 ## number of entries to keep in buffer
      # Include top level metadata. Default yes.
      #metadata: no
      # include the name of the input pcap file in pcap file processing mode
```

```
      pcap-file: false
      # Community Flow ID
      # Adds a 'community_id' field to EVE records. These are meant to give
      # records a predictable flow ID that can be used to match records to
      # output of other tools such as Zeek (Bro).
      #
      # Takes a 'seed' that needs to be same across sensors and tools
      # to make the id less predictable.
      # enable/disable the community id feature.
      community-id: false
      # Seed value for the ID output. Valid values are 0-65535.
      community-id-seed: 0
      xff:
        enabled: no
        # Two operation modes are available: "extra-data" and "overwrite".
        mode: extra-data
        # Two proxy deployments are supported: "reverse" and "forward". In
        # a "reverse" deployment the IP address used is the last one, in a
        # "forward" deployment the first IP address is used.
        deployment: reverse
        # Header name where the actual IP address will be reported. If more
        # than one IP address is present, the last IP address will be the
        # one taken into consideration.
        header: X-Forwarded-For
      types:
        - alert:
            tagged-packets: yes
        - frame:
            enabled: no
        - anomaly:
            enabled: yes
            types:
              # decode: no
              # stream: no
              # applayer: yes
        - http:
            extended: yes     # enable this for extended logging information
            # custom allows additional HTTP fields to be included in eve-log.
            # the example below adds three additional fields when uncommented
            #custom: [Accept-Encoding, Accept-Language, Authorization]
            # set this value to one and only one from {both, request, response}
            # to dump all HTTP headers for every HTTP request and/or response
            # dump-all-headers: none
        - dns:
            # This configuration uses the new DNS logging format,
            # the old configuration is still available:
            # https://docs.suricata.io/en/latest/output/eve/eve-json-output.html#dns-
v1-format

            # As of Suricata 5.0, version 2 of the eve dns output
            # format is the default.
            #version: 2
            # Enable/disable this logger. Default: enabled.
            #enabled: yes
            # Control logging of requests and responses:
            # - requests: enable logging of DNS queries
            # - responses: enable logging of DNS answers
            # By default both requests and responses are logged.
            #requests: no
            #responses: no
            # Format of answer logging:
            # - detailed: array item per answer
            # - grouped: answers aggregated by type
            # Default: all
```

```
            #formats: [detailed, grouped]
            # DNS record types to log, based on the query type.
            # Default: all.
            #types: [a, aaaa, cname, mx, ns, ptr, txt]
        - tls:
            extended: yes     # enable this for extended logging information
            # output TLS transaction where the session is resumed using a
            # session id
            #session-resumption: no
            # custom controls which TLS fields that are included in eve-log
            #custom: [subject, issuer, session_resumed, serial, fingerprint, sni,
version, not_before, not_after, certificate, chain, ja3, ja3s]
        - files:
            force-magic: no   # force logging magic on all logged files
            # force logging of checksums, available hash functions are md5,
            # sha1 and sha256
            #force-hash: [md5]
        - drop:
            alerts: yes      # log alerts that caused drops
            flows: all       # start or all: 'start' logs only a single drop
            verdict: yes
        - smtp:
            #extended: yes # enable this for extended logging information
            # this includes: bcc, message-id, subject, x_mailer, user-agent
            # custom fields logging from the list:
            #  reply-to, bcc, message-id, subject, x-mailer, user-agent, received,
            #  x-originating-ip, in-reply-to, references, importance, priority,
            #  sensitivity, organization, content-md5, date
            #custom: [received, x-mailer, x-originating-ip, relays, reply-to, bcc]
            # output md5 of fields: body, subject
            # for the body you need to set app-layer.protocols.smtp.mime.body-md5
            # to yes
            #md5: [body, subject]
        - ftp
        - rdp
        - nfs
        - smb
        - tftp
        - ike
        - dcerpc
        - krb5
        - bittorrent-dht
        - snmp
        - rfb
        - sip
        - quic
        - dhcp:
            enabled: yes
            extended: no
        - ssh
        - mqtt:
            # passwords: yes           # enable output of passwords
        - http2
        - pgsql:
            enabled: no
            # passwords: yes           # enable output of passwords. Disabled by
default
        #- stats:
        #    totals: yes       # stats for all threads merged together
        #    threads: no       # per thread stats
        #    deltas: no        # include delta values
        - flow

        - netflow
```

Настройку источника можно выполнить двумя способами:

1. Активный сбор через подключение к хосту с Suricata с помощью модуля SFTP/SSH профиля сбора.
2. Пассивный сбор от хоста с Suricata.

Способ 1. Активный сбор через подключение к хосту с Suricata с помощью модуля SFTP/SSH

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Suricata** и настройте соответствующий профиль сбора:

- «Модуль sftp_input»;
- «Модуль ssh_collector_input».

Способ 2. Пассивный сбор от хоста с Suricata.

1. Создайте файл настроек для `rsyslog` со следующими параметрами:

```
module(load="imfile" PollingInterval="5")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/suricata/eve.json"
      Tag="suricata"
      ruleset="surifwd")
ruleset(name="surifwd")
{
    action(type="omfwd"
        Target="IP-адрес коллектора"
        Port="3540"
        Protocol="tcp"
        ResendLastMSGOnReconnect="on"
        action.resumeRetryCount="100"
        queue.type="linkedList"
        queue.size="10000")
    stop
}
```

2. Сохраните файл в директории `/etc/rsyslog.d/` и перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog
```

3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Suricata**.

4.3.19 Usergate UTM Firewall

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	UserGate-UTM
Номер (Порт)	2545
Вендор	Usergate

Характеристика	Значение
Тип	Firewall
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс UserGate UTM, перейдите в раздел **Настройки** и выберите вкладку "Журналы и отчеты" (см. «Рис. 208»).

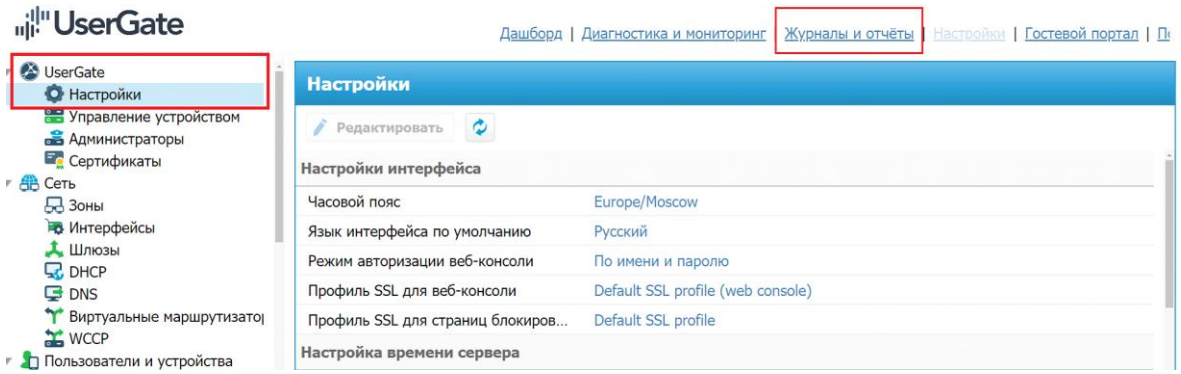


Рис. 208 – Настройка Usergate. Журналы и отчеты

2. Выберите подраздел **Экспорт журналов** и нажмите кнопку **Добавить** (см. «Рис. 209»).

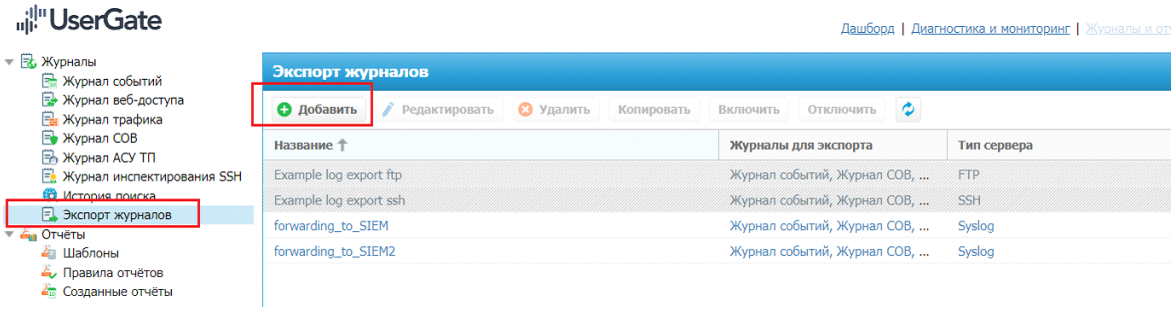


Рис. 209 – Экспорт журналов

3. В открывшемся окне "Свойства правила экспорта журналов" выполните следующие действия:

   Примечание: все отдельные слова в названии необходимо писать через нижнее подчеркивание

   - Перейдите на вкладку "Общие" (см. «Рис. 210») и укажите следующую информацию:
     - в поле **Включено** установите соответствующий флаг;
     - в поле **Название** укажите наименование свойства.

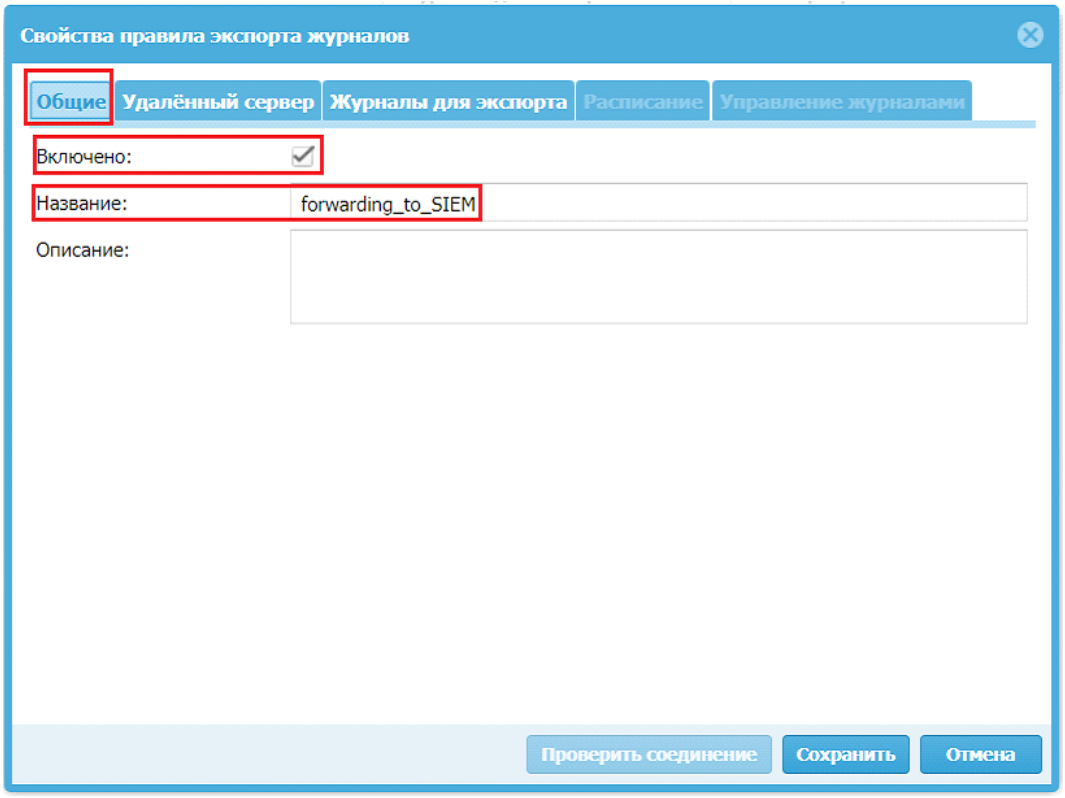


Рис. 210 – Свойства правила экспорта журналов.

- Перейдите на вкладку "Удаленный сервер" (см. «Рис. 211») и укажите следующую информацию:

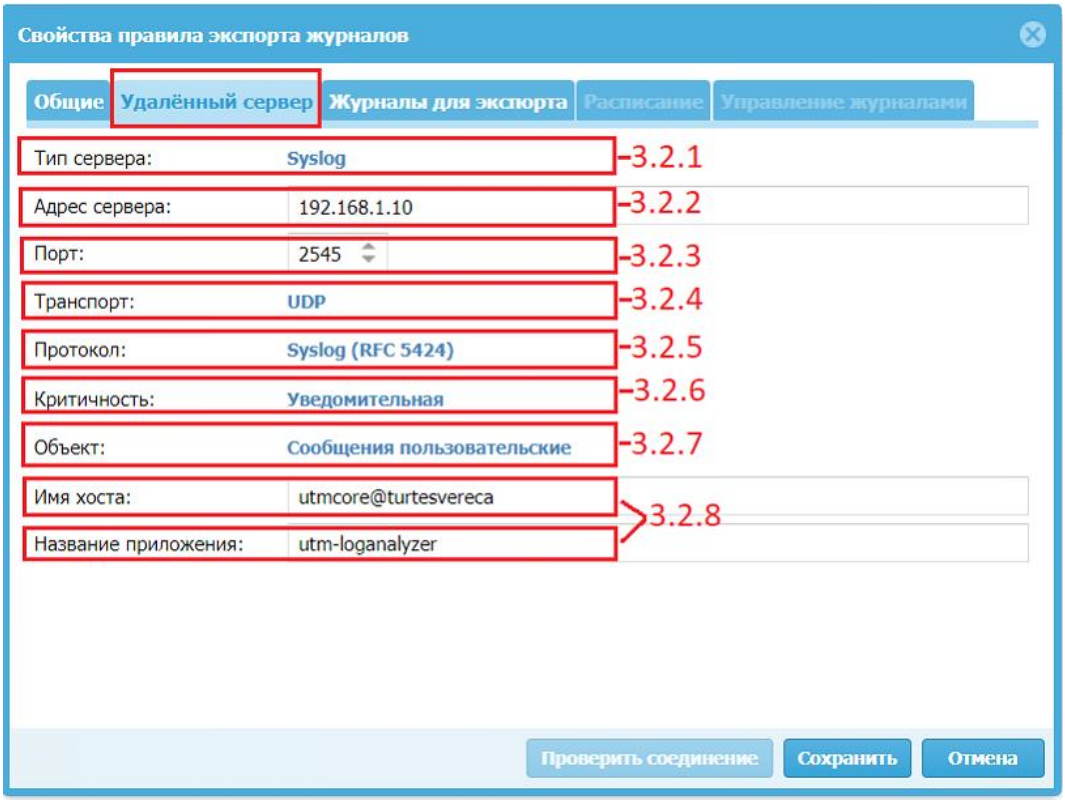


Рис. 211 – Свойства удаленного сервера.

  - в поле **Тип сервера** установите значение "Syslog";
  - в поле **Адрес сервера** укажите IP-адрес агента сбора лог-коллектора;

- в поле **Порт** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
- в поле **Транспорт** установите значение "UDP";
- в поле **Протокол** установите значение "Syslog (RFC 5424)";
- в поле **Критичность** установите значение "Уведомительная";
- в поле **Объект** установите значение "Сообщения пользовательские";
- в поле **Имя хоста** и **Название приложения** укажите соответствующие значения без пробелов.

- Перейдите на вкладку "Журналы для экспорта" (см. «Рис. 212») и выберите журналы для отправки установив следующие флаги:

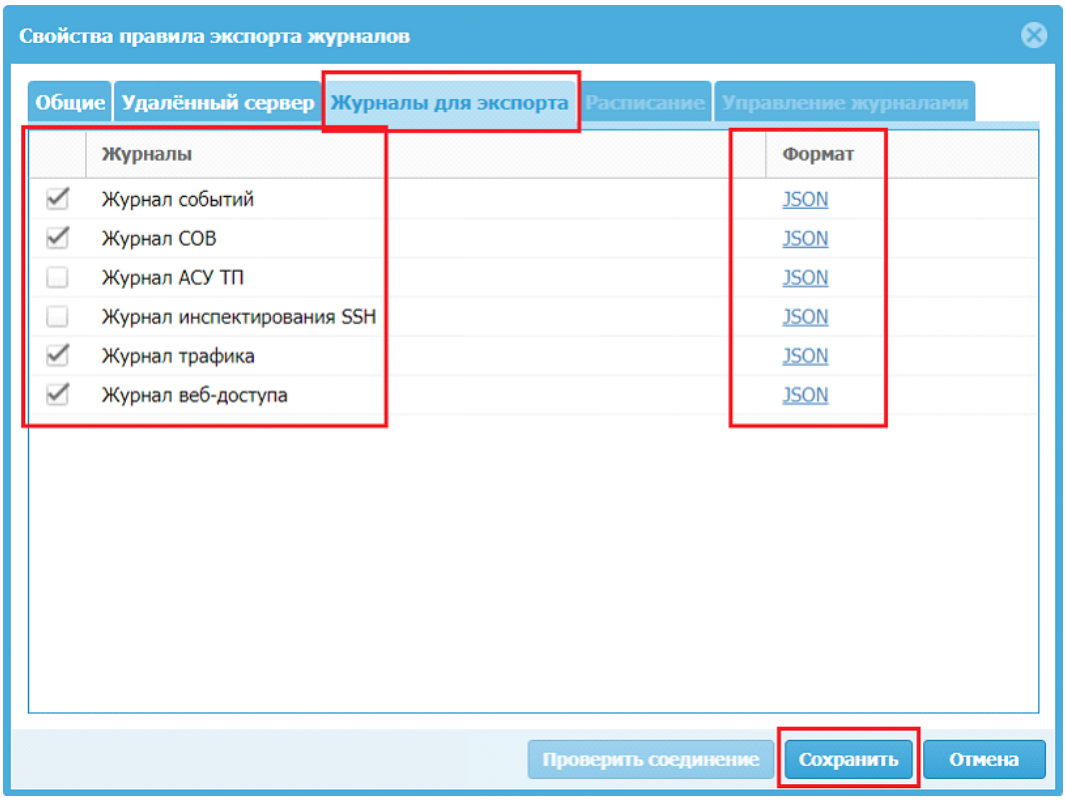


Рис. 212 – Выбор журналов для экспорта

- **Журнал событий**;
- **Журнал СОВ**;
- **Журнал трафика**;
- **Журнал веб-доступа**;
- для всех журналов в графе **Формат** установите значение "JSON".

- Нажмите кнопку **Сохранить**.

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **UserGate-UTM**.

4.3.20 ViPNet Coordinator

Программно-аппаратные комплексы (ПАК) ViPNet Coordinator HW 4 — модельный ряд шлюзов безопасности, предназначенных для построения виртуальной сети ViPNet и обеспечения безопасной передачи данных между её защищенными сегментами, а также фильтрации IP-трафика.

ViPNet Coordinator имеет возможность отправлять события журнала регистрации IP-пакетов (формат CEF) и журнала работы служб *iplircfg*, *mftpd*, *failoverd*.

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	ViPNet
Номер (Порт)	2211
Вендор	infotecs
Тип	HW
Профиль сбора	«Модуль udp_input»

Примечание: *По умолчанию источник ViPNet-Coordinator не имеет возможность изменить порт и протокол отправки событий, поэтому сбор событий агентом сбора лог-коллектора происходит по 514/UDP*.

Внимание! *Все команды выполняются в режиме администратора. Чтобы войти в режим администратора введите enable и пароль администратора. В консольной строке знак > рядом с именем хоста сменится на #.*

Настройка источника включает в себя следующие шаги:

1. Настройка журнала работы служб.
2. Настройка журнала регистрации IP-пакетов.
3. Включение источника в платформе.

Шаг 1. Настройка журнала работы служб

Внимание! *При настройке удаленного протоколирования событий, прекращается ведение журналов на локальном хосте. Если ViPNet Coordinator HW используется в режиме кластера горячего резервирования, то необходимо настроить удаленное протоколирование на обоих узлах*.

Задайте уровень ведения журнала в секции `debug` файлов конфигурации `iplir.conf`, `failover.ini`, `mftp.conf`:

```
[debug]
debuglevel= 3
debuglogfile= syslog:daemon.debug
```

Где:

- `debuglevel= 3` – уровень важности событий, записываемых в журнал. Возможные значения: от -1 до 4 (по умолчанию 3, -1 - отключает ведение журнала);
- `debuglogfile= syslog:daemon.debug` – источник информации, выводимой в журнал. Значение `syslog:<facility.level>`, где:
  - `facility` – процесс, формирующий информацию. Возможные значения: kern (ядро), user (пользовательские программы) или daemon (системные службы);
  - `level` – уровень важности информации. Возможные значения: err (ошибка), info (информационное сообщение) или debug (отладочная информация).

Примечание: *обычно достаточно указанных параметров по умолчанию*.

Если вы хотите изменить настройки службы, то необходимо выполнить следующие действия:

1. Остановите соответствующую службу.
2. Внесите изменения в конфигурационный файл службы.
3. Сохраните изменения.
4. Закройте редактор и запустите службу.

Включите отправку событий журнала служб, указав IP-адрес агента сбора лог-коллектора:

```
hostname# machine set loghost <IP-адрес агента сбора лог-коллектора>
```

Добавьте разрешающее исходящее правило, указав IP-адрес агента сбора лог-коллектора:

```
hostname# firewall local add src @local dst <IP-адрес агента сбора лог-коллектора>
udp dport 514 pass
```

Шаг 2. Настройка журнала регистрации IP-пакетов в формате syslog + CEF

Остановите службу `iplircfg` и откройте файл конфигурации `iplir.conf`. В секции `misc` укажите параметры экспорта журнала регистрации IP-пакетов:

```
cef_enabled= yes
cef_ip= <IP-адрес агента сбора лог-коллектора>
cef_port= <порт для данного источника> (по умолчанию: 514)
```

Где:

- `cef_enabled= yes` – разрешение экспорта записей журнала по сети;
- `cef_ip` – IP-адрес лог-коллектора, на который будут отправляться сообщения CEF;
- `cef_port` – порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

Сохраните изменения (сочетание клавиш **Ctrl+O**), закройте редактор (сочетание клавиш **Ctrl+X**).

Запустите службу `iplircfg`:

```
hostname# iplir start
```

Добавьте разрешающее исходящее правило, указав IP-адрес агента сбора лог-коллектора:

```
hostname# firewall local add src @local dst <IP-адрес агента сбора лог-коллектора> udp dport 514 pass
```

Настройка журналирования IP-пакетов для определенного интерфейса

При необходимости вы можете настроить журналирование IP-пакетов для определенного интерфейса. Данная настройка производится в файле конфигурации интерфейса `iplir.conf-eth<номер>` при помощи команды:

```
hostname# iplir config eth<номер>
```

Секция [db]:

- `registerall= <on/off>` – включение или выключение регистрации записей обо всех пакетах. Допустимые значения:
  - `off` – регистрируются только заблокированные пакеты (значение по умолчанию);
  - `on` – регистрируются все пакеты.

Секция [cef]:

- `event= blocked` – формирование сообщений CEF (которые и будут отправляться) при регистрации IP-пакетов, проходящих через интерфейс
  - `all` – для всех IP-пакетов;
  - `blocked` – только для блокированных IP-пакетов.
- `exclude=` – указываются номера типов событий, которые должны быть исключены из формирования сообщений CEF (указываются номера типов событий через запятую).

Примечание: *номера типов событий указаны в документе "02 ViPNet Coordinator HW 4. Настройка в CLI.pdf", входящий в Комплект документации на ViPNet Coordinator HW 4*.

Сохраните изменения (сочетание клавиш **Ctrl+O**), закройте редактор (сочетание клавиш **Ctrl+X**).

Запустите службу `iplircfg`:

```
hostname# iplir start
```

Добавьте разрешающее исходящее правило, указав IP-адрес агента сбора лог-коллектора:

```
hostname# firewall local add src @local dst <IP-адрес агента сбора лог-коллектора> udp dport 514 pass
```

Шаг 3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **ViPNet**.

4.3.21 WireGuard EdgeSecurity

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	EdgeSecurity-WireGuard
Номер (Порт)	2182

Характеристика	Значение
Вендор	EdgeSecurity
Тип	WireGuard
Профиль сбора	«Модуль tcp_input»

Примечание: *WireGuard по умолчанию не записывает свои события. Журналирование событий WireGuard можно включить, используя модуль ядра wireguard linux (в версиях ядра 5.6 или новее), включив ведение журнала dyndbg, который отправляет сообщения журнала в буфер сообщений ядра.*

Для настройки источника выполните следующие действия:

1. Проверьте состояние журналирования событий системы:

   ```
   # cat /sys/kernel/debug/dynamic_debug/control | grep "wireguard
   ```

2. Если после выполнения команды ничего не выводится, то включите журналирование событий:

   ```
   # modprobe wireguard
   # echo module wireguard +p > /sys/kernel/debug/dynamic_debug/control
   ```

   События можно посмотреть любой из следующих команд:

   ```
   # dmesg | grep “wireguard
   # tail -n 300 /var/log/kern.log
   ```

3. Настройте запись журналов в отдельный файл `/var/log/wireguard.log`:

   - создайте файл:

     ```
     # nano /etc/rsyslog.d/10-wireguard.conf
     ```

   - добавьте в него следующие настройки:

     ```
     :msg,contains,"wireguard: " /var/log/wireguard.log
     & stop
     ```

4. Для настройки отправки событий источника на агент сбора лог-коллектора создайте файл `nano /etc/rsyslog.d/30-wireguard-lc.conf` и укажите следующие настройки:

```
module(load="imfile" PollingInterval="5")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/wireguard.log"
      Tag="wireguard"
      ruleset="sendlc")

ruleset(name="sendlc")
{
    action(type = "omfwd"
        Target="<IP-адрес агента сбора лог-коллектора>"
        Port="<порт, указанный в настройках профиля сбора>"
        Protocol="udp"
        ResendLastMSGOnReconnect="on"
```

```
        action.resumeRetryCount="100"
        queue.type="linkedList"
        queue.size="10000")
    stop
}
```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **EdgeSecurity-WireGuard**.

4.3.22 Zeek (IDS Bro-ids)

Zeek (ранее **Bro**) относится к сетевым системам обнаружения вторжения, основанная на Unix-системах, которая наблюдает за сетевыми данным и обнаруживает подозрительную активность.

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Zeek
Номер (Порт)	2685
Вендор	Zeek
Тип	IDS
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. В политике системы `/opt/zeek/share/zeek/site/local.zeek` включите запись журналов в формате JSON:

   ```
   # Output in JSON format
   @load policy/tuning/json-logs.zeek
   ```

2. Запустите `zeekctl deploy` для применения конфигурации.
3. При необходимости удостоверьтесь, что конфигурация применилась правильно. Для этого введите команду ниже и проверьте статус узла:

   ```
   # zeekctl status
   ```

4. Проверьте отображение событий в формате JSON:

   ```
   # tail /opt/zeek/logs/current/conn.log
   ```

5. В конфигурационный файл `local.zeek` добавьте поля `stream` и `process`:

   ```
   type Extension: record {
    stream: string &log;
    process: string &log;
    };

   function add_extension(path: string): Extension
   ```

```
{
return Extension($stream = path,
$process = "zeek");
}

redef Log::default_ext_func = add_extension;
```

6. Запустите `zeekctl deploy` для применения конфигурации.

   Внимание! *На данном этапе можно получить ошибку Your interface is likely receiving invalid TCP checksums, most likely from NIC checksum offloading. By default, packets with invalid checksums are discarded by Zeek unless using the -C command-line option or toggling the 'ignore_checksums' variable. Alternatively, disable checksum offloading by the network adapter to ensure Zeek analyzes the actual checksums that are transmitted. Из-за нее могут не приходит нужные поля в журналах. Для исправления ошибки в конфигурационный файл local.zeek добавьте настройку: edef ignore_checksums = T;.*

7. Для сбора журналов создайте файл `/etc/rsyslog.d/zeek-ssh.conf` со следующими настройками:

```
module(load="imfile" PollingInterval="5")
input(type="imfile"
    reopenOnTruncate="on"
    File="/opt/zeek/logs/current/ssh.log"
    Tag="zeekssh:"
        ruleset="zeekssh")
ruleset(name="zeekssh")
{
    action(type="omfwd"
        Target="<IP-адрес агента сбора лог-коллектора"
        Port="<порт, указанный в настройках профиля сбора>"
        Protocol="tcp"
        ResendLastMSGOnReconnect="on"
        action.resumeRetryCount="100"
        queue.type="linkedList"
        queue.size="10000")
    stop
}
```

8. Сохраните изменения и перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog
```

9. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Zeek**.

4.4 Решения System Security

При работе по подключению решений System Security в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.4.1 Confident Dallaslock

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	DallasLock
Номер (Порт)	2676
Вендор	Confident
Тип	SZI
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Войдите в интерфейс администратора Dallaslock и перейдите на вкладку **Параметры безопасности → Аудит**.
2. Выберите пункт **Выгрузка журналов**, вызовите контекстное меню и выберите пункт **Свойства** (см. «Рис. 213»).

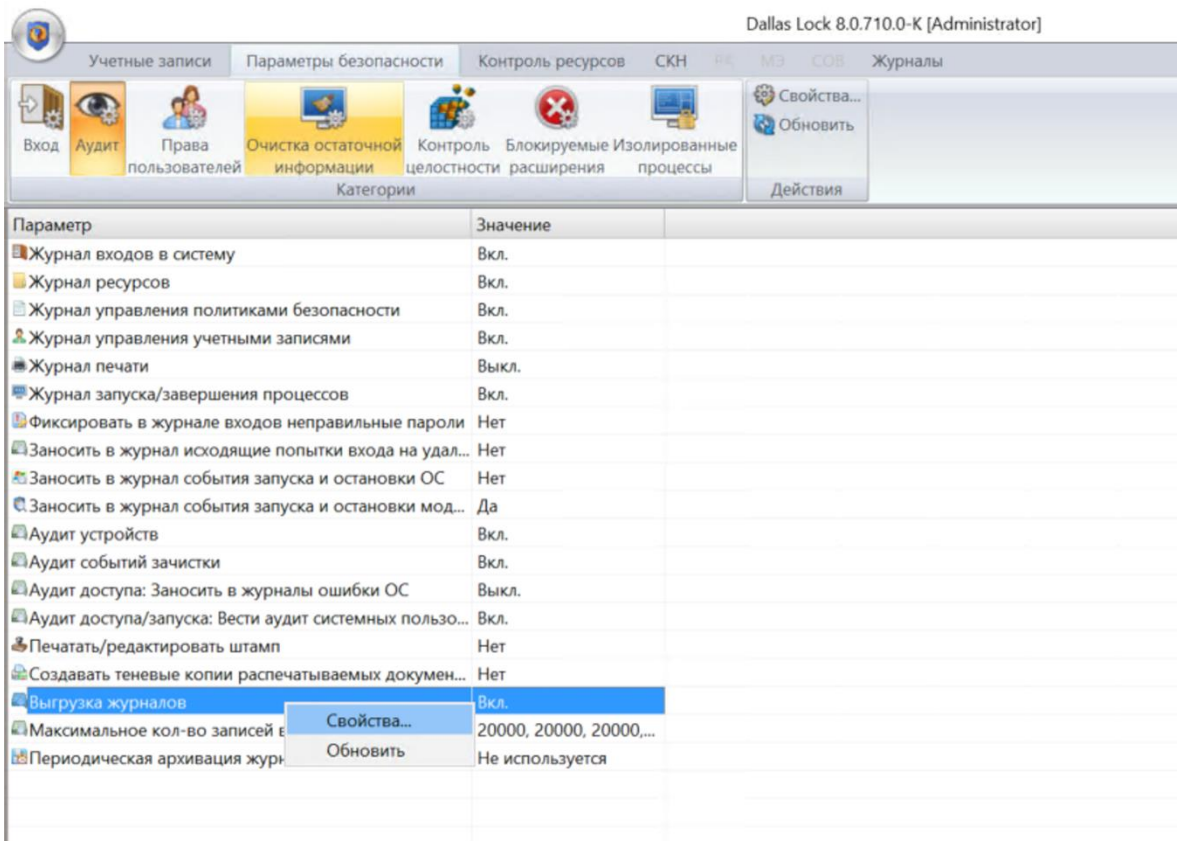


Рис. 213 – Dallaslock. Настройка аудита

3. Откроется окно **Выгрузка журналов** (см. «Рис. 214»).

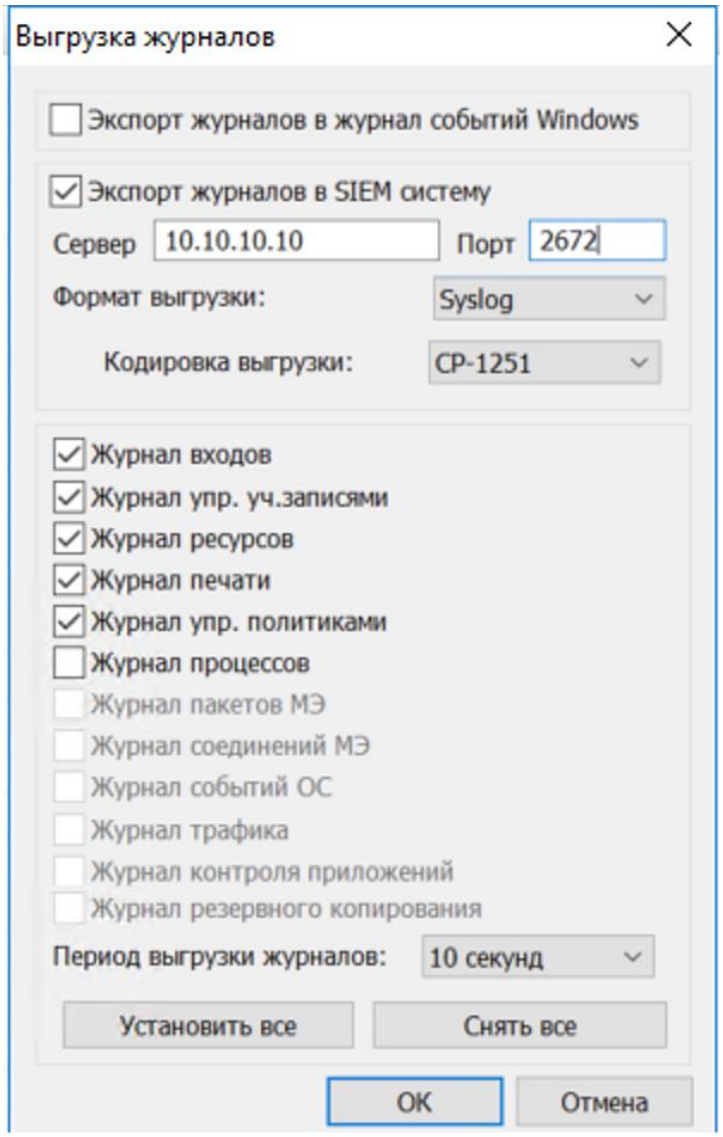


Рис. 214 – Окно "Выбор журналов"

4. В окне выполните следующие действия:
   - установите флаг **Экспорт журналов в SIEM систему**;
   - в поле **Сервер** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Порт** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - в поле **Формат выгрузки** из выпадающего списка выберите значение "*Syslog*";
   - в поле **Кодировка выгрузки** из выпадающего списка выберите значение "*CP-1251*";
   - выберите журналы для отправки, установив соответствующие флаги;
   - нажмите кнопку **OK**.
5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **DallasLock**.

4.4.2 Kaspersky Anti Targeted Attack Platform

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Kaspersky-Anti-Targeted-Attack-Platform
Номер (Порт)	2602
Вендор	Kaspersky
Тип	APT-protection
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс системы Kaspersky Anti Targeted Attack под учетной записью с правами администратора.
2. Перейдите в раздел **Settings** → **SIEM system** (см. «Рис. 215»).

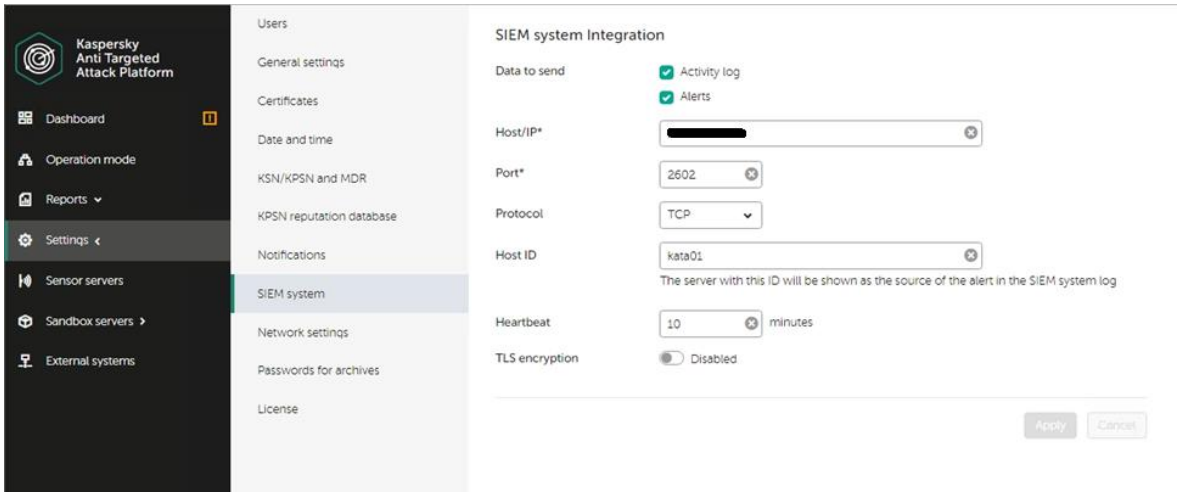


Рис. 215 – Применение настройки отправки событий Kaspersky Anti Targeted Attack

3. Укажите следующие настройки:
   - в поле **Data to send** установите флаги "*Activity log*" и "*Alerts*";
   - в поле **Host/IP** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Port** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - в поле **Protocol** из выпадающего списка выберите протокол взаимодействия: "*TCP*";
   - в поле **Host ID** укажите ID устройства;
   - в поле **Heartbeat** укажите интервал отправки событий с информацией о состоянии системы;

- при необходимости шифрования отправки событий в поле **TLS encryption** установите переключатель в "*Enable*".

4. Для сохранения изменений нажмите кнопку **Apply**.
5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Kaspersky-Anti-Targeted-Attack-Platform**.

4.4.3 Kaspersky Secure Mail Gateway

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Kaspersky-Secure-Mail-Gateway
Номер (Порт)	2608
Вендор	Kaspersky
Тип	KSMG
Профиль сбора	«Модуль tcp_input»

Настройка источника включает в себя следующие шаги:

1. Настройка SSH подключения Kaspersky Secure Mail Gateway.
2. Настройка экспорта событий в формате CEF.
3. Настройка отправки событий в **Платформу Радар**.
4. Включение источника в платформе.

Шаг 1. Настройка SSH подключения Kaspersky Secure Mail Gateway

1. Откройте терминал и выполните команду:

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

2. На консоль будет выведено следующее сообщение:

   ```
   Enter file in which to save the key (/home/user/.ssh/id_rsa):
   ```

3. Нажмите на клавишу **Enter**. Далее система предложит ввести кодовую фразу для дополнительной защиты SSH-подключения:

   ```
   Enter passphrase (empty for no passphrase):
   ```

4. Этот шаг можно пропустить. При ответе на этот и следующий вопрос просто нажмите клавишу **Enter**. После этого ключ будет создан.

5. Выведете ключ в консоль и **скопируйте** его в буфер обмена:

   ```
   $ cat ~/.ssh/id_rsa.pub
   ```

   Примечание: убедитесь, что вы скопировали все содержимое ключа: тело ключа, адрес электронной почты, без дополнительных символов и знаков переноса. Для проверки вы можете вставить скопированный ключ в блокнот - должна получиться одна строка.

6. Войдите в веб-интерфейс Kaspersky Secure Mail Gateway и перейдите в раздел **Settings → Application access → SSH access** (см. «Рис. 216»).

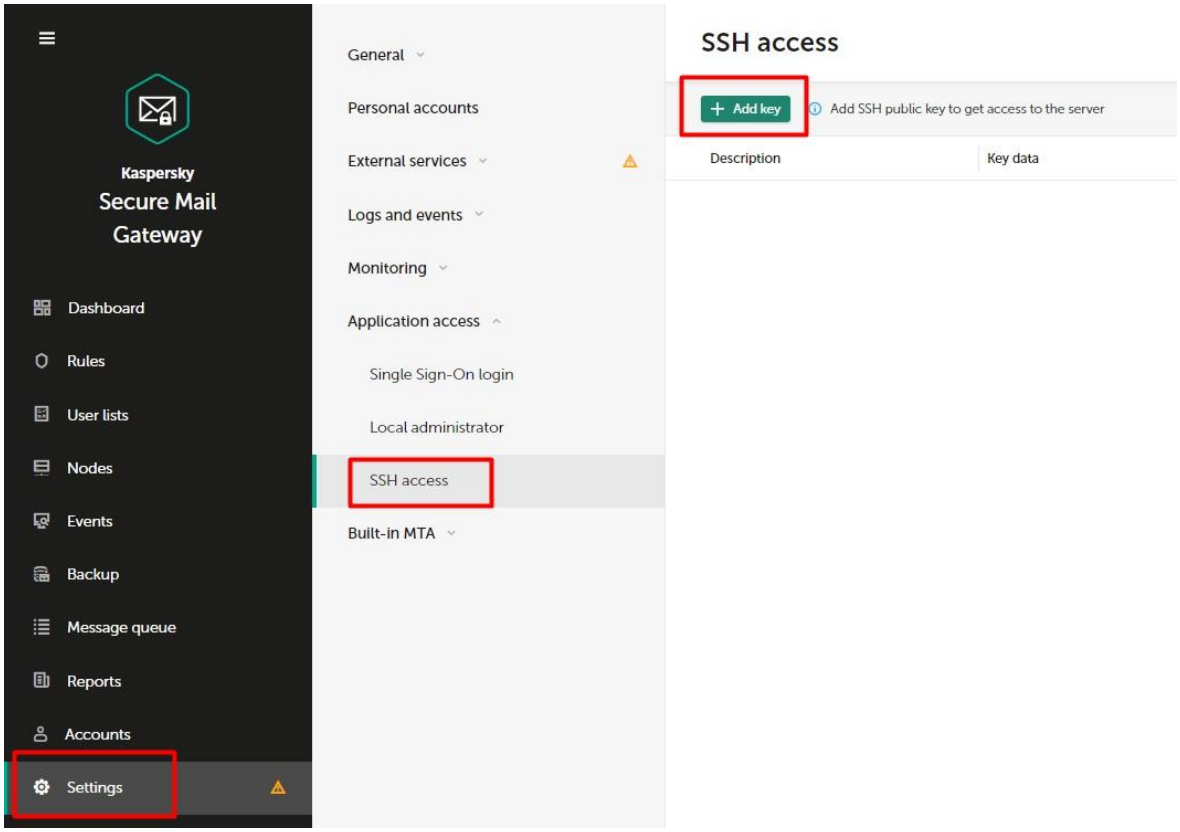


Рис. 216 – Kaspersky Secure Mail Gateway. SSH access

7. Нажмите на кнопку **Add key**. Откроется окно "Add an SSH public key" (см. «Рис. 217»).

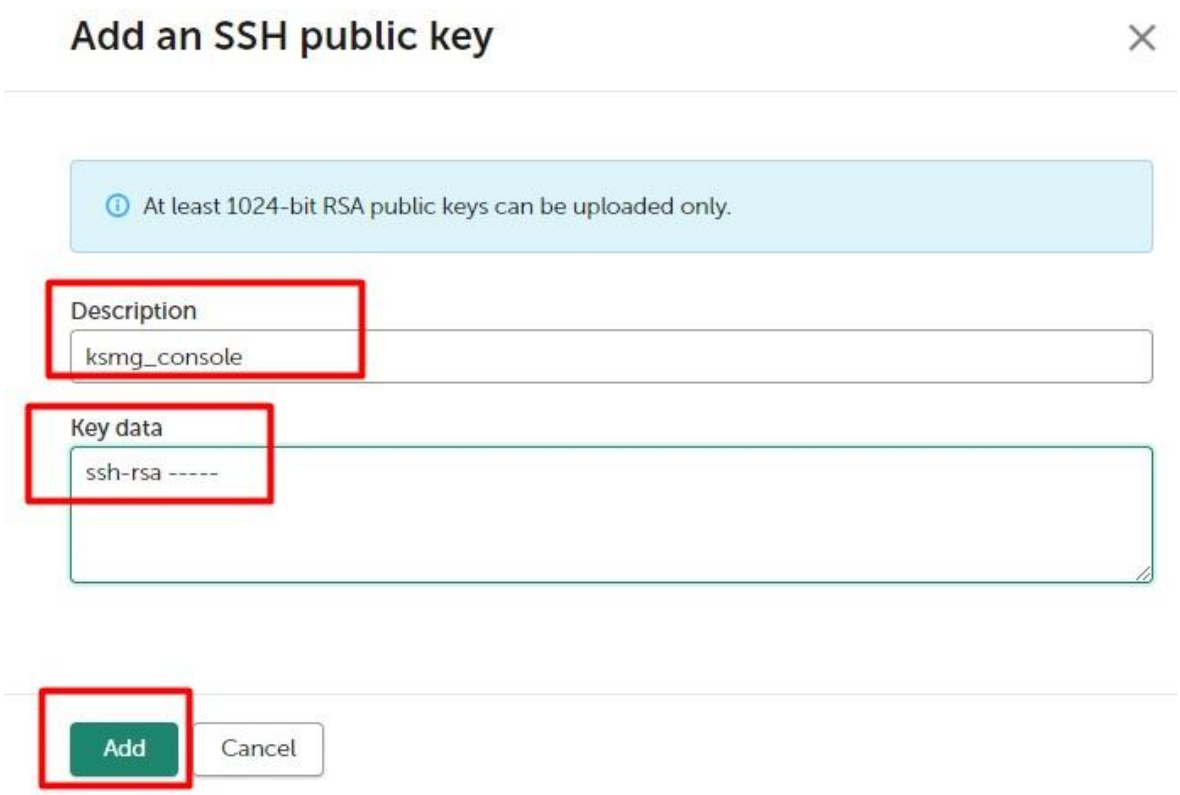


Рис. 217 – Окно "Add an SSH public key"

8. В поле **Description** укажите дополнительную информацию о загружаемом ключе SSH.
9. В поле **Key Data** вставьте скопированный ранее открытый ключ SSH.
10. Нажмите на кнопку **Add**.

Открытый ключ SSH будет добавлен. Администратор системы Kaspersky Secure Mail Gateway сможет подключиться к любому узлу кластера при наличии соответствующего ключа SSH.

При необходимости проверьте подключение командой:

```
# ssh -vvv -i .ssh/ksmg_rsa root@your-ksmg-ip-address
```

Где:

- `.ssh/ksmg_rsa` - путь к вашему ключу SSH;
- `your-ksmg-ip-address` - IP-адрес Kaspersky Secure Mail Gateway.

Шаг 2. Настройка экспорта событий в формате CEF

1. Подключитесь к консоли управления виртуальной машиной Kaspersky Secure Mail Gateway под учетной записью root, используя ключ SSH. Запустится режим **Technical Support Mode**.
2. Откройте файл с параметрами экспорта событий:

   `/opt/kaspersky/ksmg/share/templates/core_settings/event_logger.json.template`
3. В блоке **siemSettings** выполните следующие настройки:
   - укажите категорию (facility) для syslog. Рекомендуется указать такую категорию (facility) для syslog, которая не используется другими программами на сервере. По умолчанию установлено значение local2. Допустимые значения:

     `Auth.`
     `Authpriv.`
     `Cron.`
     `Daemon.`
     `Ftp.`
     `Lpr.`
     `Mail.`
     `News.`
     `Syslog.`
     `User.`
     `Uucp.`
     `Local0.`
     `Local1.`
     `Local2.`
     `Local3.`
     `Local4.`
     `Local5.`
     `Local6.`
     `Local7.`

- включите экспорт журналов установив значение параметра `enabled` равным `true`;
- задайте уровень детализации экспорта журналов, установив одно из следующих значений параметра `logLevel`:
  - `Error` – экспорт событий, связанных с возникновением ошибок;
  - `Info` – экспорт всех событий.

  Пример:

```
"siemSettings":
     {
     "enabled": true,
     "facility": "Local2",
     "logLevel": "Info",
 }
```

- для корректного выполнения операции парсинга **Платформой Радар** всех журналов поставьте пробел в следующей строке (см. «Рис. 218»).

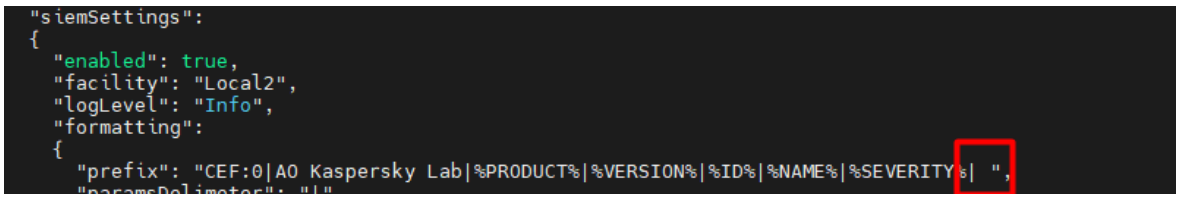


Рис. 218 – Редактирование файла конфигурации.

Примечание: *источник отправляет часть логов без обязательного поля Extension. Пробел решает эту проблему и все журналы проходят операцию парсинга правильно*.

4. Откройте файл /etc/rsyslog.conf и выполните следующие настройки:
   - измените строку:

     `*.info;mail.none;authpriv.none;cron.none;local0.none;local1.none /var/log/messages`

     указав в ней значение facility:

     `*.info;mail.none;authpriv.none;cron.none;local0.none;local1.none;<категория (facility), выбранная на шаге 2>.none /var/log/messages`
   - добавьте в файл следующую строку:

     `<категория (facility), выбранная на шаге 2>.* -/var/log/ksmg-cef-messages`
5. Создайте файл `/var/log/ksmg-cef-messages` и настройте права доступа к нему. Для этого выполните команды:

```
# touch /var/log/ksmg-cef-messages
# chown root:klusers /var/log/ksmg-cef-messages
# chmod 640 /var/log/ksmg-cef-messages
```

6. Настройте правила ротации файлов с экспортированными событиями. Для этого добавьте в файл `/etc/logrotate.d/ksmg-syslog` следующие строки:

```
/var/log/ksmg-cef-messages

{
    size 500M
    rotate 10
    notifempty
    sharedscripts
    postrotate
    /usr/bin/systemctl kill -s HUP rsyslog.service >/dev/null 2>&1 || true
    endscript
}
```

7. Перезапустите службу `rsyslog`. Для этого выполните команду:

   ```
   # service rsyslog restart
   ```

8. Для синхронизации параметров между узлами кластера и применения изменений, внесенных в конфигурационный файл, выполните следующие действия:

   - войдите в веб-интерфейс Kaspersky Secure Mail Gateway и перейдите в раздел **Параметры → Журналы и события → События**;
   - внесите произвольное изменение в значение любого параметра и нажмите на кнопку **Сохранить**;
   - после этого вы можете вернуть исходное значение измененного параметра. Экспорт событий в формате CEF будет настроен.

Шаг 3. Настройка отправки событий в Платформу Радар

Внимание! *Действия, описанные в разделе, необходимо выполнить на каждом узле кластера, события с которого вы хотите отправлять в* ***Платформу Радар****. Перед внесением изменений в конфигурационные файлы рекомендуется сделать их резервные копии*.

1. Подключитесь к консоли управления виртуальной машиной Kaspersky Secure Mail Gateway под учетной записью root, используя ключ SSH. Запустится режим **Technical Support Mode**.
2. Укажите необходимое значение facility, IP-адрес лог-коллектора и порт, по которому лог-коллектор будет принимать события от данного источника: "*2608*". Для этого добавьте в конец файла `/etc/rsyslog.conf` следующие строки:

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   $ActionResumeRetryCount -1
   <категория (facility)>.* @@<IP-адрес лог коллектора>:<порт(TCP)>
   ```

3. Перезапустите службу `rsyslog`. Для этого выполните команду:

   ```
   # service rsyslog restart
   ```

Шаг 4. Включение источника в платформе

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Kaspersky-Secure-Mail-Gateway**.

4.4.4 Papercut-NG

PaperCut NG - это средство отслеживания заданий печати и отчетности.

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Papercut-NG
Номер (Порт)	2889
Вендор	Papercut
Тип	Print-Management
Профиль сбора	«Модуль odbc_input»

Настройка источника включает в себя следующие шаги:

1. Переключение используемой базы данных на MSSQL.
2. Настройка сетевого подключения к MSSQL.
3. Настройка ODBC драйвера.
4. Включение источника в платформе.

Шаг 1. Переключение базы данных на MSSQL

По умолчанию события аудита хранятся в базе данных Papercut-NG, которая использует Apache-Derby, к которой нет возможности подключиться для извлечения журналов. Чтобы была возможность подключаться к базе данных и свободно получать из неё нужные события, необходимо переключить работу приложения на базу данных от MSSQL.

Примечание: *перед началом работы скачайте и установите MSSQL и SSMS (sql management studio).*

Для переключения базы данных на MSSQL выполните следующие действия:

1. Остановите службу **PaperCut Application Server**.
2. Откройте командную строку и перейдите в каталог с установленным приложением:
   ```
   cd "C:\Program Files\PaperCut NG\server\bin\win"
   ```
3. Выполните экспорт существующей базы данных:
   ```
   db-tools export-db
   ```
4. В установленной MSSQL создайте базу данных papercut и пользователя **papercut**.
5. Выдайте пользователю **papercut** права владельца базой данных.

6. Настройте конфигурационный файл приложения **Papercut** C:\Program Files\PaperCut NG\server\server:

   - закомментируйте строку database.type=Internal;
   - раскомментируйте строки относящиеся к MSSQL;
   - укажите наименование базы данных, имя и пароль владельца базы данных:

```
### Database Settings ###
#database.type=Internal
#database.driver=
#database.url=
#database.username=
#database.password=
# MS SQLServer connection example
# IMPORTANT: The username below is a SQL Server user, not a Windows user
# For Integrated/Windows authentication add integratesSecurity=true
property to the connection string
# Eg:
jdbc:sqlserver://localhost1433;databasename=papercut;integratesSecurity=t
rue
database.type=SQLServer
database.driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
database.url=jdbc:sqlserver://localhost:1433;databaseName=papercut
database.username=papercut
database.password=papercut
```

Шаг 2. Настройка сетевого подключения к MSSQL

1. На ОС Windows перейдите в **Управление компьютером → Службы и приложения → Диспетчер конфигурации SQL Server → Сетевая конфигурация SQL Server** и включите протокол **TCP/IP** (см. «Рис. 219»).

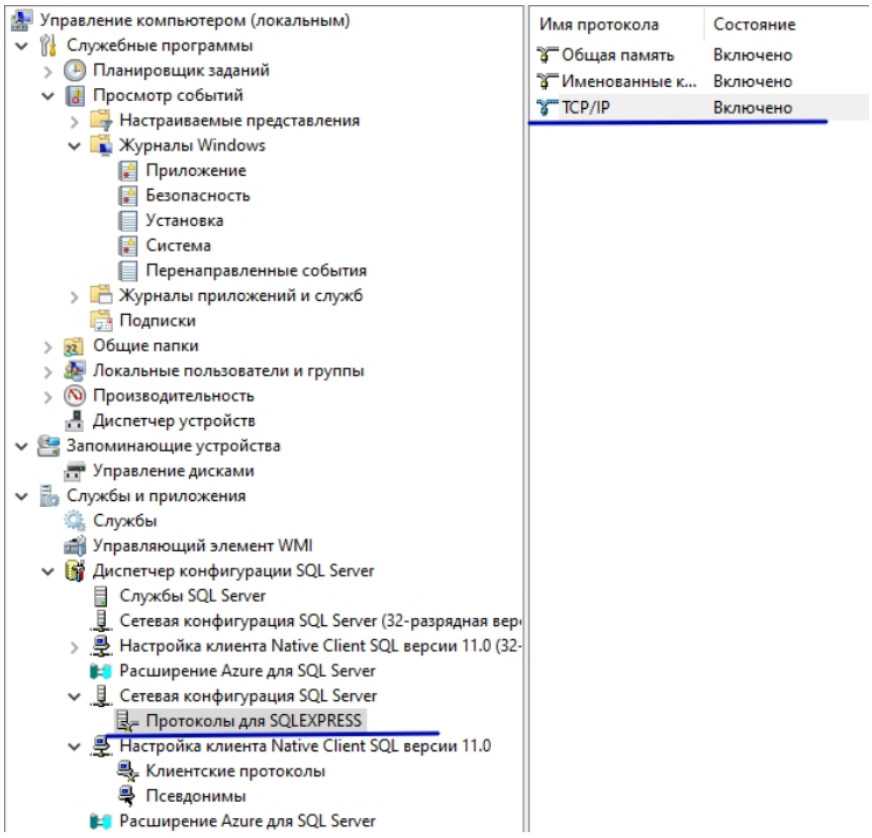


Рис. 219 – Сетевая конфигурация SQL Server. Настройка протоколов

2. Вызовите контекстное меню и выберите пункт свойства. Откроется окно "Свойства TCP/IP" (см. «Рис. 220»).

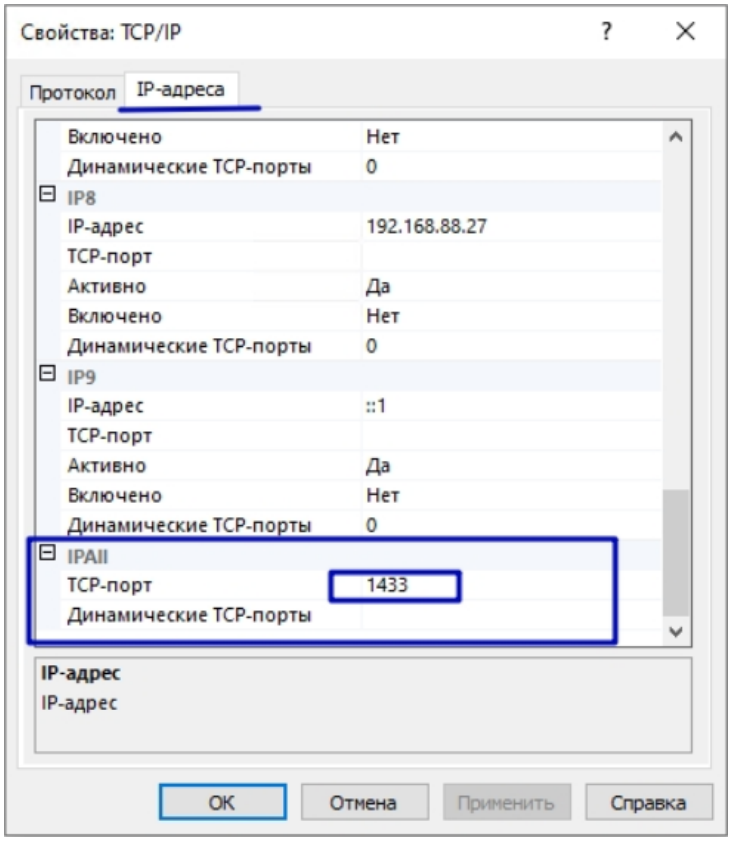


Рис. 220 – Окно "Свойства TCP/IP". Вкладка "IP-адреса"

3. Перейдите на вкладку "IP-адреса" и в блоке **IPALL** укажите порт "*1433*" (см. рисунок 10).
4. Перезапустите службу **SQL сервер**.
5. Запустите командную строку и инициализируйте новую базу данных:

```
cd "C:\Program Files\PaperCut NG\server\bin\win
db-tools init-db
```

6. Загрузите «backup» базы данных:

```
cd "C:\Program Files\PaperCut NG\server\bin\win
db-tools import-db "backup file name"
```

7. Запустите службу **PaperCut Application Server**.

Шаг 3. Настройка ODBC драйвера

Для извлечения данных из базы с помощью лог-коллектора необходимо настроить ODBC драйвер:

1. На ОС Windows перейдите в **Панель управления → Система и безопасность → Администрирование**.
2. Откройте "Источники данных ODBC (64-разрядная версия)", перейдите на вкладку "Системный DSN" и нажмите кнопку **Добавить**. Откроется окно "Создание нового источника данных" (см. «Рис. 221»).

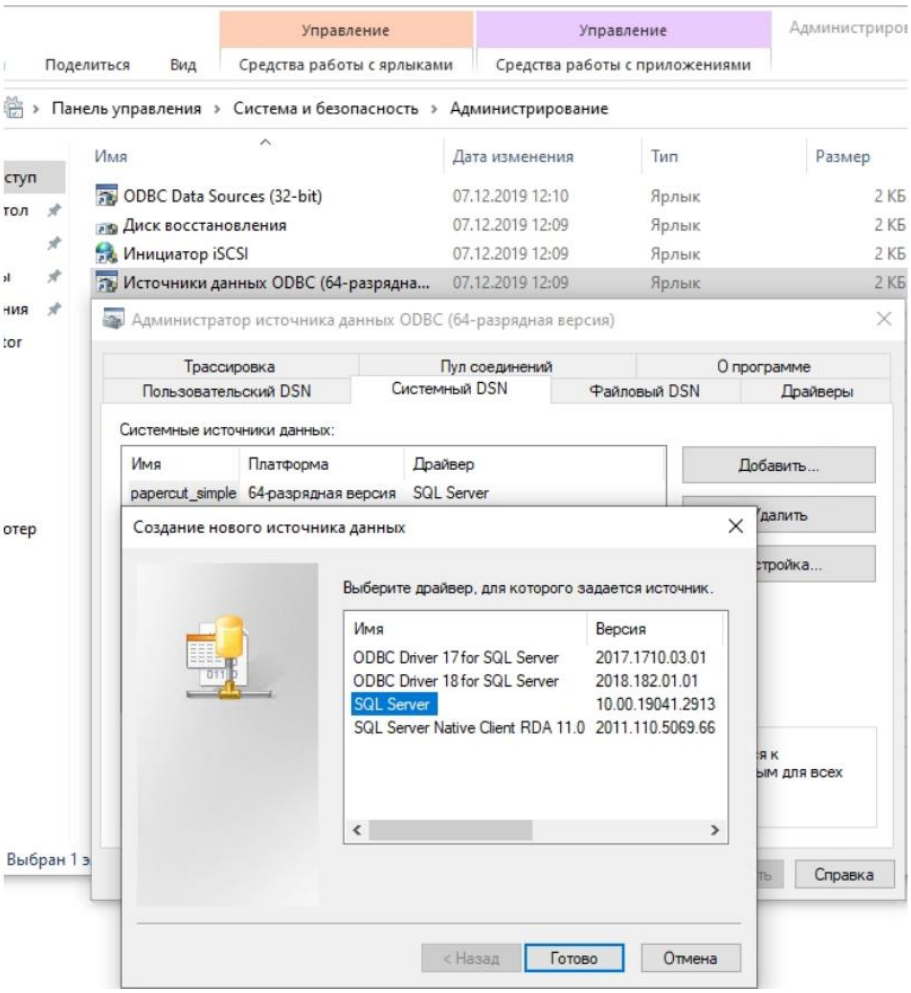


Рис. 221 – Окно "Создание нового источника данных"

3. Выберите драйвер SQL Server и нажмите **Далее**.
4. Укажите наименование нового источника и наименование вашего SQL экземпляра. Нажмите **Далее**.
5. Включите проверку подлинности учетной записи SQL Server, установив соответствующий флаг и укажите логин и пароль sql-пользователя. Нажмите **Далее**.
6. На последнем шаге убедитесь, что подключение к базе данных произошло успешно и нажмите кнопку **Готово**.

Шаг 4. Настройка лог-коллектора и включение источника в платформе

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Papercut-NG**.

4.4.5 Sysmon-Windows

Sysmon (System Monitor) - утилита, которая позволяет получить более полные сведения о событиях Windows.

Перед началом работы с источником рекомендуется выполнить следующие действия:

- ознакомьтесь со справочной информацией об утилите Sysmon;
- скачайте актуальную версию с официального ресурса Microsoft;

- скачайте конфигурационный файл sysmonconfig.xml.

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Sysmon-Windows
Номер (Порт)	1513
Вендор	Microsoft
Тип	Sysmon
Профиль сбора (локальный сбор)	«Модуль eventlog_input_local»
Профиль сбора (удаленный сбор)	«Модуль eventlog_input_remote»

Примечание: *для запуска утилиты необходимо, чтобы на машине, на которой планируется сбор событий, было расположено два файла: файл-установщик с расширением .bat или .exe и файл конфигурации с расширением .xml. Для удобства работы рекомендуется расположить эти файлы в одной папке*.

Для настройки источника выполните следующие действия:

1. Установите и настройте утилиту Sysmon:
   - создайте каталог C:\ProgramData\sysmon\;
   - в созданный каталог скопируйте дистрибутив и конфигурационный файл;
   - откройте командную строку от имени администратора (cmd);
   - перейдите в созданный каталог и установите утилиту:

     ```
     cd C:\ProgramData\sysmon\
     sysmon64.exe -accepteula -i sysmonconfig.xml
     ```
2. После успешной установки в **Просмотре событий Windows** (Event Viewer) появится новый журнал (Channel) **Microsoft-Windows-Sysmon/Operational**, в котором будут храниться все события.
3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Sysmon-Windows**.

4.4.6 Бастион СКДПУ НТ

Система контроля действий привилегированных пользователей «Новые технологии» (СКДПУ НТ) обеспечивает мониторинг подключений и действий, выполняемых привилегированными пользователями на администрируемых устройствах: бизнес-приложениях, базах данных, гипервизорах, серверах Windows и Unix/Linux, сетевых устройствах и т.д. СКДПУ позволяет осуществлять мониторинг подключений к ИТ-системам в реальном времени и ретроспективно, на основании архива сессий.

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Bastion-SKDPU-NT
Номер (Порт)	2300
Вендор	IT-Bastion
Тип	Access-Gateway
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс системы СКДПУ НТ под учетной записью с правами администратора.
2. Перейдите в раздел **Система → Интеграция с SIEM** и укажите следующую информацию:
   - в поле **Роутинг** из выпадающего списка выберите значение **Включено**;
   - в поле **Доменное имя или IP** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Порт** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора";
   - в поле **Протокол** из выпадающего списка выберите протокол взаимодействия: "*UDP*";
   - в поле **Log format** из выпадающего списка выберите формат отправки событий: "*rfc5424*";
   - в поле **Формат времени** из выпадающего списка выберите формат отображения времени в отправляемом событии: "*rfc3164*";
   - нажмите кнопку **«+»** для добавления конфигурации, а затем кнопку **Применить** для сохранения изменений.
3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Bastion-SKDPU-NT**.

4.4.7 Бастион СКДПУ НТ модуль UEBA

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Bastion-UEBA
Номер (Порт)	2301

Характеристика	Значение
Вендор	IT-Bastion
Тип	UEBA
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс модуля UEBA системы СКДПУ НТ под учетной записью с правами администратора.
2. Перейдите в раздел **Настройки → Конфигурация журналирования** (см. рисунок 10).

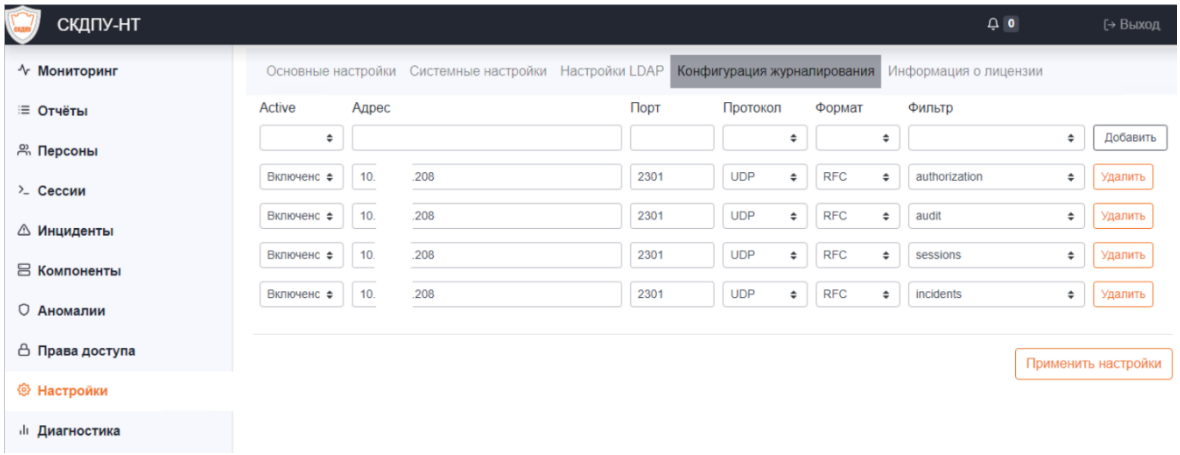


Рис. 222 – Модуль UEBA. Раздел "Конфигурация журналирования"

3. Укажите в разделе следующую информацию:
   - в поле **Active** из выпадающего списка выберите значение **Включено**;
   - в поле **Адрес** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Порт** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - в поле **Протокол** из выпадающего списка выберите протокол взаимодействия: "*UDP*";
   - в поле **Формат** из выпадающего списка выберите формат отправки событий: "*RFC*";
   - в поле **Фильтр** из выпадающего списка выберите тип событий, отправляемых в платформу: "*authorization*", "*audit*", "*sessions*" или "*incidents*";
   - нажмите кнопку **Добавить** для добавления конфигурации. Добавьте таким образом необходимое количество конфигураций;
   - нажмите кнопку **Применить настройки** для сохранения всех добавленных конфигураций.
4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Bastion-UEBA**.

4.5 Решения Endpoint Security

При работе по подключению решений Endpoint Security в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.5.1 ESET Security Management Center

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	ESET-Security-Management-Center
Номер (Порт)	2609
Вендор	ESET
Тип	SMC
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс системы ESET Protect (см. «Рис. 223»).

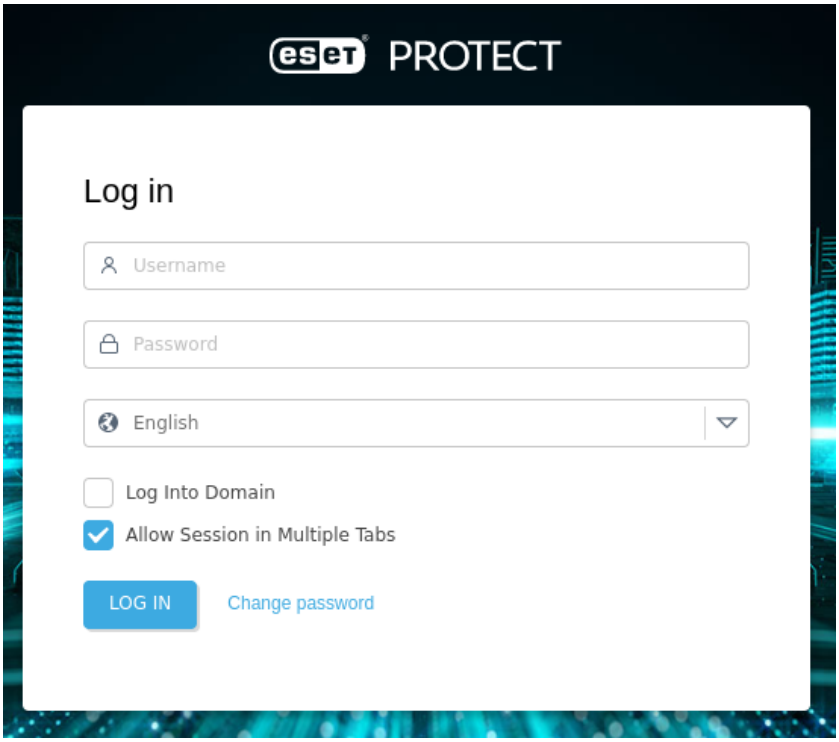


Рис. 223 – Вход в систему ESET Protect

2. Перейдите в настройки системы и откройте **Advanced settings** (см. «Рис. 224»).

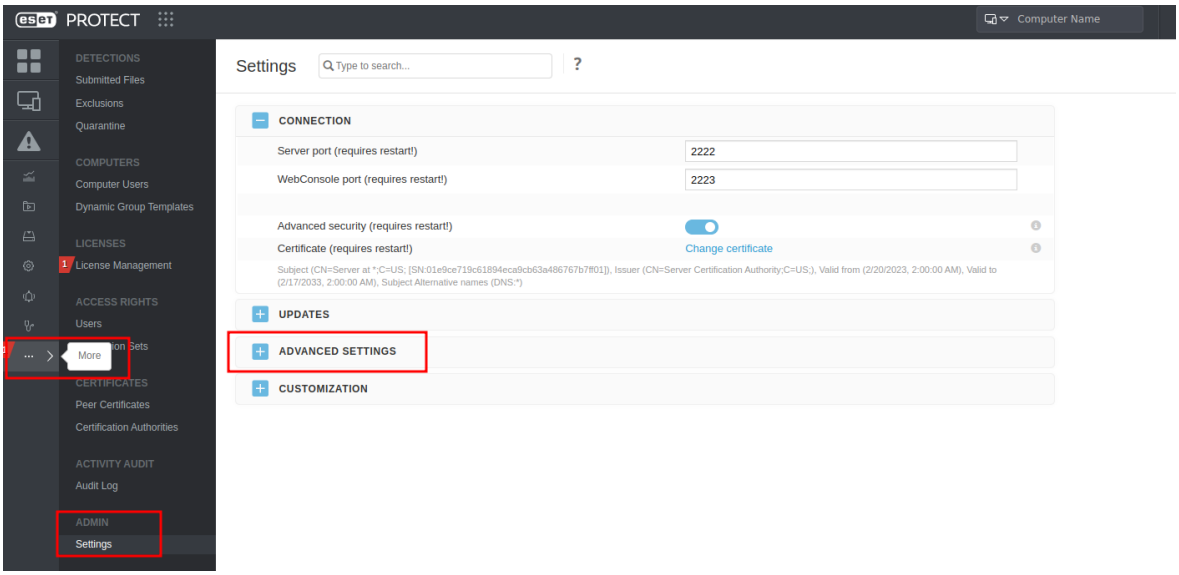


Рис. 224 – Вход в систему ESET Protect

3. В блоке **SYSLOG SERVER** (см. «Рис. 225») укажите следующие настройки:

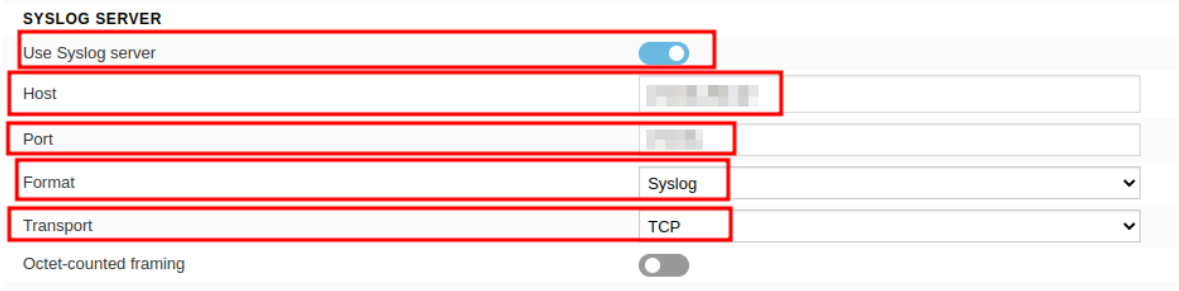


Рис. 225 – Настройка SYSLOG SERVER

- в поле **Use Syslog server** установите переключатель в положение "включен";
- в поле **Host** укажите IP-адрес агента сбора лог-коллектора;
- в поле **Формат** выберите значение "*Syslog*";
- в поле **Transport** выберите протокол взаимодействия: "*TCP*".

4. В блоке **LOGGING** (см. «Рис. 226») укажите следующие настройки:

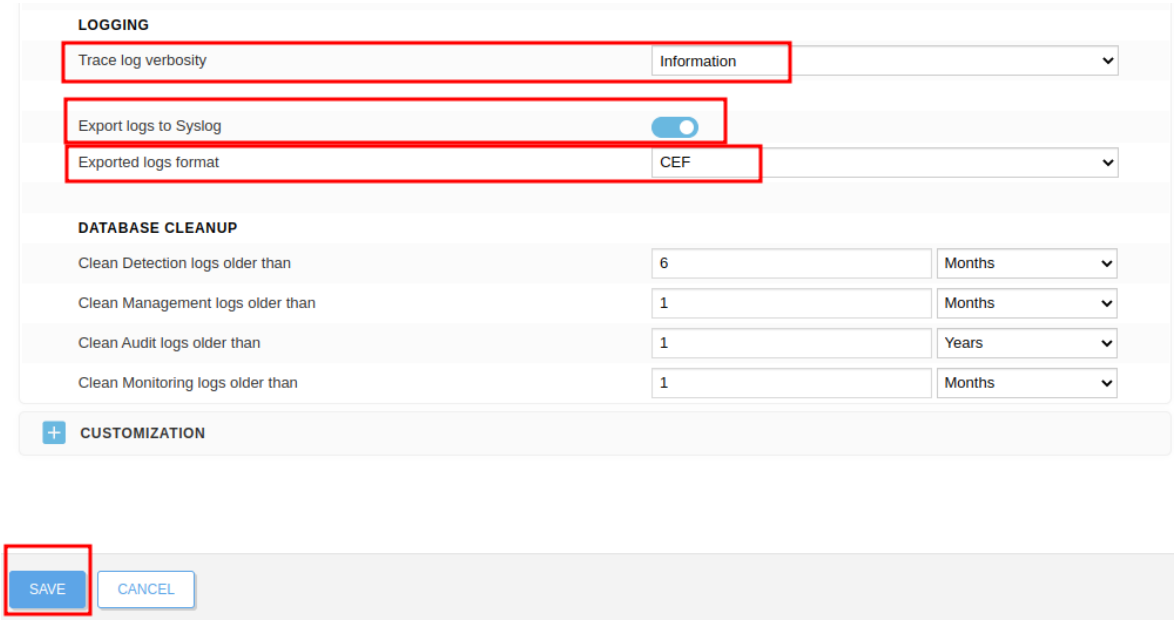


Рис. 226 – Настройка LOGGING

- в поле **Trace log verbosity** из выпадающего списка выберите уровень детализации журналов: "*Information*";
- в поле **Export logs to Syslog** включите экспорт журналов в формате `syslog`;
- в поле **Export logs format** из выпадающего списка выберите значение "*CEF*".

5. Нажмите кнопку **SAVE**.
6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **ESET-Security-Management-Center**.

4.5.2 FireEye HX

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	FireEye-HX
Номер (Порт)	4560
Вендор	IT-Bastion
Тип	FireEye
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Подключитесь к устройству FireEye HX с помощью интерфейса командной строки.
2. Активируйте режим конфигурации:

```
# enable
# configure terminal
```

3. Настройте отправку событий на агент сбора лог-коллектора:

```
# logging <IP_address агента сбора лог-коллектора> trap none

# logging <IP_address агента сбора лог-коллектора> trap override class cef priority info
```

4. Сохраните изменения:

```
# write mem
```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **FireEye-HX**.

4.5.3 Kaspersky Security Center. Общая информация

В Kaspersky Security Center существуют следующие типы событий:

- **Общие события** - это события, которые возникают во всех управляемых программах "Лаборатории Касперского". Например, общее событие **Вирусная атака**. Общие события имеют строго определенный синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга;
- **Специфические события управляемых программ "Лаборатории Касперского"**. Каждая управляемая программа "Лаборатории Касперского" имеет собственный набор событий.

В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- **Критическое событие** – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке;
- **Отказ функционирования** – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры;
- **Предупреждение** – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к **Предупреждениям**, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей;
- **Информационное сообщение** – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе программы или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть и изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных "Сервера администрирования" по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных "Сервера администрирования" не менее одного дня.

4.5.4 Kaspersky Security Center. Отправка событий в формате syslog

Только общие события могут быть экспортированы от управляемых программ в форматах CEF и LEEF. Если необходимо экспортировать и общие и специфические события

управляемых программ или пользовательский набор событий, который настроен с помощью политик управляемых программ, используйте экспорт событий в формате syslog.

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Kaspersky-Security-Center-syslog
Номер (Порт)	2605
Вендор	Kaspersky
Тип	KSC
Профиль сбора	«Модуль udp_input»

Настройка источника включает в себя следующие шаги:

1. Настройка автоматического экспорта событий.
2. Настройка событий для отправки в **Платформу Радар**.
3. Включение источника в платформе.

Шаг 1. Настройка автоматического экспорта событий

Чтобы включить автоматический экспорт общих событий выполните следующие действия:

1. Войдите в Kaspersky Security Center и перейдите в раздел **<Наименование Сервера администрирования>**, события которого необходимо экспортировать.
2. В рабочей области выбранного "Сервера администрирования" перейдите на вкладку **События**.
3. Нажмите на кнопку **Настроить параметры уведомлений и экспорта событий** и в выпадающем списке выберите пункт **Настроить экспорт в SIEM-систему**. Откроется окно "Свойства событий".
4. В открывшемся окне перейдите в раздел **Экспорт событий** и укажите следующие параметры экспорта:
   - включите автоматический экспорт событий в базу SIEM-системы, установив соответствующий флаг;
   - в поле **SIEM-система** выберите значение: "*Формат Syslog (RFC 5424)*";
   - в поле **Адрес сервера SIEM-системы** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Протокол** из выпадающего списка выберите протокол взаимодействия: "*UDP*";
   - в поле **Максимальный размер сообщения в байтах** укажите значение: "*2048*".
5. Нажмите на кнопку **OK**.

Если требуется выполнить экспорт в **Платформу Радар** событий, произошедших после определенной даты, нажмите на кнопку **Экспортировать архив** и укажите дату, начиная с которой будет выполнен экспорт событий. По умолчанию экспорт событий начинается сразу после включения.

Шаг 2. Выбор событий для отправки в Платформу Радар

Вы можете настроить экспорт событий в формате syslog в **Платформу Радар** на основе одного из следующих условий:

- **Выбор общих событий**. Если вы выберите экспортируемые события в политике (в свойствах события или в свойствах "Сервера администрирования"), то в **Платформу Радар** будут переданы выбранные события, которые произошли во всех программах, управляемых данной политикой, но вам не удастся их переопределить для отдельной программы, управляемой этой политикой.
- **Выбор событий для управляемой программы**. Если вы выбираете экспортируемые события для управляемой программы, установленной на управляемых устройствах, то в **Платформу Радар** будут переданы только события, которые произошли в этой программе.

Выбор событий для управляемой программы:

1. Войдите в Kaspersky Security Center, перейдите в раздел **Управляемые устройства** и откройте вкладку **Устройства**.
2. Выберите устройство, вызовите контекстное меню и выберите пункт **Свойства**.
3. В открывшемся окне "Свойства устройства" выберите вкладку **Программы**.
4. В списке программ выберите программу, события которой требуется экспортировать и нажмите на кнопку **Свойства**.
5. В открывшемся окне "Свойства программы" выберите раздел **Настройка событий**.
6. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в **Платформу Радар** и нажмите на кнопку **Свойства**.
7. В открывшемся окне "Свойства событий" выполните следующие действия:
    - выберите параметр **Экспортировать в SIEM-систему по протоколу Syslog** для тех событий, которые нужно экспортировать в формате syslog;
    - выключите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отменить выбор событий для экспорта в формате syslog;
    - нажмите на кнопку **OK**.
8. Нажмите на кнопку **OK** в окне свойств программы и в окне свойств устройства.

Выбор общих событий:

1. Войдите в Kaspersky Security Center и перейдите в раздел **Политики**.
2. Выберите политику, откройте контекстное меню и выберите пункт **Свойства**.
3. В открывшемся окне "Свойства политики" выберите раздел **Настройка событий**.

4. В списке событий выберите одно или несколько событий, которые требуется экспортировать в **Платформу Радар**, и нажмите на кнопку **Свойства**.
5. В открывшемся окне "Свойства событий" выполните следующие действия:
   - выберите параметр **Экспортировать в SIEM-систему по протоколу Syslog** для тех событий, которые нужно экспортировать в формате syslog;
   - снимите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отменить выбор событий для экспорта в формате syslog;
   - нажмите на кнопку **OK**.
6. В окне свойств политики нажмите на кнопку **OK**.

Шаг 3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Kaspersky-Security-Center-syslog**.

4.5.5 Kaspersky Security Center. Отправка событий через Microsoft SQL Server

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Kaspersky-SecurityCenter-db
Номер (Порт)	2604
Вендор	Kaspersky
Тип	KSC-db
Профиль сбора	«Модуль odbc_input»

Настройка источника включает в себя следующие шаги:

1. Создание учетной записи Microsoft SQL Server.
2. Предоставление доступа к БД KAV.
3. Предоставление удаленного сетевого доступа.
4. Настройка профиля сбора.
5. Включение источника в платформе.

Шаг 1. Создание учетной записи Microsoft SQL Server

Примечание: создание учетной записи Microsoft SQL Server необходимо выполнять от имени учетной записи, имеющей права локального администратора ОС Windows.

1. Откройте среду разработки **MS SQL Management Studio**.
2. В окне "Connect to Server" подключитесь к экземпляру необходимой базы данных с правами администратора (см. «Рис. 227»).

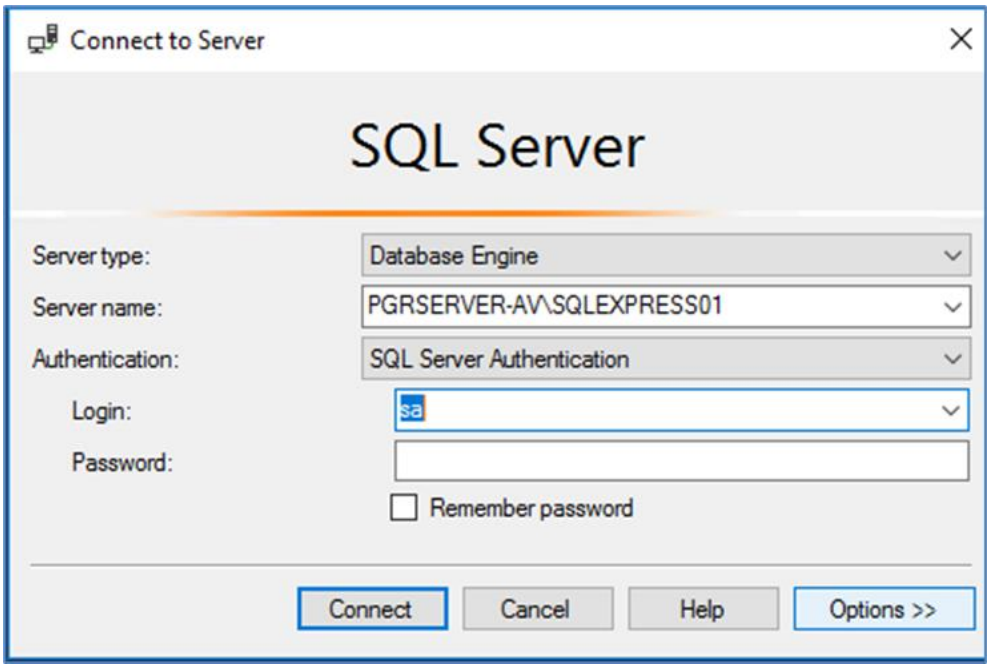


Рис. 227 – Подключение к экземпляру БД

3. Откройте окно "Object Explorer" (см. «Рис. 228»).

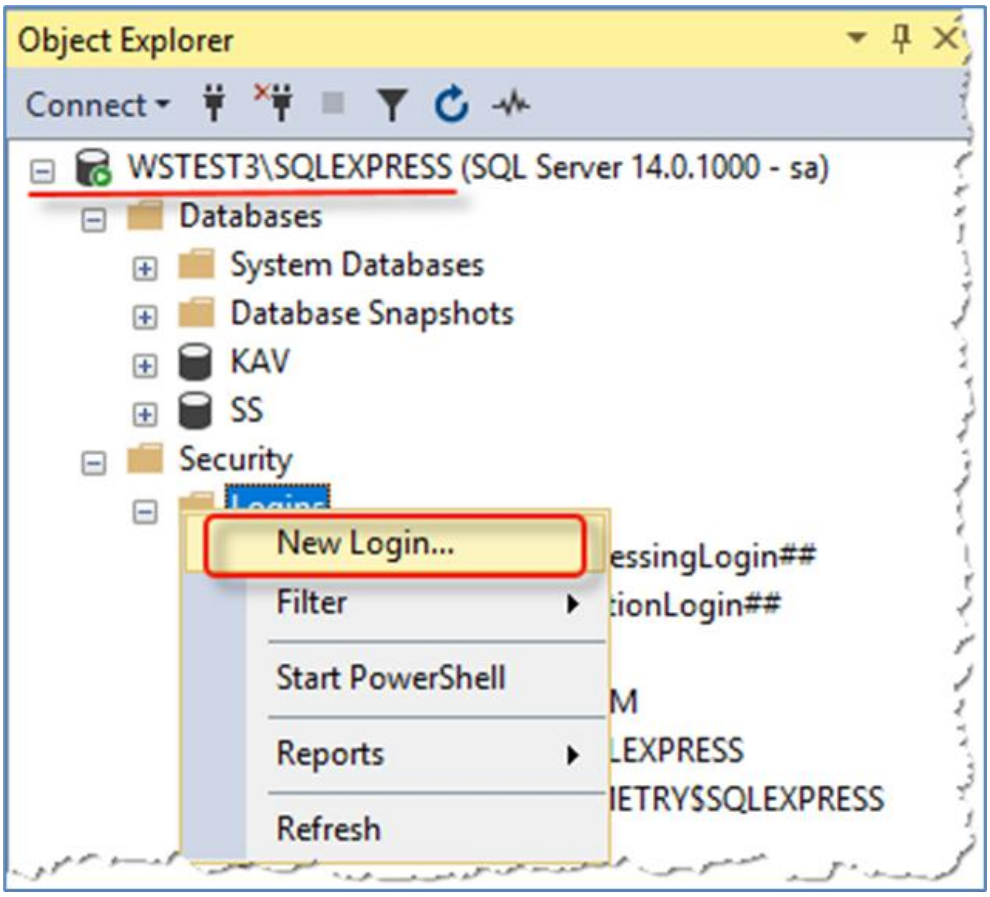


Рис. 228 – Окно "Object Explorer"

4. Выберите раздел **Logins**, вызовите контекстное меню и выберите пункт **New Login...**. Откроется окно "Login--New" (см. «Рис. 229»).

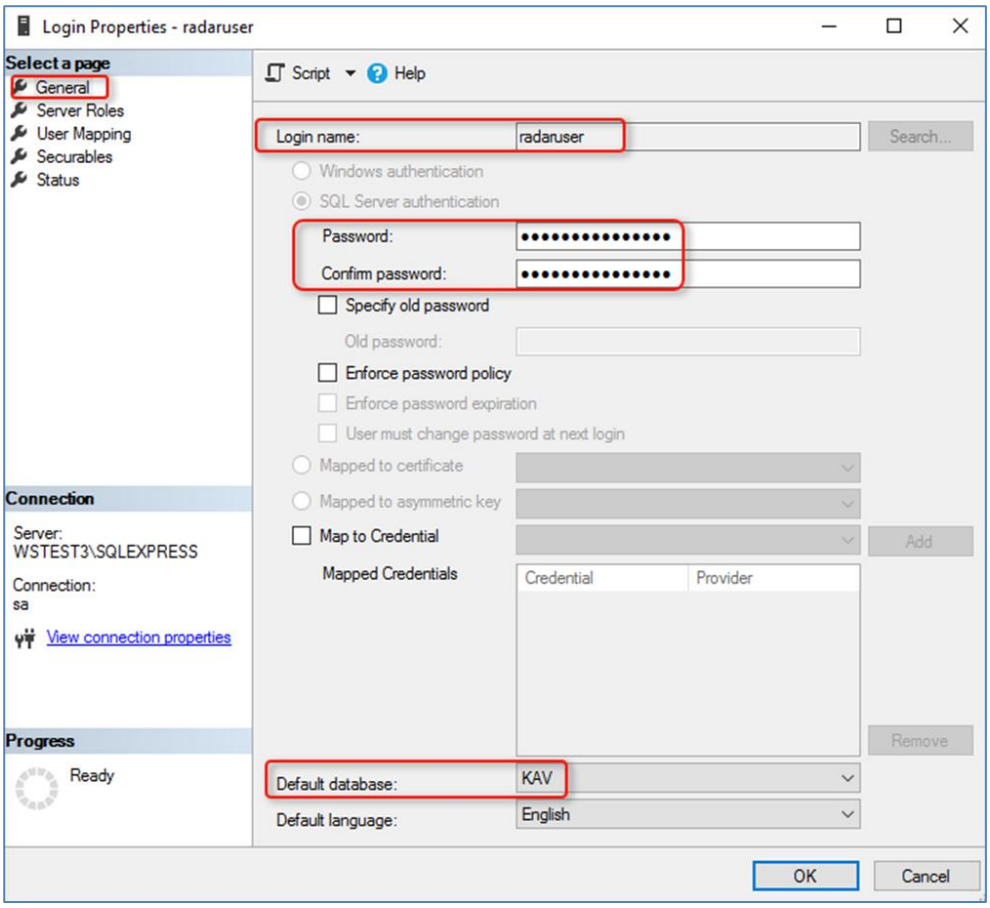


Рис. 229 – Создание нового пользователя экземпляра БД

5. В открывшемся окне перейдите в раздел **General** и выполните следующие настройки:
   - включите режим **SQL Server authentication**;
   - в поле **Login name** укажите имя пользователя "*radaruser*";
   - в полях **Password** и **Confirm password** установите и подтвердите пароль пользователя;
   - при необходимости включите использование политики паролей и задайте срок окончания действия пароля в полях **Enforce password policy** и **Enforce password expiration**;
   - в поле **Default database** выберите значение "*KAV*".
6. Перейдите в раздел **Server Roles** и предоставьте пользователю роль public (см. «Рис. 230»).

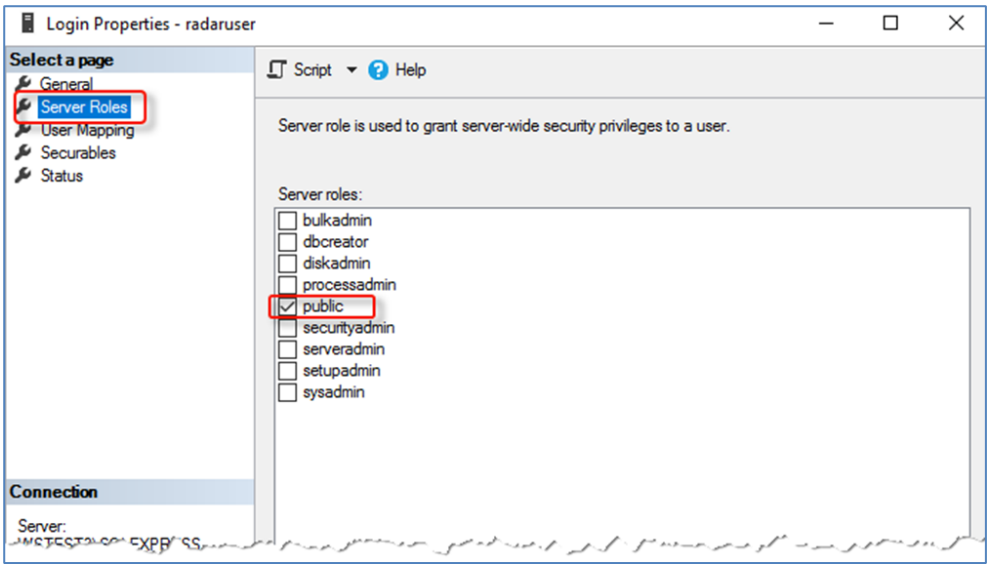


Рис. 230 – Предоставление роли пользователю

7. Перейдите в раздел **User Mapping** (см. «Рис. 231») и выполните следующие настройки:

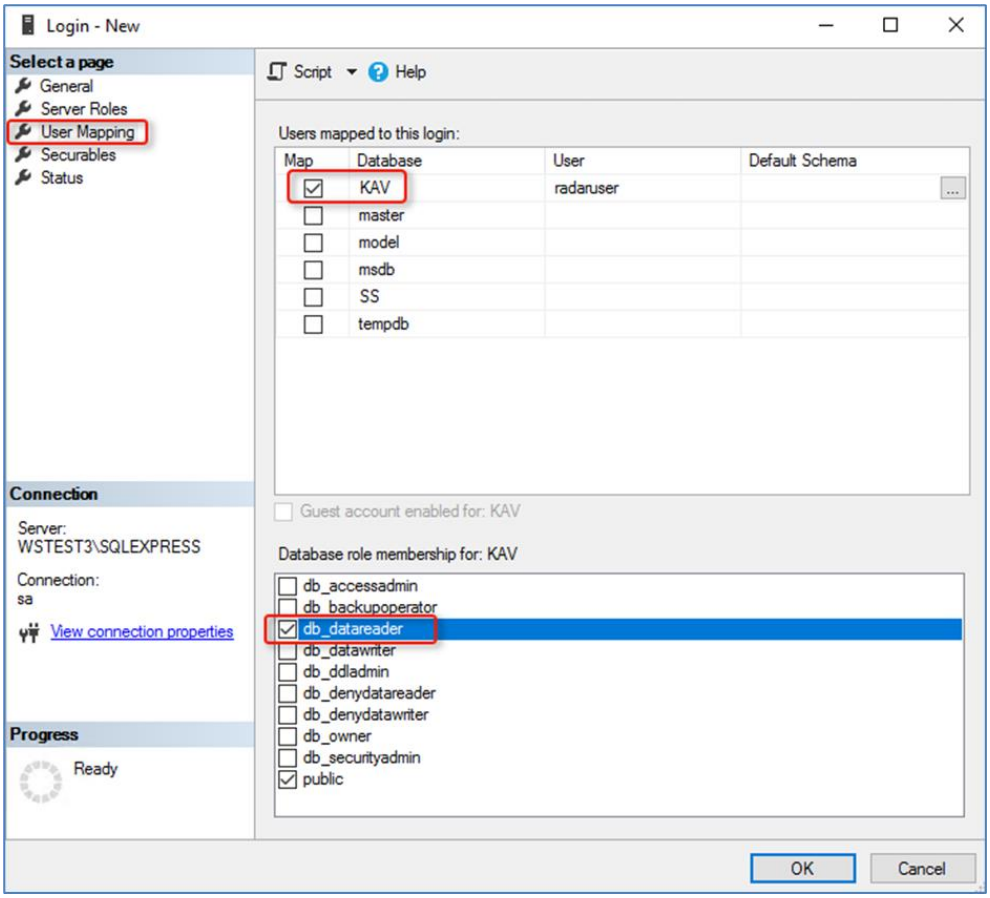


Рис. 231 – Настройка прав доступа к БД KAV

- В блоке **User mapped to this login** предоставьте разрешение на подключение и чтение к БД KAV.
- В блоке **Database role membership for: <имя БД>** установите для выбранной БД роль "*db_datareader*".

8. Перейдите в раздел **Securables** (см. «Рис. 232») и в блоке **Permission for: <имя сервера СУБД>** установите следующее разрешение: "*Connect SQL - Grant*".

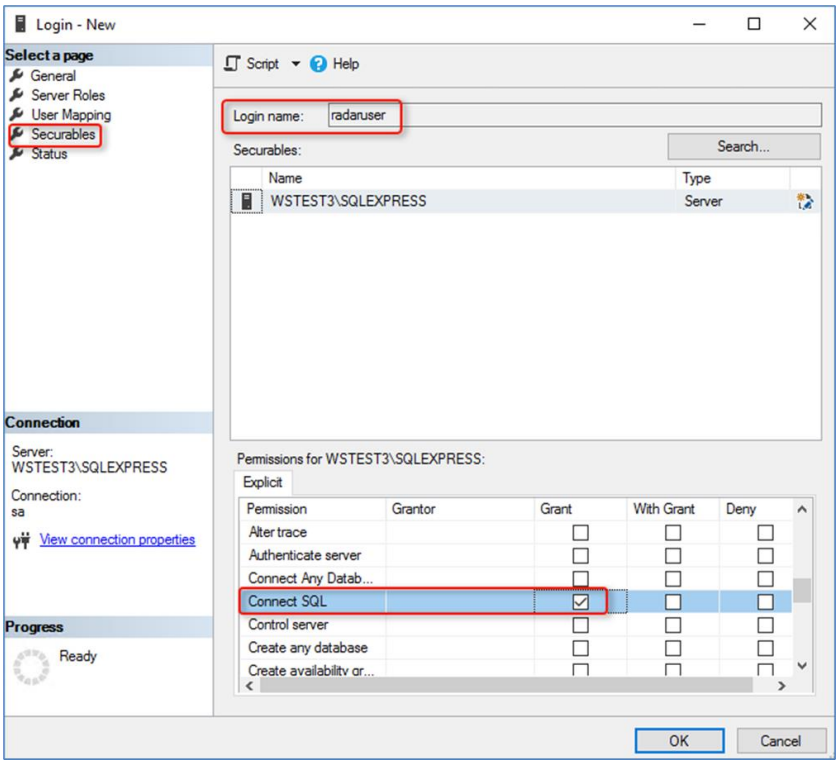


Рис. 232 – Установка разрешения на подключение к БД

9. Нажмите кнопку **OK**.

Шаг 2. Предоставление доступа к БД KAV

Для предоставления доступа к БД KAV выполните следующие действия:

1. Войдите в среду разработки **MS SQL Management Studio**, откройте окно "Object Explorer" и выберите раздел **Databases → KAV → Security → Users** (см. «Рис. 233»):

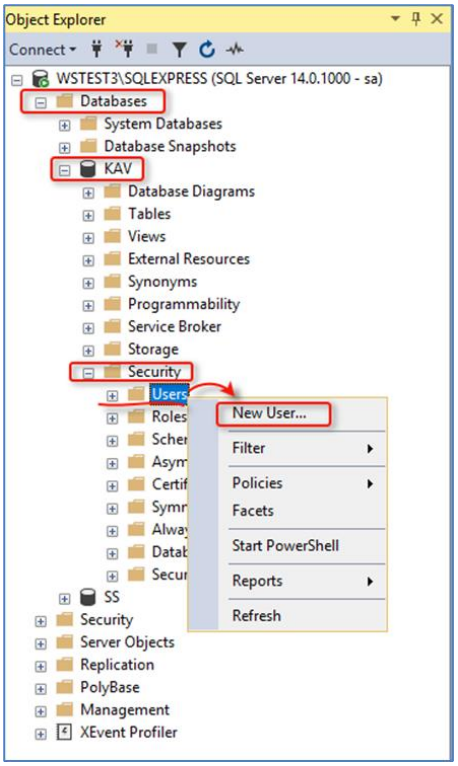


Рис. 233 – Функция создания пользователя в БД KAV

2. Вызовите контекстное меню и выберите пункт **New User...**. Откроется окно создания нового пользователя в БД KAV (см. «Рис. 234»).

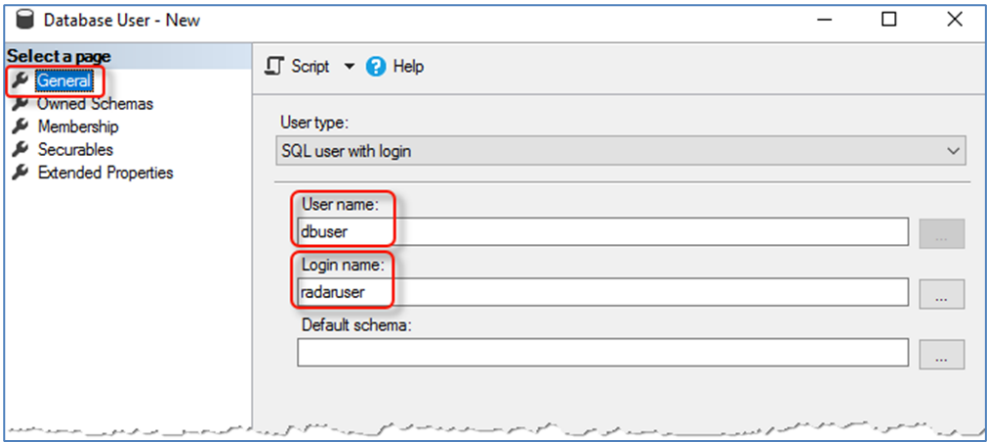


Рис. 234 – Регистрация пользователя в БД KAV

3. В открывшемся окне перейдите в раздел **General** и установите следующие параметры (см. «Рис. 234»):
   - в поле **User name** установите имя пользователя "*dbuser*";
   - в поле **Login name** выберите пользователя "*radaruser*".
4. Перейдите в раздел **Membership** и установите для пользователя роль "*db_datareader*" (см. «Рис. 235»).

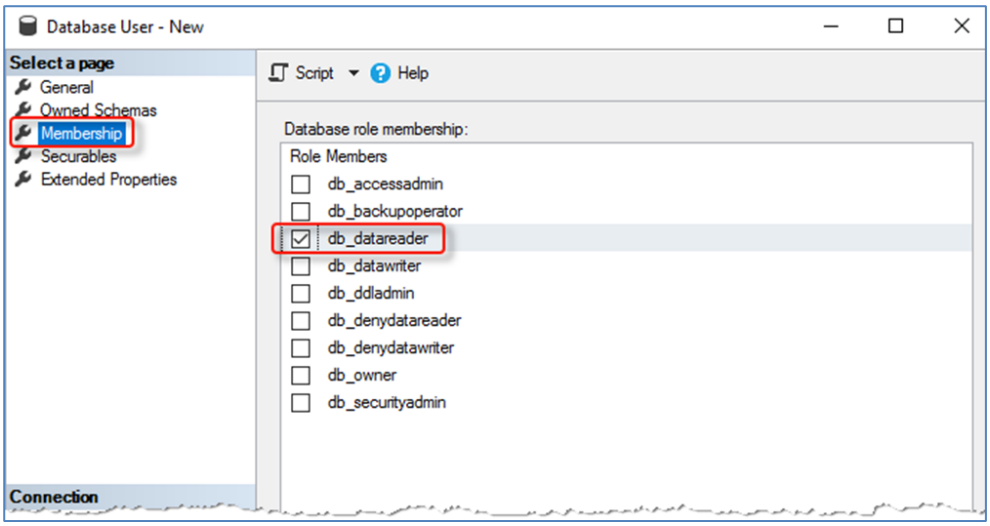


Рис. 235 – Назначение роли

5. Нажмите кнопку **OK**.

Шаг 3. Предоставление удаленного сетевого доступа

1. Откройте диспетчер конфигурации **SQL Server Configuration Manager**.
2. Выберите службу **SQL Server Network Configuration → Protocols for SQLEXPRESS** (см. «Рис. 236»).

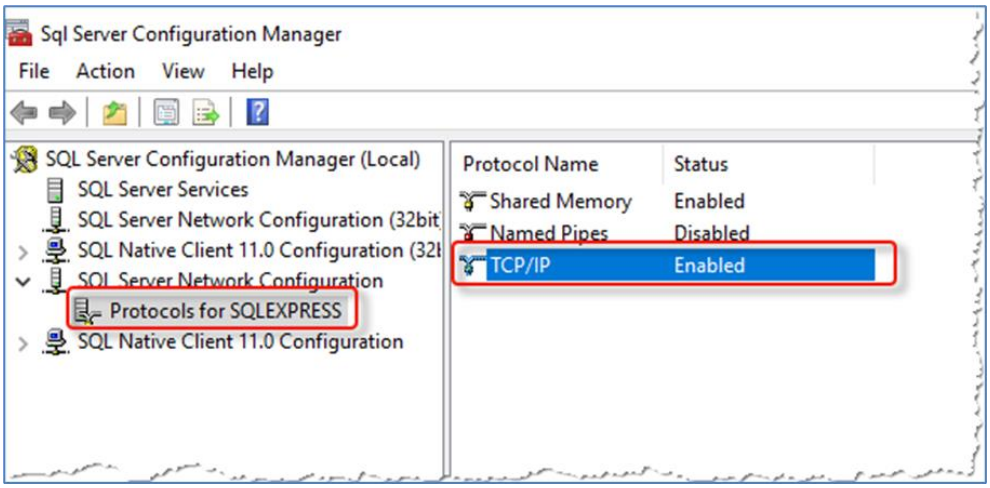


Рис. 236 – Подключение по протоколу TCP/IP

3. В списке протоколов выберите протокол **TCP/IP**, вызовите контекстное меню и установите статус "*Enabled*". Затем из контекстного меню выберите пункт **Properties**. Откроется окно "TCP/IP Properties" (см. «Рис. 237»).

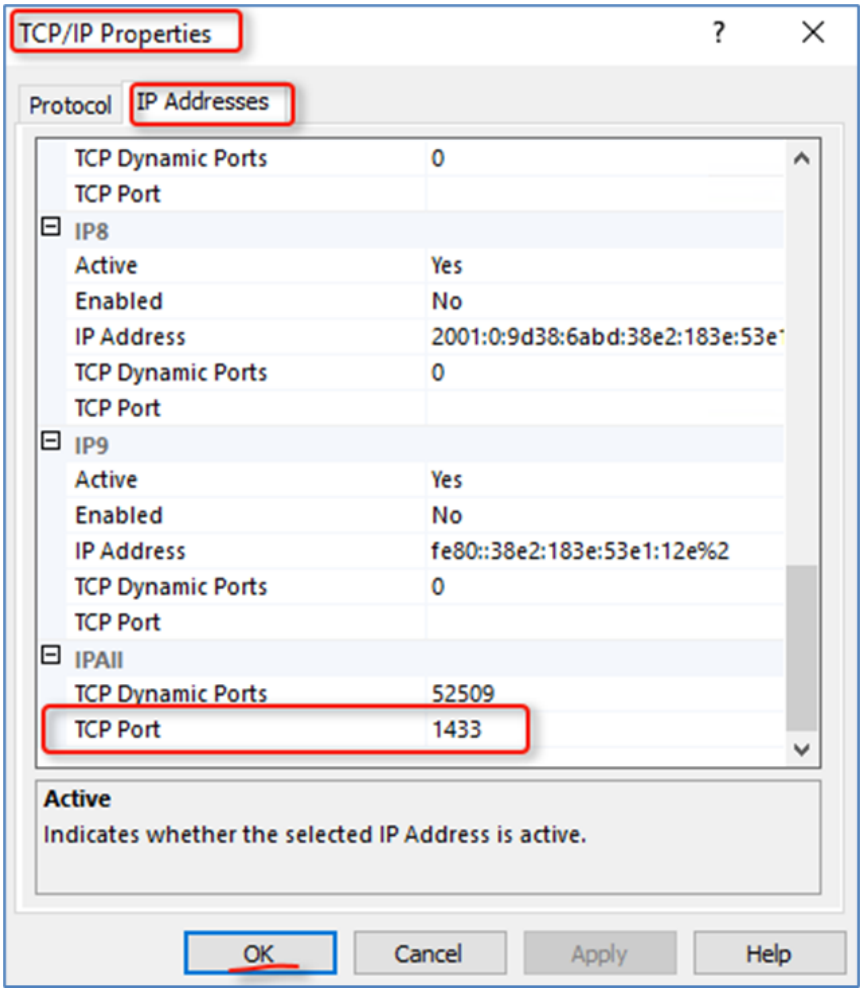


Рис. 237 – Пример настройки протокола для удаленного доступа к БД

4. В открывшемся окне перейдите на вкладку **IP Adresses** и в блоке параметров **IPAll** укажите TCP порт для данного источника: "*1433*".
5. Нажмите кнопку **OK**.

6. Перезапустите службу **MS SQL Server**:
   - запустите управление службами (см. «Рис. 238»);

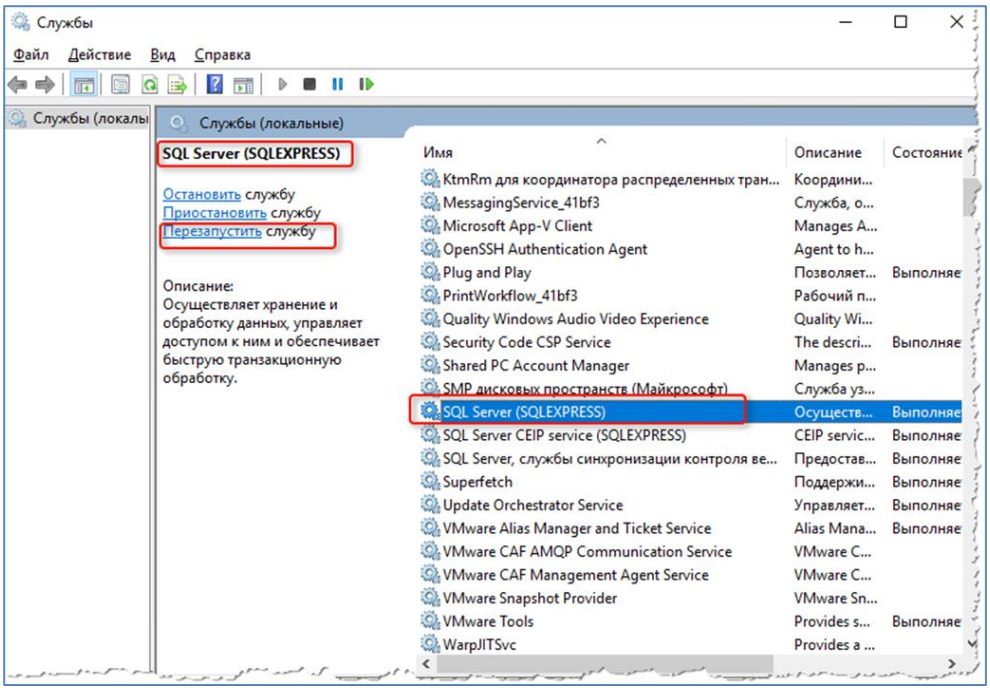


Рис. 238 – Перезапуск службы MS SQL Server

   - выберите службу **SQL Server** с запущенным экземпляром БД (SQLEXPRESS) и нажмите кнопку **Перезапустить службу**.

Шаг 4. Настройте профиль сбора для данного источника

Для настройки профиля сбора выполните следующие действия:

1. Начните процесс настройки профиля сбора для источника **2604 Kaspersky Security Center Database** и выберите модуль «Модуль odbc_input» (см. «Рис. 239»):

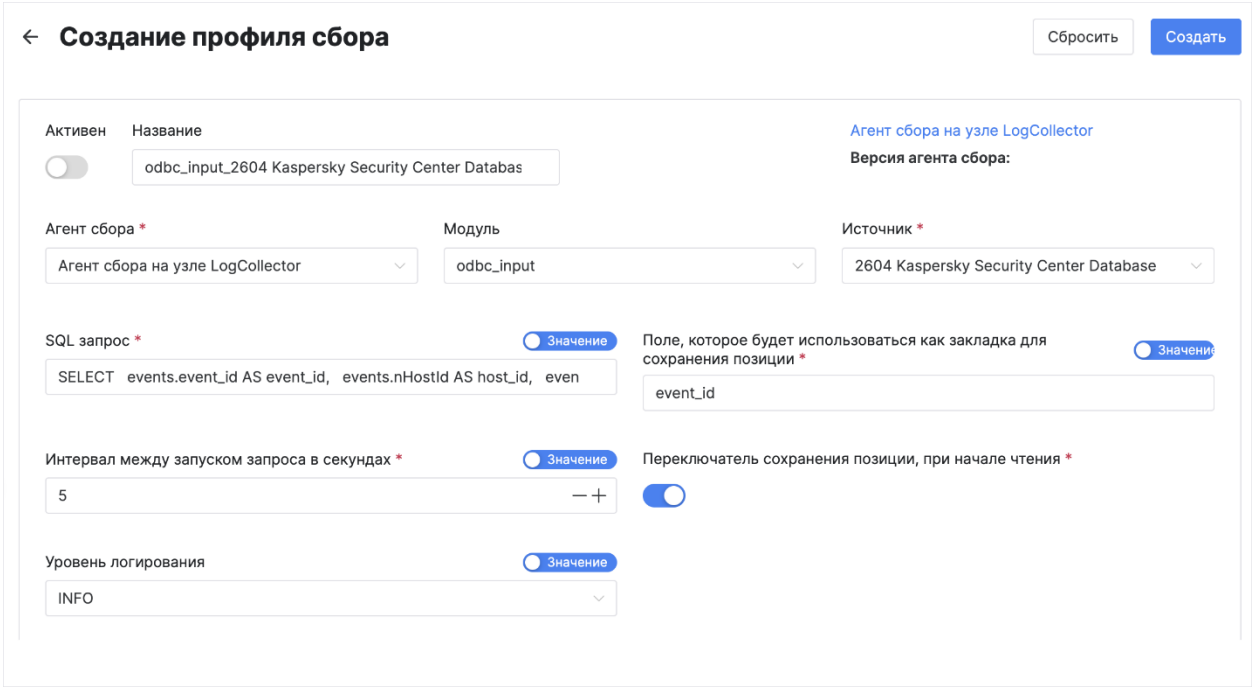


Рис. 239 -- Создание профиля сбора. Модуль "odbc_input"

2. В поле **SQL запрос** укажите запрос, которым будут запрашиваться события из базы данных KSC. Пример запроса:

```
SELECT
  events.event_id AS event_id,
  events.nHostId AS host_id,
  events.severity AS severity,
  events.group_name AS group_name, event_type,
  events.event_type_display_name AS event_name,
  FORMAT(events.rise_time AT TIME ZONE 'UTC', 'yyyy-MM-ddTHH:mm:ss.fffffffzzz')
AS event_time,
  events.descr AS description,
  events.task_display_name AS task_name,
  events.task_id AS task_id,
  events.product_displ_version AS product_version,
  events.par1,
  events.par2,
  events.par3,
  events.par4,
  events.par5,
  events.par6,
  events.par7,
  events.par8,
  events.par9,
  events.product_name,
  hosts_view.strDisplayName AS hostname,
  dnsdomains.strName AS domain,
  fqdns.wstrfqdn AS fqdn,
  CAST(((hosts.nIpAddress / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((hosts.nIpAddress / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((hosts.nIpAddress / 256) & 255) AS varchar(4)) + '.' +
  CAST(((hosts.nIpAddress) & 255) AS varchar(4)) AS ip_address,
  hosts_view.nPlatformType AS platform_id,
  hosts_view.tmLastInfoUpdate AS last_update,
  hosts_view.nVirusCount AS virus_count
FROM KAV.dbo.ev_event AS events
JOIN KAV.dbo.Hosts AS hosts ON hosts.nId = events.nHostId
JOIN KAV.dbo.v_hosts AS hosts_view ON hosts_view.nId = hosts.nId
JOIN KAV.dbo.v_hst_fqdns AS fqdns ON fqdns.nId = hosts.nId
RIGHT JOIN KAV.dbo.DnsDomains AS dnsdomains ON dnsdomains.nId =
hosts.nDnsDomain
WHERE events.event_type IN (
    'FSEE_AKPLUGIN_AVDB_TOTALY_EXPIRED',
    'FSEE_AKPLUGIN_CRITICAL_PATCHES_AVAILABLE',
    'FSEE_AKPLUGIN_LICENSE_ERROR',
    'FSEE_AKPLUGIN_OBJECT_BACKED_UP',
    'FSEE_AKPLUGIN_OBJECT_FOUND',
    'FSEE_AKPLUGIN_OBJECT_NOT_DELETED',
    'FSEE_AKPLUGIN_OBJECT_NOT_ISOLATED',
    'FSEE_AKPLUGIN_OBJECT_NOT_PROCESSED',
    'FSEE_AKPLUGIN_PEP_APPLICATION_AUDIT_DENIED',
    'FSEE_AKPLUGIN_TASK_LICENSE_ERROR',
    'FSEE_AKPLUGIN_UPDATE_ERROR',
    'GNRL_EV_ANTIVIRAL_BASES_EXPIRED',
    'GNRL_EV_APP_LAUNCH_TESTED_DENIED',
    'GNRL_EV_APPLICATION_LAUNCH_DENIED',
    'GNRL_EV_APPLICATION_WAS_RESTARTED',
    'GNRL_EV_ATTACK_DETECTED',
    'GNRL_EV_DEVCTRL_DEV_PLUGGED',
    'GNRL_EV_DEVCTRL_DEV_UNPLUGGED',
    'GNRL_EV_FULLSCAN_STATUS_NOTIFICATION',
    'GNRL_EV_INTERNAL_ERROR',
```

```
'GNRL_EV_LICENSE_EXPIRATION',
'GNRL_EV_OBJECT_BLOCKED',
'GNRL_EV_OBJECT_CURED',
'GNRL_EV_OBJECT_DELETED',
'GNRL_EV_OBJECT_NOTCURED',
'GNRL_EV_OBJECT_QUARANTINED',
'GNRL_EV_OBJECT_REPORTED',
'GNRL_EV_PASSWD_ARCHIVE_FOUND',
'GNRL_EV_PTOTECTION_LEVEL_CHANGED',
'GNRL_EV_SUSPICIOUS_OBJECT_FOUND',
'GNRL_EV_VIRUS_FOUND',
'GNRL_EV_VIRUS_FOUND_AND_BLOCKED',
'GNRL_EV_VIRUS_FOUND_BY_KSN',
'GNRL_EV_VIRUS_OUTBREAK',
'KLAUD_EV_ADMGROUP_CHANGED',
'KLAUD_EV_OBJECTMODIFY',
'KLAUD_EV_SERVERCONNECT',
'KLAUD_EV_SERVERDISCONNECT',
'KLAUD_EV_SIEM_TEST_FAILED',
'KLAUD_EV_TASK_STATE_CHANGED',
'KLEVP_GroupTaskSyncState',
'KLNAG_EV_DEVICE_ARRIVAL',
'KLNAG_EV_DEVICE_REMOVE',
'KLNAG_EV_INV_APP_INSTALLED',
'KLNAG_EV_INV_APP_UNINSTALLED',
'KLNAG_EV_INV_CMPTR_APP_INSTALLED',
'KLPRCI_TaskState',
'KLSRV_DATABASE_UNAVAILABLE',
'KLSRV_DISK_FULL',
'KLSRV_EV_LICENSE_SRV_EXPIRE_SOON',
'KLSRV_EV_LICENSE_SRV_LIMITED_MODE',
'KLSRV_EV_MASTER_SRV_CONNECTED',
'KLSRV_EV_MASTER_SRV_DISCONNECTED',
'KLSRV_EVENT_HOSTS_CONFLICT',
'KLSRV_EVENT_HOSTS_NEW_DETECTED',
'KLSRV_EVENT_HOSTS_NOT_VISIBLE',
'KLSRV_HOST_MOVED_WITH_RULE_EX',
'KLSRV_HOST_STATUS_CRITICAL',
'KLSRV_HOST_STATUS_WARNING',
'KLSRV_INVISIBLE_HOSTS_REMOVED',
'KLSRV_NO_SPACE_ON_VOLUMES',
'KLSRV_RUNTIME_ERROR',
'KLSRV_SEAMLESS_UPDATE_REGISTERED',
'KLSRV_UPD_BASES_UPDATED',
'KSNPROXY_STARTED_CON_CHK_FAILED',
'KSNPROXY_STARTED_CON_CHK_OK',
'KSNPROXY_STOPPED',
'KSWS_OBJECT_DELETED_ONREBOOT',
'ServerCertificateRenewed',
'000000cc',
'000000cf',
'000000d1',
'000000d2',
'000000d3',
'000000d4',
'000000d5',
'000000d6',
'000000d8',
'000000d9',
'000000da',
'000000db',
'000000dc',
'000000dd',
'000000de',
```

```
        '000000df',
        '000000fc',
        '0000012f',
        '00000134',
        '00000136',
        '0000013a',
        '00000141',
        '0000014d',
        '0000014e',
        '0000014f',
        '00000150',
        '00000191',
        '00000192',
        '00000193',
        '000001c4',
        '000001c7',
        '000002c3',
        '000002c4',
        '00000321',
        '000003a3',
        '000003e9',
        '000003fa',
        '0000051e',
        '000007d0',
        '000007d4',
        '000007e4',
        '000007e5',
        '000007e6',
        '000007e7'
    )
    AND event_id > ?;
```

3. В поле **Поле, которое будет использоваться как закладка для сохранения позиции** укажите значение *event_id*, оно используется для сохранения позиции вычитки между запросами.
4. В блоке **Данные для подключения** (см. «Рис. 240») выполните следующие настройки:

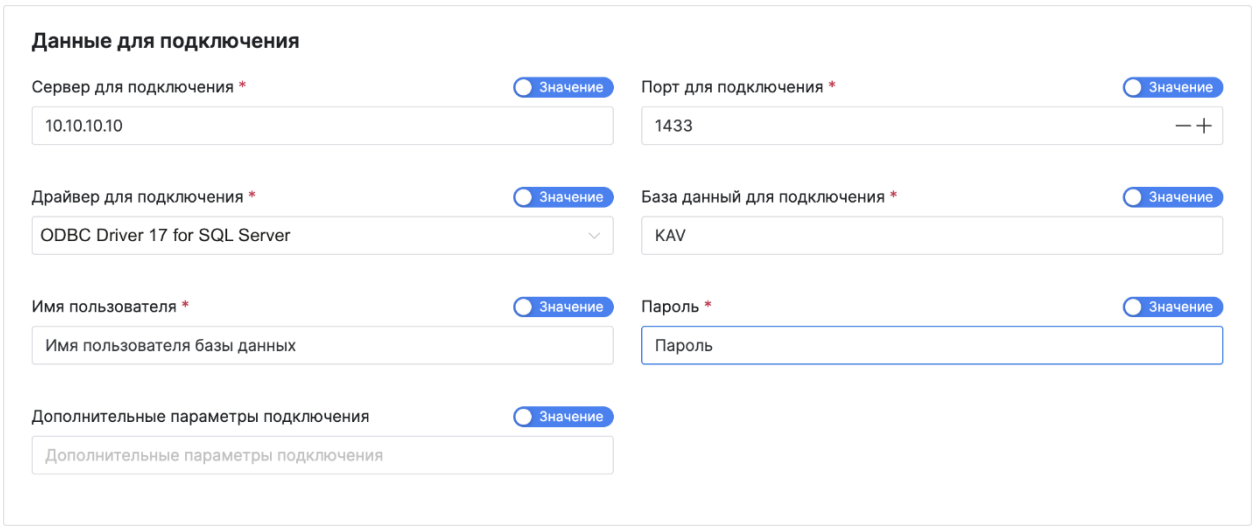


Рис. 240 -- Создание профиля сбора. Модуль "odbc_input". Блок "Данные для подключения"

- в поле **Драйвер для подключения** выберите значение *ODBC Driver 17 for SQL Server*;
- остальные поля заполните соответствующими сетевыми и учетными данными для подключения.

5. Сохраните профиль сбора.

Шаг 5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Kaspersky-SecurityCenter-db**.

4.5.6 Kaspersky Security Center. Отправка событий через MariaDB

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Kaspersky-SecurityCenter-db
Номер (Порт)	2604
Вендор	Kaspersky
Тип	KSC-db
Профиль сбора	«Модуль odbc_input»

Для подключения в качестве источника Kaspersky Security Center, работающего на базе данных MariaDB, выполните следующие действия:

1. Войдите в CMD MariaDB (см. «Рис. 241»).

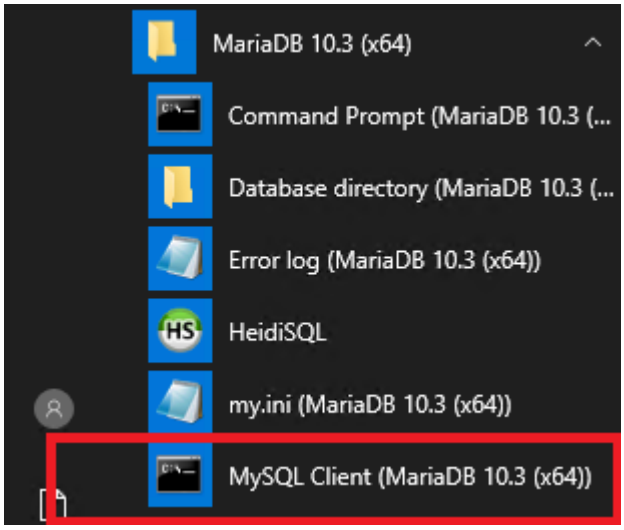


Рис. 241 – CMD MariaDB.

2. Создайте пользователя с правами удаленного подключения:

```
CREATE USER '<имя пользователя>'@'<ip-адрес агента сбора лог-коллектора>'
IDENTIFIED BY '<Пароль Пользователя>';
```

3. Выдайте права на чтение таблиц в базе Kaspersky Security Center:

```
GRANT SELECT ON KAV.ev_event TO '<имя пользователя>'@'<ip-адрес агента сбора
лог-коллектора>' IDENTIFIED BY '<Пароль Пользователя>';
GRANT SELECT ON KAV.dnsdomains TO '<имя пользователя>'@'<ip-адрес агента сбора
лог-коллектора>' IDENTIFIED BY '<Пароль Пользователя>';
GRANT SELECT ON KAV.v_hst_fqdns TO '<имя пользователя>'@'<ip-адрес агента сбора
лог-коллектора>' IDENTIFIED BY '<Пароль Пользователя>';
```

```
GRANT SELECT ON KAV.hosts TO '<имя пользователя>'@'<ip-адрес агента сбора лог-коллектора>' IDENTIFIED BY '<Пароль Пользователя>';
GRANT SELECT ON KAV.v_hosts TO '<имя пользователя>'@'<ip-адрес агента сбора лог-коллектора>' IDENTIFIED BY '<Пароль Пользователя>';
```

4. Запустите веб-интерфейс **Платформы Радар** и выполните следующие действия:
   - перейдите в раздел **Администрирование → Кластер → Узлы** и перейдите к настройкам узла, на котором расположен агент сбора лог-коллектора;
   - в разделе **Секреты Агента** добавьте два секрета:
     - для "Имени пользователя" укажите в соответствующих полях "Название секрета" и "Значение секрета";
     - для "Пароля пользователя" укажите в соответствующих полях "Название секрета" и "Значение секрета".
5. Начните процесс настройки профиля сбора для источника **2604 Kaspersky Security Center Database** и выберите модуль odbc_input (см. «Рис. 242»):

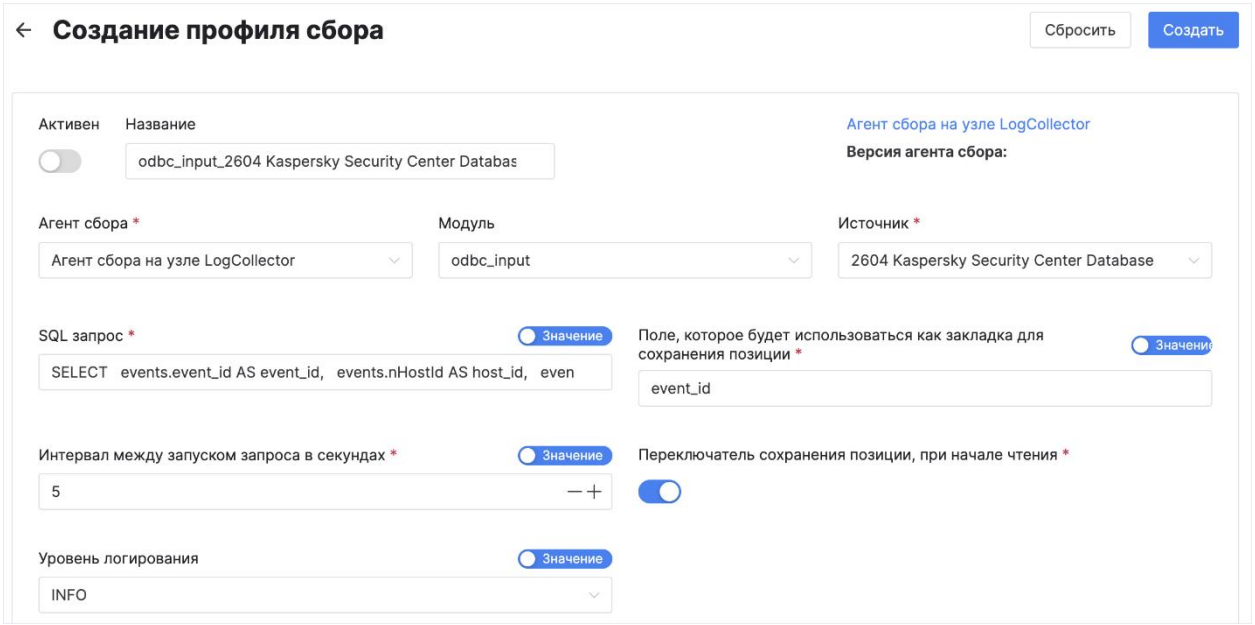


Рис. 242 -- Создание профиля сбора. Модуль "odbc_input"

6. В поле **SQL запрос** укажите запрос, которым будут запрашиваться события из базы данных KSC. Пример запроса:

```
SELECT
  events.event_id AS event_id,
  events.nHostId AS host_id,
  events.severity AS severity,
  events.group_name AS group_name, event_type,
  events.event_type_display_name AS event_name,
  DATE_FORMAT(CONVERT_TZ(events.rise_time, @@session.time_zone, '+00:00'),'%Y-%m-%dT%H:%i:%s.%fZ') AS event_time,
  events.descr AS description,
  events.task_display_name AS task_name,
  events.task_id AS task_id,
  events.product_displ_version AS product_version,
```

```
  events.par1,
  events.par2,
  events.par3,
  events.par4,
  events.par5,
  events.par6,
  events.par7,
  events.par8,
  events.par9,
  events.product_name,
  hosts_view.strDisplayName AS hostname,
  dnsdomains.strName AS domain,
  fqdns.wstrfqdn AS fqdn,
  CONCAT(CAST(((hosts.nIpAddress DIV 16777216) & 255) AS CHAR),
  '.',
  CAST(((hosts.nIpAddress DIV 65536) & 255) AS CHAR),
  '.',
  CAST(((hosts.nIpAddress DIV 256) & 255) AS CHAR),
  '.',
  CAST((hosts.nIpAddress & 255) AS CHAR)
  ) AS ip_address,
  hosts_view.nPlatformType AS platform_id,
  hosts_view.tmLastInfoUpdate AS last_update,
  hosts_view.nVirusCount AS virus_count
FROM `KAV`.`ev_event` AS events
JOIN `KAV`.`Hosts` AS hosts ON hosts.nId = events.nHostId
JOIN `KAV`.`v_hosts` AS hosts_view ON hosts_view.nId = hosts.nId
JOIN `KAV`.`v_hst_fqdns` AS fqdns ON fqdns.nId = hosts.nId
RIGHT JOIN `KAV`.`DnsDomains` AS dnsdomains ON dnsdomains.nId =
hosts.nDnsDomain
WHERE events.event_type IN (
    'FSEE_AKPLUGIN_AVDB_TOTALY_EXPIRED',
    'FSEE_AKPLUGIN_CRITICAL_PATCHES_AVAILABLE',
    'FSEE_AKPLUGIN_LICENSE_ERROR',
    'FSEE_AKPLUGIN_OBJECT_BACKED_UP',
    'FSEE_AKPLUGIN_OBJECT_FOUND',
    'FSEE_AKPLUGIN_OBJECT_NOT_DELETED',
    'FSEE_AKPLUGIN_OBJECT_NOT_ISOLATED',
    'FSEE_AKPLUGIN_OBJECT_NOT_PROCESSED',
    'FSEE_AKPLUGIN_PEP_APPLICATION_AUDIT_DENIED',
    'FSEE_AKPLUGIN_TASK_LICENSE_ERROR',
    'FSEE_AKPLUGIN_UPDATE_ERROR',
    'GNRL_EV_ANTIVIRAL_BASES_EXPIRED',
    'GNRL_EV_APP_LAUNCH_TESTED_DENIED',
    'GNRL_EV_APPLICATION_LAUNCH_DENIED',
    'GNRL_EV_APPLICATION_WAS_RESTARTED',
    'GNRL_EV_ATTACK_DETECTED',
    'GNRL_EV_DEVCTRL_DEV_PLUGGED',
    'GNRL_EV_DEVCTRL_DEV_UNPLUGGED',
    'GNRL_EV_FULLSCAN_STATUS_NOTIFICATION',
    'GNRL_EV_INTERNAL_ERROR',
    'GNRL_EV_LICENSE_EXPIRATION',
    'GNRL_EV_OBJECT_BLOCKED',
    'GNRL_EV_OBJECT_CURED',
    'GNRL_EV_OBJECT_DELETED',
    'GNRL_EV_OBJECT_NOTCURED',
    'GNRL_EV_OBJECT_QUARANTINED',
    'GNRL_EV_OBJECT_REPORTED',
    'GNRL_EV_PASSWD_ARCHIVE_FOUND',
    'GNRL_EV_PTOTECTION_LEVEL_CHANGED',
    'GNRL_EV_SUSPICIOUS_OBJECT_FOUND',
    'GNRL_EV_VIRUS_FOUND',
    'GNRL_EV_VIRUS_FOUND_AND_BLOCKED',
    'GNRL_EV_VIRUS_FOUND_BY_KSN',
```

```
'GNRL_EV_VIRUS_OUTBREAK',
'KLAUD_EV_ADMGROUP_CHANGED',
'KLAUD_EV_OBJECTMODIFY',
'KLAUD_EV_SERVERCONNECT',
'KLAUD_EV_SERVERDISCONNECT',
'KLAUD_EV_SIEM_TEST_FAILED',
'KLAUD_EV_TASK_STATE_CHANGED',
'KLEVP_GroupTaskSyncState',
'KLNAG_EV_DEVICE_ARRIVAL',
'KLNAG_EV_DEVICE_REMOVE',
'KLNAG_EV_INV_APP_INSTALLED',
'KLNAG_EV_INV_APP_UNINSTALLED',
'KLNAG_EV_INV_CMPTR_APP_INSTALLED',
'KLPRCI_TaskState',
'KLSRV_DATABASE_UNAVAILABLE',
'KLSRV_DISK_FULL',
'KLSRV_EV_LICENSE_SRV_EXPIRE_SOON',
'KLSRV_EV_LICENSE_SRV_LIMITED_MODE',
'KLSRV_EV_MASTER_SRV_CONNECTED',
'KLSRV_EV_MASTER_SRV_DISCONNECTED',
'KLSRV_EVENT_HOSTS_CONFLICT',
'KLSRV_EVENT_HOSTS_NEW_DETECTED',
'KLSRV_EVENT_HOSTS_NOT_VISIBLE',
'KLSRV_HOST_MOVED_WITH_RULE_EX',
'KLSRV_HOST_STATUS_CRITICAL',
'KLSRV_HOST_STATUS_WARNING',
'KLSRV_INVISIBLE_HOSTS_REMOVED',
'KLSRV_NO_SPACE_ON_VOLUMES',
'KLSRV_RUNTIME_ERROR',
'KLSRV_SEAMLESS_UPDATE_REGISTERED',
'KLSRV_UPD_BASES_UPDATED',
'KSNPROXY_STARTED_CON_CHK_FAILED',
'KSNPROXY_STARTED_CON_CHK_OK',
'KSNPROXY_STOPPED',
'KSWS_OBJECT_DELETED_ONREBOOT',
'ServerCertificateRenewed',
'000000cc',
'000000cf',
'000000d1',
'000000d2',
'000000d3',
'000000d4',
'000000d5',
'000000d6',
'000000d8',
'000000d9',
'000000da',
'000000db',
'000000dc',
'000000dd',
'000000de',
'000000df',
'000000fc',
'0000012f',
'00000134',
'00000136',
'0000013a',
'00000141',
'0000014d',
'0000014e',
'0000014f',
'00000150',
'00000191',
'00000192',
```

```
        '00000193',
        '000001c4',
        '000001c7',
        '000002c3',
        '000002c4',
        '00000321',
        '000003a3',
        '000003e9',
        '000003fa',
        '0000051e',
        '000007d0',
        '000007d4',
        '000007e4',
        '000007e5',
        '000007e6',
        '000007e7'
    )
    AND event_id > ?;
```

7. В поле **Поле, которое будет использоваться как закладка для сохранения позиции** укажите значение *event_id*, оно используется для сохранения позиции вычитки между запросами.
8. В блоке **Данные для подключения** (см. «Рис. 243») выполните следующие настройки:

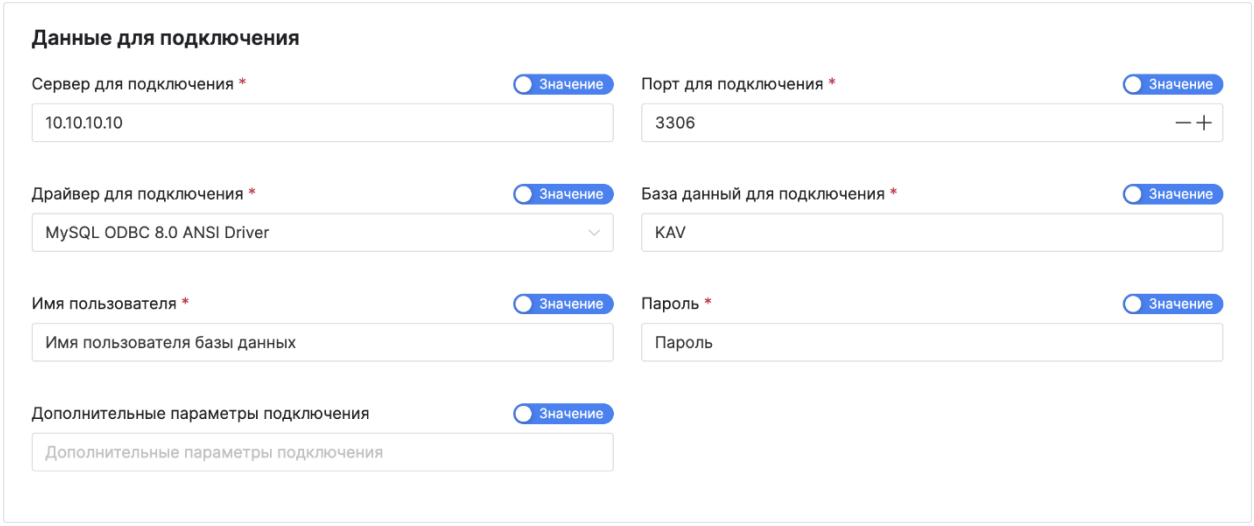


Рис. 243 -- Создание профиля сбора. Модуль "odbc_input". Блок "Данные для подключения"

   - в поле **Драйвер для подключения** выберите значение *MySQL ODBC 8.0 ANSI Driver*;
   - остальные поля заполните соответствующими сетевыми и учетными данными для подключения.
9. Сохраните профиль сбора.
10. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Kaspersky-SecurityCenter-db**. Не забудьте в настройках профиля сбора для данного источника указать соответствующие секреты.

4.5.7 Microsoft Windows AppLocker

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Microsoft-Windows-AppLocker
Номер (Порт)	1528
Вендор	Microsoft
Тип	AppLocker
Профиль сбора	«Модуль eventlog_input_local»

Примечание: *агент сбора лог-коллектора должен быть установлен на том же сервере, где и Microsoft Windows AppLocker*.

Для настройки источника выполните следующие действия:

1. Включите службы **Application Management** и **Application Identity**.
2. Откройте локальные политики безопасности (secpol.msc) и перейдите в раздел **Application Control Policies → AppLocker → Configure rule enforcement** (см. «Рис. 244»).

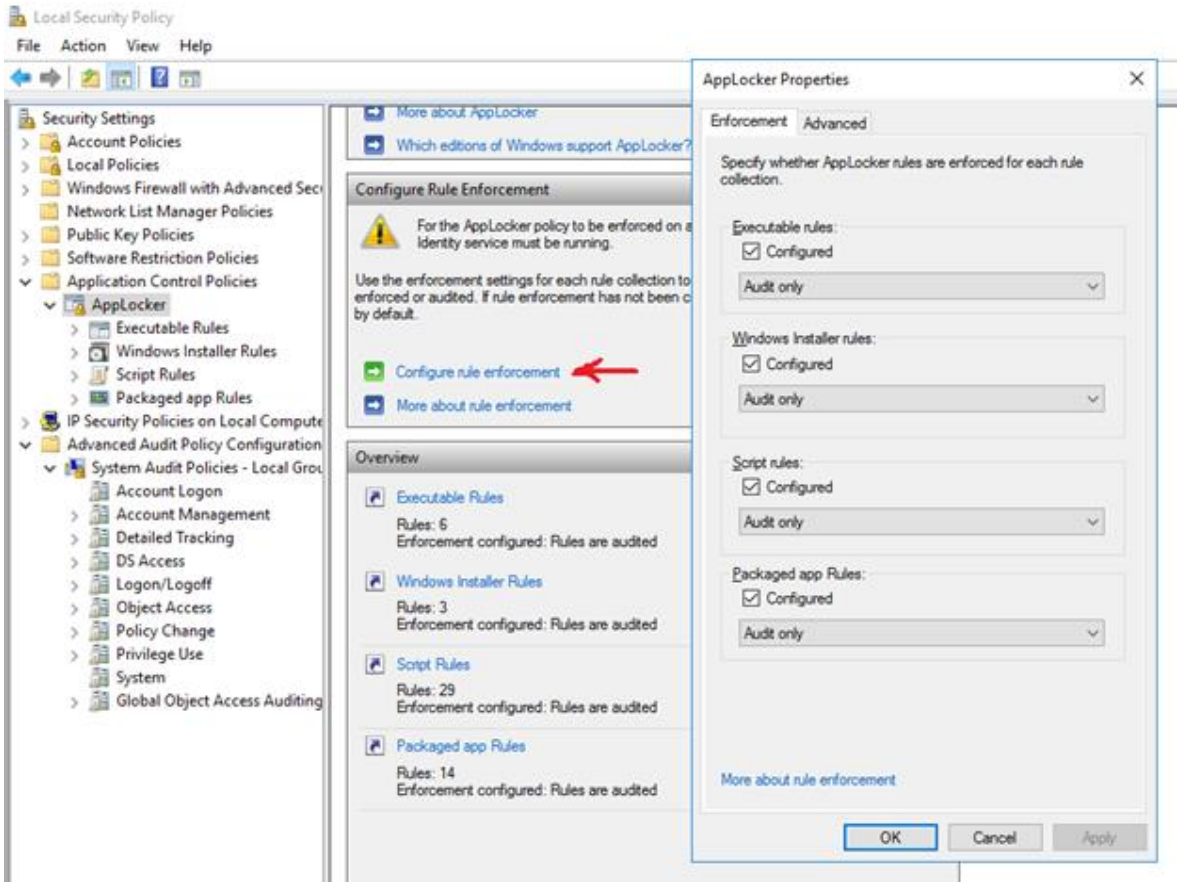


Рис. 244 – Local Security Policy. Configure rule enforcement

3. Откроется окно "AppLocker Properties" (см. «Рис. 245»).

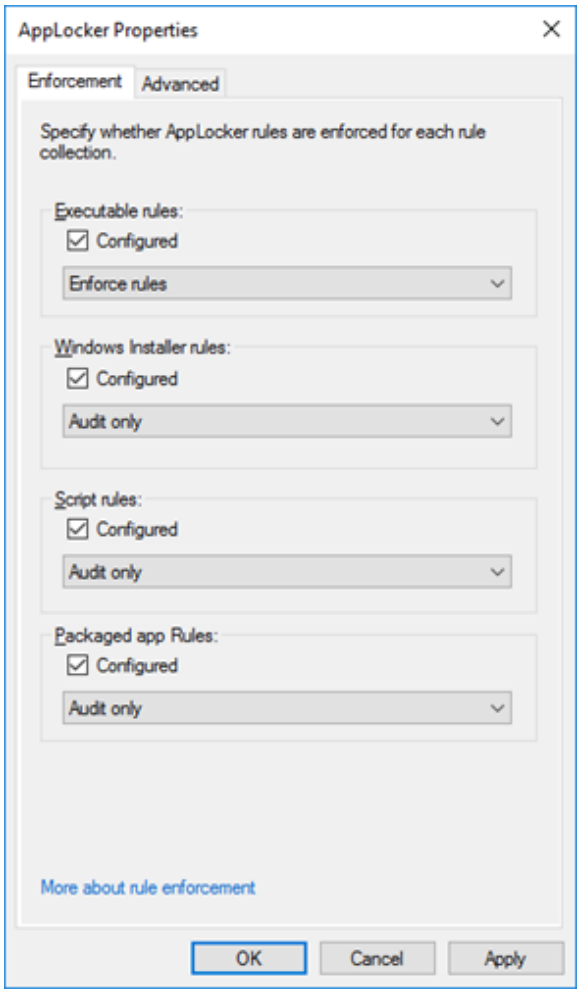


Рис. 245 – Окно "AppLocker Properties"

4. Выполните в окне следующие действия:
   - в поле **Executable rules** установите флаг "Configured" и из выпадающего списка выберите значение "*Enforce rules*";
   - в полях **Windows installer rules**, **Script rules**, **Packaged app Rules** установите флаг "Configured" и из выпадающего списка выберите значение "*Audit only*";
   - нажмите кнопку **OK**. Будут созданны соответствующие наборы правил.
5. Наполните созданные наборы правил **Executable rules**, **Windows installer rules**, **Script rules**, **Packaged app Rules** одним из следующих способом:
   - автоматически;
   - вручную.
6. Способ 1. Автоматически:
   - В разделе **Application Control Policies → AppLocker** выберите необходимый набор правил, вызовите контекстное меню и выберите пункт **Automatically Generate Rules...** (см. «Рис. 246»).

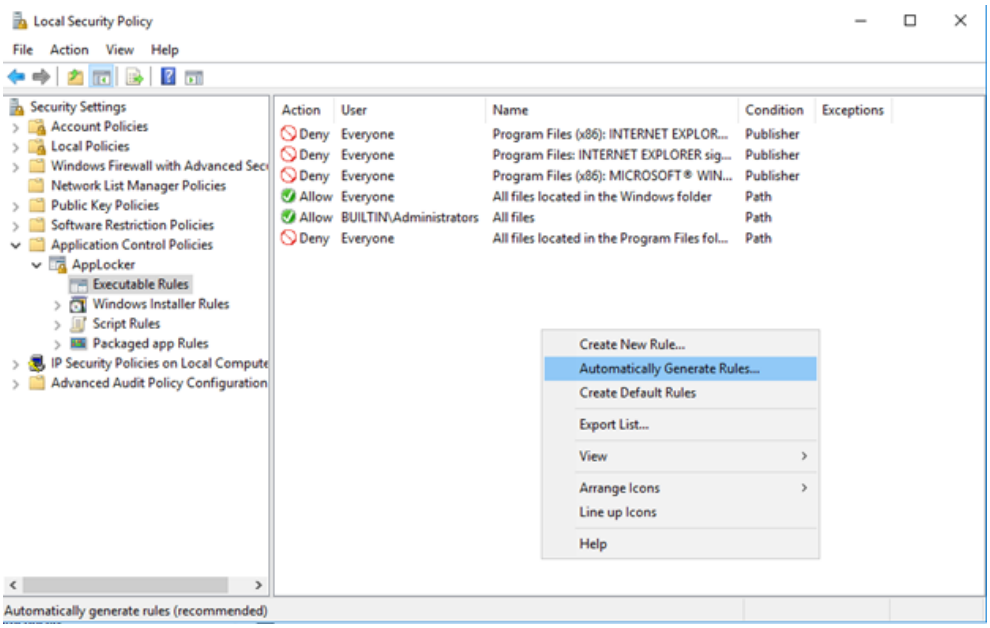


Рис. 246 – Выбор способа генерации правил

- На первом шаге укажите пользователя или группу пользователей, на кого будет применяться правило и путь к файлам для анализа (см. «Рис. 247»).

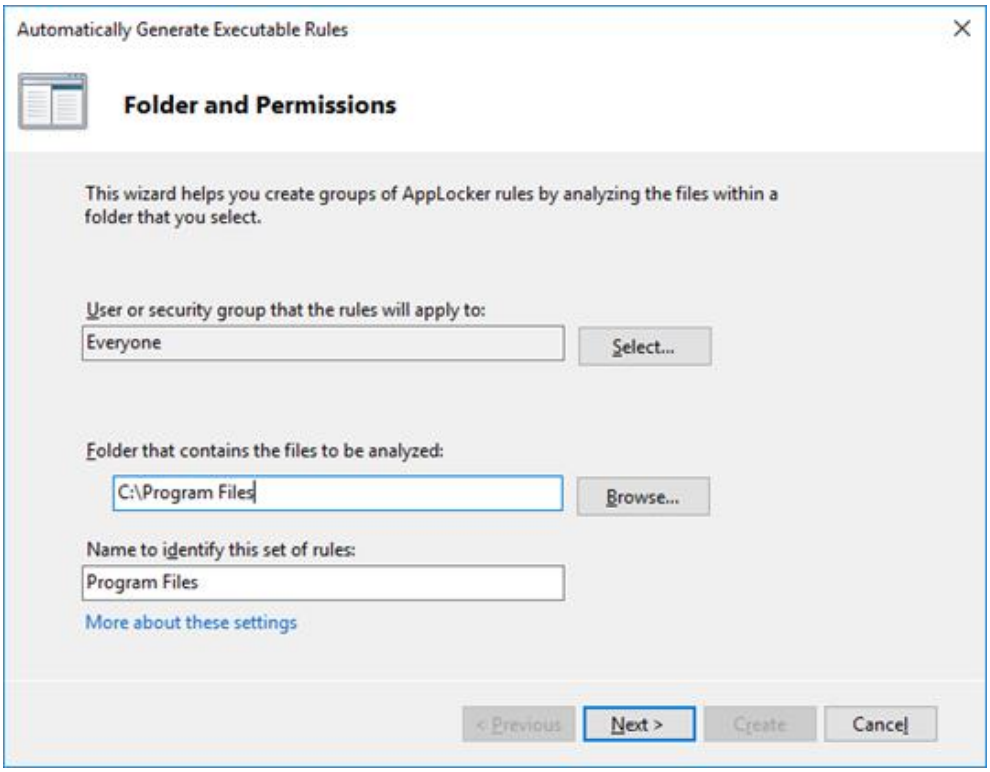


Рис. 247 – Автоматическая генерация правил. Шаг 1

Нажмите кнопку **Next**.

- На втором шаге укажите, как будут анализироваться файлы: по сертификату, по хэшу или по пути (см. «Рис. 248»).

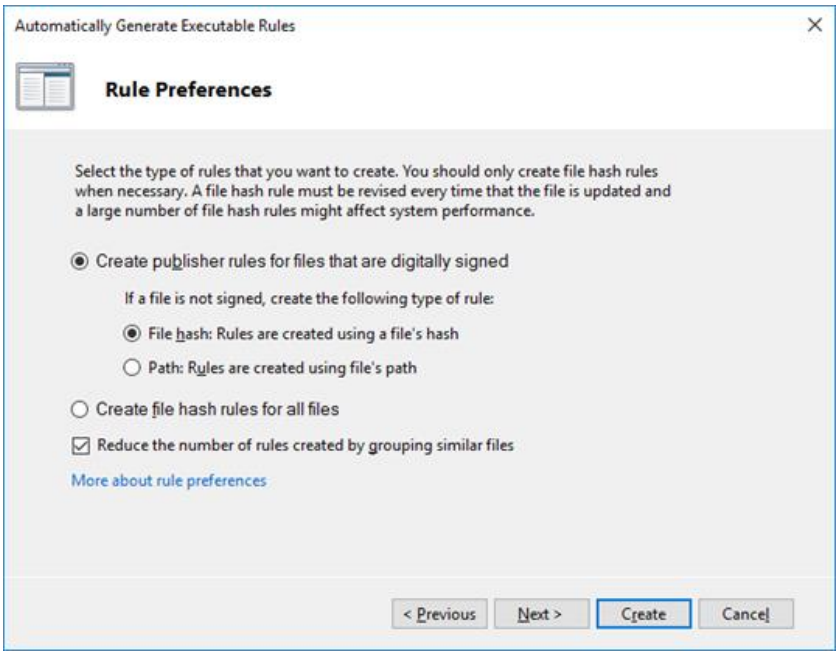


Рис. 248 – Автоматическая генерация правил. Шаг 2

Нажмите кнопку **Next**.

- Проверьте информацию, указанную в правиле, и нажмите кнопку **Create** (см. «Рис. 249»).

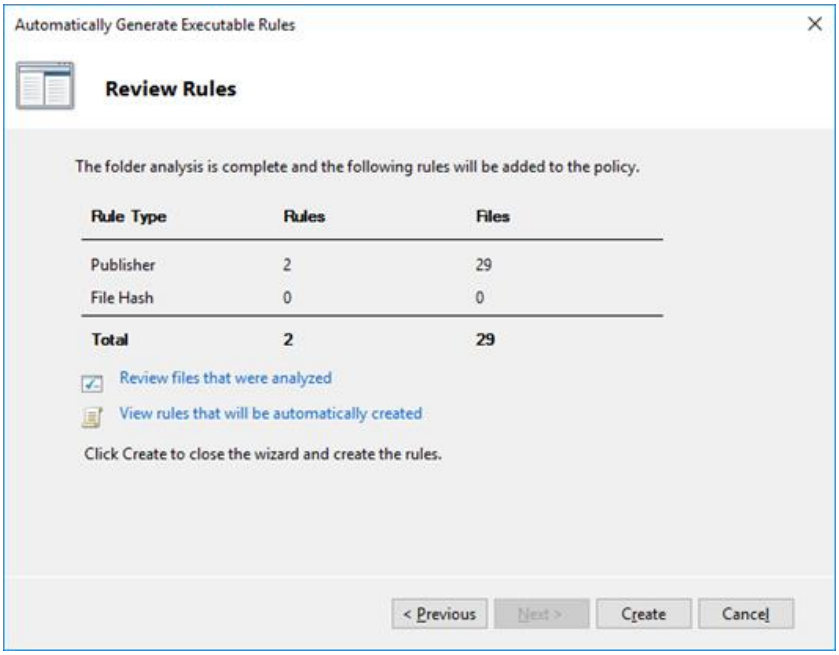


Рис. 249 – Автоматическая генерация правил. Шаг 3

Правило будет создано.

- Повторите действия для каждого набора правил **Executable rules**, **Windows installer rules**, **Script rules**, **Packaged app Rules**.

7. Способ 2. Вручную:

- В разделе **Application Control Policies → AppLocker** выберите необходимый набор правил, вызовите контекстное меню и выберите пункт **New Rule** (см. «Рис. 246»). Отроется окно "Create Rules" (см. «Рис. 250»).

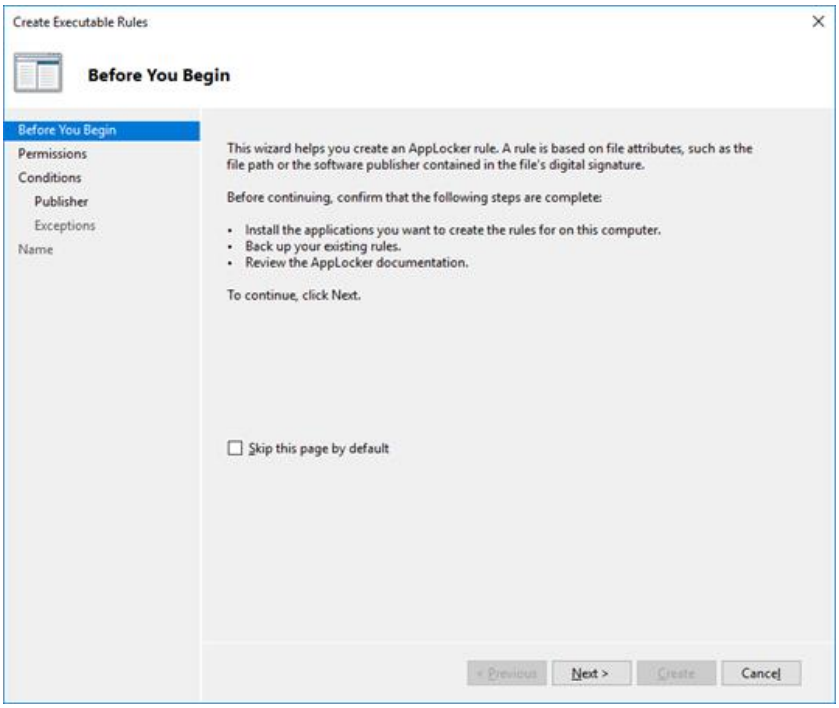


Рис. 250 – Ручная генерация правил. Шаг 1

Ознакомьтесь с информацией в окне и нажмите кнопку **Next**.

- На втором шаге выберите действие (разрешить или запретить запуск) и пользователя (группу пользователей), на кого применится правило (см. «Рис. 251»).

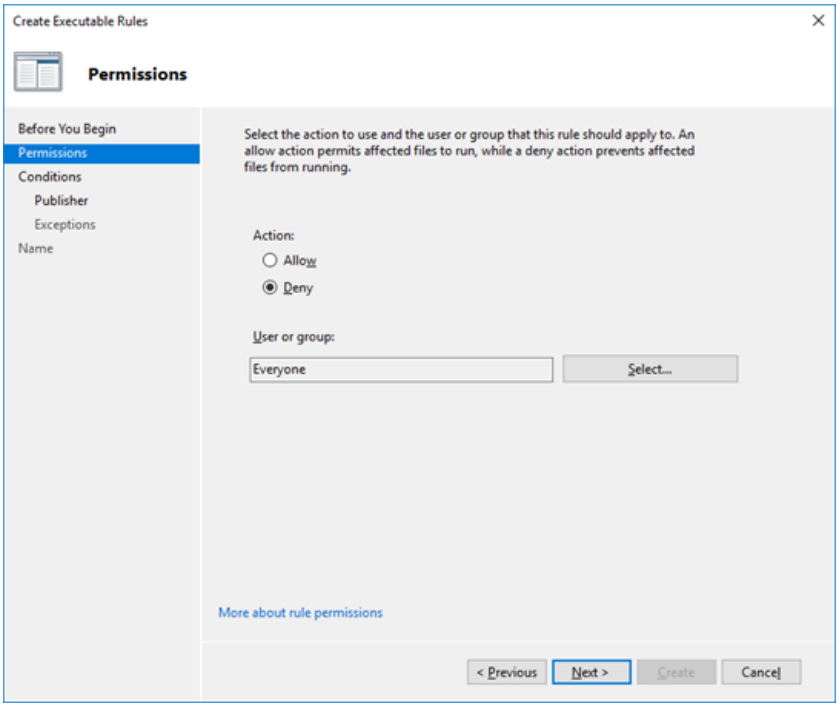


Рис. 251 – Ручная генерация правил. Шаг 2

Нажмите кнопку **Next**.

- На третьем шаге выберите тип проверки файла: по сертификату, либо по пути, либо по хэшу (см. «Рис. 252»).

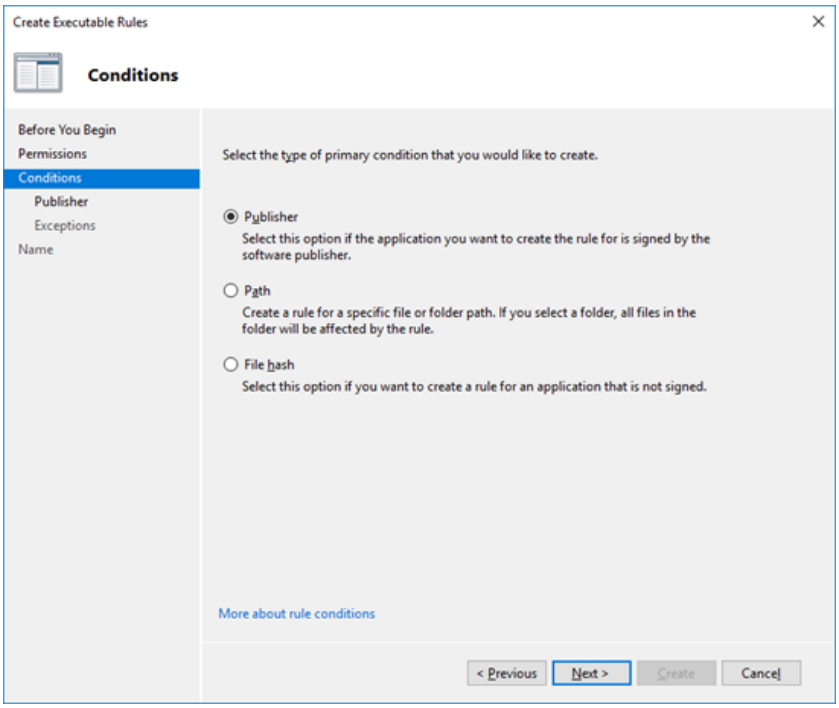


Рис. 252 – Ручная генерация правил. Шаг 3

Нажмите кнопку **Next**.

- На четвертом шаге в зависимости от выбранного типа проверки файлов добавьте соответствующее условие (путь, либо хэш, либо сертификат) (см. «Рис. 253»).

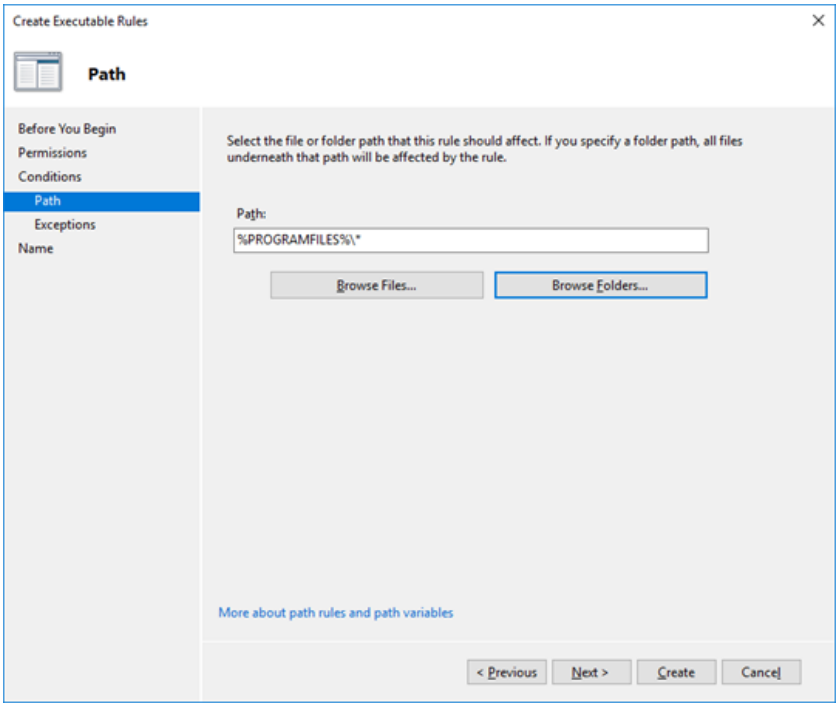


Рис. 253 – Ручная генерация правил. Шаг 4

Нажмите кнопку **Next**.

- На пятом шаге при необходимости добавьте исключения из правила (см. «Рис. 254»).

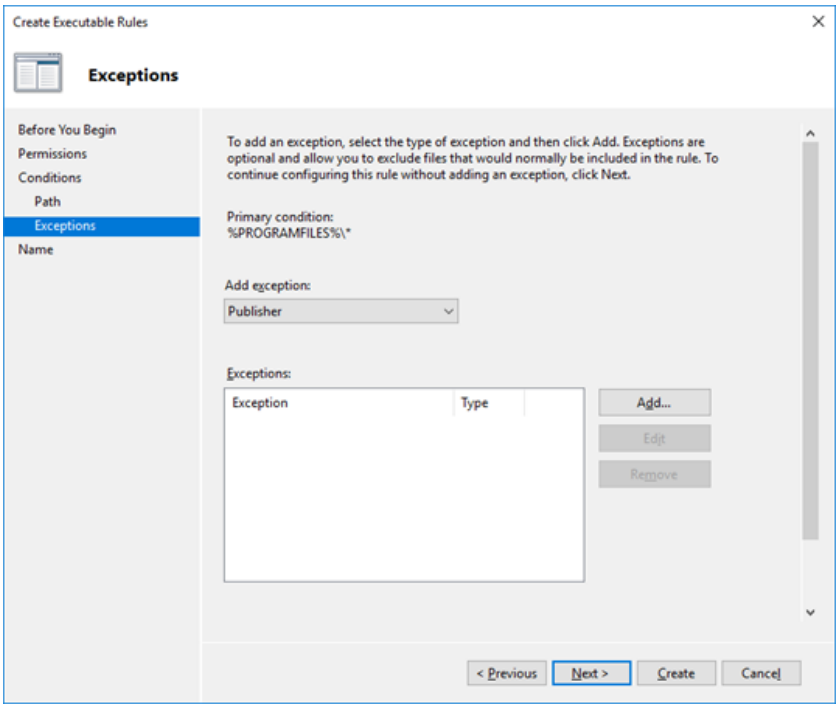


Рис. 254 – Ручная генерация правил. Шаг 5

Нажмите кнопку **Next**.

- На шестом шаге укажите наименование правила и нажмите кнопку **Create** (см. «Рис. 254»).

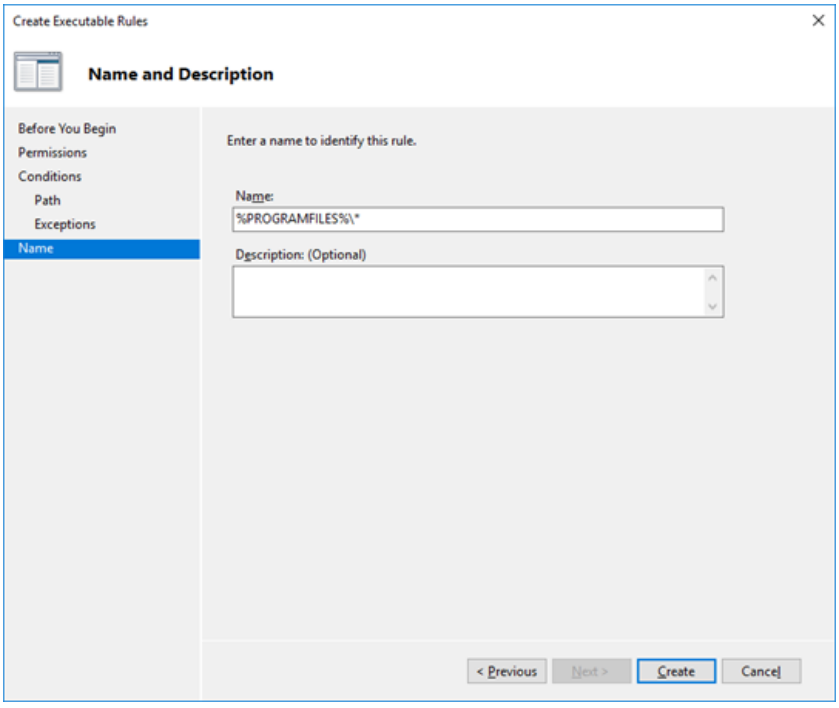


Рис. 255 – Ручная генерация правил. Шаг 6

Правило будет создано.

- Повторите действия для каждого набора правил **Executable rules**, **Windows installer rules**, **Script rules**, **Packaged app Rules**.

8. Примените политику, выполнив следующую команду в консоли:

```
gpupdate /force
```

9. Проверить наличие событий в разделе **AppLocker: EventViewer.msc → Application and Service Log → Microsoft → Windows → AppLocker** (см. «Рис. 256»).

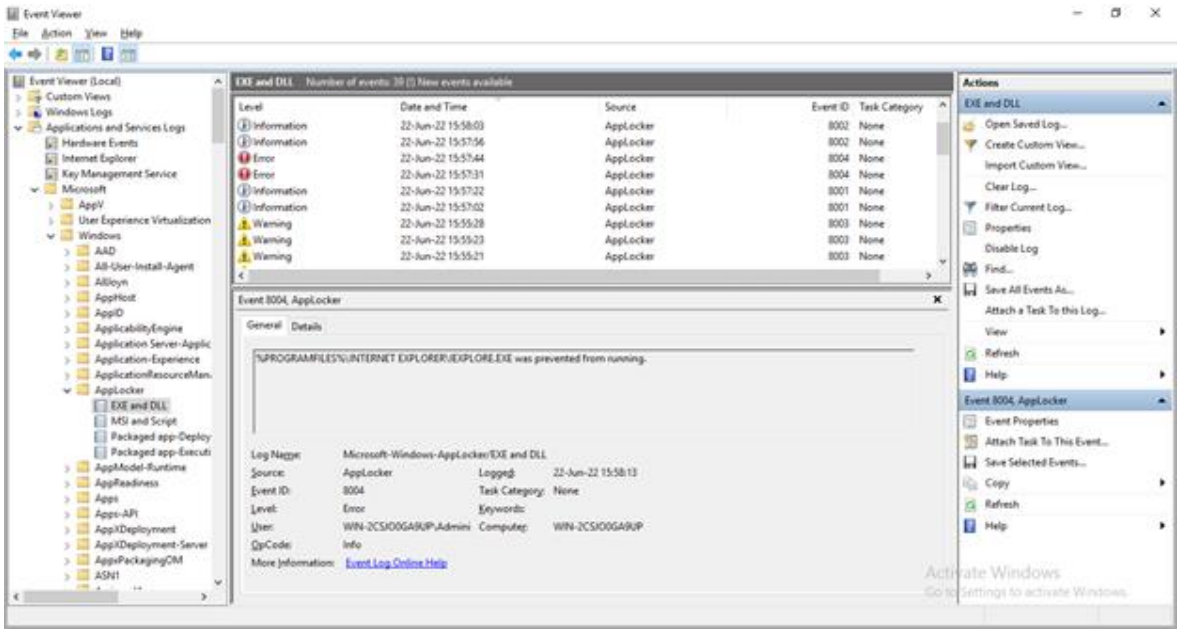


Рис. 256 – Проверка наличия событий

10. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Windows-AppLocker**.

4.5.8 Microsoft Windows Defender

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-Windows-Defender
Номер (Порт)	1511
Вендор	Microsoft
Тип	Defender
Профиль сбора	«Модуль eventlog_input_local»

Примечание: *события от источника включены по умолчанию и записываются в журнал Windows по пути* ***Microsoft-Windows-Windows Defender/Operational****. Агент сбора лог-коллектора должен быть установлен на том же сервере, где и Microsoft Windows Defender*.

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Windows-Defender**.

4.5.9 Microsoft Windows Firewall

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Microsoft-Windows-Firewall
Номер (Порт)	1512
Вендор	Microsoft
Тип	Firewall
Профиль сбора	«Модуль eventlog_input_local»

Примечание: *агент сбора лог-коллектора должен быть установлен на том же сервере, где и Microsoft Windows Firewall.*

Для настройки источника выполните следующие действия:

1. Запустите консоль **Powershell** от имени администратора.
2. Включите журналирование для **Windows Firewall** (для каждого профиля, журналирование включается отдельно):

```
Set-NetFireWallProfile -Profile Domain -LogBlocked True -LogAllowed True -LogMaxSize
4096 -LogFileName "$env:systemroot\system32\LogFiles\Firewall\pfirewall.log"
Set-NetFireWallProfile -Profile Public -LogBlocked True -LogAllowed True -LogMaxSize
4096 -LogFileName "$env:systemroot\system32\LogFiles\Firewall\pfirewall.log"
Set-NetFireWallProfile -Profile Private -LogBlocked True -LogAllowed True -LogMaxSize
4096 -LogFileName "$env:systemroot\system32\LogFiles\Firewall\pfirewall.log"
```

3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Windows-Firewall**.

4.6 Сетевые устройства

При работе по подключению сетевых устройств в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.6.1 Cisco Aironet 4404 Wireless LAN Controller

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Cisco-Aironet
Номер (Порт)	2526
Вендор	Cisco

Характеристика	Значение
Тип	Switch
Профиль сбора	«Модуль udp_input»

Настройку источника можно выполнить следующими способами:

- с помощью консоли устройства;
- с помощью веб-интерфейса.

Способ 1. С помощью консоли устройства:

Внимание! *Все команды по настройке источника выполняются в* ***режиме глобальной конфигурации****. Для этого перейдите в привилегированный режим: введите* enable *и пароль администратора. В консольной строке знак > рядом с именем хоста сменится на #. Затем введите команду #configure terminal. В консольной строке знак # рядом с именем хоста сменится на (config)#.*

1. Включите журналирование событий:

   ```
   (config)# logging on
   ```

2. Установите необходимый уровень facility (по умолчанию local7):

   ```
   (config)# logging <facility>
   ```

3. Укажите IP-адрес агента сбора лог-коллектора:

   ```
   (config)# logging <IP-адрес агента сбора лог-коллектора>
   ```

4. Включите запись временных меток при журналировании событий:

   ```
   (config)# service timestamp log datatime
   ```

5. Сохраните изменения:

   ```
   (config)# copy running-config startup-config
   ```

Способ 2. С помощью веб-интерфейса:

1. Войдите в веб-интерфейс устройства.
2. Перейдите в раздел **Management → Logs → Configs** (см. «Рис. 257»).

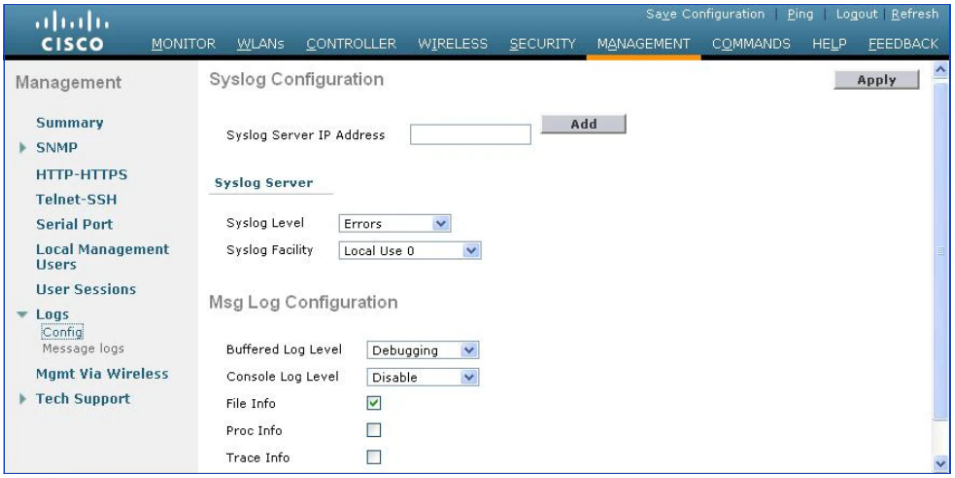


Рис. 257 – Cisco Aironet. Настройка журналирования

3. Укажите в разделе следующую информацию:
    - в поле **Syslog Server IP Addres** укажите IP-адрес агента сбора лог-коллектора и нажмите кнопку **Add**;
    - в поле **Syslog Level** из выпадающего списка выберите уровень журналирования;
    - в поле **Facility** и выпадающего списка выберите необходимый уровень facility.
    - нажмите кнопку **Apply**.
4. Нажмите кнопку **Save Configuration**.

Далее перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Cisco-Aironet**.

4.6.2 Cisco IOS. Netflow

Платформа Радар поддерживает работу с устройствами Cisco, работающими по следующим версиям протокола Netflow:

- v5;
- v9.

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Cisco-NetFlow
Номер (Порт)	2162
Вендор	Cisco
Тип	NetFlow
Профиль сбора	«Модуль nf_input»

Внимание! *Все команды по настройке источника выполняются в **режиме глобальной конфигурации**. Для этого перейдите в привилегированный режим: введите enable и пароль администратора. В консольной строке знак > рядом с именем хоста сменится на #. Затем введите команду #configure terminal. В консольной строке знак # рядом с именем хоста сменится на (config)#.*

Для настройки источника выполните следующие действия:

1. Подключитесь к консоли устройства и перейдите в режим глобальной конфигурации.
2. Включите экспорт статистики сетевого трафика:

```
(config)# ip-flow-export destination <IP-адрес агента сбора лог-коллектора>
<порт, указанный в профиле сбора>
(config)# ip flow-export version <версия протокола> (допустимые значения: 5 или
9)
```

```
(config)# interface <интерфейс, с которого необходимо собирать статистику>
(config)# ip flow ingress
(config)# ip flow egress
```

3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Cisco-NetFlow**.

4.6.3 Cisco IOS Router. System logging

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Cisco-IOSRouter
Номер (Порт)	2524
Вендор	Cisco
Тип	IOSRouter
Профиль сбора	«Модуль tcp_input»

Внимание! *Все команды по настройке источника выполняются в **режиме глобальной конфигурации**. Для этого перейдите в привилегированный режим: введите enable и пароль администратора. В консольной строке знак > рядом с именем хоста сменится на #. Затем введите команду #configure terminal. В консольной строке знак # рядом с именем хоста сменится на (config)#.*

Для настройки источника выполните следующие действия:

1. Подключитесь к консоли устройства и перейдите в режим глобальной конфигурации.
2. Включите логирование попыток подключения к устройству:

```
(config)# service timestamps log datetime localtime show-timezone year
(config)# logging userinfo
(config)# login on-failure log
(config)# login on-success log
```

3. Включите логирование изменений конфигурации устройства:

```
(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# logging enable
(config-archive-log-cfg)# notify syslog
(config-archive-log-cfg)# hidekeys
```

4. Настройте отправку событий на агент сбора лог-коллектора, указав его IP-адрес, порт, указанный в настройках соответствующего профиля сбора и значение facility (по умолчанию local5):

```
(config)# logging facility local5
(config)# logging host <IP-адрес агента сбора лог-коллектора> transport tcp
port <порт, указанный в профиле сбора>
```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Cisco-IOSRouter**.

4.6.4 Cisco IOS Switch. System logging

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Cisco-IOS-Switch
Номер (Порт)	2523
Вендор	Cisco
Тип	IOS-Switch
Профиль сбора	«Модуль tcp_input»

Внимание! *Все команды по настройке источника выполняются в **режиме глобальной конфигурации**. Для этого перейдите в привилегированный режим: введите enable и пароль администратора. В консольной строке знак > рядом с именем хоста сменится на #. Затем введите команду #configure terminal. В консольной строке знак # рядом с именем хоста сменится на (config)#.*

Для настройки источника выполните следующие действия:

1. Подключитесь к консоли устройства и перейдите в режим глобальной конфигурации.
2. Включите логирование попыток подключения к устройству:

```
(config)# service timestamps log datetime localtime show-timezone year
(config)# logging userinfo
(config)# login on-failure log
(config)# login on-success log
```

3. Включите логирование изменений конфигурации устройства:

```
(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# logging enable
(config-archive-log-cfg)# notify syslog
(config-archive-log-cfg)# hidekeys
```

4. Настройте отправку событий на агент сбора лог-коллектора, указав его IP-адрес, порт, указанный в настройках соответствующего профиля сбора и значение facility (по умолчанию "*local5*"):

```
(config)# logging facility local5
(config)# logging host <IP-адрес агента сбора лог-коллектора> transport tcp
port <порт, указанный в профиле сбора>
```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Cisco-IOS-Switch**.

4.6.5 Cisco Nexus Switch

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Cisco-Nexus-Switch
Номер (Порт)	2525
Вендор	Cisco
Тип	Nexus-Switch
Профиль сбора	«Модуль udp_input»

Примечание: *по умолчанию источник Cisco Nexus Switch не имеет возможности изменить порт и протокол отправки событий, поэтому сбор событий агентом сбора лог-коллектора происходит по 514/UDP*.

Внимание! *Все команды по настройке источника выполняются в **режиме глобальной конфигурации**. Для этого перейдите в привилегированный режим: введите enable и пароль администратора. В консольной строке знак > рядом с именем хоста сменится на #. Затем введите команду #configure terminal. В консольной строке знак # рядом с именем хоста сменится на (config)#.*

Для настройки источника выполните следующие действия:

1. Подключитесь к консоли устройства и перейдите в режим глобальной конфигурации.
2. Включите логирование и настройте отправку событий на агент сбора лог-коллектора:

```
switch(config)# logging message interface type ethernet description
switch(config)# logging event link-status enable
switch(config)# logging event trunk-status enable
switch(config)# logging level all 6
switch(config)# logging origin-id hostname
switch(config)# logging server <IP-адрес агента сбора лог-коллектора> 6
facility local5
```

3. Вернитесь в привилегированный режим и сохраните изменения:

```
switch# copy run star
```

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Cisco-Nexus-Switch**.

4.6.6 Cisco SG200 Switch

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Cisco-Nexus-Switch
Номер (Порт)	2525
Вендор	Cisco
Тип	Nexus-Switch
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс устройства.
2. Перейдите в **Administration → System Log → Remote Log Servers** (см. «Рис. 258»).

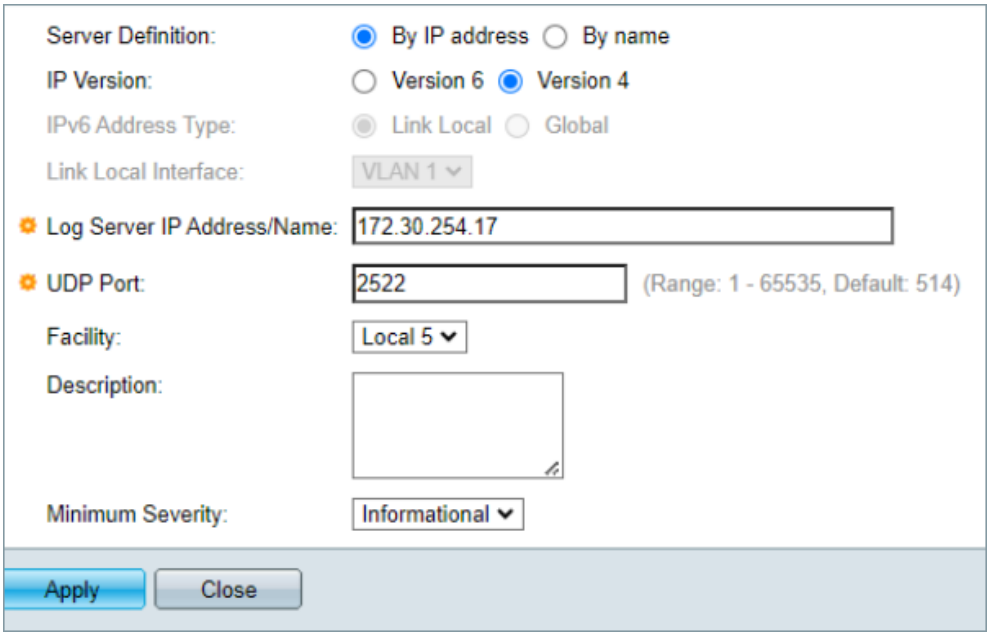


Рис. 258 – Cisco SG200 Switch. Настройка отправки событий

3. Укажите в разделе следующую информацию:
   - в поле **Log Server IP Address/Name** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **UDP Port** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;

- в поле **Facility** и выпадающего списка выберите необходимый уровень facility: "*Local 5*".

4. Перейдите в раздел **Administration → System Log → Log Settings** и задайте параметры в соответствии с «Рис. 259»:

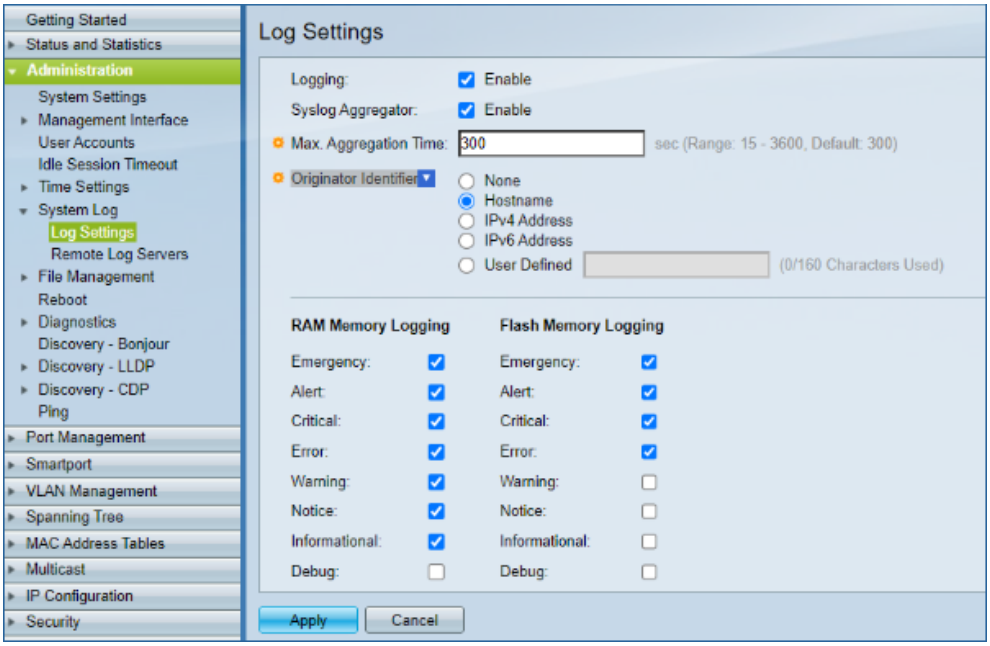


Рис. 259 – Cisco SG200 Switch. Настройка журналирования

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Cisco-SG200-Switch**.

4.6.7 D-link xStack

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Dlink-xstack
Номер (Порт)	2773
Вендор	D-link
Тип	Switch
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс устройства.
2. Перейдите в раздел **Administration → System Log → System Log Host**.
3. Откройте **System Log Server** или **System Log Server-Add** (см. «Рис. 260»).

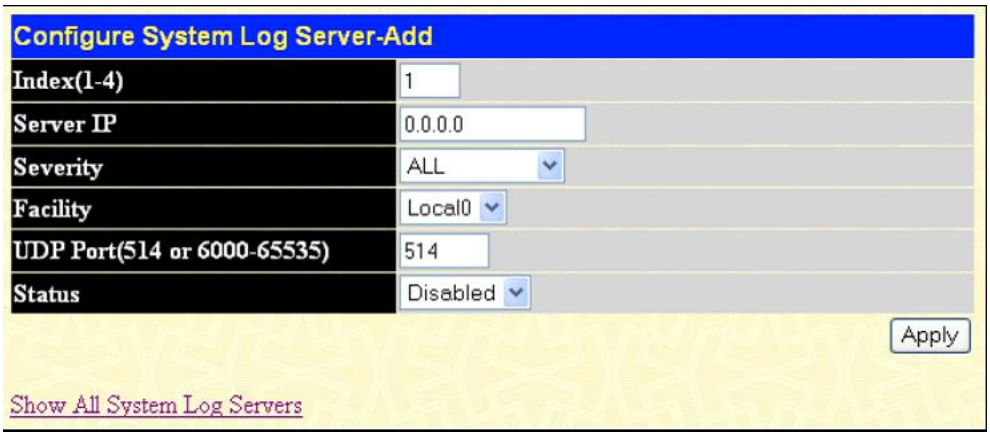


Рис. 260 – Пример окна настройки добавления отправки событий

4. Укажите следующую информацию:
    - в поле **Index** установите значение "*1*". Если устройство уже настроено на отправку на другие серверы, то выберите свободный ключ в диапазоне от "*1*" до "*4*";
    - в поле **Server IP** укажите IP-адрес агента сбора лог-коллектора;
    - в поле **Severity** из выпадающего списка выберите значение "*ALL*";
    - в поле **Facility** из выпадающего списка выберите значение "*Local4 (security/authorization messages)*";
    - в поле **UDP Port** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
    - в поле **Status** из выпадающего списка выберите значение "*Enabled*";
    - нажмите кнопку **Apply**.
5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Dlink-xstack**.

4.6.8 Eltex Switch

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Eltex-Switch
Номер (Порт)	2533
Вендор	Eltex
Тип	Switch
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс устройства.

2. Перейдите в раздел **System** → **Logs** → **Servers** (см. «Рис. 261»).

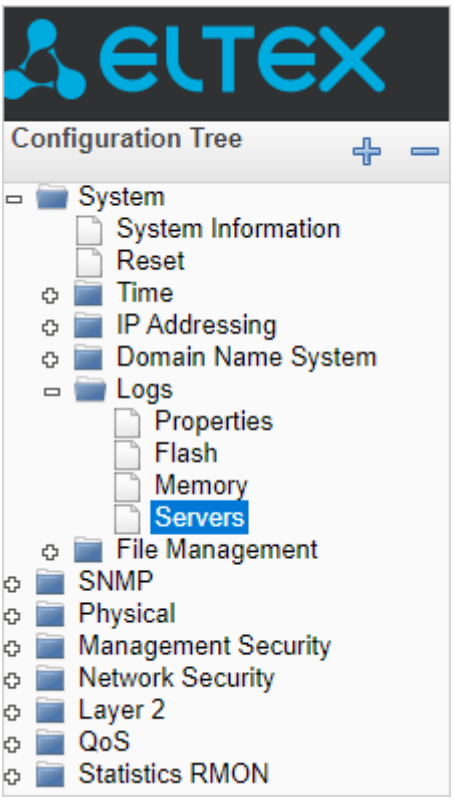


Рис. 261 – Веб-интерфейс устройства. Настройка журналирования

3. Нажмите кнопку **Add** (+). Откроется окно "Add Syslog Server" (см. «Рис. 262»).

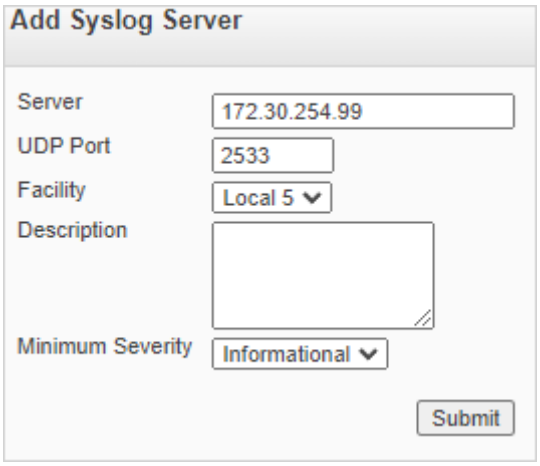


Рис. 262 – Окно "Add Syslog Server"

4. В окне выполните следующие действия:

   - в поле **Server** укажите IP-адрес агента сбора лог-коллектора.
   - в поле **UDP Port** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - в поле **Facility** из выпадающего списка выберите значение "*Local 5*".
   - в поле **Minimum Severity** из выпадающего списка выберите значение "*Informational*".

- нажмите кнопку **Submit**.

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Eltex-Switch**.

4.6.9 HP Switch

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	HP-Switch
Номер (Порт)	4530
Вендор	HP
Тип	Switch
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс устройства.
2. Перейдите в раздел **Log → Setting**.
3. В блоке **Log to hosts** укажите IP-адрес агента сбора лог-коллектора и порт (должен совпадать со значением, указанным в настройках соответствующего профиля сбора).
4. Нажмите кнопку **Сохранить и Применить**.
5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **HP-Switch**.

4.6.10 Huawei Switch

Платформа Радар поддерживает работу со следующими версиями устройства:

- Huawei S Series Switch;
- Huawei AR Series Router;
- Huawei USG Series Firewall.

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Huawei-Switch
Номер (Порт)	2531
Вендор	Huawei
Тип	Switch

Характеристика	Значение
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в интерфейс командной строки (CLI) маршрутизатора Huawei серии AR, коммутатора Huawei серии S или межсетевого экрана серии USG.
2. Получите доступ к системному представлению:

   ```
   system-view
   ```

3. Включите информационный центр:

   ```
   info-center enable
   ```

4. Настройте отправку сообщений информационного уровня:

   ```
   info-center source default channel loghost log level informational debug state off trap state off
   ```

5. Проверьте исходную конфигурацию маршрутизатора Huawei серии AR, коммутатора Huawei серии S или межсетевого экрана серии USG:

   ```
   display channel loghost
   ```

6. Укажите IP-адрес агента сбора лог-коллектора в качестве хоста журнала для вашего коммутатора и задайте facility:

   ```
   info-center loghost <ip-адрес агента сбора лог-коллектора> facility <значение facility> (например, local0)
   ```

7. Сохраните изменения и закройте интерфейс командной строки:

   ```
   quit
   ```

8. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Huawei-Switch**.

4.6.11 MikroTik Router

Платформа Радар поддерживает работу со следующими версиями устройства:

- Mikrotik-hEX-S;
- Mikrotik-hAP-ac2.

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Mikrotik-hEX-S Mikrotik-hAP-ac2
Номер (Порт)	Mikrotik-hEX-S - 2598 Mikrotik-hAP-ac2 - 2599
Вендор	Mikrotik
Тип	Switch

Характеристика	Значение
Профиль сбора	«Модуль udp_input»

Настройку источника можно выполнить следующими способами:

- с помощью консоли устройства;
- с помощью веб-интерфейса.

Способ 1. С помощью консоли устройства:

1. Войдите в **Winbox** и откройте **New Terminal**.
2. Выполните настройку действий по ведению системного журнала:

```
/system logging action
add bsd-syslog=yes - включение BSD Syslog
name=syslog
target=remote
remote=<ip-адрес агента сбора лог-коллектора>
remote-port=<порт, указанный в соответствующем профиле сбора>
```

3. Выполните настройку уровня детализации ведения журнала:

```
/system logging
add action=syslog topics=info
add action=syslog topics=critical
add action=syslog topics=error
add action=syslog topics=warning
```

Способ 2. С помощью веб-интерфейса:

1. Войдите в **Winbox** и перейдите в раздел **System → Logging → Action**.
2. Для создания нового **Action** нажмите кнопку **+**.
3. В открывшемся окне укажите следующую информацию:
    - в поле **Type** из выпадающего списка выберите значение **Remote**;
    - в поле **Remote Address**: укажите IP-адрес агента сбора лог-коллектора;
    - в поле **Remote Port**: укажите порт, указанный в соответствующем профиле сбора;
    - установите флаг **BSD Syslog**;
    - нажмите кнопку **Ok**.
4. Перейдите на вкладку **Rules** и добавьте четыре топика: **info**, **critical**, **error**, **warning**.
5. Для создания топика нажмите кнопку **+**.
6. В открывшемся окне укажите следующую информацию:
    - в поле **Topics** из выпадающего списка выберите необходимый топик, например **info**;
    - в поле **Action** из выпадающего списка выберите значение **syslog**;

- нажмите кнопку **Ok**.

7. Повторите действия 5-6 для создания всех четырех топиков.

Далее перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для соответствующего источника:

- **Mikrotik-hEX-S**;
- **Mikrotik-hAP-ac2**.

4.6.12 Ubiquiti Switch

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Ubiquiti-switch
Номер (Порт)	2557
Вендор	Ubiquiti
Тип	Switch
Профиль сбора	«Модуль udp_input»

Настройку источника можно выполнить следующими способами:

- с помощью консоли устройства;
- с помощью веб-интерфейса.

Способ 1. С помощью консоли устройства:

Внимание! *Все команды по настройке источника выполняются в **режиме глобальной конфигурации**. Для этого перейдите в привилегированный режим: введите enable и пароль администратора. В консольной строке знак > рядом с именем хоста сменится на #. Затем введите команду #configure terminal. В консольной строке знак # рядом с именем хоста сменится на (config)#.*

1. Включите журналирование и настройте подключение к агенту сбора лог-коллектора:

   ```
   (config)# logging syslog
   (config)# logging host <IP-адрес агента сбора лог-коллектора> ipv4 port 6
   ```

   Где:

   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - `6` - необходимый уровень severity.

2. Проверьте подключение к агенту сбора лог-коллектора:

```
(config)# show logging hosts
```

Пример ответа:

```
Index  IP Address/Hostname        Severity   Port   Status
-----  -------------------------- --------- ------ ----------

1      <IP-адрес агента сбора>     info       2557   Active
```

3. Проверьте настройки:

```
(config)# show logging
```

Пример ответа:

```
Logging Client Local Port           : 2557
Logging Client Source Interface     : (not configured)
CLI Command Logging                 : enabled
Console Logging                     : enabled
Console Logging Severity Filter     : info
Buffered Logging                    : enabled
Buffered Logging Severity Filter    : info
Persistent Logging                  : disabled
Persistent Logging Severity Filter  : alert
Syslog Logging                      : enabled
```

Способ 2. С помощью веб-интерфейса:

1. Войдите в веб-интерфейс устройства.
2. Перейдите в раздел **System** → **Logs** → **Configuration**.
3. Укажите в разделе следующие настройки:

```
Log Configuration
Buffered Log Configuration
Admin Mode   Enable
Behavior     Wrap
Command Logger Configuration
Admin Mode   Enable
Console Log Configuration
Admin Mode   Enable
Severity Filter  Info
Persistent Log Configuration
Admin Mode   Disable
Severity Filter  Alert
Syslog Configuration
Admin Mode   Enable
Local UDP Port  port (1 to 65535)
```

4. Сохраните изменения.

Далее перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Ubiquiti-switch**.

4.7 Системы защиты электронной почты

При работе по подключению систем защиты электронной почты в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.7.1 IBM Postfix

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	IBM-Postfix
Номер (Порт)	1534
Вендор	IBM
Тип	MTA
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Подключитесь по SSH к узлу с установленным Postfix MTA.
2. В конфигурационном файле `/etc/rsyslog.conf` укажите следующие настройки:

   ```
   mail.*@<IP-адрес агента сбора лог-коллектора>:port
   ```

   Где:

   - `mail` - значение facility (по умолчанию);
   - `@` - передача данных по протоколу **UDP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

Примечание: *при необходимости вы можете изменить значение facility, заданное по умолчанию. Для этого в конфигурационном файле* `/etc/postfix/main.cf` *укажите необходимое значение в строке* `syslog_facility` *и перезапустите службу* ***Postfix****. Затем укажите данное значение в конфигурационном файле* `/etc/rsyslog.conf` *вместо значения по умолчанию* `mail`.

3. Сохраните изменения и перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **IBM-Postfix**.

4.7.2 Microsoft Exchange Server. Audit

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Microsoft-Exchange-Audit
Номер (Порт)	1533
Вендор	Microsoft
Тип	Exchange audit
Профиль сбора (локальный сбор)	«Модуль eventlog_input_local»
Профиль сбора (удаленный сбор)	«Модуль smb_input»

Для настройки источника выполните следующие действия:

Примечание: *события от источника включены по умолчанию и записываются в журнал по пути* ***C:\Program Files\Microsoft\Exchange Server\V15\Logging\CosmosQueue***.

Рекомендуется устанавливать агент сбора лог-коллектора на том же сервере, где и Microsoft Exchange Server, но при необходимости вы можете его настроить на удаленном сервере (подробнее см. раздел «Microsoft Exchange Server. Сбор событий по сети»).

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Exchange-Audit**.

4.7.3 Microsoft Exchange Server. Message Tracking

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Microsoft-Exchange-MessageTracking
Номер (Порт)	1532
Вендор	Microsoft
Тип	Message Tracking
Профиль сбора (локальный сбор)	«Модуль eventlog_input_local»
Профиль сбора (удаленный сбор)	«Модуль smb_input»

Примечание: *события от источника необходимо включить через консоль. События будут записываться в журнал по пути* ***C:\Program Files\Microsoft Exchange Server\V15\TransportRoles\Logs\MessageTracking***.

Рекомендуется устанавливать агент сбора лог-коллектора на том же сервере, где и Microsoft Exchange Server, но при необходимости вы можете настроить его на удаленном сервере (подробнее см. раздел «Microsoft Exchange Server. Сбор событий по сети»).

Для настройки источника выполните следующие действия:

1. Войдите в консоль Exchange Administration Center и перейдите в раздел **Servers** (см. «Рис. 263»).

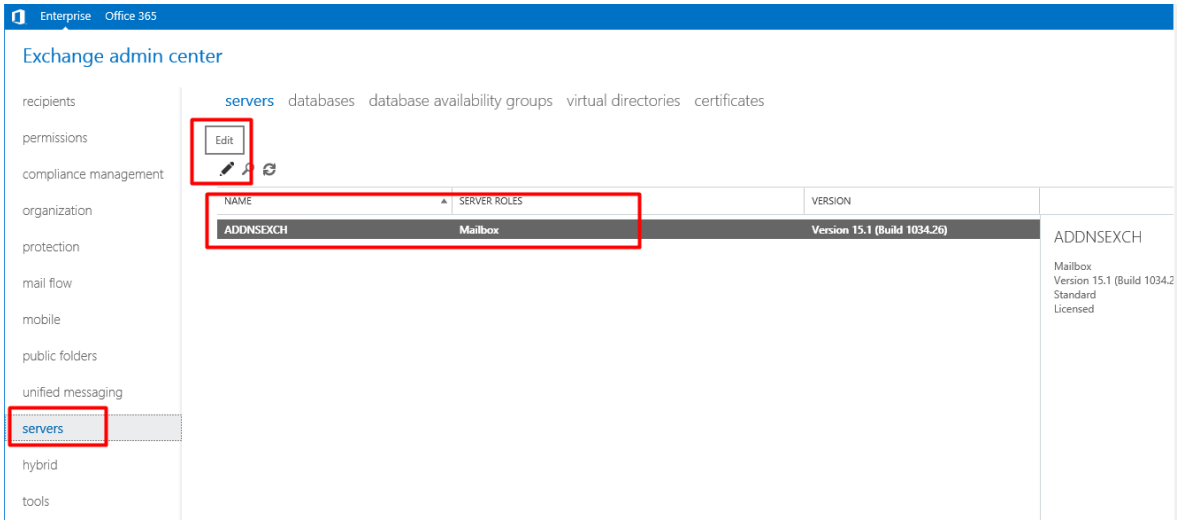


Рис. 263 – Выбор почтового сервера

2. Выберите нужный почтовый сервер, нажмите кнопку **Edit** и в открывшемся окне перейдите на вкладку "transport logs" (см. «Рис. 264»).

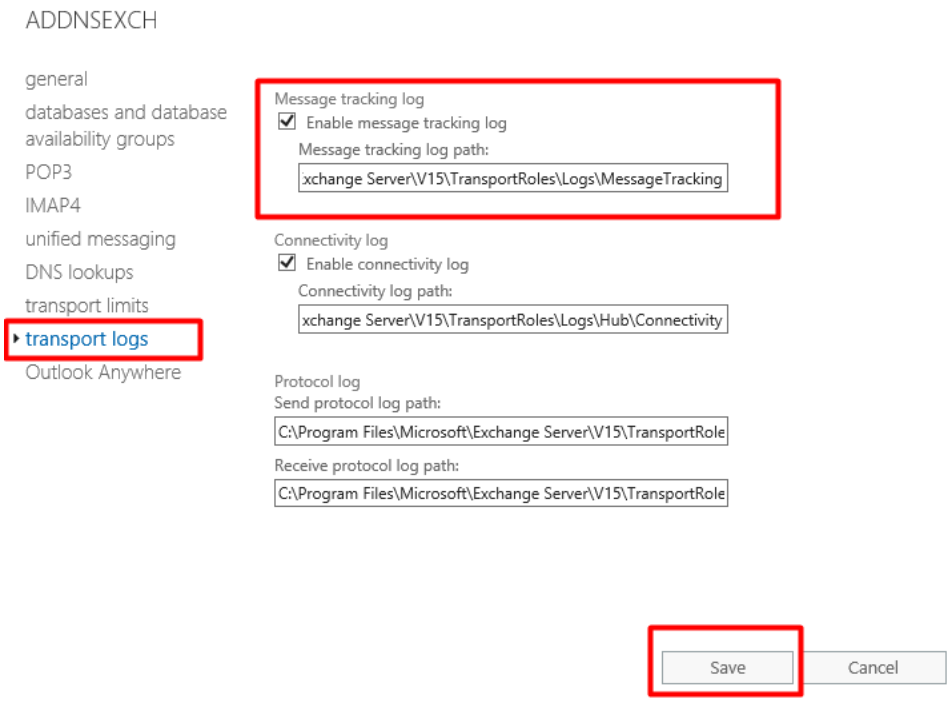


Рис. 264 – Настройка почтового сервера. Вкладка "transport logs"

3. На вкладке "transport logs" укажите следующие настройки:
   - в поле **Enable message tracking log** включите отслеживание сообщений на сервере, установив соответствующий флаг;

- в поле **Message tracking log path** укажите путь к файлу журнала;
- нажмите кнопку **Save**.

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Exchange-MessageTracking**.

4.7.4 Microsoft Exchange Server. OWA

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-Exchange-OWA
Номер (Порт)	1530
Вендор	Microsoft
Тип	OWA
Профиль сбора (локальный сбор)	«Модуль eventlog_input_local»
Профиль сбора (удаленный сбор)	«Модуль smb_input»

Примечание: *события от источника включены по умолчанию и записываются в журналы по пути* ***C:\inetpub\logs\LogFiles\W3SVC1*** *и* ***C:\inetpub\logs\LogFiles\W3SVC2***.

Рекомендуется устанавливать агент сбора лог-коллектора на том же сервере, где и Microsoft Exchange Server, но при необходимости вы можете настроить его на удаленном сервере (подробнее см. раздел «Microsoft Exchange Server. Сбор событий по сети»).

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Exchange-OWA**.

4.7.5 Microsoft Exchange Server. SMTP

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-Exchange-SMTP
Номер (Порт)	1531
Вендор	Microsoft
Тип	SMTP
Профиль сбора (локальный сбор)	«Модуль eventlog_input_local»
Профиль сбора (удаленный сбор)	«Модуль smb_input»

Примечание: *события от источника необходимо включить через консоль. События будут записываться в журнал по пути* ***C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd\ProtocolLog****.*

Рекомендуется устанавливать агент сбора лог-коллектора на том же сервере, где и Microsoft Exchange Server, но при необходимости вы можете настроить его на удаленном сервере (подробнее см. раздел «Microsoft Exchange Server. Сбор событий по сети»).

Для настройки источника выполните следующие действия:

1. Войдите в консоль Exchange Administration Center и перейдите в раздел **Mail Flow → Receive Connectors** (см. «Рис. 265»).

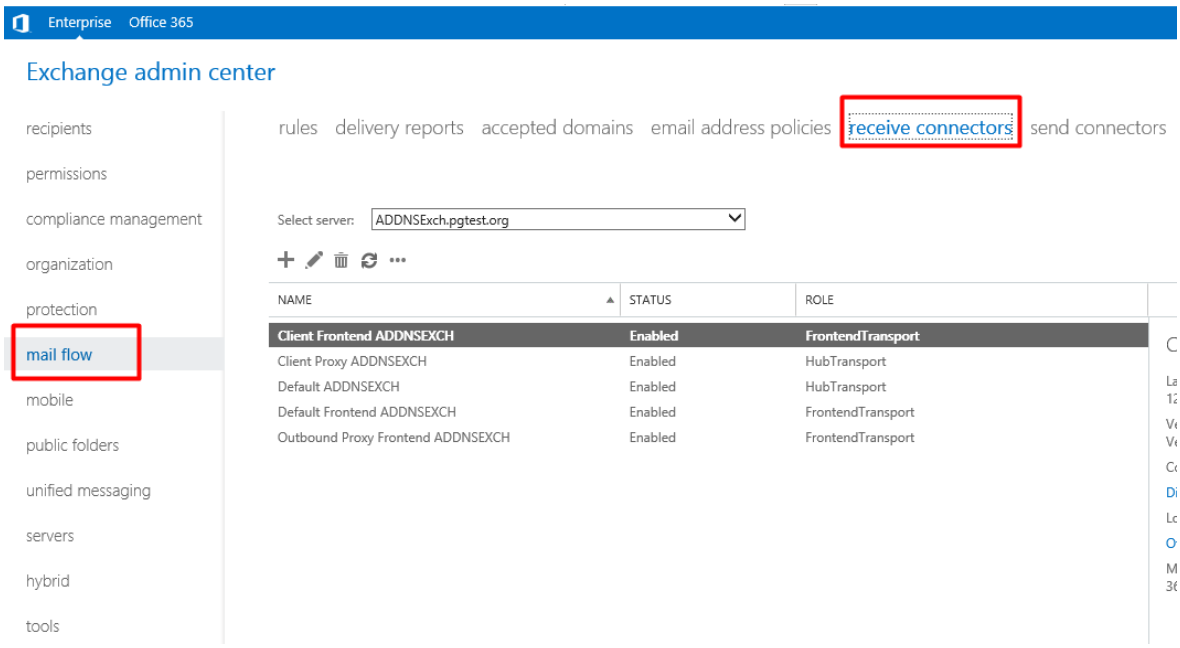


Рис. 265 – Раздел "Mail Flow"

2. Выберите нужный коннектор, нажмите кнопку **Edit** и в открывшемся окне перейдите на вкладку "general" (см. «Рис. 266»).

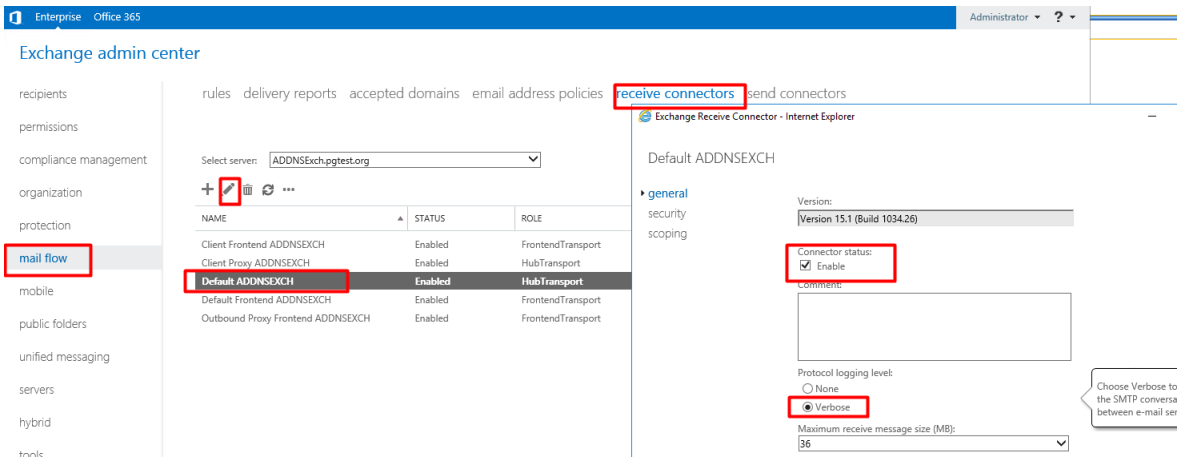


Рис. 266 – Настройка параметров логирования.

3. На вкладке "general" укажите следующие настройки:
   - в поле **Connector status** установите флаг **Enable**;
   - в поле **Protocol logging level list** выберите значение "*Verbose*";

- нажмите кнопку **Save**.

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Exchange-SMTP**.

4.7.6 Microsoft Exchange Server. Сбор событий по сети

При необходимости можно настроить сбор событий по сети для следующих источников:

- «Microsoft Exchange Server. Audit»;
- «Microsoft Exchange Server. Message Tracking»;
- «Microsoft Exchange Server. OWA»;
- «Microsoft Exchange Server. SMTP».

Для этого необходимо открыть сетевой доступ к каталогам с журналами и настроить удаленный агент сбора лог-коллектора для сбора данных по сети.

Примечание: предпочтительным способом сбора данных, как наиболее безопасным, является установка агента сбора лог-коллектора на серверах Exchange, поскольку в данном случае не придется открывать сетевой доступ к каталогам с журналами.

Для настройки сбора событий по сети выполните следующие действия:

1. Откройте сетевой доступ к каталогам с журналами.
2. Создайте пользователя с правами доступа к этим каталогам по сети.
3. На удаленном агенте сбора лог-коллектора настройте профиль сбора **smb_input** для соответствующего источника (подробнее см. раздел «Модуль smb_input»).
4. Проверьте доступность необходимых адресов и портов, в случае недоступности откройте их на межсетевом экране.
5. Далее перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для соответствующего источника:
    - **Microsoft-Exchange-Audit**;
    - **Microsoft-Exchange-MessageTracking**;
    - **Microsoft-Exchange-OWA**;
    - **Microsoft-Exchange-SMTP**.

4.7.7 Zimbra

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Zimbra
Номер (Порт)	1599
Вендор	Synacor

Характеристика	Значение
Тип	MTA
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Откройте конфигурационный файл службы `rsyslog`:

   ```
   # nano /etc/rsyslog.conf
   ```

2. В конфигурационном файле `/etc/rsyslog.conf` укажите следующие настройки:

   ```
   module(load="imfile" PollingInterval="5")
   input(type="imfile"
         reopenOnTruncate="on"
         File="/opt/zimbra/log/audit.log"
         Tag="zimbra-audit"
         ruleset="zimbrafwd")
   input(type="imfile"
         reopenOnTruncate="on"
         File="/opt/zimbra/log/mailbox.log"
         Tag="zimbra-mailbox"
         ruleset="zimbrafwd")
   ruleset(name="zimbrafwd")
   {
       action(type="omfwd"
           Target="IP-адрес коллектора"
           Port="1599"
           Protocol="tcp"
           ResendLastMSGOnReconnect="on"
           action.resumeRetryCount="100"
           queue.type="linkedList"
           queue.size="10000")
       stop
   }

   ### begin forwarding rule ###
   *.* @@<IP-адрес агента сбора лог-коллектора>:port
   ### end of the forwarding rule ###
   ```

   Где:

   - `@@` - передача данных по протоколу **TCP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

3. Перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Zimbra**.

4.8 Инфраструктурные системы

При работе по подключению инфраструктурных систем в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.8.1 Citrix ADC (Netscaler)

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Citrix-ADC
Номер (Порт)	2870
Вендор	Citrix
Тип	Citrix-Netscaler
Профиль сбора	«Модуль tcp_input»

Примечание: *рекомендуется настраивать источник через веб-интерфейс и использовать указанные параметры конфигурации. При конфигурировании через командную сроку используйте точно такие же параметры. Изменение любого из них может повлиять на корректность работы правил разбора в **Платформе Радар**.*

Информацию о параметрах, а также о способе настройки источника с помощью командной строки, можно получить в документации на сайте вендора.

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс Citrix ADC (см. «Рис. 267»).

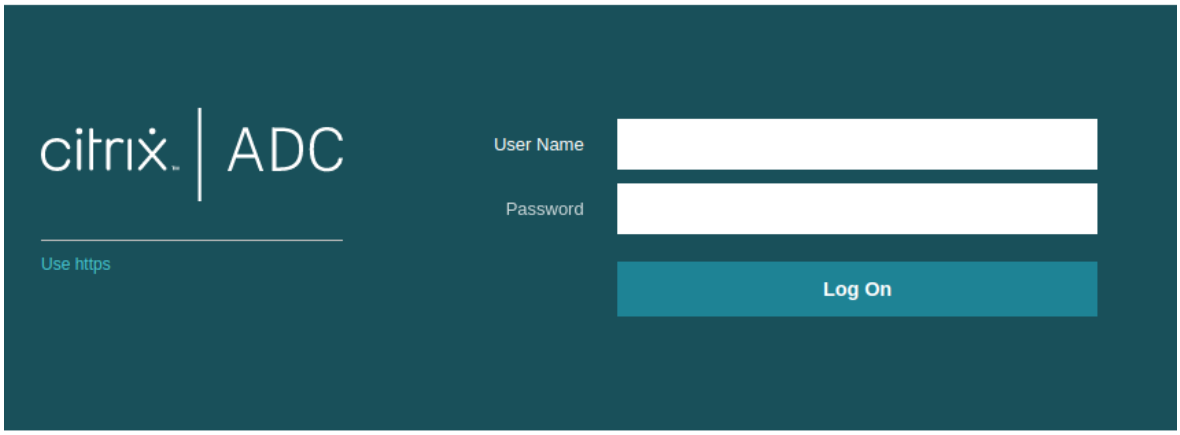


Рис. 267 – Вход в веб-интерфейс Citrix ADC

2. Перейдите в раздел **Configuration** → **System** → **Auditing** → **Syslog** (см. «Рис. 268»).

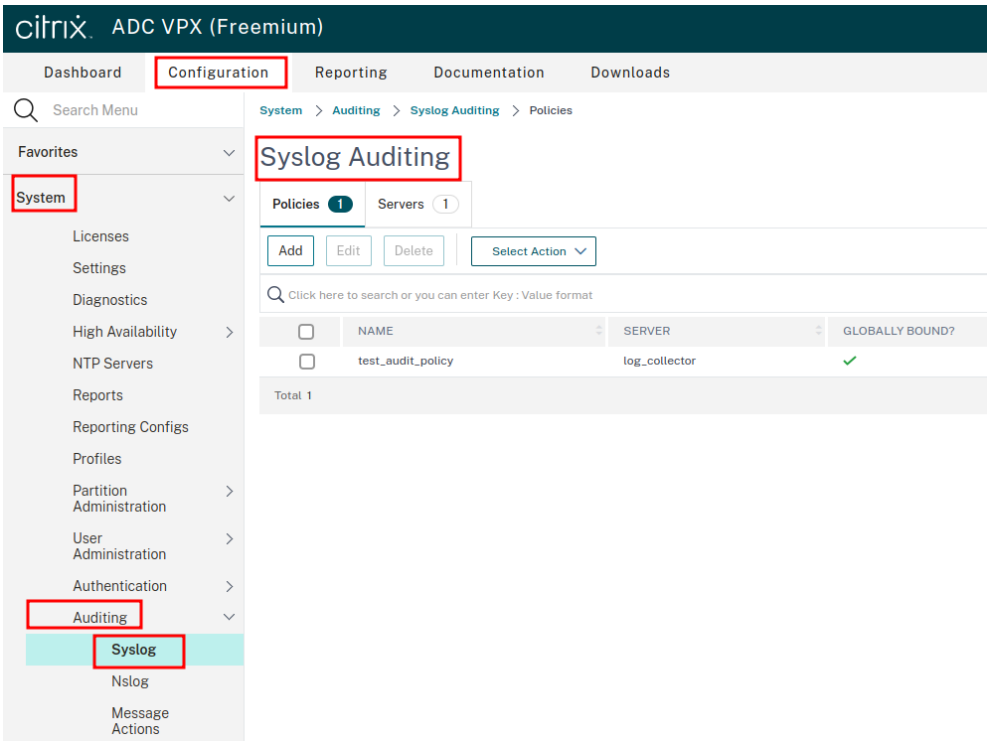


Рис. 268 – Настройки журналирования

3. Перейдите на вкладку **Servers** и нажмите кнопку **Add**. Откроется окно "Create Auditing Server" (см. «Рис. 269»).

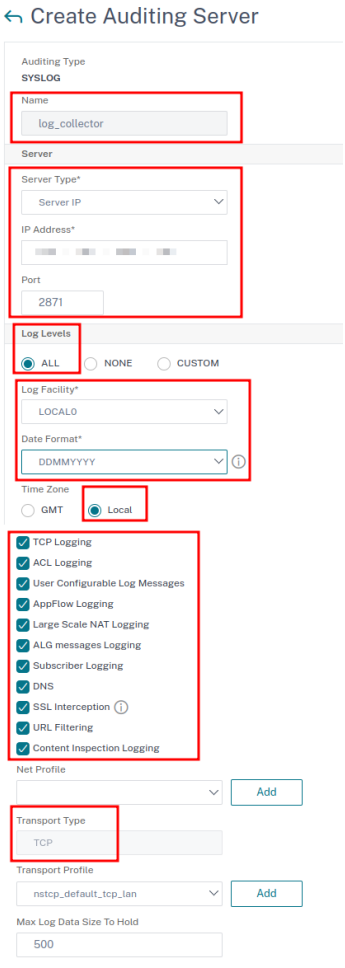


Рис. 269 – Окно "Create Auditing Server"

4. Укажите в окне следующие настройки:
    - в поле **Name** укажите наименование сервера;
    - в поле **Server Type** из выпадающего списка выберите значение "*Server IP*";
    - в поле **IP Address** укажите IP-адрес агента сбора лог-коллектора;
    - в поле **Port** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Опциональный параметр;
    - в поле **Log Levels** выберите значение "*ALL*";
    - в поле **Log Facility** выберите необходимый уровень facility;
    - выберите журналы которые необходимо отправлять в **Платформу Радар**, установив соответствующие флаги.
    - нажмите кнопку **Create**.
5. Создайте политику журналирования. Для этого перейдите на вкладку **Policies** и нажмите кнопку **Add**. Откроется окно "Create Auditing Syslog Policy" (см. «Рис. 270»).

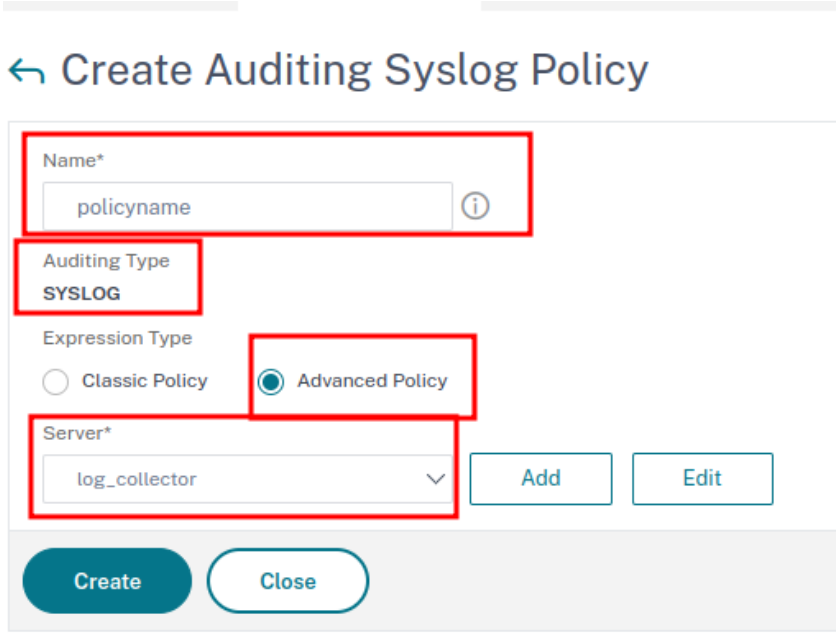


Рис. 270 – Окно "Create Auditing Syslog Policy"

6. Укажите в окне следующие настройки:
    - в поле **Name** укажите наименование политики;
    - в поле **Expression Type** выберите значение "*Advanced Policy*";
    - в поле **Server** из выпадающего списка выберите сервер, который был создан ранее;
    - нажмите кнопку **Create**.
7. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Citrix-ADC**.

4.8.2 Dell IDRAC

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	IDRAC
Номер (Порт)	4529
Вендор	Dell
Тип	remote_access_control
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Войдите в интерфейс Chassis Management Controller и перейдите в раздел **Server Overview → Properties → Status** (см. «Рис. 271»).

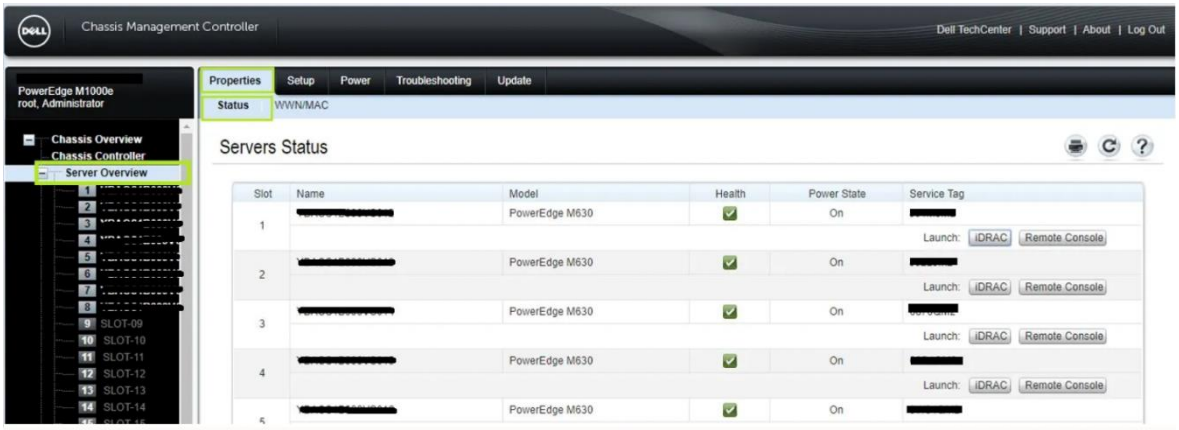


Рис. 271 – Chassis Management Controller UI. Настройки

2. Включите журналирование на нужных серверах. Для этого нажмите на кнопку **IDRAC** в строке соответствующего сервера (см. «Рис. 272»).

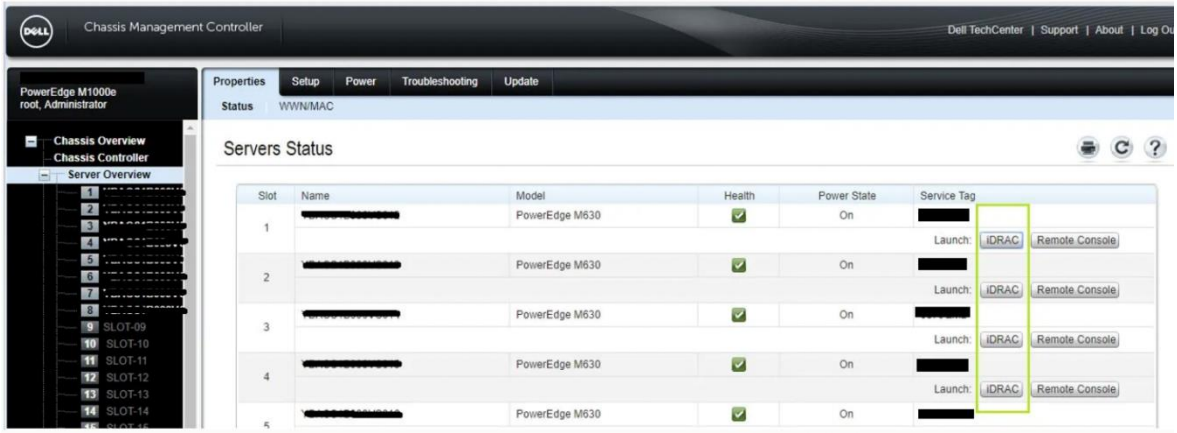


Рис. 272 – Список серверов

3. Перейдите в раздел **Server → Logs → Settings** (см. «Рис. 273»).

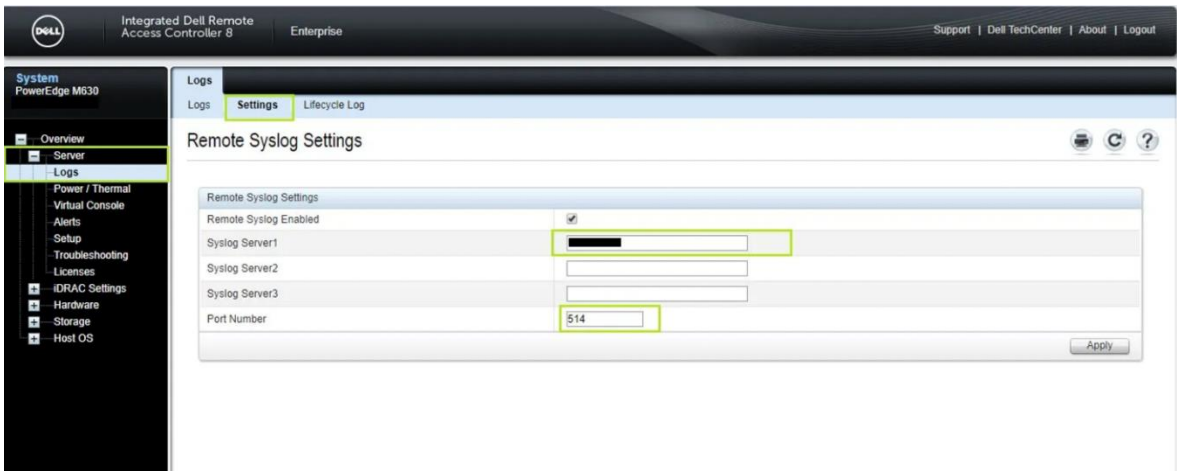


Рис. 273 – Настройка параметров журналирования

4. В разделе укажите следующие настройки:
   - установите флаг **Remote Syslog Settings**;
   - в поле **Syslog Server** укажите IP-адрес агента сбора лог-коллектора;
   - в поле **Port Number** укажите порт, по которому агент сбора лог-коллектора будет принимать события;
   - нажмите кнопку **Apply**.
5. Перейдите в раздел **Server → Alerts** (см. «Рис. 274»).

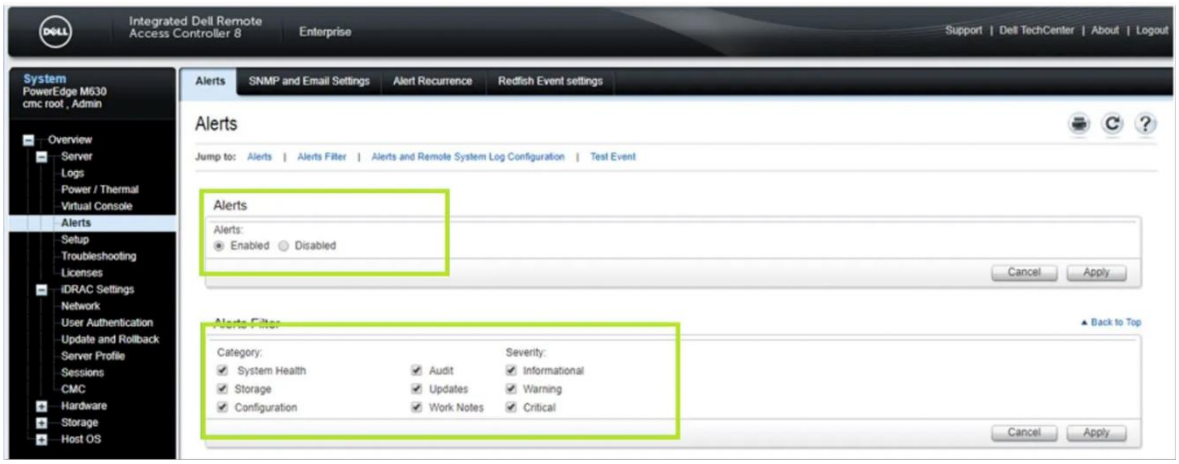


Рис. 274 – Настройка предупреждений. Часть 1

6. В разделе укажите следующие настройки:
   - в блоке **Alerts** включите предупреждения и нажмите кнопку **Apply**;
   - в блоке **Alert Filter** выберите необходимые фильтры, установив соответствующие флаги и нажмите кнопку **Apply**;
   - в блоке **Alerts and Remote System Log Configuration** установите соответствующие флаги в графе таблицы "Remote System Log" и нажмите кнопку **Apply** (см. «Рис. 275»).

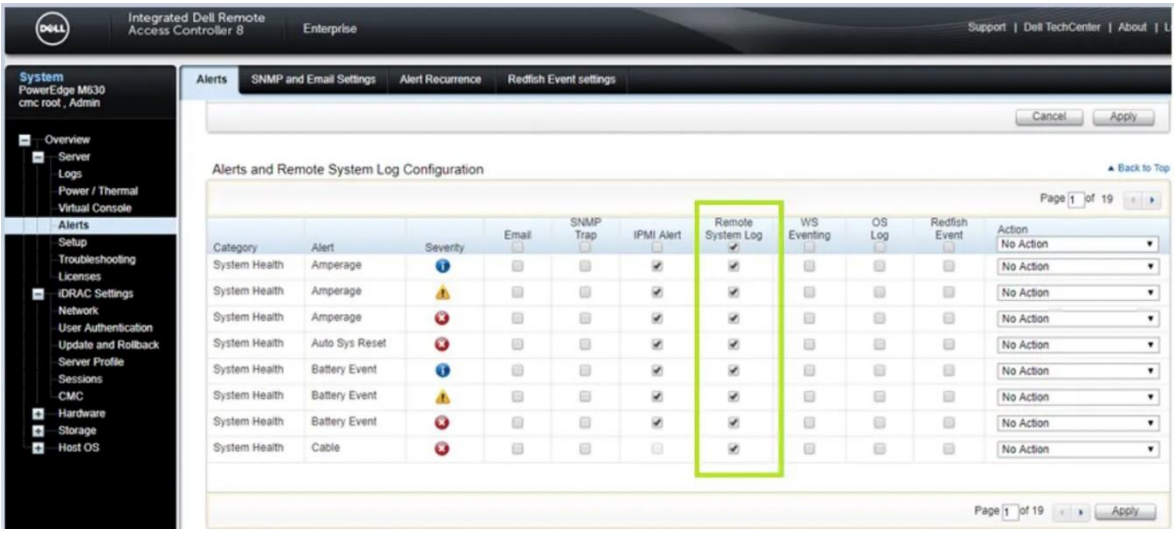


Рис. 275 – Настройка предупреждений. Часть 2

7. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **IDRAC**.

4.8.3 FreeIpa

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	FreeIpa
Номер (Порт)	1600
Вендор	Red-Hat
Тип	LDAP
Профиль сбора	«Модуль udp_input»

События от источника включены по умолчанию и записываются в следующие журналы:

- `/var/log/krb5kdc.log` - содержит информацию о работе службы Kerberos 5 Key Distribution Center (KDC);
- `/var/log/dirsrv/slapd-YOURDOMAIN-LOCAL/access` - содержит информацию о запросах на чтение данных из каталога LDAP;
- `/var/log/dirsrv/slapd-YOURDOMAIN-LOCAL/errors` - содержит информацию об ошибках в работе службы каталога LDAP.

Для настройки источника выполните следующие действия:

1. Откройте конфигурационный файл службы `rsyslog`:

   ```
   # nano /etc/rsyslog.conf
   ```

2. В конфигурационном файле `/etc/rsyslog.conf` укажите следующие настройки:

```
module(load="imfile" PollingInterval="10")
input(type="imfile"
reopenOnTruncate="on"
File="/var/log/krb5kdc.log"
Tag="tag_freeipa_log")

input(type="imfile"
reopenOnTruncate="on"
File="/var/log/dirsrv/slapd-PGR-LOCAL/access"
Tag="tag_freeipa_log")

input(type="imfile"
reopenOnTruncate="on"
File="/var/log/dirsrv/slapd-PGR-LOCAL/errors"
Tag="tag_freeipa_log")

if $syslogtag == 'tag_freeipa_log' then @<IP-адрес агента сбора лог-
коллектора>:port
& stop
```

Где:

- `@` - передача данных по протоколу **UDP**;
- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

3. Перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **FreeIpa**.

4.8.4 FreeRADIUS

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	FreeRADIUS
Номер (Порт)	2935
Вендор	FreeRADIUS
Тип	RADIUS-Server
Профиль сбора	«Модуль tcp_input»

Для отправки событий с сервера FreeRADIUS используется служба `rsyslog`. События записываются и забираются из файла `radius.log`.

Для настройки источника выполните следующие действия:

1. Откройте конфигурационный файл `radiusd.conf`:

   ```
   # nano /etc/freeradius/3.0/radiusd.conf
   ```

2. Настройте блок `log` следующим образом:

   ```
   log {
    destination = syslog
    file = syslog
    syslog_facility = local2
    stripped_names = no
    auth = yes
    auth_badpass = no
    auth_goodpass = no
   # msg_goodpass = ""
   # msg_badpass = ""
   }
   ```

3. В конфигурационном файле найдите пункт `logdir = /var/log/freeradius/radius.log` и замените его на `logdir = syslog`.

4. Подготовьте конфигурационный файл для службы `rsyslog` со следующей настройкой:

   ```
   local2.*        @@<IP-адрес агента сбора лог-коллектора>:port
   ```

   Где: - `local2.*` - необходимый уровень `facility;` - `@@` - передача данных по протоколу **TCP**; - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора; - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

5. Поместите его в директорию `/etc/rsyslog.d/` и перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog
   ```

6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **FreeRADIUS**.

4.8.5 Gitlab

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Gitlab-DevOps-Platform
Номер (Порт)	4450
Вендор	Gitlab
Тип	DevOps-Platform
Профиль сбора	«Модуль udp_input»

События аутентификации и изменение конфигураций сохраняются в журнал **application.log** по пути `/var/log/gitlab/gitlab-rails/`.

Для настройки источника выполните следующие действия:

1. Создайте шаблон `/etc/rsyslog.d/gitlab_to_pangeoradar.conf` для службы `rsyslog` и откройте его на редактирование:

   ```
   sudo nano /etc/rsyslog.d/gitlab_to_pangeoradar.conf
   ```

2. Настройте отправку сообщений в **Платформу Радар**:

   ```
   module(load="imfile" PollingInterval="10")
   input(type="imfile"
         reopenOnTruncate="on"
         File="/var/log/gitlab/gitlab-rails/application.log"
         Tag="tag_gitlab_log")
   if $syslogtag == 'tag_gitlab_log' then @<IP-адрес агента сбора лог-
   коллектора>:port
   & stop
   ```

   Где:

   - `@` - передача данных по протоколу **UDP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

3. Откройте конфигурационный файл `/etc/rsyslog.d/rsyslog.conf` и закомментируйте следующие строки:

   ```
   #$FileOwner syslog
   #$FileGroup adm
   #$FileCreateMode 0640
   #$DirCreateMode 0755
   #$Umask 0022
   #$PrivDropToUser git
   #$PrivDropToGroup git
   #$PrivDropToUser syslog
   #$PrivDropToGroup syslog
   ```

4. Сохраните изменения и перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog
   ```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Gitlab-DevOps-Platform**.

4.8.6 ISC Bind DNS

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	BIND
Номер (Порт)	2800
Вендор	ISC
Тип	DNS
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Настройте журналирование системы **Bind**. Для этого в файл `/etc/bind/named.conf` добавьте следующие строки:

```
logging {
    channel named {
        file "/var/log/named/named.log" versions 10 size 20M;
        severity info;
        print-time yes;
        print-category yes;
        print-severity yes;
    };

    channel security {
        file "/var/log/named/security.log" versions 10 size 20M;
        severity info;
        print-time yes;
        print-severity yes;
    };

    channel dnssec {
        file "/var/log/named/dnssec.log" versions 10 size 20M;
        severity info;
        print-time yes;
        print-severity yes;
    };

    channel resolver {
        file "/var/log/named/resolver.log" versions 10 size 20M;
        severity info;
        print-time yes;
        print-severity yes;
    };

    channel query_log {
        file "/var/log/named/query.log" versions 10 size 80M;
        severity info;
        print-time yes;
        print-severity yes;
    };

    channel query_error {
        file "/var/log/named/query_errors.log" versions 10 size 20M;
        severity info;
        print-time yes;
```

```
        print-severity yes;
    };

    channel lame_servers {
        file "/var/log/named/lame-servers.log" versions 10 size 20M;
        severity info;
        print-time yes;
        print-severity yes;
    };

    channel capacity {
        file "/var/log/named/capacity.log" versions 10 size 20M;
        severity info;
        print-time yes;
        print-severity yes;
    };

    channel database {
        file "/var/log/named/database.log" versions 10 size 20M;
        severity info;
        print-time yes;
        print-severity yes;
    };

    channel update {
        file "/var/log/named/update.log" versions 10 size 10M;
        severity info;
        print-time yes;
        print-severity yes;
    };

    category default        { default_syslog; named; };
    category general        { default_syslog; named; };
    category security       { security; };
    category queries        { query_log; };
    category query-errors   { query_error; };
    category lame-servers   { lame_servers; };
    category dnssec         { dnssec; };
    category edns-disabled  { default_syslog; resolver; };
    category config         { default_syslog; named; };
    category resolver       { resolver; };
    category cname          { resolver; };
    category spill          { capacity; };
    category rate-limit     { capacity; };
    category database       { database; };
    category client         { default_syslog; named; };
    category network        { default_syslog; named; };
    category unmatched      { named; };
    category delegation-only { named; };
    category update         { default_syslog; update; };
    category update-security { default_syslog; update; };
};
```

2. Сохраните изменения и проверьте конфигурацию:

```
# sudo named-checkconf /etc/bind/named.conf.options
```

3. Для организации хранения файлов журнала создайте директорию, настройте необходимые разрешения и владельцев:

```
# mkdir -p /var/log/named
# touch /var/log/named/named.log
# touch /var/log/named/security.log
# touch /var/log/named/dnssec.log
# touch /var/log/named/resolver.log
# touch /var/log/named/query.log
# touch /var/log/named/query_errors.log
# touch /var/log/named/lame-servers.log
# touch /var/log/named/capacity.log
# touch /var/log/named/database.log
# touch /var/log/named/update.log
# chown bind:bind /var/log/named
# chown bind:bind /var/log/named/*.log
# chmod 640 /var/log/named/*.log
```

4. Перезапустите сервис **Bind9**.

   ```
   # service bind9 restart
   ```

5. Настройте службу `rsyslog` на сервере **Bind**. Для этого создайте шаблон по пути `/etc/rsyslog.d/`:

   ```
   # sudo nano /etc/rsyslog.d/bind.conf
   ```

   И укажите в нем следующие настройки:

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

input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/capacity.log"
      Tag="tag_dns_log")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/dnssec.log"
      Tag="tag_dns_log")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/named.log"
      Tag="tag_dns_log")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/query.log"
      Tag="tag_dns_log")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/security.log"
      Tag="tag_dns_log")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/database.log"
      Tag="tag_dns_log")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/lame-servers.log"
      Tag="tag_dns_log")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/query_errors.log"
      Tag="tag_dns_log")
input(type="imfile"
```

```
      reopenOnTruncate="on"
      File="/var/log/named/resolver.log"
      Tag="tag_dns_log")
input(type="imfile"
      reopenOnTruncate="on"
      File="/var/log/named/update.log"
      Tag="tag_dns_log")
if $syslogtag == 'tag_dns_log' then @<IP-адрес агента сбора лог-
коллектора>:port
& stop
```

Где:

- `@` - передача данных по протоколу **UDP**;
- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

6. Перезапустите службу `rsyslog`.

```
# systemctl restart rsyslog
```

7. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **BIND**.

4.8.7 Linux NFS Server

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Linux-NFS
Номер (Порт)	4570
Вендор	Linux-NFS-Project
Тип	Storage
Профиль сбора	«Модуль tcp_input»

Примечание: *все настройки, должны осуществляться с правами администратора (root). Пример конфигурации приведен для сервера под управлением ОС Debian*.

Для настройки источника выполните следующие действия:

1. Откройте файл `/etc/default/nfs-kernel-server`:

```
# nano /etc/default/nfs-kernel-server
```

Укажите в нем следующую настройку:

```
RPCNFSDOPTS="--syslog"
```

2. Откройте файл `/etc/idmapd.conf`:

```
# nano /etc/idmapd.conf
```

Укажите в нем следующую настройку:

```
Verbosity = 4
```

3. Выполните команду:

   ```
   # rpcdebug -m nfsd -s all
   ```

4. Перезапустите службу `nfs-kernel-server`:

   ```
   # systemctl restart nfs-kernel-server.service
   ```

5. Откройте конфигурационный файл службы `rsyslog`:

   ```
   # nano /etc/rsyslog.conf
   ```

   Добавьте в конец файла следующую строку:

   ```
   :msg,contains,"nfsd" @@<IP-адрес агента сбора лог-коллектора>:port
   ```

   Где:

   - `@@` - передача данных по протоколу **TCP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

6. Перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

7. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Linux-NFS**.

4.8.8 Microsoft Windows DNS

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-Windows-DNS
Номер (Порт)	1516
Вендор	Microsoft
Тип	DNS
Профиль сбора (локальный сбор)	«Модуль file_input»
Профиль сбора (удаленный сбор)	«Модуль smb_input»

Примечание: *в зависимости от сценария развертывания агента сбора лог-коллектора, локально или удаленно, используйте соответствующий профиль сбора для настройки данного источника*.

Для настройки источника выполните следующие действия:

1. Откройте свойства DNS сервера и перейдите в раздел **Ведение журнала отладки** (см. «Рис. 276»).

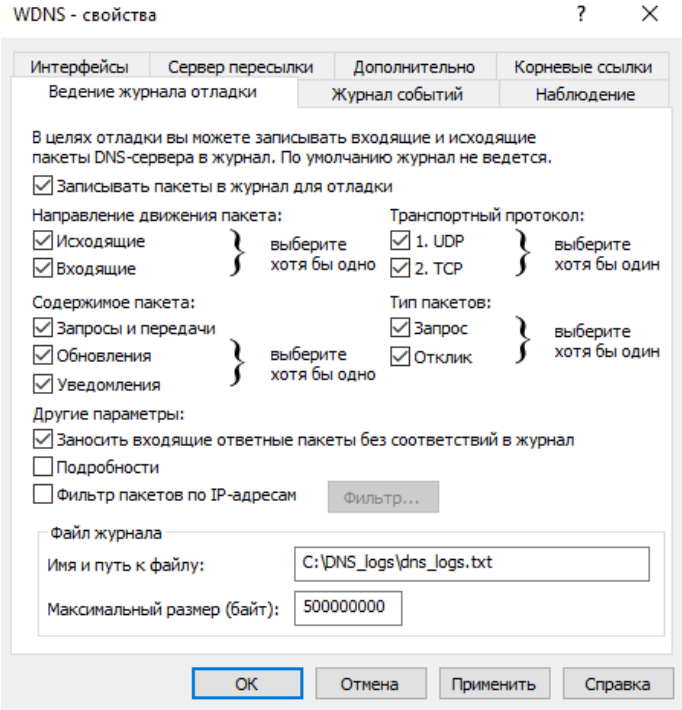


Рис. 276 – Ведение журнала отладки.

2. В разделе укажите следующие настройки:
   - включите запись пакетов в журнал для отладки, установив соответствующий флаг;
   - настройте параметры в блоках **Направление движения пакета**, **Содержимое пакета**, **Другие параметры**, установив соответствующие флаги;
   - в поле **Имя и путь к файлу** укажите файл, куда DNS сервер будет сохранять события.
   - нажмите кнопку **Применить**.
3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Windows-DNS**.

4.8.9 Microsoft Windows RDS-GW

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-Windows-RDS-GW
Номер (Порт)	1510
Вендор	Microsoft
Тип	Gateway

Характеристика	Значение
Профиль сбора	«Модуль eventlog_input_local»

Примечание: *события от источника включены по умолчанию и записываются в следующие журналы Windows:* ***Microsoft-Windows-TerminalServices-Gateway/Admin*** *и -* ***Microsoft-Windows-TerminalServices-Gateway/Operational****. Агент сбора лог-коллектора должен быть установлен на том же сервере, где и Microsoft-Windows-RDS-GW.*

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Windows-RDS-GW**.

4.8.10 Simon Kelley DNSmasq

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	DNSmasq
Номер (Порт)	3011
Вендор	Simon-Kelley
Тип	DNS
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. При необходимости установите `dnsmasq`:

   ```
   # apt install dnsmasq resolvconf
   ```

2. Настройте конфигурационный файл `/etc/dnsmasq.conf`:

   Раскомментируйте следующие параметры

   ```
   no-resolv
   server=8.8.8.8
   listen-address=0.0.0.0
   bind-interfaces
   ```

   Добавьте в конец файла следующий параметр

   ```
   log-facility=/var/log/dnsmasq.log
   ```

   Где

   - `no-resolv` - параметр, отключающий загрузку настроек из `/etc/resolv.conf`, с целью загрузки настроек только из родного конфига /etc/dnsmasq.conf;
   - `server=8.8.8.8` - адрес публичного DNS-сервера, на который будут отправляться те запросы, какие не сможет обработать Dnsmasq будут направлены на этот сервер;

- `listen-address=0.0.0.0` - настройка для осуществления подключения к DNS-серверу с других хостов;
- `bind-interfaces` - отключает привязку к интерфейсам на DNS-сервере;
- `log-facility=/var/log/dnsmasq.log` - включает отдельный лог для dnsmasq.

3. Для предотвращения конфликтов с `system-resolve` настройте конфигурационный файл `/etc/systemd/resolved.conf`

   Раскомментируйте данный параметр и укажите значение "no":

   ```
   DNSStubListener=no
   ```

4. Перезапустите службы:

   ```
   # systemctl restart systemd-resolved.service
   ```

   ```
   # systemctl start dnsmasq
   ```

5. Создайте шаблон `/etc/rsyslog.d/10-dnsmasq.conf` для службы `rsyslog` и укажите в нем следующие настройки:

   ```
   # Input modules
   module(load="imfile" mode="inotify" PollingInterval="10")

   # dnsmasq log
   input(type="imfile" File="/var/log/dnsmasq.log"
       Tag="ubuntu_dns"
       Severity="info"
       Facility="local3")
   ```

   ```
   local3.*  @@<IP-адрес агента сбора лог-коллектора>:port
   ```

   Где:

   - `@@` - передача данных по протоколу **TCP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **DNSmasq**.

4.8.11 Unbound_DNS

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Unbound-Unbound_DNS
Номер (Порт)	3010
Вендор	Unbound

Характеристика	Значение
Тип	Unbound_DNS
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Откройте конфигурационный файл `unbound.conf`:

   ```
   # sudo nano /etc/unbound/unbound.conf
   ```

2. Включите использование `syslog`:

   ```
   server:
   use-syslog: yes
   ```

3. Сохраните изменение и перезапустите службу:

   ```
   # sudo service unbound restart
   ```

4. Создайте шаблон `/etc/rsyslog.d/30-unbound.conf` для службы `rsyslog` и откройте его на редактирование:

   ```
   sudo nano /etc/rsyslog.d/30-unbound.conf
   ```

5. Настройте отправку сообщений в **Платформу Радар**:

   ```
   template (name="radar" type="string"
   string="<%PRI%>%TIMESTAMP:::date-rfc3339% %HOSTNAME% %syslogtag

   `$.suffix`

   msg:::sp-if-no-1st-sp%%msg%")
   :syslogtag, contains, "unbound" @@<IP-адрес агента сбора лог-коллектора>:port;radar
   ```

   Где:

   - `@@` - передача данных по протоколу **TCP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

6. Перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog
   ```

7. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Unbound-Unbound_DNS**.

4.9 Системы виртуализации

При работе по подключению систем виртуализации в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.9.1 KVM Hypervisor. Libvirt

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	KVM-Hypervisor
Номер (Порт)	2746
Вендор	RedHat
Тип	Hypervisor
Профиль сбора	«Модуль tcp_input» «Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Настройте службу `rsyslog`:
    - журнал Libvirt располагается в директории:

      `/var/log/libvirt/libvirtd.log`
    - настройте доступ к соответствующему файлу:

      `# chmod 644 /var/log/libvirt/libvirtd.log`
    - подготовьте конфигурационный файл для `rsyslog` и поместите его в директорию `/etc/rsyslog.d/`. Рекомендуется назвать файл в соответствии с системным шаблоном: `[00]-<name>.conf`, где `[00]` - приоритетный номер конфигурации в директории `rsyslog.d`, а `<name>` - имя источника. Чем меньше номер конфигурации, тем выше приоритет его обработки системой.

      `# sudo vi /etc/rsyslog.d/30-kvm.conf`
    - укажите в конфигурационном файле следующие настройки:

```
#KVM Log Forwarding Configuration

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

#KVM libvirt log

input(
type="imfile"
File="<Ваш путь к файлу с логами>"
Tag="kvm:"
```

```
Severity="info"
Facility="local3"
)

#Forward to remote server

local3.* @@<Ip-адрес агента сбора лог-коллектора>:<Порт>
```

Где:

- `imfile` - модуль, обрабатывающий журналы;
- `File` - полный путь к файлу журнала;
- `Tag` - тег, который будет использоваться для записей, полученных из указанного выше файла журнала;
- `Severity` - уровень критичности события (info, debug, warning, error);
- `Facility` - необходимый уровень facility, например local3;
- `local3.* @@<IP-адрес агента сбора лог-коллектора>:port` - используемый протокол (@@ - TCP, @ - UDP), IP-адрес агента сбора лог-коллектора и порт, по которому агент сбора лог-коллектора будет принимать события. Порт должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

2. Проверьте конфигурацию службы `rsyslog`:

```
# rsyslogd -N1
# rsyslogd: version 8.2310.0-1.fc38, config validation run (level 1), master
config /etc/rsyslog.conf
# rsyslogd: End of config validation run. Bye.
```

3. Для проверки конкретного файла конфигурации используйте следующие команды:

```
# rsyslogd -f /etc/rsyslog.d/30-kvm.conf -N1
# rsyslogd: version 8.2310.0-1.fc38, config validation run (level 1), master
config /etc/rsyslog.d/30-kvm.conf.conf
# rsyslogd: End of config validation run. Bye.
```

4. Перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog
```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **KVM- Hypervisor. Libvirt**.

4.9.2 Microsoft Windows HyperV

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-Windows-HyperV
Номер (Порт)	1517
Вендор	Microsoft

Характеристика	Значение
Тип	Hypervisor
Профиль сбора	«Модуль eventlog_input_local»

События от источника включены по умолчанию и записываются в следующие журналы Windows:

- **Microsoft-Windows-Hyper-V-VMMS-Admin**;
- **Microsoft-Windows-Hyper-V-VMMS-Operational**;
- **Microsoft-Windows-Hyper-V-Worker-Admin**.

Примечание: *Лог-коллектор должен быть установлен на том же сервере, где и Microsoft Windows HyperV.*

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Windows-HyperV**.

4.9.3 Proxmox

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Proxmox
Номер (Порт)	4400
Вендор	Proxmox
Тип	Hypervisor
Профиль сбора	«Модуль udp_input»

Журналирование событий **Proxmox** выполняется в системный журнал `syslog`. За журналирование отвечает демон `pvedaemon`.

Для настройки источника выполните следующие действия:

1. Создайте шаблон для службы `rsyslog` по пути `/etc/rsyslog.d/`. Например, `proxmox_to_pangeoradar.conf`:

   ```
   # sudo nano /etc/rsyslog.d/proxmox_to_pangeoradar.conf
   ```

2. Добавьте пустую строку в шаблон и сохраните изменения.
3. После создания шаблона, журналы событий в системе **Proxmox** перестанут сохраняться. При необходимости настройте дополнительное сохранение отправляемых журналов в **Proxmox**. Для этого в шаблоне укажите следующие настройки:

   ```
   if $programname == 'pvedaemon'
   ```

```
then
    /var/log/proxmox.log
    action(
        type="omfwd"
        target="<IP>"
        port="<PORT>"
        protocol="udp"
        action.resumeRetryCount="100"
        queue.type="linkedList"
        queue.size="10000"
    )
& stop
```

4. Перезапустите службу `rsyslog`.

   ```
   # systemctl restart rsyslog
   ```

5. При необходимости исключите ненужные журналы при отправке. Для этого в функции `$msg contains` добавьте отрицание `not` и укажите слово, характеризующее журнал, например:

   ```
   if ($programname == 'pvedaemon') and not ($msg contains 'worker') then @IP:PORT
   ```

   Где:

   - `worker` - будут отправлены все журналы, кроме тех, в которых встречается слово **worker**;
   - `IP`- IP-адрес агента сбора лог-коллектора;
   - `PORT` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
   - `@` - отправка журналов по протоколу **UDP**.

6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Proxmox**.

4.9.4 vGate

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	vGate
Номер (Порт)	2745
Вендор	Security-Code
Тип	Hypervisor
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в консоль управления системой.
2. Перейдите в раздел **Настройки → Аудит** и нажмите на ссылку **Настройки сбора сообщений**. Откроется окно "Настройка аудита события" (см. «Рис. 277»).

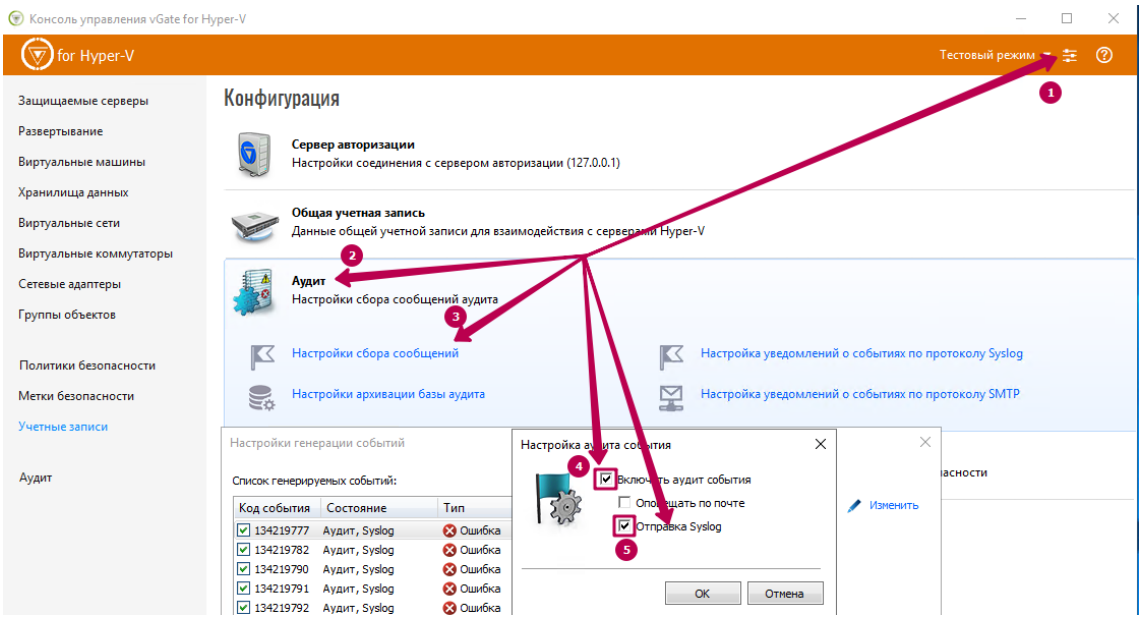


Рис. 277 – Настройка аудита события

3. В окне "Настройка аудита события" установите флаги **Включить аудит события** и **Отправка Syslog**.
4. Нажмите кнопку **OK**.
5. Отметьте уведомления, которые необходимо отправлять в **Платформу Радар**, установив соответствующие флаги (см. «Рис. 278»).

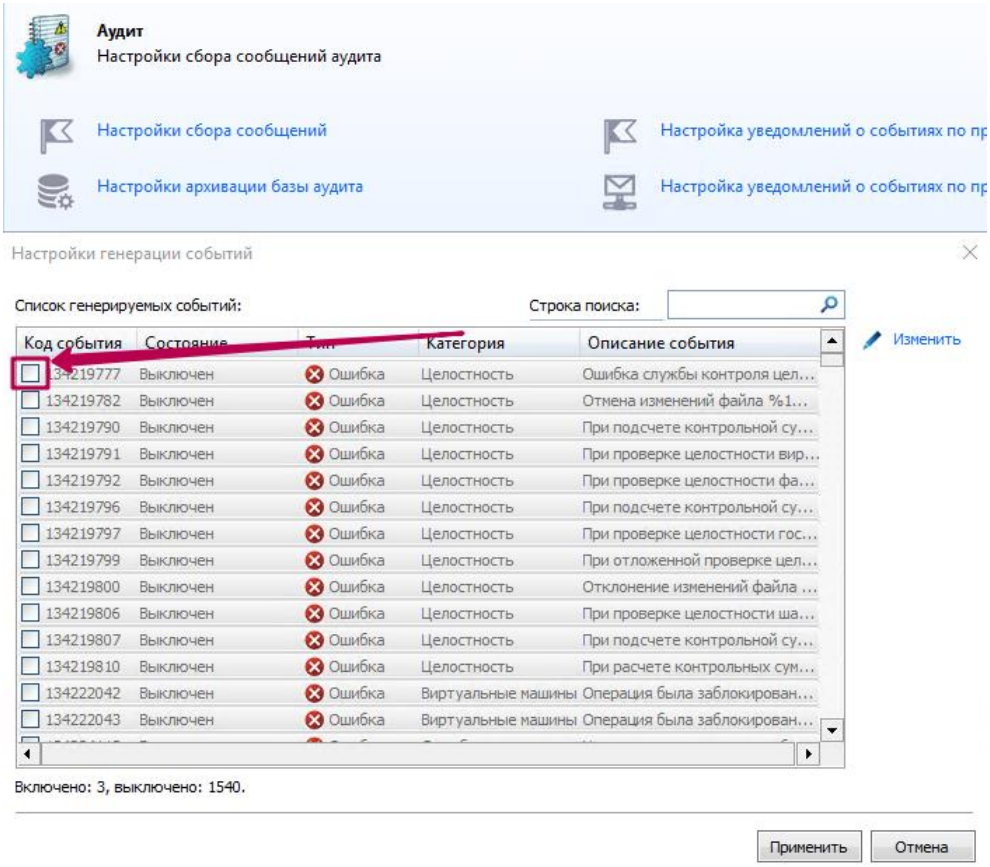


Рис. 278 – Выбор уведомлений для отправки

6. Нажмите кнопку **Применить**.
7. Нажмите на ссылку **Настройка уведомлений о событиях по протоколу Syslog**. Откроется окно "Настройка отправки сообщений Syslog" (см. «Рис. 279»).

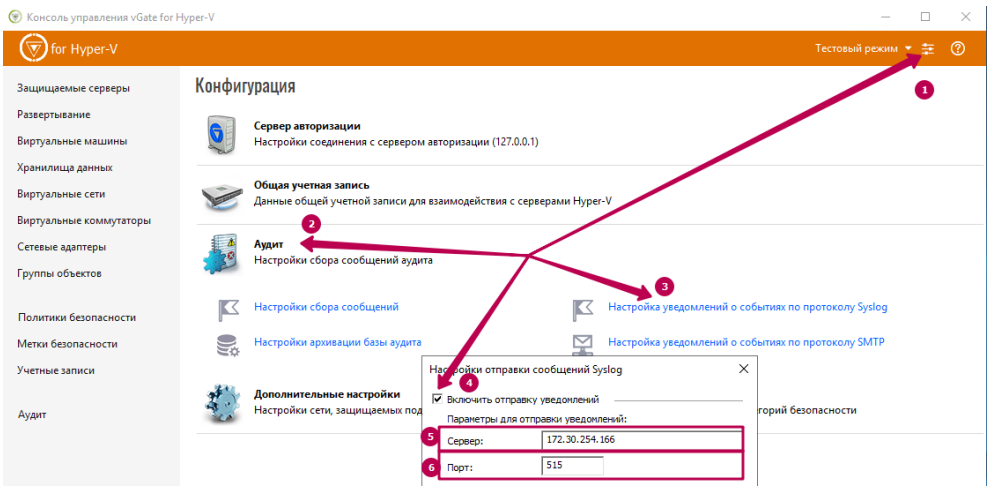


Рис. 279 – Окно "Настройка отправки сообщений Syslog"

8. В окне укажите следующие настройки:
   - включите отправку уведомлений установив соответствующий флаг;
   - в поле **Сервер** укажите IP-адрес агента сбора лог-коллектора;

- в поле **Порт** укажите порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора;
- нажмите кнопку **OK**.

9. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **vGate**.

4.9.5 VMware ESXi

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Vmware-ESXi
Номер (Порт)	2740
Вендор	Vmware
Тип	Hypervisor
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Войдите в интерфейс системы под учетной записью с правами администратора.
2. Перейдите в раздел **Manage → System → Advanced settings**.
3. Откройте на редактирование настройку **Syslog.global.logHost** (см. «Рис. 280»).

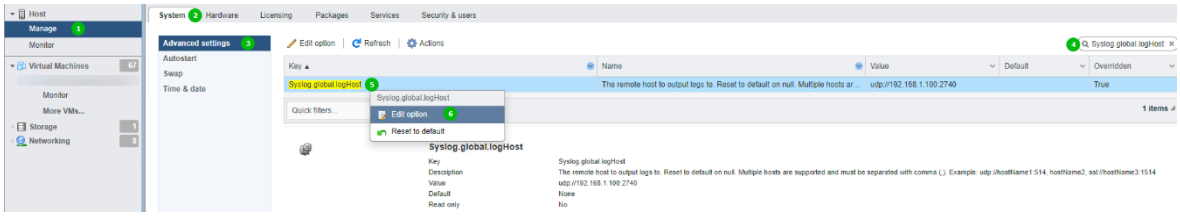


Рис. 280 – Настройка Syslog.global.logHost

4. В открывшемся окне (см. «Рис. 281») укажите IP-адрес агента сбора лог-коллектора и порт, указанный в настройках соответствующего профиля сбора.

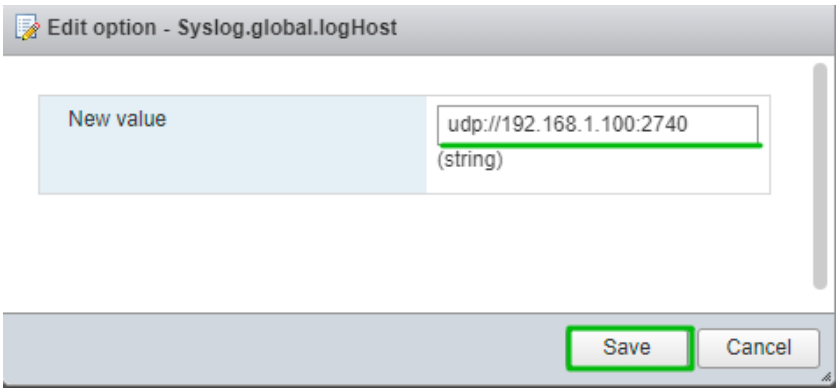


Рис. 281 – Настройка Syslog.global.logHost

5. Создайте правило службы `firewall` для **ESXi**:
   - перейдите в консоль **ESXi**;
   - сделайте резервную копию конфигурационного файла с правилами службы `firewall`:

     ```
     # cp /etc/vmware/firewall/service.xml /etc/vmware/firewall/service.xml.bak
     ```
   - выдайте разрешение на запись конфигурационного файла:

     ```
     # chmod 644 /etc/vmware/firewall/service.xml
     ```
   - установите `sticky bit flag`:

     ```
     # chmod +t /etc/vmware/firewall/service.xml
     ```
   - откройте на редактирование конфигурационный файл службы:

     ```
     # vi /etc/vmware/firewall/service.xml
     ```
   - перед последней строчкой файла укажите следующее правило:

     ```
     <service id='0045'>
         <id>CustomSyslog</id>
         <rule id='0000'>
           <direction>outbound</direction>
           <protocol>udp</protocol>
           <porttype>dst</porttype>
           <port>порт, указанный в профиле сбора</port>
         </rule>
         <enabled>true</enabled>
         <required>true</required>
     </service>
     ```
   - сохраните внесенные изменения;
   - верните права на запись конфигурационного файла в исходное состояние:

     ```
     # chmod 444 /etc/vmware/firewall/service.xml
     ```
   - обновите состояние службы `firewall`:

     ```
     # localcli network firewall refresh
     ```
   - проверьте состояние добавленного правила (см. «Рис. 282»).

Рис. 282 – Проверка состояния добавленного правила

6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Vmware-ESXi**.

4.10 Системы управления базами данных

При работе по подключению систем управления базами данных в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.10.1 Microsoft SQL Server. Event Log

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-SQL-Server
Номер (Порт)	1519
Вендор	Microsoft
Тип	SQLServer
Профиль сбора	«Модуль eventlog_input_local»

Примечание: *агент сбора лог-коллектора должен быть установлен на том же сервере, где и Microsoft SQL Server*.

Настройка источника включает в себя следующие шаги:

1. Включение аудита MS SQL Server.
2. Создание учетной записи Windows.
3. Предоставление пользователю прав доступа к журналу событий.
4. Настройка фильтрации профиля сбора.
5. Включение источника в платформе.

Шаг 1. Включение аудита MS SQL Server

1. Запустите Microsoft SQL Server Management Studio.
2. В окне подключения к базе данных укажите название экземпляра и введите учетные данные (см. «Рис. 283»).

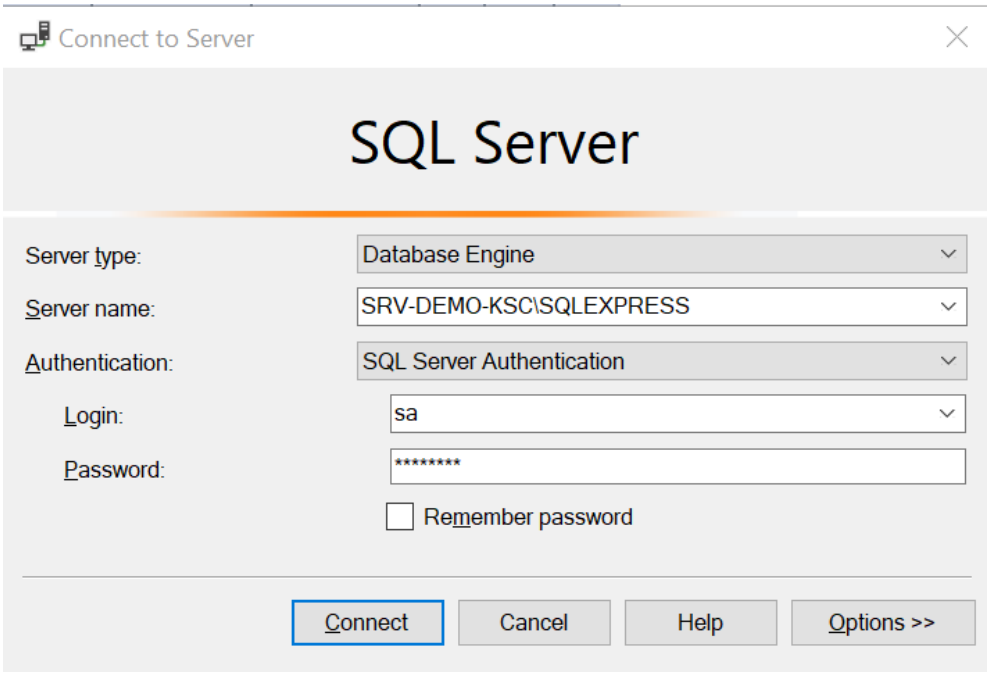


Рис. 283 – Подключение к базе данных

3. В разделе **Object explorer** перейдите во вкладку "Security" → "Audits". Вызовите контекстное меню и выберите опцию **New Audit...** (см. «Рис. 284»).

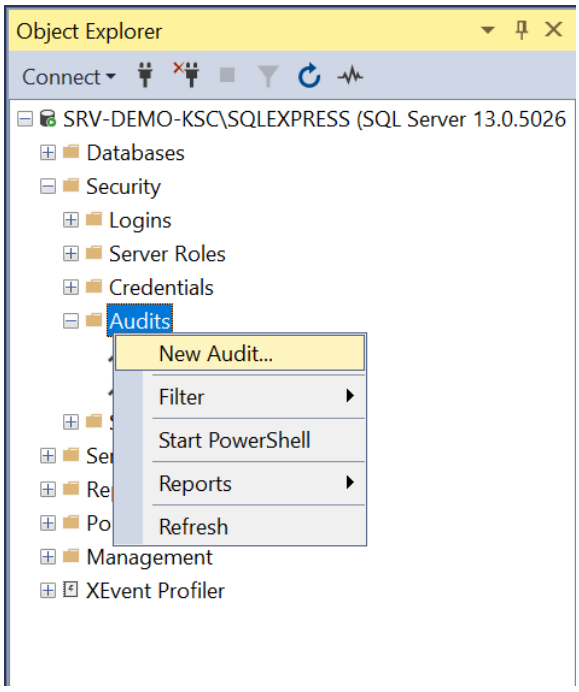


Рис. 284 – Создание аудита

4. В открывшейся вкладке "Create Audit", в поле **Audit name** укажите название аудита, в поле **Audit destination** выберите значение "*Application Log*" и нажмите кнопку **OK** (см. «Рис. 285»).

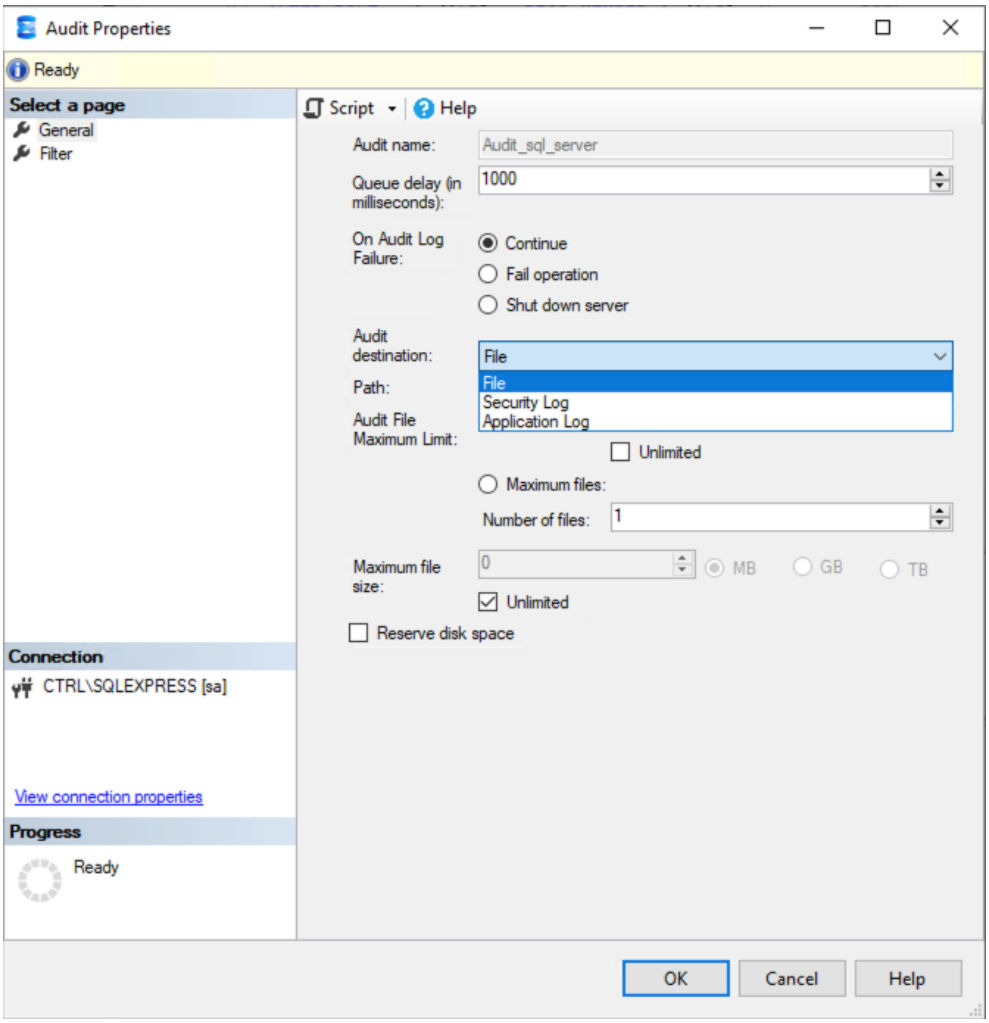


Рис. 285 – Настройка аудита

5. В разделе **Object explorer** перейдите во вкладку "Security" → "Server Audit Specification". Вызовите контекстное меню и опцию **New Server Audit Specification...** (см. «Рис. 286»).

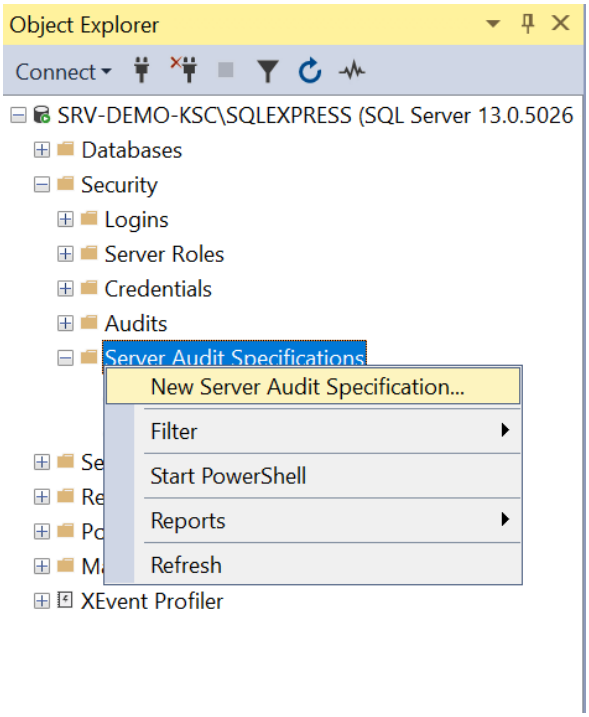


Рис. 286 – Создание спецификации аудита

6. В открывшейся вкладке "Create Server Audit Specification" (см. «Рис. 287») выполните следующие действия:
    - в поле **Name** укажите название спецификации аудита;
    - в поле **Audit** из выпадающего списка выберите ранее созданный аудит;
    - в поле **Actions** выберите типы событий для отслеживания,
    - нажмите кнопку **OK**.

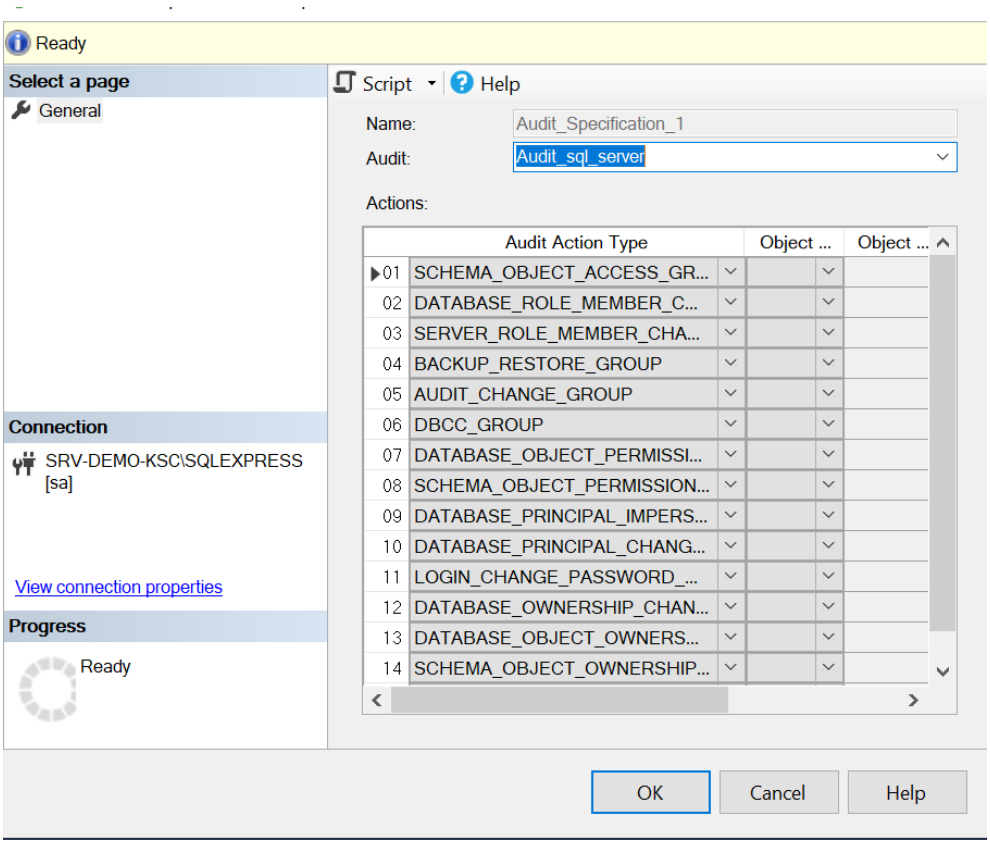


Рис. 287 – Настройка спецификации аудита

Шаг 2. Создание учетной записи Windows

1. В панели управления Windows откройте консоль **Computer Management (Управление компьютером)**.
2. В консоли откройте раздел **System Tools (Служебные программы) → Local Users and Groups (Локальные пользователи и группы) → Users (Пользователи)**, вызовите контекстное меню и выберите функцию **New User (Новый пользователь)** для создания нового пользователя (см. «Рис. 288»).

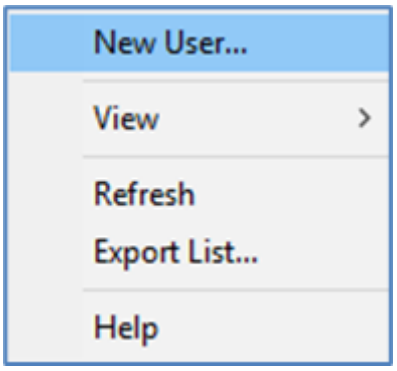


Рис. 288 – Создание пользователя

3. В открывшемся окне **New User (Новый пользователь)** (см. «Рис. 289») выполните следующие действия:
    - в поле **Name (Имя)** укажите имя нового пользователя;
    - в поле **Password (Пароль)** установите пароль и подтвердить его в поле **Confirm Password (Подтвердить)**;
    - при необходимости установите следующие флаги:
        - User cannot change password (Запретить смену пароля пользователем);
        - Password never expires (Срок действия пароля неограничен).
    - нажмите кнопку **Create**.

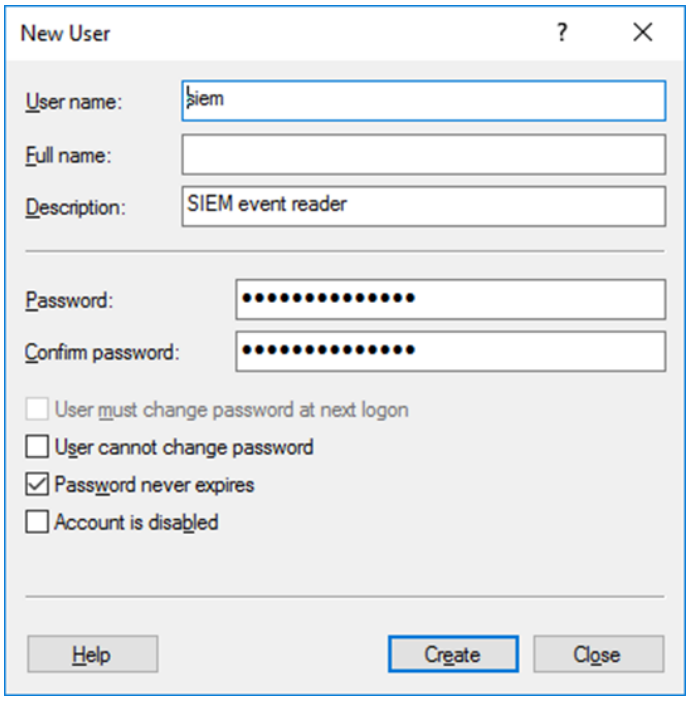


Рис. 289 – Настройка параметров пользователя

IШаг 3. Предоставление пользователю прав доступа к журналу событий

1. В консоли **Computer Management (Управление компьютером)** перейдите в раздел **System Tools (Служебные программы) → Local Users and Groups (Локальные пользователи и группы) → Groups (Группы)**.

2. Выберите в списке группу **Event Log Readers (Читатели журнала событий)**, вызовите контекстное меню и выберите пункт **Add To Group (Добавить в группу)**. Откроется окно "Event Log Readers Properties (Свойства: Читатели журнала событий)".
3. В окне выполните следующие действия:
   - нажмите кнопку **Add (Добавить)**;
   - в открывшемся окне "Select Users (Выбор: Пользователи)" выберите из списка ранее созданного пользователя и добавьте его в группу, нажав кнопку **OK**.
4. Нажмите кнопку **OK**.

Шаг 4. Настройка фильтрации профиля сбора.

1. Начните процесс настройки профиля сбора для источника **1519 Microsoft SQL Server** и выберите модуль mseven6_input.
2. При необходимости настройте фильтр для исключения лишних источников, которые находятся в журнале Application. Для этого в поле **Фильтр событий** укажите следующий фильтр:

```
<QueryList>  <Query  Id="0"  Path="Application">  <Select Path="Application">*[System[Provider[@Name='MSSQL$SQLEXPRESS'  or @Name='MSSQL$SQLEXPRESS$AUDIT']]]</Select>  </Query> </QueryList>
```

3. Пример настройки приведен на рисунке 8.

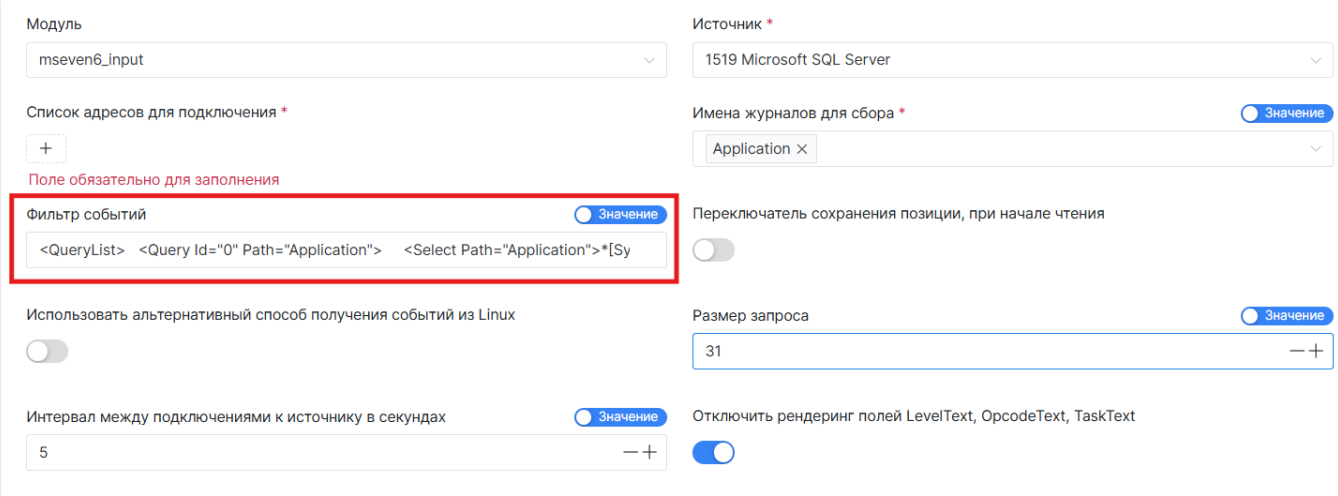


Рис. 290 – Настройка фильтра событий в профиле сбора

4. Сохраните изменения.

Шаг 5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-SQL-Server**.

4.10.2 Microsoft SQL Server. ODBC

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-SQL-Server

Характеристика	Значение
Номер (Порт)	1520
Вендор	Microsoft
Тип	SQLServer
Профиль сбора	«Модуль odbc_input»

Примечание: *агент сбора лог-коллектора должен быть установлен на том же сервере, где и Microsoft SQL Server*.

Настройка источника включает в себя следующие шаги:

1. Включение аудита MS SQL Server.
2. Установка ODBC драйвера.
3. Сетевые настройки сервера.
4. Конфигурация профиля сбора.
5. Включение источника в платформе.

Шаг 1. Включение аудита MS SQL Server

1. Запустите Microsoft SQL Server Management Studio.
2. В окне подключения к базе данных укажите название экземпляра и введите учетные данные (см. «Рис. 291»).

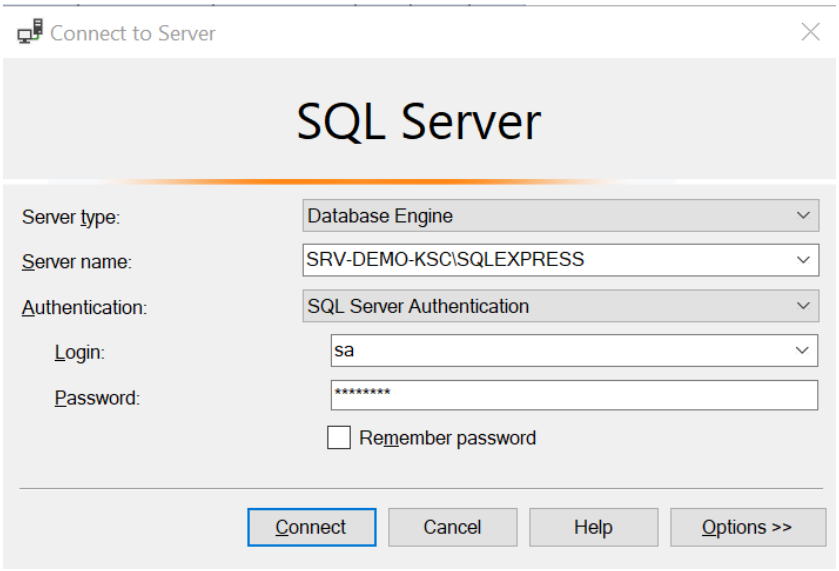


Рис. 291 – Подключение к базе данных

3. В разделе **Object explorer** перейдите во вкладку "Security" → "Audits". Вызовите контекстное меню и выберите опцию **New Audit...** (см. «Рис. 292»).

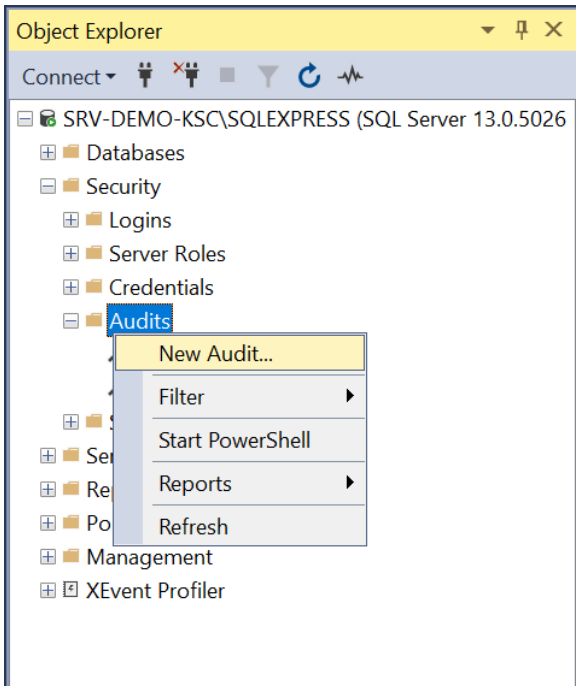


Рис. 292 – Создание аудита

4. В открывшейся вкладке "Create Audit", в поле **Audit name** укажите название аудита, в поле **Audit destination** выберите значение "*File*", в поле **Path** укажите путь к каталогу хранения файла журнала и нажмите кнопку **OK** (см. «Рис. 293»).

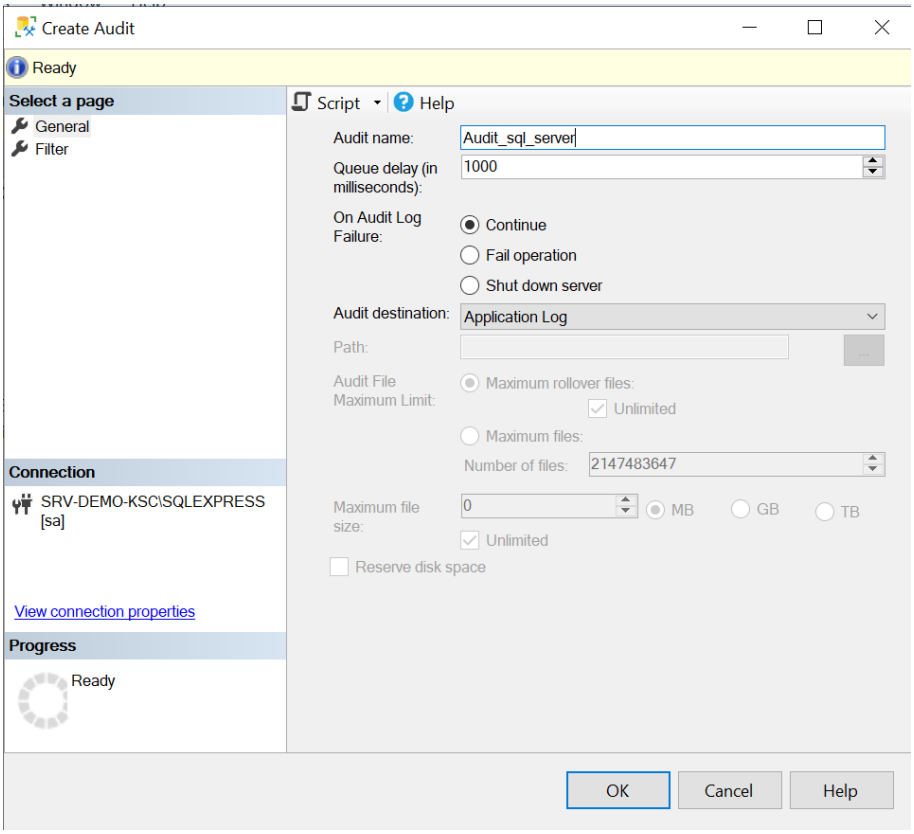


Рис. 293 – Настройка аудита

5. В разделе **Object explorer** перейдите во вкладку "Security" → "Server Audit Specification". Вызовите контекстное меню и опцию **New Server Audit Specification...** (см. «Рис. 294»).

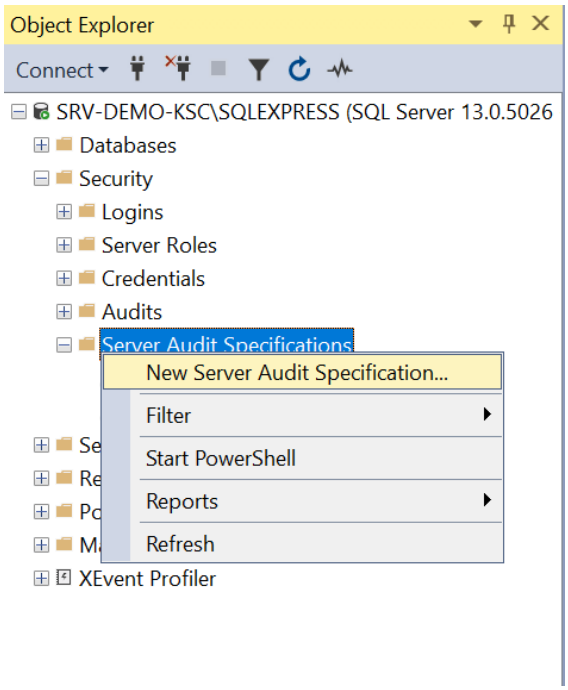


Рис. 294 – Создание спецификации аудита

6. В открывшейся вкладке "Create Server Audit Specification" (см. «Рис. 295») выполните следующие действия:
   - в поле **Name** укажите название спецификации аудита;
   - в поле **Audit** из выпадающего списка выберите ранее созданный аудит;
   - в поле **Actions** выберите типы событий для отслеживания;
   - нажмите кнопку **OK**.

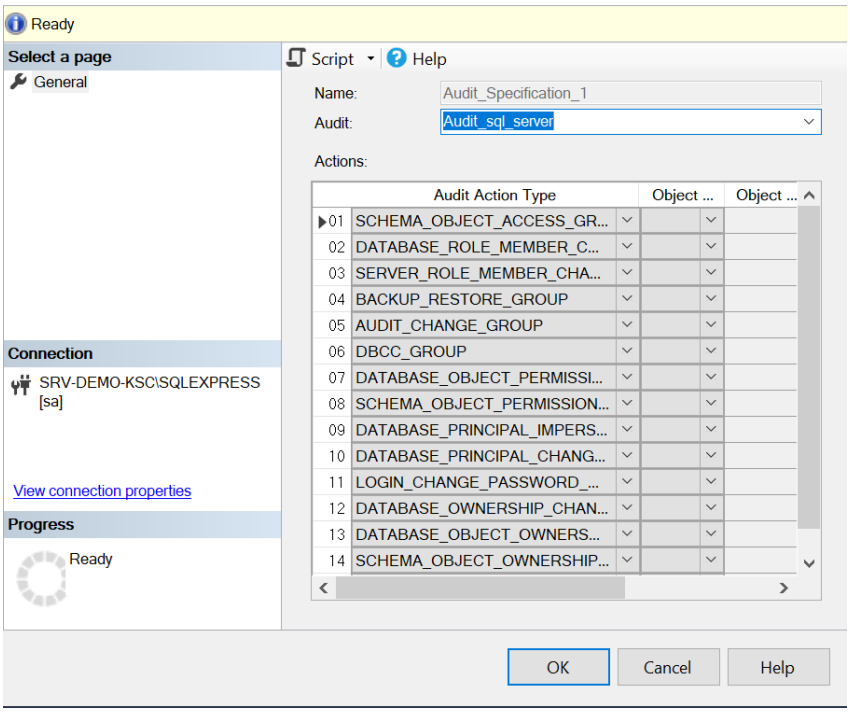


Рис. 295 – Настройка спецификации аудита

Шаг 2. Установка ODBC драйвера

1. С официального сайта скачайте ODBC Driver for SQL Server.
2. Установите скачанный драйвер на сервер с коллектором.
3. Узнайте точное название драйвера. Для этого запустите **Administrative Tools → ODBC Data Sources (64-bit)** (см. «Рис. 296») во вкладке Drivers (поле Name).

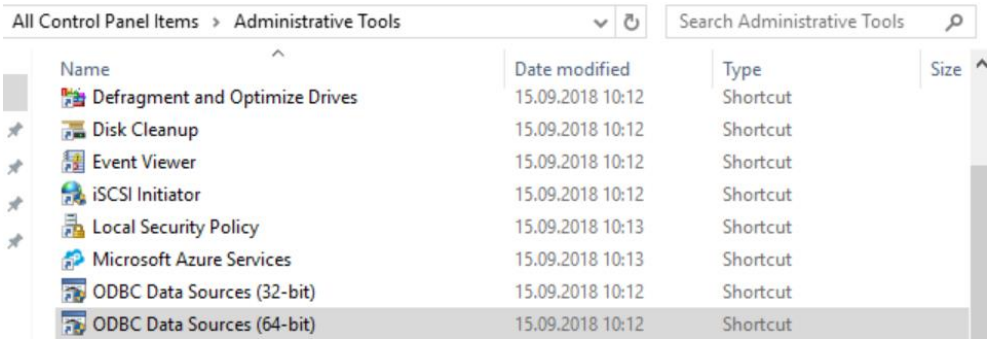


Рис. 296 – Раздел "Administrative Tools"

4. Откроется окно просмотра информации о драйвере. Необходимое значение отображается на вкладке "Drivers" в поле **Name** (см. «Рис. 297»).

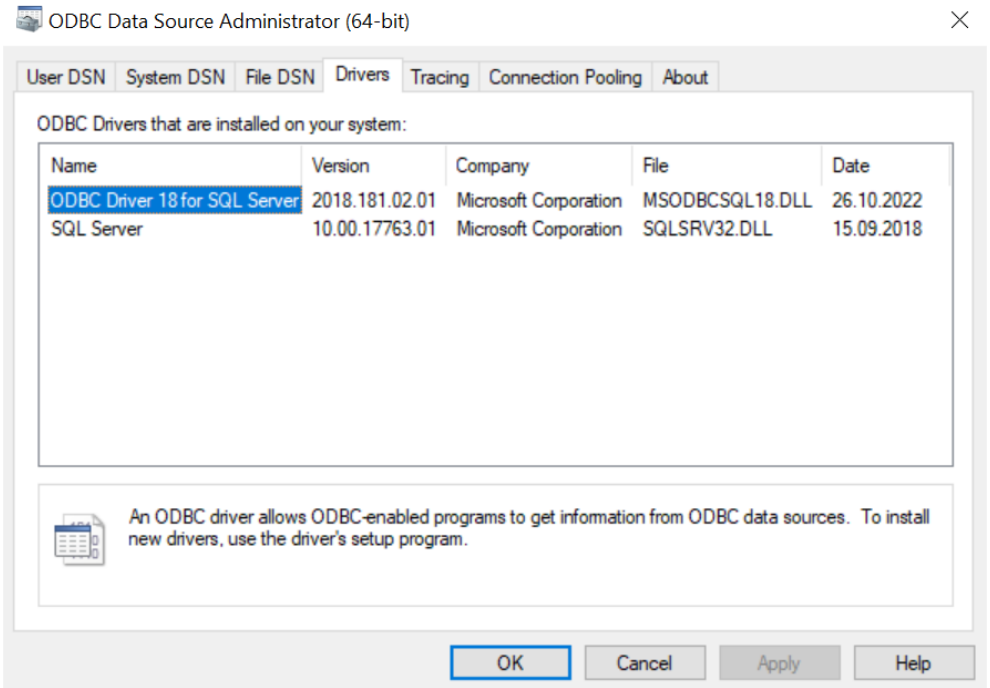


Рис. 297 – Просмотр информации о драйвере

Шаг 3. Сетевые настройки сервера

1. Откройте диспетчер конфигурации **SQL Server Configuration Manager**.
2. Выберите службу **SQL Server Network Configuration → Protocols for SQLEXPRESS** (см. «Рис. 298»).

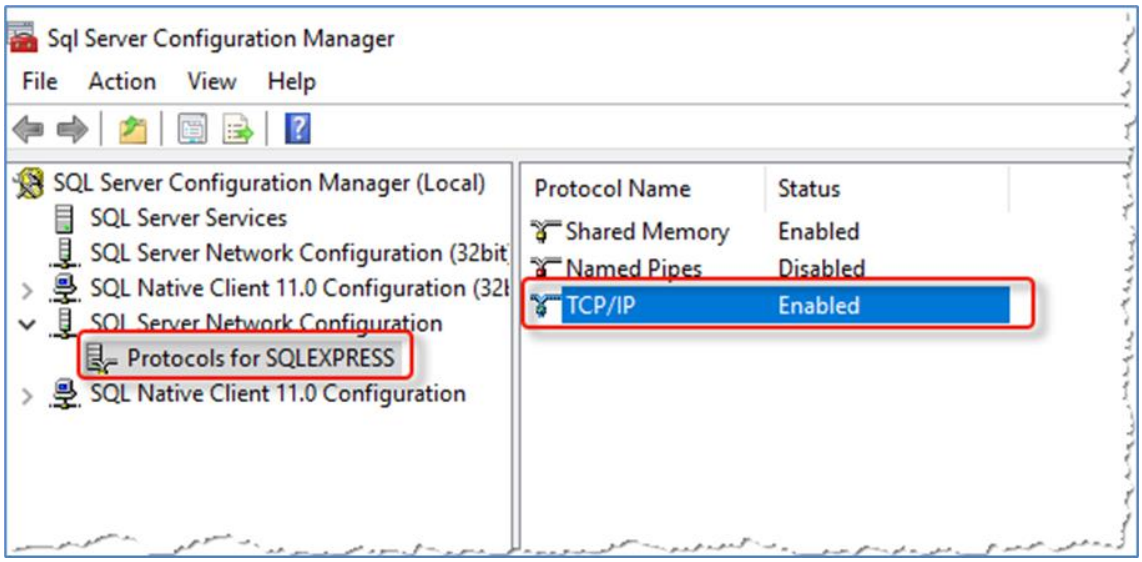


Рис. 298 -- Подключение по протоколу TCP/IP

3. В списке протоколов выберите протокол **TCP/IP**, вызовите контекстное меню и установите статус "*Enabled*" . Затем из контекстного меню выберите пункт **Properties**. Откроется окно "TCP/IP Properties" (см. «Рис. 299»).

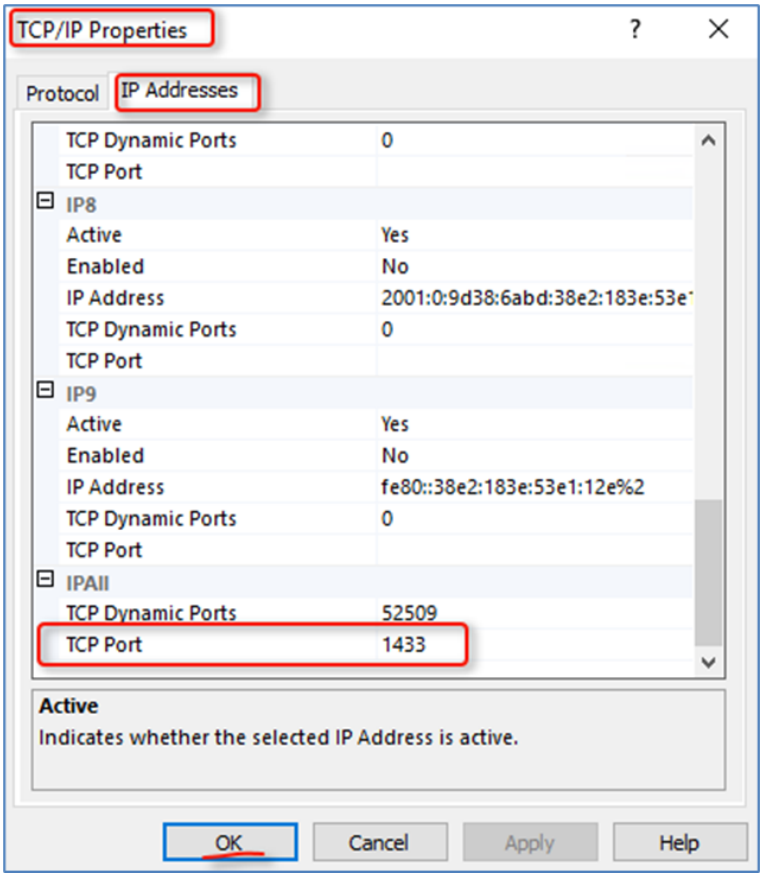


Рис. 299 -- Пример настройки протокола для удаленного доступа к БД

4. В открывшемся окне перейдите на вкладку **IP Adresses** и в блоке параметров **IPAll** укажите TCP порт для данного источника: "*1433*".
5. Нажмите кнопку **OK**.
6. Перезапустите службу **MS SQL Server**:

- запустите управление службами (см. «Рис. 300»);

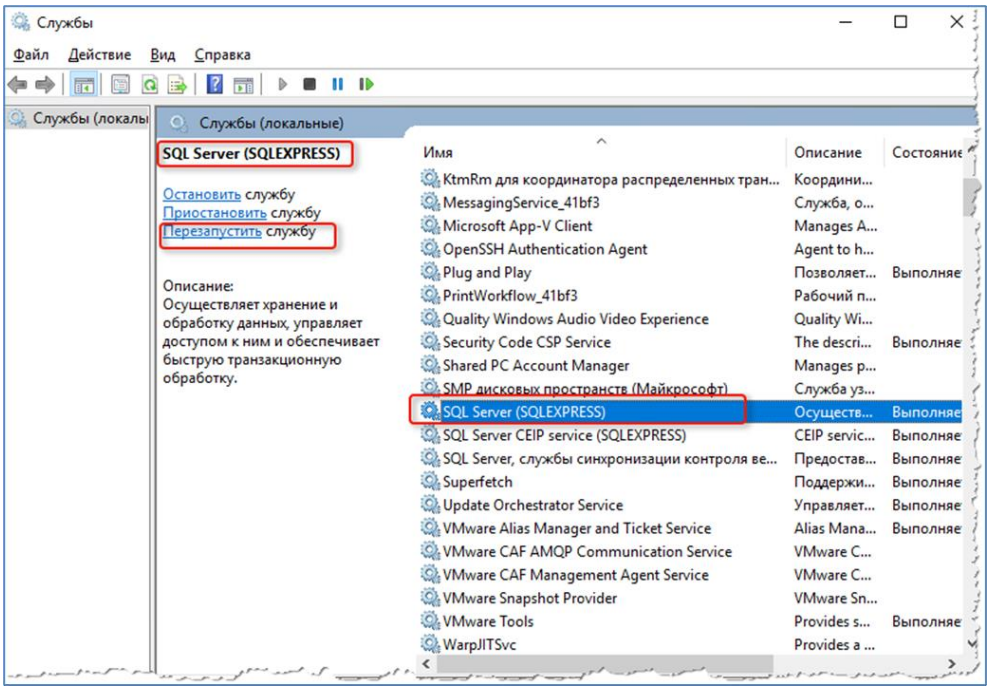


Рис. 300 -- Перезапуск службы MS SQL Server

- выберите службу **SQL Server** с запущенным экземпляром БД (SQLEXPRESS) и нажмите кнопку **Перезапустить службу**.

Шаг 4. Настройте профиль сбора для данного источника

Для настройки профиля сбора выполните следующие действия:

1. Начните процесс настройки профиля сбора для источника **1520 Microsoft SQL Server ODBC** и выберите «Модуль odbc_input» (см. «Рис. 301»):

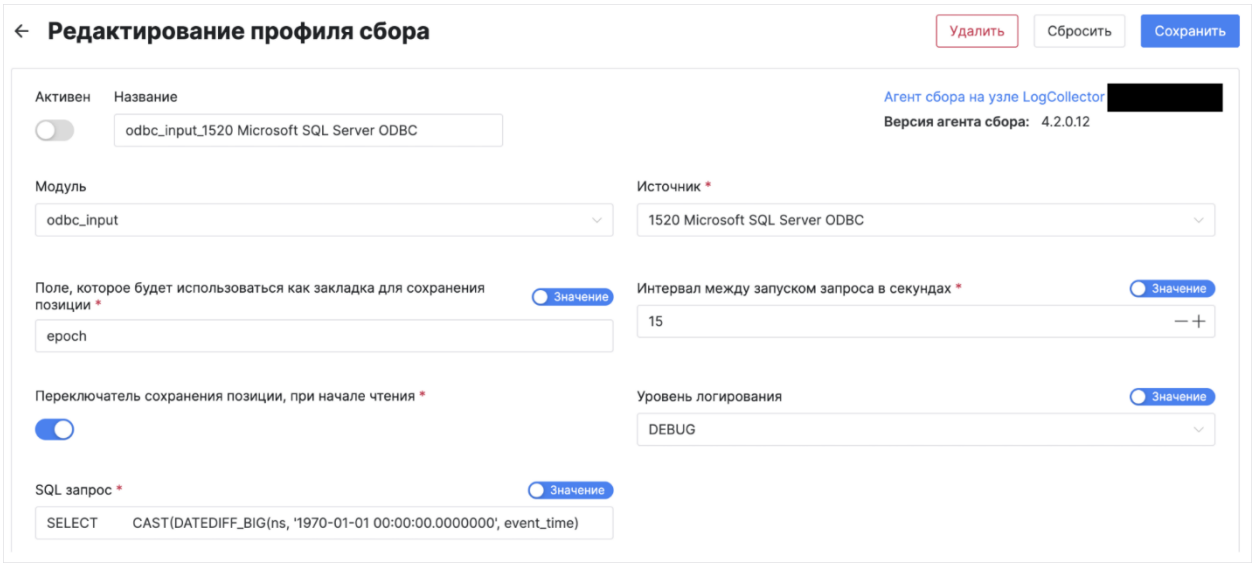


Рис. 301 -- Создание профиля сбора. Модуль "odbc_input"

2. В поле **SQL запрос** укажите запрос, которым будут запрашиваться события из системных журналов. Пример запроса:

```
sql: >
    SELECT
```

```
        CAST(DATEDIFF_BIG(ns, '1970-01-01 00:00:00.0000000', event_time) AS
BIGINT) as epoch,
        event_time,
        action_id,
        succeeded,
        session_id,
        class_type,
        session_server_principal_name,
        server_principal_name,
        server_principal_sid,
        database_principal_name,
        target_server_principal_name,
        target_server_principal_sid,
        target_database_principal_name,
        server_instance_name,
        database_name,
        schema_name,
        object_name,
        statement,
        additional_information,
        transaction_id
    FROM fn_get_audit_file ('C:\Program Files\Microsoft SQL
Server\MSSQL13.SQLEXPRESS\MSSQL\DATA\*.sqlaudit', default, default)
    WHERE CAST(DATEDIFF_BIG(ns, '1970-01-01 00:00:00.0000000', event_time) AS
BIGINT) > ?
```

Где (`'C:\Program Files\Microsoft SQL Server\MSSQL13.SQLEXPRESS\MSSQL\DATA\*.sqlaudit', default, default`) путь к файлам журнала. Указанные в строке данные, должны совпадать с путем фактического размещения файлов журналов.

3. В поле **Поле, которое будет использоваться как закладка для сохранения позиции** укажите значение *epoch*, оно используется для сохранения позиции вычитки между запросами.
4. В блоке **Данные для подключения** выполните следующие настройки:
   - в поле **Драйвер для подключения** выберите значение *MS SQL*;
   - остальные поля заполните соответствующими сетевыми и учетными данными для подключения.
5. Сохраните профиль сбора.

Шаг 5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-SQL-Server**.

4.10.3 Oracle Database. Audit

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Oracle-Database
Номер (Порт)	2770
Вендор	Oracle

Характеристика	Значение
Тип	Database
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Подключитесь к СУБД локально с привилегиями `sysdba`:

   ```
   # sqlplus / as sysdba
   ```

2. Выполните команду:

   ```
   # alter session set "_ORACLE_SCRIPT"=true
   ```

3. Установите журнал аудита XML:

   ```
   # ALTER SYSTEM SET audit_trail=XML SCOPE=SPFILE
   ```

4. Выключите и включите СУБД:

   ```
   # Shutdown
   # Startup
   ```

5. Проверьте параметры аудита командой:

   ```
   # show parameter audit
   ```

   Убедитесь, что `audit_trail` принял значение XML. Запишите значение `audit_file_dest`, оно понадобится при настройке отправки сообщений в профиле сбора для параметра **Файл (File)**.

6. Выполните команду:

   ```
   # ALTER SYSTEM SET audit_sys_operations=true SCOPE=SPFILE
   ```

7. Установите важность событий командой:

   ```
   # alter system set audit_syslog_level='local5.info' scope=spfile sid='*'
   ```

8. Выполните последовательно команды:

   ```
   # Shutdown
   # Startup
   # Show parameter audit
   ```

   На выходе должны появиться сообщения (см. «Рис. 302»).

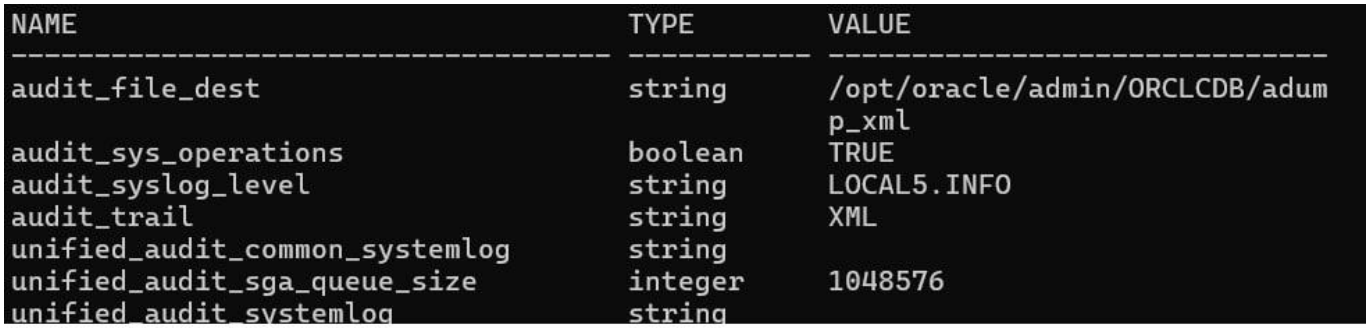


Рис. 302 – Вывод сообщений

9. Настройте параметры аудита:

```
AUDIT ALTER SYSTEM BY ACCESS;
AUDIT DELETE ON SYS.AUD$ BY ACCESS;
AUDIT DELETE ON SYS.FGA_LOG$ BY ACCESS;
AUDIT EXECUTE ON SYS.DBMS_FGA BY ACCESS;
AUDIT INSERT ON SYS.AUD$ BY ACCESS;
AUDIT INSERT ON SYS.FGA_LOG$ BY ACCESS;
AUDIT SELECT ON SYS.DBA_USERS BY ACCESS;
AUDIT SELECT ON SYS.LINK$ BY ACCESS;
AUDIT SELECT ON SYS.USER_DB_LINKS BY ACCESS;
AUDIT SELECT ON SYS.USER_HISTORY$ BY ACCESS;
AUDIT SYSTEM AUDIT BY ACCESS;
AUDIT TABLE BY ACCESS;
AUDIT UPDATE ON SYS.AUD$ BY ACCESS;
AUDIT UPDATE ON SYS.FGA_LOG$ BY ACCESS;
```

10. В каталоге `/etc/rsyslog.d/` создайте конфигурационный файл `oracle_audit.conf` и укажите в нем следующие настройки:

```
module(load="imfile")

input(
    type="imfile"
    File="<Значение из audit_file_dest из п.5>/*.xml"
    Tag="oracle_audit"
    Facility="local7"
    Severity="info"
    PersistStateInterval="100"
    endmsg.regex="</AuditRecord>$"
)

local7.*    /var/log/oracle_audit.log
local7.* @@<IP-адрес агента сбора лог-коллектора>:<порт>
```

Где:

- `local7` - необходимое значение facility;
- `@@` - передача данных по протоколу **TCP**;
- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес, на котором развернут агент сбора лог-коллектора;
- `<порт>` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

11. Сохраните изменения и перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog.service
```

12. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Oracle-Database**.

4.10.4 Oracle Database. NetListener

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Oracle-MySQL
Номер (Порт)	4005
Вендор	Oracle
Тип	MySQL
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Запустите **LSNRCTL** командой:

   ```
   # LSNRCTL
   ```

2. Определите экземпляр используемой службы **Oracle NetListener** командой:

   ```
   # show current_listener
   ```

   После выполнения команды отобразится имя экземпляра СУБД.

3. Для смены используемого экземпляра используется команда:

   ```
   # set current_listener
   ```

4. Проверьте статус журналирования:

   ```
   # show log_status
   ```

   Если для параметра log_status указано **OFF**, то включите журналирование:

   ```
   # set log_status on save_config reload
   ```

5. В каталоге `/etc/rsyslog.d/` создайте конфигурационный файл `oracle_netlistener.conf` и укажите в нем следующие настройки:

   ```
   module(load="imfile" mode="inotify") #PollingInterval="10") #mode="inotify")
   input(type="imfile"
   File="/<параметр File из п.4 >/log.xml"
   PersistStateInterval="100"
   Tag="oracle_netlistener:"
   Severity="info"
   Facility="local3"
   readMode="2"
   )local3.* @@<IP-адрес агента сбора лог-коллектора>:port
   ```

   Где:

   - `local3` - необходимое значение facility;
   - `@@` - передача данных по протоколу **TCP**;

- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

6. Сохраните изменения и перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

7. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Oracle-Database-NetListener**.

4.10.5 Oracle MySQL

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Oracle-MySQL
Номер (Порт)	4005
Вендор	Oracle
Тип	MySQL
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Установите модуль аудита MariaDB, последовательно выполнив команды:

   ```
   # wget http://mirror.mephi.ru/mariadb/mariadb-10.1.45/bintar-linux-
   x86_64/mariadb-10.1.45-linux-x86_64.tar.gz
   # sudo tar -xzf mariadb-10.5.5-linux-x86_64.tar.gz
   # sudo install mariadb-10.1.45-linux-x86_64/lib/plugin/server_audit.so
   /usr/lib/mysql/plugin
   # sudo install mariadb-10.5.5-linux-x86_64/lib/plugin/server_audit.so
   /usr/lib/mysql/plugin
   # Sudo mysql
   # INSTALL PLUGIN server_audit SONAME 'server_audit.so'
   # SHOW PLUGINS
   # Set Global server_audit_logging=on
   # EXIT
   ```

2. В конфигурационном файле `/etc/mysql/mysql.conf.d/mysqld.cnf` укажите следующие настройки:

   ```
   plugin-load=server_audit=server_audit.so
   server_audit_logging=on
   server_audit_events=connect,query,table,query_ddl,query_dml,query_dcl
   server_audit_output_type = SYSLOG
   server_audit_syslog_facility = LOG_SYSLOG
   server_audit_file_path = /var/log/mysql/audit.log
   ```

3. Перезапустите сервис MySQL:

   ```
   service mysql restart
   ```

4. В каталоге `/etc/rsyslog.d/` создайте конфигурационный файл 20-mysql.conf и укажите в нем следующие настройки:

   ```
   template (name="radar" type="string"
   string="<%PRI%>%TIMESTAMP:::date-rfc3339% %HOSTNAME%
   %syslogtag%%$.suffix%%msg:::sp-if-no-1st-sp%%msg%")
   :syslogtag, contains, "mysql" @@<IP-адрес агента сбора лог-
   коллектора>:port;radar
   ```

   Где:

   - `@@` - передача данных по протоколу **TCP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

5. Сохраните изменения и перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Oracle-MySQL**.

4.10.6 PostgreSQL

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	PostgreSQL
Номер (Порт)	4000
Вендор	PostgreSQL
Тип	PostgreSQL
Профиль сбора	«Модуль udp_input»

Для настройки источника выполните следующие действия:

1. Узнайте расположение конфигурационного файла `postgresql.conf` на сервере:

   ```
   # psql -U <username> -c 'SHOW config_file'
   ```

   Пример ответа:

   ```
   /var/app/data/postgresql.conf
   ```

2. В конфигурационный файл `postgresql.conf` укажите следующие настройки:

```
log_destination = 'syslog'
logging_collector = off
syslog_facility = 'LOCAL0'
syslog_ident = 'postgres'
syslog_sequence_numbers = on
syslog_split_messages = off
client_min_messages = log
log_min_messages = info
log_min_error_statement = info
log_checkpoints = off
log_connections = on
log_disconnections = on
log_duration = off
log_error_verbosity = default
log_hostname = on
log_line_prefix = 'pgmessage: %m %a %u %d %r %i %e '
log_statement = 'mod'
lc_messages = 'en_US.UTF-8'
```

3. Перезапустите службу `postgresql`.
4. В каталоге `/etc/rsyslog.d/` создайте конфигурационный файл `10-pgsql.conf` и укажите в нем следующие настройки:

   ```
   if $programname == 'postgres' then @<IP-адрес агента сбора лог-коллектора>:port
   ```

   Где:

   - `@` - передача данных по протоколу **UDP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.
5. Сохраните изменения и перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```
6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **PostgreSQL**.

4.11 WEB-серверы

При работе по подключению WEB-серверов в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.11.1 Apache HTTP Server

Характеристики источника в **Платформе Радар**:

Характеристика	Значение

Характеристика	Значение
Название	Apache-Http-Server
Номер (Порт)	2830
Вендор	Apache-Software-Foundation
Тип	Http-Server
Профиль сбора	«Модуль tcp_input»

Конфигурационный файл системы располагается по следующему пути:

- для систем на базе "Debian" -- `/etc/apache2/apache2.conf`;
- для систем на базе "RHEL" -- `/etc/httpd/conf/httpd.conf`.

Для настройки источника выполните следующие действия:

1. В конфигурационном файле системы укажите уровень журналирования:

   ```
   LogLevel info
   ```

2. Обновите сервис `apache`:

   ```
   # systemctl reload apache2.service
   ```

3. Проверьте состояние сервиса:

   ```
   # systemctl status apache2.service
   ```

4. В каталоге `/etc/rsyslog.d/` создайте конфигурационный файл `apache2.conf` и укажите в нем следующие настройки:

   ```
   # Apache2 logs
   input(type="imfile"
         File="/var/log/apache2/access.log"
         Tag="apache2-accesslog"
         Severity="warn"
         Facility="local2")

   input(type="imfile"
         File="/var/log/apache2/error.log"
         Tag="apache2-errorlog"
         Severity="warn"
         Facility="local3")

   local2,local3.*  @@<IP-адрес агента сбора лог-коллектора>:port
   ```

   Где:

   - `local2,local3` - значение facility для журналов *Access.log* и *Error.log*;
   - `@@` - передача данных по протоколу **TCP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;

- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

5. Сохраните изменения и перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

6. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Apache-Http-Server**.

4.11.2 Apache HTTP Server. Windows

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Apache-Http-Server
Номер (Порт)	2830
Вендор	Apache-Software-Foundation
Тип	Http-Server
Профиль сбора (сценарий 1)	«Модуль http_collector_input»
Профиль сбора (сценарий 2)	«Модуль smb_input»

Сбор событий может выполняться по следующим сценариям:

- сценарий 1 - агент сбора лог-коллектора развёрнут на том же хосте, где и сам DNS сервер;
- сценарий 2 - агент сбора лог-коллектора забирает события с DNS сервера по SMB.

Для настройки источника выполните следующие действия:

1. В конфигурационном файле системы <путь до каталога Apache>/conf/httpd.conf укажите следующие настройки:

   ```
   ErrorLog "logs/error.log"
   <IfModule log_config_module>
       LogFormat "%h %l %u %t \"%r\" %\>s %b \"%{Referer}i\" \"%{User-Agent}i\""
   combined
       LogFormat "%h %l %u %t \"%r\" %>s %b" common
   CustomLog "logs/access.log" common
   </IfModule>
   ```

2. В ОС Windows перезапустите службу `apache`.
3. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Apache-Http-Server**.

4.11.3 Apache Tomcat

Apache Tomcat - это служба, которая может использоваться в следующих сценариях:

- в качестве самостоятельного веб-сервера;
- в качестве контейнера сервлетов вместе с Glassfish, JBoss;
- в качестве сервера контента, вместе с Apache HTTP Server.

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Apache-Tomcat-Web-Server
Номер (Порт)	2911
Вендор	Apache-Software-Foundation
Тип	Web-Server
Профиль сбора	«Модуль tcp_input»

События от источника включены по умолчанию и записываются в следующие журналы:

- `catalina.out` и `catalina.$(date).log` - журнал контейнера сервлетов, основные события, произошедшие с ядром Tomcat;
- `localhost.$(date).log` - журнал событий локального экземпляра Tomcat, в который, как правило, сохраняются основные внутренние ошибки;
- `localhost_access_log.$(date).txt` - журнал запросов (access log), эквивалентный журналу службы httpd (параметры доступа определяются в файле `/opt/tomcat/conf/server.xml`);
- журналы `manager.$(date).log` и `host-manager.$(date).log` - журналы работы веб-приложений, функционирующих в составе Tomcat.

Для настройки источника выполните следующие действия:

1. В каталоге `/etc/rsyslog.d/` создайте конфигурационный файл `tomcat.conf` и укажите в нем следующие настройки:

```
# Apache Tomcat logs
input(type="imfile"
      File="/opt/tomcat/logs/localhost_access_log*.txt"
      Tag="catalina-access"
      Severity="info"
      Facility="local1")
input(type="imfile"
      File="/opt/tomcat/logs/catalina.out"
      Tag="catalina-out"
      Severity="info"
      Facility="local2")

local1,local2.*  @@<IP-адрес агента сбора лог-коллектора>:port
```

Где:

- `local1,local2` - значение facility для журналов *Access.log* и *Catalina.out*;
- `@@` - передача данных по протоколу **TCP**;
- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

Внимание! *В случае, если Tomcat запущен из-под выделенной учетной записи, необходимо предоставить соответствующие права на чтение для каталога с журналами. Также, в конфигурации Tomcat для файлов журналов должно быть задано корректное значение UMASK (0022).*

2. Откройте конфигурационный файл службы `rsyslog`:

   ```
   # nano /etc/rsyslog.conf
   ```

3. В конфигурационном файле `/etc/rsyslog.conf` укажите следующие настройки:

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

4. Перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Apache-Tomcat-Web-Server**.

4.11.4 Mantis Bug Tracker

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	MantisBT-System
Номер (Порт)	2962
Вендор	MantisBT Team
Тип	Bug Tracking System
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. В конфигурационном файле `Mantis /etc/apache2/sites-enabled/` укажите пути к файлам журналов:

   ```
   ErrorLog "/var/log/apache2/mantisbt-error_log"
   TransferLog "/var/log/apache2/mantisbt-access_log"
   ```

2. В каталоге `/etc/rsyslog.d/` создайте конфигурационный файл `70-mantis.conf` и укажите в нем следующие настройки:

```
module(load="imfile" PollingInterval="1")
input(type="imfile"
      File="/var/log/nginx/access.log"
      Tag="nginx-access"
      Severity="info"
      Facility="local0")
input(type="imfile"
      File="/var/log/nginx/error.log"
      Tag="nginx-error"
      Severity="warn"
      Facility="local1")
local0,local1.* @@<IP-адрес агента сбора лог-коллектора>:port
```

Где:

- `local0,local1` - значение facility для журналов *Access.log* и *Error.log*;
- `@@` - передача данных по протоколу **TCP**;
- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

3. Сохраните изменения и перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog.service
```

4. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **MantisBT-System**.

4.11.5 Microsoft Sharepoint

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Microsoft-Sharepoint
Номер (Порт)	1529
Вендор	Groupware
Тип	Sharepoint
Профиль сбора	«Модуль odbc_input»

Настройка источника включает в себя следующие шаги:

1. Настройка аудита в Microsoft Sharepoint.
2. Создание MSSQL пользователя с ограниченными правами.
3. Включение источника в платформе.
4. Тонкая настройка SQL-запроса для извлечения информации из всех сайтов системы.

Шаг 1. Настройка аудита в Microsoft Sharepoint

Включение аудита происходит для каждого сайта отдельно.

Для включения аудита сайта выполните следующие действия:

1. Войдите на сайт, аудит которого необходимо включить.
2. Откройте **Настройки сайта** и выберите пункт **Сведения о сайте** (см. «Рис. 303»).

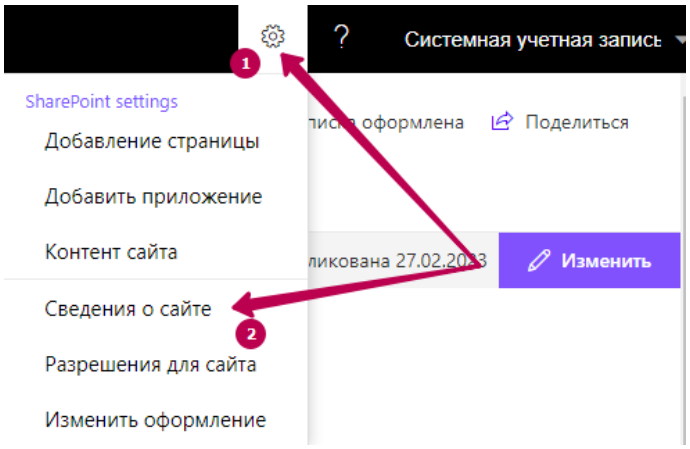


Рис. 303 – Microsoft Sharepoint. Настройки сайта

3. В открывшемся окне выберите пункт **Просмотреть все параметры сайта** (см. «Рис. 304»).

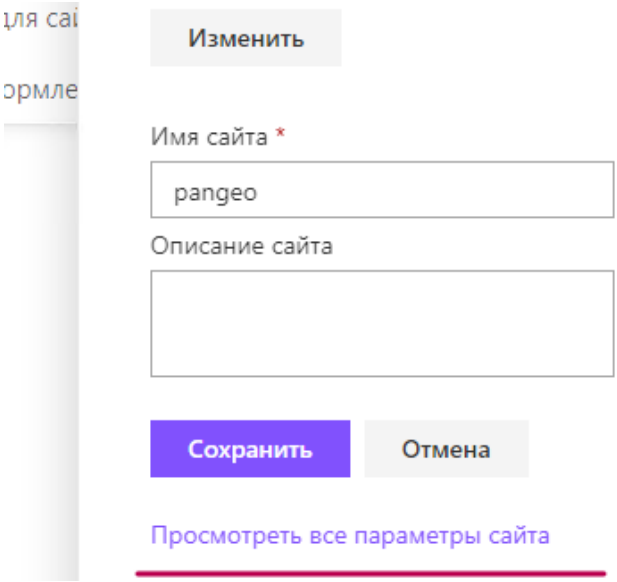


Рис. 304 – Microsoft Sharepoint. Просмотреть все параметры сайта

4. В открывшемся окне перейдите к блоку **Администрирование семейств сайтов** и выберите пункт **Возможности семейства сайтов** (см. «Рис. 305»).

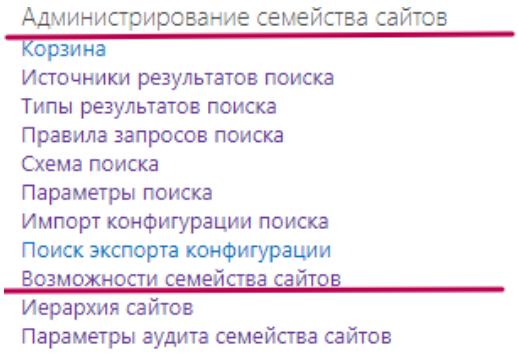


Рис. 305 – Администрирование семейств сайтов. Возможности семейства сайтов

5. Перейдите к блоку **Отчеты** и активируйте создание отчетов с анализом информации, содержащейся в Microsoft Sharepoint (см. «Рис. 306»).

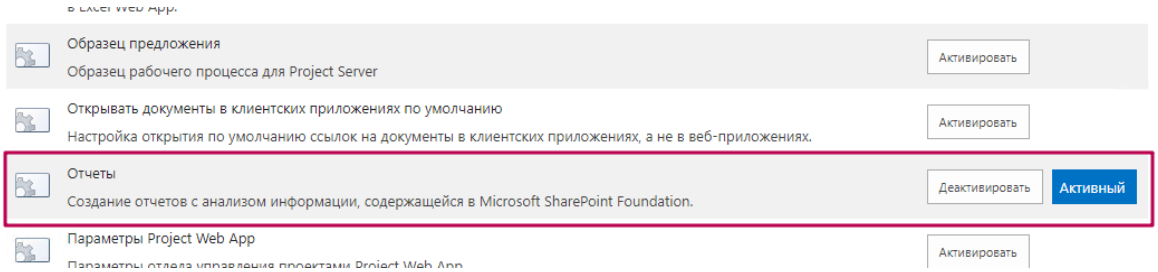


Рис. 306 – Microsoft Sharepoint. Активация создания отчетов

6. Вернитесь в **Администрирование семейств сайтов** и выберите пункт **Параметры аудита семейства сайтов** (см. «Рис. 307»).

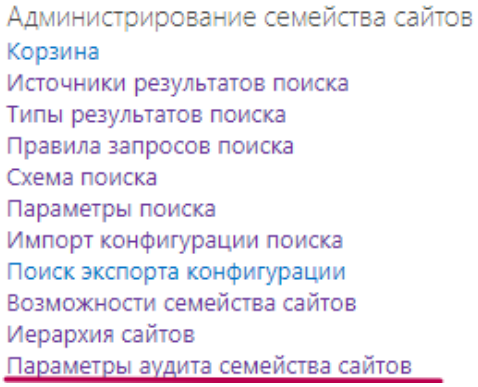


Рис. 307 – Администрирование семейств сайтов. Параметры аудита семейства сайтов

7. В открывшемся окне **Настройка параметров аудита** укажите события, подлежащие аудиту, установив соответствующие флаги и нажмите кнопку **ОК** (см. «Рис. 308»).

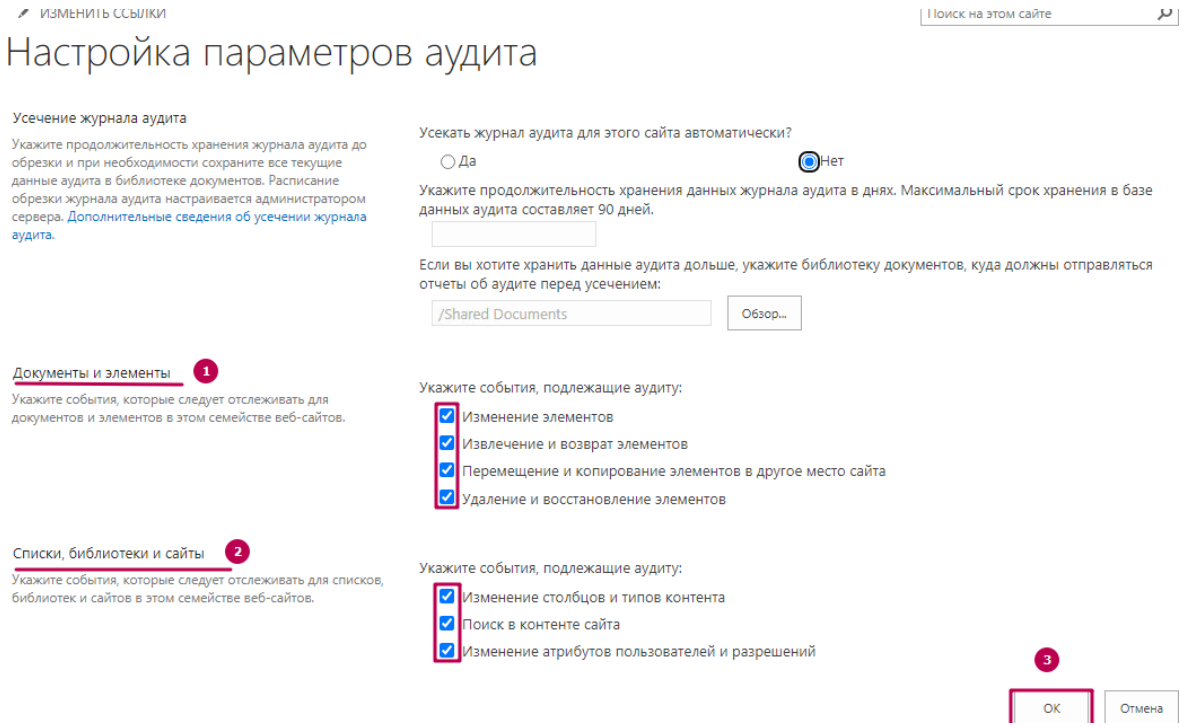


Рис. 308 – Окно "Настройка параметров аудита". Выбор событий, подлежащих аудиту

После этого в **Администрирование семейств сайтов** появится новый пункт **Отчеты по журналу аудита**, который позволяет вручную выгружать отчёты по нужным критериям (см. «Рис. 309»).

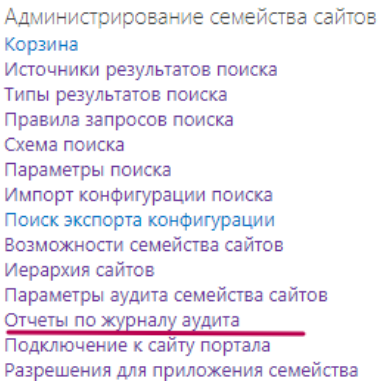


Рис. 309 – Администрирование семейств сайтов. Отчеты по журналу аудита

Шаг 2. Создание MSSQL пользователя с ограниченными правами

На данном шаге выполняется создание пользователя "*AuditReader*", который будет иметь права только на выполнение SQL-запроса в базе **WSS_Content**. Подробнее о SQL-запросе описано на четвертом шаге настройки источника.

1. Создаёте логин "*AuditReader*" и укажите пароль:

```
USE [master];
GO
CREATE LOGIN AuditReader WITH PASSWORD = 'Password';
```

2. Создайте пользователя **AuditReader** в базе **WSS_Content** и присвойте ему логин "*AuditReader*":

```
USE [WSS_Content];
GO
CREATE USER AuditReader FOR LOGIN AuditReader;
```

3. Выдайте пользователю **AuditReader** право выполнять только операцию SELECT в следующих таблицах:

```
USE [WSS_Content];
GO
GRANT SELECT ON dbo.AuditData TO AuditReader;
GRANT SELECT ON dbo.UserInfo TO AuditReader;
GRANT SELECT ON dbo.WebsPlus TO AuditReader;
```

4. Ограничьте доступ пользователя **AuditReader** к базе **WSS_Content**:

```
USE [master];
GO
DENY VIEW ANY DATABASE TO AuditReader;
GO
USE [WSS_Content];
GO
DENY VIEW DEFINITION TO AuditReader;
GO
```

Шаг 3. Настройка лог-коллектора и включение источника в платформе

Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Microsoft-Sharepoint**.

Шаг 4. Тонкая настройка SQL-запроса для извлечения информации из всех сайтов системы

SQL-запрос извлекает информацию о событиях аудита из таблицы **AuditData**, которая хранится в базе данных **WSS_Content**.

Пример запроса:

```
SELECT
    ad.Occurred AS [Date],
    u.tp_Title AS [User],
    u.tp_Login AS [UserLogin],
    ad.Event AS [EventID],
    ad.ItemType AS [ItemTypeID],
    ad.DocLocation AS [DocLocationID],
    ad.EventData AS [EventData],
    ad.MachineName,
    ad.MachineIP,
    wp.TitleResource AS [SiteName],
    ad.UserId AS [UserID],
    ad.SiteId AS [SiteId],
    ad.ItemId AS [ItemId],
CAST(DATEDIFF_BIG(ns, '1970-01-01 00:00:00.0000000', ad.Occurred) AS BIGINT) AS epoch
FROM
    [WSS_Content].[dbo].[AuditData] ad
LEFT JOIN
    [WSS_Content].[dbo].[UserInfo] u ON ad.UserId = u.tp_ID
LEFT JOIN
    [WSS_Content].[dbo].[WebsPlus] wp ON ad.SiteId = wp.SiteId
WHERE
CAST(DATEDIFF_BIG(ns, '1970-01-01 00:00:00.0000000', ad.Occurred) AS BIGINT) > ?
ORDER BY
    ad.Occurred DESC;
```

Где:

- `Occurred` - содержит дату и время, когда произошло событие аудита;
- `tp_Title` - содержит название пользователя, связанного с событием аудита;
- `tp_Login` - содержит логин пользователя, связанного с событием аудита;
- `Event` - содержит числовой идентификатор события аудита;
- `ItemType` - возвращает тип объекта, к которому относится событие аудита;
- `DocLocation` - показывает местоположение документа или объекта, которое было изменено или на которое было совершено действие;
- `EventData` - содержит дополнительные данные, связанные с событием, которое было зафиксировано;
- `MachineName` и `MachineIP` - показывают имя компьютера и IP-адрес, с которых было совершено действие;
- `UserID` - идентификатор пользователя, совершившего действие;

- `SiteId` - идентификатор сайта, на котором произошло событие;
- `ItemId` - идентификатор элемента, на котором было совершено действие.

За присоединение таблицы **WebsPlus** к таблице **AuditData** для получения имени сайта, связанного с событием, отвечает строка:

```
wp.TitleResource AS [SiteName],
```

Где, `SiteName` - имя сайта, на котором произошло событие.

За преобразование даты и времени возникновения события в формат `epoch`, значение которого будет использоваться в качестве уникального идентификатора события, по которому будет работать лог-коллектор, отвечает строка:

```
CAST(DATEDIFF_BIG(ns, '1970-01-01 00:00:00.0000000', ad.Occurred) AS BIGINT) AS epoch
```

За объединение таблиц **AuditData**, **UserInfo** и **WebsPlus** отвечают два оператора `LEFT JOIN`:

```
FROM
    [WSS_Content].[dbo].[AuditData] ad
LEFT JOIN
    [WSS_Content].[dbo].[UserInfo] u ON ad.UserId = u.tp_ID
LEFT JOIN
    [WSS_Content].[dbo].[WebsPlus] wp ON ad.SiteId = wp.SiteId
```

В первом операторе `LEFT JOIN` выполняется присоединение таблицы **UserInfo**, которая содержит информацию о пользователях SharePoint.

Во втором операторе `LEFT JOIN` выполняется присоединение таблицы **WebsPlus**, которая содержит информацию о сайтах SharePoint.

Оба оператора `LEFT JOIN` используются, чтобы сохранить все строки из таблицы **AuditData**, даже если нет соответствующих записей в таблицах **UserInfo** и **WebsPlus**. Если соответствующая запись не найдена, значения в столбцах, которые соответствуют отсутствующим записям, будут `NULL`.

Для корректной работы лог-коллектора необходимо добавить условие в запрос для выбора только тех строк, у которых разница между датой в столбце Occurred и датой "1970-01-01 00:00:00.0000000" больше, чем значение, которое будет заменено на место знака вопроса в момент выполнения запроса:

```
WHERE
CAST(DATEDIFF_BIG(ns, '1970-01-01 00:00:00.0000000', ad.Occurred) AS BIGINT) > ?
```

За сортировку событий от последнего к первому отвечает строка:

```
ORDER BY
    ad.Occurred DESC
```

4.11.6 Nginx

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Nginx-Web-server
Номер (Порт)	2960
Вендор	Nginx
Тип	Web-Server
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. В конфигурационных файлах `/etc/nginx/nginx.conf` и `/opt/pangeoradar/configs/nginx.conf` в блоке `# Logging Setting` укажите пути для регистрации событий *Access.log* и *Error.log*:

   ```
   ##
   # Logging Settings
   ##
          access_log /var/log/nginx/access.log;
          error_log /var/log/nginx/error.log;
   ```

2. В конфигурационном файле `/etc/rsyslog.conf` добавьте следующее значение:

   ```
   # Include all config files in /etc/rsyslog.d/
         $IncludeConfig /etc/rsyslog.d/*.conf
   ```

3. Создайте файл `/etc/rsyslog.d/nginx.conf` и укажите в нем следующие настройки:

   ```
   input(type="imfile"
         File="/var/log/nginx/access.log"
         Tag="nginx-access"
         Severity="info"
         Facility="local0")
   input(type="imfile"
         File="/var/log/nginx/error.log"
         Tag="nginx-error"
         Severity="warn"
         Facility="local1")
   local0,local1.* @@<IP-адрес агента сбора лог-коллектора>:port
   ```

   Где:

   - `local0,local1` - значение facility для журналов *Access.log* и *Error.log*;
   - `@@` - передача данных по протоколу **TCP**;
   - `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
   - `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

4. Сохраните изменения и перезапустите службу `rsyslog`:

   ```
   # systemctl restart rsyslog.service
   ```

5. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Nginx-Web-server**.

4.12 Системы контроля привилегированного доступа

При работе по подключению систем контроля привилегированного доступа в качестве источника событий в **Платформу Радар** вам может пригодиться следующая справочная информация:

- «Источники»;
- «Настройка лог-коллектора».

4.12.1 Solar Dozor

Характеристики источника в **Платформе Радар**:

Характеристика	**Значение**
Название	Solar-Dozor
Номер (Порт)	2593
Вендор	Rostelecom-Solar
Тип	DLP
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Для включения записи журналов войдите в веб-интерфейс системы Solar-Dozor и перейдите в раздел **Система → Конфигурация → Расширенные настройки → Интерфейс → Вебсервер (webserver.conf)**.
2. Установите флаг **Запись журналов действий в syslog в формате CEF** (см. «Рис. 310»).

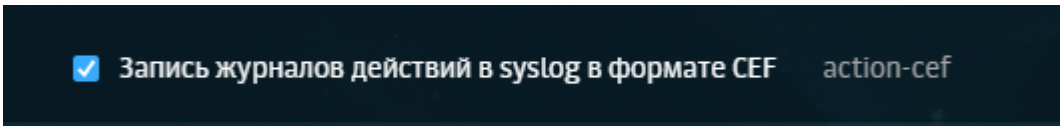


Рис. 310 – Включение записи в журналы

3. Сохраните и примените настройки. Будет включена запись действий пользователей в веб-интерфейсе системы в системный журнал /var/log/messages в формате CEF.
4. В конфигурационном файле /etc/rsyslog.conf, мастер-сервера DLP-системы, укажите следующие настройки:

```
$ActionQueueFileName SIEMForwarder
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
```

```
$ActionResumeRetryCount -1
if $msg contains 'CEF' then @@<IP-адрес агента сбора лог-коллектора>:port
```

Где:

- `@@` - передача данных по протоколу **TCP**;
- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

5. Для включения регистрации событий войдите в веб-интерфейсе системы Solar-Dozor перейдите в раздел **Система → Конфигурация → Расширенные настройки → События и инциденты → Сервис хранения и индексации событий и инцидентов (settings.json))** (см. «Рис. 311»).

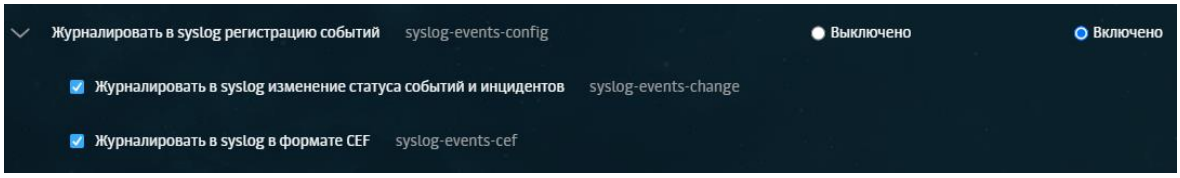


Рис. 311 – Включение регистрации событий

6. Укажите в разделе следующие настройки:
   - включите журналирование в syslog регистрацию событий (syslog-events-config);
   - установите флаг **Журналировать в syslog изменение статуса событий и инцидентов (syslog-events-change)**;
   - установите флаг **Журналировать в syslog в формате CEF (syslog-events-cef)**;
   - сохраните и примените настройки.
7. Для включения журналирования действий над сообщениями в веб-интерфейсе системы Solar-Dozor перейдите в раздел **Система → Конфигурация → Расширенные настройки → Обработка сообщений → Сервис фильтрации сообщений (mailfilter.edn)** (см. «Рис. 312»).

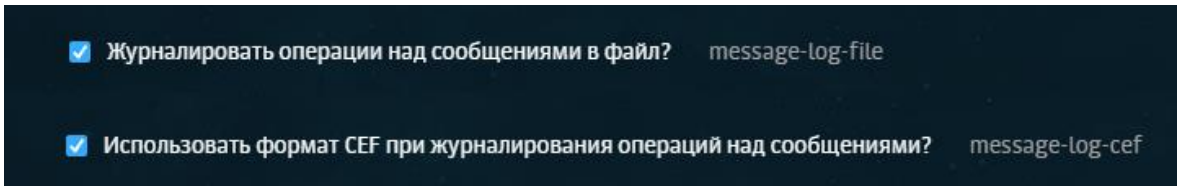


Рис. 312 – Включение журналирования над сообщениями

8. Укажите в разделе следующие настройки:
   - установите флаг **Журналировать операции над сообщениями в файл (message-log-file)**;
   - установите флаг **Использовать формат CEF при журналировании операций над сообщениями**;
   - сохраните и примените настройки.

9. В случае активации данных настроек на всех узлах с ролью “Фильтр почтового потока” (mailfilter) будет создан файл, содержащий записи действий над сообщениями - `/opt/dozor/var/log/message-stat.log`.
10. Для отправки журналов в **Платформу Радар** в каталоге `/etc/rsyslog.d/` создайте конфигурационный файл `04-send_dozor_mail.conf` и укажите в нем следующие настройки:

```
module(load="imfile" PollingInterval="10")
input(type="imfile"
      reopenOnTruncate="on"
      File="/opt/dozor/var/log/message-stat.log"
      Tag="solar-dozor-mail"
      )
$template rawSmap,"<%PRI%>%TIMESTAMP% %HOSTNAME% %syslogtag%%msg%\n"
if $msg contains 'CEF' then @@<IP-адрес агента сбора лог-
коллектора>:port;rawSmap
```

Где:

- `@@` - передача данных по протоколу **TCP**;
- `<IP-адрес агента сбора лог-коллектора>` - IP-адрес агента сбора лог-коллектора;
- `port` - порт, по которому агент сбора лог-коллектора будет принимать события. Должен совпадать со значением, указанным в настройках соответствующего профиля сбора.

11. Сохраните изменения и перезапустите службу `rsyslog`:

```
# systemctl restart rsyslog.service
```

12. На всех узлах системы Solar Dozor с ролью “Фильтр почтового потока” настройте ротацию журнала действий над сообщениями. Для этого создайте файл `/etc/logrotate.d/smap-maillog` со следующим содержимым:

```
/opt/dozor/var/log/message-stat.log {
    weekly
    rotate 4
    missingok
    notifempty
    nomail
    compress
    create 0644 dozor dozor
    minsize 50M
}
```

Выполните проверку условия logrotate с помощью команды:

```
# logrotate -df /etc/logrotate.d/smap-maillog
```

Запуск ротации вручную выполняется следующей командой:

```
# logrotate -f /etc/logrotate.d/smap-maillog
```

13. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Solar-Dozor**.

4.12.2 Staffcop Enterprise

Характеристики источника в **Платформе Радар**:

Характеристика	Значение
Название	Staffcop-Enterprise
Номер (Порт)	2512
Вендор	Atom_security
Тип	DLP
Профиль сбора	«Модуль tcp_input»

Для настройки источника выполните следующие действия:

1. Войдите в веб-интерфейс системы Staffcop-Enterprise и перейдите в раздел **Фильтры → Политики → Системные политики** (см. «Рис. 313»).

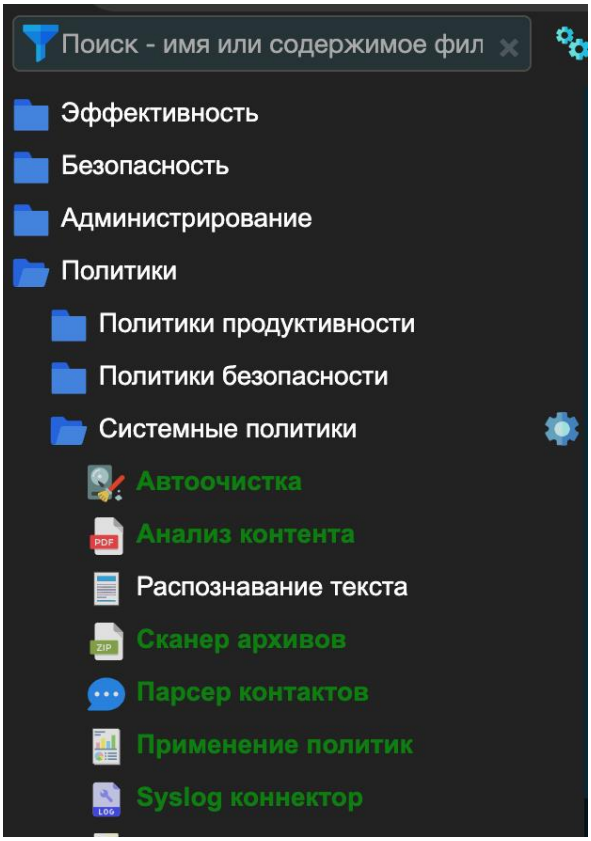


Рис. 313 – Системные политики

2. Выберите политику **Syslog-коннектор** и откройте ее на редактирование.
3. Перейдите на вкладку "Фильтр" и задайте необходимые параметры для событий (см. «Рис. 314»).

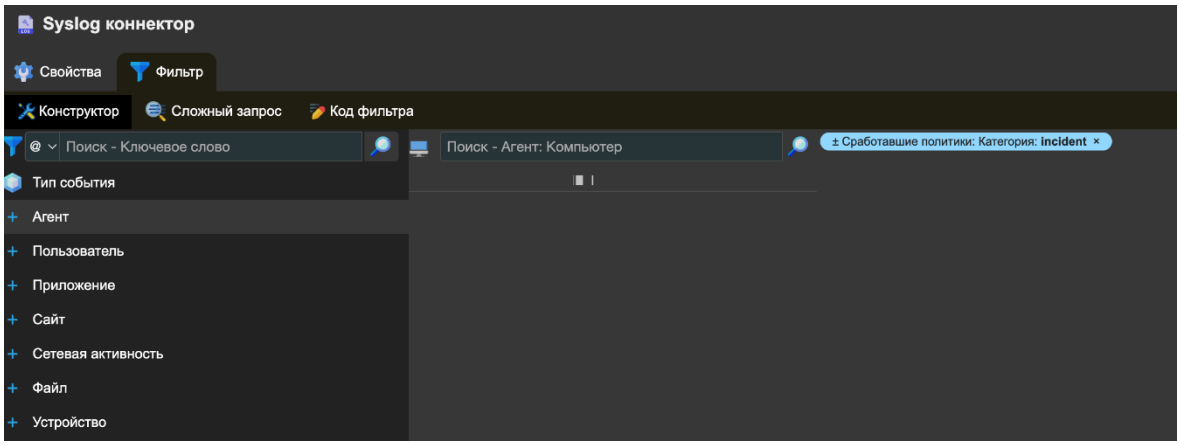


Рис. 314 – Параметры для событий

4. Перейдите на вкладку "Свойства" и установите флаги **Политика активна**, **Формат логов: CEF**.
5. Примените настройку только к новым или ко всем предыдущим событиям и сохраните изменения (см. «Рис. 315»).

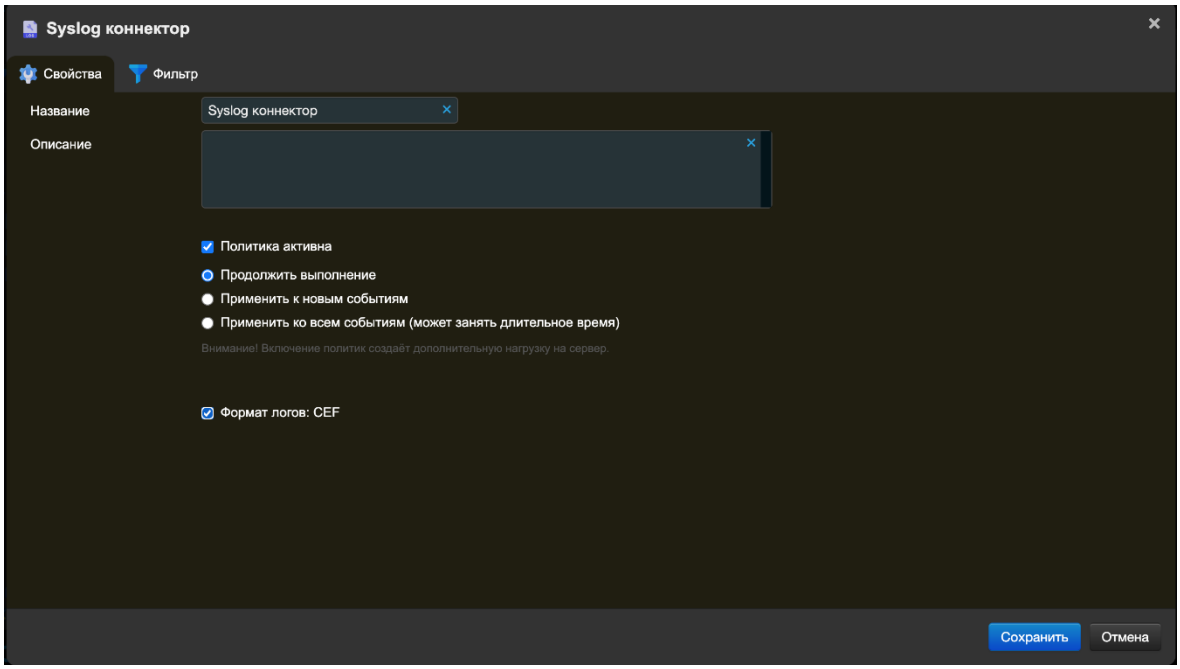


Рис. 315 – Сохранение изменений.

6. Выбранные события раз в 5 минут будут помещаться в журнал `/var/log/syslog`.
7. Перейдите на сервер системы **StaffCop** и выполните следующие настройки:
   - проверьте наличие и активность службы `rsyslog`:

     ```
     # service rsyslog status
     ```

   - по умолчанию служба должна быть установлена и запущена (см. «Рис. 316»);

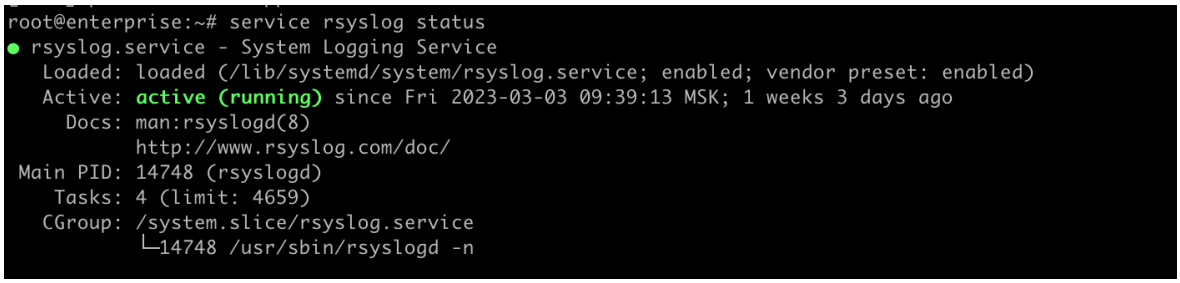


Рис. 316 – Состояние службы rsyslog

- создайте и откройте для редактирования конфигурационный файл `50-siem.conf`

  ```
  # nano /etc/rsyslog.d/50-siem.conf
  ```

- укажите в файле протокол передачи данных **TCP** (@@), IP-адрес агента сбора лог-коллектора и порт (должен совпадать со значением, указанным в настройках соответствующего профиля сбора), по которому агент сбора лог-коллектора будет принимать события от данного источника:

  ```
  If $programname==’staffcop’ then @@<IP-адрес агента сбора лог-коллектора>:port
  ```

- сохраните изменения и перезапустите службу `rsyslog`:

  ```
  # systemctl restart rsyslog.service
  ```

8. Перейдите в веб-интерфейс платформы и выполните действие «Включение источника» для источника **Staffcop-Enterprise**.