Платформа Радар

Руководство администратора

Версия 3.5.4

ООО Пангео Радар

Оглавление

1. Интерфейс администратора

По умолчанию интерфейс пользователя доступен по URL http://<адрес сервера>.

Процедура входа и общее описание интерфейса подробно описано в «Руководстве оператора».

При наличии дополнительных прав пользователю доступен раздел «Администрирование», который содержит следующий пункты (см. рисунок 1):

- **Пользователи и права** - управление пользователями;
- **Кластер** - управление Платформой;
- **Источники** - управление подключением источников событий;
- **Мониторинг** - просмотр метрик работоспособности компонентов Платформы;
- **Репутационные списки** - управление списками индикаторов компрометации;
- **База знаний** - управление базой знаний по типам инцидентов и правилам корреляции.
- **Лицензия** - управление параметрами лицензии.

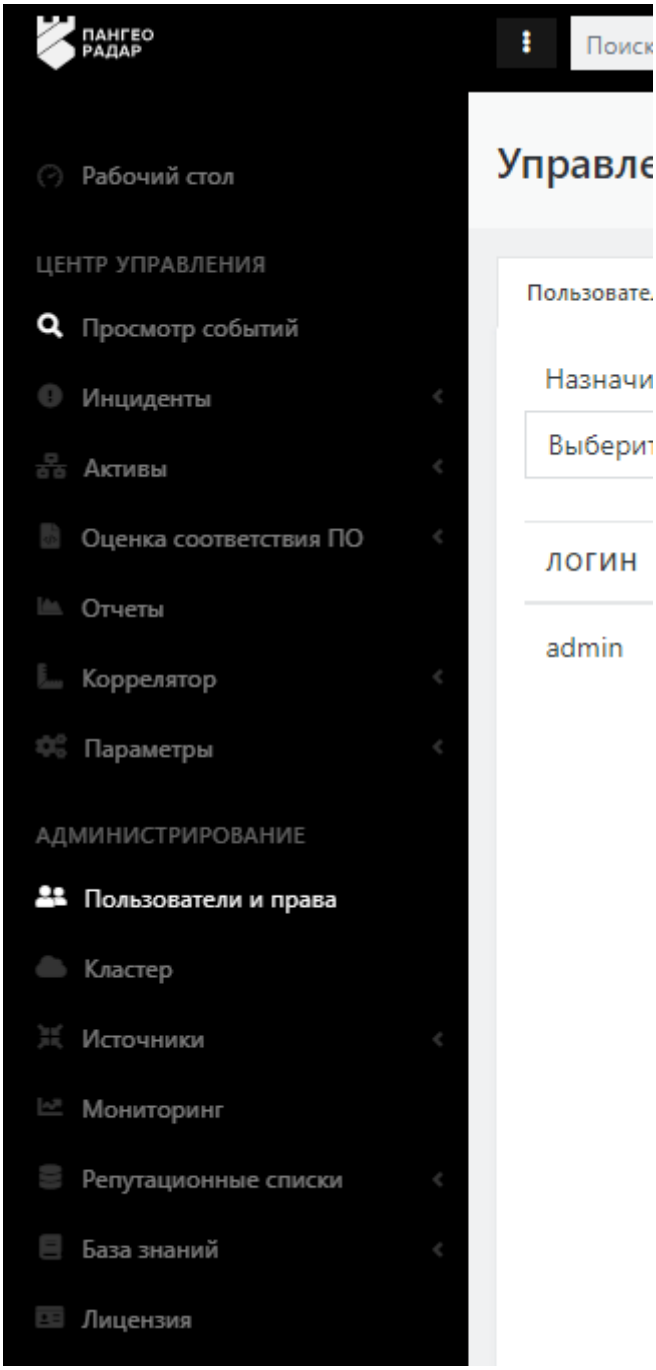

Рисунок 1 - Пункты меню раздела «Администрирование»

2. Управление пользователями

2.1. Общее описание

В Платформе Радар предусмотрена возможность многопользовательской работы. Каждый пользователь работает под своими учетными данными. Для построения рабочего процесса по управлению инцидентами пользователи включаются в группы согласно выполняемым функциям.

Основной раздел интерфейса «**Пользователи и группы**» предназначен для выполнения следующих функций:

- управление учетными записями пользователей;
- контроль состояния активности пользователя;
- управления ролями и группами пользователей.

Раздел содержит следующие вкладки:

- "**Пользователи**" — вкладка предназначена для управления учётными записями пользователей.
- "**Группы**" — вкладка предназначена для управления группами пользователей.
- "**Роли**" — вкладка предназначена для управления ролями, назначаемыми пользователям.
- "**Аудит действий**" — вкладка предназначена для просмотра действий пользователей.
- "**События входа**" - вкладка предназначена для просмотра событий входа пользователей в **Платформу Радар**.
- "**LDAP**" - вкладка предназначена для интеграции со службой каталогов.
- "**Доступ к данным**" - вкладка предназначена для управления доступом пользователей и групп пользователей к разделам **Платформы Радар**.

2.2. Управление учетными записями пользователей

2.2.1. Вкладка "Пользователи". Общее описание

Вкладка "**Пользователи**" содержит (см. рисунок 2):

- Текущий список зарегистрированных на Платформе пользователей в виде табличного списка.
- Форму для создания нового пользователя на Платформе — форма "Создать нового".
- Функцию назначения пользователю роли.
- Функцию добавления пользователя в группу.

На вкладке "**Пользователи**" доступны следующие опции по управлению учетными записями пользователей:

- Создание нового пользователя;
- Редактирование существующего;
- Удаление пользователя;
- Переключение статуса активности пользователя;
- Назначение пользователю групп и ролей;
- Исключение пользователя из группы;
- Снятие с пользователя определенной роли;
- Смена пароля пользователю.

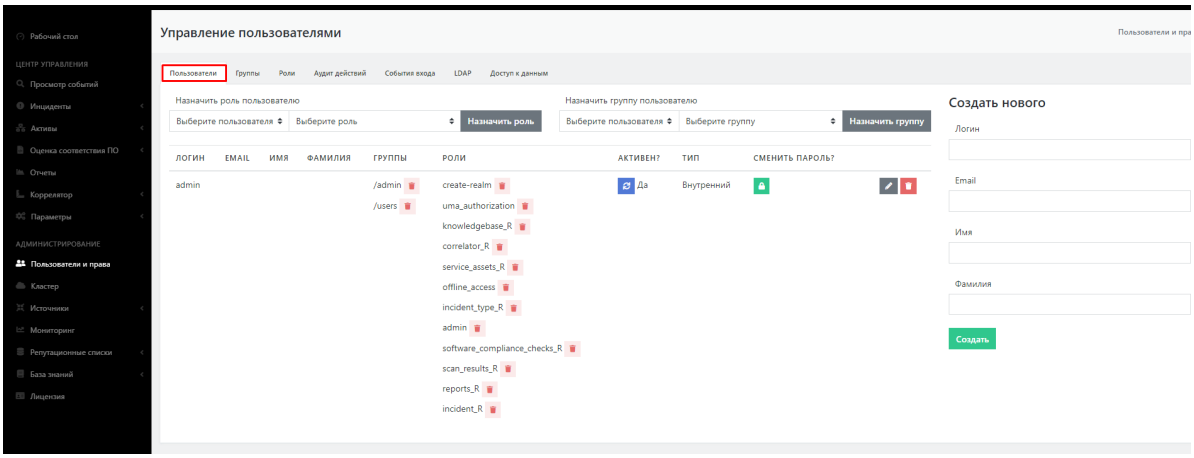

Рисунок 2 - Экран управления учетными записями пользователя (вкладка "Пользователи

2.2.1.1. Создание нового пользователя

Для создания нового пользователя в Платформе необходимо выполнить следующие действия:

1. Заполнить форму "Создать нового" (см. рисунок 3). При создании формы обязательны к заполнению все поля формы.
2. Сохранить введенные данные нажав на кнопку "Создать".

   В таблице пользователей должна появится строка с новым пользователем. Пользователь автоматически создается с ролью user и включен в соответствующую группу.
3. Сгенерировать пароль для нового пользователя нажав на пиктограмму  ;
4. При необходимости провести настройку групп и ролей пользователя (см. раздел "Присвоение роли и группы пользователю").

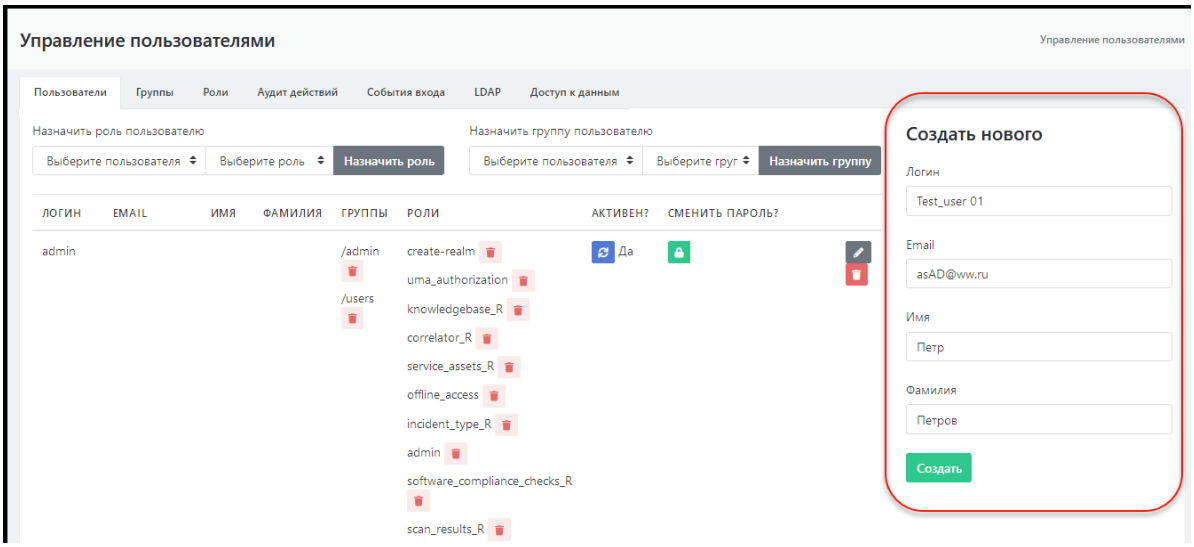

Рисунок 3 - Форма создания нового пользователя

2.2.1.2. Редактирование данных пользователя

Для внесения изменений в данные пользователя необходимо:

1. Нажать на пиктограмму  в строке интересующего пользователя. Откроется форма "Изменение" с данными пользователя доступными для редактирования (см. рисунок 4).
2. Внести необходимые изменения и нажать кнопку «Обновить» для сохранения изменений или кнопку «Отменить» (для отмены).

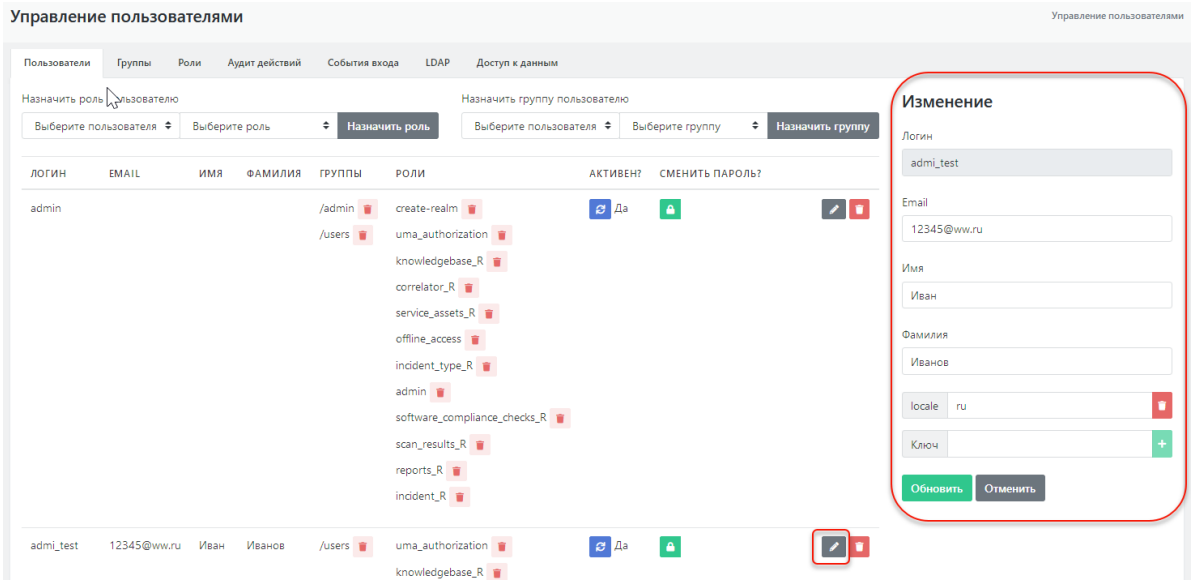

Рисунок 4 - Форма редактирования данных пользователя

2.2.1.3. Изменение пароля

Для изменения пароля пользователя необходимо нажать на пиктограмму  , после чего будет сгенерирован новый пароль в появившейся форме рядом (см. рисунок 5).

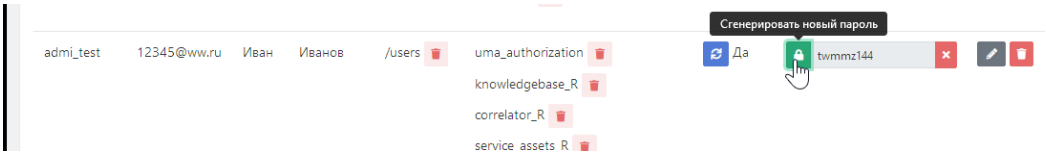

Рисунок 5 - Генерация нового пароля пользователя

2.2.1.4. Удаление пользователя

Для удаления пользователя с Платформы необходимо:

1. Нажать на пиктограмму  .
2. В открывшемся окне подтвердить удаление пользователя (см. рисунок 6).

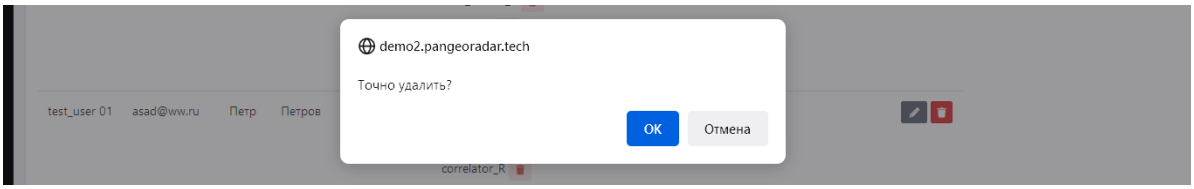

Рисунок 6 - Удаление пользователя

2.2.1.5. Присвоение роли пользователю. Отключение роли

Для присвоения пользователю новой роли необходимо (см. рисунок 7):

1. В области "Назначить роль пользователю" выбрать в раскрывающемся списке пользователей интересующего пользователя.
2. Выбрать в раскрывающемся списке ролей необходимую роль.
3. Нажать на кнопку "Назначить роль".

Указанная роль должна появится в списке ролей пользователя (колонка таблицы "Роли").

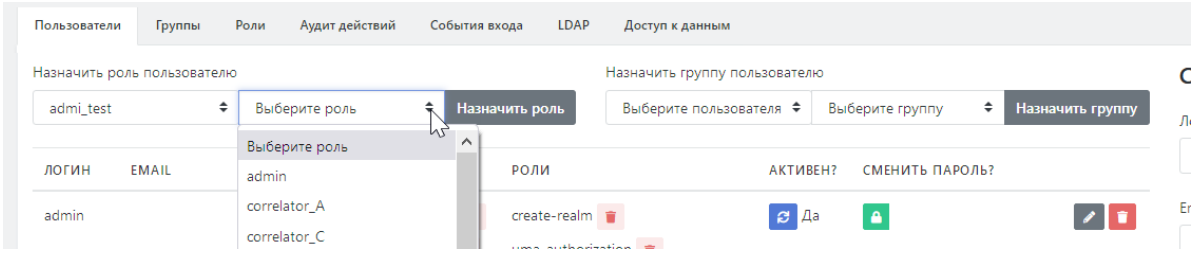

Рисунок 7 - Присвоение пользователю новой роли

Для отключения роли от пользователя необходимо выбрать в списке нужного пользователя и в колонке "Роли" нажать на пиктограмму  рядом с названием той роли, которую необходимо отключить от данного пользователя. Указанная роль будет удалена из строки пользователя.

Таким образом можно удалить только отдельно добавленную пользователю роль. Роль, привязанную к группе и добавленную пользователю при включении его в группу удалить таким образом невозможно. Роли, ассоциированные с группой, удаляются у пользователя, только тогда, когда его исключают из этой группы.

2.2.1.6. Включение пользователя в группу. Удаление из группы

Для включения пользователя в новую группу (см. рисунок 8):

1. В области "Назначить группу пользователю" выбрать в раскрывающемся списке пользователей интересующего пользователя.
2. Выбрать в раскрывающемся списке групп необходимую группу.
3. Нажать на кнопку "Назначить группу".

Указанная группа должна появится в списке групп пользователя (колонка таблицы "Группы").

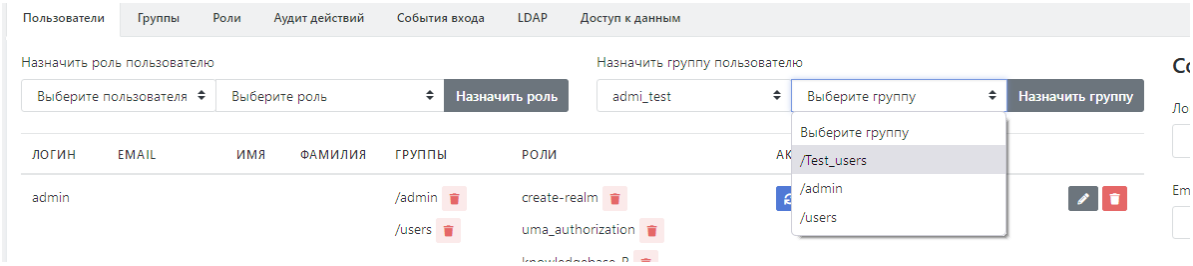

Рисунок 8 - Включение пользователя в группу

Для исключения пользователя из группы выберете в списке нужного пользователя и в колонке "Группы" нажать на пиктограмму  рядом с именем той группы, из которой необходимо удалить данного пользователя. Указанная группа будет удалена из строки пользователя.

2.2.1.7. Изменение атрибутов пользователя

Пользователю могут быть назначены разного рода атрибуты, влияющие на поведение Платформы или содержащие информационный характер.

1. Для добавления нового атрибута пользователю необходимо открыть форму редактирования данных пользователя (см. раздел "Редактирование данных пользователя")(см. рисунок 9).
2. Ввести в поле "Ключ" название нового атрибута и нажать на пиктограмму  .

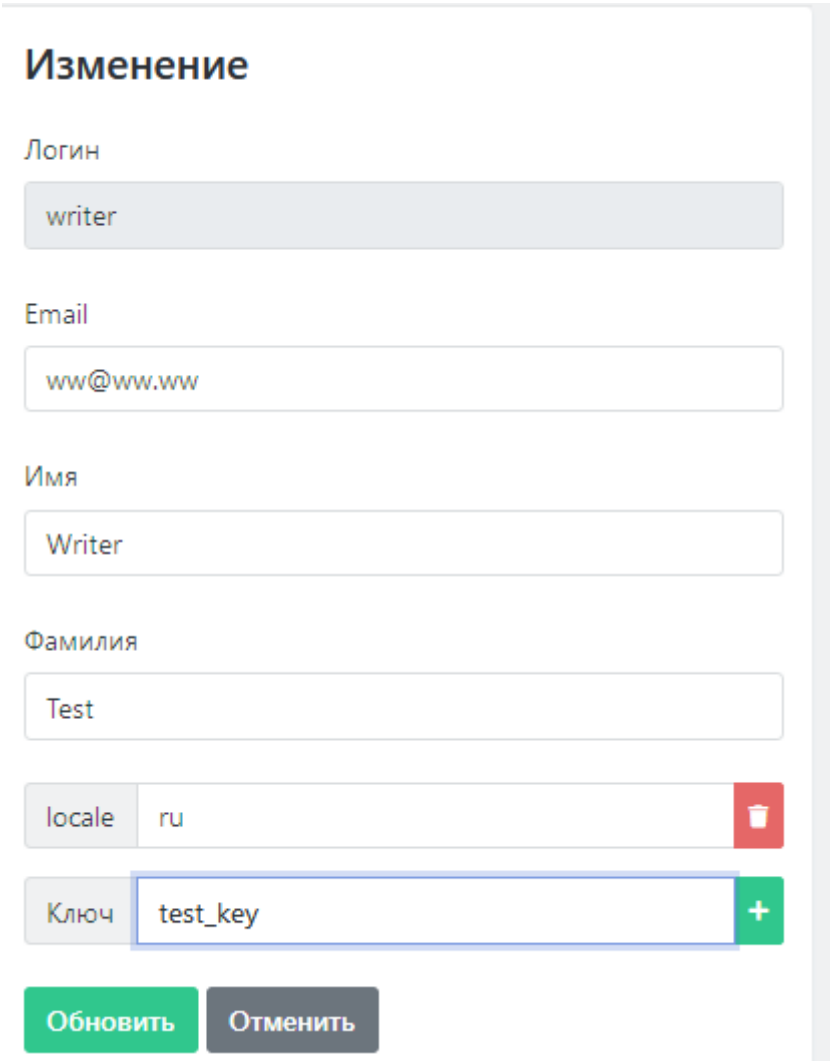

Рисунок 9 - Создание нового атрибута пользователя

В форме редактирования добавится поле нового атрибута (см. рисунок 10). В данное поле можно внести соответствующее значение.

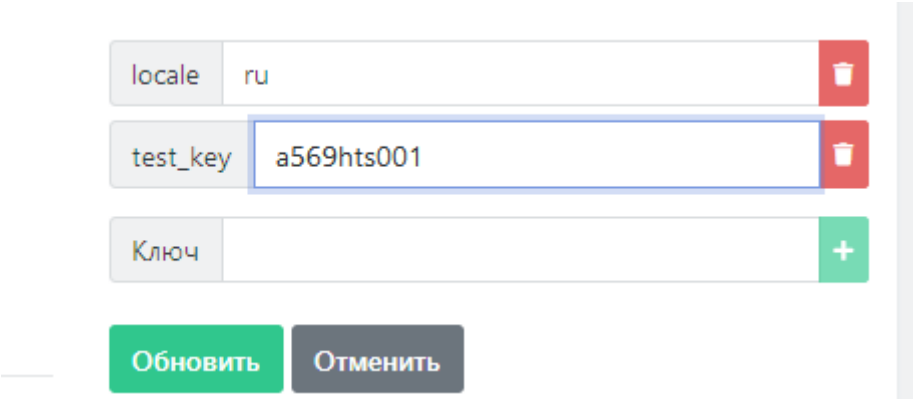

Рисунок 10 - Изменение значения нового атрибута пользователя

По завершению внесения изменений их необходимо сохранить, нажав на кнопку «Обновить» (см. рисунок 9).
Для удаления атрибута из профиля пользователя необходимо нажать на соответствующую атрибуту пиктограмму .

Ниже в таблице 1 приведен список используемых системных атрибутов.

Таблица 1 -- Список системных атрибутов:

Название	Описание
tz	Строковое значение отвечающее за конвертацию временных меток в интерфейсе в нужную таймзону пользователю. По умолчанию — Europe/Moscow.
is_system_notification	Строковое значение с любым содержимым отвечает за доставку системных уведомлений от Платформы пользователю на E-mail

2.2.2. Управление группами пользователей

2.2.2.1. Вкладка "Группы". Общее описание

Вкладка "**Группы**" содержит (см. рисунок 11):

- Текущий список зарегистрированных на Платформе групп пользователей в виде табличного списка.
- Поле для создания новой группы пользователей на Платформе — форма "Создать".
- Функцию ассоциации роли с группой.

На вкладке "**Группы**" доступны следующие опции по управлению группами (см. рисунок 11) :

- Просмотр существующих групп пользователей;
- Создание новой группы пользователей;
- Изменений существующей группы пользователей;
- Удаление группы.
- Назначение пользовательских ролей группам;
- Отключение пользовательских ролей от группы.

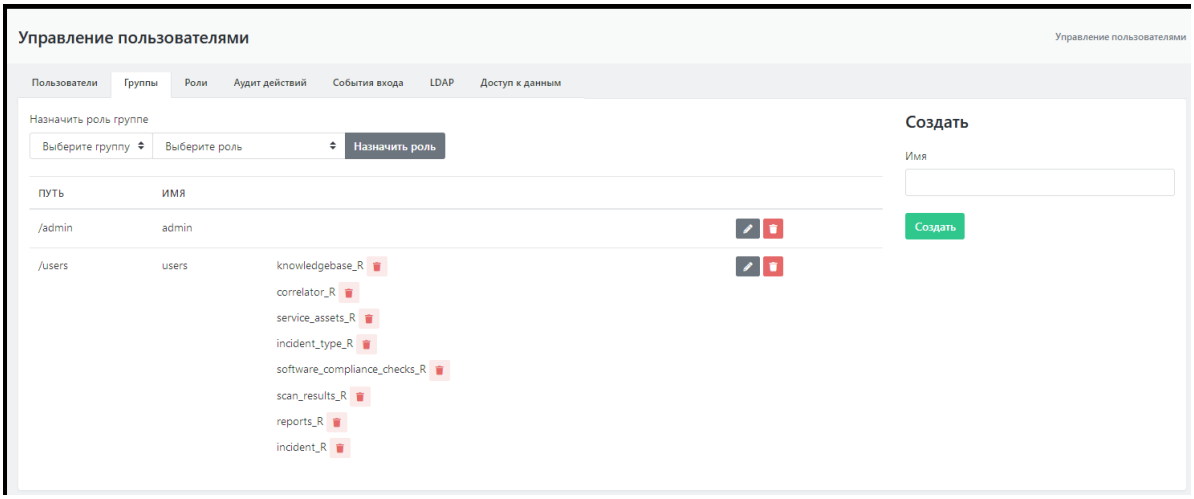

Рисунок 11 - Экран управления пользовательскими группами (вкладка "Группы

2.2.2.2. Создание группы пользователей

Для создания новой группы необходимо ввести имя группы в форму "Создать" и нажать на кнопку "Создать" (см. рисунок 12). Новая группа отобразится в списке пользовательских групп Платформы.

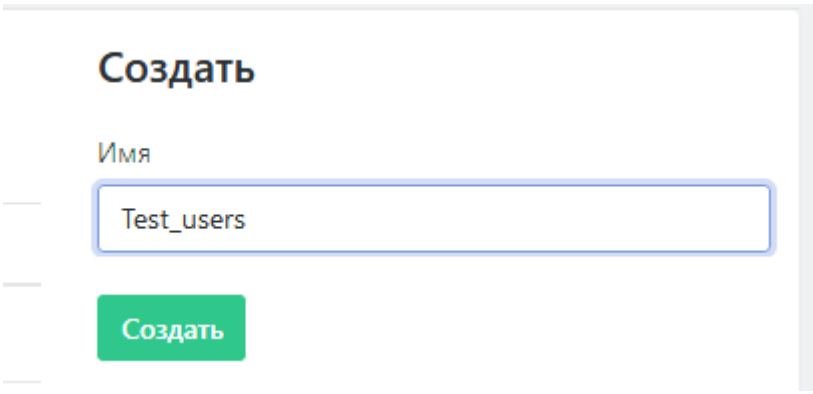

Рисунок 12 - Форма создания новой группы

2.2.2.3. Редактирование данных группы пользователей

Для внесения изменений в данные пользователя необходимо:

1. Нажать на пиктограмму  в строке интересующей группы. Откроется форма "Изменение" с данными группы, доступными для редактирования (см. рисунок 13).
2. Внести необходимые изменения и нажать кнопку «Обновить» для сохранения изменений или кнопку «Отменить» (для отмены).

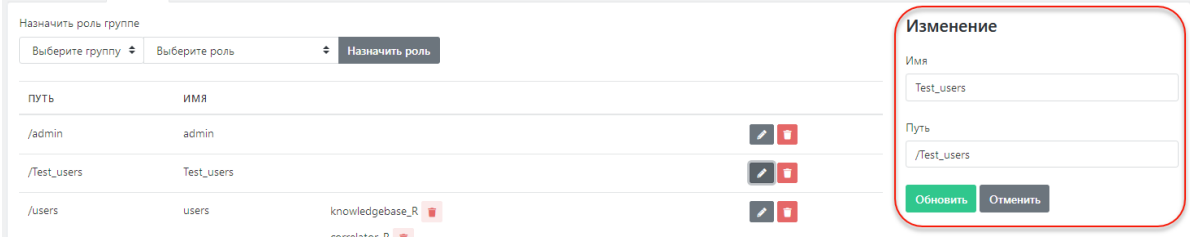

Рисунок 13 - Форма редактирования группы

2.2.2.4. Присвоение роли группе пользователей. Отключение роли от группы

Для присвоения группе пользователей новой роли необходимо (см. рисунок 14):

1. В области "Назначить роль группе" выбрать в раскрывающемся списке групп интересующую группу пользователей.
2. Выбрать в раскрывающемся списке ролей необходимую роль.
3. Нажать на кнопку "Назначить роль".

Указанная роль должна появится в списке ролей выбранной группы (колонка таблицы "Роли").

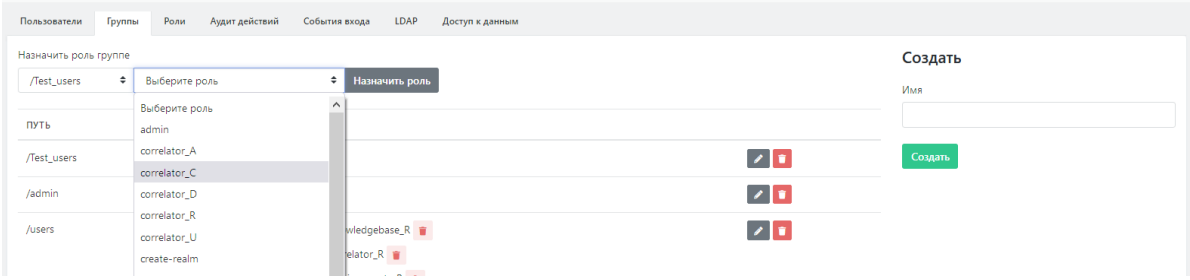

Рисунок 14 - Присвоение пользователю новой роли

Для отключения пользовательской роли от группы необходимо выбрать в списке нужную группу и в колонке "Роли" нажать на пиктограмму  рядом с названием той роли, которую необходимо отключить от данной пользовательской группы. Указанная роль будет удалена из строки группы.

2.2.2.5. Предустановленный список групп пользователей

В Платформе Радар используются группы пользователей по умолчанию, представленные в таблице 2.

Таблица 2 -- Предустановленные группы пользователей

Название группы	**Включенные роли**
admin	
users	- knowledgebase_R - correlator_R - service_assets_R - incident_type_R - software_compliance_checks_R -scan_results_R - reports_R - incident_R

> **Внимание!** Группа «Users» добавляется всем пользователям по умолчанию. Её наличие необходимо для корректной работы пользователя с Платформой.

> **Внимание!** Пользователи, включенные в группу «Admin», имеют доступ ко всем разделам и настройкам Платформы.

2.2.3. Управление ролями пользователей

2.2.3.1. Вкладка "Роли". Общее описание

Вкладка "**Роли**" содержит (см. рисунок 15):

- Текущий список созданных на Платформе ролей пользователей в виде табличного списка.
- Поле для создания новой роли пользователя на Платформе - форма "Создать".

На вкладке "**Роли**" доступны следующие опции по управлению ролями (см. рисунок 15) :

- Просмотр существующих ролей пользователей;
- Создание новой роли пользователей;
- Изменений существующей роли пользователей;
- Удаление роли.

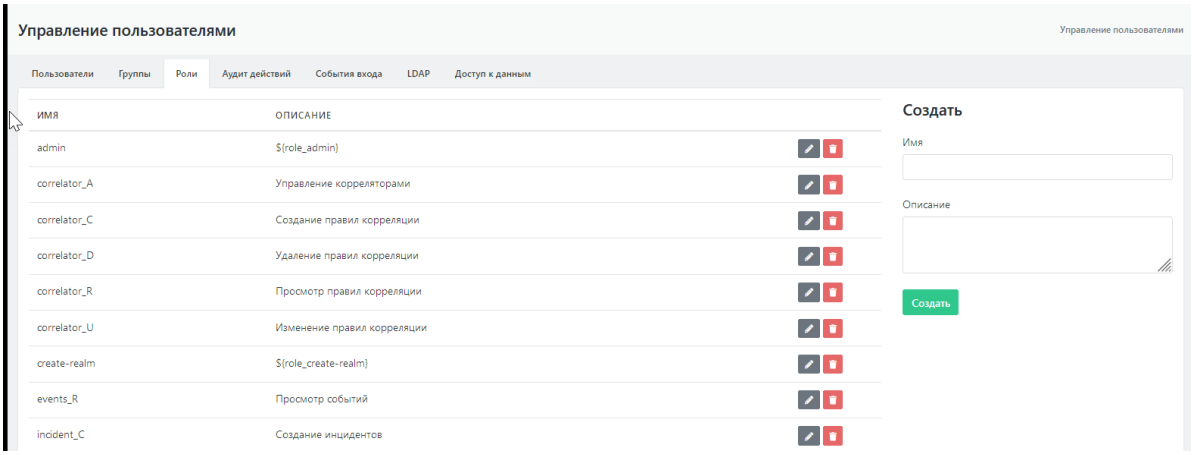

Рисунок 15 - Экран управления ролями пользователей (вкладка "Роли

2.2.3.2. Создание пользовательской роли

Для создания новой роли необходимо ввести имя и описание роли в форму "Создать" и нажать на кнопку "Создать" (см. рисунок 16). Новая роль отобразится в списке ролей Платформы.

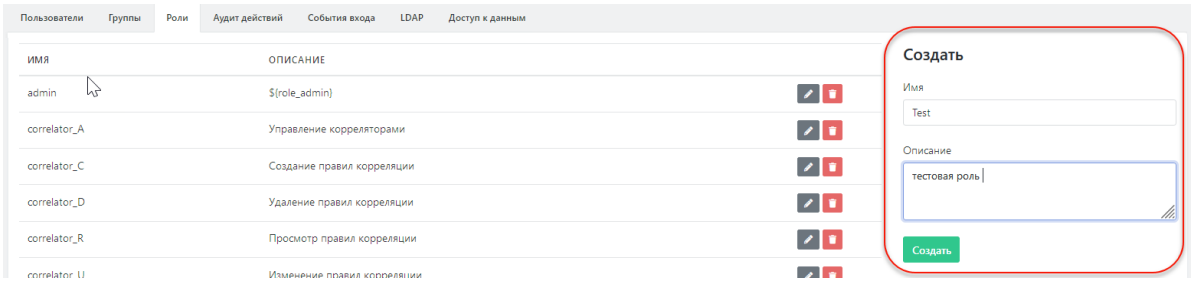

Рисунок 16 - Форма создания новой пользовательской роли

2.2.3.3. Редактирование данных пользовательской роли

Для внесения изменений в данные роли необходимо:

1. Нажать на пиктограмму  в строке интересующей роли. Откроется форма "Изменение" с параметрами роли, доступными для редактирования (см. рисунок 17).
2. Внести необходимые изменения и нажать кнопку «Обновить» для сохранения изменений или кнопку «Отменить» (для отмены).

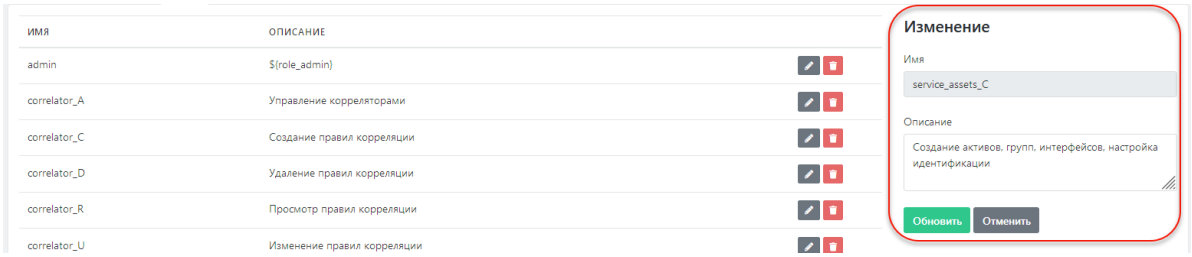

Рисунок 17 - Форма редактирования параметров пользовательской роли

2.2.3.4. Предустановленный список ролей пользователей

В системе есть предустановленный набор привилегий (ролей), которые могут быть назначены пользователям (см. таблицу 3).

Таблица 3 -- Предустановленные пользовательские роли

Название роли	Описание роли

Название роли	Описание роли
admin	Администратор системы
correlator_A	Управление корреляторами
correlator_C	Создание правил корреляции
correlator_D	Удаление правил корреляции
correlator_R	Просмотр правил корреляции
correlator_U	Изменение правил корреляции
events_R	Просмотр событий
incident_C	Создание инцидентов
incident_D	Удаление инцидентов
incident_mass_U	Массовые действия с инцидентами
incident_R	Просмотр инцидентов
incident_status_U	Изменять статус инцидента
incident_type_C	Создание типов инцидентов
incident_type_D	Удаление типов инцидентов
incident_type_R	Просмотр типов инцидентов
incident_type_U	Изменение типов инцидентов
incident_U	Изменение инцидентов
incident_users_U	Назначения пользователей для инцидента
knowledgebase_C	Создание записей базы знаний
knowledgebase_D	Удаление записей базы знаний
knowledgebase_R	Просмотр записей базы знаний
knowledgebase_U	Изменение записей базы знаний
reports_C	Создание отчетов
reports_D	Удаление отчетов
reports_R	Просмотр отчетов
reports_U	Изменение отчетов
scan_results_C	Загрузка результатов сканирования
scan_results_D	Удаление результатов сканирования
scan_results_R	Просмотр результатов сканирования

Название роли	Описание роли
scan_results_U	Изменение результатов сканирования
service_assets_C	Создание активов, групп, интерфейсов, настройка идентификации
service_assets_D	Удаление активов, групп, интерфейсов, настройка идентификации
service_assets_R	Просмотр активов, групп, интерфейсов, настройка идентификации
service_assets_U	Изменение активов, групп, интерфейсов, настройка идентификации
software_compliance_checks_C	Создание правил и наборов правил оценки соответствия ПО
software_compliance_checks_D	Удаление правил и наборов правил оценки соответствия ПО
software_compliance_checks_R	Просмотр всех сущностей оценки соответствия ПО
software_compliance_checks_U	Изменение правил и наборов правил оценки соответствия ПО

> **Внимание!** Пользователи с назначенной ролью «Admin» будут иметь доступ ко всем разделам и настройкам Платформы.

2.2.4. Аудит действий пользователя

2.2.4.1. Общее описание

На вкладке «**Аудит действий**» администратору Платформы представляются функции просмотра всех совершаемых пользователями действий по внесению изменений в Платформу.

Для настройки просмотра используются следующие фильтры:

- По временному окну.
- По пользователю (по всем пользователям или по выбранному).
- По сервису (по всем сервисам или по выбранному).
- По сущности (фильтр доступен при выборе отдельного сервиса).

Для осуществления поиска действий необходимо выбрать временное окно и нажать кнопку «Поиск» (см. рисунок 18). По умолчанию поиск действий будет произведен по всем пользователям и по всем сервисам.

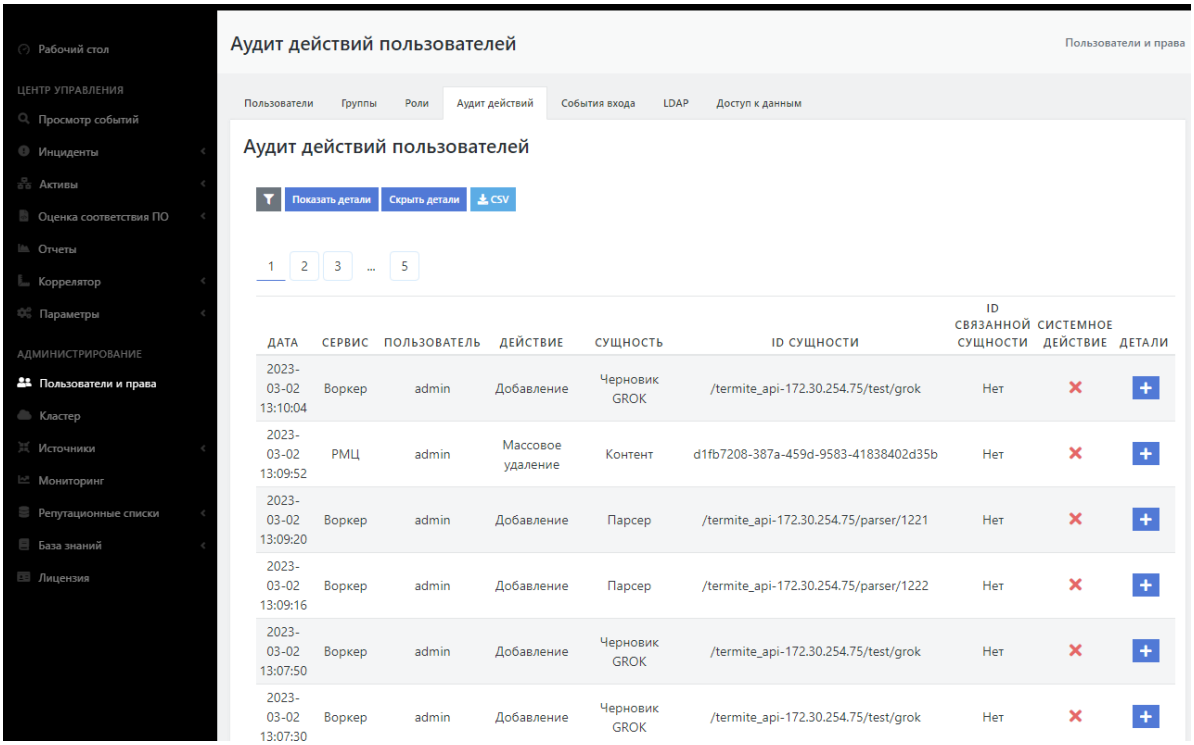

Рисунок 18 - Экран просмотра действий пользователя до ввода данных

2.2.4.2. Настройка списка действий пользователя

Для проведения поиска по действиям конкретного пользователя необходимо выбрать данного пользователя в раскрывающемся списке "Пользователь".

Для проведения поиска по действиям, связанным с конкретным сервисом, необходимо выбрать интересующий сервис в раскрывающемся списке "Сервис".

Результаты поиска представляют собой список действий пользователя (всех пользователей) на выбранном сервисе (или всех сервисах) за указанный период времени (см. рисунок 19).

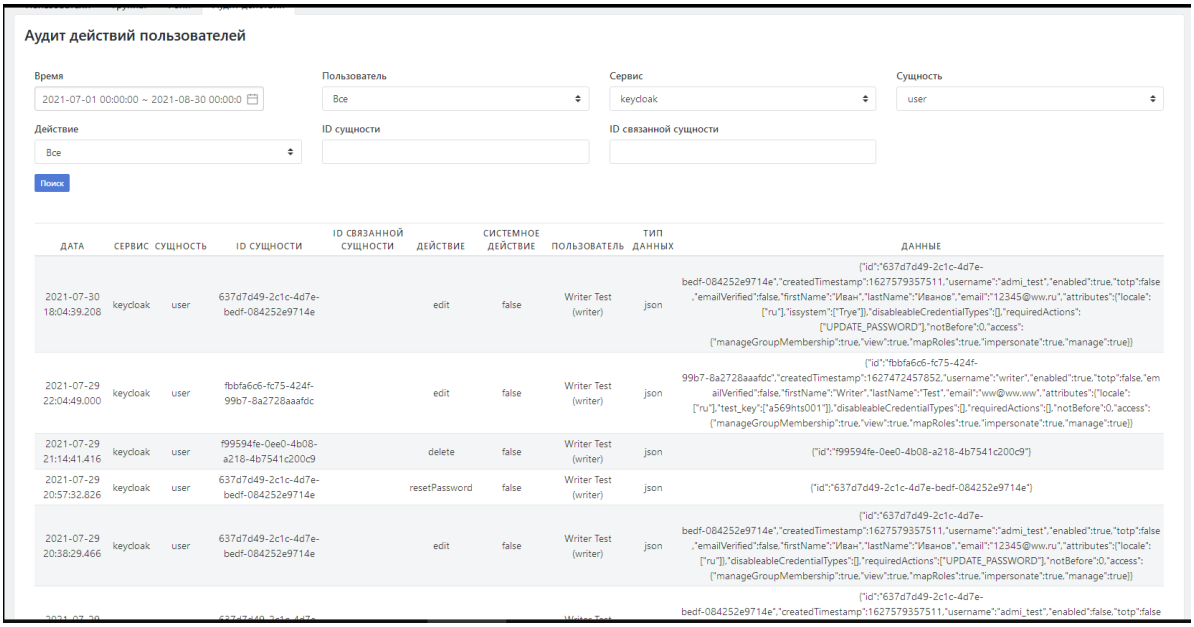

Рисунок 19 - Список действий пользователя

При выборе поиска по отдельному сервису добавляется фильтр по сущности, ассоциированной с сервисом. При выборе какой-либо сущности на экран добавляются возможности фильтрации по действиям сущности, ID сущности и ID связанной сущности (см. рисунок 19).

2.2.4.3. Расширенный лог действий, связанных с авторизацией

Также есть расширенный лог действий связанный с авторизацией. Он доступен по адресу http://<адрес сервера>:8180/auth/admin/master/console/#/realms/master/events

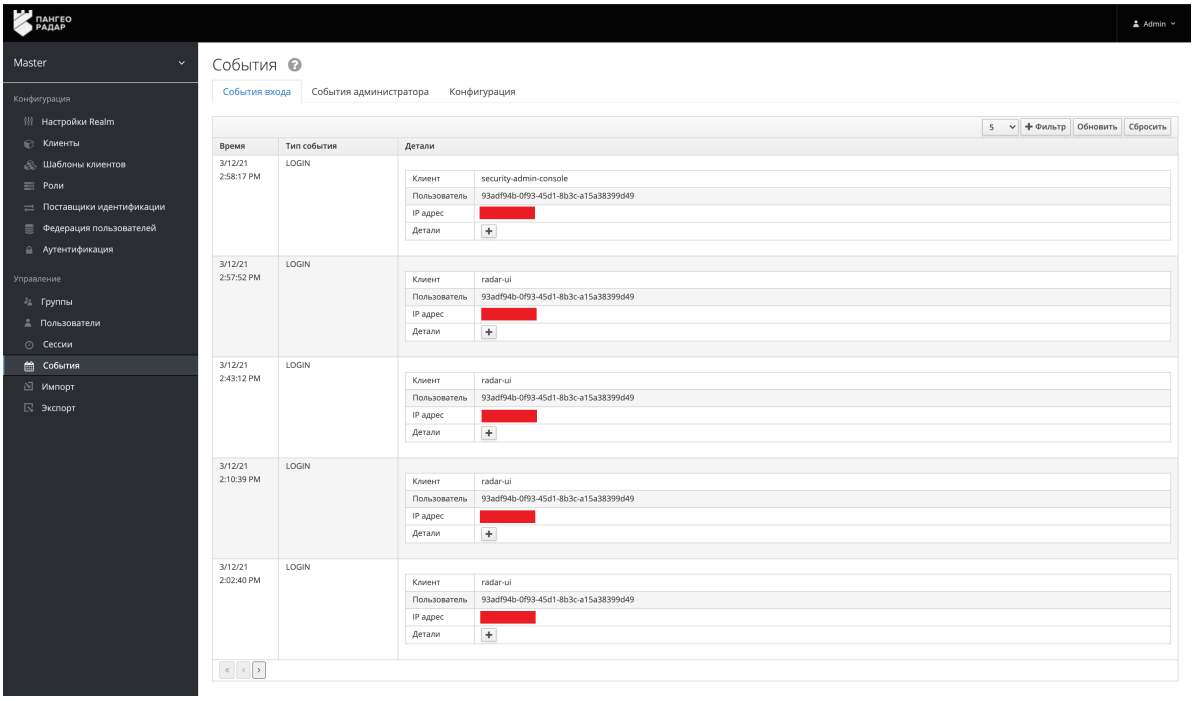

Рисунок 20 - Расширенный интерфейс управления пользователями, просмотр событий входа

Данный интерфейс является частью службы централизованной аутентификации Платформы и не предназначен для ручного администрирования без необходимости.

Для возврата в интерфейс Платформы воспользуйтесь переходом из пользовательского меню (см. рисунок 21)

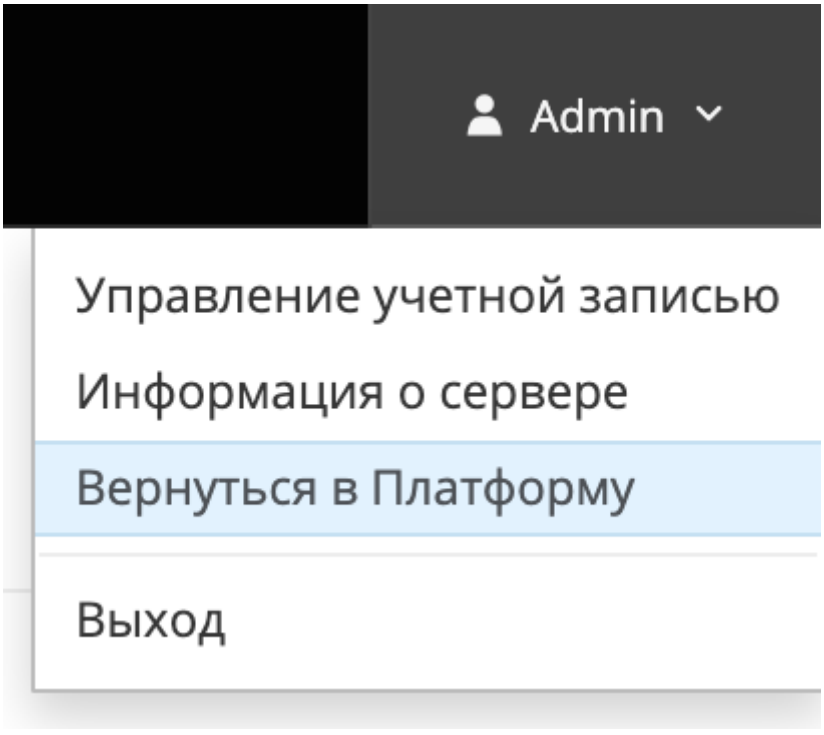

Рисунок 21 - пользовательское меню службы централизованной аутентификации.

2.2.5. Просмотр событий входа во вкладке "События вход"

На вкладке «**События входа**» (см. рисунок 22) отображаются события получения доступа пользователями к **Платформе Радар**.

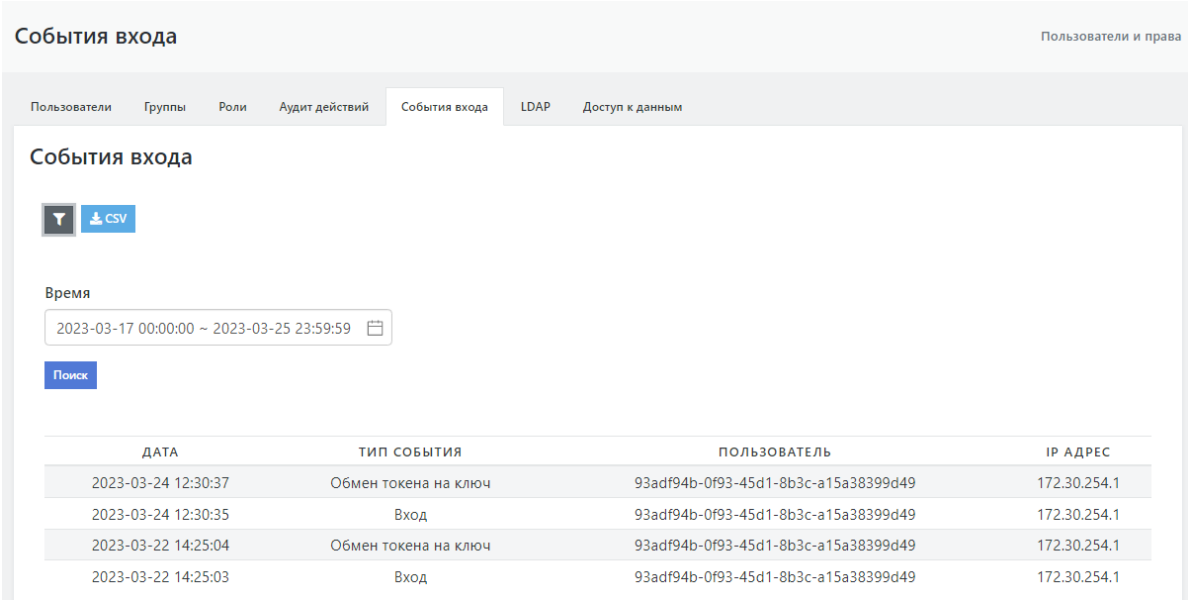

Рисунок 22 - Экран просмотра событий доступа к Платформе

Для настройки просмотра используется фильтр по временному диапазону событий.

2.2.6. Вкладка "LDAP"

На вкладке LDAP отображается перечень интеграций со службами каталогов (см. рисунок 23).

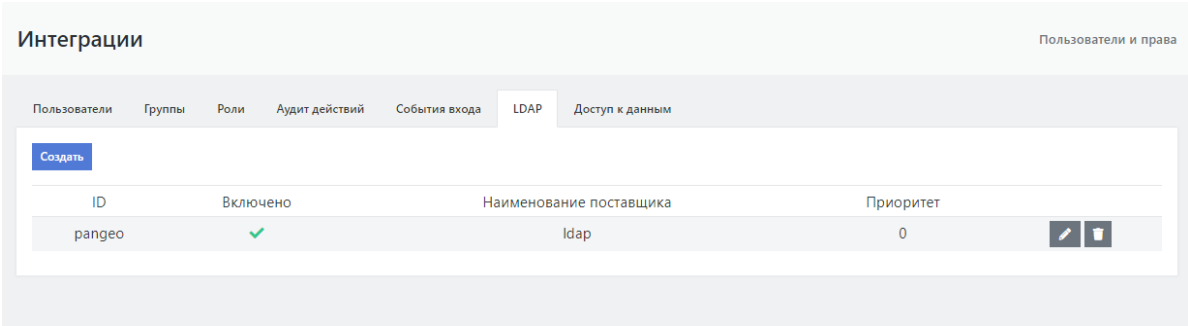

Рисунок 23 - Перечень интеграций со службами каталогов

В таблице с интеграциями отображаются:

- **ID** - идентификатор интеграции, задается вручную.
- **Включено** - флаг активности интеграции.
- **Наименование поставщика** - протокол доступа к службе каталогов (LDAP).
- **Приоритет** - приоритет обработки интеграции.
- кнопки редактирования  и удаления  интеграции.

2.2.6.1. Создание / редактирование интеграции с LDAP

Для создания новой интеграции нажмите кнопку "**Создать**". Для редактирования существующей интеграции нажмите иконку редактирования  выбранной интеграции.

Настройки каждой интеграции разбиты по отдельным вкладкам.

На вкладке "Основные настройки" доступны настройки:

- **Включена** - если интеграция выключена, она не будет использована при запросах, а импортированные пользователи будут деактивированы и переведны в состояние "только чтение", пока интеграция не будет включена снова.
- **Название** - идентификатор интеграции.
- **Приоритет** - приоритет службы при поиске пользователя. Меньшие значения имеют более высокий приоритет.
- **Импортировать пользователей** - если включено, пользователи LDAP будут импортированы в базу данных Keycloak и синхронизированы через сконфигурированные политики синхронизации.
- **Режим редактирования** - "Только чтение" означает доступ только на чтение из LDAP. "Записываемый" означает, что данные будут обратно синхронизированы в LDAP по заявке. "Несинхронизированный" означает, что данные пользователя будут импортированы, но не синхронизированы обратно в LDAP.
- **Синхронизировать регистрации** - включение опции создает вновь созданных пользователей в хранилище LDAP. Приоритет определяет какой из поставщиков будет выбран для синхронизации нового пользователя.
- **Поставщик** - LDAP поставщик (провайдер).
- **Атрибут Username в LADP** - наименование LDAP атрибута, которое отображается как имя пользователя в Keycloak. Для множества серверов LDAP это может быть 'uid'. Для Active directory это может быть 'sAMAccountName' или 'cn'. Атрибут должен быть заполнен для всех LDAP записей пользователей, которые вы хотите импортировать из LDAP в Keycloak.
- **Атрибут RDN в LDAP** - наименование атрибутов LDAP, которое используется как RDN (верхний атрибут) обычного пользователя DN. Обычно оно такое же, как атрибут имени пользователя LDAP, однако он не обязателен. Для примера, для Active directory обычно используется 'cn' как атрибут RDN, в то время как атрибут имени пользователя может быть 'sAMAccountName'.
- **Атрибут UUID в LDAP** - наименование LDAP атрибута,которое используется как уникальный идентификатор объектов (UUID) в LDAP. Для множества LDAP серверов это 'entryUUID' однако некоторые могут отличаться. Для примера, для Active directory он должен быть 'objectGUID'. Если ваш LDAP сервер действительно не поддерживает понятие UUID, вы можете использовать любой другой атрибут, который должен быть уникальным среди пользователей в дереве LDAP. Например 'uid' или 'entryDN'.
- **Классы объектов пользователя** - все значения из LDAP objectClass атрибутов для пользователей в LDAP, разделенные запятой. Например: 'inetOrgPerson, organizationalPerson' . Вновь созданные пользователи Keycloak будут записаны в LDAP вместе с этими классами объектов, а существующие записи пользователей LDAP будут найдены только если они содержат все эти классы объектов.
- **URL подключения** - URL соединения с вашим сервером LDAP. Соединение можно протестировать кнопкой "Тест подключения".
- **Пользователи DN** - полный DN из дерева LDAP где присутствуют ваши пользователи. Этот DN является родителем пользователей LDAP. Он может быть, для примера 'ou=users,dc=example,dc=com' при условии, что ваш обычный пользователь будет иметь DN похожий на'uid=john,ou=users,dc=example,dc=com'.
- **Пользовательский Фильтр LDAP пользователей** - дополнительный фильтр LDAP для фильтрации искомых пользователей. Оставьте поле пустым, если не нуждаетесь в дополнительном фильтре. Убедитесь, что он начинается с '(' и заканчивается ')'.
- **Поиск области** - для одного уровня пользователи ищутся только в DN, определенных как пользовательские DN. Для поддеревьев ищутся пользователи полностью в их поддеревьях. Смотрите документацию LDAP для подробных деталей.

- **Тип аутентификации** - тип LDAP аутентификации. Сейчас доступны только механизмы 'none' (анонимная аутентификация LDAP) или 'simple' (Аутентификация по сопоставленным логину и паролю).
- **Сопоставление DN** - DN администратора LDAP, которые будут использованы Keycloak для доступа на сервер LDAP.
- **Сопоставление учетных данных** - пароль администратора LDAP. Проверку правильности ввода учетных данных можно сделать с помощью кнопки "Проверка аутентификации".

На вкладке "Расширенные настройки" доступны настройки:

- **Включить StartTLS** - шифрует соединение к LDAP используя STARTTLS, применение которого отключает пулинг соединений.
- **Расширенная операция LDAPv3 изменения пароля** - использование расширенной операция LDAPv3 изменения пароля (RFC-3062). Для расширенной операции изменения пароля обычно требуется, чтобы у LDAP пользователя уже был выставлен пароль на сервере. Когда эта опция используется вместе с "Синхронизацией зарегистрированных" желательно также добавить "Фиксированный LDAP маппер атрибутов", содержащий случайно сгенерированное начальное значение для пароля.
- Кнопка **Проверить поддержку расширения** - опрашивает LDAP сервер касательно поддержки "Расширенной операции LDAPv3 изменения пароля" и автоматически выставляет нужное значение в настройках.
- **Политика проверки пароля** - определяет должен ли Keycloak, перед тем как обновлять пароль, валидировать его согласно политике паролей области.
- **Подтверждение почтового адреса** - если включено, то E-mail, предоставленный этим поставщиком, не будет подтвержденным даже если подтверждение включено для области.
- **Использование доверенных сертификатов SPI** - определяет, будет ли соединение с LDAP использовать хранилище доверенных сертификатов SPI вместе с сертификатами, сконфигурированными в keycloak-server.json. 'Всегда' означает, что они будут использоваться всегда. 'Никогда' означает, что они никогда не будут использованы. 'Только для ldap'ов' означает, что они будут использованы вместе с вашими соединениями к ldap серверам. Обратите внимание, что если keycloak-server.json не сконфигурирован, то по умолчанию Java будет использовать cacerts или сертификат, определенный в 'javax.net.ssl.trustStore'.
- **Таймаут соединения** - таймаут соединения с LDAP в миллисекундах.
- **Таймаут чтения** - таймаут чтения из LDAP в миллисекундах. Этот таймаут применяется к операциям чтения из LDAP.
- **Постраничный вывод** - должен ли LDAP сервер поддерживать постраничный вывод.

На вкладке "Пул соединений" доступны настройки:

- **Пул соединений** - должен ли Keycloak использовать пул соединений для доступа к LDAP серверу.
- **Пулинг аутентификационных соединений** - разделенный пробелом список аутентификационных типов соединений, которе могут быть помещены в пул. Валидные значения: "none", "simple" и "DIGEST-MD5".
- **Уровень отладки пула соединений** - уровень отладки. Валиданые значения: "fine" (логирует создание и удаление соединений) и "all" (полный вывод всей отладочной информации).
- **Начальный размер пула соединений** - число изначально создаваемых соединений к каждому из узлов.
- **Максимальный размер пула соединений** - максимальное число одновременных соединений к узлу.

- **Предпочтительный размер пула соединений** - предпочтительное число одновременных соединений к узлу.
- **Протокол пула соединений** - разделенный пробелом список протоколов соединений, которые можно поместить в пул. Валидные значения: "plain" и "ssl".
- **Таймаут пула соединений** - сколько миллисекунд неактивное соединение может пребывать в пуле перед тем как оно будет закрыто и удалено из него.

На вкладке "Интеграция с Kerberos" доступны настройки:

- **Разрешить аутентификацию Kerberos** - включить/выключить аутентификацию HTTP пользователей с токенами SPNEGO/Kerberos. Данные об аутентифицированых пользователях будут предусмотрены из этого LDAP сервера.
- **Использовать Kerberos для аутентификации по паролю** - Использовать модуль входа Kerberos для аутентификации по логин/пароль с сервера Kerberos вместо аутентификации на сервере LDAP с Directory Service API

На вкладке "Синхронизировать настройки" доступны настройки:

- **Размер пачки** - количество пользователей LDAP, которые будут импортированы в Keycloak за одну транзакцию.
- **Периодическая полная синхронизация** - должна ли быть включена полная периодическая синхронизация пользователей LDAP в Keycloak или нет.
- **Периодическая синхронизация изменений пользователей** - должна ли быть включена периодическая синхронизация новых и измененных пользователей LDAP в Keycloak или нет.

На вкладке "Настройки кэширования" доступна настройка:

- **Политики кэширования** - политики кэширования для этого поставщика хранения. 'По умолчанию' представляет настройки по-умолчанию для глобального пользовательского кэша. 'Вытеснять каждый день' время каждого дня, после которого пользовательский кэш инвалидируется. 'Вытеснять каждую неделю' день и время недели после которого пользовательский кэш инвалидируется. 'По максимальному времени жизни' время в миллисекундах, в течение которого будет существовать жизненный цикл записи в кэше.

При редактировании интеграции отдельно доступны действия:

- **Синхронизация измененных пользователей** - принудительная синхронизация измененных пользователей LDAP в Keycloak.
- **Синхронизация всех пользователей** - принудительная синхронизация всех пользователей LDAP в Keycloak.
- **Удалить импортированных** - удаление пользователей, импортированных при синхронизации с LDAP. При этом не удаляются пользователи, изначально созданные в **Платформе Радар**.
- **Отвязать пользователей** - принудительная отвязка пользователей от службы каталогов. По отвязанным пользователям в дальнейшем не будет доступна синхронизация со службой каталогов.
- **Настройка маппинга** - переход к настройке Keycloack, позволяет задать сопоставление полей Keycloack полям LDAP.

2.2.7. Вкладка "Доступ к данным"

На вкладке "**Доступ к данным**" отображаются права доступа пользователей и групп пользователей к разделам **Платформы Радар** (см. рисунок 24).

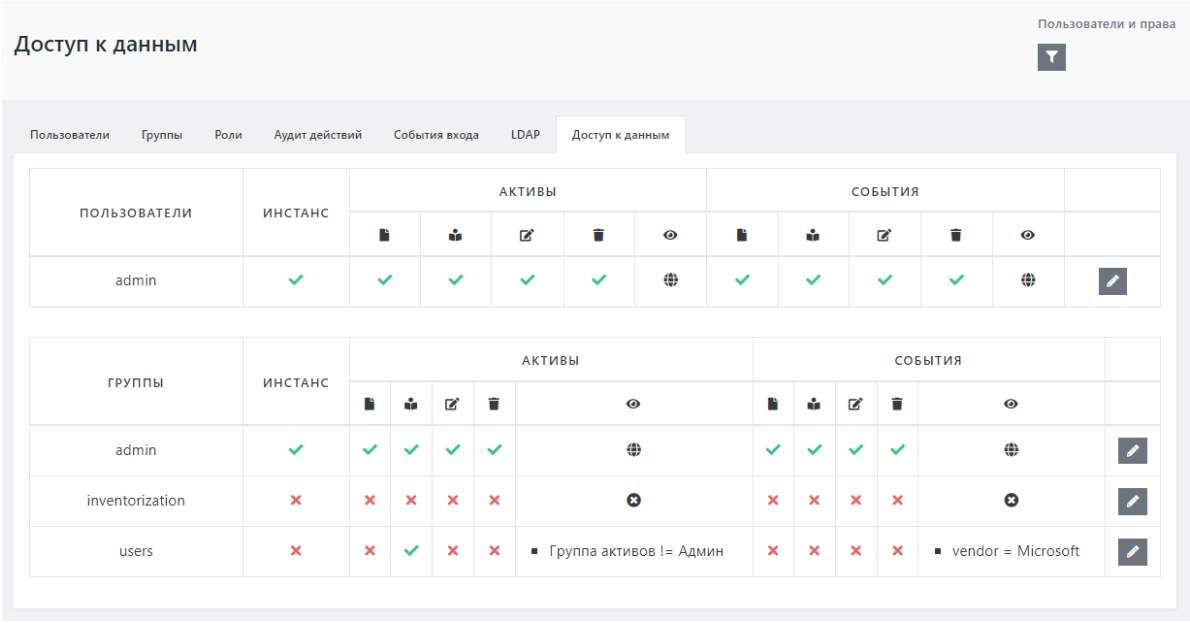

Рисунок 24 - Экран просмотра доступа к Платформе

2.2.7.1. Просмотр правил доступа

По умолчанию раздел содержит две таблицы: таблица доступа для пользователей и таблица доступа для групп пользователей.

В каждой таблице отображается доступ к:

- инстансу
- активам
- событиям

Иконки доступа обозначают:

- - доступ разрешен
- - доступ запрещен

Для активов и событий доступ разделен по видам действий:

- - доступ к созданию
- - доступ к просмотру
- - доступ к редактированию
- - доступ к удалению

Помимо этого иконкой опредедяются правила доступа:

- - доступ предоставлен ко всем активам или событиям
- - правила доступа не определены
- правила доступа перечислены в ячейке

Иконка фильтрации откроет окно фильтров просмотра доступа к данным (см. рисунок 25).

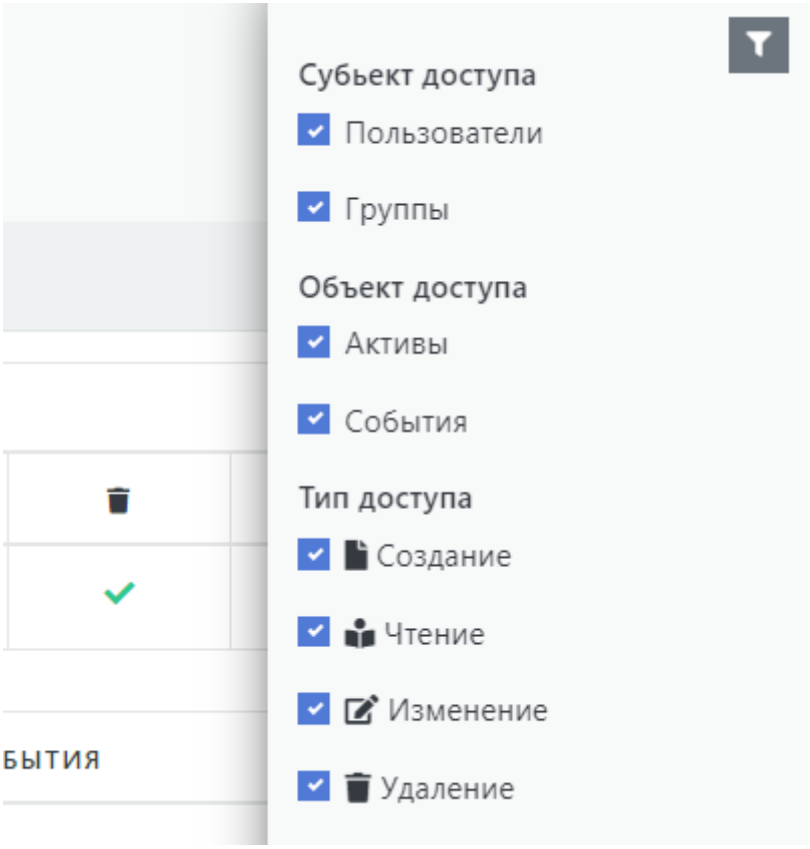

Рисунок 25 - Фильтры просмотра доступа к данным

2.2.7.2. Редактирование правил доступа к данным

Для редактирования правил доступа к данным кликните иконку напротив выбранного пользователя или группы пользователей, в результате чего откроется окно редактирования правил доступа (см. рисунок 26).

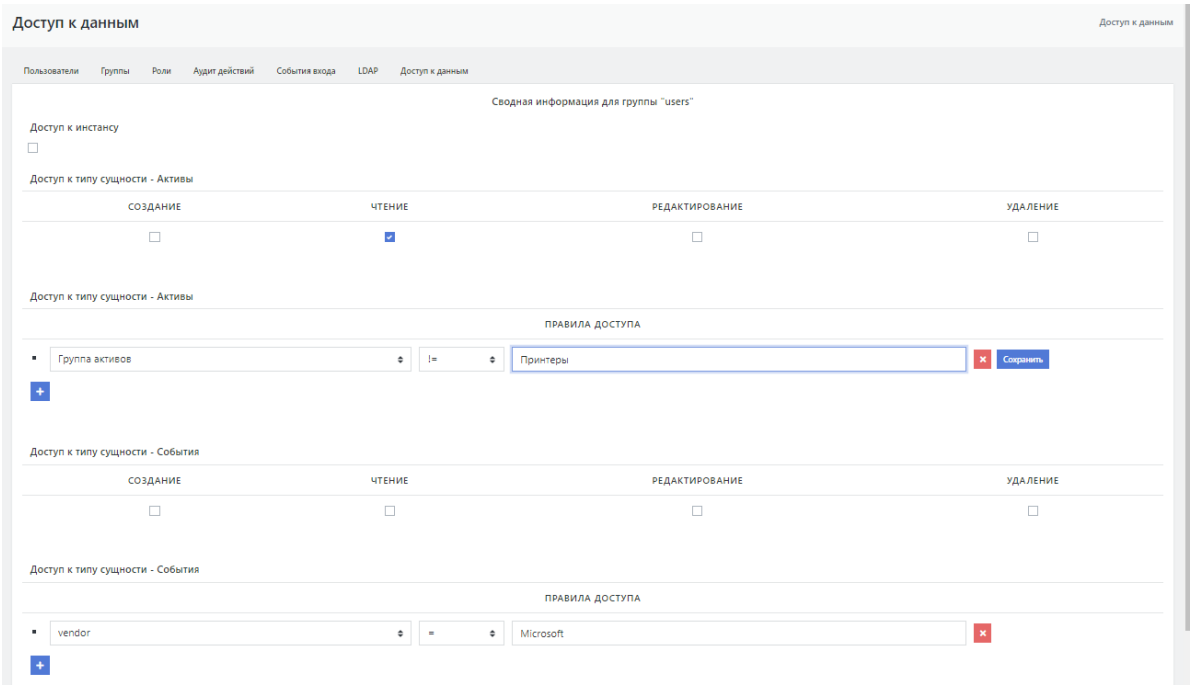

Рисунок 26 - Экран редактирования правила доступа к данным

При редактировании правил доступа настраиваются:

- доступ к инстансу
- доступ к активам и событиям:

- создание
- чтение
- редактирование
- удаление

Помимо этого, для активов и событий доступно управление правилами доступа.

Иконка  позволяет добавить новое правило.

Иконка  удаляет правило.

Каждое правило выглядит следующим образом

Выбранное правило равно/не равно *значение*

Правило выбирается из списка.

Для активов доступны:

- **Актив**
- **Группа активов**

Для событий доступно:

- **vendor** - наименование вендора
- **subsystem** - наименование подсистемы
- **product** - наименование продукта
- **name** - наименование события
- **application** - наименование приложения
- **fqdn** - наименование домена
- **hostname** - наименование хоста в сети
- **ip** - ip-адрес хоста в сети

Значение задается вручную.

После ввода значений правила сохраните его нажатием на кнопку **Сохранить**.

3. Управление кластером Платформы

3.1. Управление кластером Платформы

Раздел «Кластер» предоставляет инструментарий для упрощенного управления Платформой без необходимости подключения к серверам через терминальные соединения.

Раздел предоставляет следующие возможности (см. рисунок 27):

- управление узлами кластера и контроль состояния узлов;
- управление скриптами установки и конфигурационные файлами сервисов;
- управление учетными записями для сбора данных, протоколами и API ключами;
- планирование задач;
- управление конфигурацией;
- управление мультиарендностью.

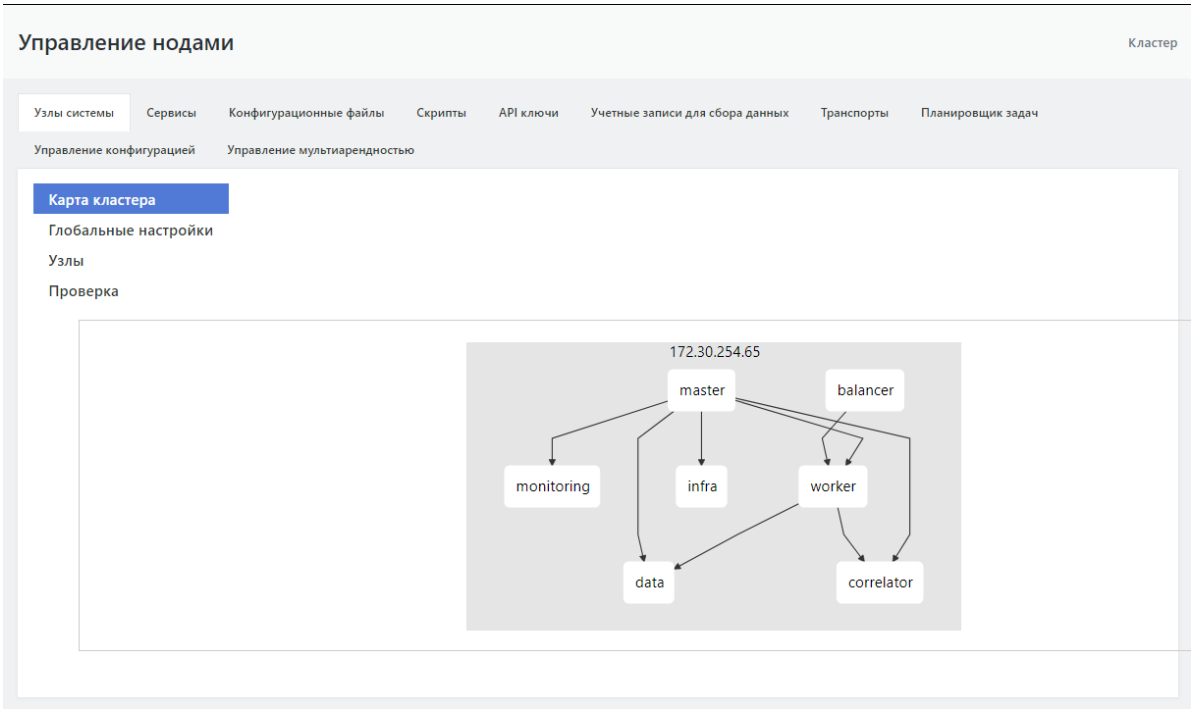

Рисунок 27 - Главный экран раздела «Кластер»

3.1.1. Концепция кластера Платформы Радар

Кластер Платформы Радар состоит из трех составляющих:

- Агент управления узлом кластера;
- Менеджер управления агентами;
- Интерфейс управления менеджером.

На каждый узел кластера необходимо установить Агент управления, через который будет осуществляться управление и контроль состояния узла.

Интерфейс и Менеджер управления агентами должны находиться на одном сервере, по умолчанию они находятся на сервере с ролью MASTER.

3.1.2. Добавление узла кластера

Для добавления нового узла должно быть соблюдено несколько подготовительных условий:

- Узел развернут и готов принимать внешние соединения.
- На узле установлена ОС - Debian 10 x64.
- На узле поднят ssh сервер.
- Узел разрешает соединения под привилегированным пользователем root с паролем.

После установки Агента сервер может быть закрыт для подключения по ssh с паролем. При установке Агента на сервер прописывается доверенный сертификат мастер-сервера для подключения без ввода пароля. Пароль в системе не сохраняется.

Для добавления узла и начала установки Агента на узел необходимо выполнить следующие действия :

1. На вкладке "Узлы системы" выбрать подраздел "Узлы" (см. рисунок 28).
2. Заполнить форму "Добавление нового узла". Все поля формы обязательны к заполнению.
3. Для создания кластера нажать на кнопку "Добавить".
4. Присвоить новому кластеру одну или несколько ролей, указав их в области "Добавление ролей к узлам". Для добавления роли необходимо выбрать нужную роль из списка и нажать

либо на кнопку «+», либо на кнопку «Добавить все» (см. Рисунок 28).

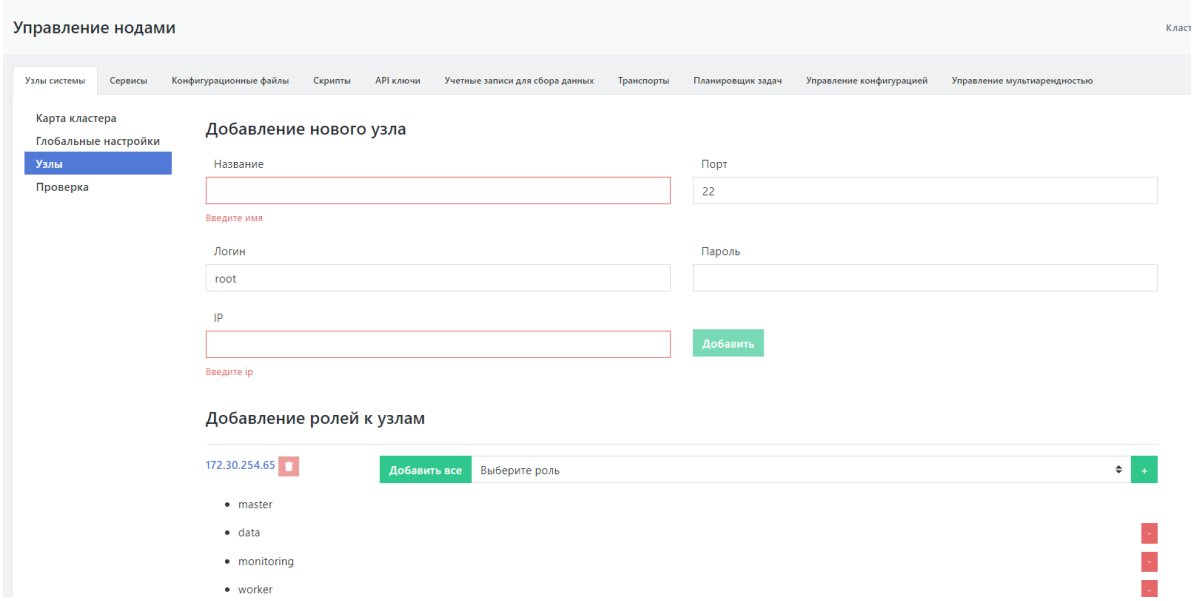

Рисунок 28 - Экран добавления узла Платформы

По умолчанию все необходимое программное обеспечение для узла регулируется ролью, закрепленной за узлом.

После добавления узла назначение ему роли и установки Агента станет доступно управление узлом кластера, расположенное на специальном экране "Управление хостом <адрес хоста>". Данный экран содержит функции редактирования роли кластера.

3.1.3. Управление узлом кластера

3.1.3.1. Экран управления узлом, общее описание

Управление узлом кластера осуществляется на отдельном экране интерфейса, перейти на который возможно следующим способом:

- из подраздела "Узлы", область "Добавление ролей к узлам" при нажатии на название узла (IP-адреса, см. рисунок 28) ;
- из подраздела «Проверка» - нажать на кнопку «Настройка» рядом с названием узла (см. рисунок 29).

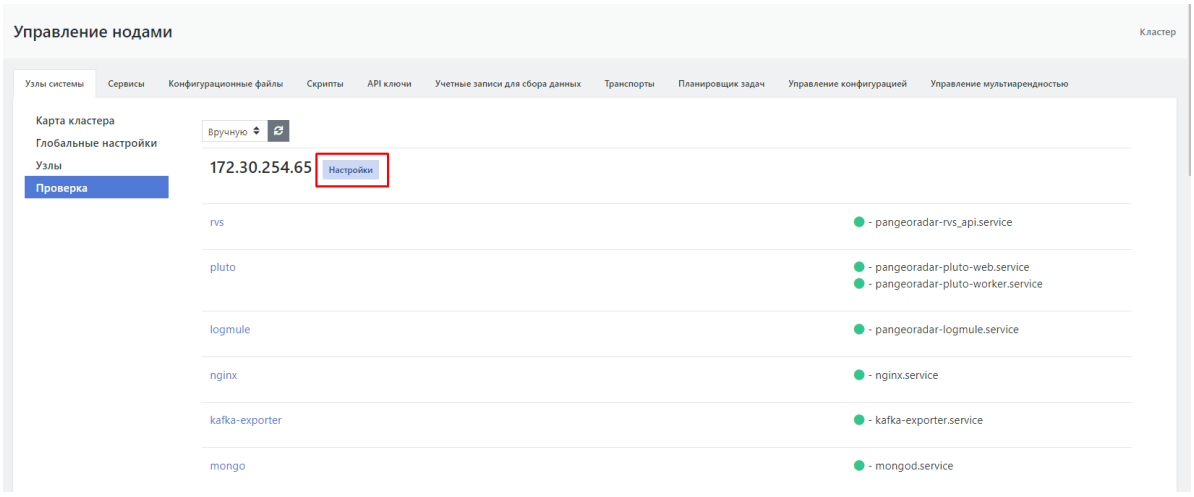

Рисунок 29 - Переход на экран управления узлом кластера из подраздела "Проверка"

Экран управления узлом предоставляет следующие возможности (см. рисунок 30):

- управление серверными ролям узла;
- управление сервисами узла;
- контроль состояния работы сервисов;
- контроль работы узла;
- выполнение скриптов на узле.

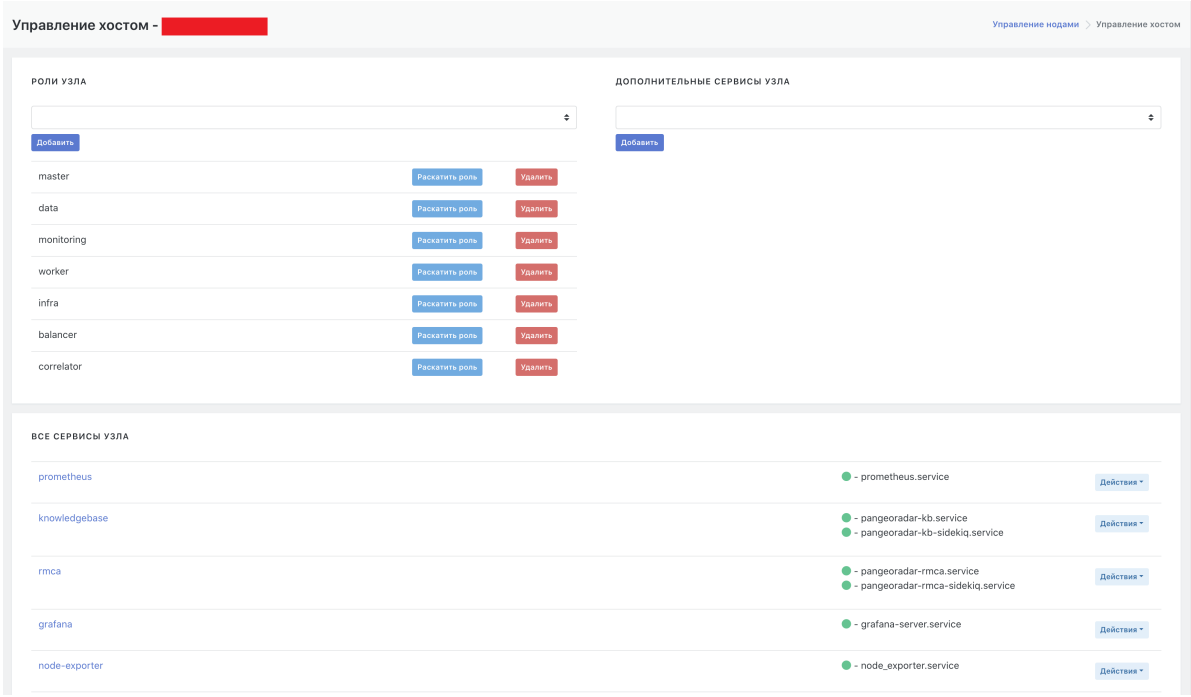

Рисунок 30 - Экран управления узлом

3.1.3.2. Управление сервисами узла кластера

Функции управления сервисами расположены в области "Все сервисы узла" (см. рисунок 30). Каждый сервис узла кластера может предоставить информацию о своем статусе и последних логах. Для получения информации необходимо нажать на кнопку «Действия» и выбрать соответствующий пункт меню (см. рисунок 31). Также через данное меню доступны:

- переустановка сервиса;
- перезапуск сервиса.

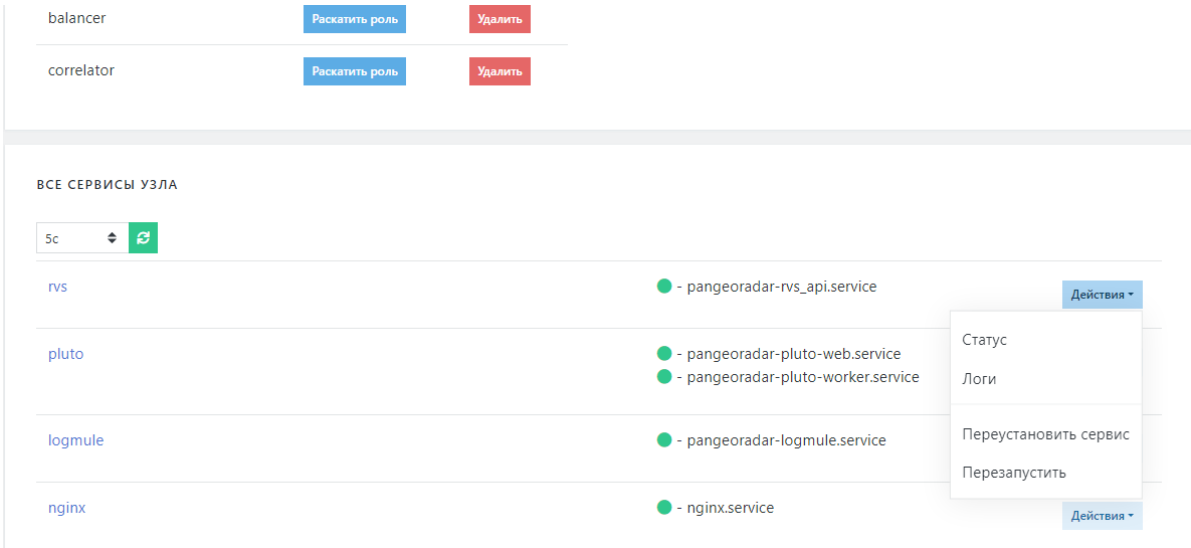

Рисунок 31 - Информация о статусе и последних логах выбранного узла кластера

3.1.3.3. Установка сервиса на узел кластера

Для установки на узел отдельно выбранного сервиса (не рекомендуется так делать) на экране управления узлом кластера необходимо выполнить следующие действий:

1. В области "Дополнительные сервисы узла" выбрать в раскрывающемся списке дополнительных сервисов необходимый сервис (см. рисунок 32).
2. Нажать на кнопку «Добавить». Сервис добавится в общий список сервисов на узле в области "Все сервисы узла" .
3. В строке нового сервиса нажать на кнопку «Действия» и в раскрывшемся меню выбрать функцию «Переустановить сервис» (см. рисунок 31). Дождаться завершения процесса.
4. В строке нового сервиса нажать на кнопку «Действия» и в раскрывшемся меню выбрать функцию «Обновить конфиг» (см. рисунок 31). Дождаться завершения процесса.

В процессе переустановки сервиса будет показан лог действий установщика.

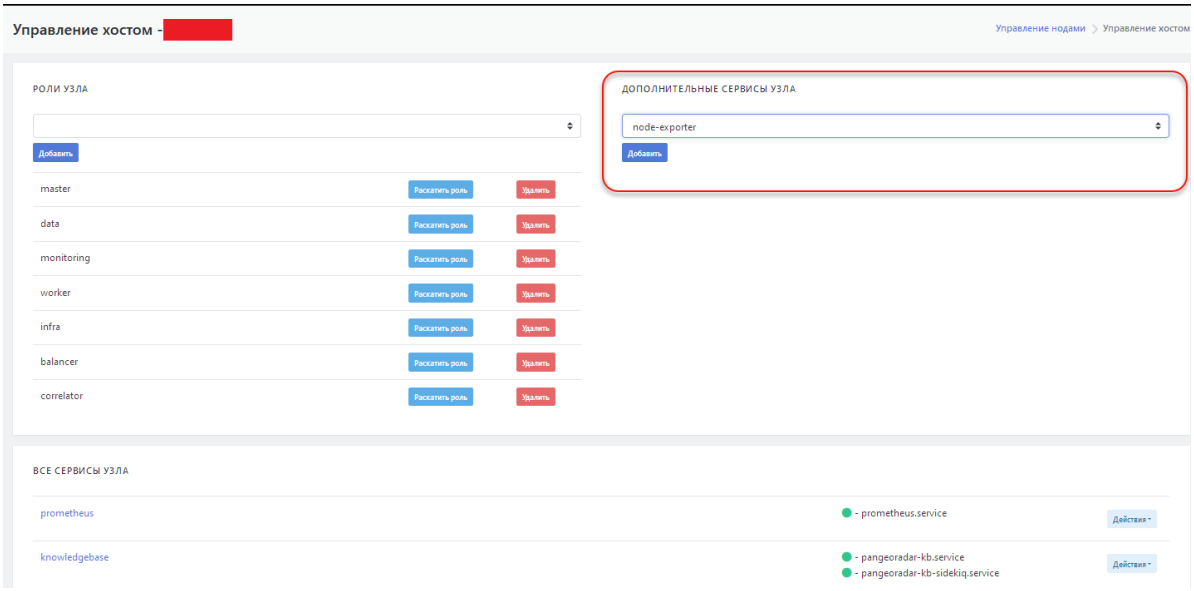

Рисунок 32 - Выбор дополнительного сервиса

3.1.3.4. Установка серверной роли на узел кластера

Рекомендуется использовать серверные роли как абстракцию установки программного обеспечения на узел кластера.

На экране управления узлом кластера для присвоение новой роли узлу необходимо выполнить следующие действия (см. рисунок 33):

1. В области "Роли узла" в раскрывающемся списке выбрать нужную роль.
2. Нажать на кнопку «Добавить». Выбранная роль будет добавлена к списку ниже.
3. В строке добавленной роли нажать на кнопку «Раскатить роль» для запуска процесса установки на узел кластера ПО, соответствующего роли.

Процесс установки представлен в виде обновляемого лога установки.

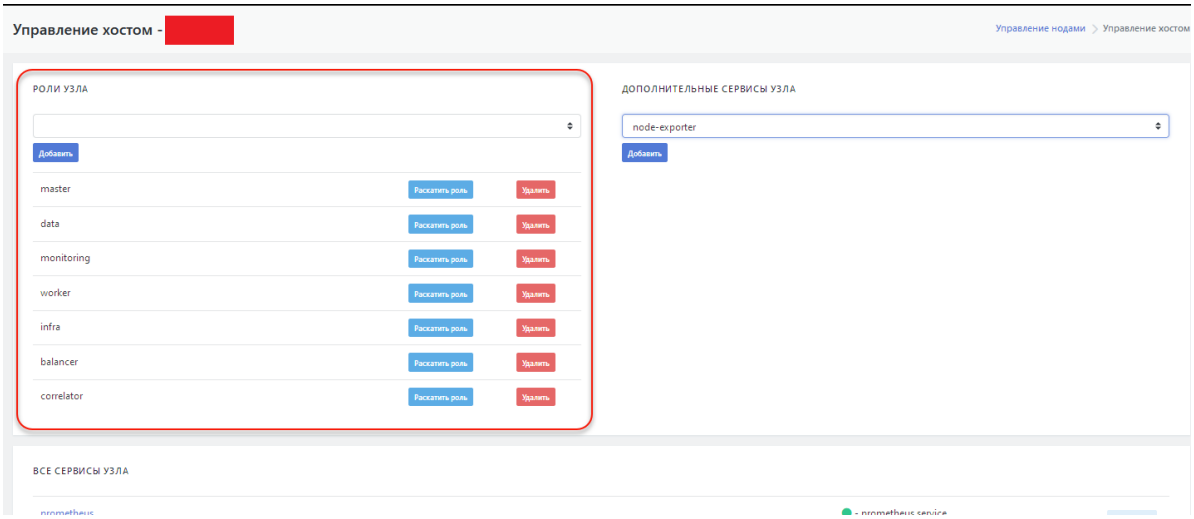

Рисунок 33 - Установка серверной роли на узел кластера

3.1.4. Управление сервисами

3.1.4.1. Набор сервисов, добавление/удаление сервисов

В интерфейсе Платформы Радар набор доступных сервисов платформы отображается в разделе "Управление кластером" на вкладке "Сервисы" в виде таблицы. Область справа от таблицы позволяет добавлять новые сервисы (см. рисунок 34).
Можно удалить существующий сервис из таблицы нажав на кнопку "Удалить" в строке соответствующего сервиса.

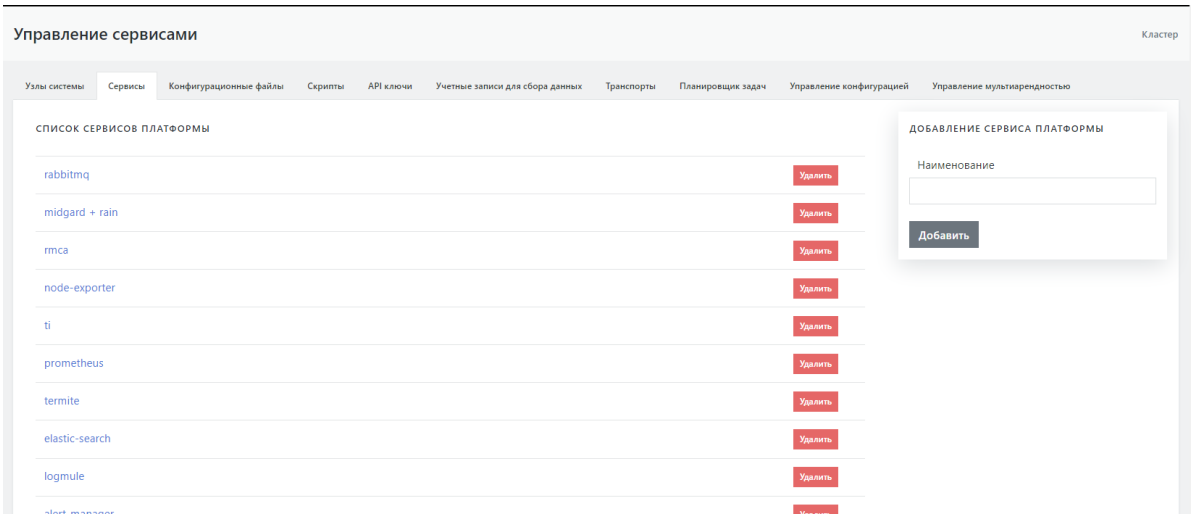

Рисунок 34 - Набор сервисов Платформы

3.1.4.2. Экран управления сервисами

При выборе в таблице интересующего сервиса открывается экран управления данным сервисом, который содержит следующие области задач (см. рисунок 35):

- область "**Ассоциирован с ролями**" - обеспечивает настройку списка ролей, с которыми ассоциирован данный сервис;
- область "**Ассоциированные конфиги**" - обеспечивает настройку списка конфигурационных файлов, ассоциированных с данным сервисом;
- область "**Доступные скрипты**" - содержит перечень скриптов, доступных для данного сервиса;
- область "**Ассоциирован с узлами**" - содержит список названий (ролей) кластерного узла с которыми ассоциирован данный сервис.

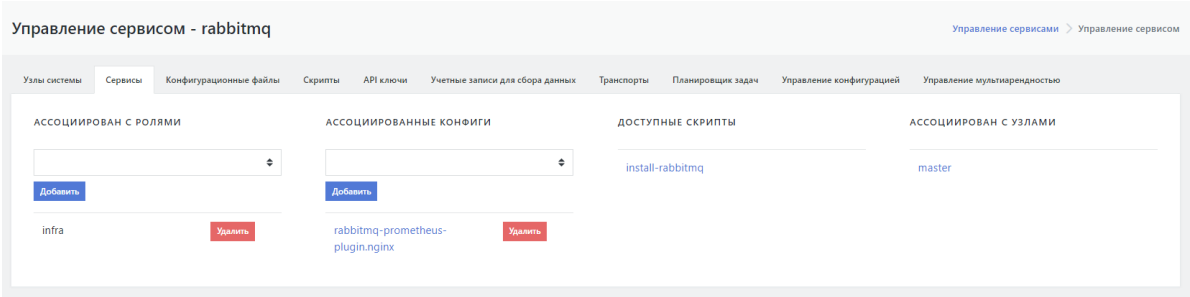

Рисунок 35 - Экран управления сервисами

3.1.4.3. Настройка списка ролей, с которыми ассоциирован сервис

Для проведения ассоциации сервиса с новой ролью необходимо:

1. Перейти на вкладку «Сервисы».
2. Выбрать нужный сервис в таблице. Откроется форма настроек сервиса (см. рисунок 36).
3. В области "**Ассоциирован с ролями**" и выбрать нужную роль в раскрывающемся списке.
4. Нажать кнопку «Добавить».

Указанная роль отобразится в списке ролей, с которыми ассоциирован выбранный сервис.

Для удалении роли из списка нажать на кнопку "Удалить" в строке данной роли.

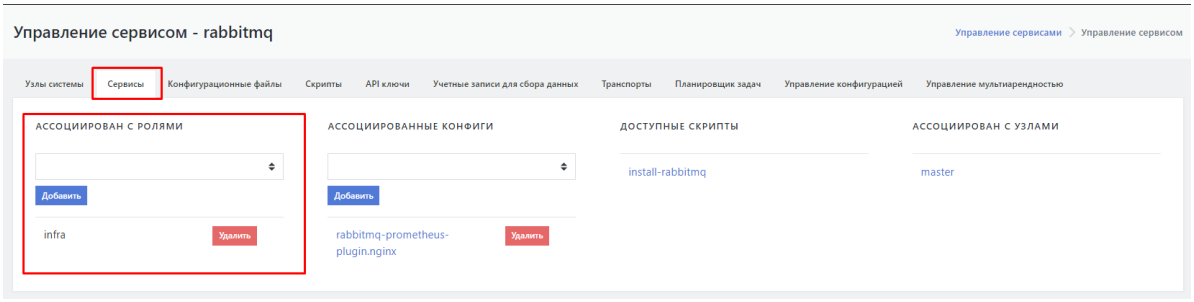

Рисунок 36 - Область настройки ролей, с которыми ассоциирован сервис

3.1.4.4. Настройка списка конфигурационных файлов, ассоциированных с сервисом

Для ассоциации конфигурационного файла с сервисом, необходимо:

1. Перейти на вкладку «Сервисы».
2. Выбрать нужный сервис в таблице. Откроется форма настроек сервиса (см. рисунок 37).
3. Выбрать настройку «**Ассоциированные конфиги**» и выбрать нужный конфигурационный файл в раскрывающемся списке.
4. Нажать кнопку «Добавить».

Выбранный конфигурационный файл отобразится в списке конфигурационных файлов, ассоциированных с сервисом.

Для удаления конфигурационного файла из списка нажать на кнопку "Удалить" в строке данного файла.

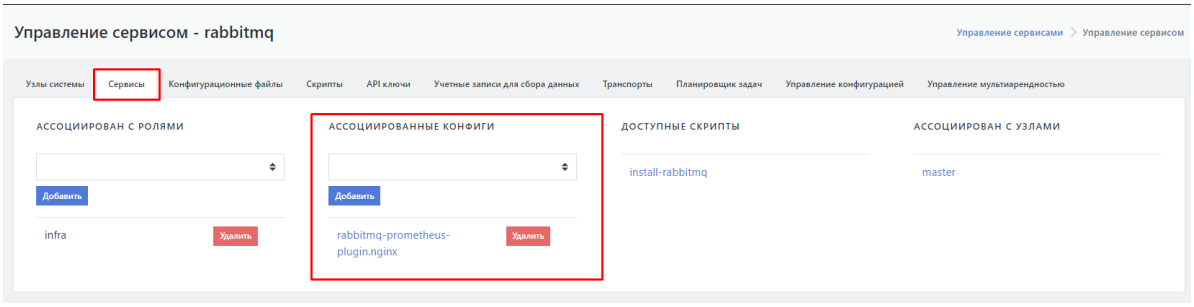

Рисунок 37 - Область настройки конфигурационных файлов ассоциированных с сервисом

3.1.5. Управление конфигурационными файлами кластера

3.1.5.1. Набор конфигурационных файлов, добавление/удаление файлов

Внимание! Не рекомендуется вносить изменения в конфигурационные файлы без консультации с разработчиками.

Все конфигурационные файлы сервисов Платформы лежат по адресу: /opt/pangeoradar/configs/.

В интерфейсе Платформы Радар данный набор конфигурационных файлов отображается в разделе "Управление кластером" на вкладке "Конфигурационные файлы" в виде таблицы. Область справа от таблицы позволяет переопределить конфигурационные файлы по умолчанию из этой или вложенных директорий путем создания одноименных файлов (см. рисунок 38).

В названии файла допускается использовать относительный путь от директории хранения конфигурационных файлов, например - termite/test.conf.

Для удаления конфигурационного файла из списка нажать на кнопку "Удалить" в строке интересующего файла.

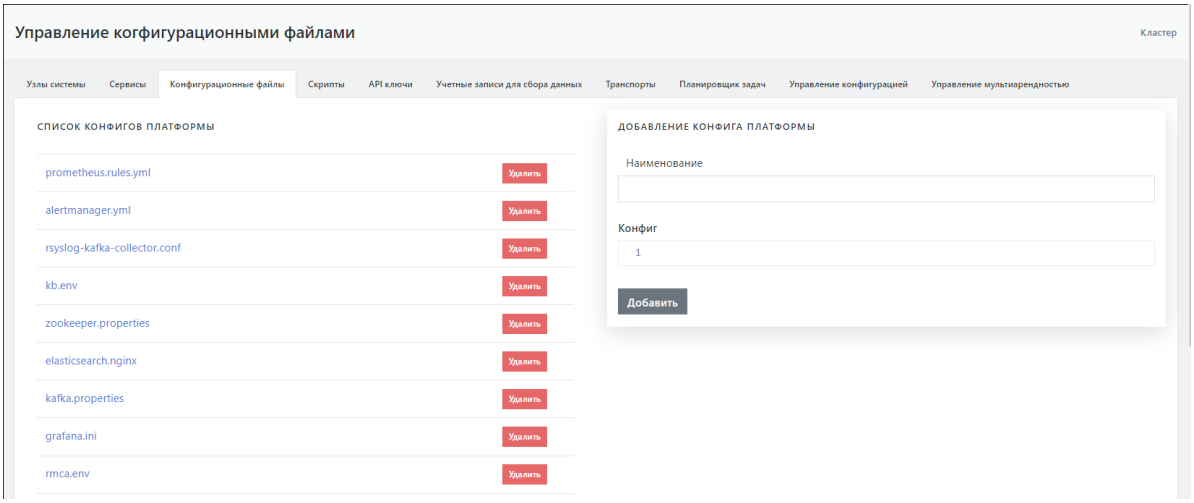

Рисунок 38 - Набор конфигурационных файлов Платформы

3.1.5.2. Экран редактирования конфигурационного файла

Внимание! Не рекомендуется вносить изменения в конфигурационные файлы без консультации с разработчиками.

При необходимости текст конфигурационного файла можно отредактировать. Для это надо надо выбрать интересующий файл в списке конфигурационных файлов. На экране откроется текст выбранного файла, доступный для редактирования (см. рисунок 39). Введенные изменения сохраняются при нажатии на кнопку "Изменить".

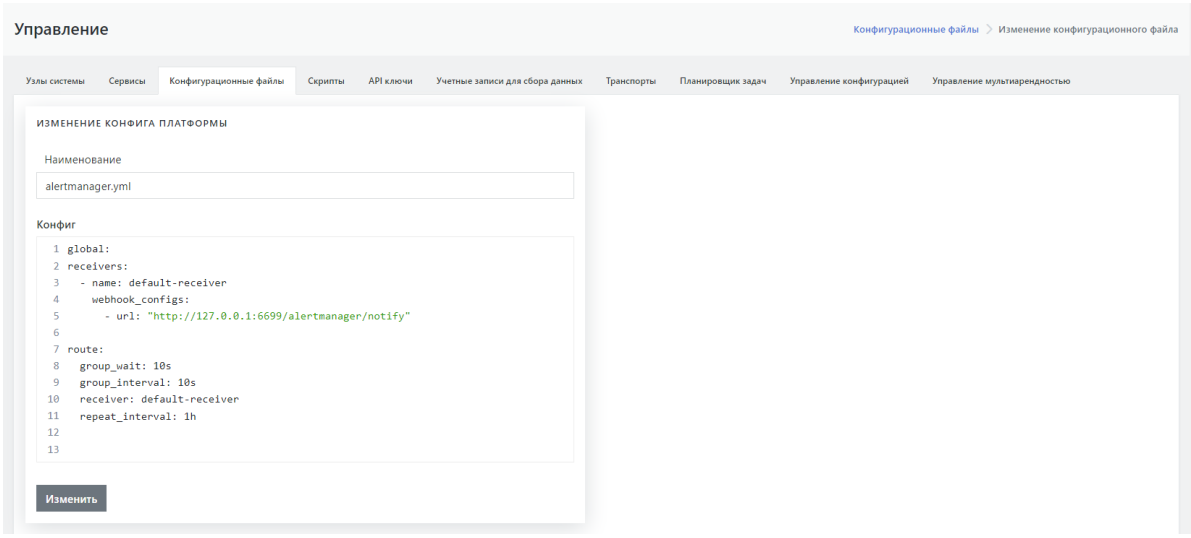

Рисунок 39 - Редактирование конфигурационного файла Платформы

3.1.6. Управление инсталляционными скриптами кластера

3.1.6.1. Набор скриптов, добавление/удаление скриптов

Внимание! Не рекомендуется вносить в скрипты изменения без консультации с разработчиками.

Инсталляционные скрипты необходимы при установке или переустановке сервисов.

Языком описания скрипта является bash.

В интерфейсе Платформы Радар набор скриптов отображается в разделе "Управление кластером" на вкладке "Скрипты" в виде таблицы. Область справа от таблицы позволяет переопределить скрипты по умолчанию (см. рисунок 40).

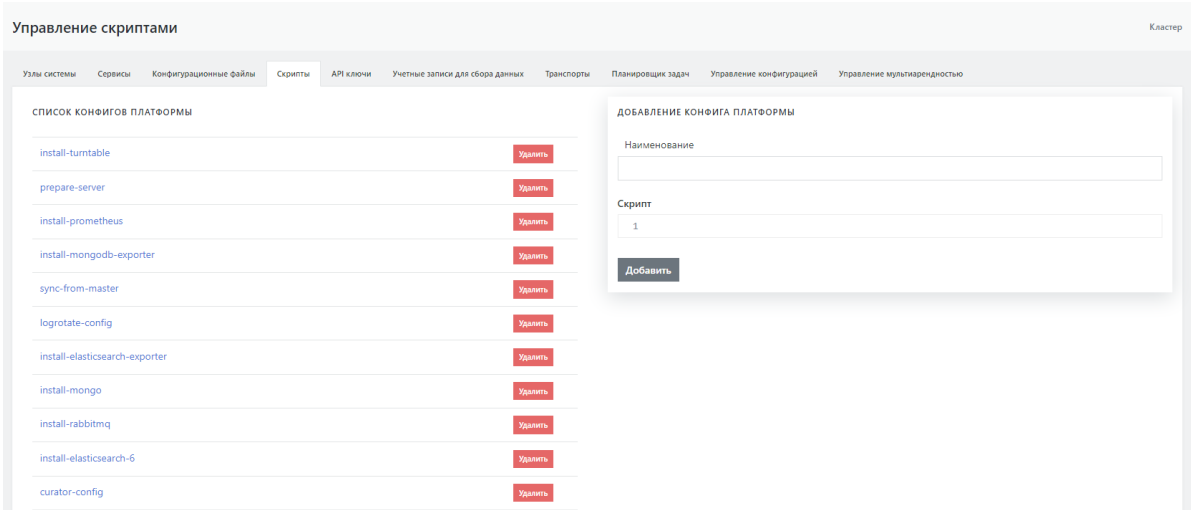

Рисунок 40 - Набор скриптов Платформы

3.1.6.2. Экран редактирования скрипта

При выборе в таблице интересующего скрипта открывается экран управления данным скриптом, который содержит следующие области задач (см. рисунок 41):

- слева расположен текст выбранного скрипта, доступный для редактирования.;
- область "**Ассоциация скрипта с ролью**" - обеспечивает ассоциацию скрипта с ролью, выбранной из раскрывающегося списка;
- область "**Ассоциация скрипта с сервисом**" - содержит список сервисов, с которыми ассоциирован данный скрипт на текущий момент, и раскрывающийся список сервисов, с которыми можно провести ассоциацию данного скрипта.

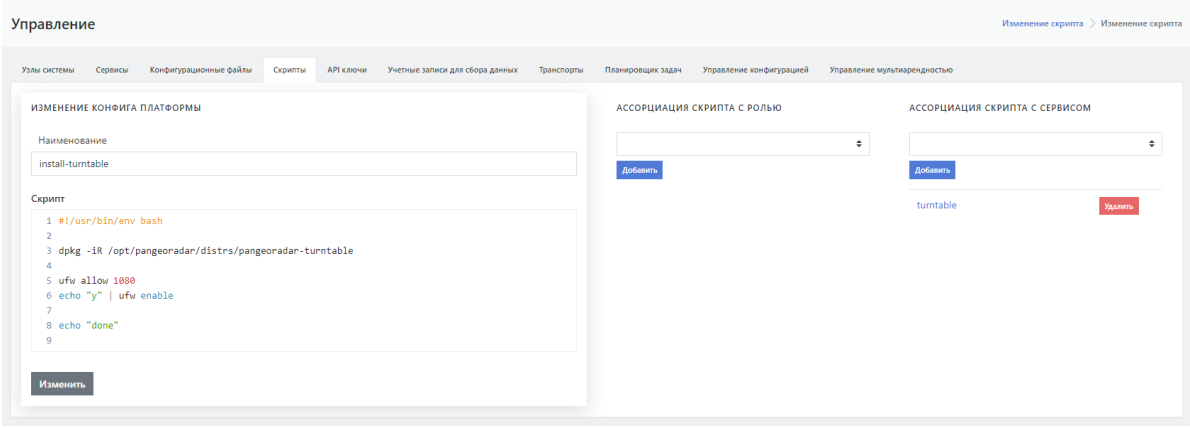

Рисунок 41 - Редактирование скрипта Платформы

3.1.7. Управление API ключами кластера {#apikey}

Доверенные ключи API используются для меж-сервисного взаимодействия. Управление ключами API реализовано на вкладке "API ключи". Экран содержит (см. рисунок 42):

- текущий список API ключей;
- область добавления новых ключей.

Не рекомендуется удалять ключ global_api_key во избежание потери работоспособности Платформы.

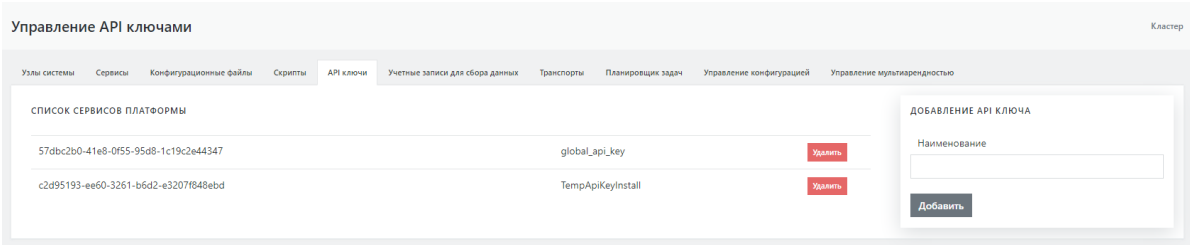

Рисунок 42 - Управление API ключами

3.1.8. Управление учетными записями для сбора данных

На вкладке "Учетные записи для сбора данных" реализовано управление авторизационными данными для сборщика данных с хостов при процедуре инвентаризации. Вкладка содержит (см. рисунок 43):

- область "**Список учетных записей**" - текущий список учётных записей;
- область **"Добавление учетной записи"** - содержит форму для введения параметров новой учетной записи.

Изменение созданной записи не предусмотренно. Возможно только удаление и повторное создание.

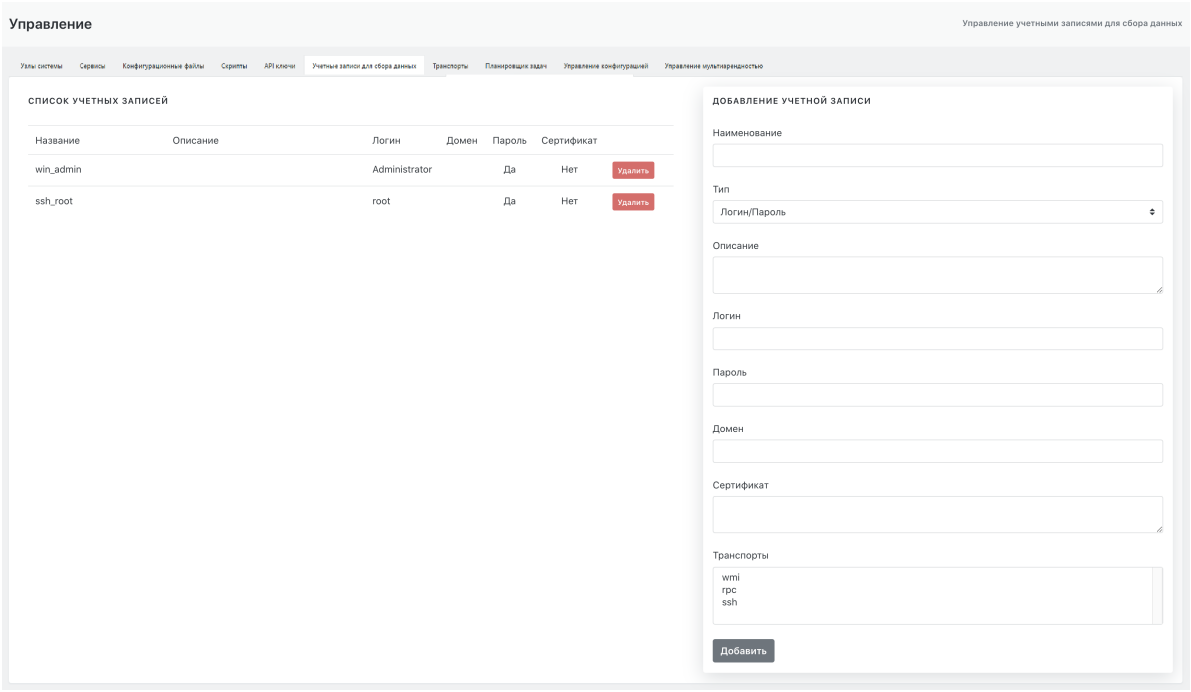

Рисунок 43 - Управление списком учетных записей для сбора данных

3.1.9. Управление транспортами сбора данных

Внимание! Не рекомендуется вносить изменения в набор транспортов без консультации с разработчиками.

На вкладке "Транспорт" реализовано управление словарем для формы добавления учетных записей для сбора данных. Вкладка содержит (см. рисунок 44):

- область "**Список транспортов платформы**" - текущий список транспортов с возможностью удаления транспорта из списка;
- область **"Добавление транспорта"** - содержит форму для добавления нового транспорта .

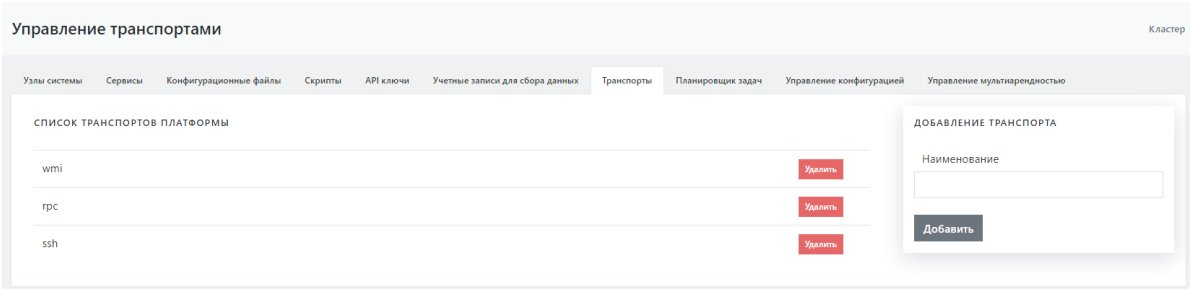

Рисунок 44 - Управление транспортами сбора данных

3.1.10. Планировщик задач {#cluster_plan}

На вкладке "Планировщик задач" реализовано управление перечнем задач, запускаемых по расписанию через CRON (см. рисунок 45).

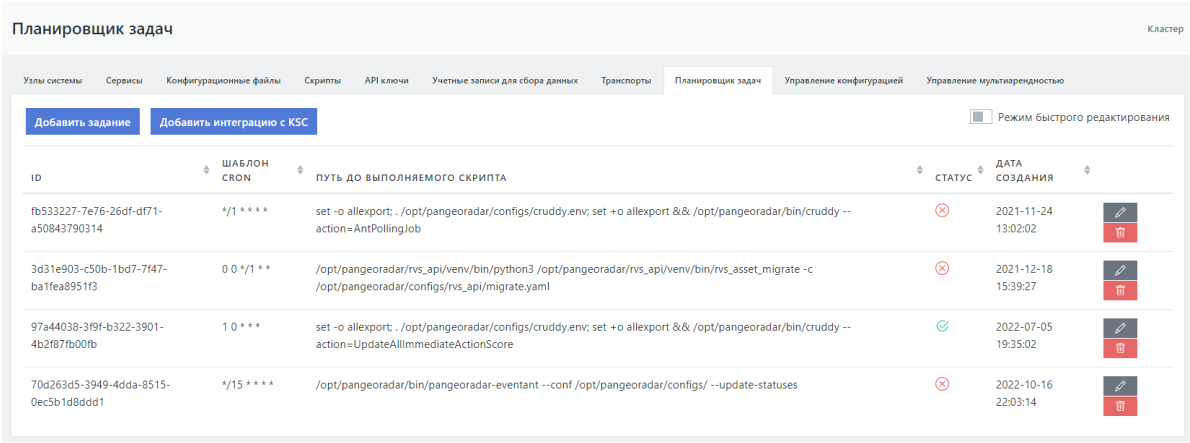

Рисунок 45 - Планировщик задач

Вкладка содержит:

- кнопку "**Добавить задание**", позволяющую добавить новое задание для планировщика CRON;
- кнопку "**Добавить интеграцию с KSC**", позволяющую добавить задание на интеграцию с KSC (Kaspersky Security Center) для инвентаризации активов, ПО на активах, аппаратной части активов;
- переключатель "**Режим быстрого редактирования**", который позволяет включить или выключить режим быстрой смены активности заданий;
- таблицу с заданиями.

В таблице располагается информация о заданиях:

- идентификатор задания;
- шаблон CRON;
- путь до выполняемого скрипта;
- иконка активности задания (- задание активно, - задание не активно);
- дата создания задания;
- иконки управления заданием (- редактирование задания, - удаление задания). Для задания интеграции с KSC дополнительно отображается иконка - просмотр лога интеграции, который становится доступным после первой синхронизации.

3.1.10.1. Добавление задания

Для добавления задания кликните кнопку "**Добавить задание**" (см. рисунок 46).

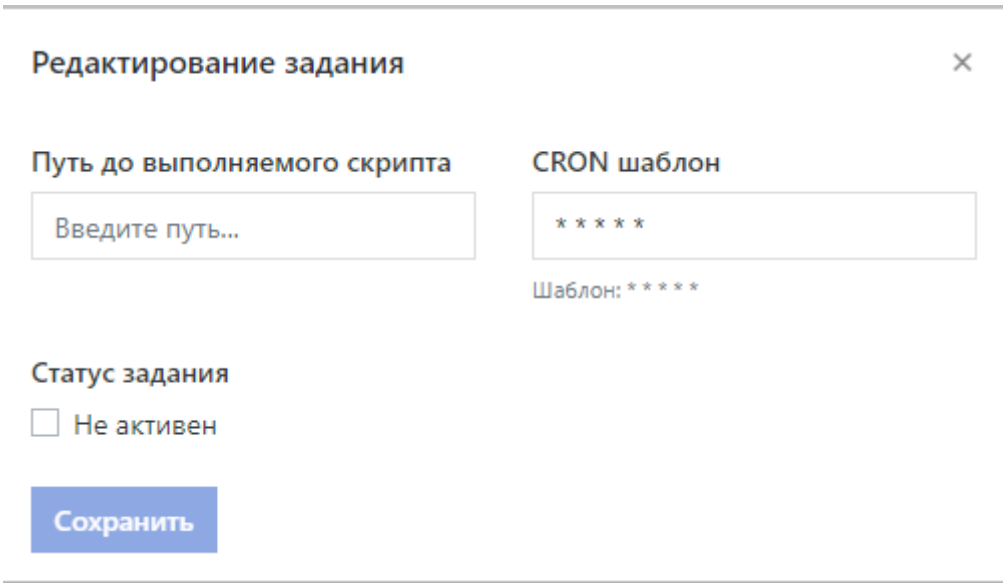

Рисунок 46 - Добавление задания

В открывшемся окне укажите **Путь до выполняемого скрипта** и **CRON шаблон**.
Для запрета выполнения задания установите признак **Не активен**.
После клика по кнопке **Сохранить** задание будет добавлено в список заданий.

3.1.10.2. Добавление интеграции с KSC (Kaspersky Security Center)

Для добавления задачи на интеграцию с KSC кликните кнопку "**Добавить интеграцию с KSC**" (см. рисунок 47).

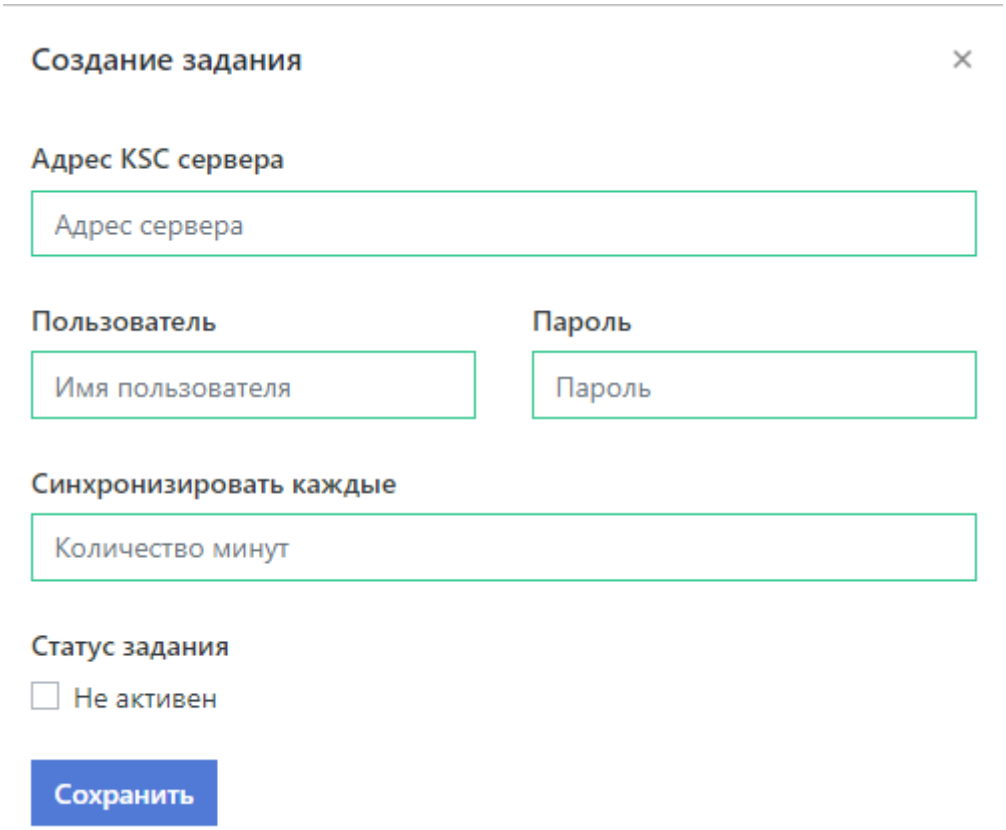

Рисунок 47 - Добавление интеграции с KSC

В открывшемся окне заполните параметры:

- **Адрес KSC сервера**. Формат http(s)://<server_name>:<port_number>
- **Пользователь**. У пользователя должны быть права на доступ по API к серверу администрирования KSC.
- **Пароль**. При вводе будет маскирован.
- **Синхронизировать каждые**. Значение интервала синхронизации в минутах.

Для запрета выполнения интеграции с KSC установите признак **Не активен**.
После клика по кнопке **Сохранить** задача на интеграцию с KSC будет добавлена в список заданий.

3.1.11. Управление конфигурацией {#cluster_config}

На вкладке "Управление конфигурацией" доступно управление конфигурационными параметрами Платформы в целом и параметрами каждого отдельного модуля Платформы (см. рисунок 48).

Внимание! Не рекомендуется вносить правки непосредственно в конфигурационные файлы, так как все настройки, представленные на вкладке, хранятся в БД. При записи конфигурации конфигурационные файлы перезаписываются значениями, сохраненными в БД.

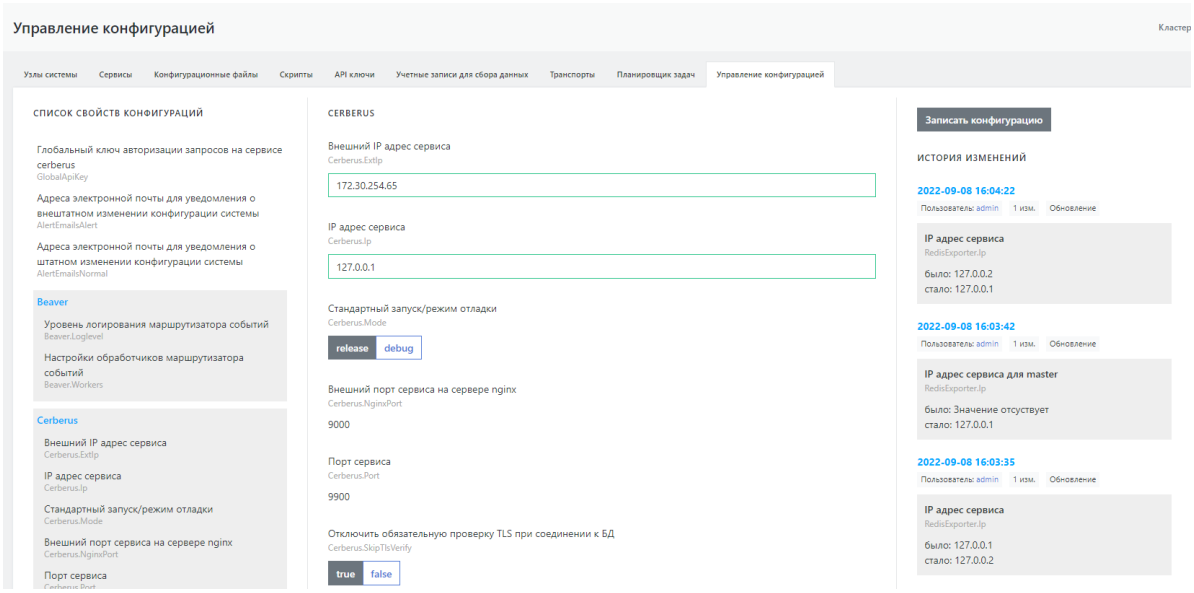

Рисунок 48 - Управление конфигурацией

На вкладке доступно изменение параметров Платформы в целом (глобальный ключ авторизации, адреса электронной почты для уведомлений) или изменение параметров отдельных модулей Платформы.

Перечень параметров и модулей Платформы располагается в левой части вкладки.

В средней части отображаются выбранные параметры. Если выбран модуль, то будут отображены и доступны для редактирования все параметры модуля (отображаются списком со скроллингом вниз). Если выбран отдельный параметр модуля, то будет отображен и доступен для редактирования только он.

После внесения изменений в конфигурацию параметров в правой части будет отображена история внесения изменений. Кликните по дате и времени изменения, чтобы отобразить детали изменения. Повторный клик скроет детали.

> При изменеии паролей в истории будет отображаться не значение пароля, а его хэшсумма.

После клика на кнопку "**Записать конфигурацию**" модули с измененными параметрами будут перезапущены.

Подробнее об управлении конфигурацией описано в документе "**Управление конфигурацией Платформы**"

3.1.12. Управление мультиарендностью {#multi}

На вкладке "Управление мультиарендностью" задается перечень инстансов **Платформы радар** (см. рисунок 49).

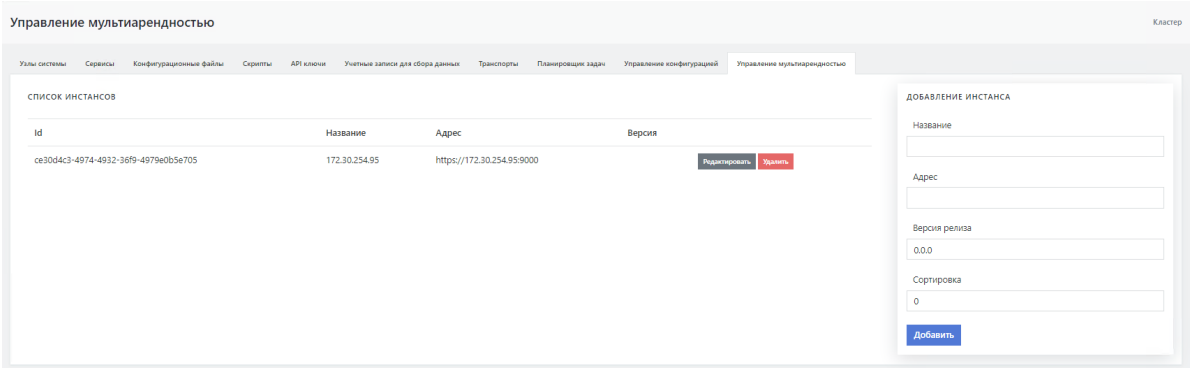

Рисунок 49 - Управление конфигурацией

Для добавления нового инстанса задайте его наименование, версию установленной на нем **Платформы Радар** и адрес. Поле "Сортировка" определяет сортировку в перечне от меньшего значения поля сортировки к меньшему.

Отредактировать данные инстанса можно, нажав на кнопку "Редактировать", рядом с ним. Кнопка "Удалить" удалит инстанс из перечня.

4. Управление источниками событий

4.1. Управление источниками событий

4.1.1. Общее описание

Раздел "Источники" отвечает за управление подключением источников событий к Платформе.

Содержит следующие вкладки:

- **Источники**
- **Правила разбора**
- **Правила нормализации**
- **Правила обработки**
- **Grok паттерны**

4.1.2. Управление источниками

Вкладка "Источники" обеспечивает выполнение следующих действий(см. рисунок 50):

- Добавление нового источника.
- Включение и отключение существующего.
- Изменение параметров существующего источника.
- Синхронизация конфигурации со всеми сервисами Платформы.
- Экспорт выбранных источников в файл архива формата ZIP.
- Импорт источников из файла архива формата ZIP.
- Удаление выбранных источников.

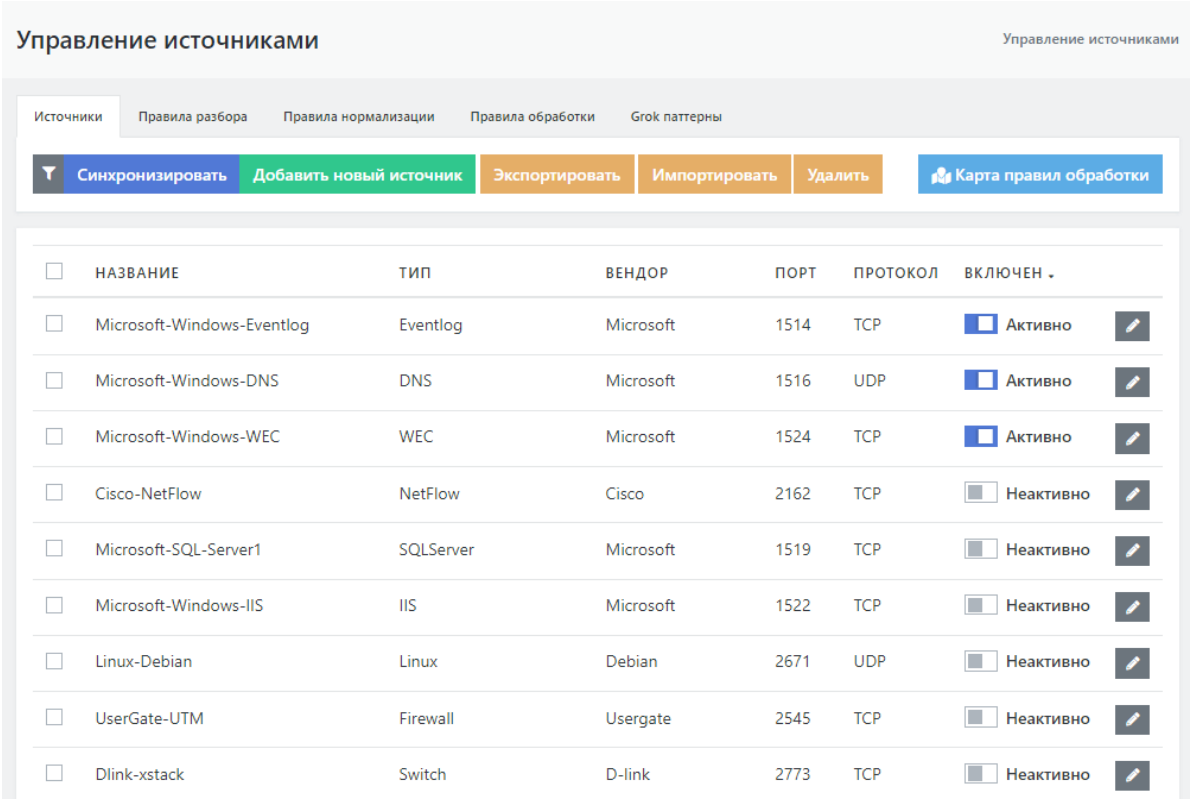

Рисунок 50 - Вкладка "Источники"

Подробная инструкция по управлению источниками приведена в отдельном разделе "Руководство по подключению источников".

4.1.3. Контроль состояния источников

Подраздел «Состояние источников» в разделе «Источники» отвечает за мониторинг состояния источников событий и создание
уведомлений (как внутрисистемных, так и на электронную почту) в случае остановки потока событий на источнике в указанный диапазон времени (см. рисунок 51).

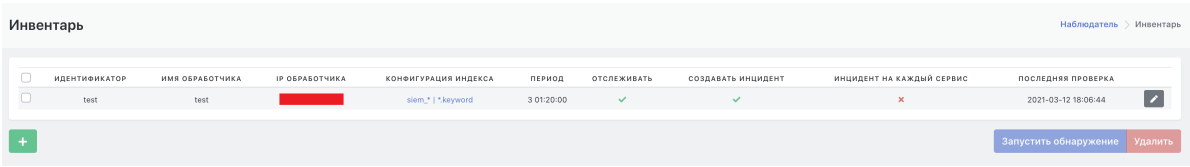

Рисунок 51 - Данные по состоянию источников

Подробная инструкция по Контролю состояния источников приведена в отдельном разделе "Руководство по подключению источников".

5. Мониторинг работы Платформы

5.1. Общее описание

Раздел интерфейса **"Мониторинг"** содержит наборы интегрированных в интерфейс Платформы Радар приборных панелей (дашбордов) Grafana. В Платформе организованы следующие наборы приборных панелей (см. рисунок 52):

- **Общий мониторинг** — мониторинг основных параметров Платформы;
- **Поток событий** — мониторинг параметров потока событий;
- **MongoDB** — мониторинг параметров СУБД MongoD;
- **RabbitMQ** — мониторинг параметров брокера сообщений RabbitMQ;
- **Kafka** — мониторинг параметров системы обмена сообщениями Kafka;
- **ElasticSearch** — мониторинг параметров поисковой системы ElasticSearch;
- **Статистика потока** - мониторинг показателей обработки потока событий

Необходимый набор приборных панелей выбирается из раскрывающегося списка (см. Рисунок 52).

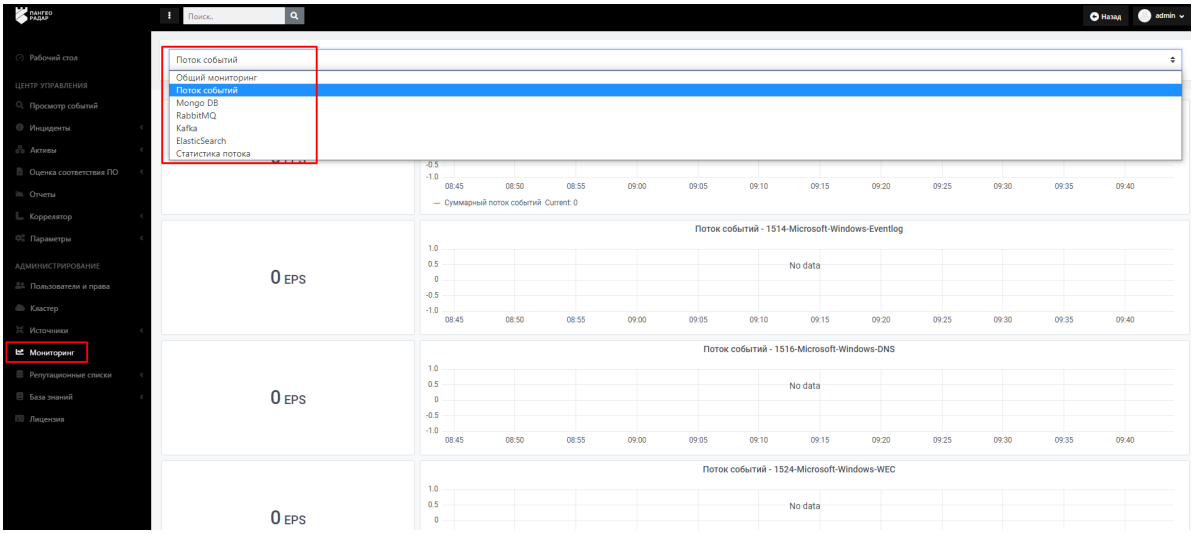

Рисунок 52 - Выбор набора приборных панелей

В разделе **"Мониторинг"** доступно переключение между встроенными в систему приборными панелями без необходимости заходить в интерфейс Grafana.

> Grafana относится к свободно распространяемому ПО. Подробную информацию о продукте можно посмотреть на сайте https://grafana.com/.

5.2. Набор приборных панелей «Общий мониторинг»

Набор приборных панелей **Общий мониторинг** предназначен для мониторинга основных параметров работы Платформы, таких как (см. рисунок 53):

- мониторинг метрик потребления памяти — виджеты *Ram Used* (текущее потребление памяти), *Memory Basic* (график потребления памяти).
- мониторинг метрик загрузки процессора — виджеты *CPU Busy* (текущая загрузка процессора), *CPU Basic* (график загрузки процессора).
- мониторинг метрик состояния дискового пространства — виджеты *Root FS Used* (текущее состояние дискового пространства), *Disk Space Used Basic* (график загрузки дискового пространства).

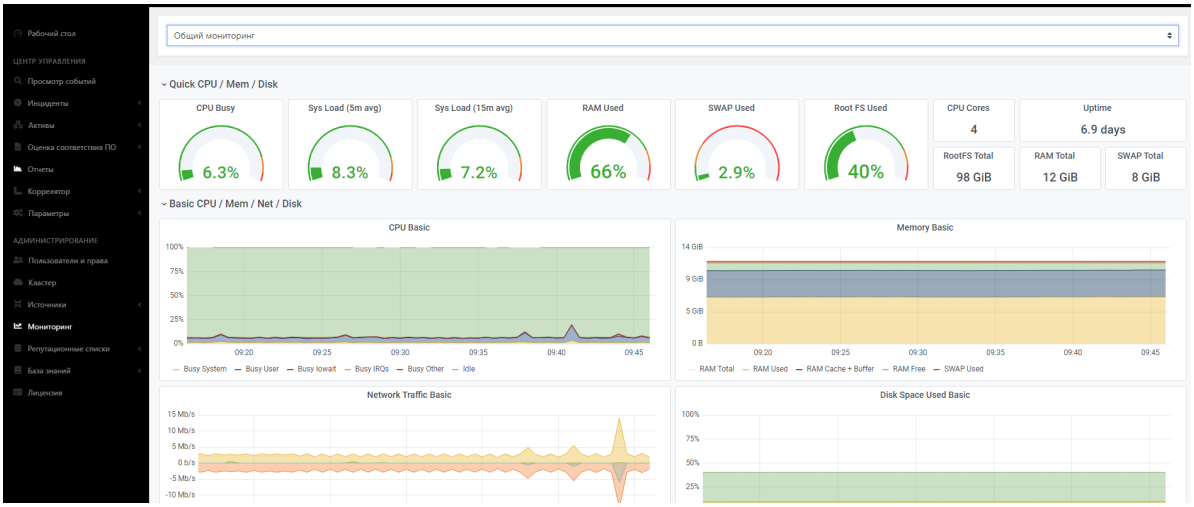

Рисунок 53 - Приборные панели из набора панелей "Общий мониторинг"

Предустановленный список приборных панелей в наборе **"Основной мониторинг"** приведен на рисунке 54. При щелчке по названию приборной панели можно открыть/скрыть набор графиков/диаграмм, входящих в приборную панель.

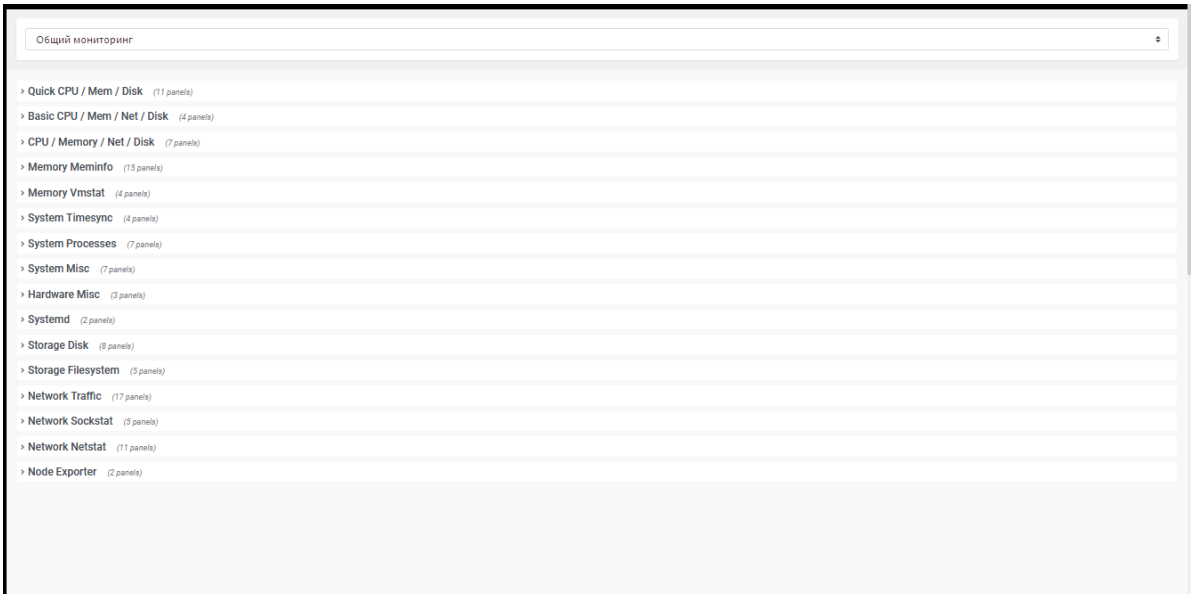

Рисунок 54 - Предустановленный список приборных панелей Платформы Радар

5.3. Приборная панель «Поток событий»

Приборная панель **Поток событий** предназначена для мониторинга метрик обрабатываемых событий в секунду (EPS) и содержит два типа виджетов (см. рисунок 55):

- виджет с отображением информации о текущем потоке событий (слева);
- виджет по потоку событий в виде линейных графиков, построенных на основе исторических данных (справа).

Первыми отображаются метрики текущего EPS в системе — **Суммарный поток событий** (см. рисунок 55). Далее следуют виджеты, где предоставляется информация по потокам от каждого из подключенных источников событий.

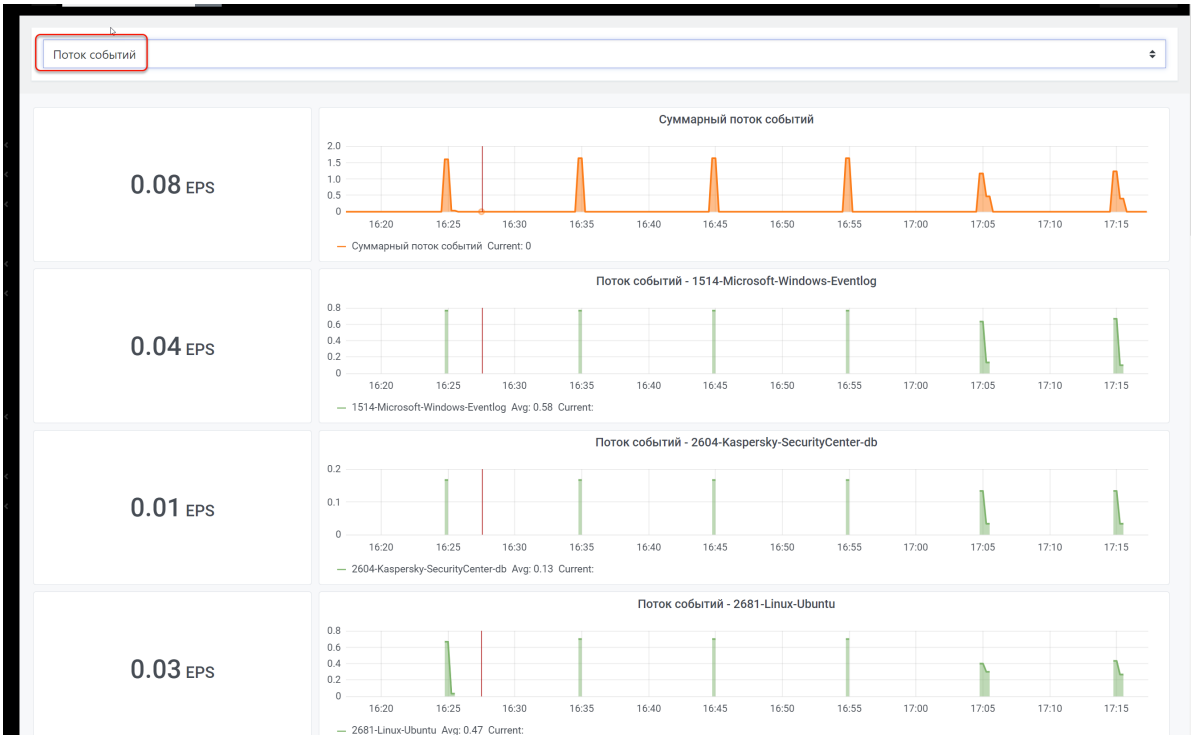

Рисунок 55 - Приборные панели из набора панелей "Суммарный поток событий"

5.4. Приборная панель «Статистика потока»

Приборная панель **Статистика потока** предназначена для мониторинга статистики потока событий и содержит два раздела (см. рисунок 56):

- общая статистика потока:
  - суммарная обработка событий (в EPS);
  - задержка разбора входящего потока событий;
  - задержка обработки событий на корреляцию;
  - задержка ответа обращения к табличным спискам;
  - график задержки разбора входящего потока событий по источнику.
- статистика обработчика событий:
  - график скорости чтения событий из балансировщика;
  - график общей производительности;
  - график скорости обработки событий по источнику;
  - график суммарного потока событий на этапе разбора;
  - график суммарного потока событий на этапе нормализации;
  - график суммарного потока событий на этапе обогащения;
  - график суммарного лага записи на хранение;
  - график суммарного потока событий на этапе корреляции.

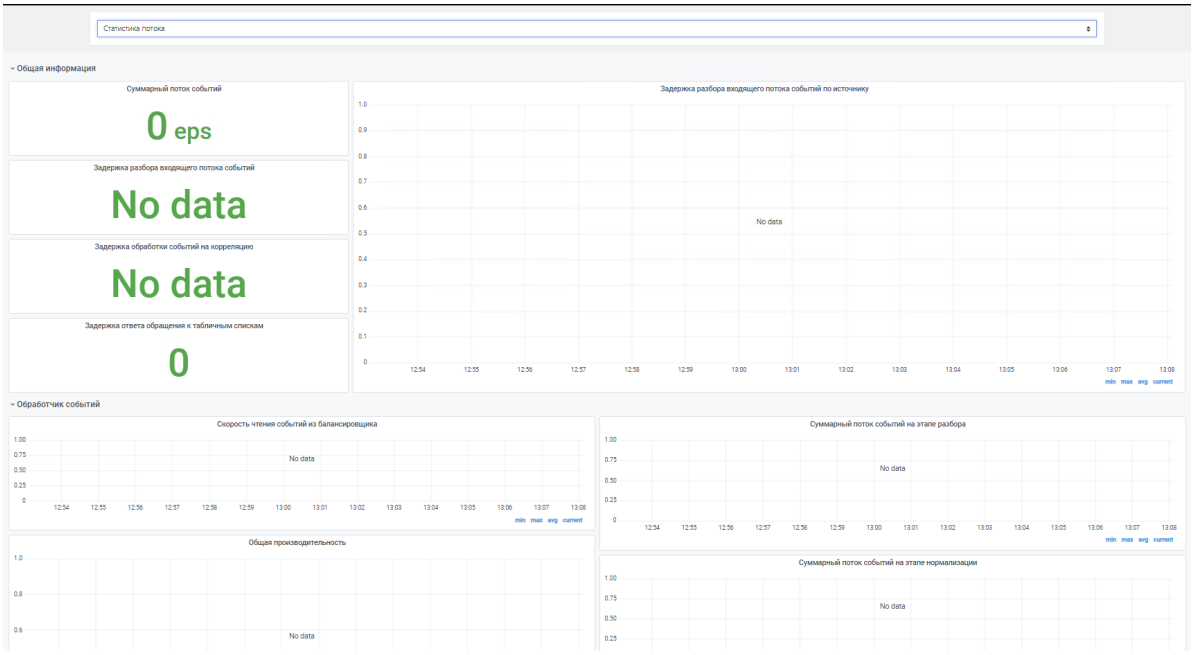

Рисунок 56 - Приборные панели из набора панелей "Статистика потока"

5.5. Работа с графиками и диаграммами приборных панелей

При щелчке справа от названия графика/диаграммы открывается меню (см. рисунок 57):

- "**View**" — раскрытие графика/диаграммы на весь экран Платформы.
- "**Share**" — поделиться панелью в виде прямой ссылки, снимка или встроенной ссылки.
- "**Inspect**" — корректировка запросов и устранение неполадок.
- "**More**" (toggle legend) — отображение/скрытие на графике легенды.

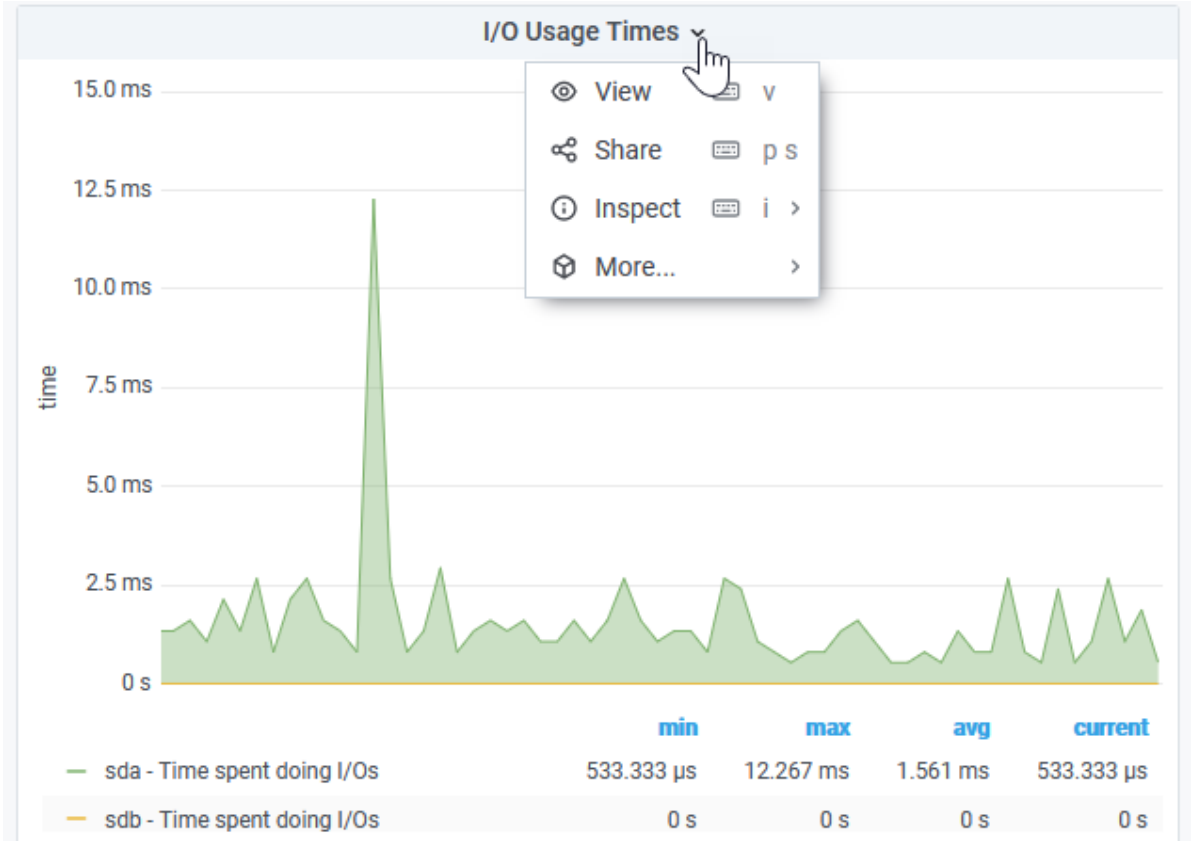

Рисунок 57 - Работа с графиком/ диаграммой

При наведении курсора на график открывается окно с данными точки, указанной курсором (см. рисунок 58).

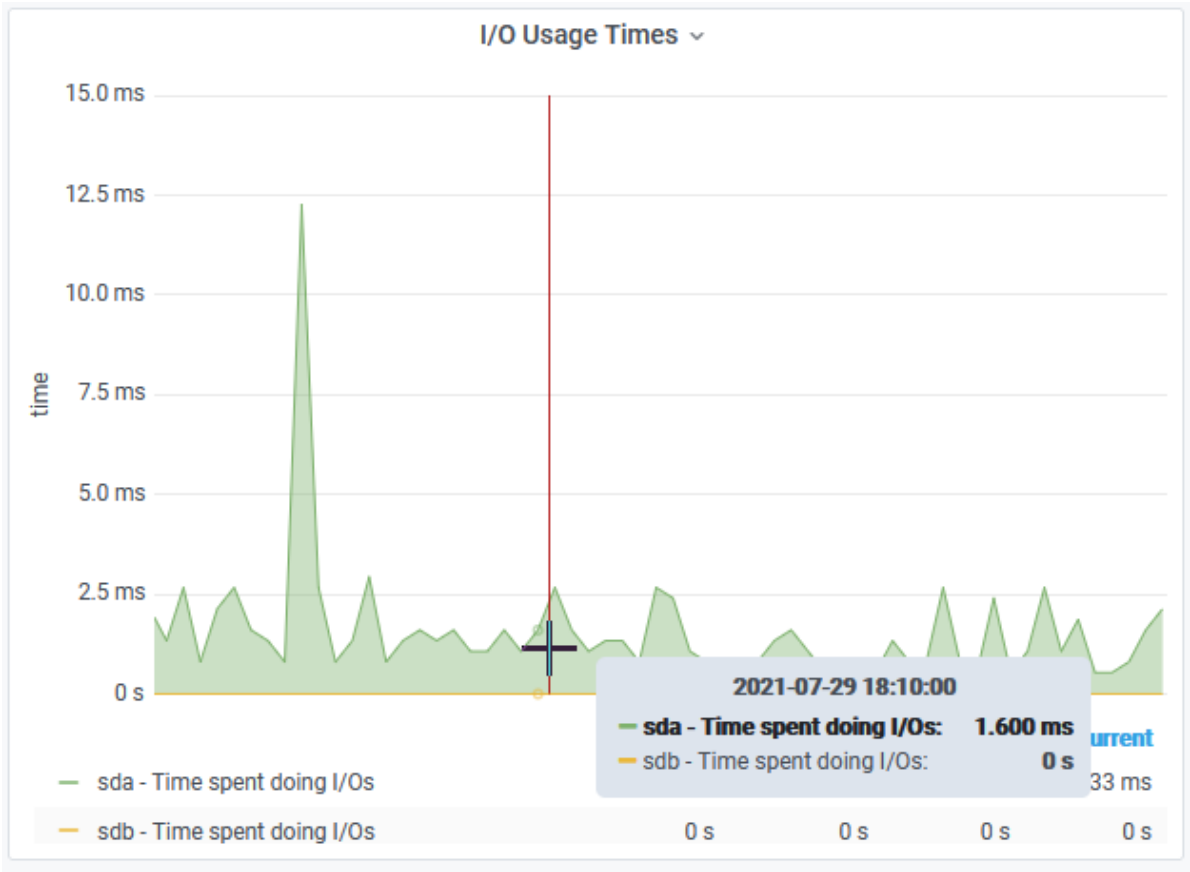

Рисунок 58 - Просмотр данных на графиках

5.6. Передача метрик производительности во внешние системы мониторинга

В Платформе предусмотрена возможность передачи метрик производительности во внешние системы мониторинга.

Платформа обеспечивает многострочный вывод метрик производительности в формате строки *Prometheus* (ключ, значение), что позволяет экспортировать метрики в систему Zabbix.

6. Репутационная база

6.1. Назначение репутационной базы

Данный модуль предназначен для обогащения событий данными, полученными из различных репутационных списков.

6.2. Состав репутационной базы

Репутационная база представлена службой `pangeoradar-ti-updater.service`

6.3. Работа с репутационными списками из UI

6.3.1. Репутационные списки

Для просмотра и управления репутационными списками необходимо перейти в раздел "Репутационные списки", "Репутационные списки".

На рисунке 59 изображено окно просмотра и управления репутационными списками.

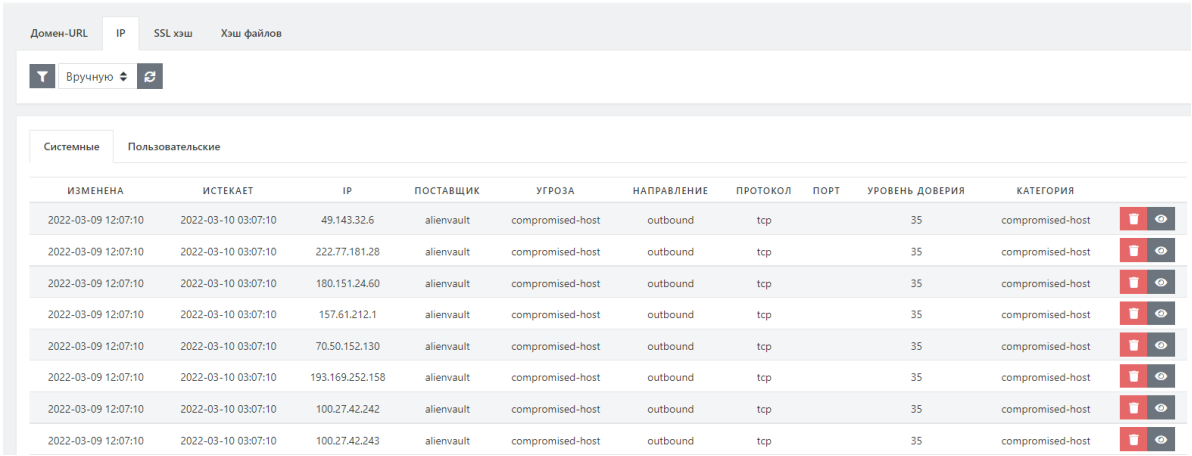

Рисунок 59 - Репутационные списки

В рассматриваемом интерфейсе присутствуют следующие функциональные возможности:

- Просмотр полного списка индикаторов компрометации;
- Фильтрация записей в репутационных списках;

  Для этого необходимо нажать на пиктограмму фильтра, выбрать поле, по которому необходимо отфильтровать записи, а также значение этого поля (полностью или частично), как изображено на рисунке 60.

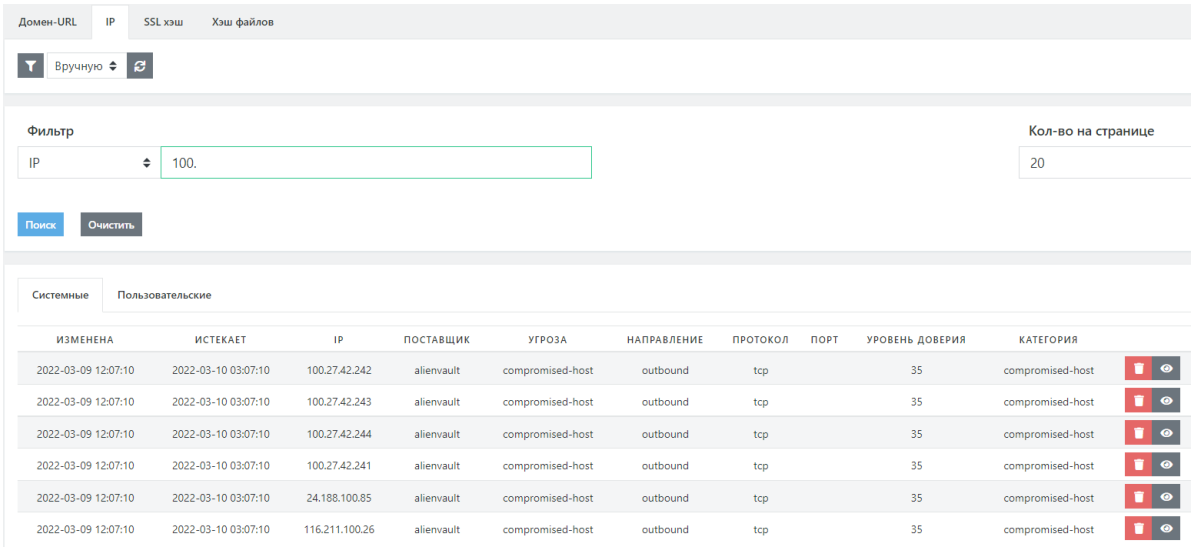

Рисунок 60 - Фильтрация репутационнных записей

- Создание пользовательских индикаторов компрометации;

  Для создания необходимо перейти во вкладку "Пользовательские", после чего нажать на кнопку "+".
  В открывшемся окне заполнить значения полей и нажать "Сохранить"

  Пример пользовательского индикатора компрометации представлен на рисунке 61

Рисунок 61 - Создание пользовательского индикатора компрометации

- Удаление индикаторов компрометации;

  Для удаления индикаторов компрометации необходимо нажать на пиктограмму урны справа от индикатора компрометации, который необходимо удалить.

6.3.2. Источники IOC

Для просмотра и управления источниками идентификаторов компрометации необходимо перейти в раздел "Репутационные списки", "Источники IOC".

На рисунке 62 изображено окно просмотра и управления источниками идентификаторов компрометации.

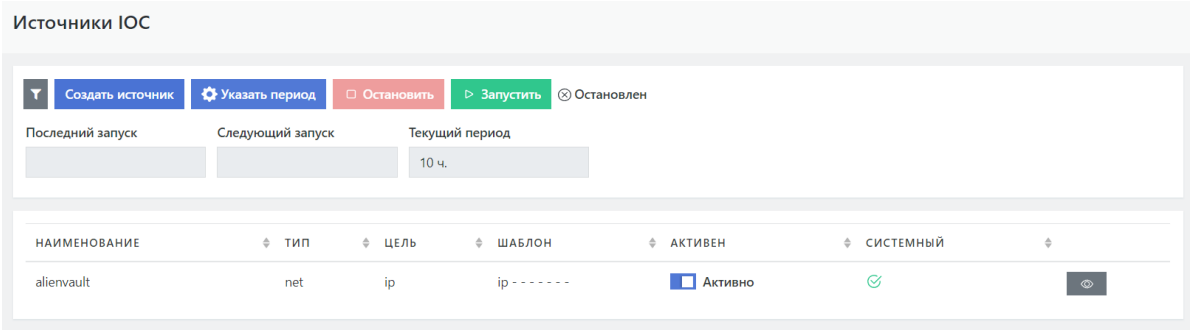

Рисунок 62 - Источники индикаторов компрометации

В рассматриваемом интерфейсе присутствуют следующие функциональные возможности:

- Включение встроенных источников идентификаторов компрометации;

  Для этого необходимо нажать на пиктограмму фильтра, перевести "Активность" в статус "Не важно".
  После, напротив нужных источников, нажать на кнопку-тумблер для перевода статуса в "Активно".
  Пример включения источника представлен на рисунке 63.

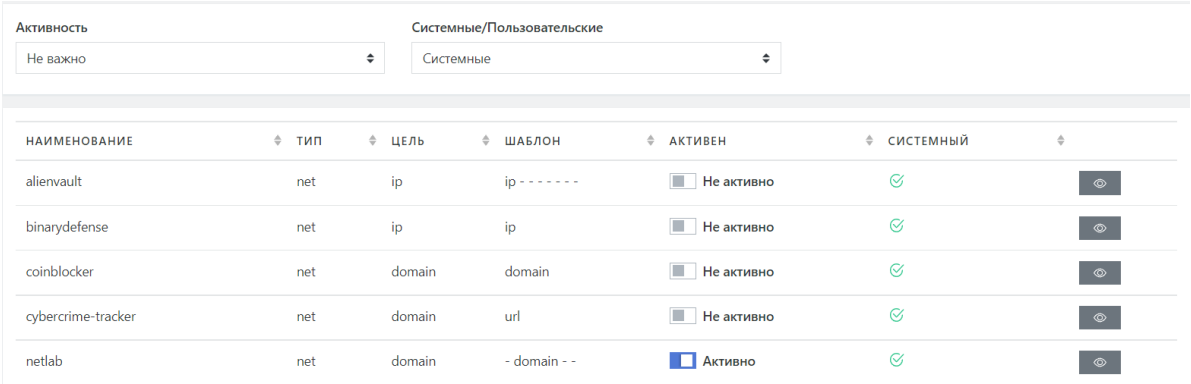

Рисунок 63 - Включение источника индикаторов компрометации

- Указание периода получения идентификаторов компрометации из активных источников;

  Для указания периода, нужно нажать на соответствующую кнопку и установить нужное количество часов (от 1 до 24)

- Ручной запуск и остановка сбора идентификаторов компрометации из активных источников;

  Для этого необходимо нажать на соответствующие кнопки в верхней части страницы, как изображено на рисунке 64.

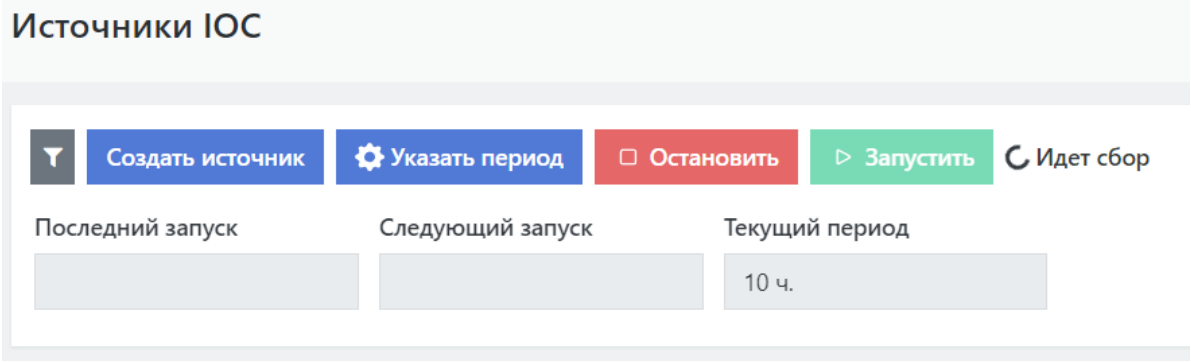

Рисунок 64 - "Включение\отключение сбора индикаторов компрометации"

- Создание пользовательского источника идентификаторов компрометации.

  Для создания пользовательского источника нужно нажать на кнопку "Создать источник", заполнить поля и нажать на "Сохранить".

7. Настройка контроля установленного ПО

7.1. Настройка контроля установленного ПО

7.1.1. Добавление правила контроля ПО

Для создания правила контроля ПО необходимо:

1. Перейти в раздел основного меню «**Оценка соответствия ПО**» и выбрать подраздел «Правила». Откроется текущий список правил (см. рисунок 65).

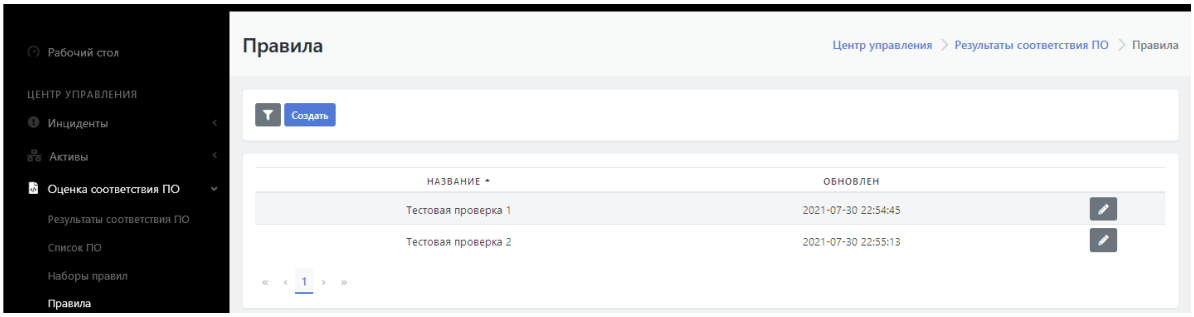

Рисунок 65 - Текущий список правил

2. Нажать на кнопку "Создать". На экране откроется форма для создания нового правила (см. рисунок 66).
3. Заполнить форму согласно подсказкам.
4. Нажать на кнопку «Сохранить».

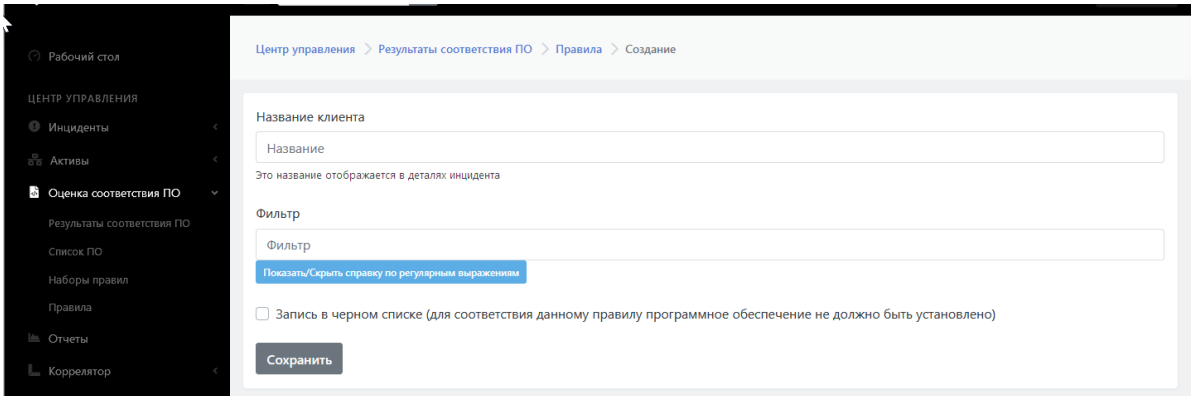

Рисунок 66 - Форма создания нового правила

В список правил добавится новое правило.

7.1.2. Редактирование правила контроля ПО. Удаление правила

Для редактирования правила контроля ПО необходимо:

1. Перейти в раздел основного меню «**Оценка соответствия ПО**» и выбрать подраздел «**Правила**». Откроется текущий список правил (см. рисунок 65).
2. Выбрать нужную строку с правилом и нажать на пиктограмму  . Откроется форма редактирования правила (см. рисунок 67).
3. Внести необходимые изменения.
4. Нажать на кнопку «Сохранить».
5. Нажать на кнопку «Удалить» если необходимо удаление правила.

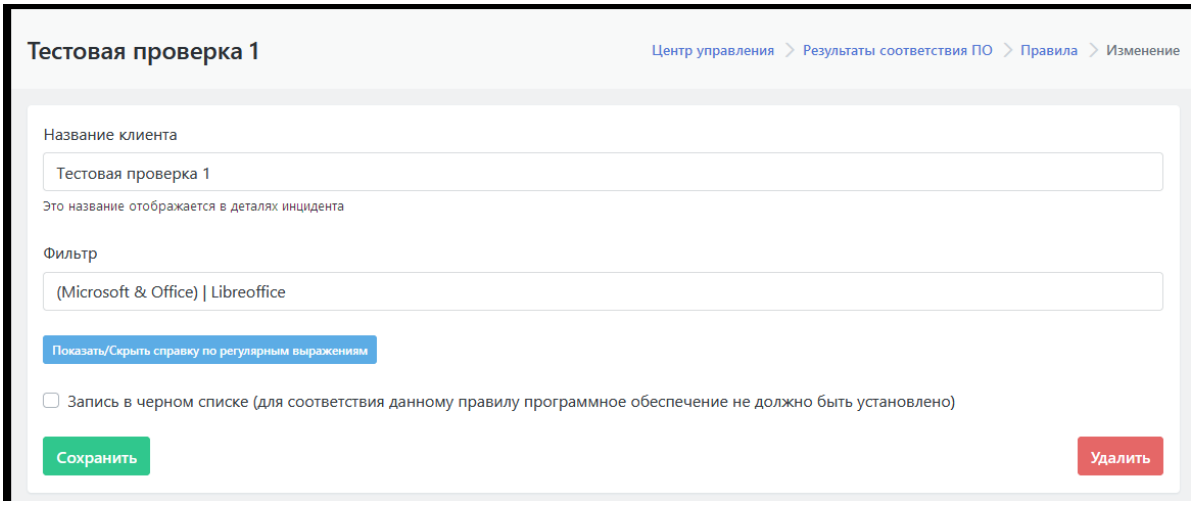

Рисунок 67 - Форма редактирования правила

8. Параметры

8.1. Параметры

8.1.1. Общее описание подраздела "Параметры"

Основное меню Центра управления Платформы Радар содержит раздел "Параметры", включающий подразделы (см. рисунок 68):

- "**Параметры**"
- "**Сопоставлениек данных**"
- "**API конструктор**"
- "**Черный список ID-плагинов**"
- "**Оповещения по задержкам в обработке**"

Подраздел "**Параметры**" предназначен для выполнения следующих функций:

- Вкладка "**Параметры**" - предназначена для обновления параметров уведомления.
- Вкладка "**Обработка уязвимостей**" - предназначена для настройки параметров автоматического переоткрытия инцидентов.
- Вкладка "**Синхронизация с Базой данных**"- предназначена для проведения синхронизации с Базой данных типов инцидентов и коррелятора.

8.1.2. Обновления параметров уведомления

Для обновления параметров уведомления необходимо зайти в раздел «Параметры», подраздел «Параметры». По умолчанию откроется вкладка «Общие», содержащая форму для ввода параметров уведомления (см. Рисунок 68).

Для обновления параметров уведомления необходимо:

1. Заполнить поле "**Название клиента**".
2. Заполнить поле "**Расположение**" (по умолчанию указана Москва).

3. Из выпадающего списка "**Группа пользователей по-умолчанию для инцидентов, связанных с активами, без определенного "ответственного пользователя"**" выбрать нужную группу пользователей.
4. Из выпадающего списка "**Стратегия идентификации активов по-умолчанию**" выбрать нужную стратегию:
    - IP;
    - FQDN;
    - MAC.
5. При необходимости включить совпадение по имени хоста (PQDN), где выбрана стратегия идентификации FQDN.
6. Нажать на кнопку "Сохранить".

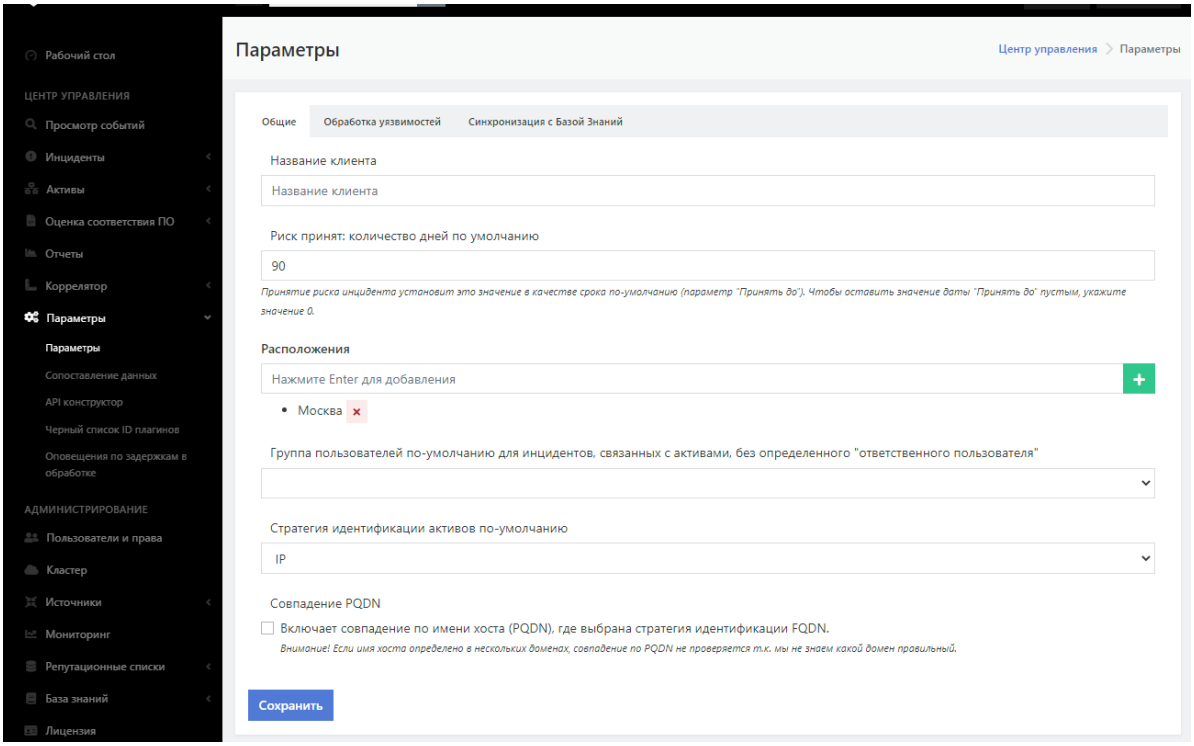

Рисунок 68 - Раздел "Параметры", вкладка "Общие"

8.1.3. Настройка автоматического переоткрытия инцидентов

Функционал по открытию инцидентов, находящихся в статусе «Закрыт», имеет ряд настроек. Для изменения настроек переоткрытия инцидентов необходимо зайти в раздел «Параметры», подраздел «Параметры» и открыть вкладку "Обработка уязвимостей" (см. рисунок 69).

Вкладка содержит следующие настройки открытия инцидента:

- Признак "**Автоматически создавать инциденты при импорте результатов сканирования**" - автоматическое создание инцидентов при получении результатов сканирования:
- "**Минимальный уровень важности для открытия инцидентов**" - инциденты с важностью ниже установленного в данном поле уровня не открывается автоматически. Из раскрывающегося списка устанавливается уровень важности.
- "**Создавать новый инцидент для повторных происшествий, если инцидент закрыт**" - правило поведения, если инцидент уже закрыт, из списка:

    - создавать новый инцидент
    - переоткрывать инцидент
- "**Минимальный уровень риска для повторного открытия инцидентов**" - инциденты с рисками ниже минимального, установленного в данном поле, не открываются автоматически.
- "**Статус повторно открытых инцидентов**"
- Нажать кнопку «Сохранить».

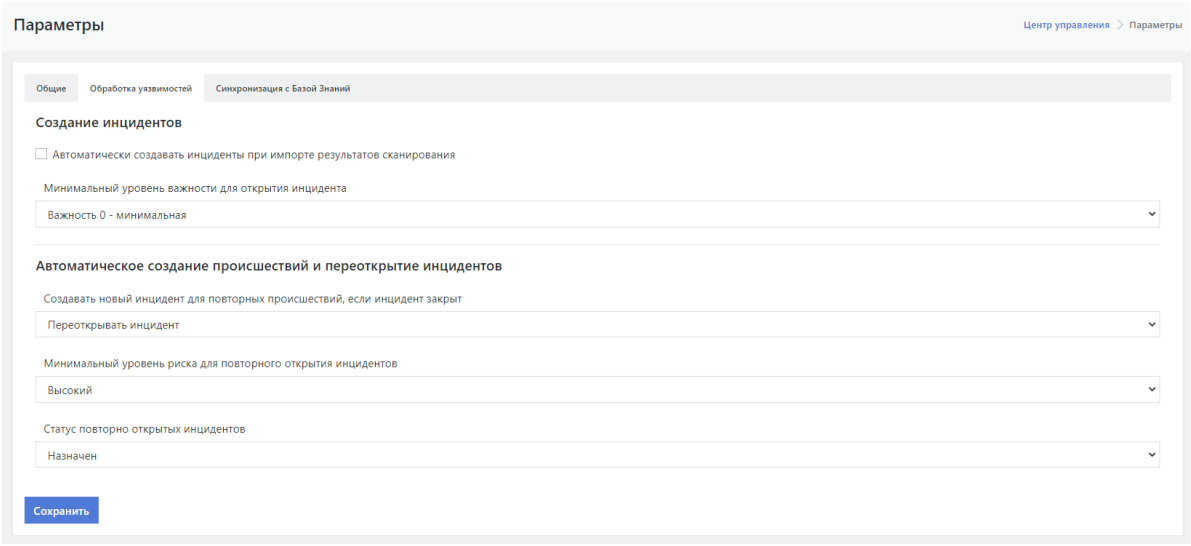

Рисунок 69 - Раздел "Параметры", вкладка "Обработка уязвимостей"

8.1.4. Синхронизация с базой знаний

Для синхронизации с Базой знаний необходимо зайти в раздел "Параметры", подраздел "Параметры" и открыть вкладку "Синхронизация с Базой знаний" (см. рисунок 70).

Нажать последовательно кнопки «**Синхронизация типов инцидентов**» и «**Синхронизация коррелятора**».

Внимание! Данная процедура требуется только при установке и обновлении Платформы.

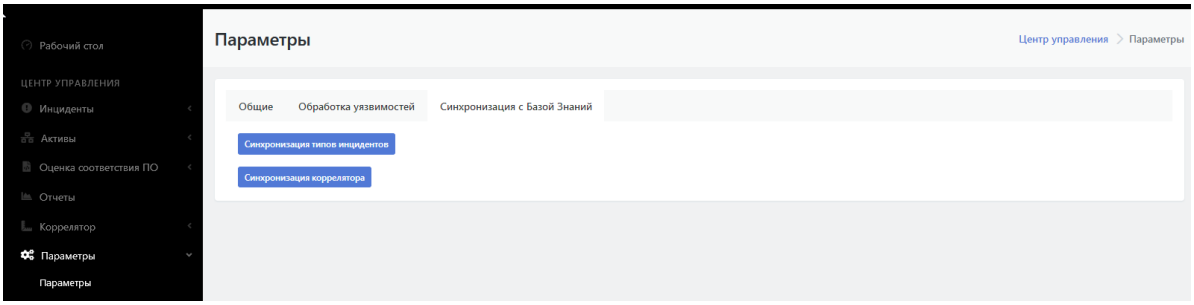

Рисунок 70 - Раздел "Параметры", вкладка "Синхронизация с Базой данных"

9. Управление лицензией

9.1. Первичная активация лицензии {#actlicense}

Первичная активация лицензии осуществляется на этапе установки **Платформы Радар**. Для этого выполните шаги:

1. На этапе установки отображается экран получения лицензии (см. рисунок 71).

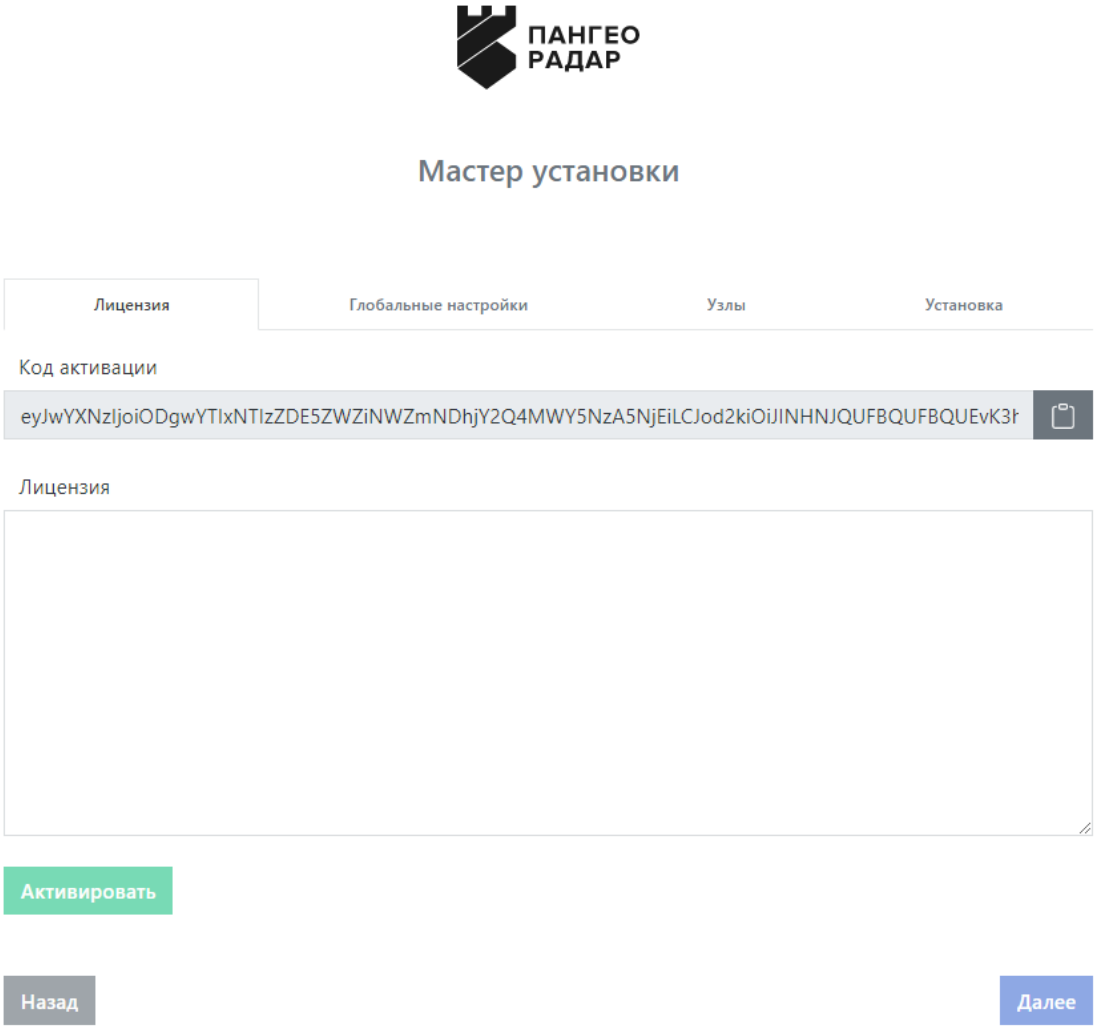

Рисунок 71 - Экран получения лицензии Платформы

2. Скопируйте в буфер обмена кликом по иконке  код активации, а затем перейдите в личный кабинет клиентского портала Платформы Радар, в котором будет доступна активация лицензии (см. рисунок 72).

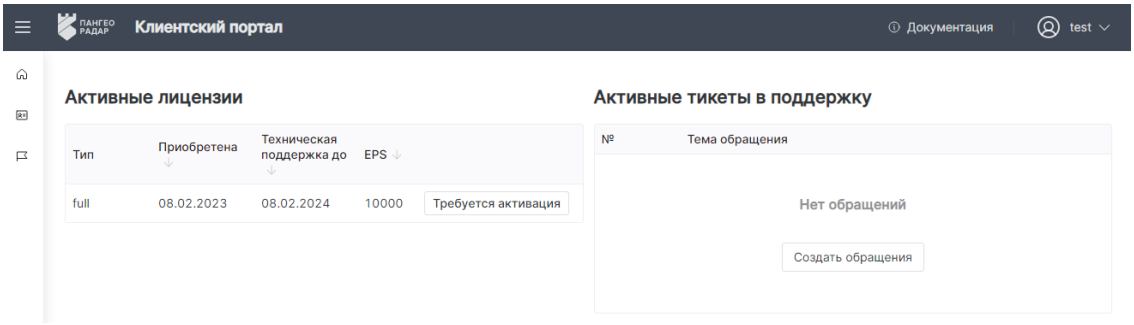

Рисунок 72 - Клиентский портал Платформы Радар

3. Нажмите на кнопку **Требуется активация**. В появившемся окне вставьте код активации и закройте окно. В личном кабинете клиентского портала Платформы Радар кнопка

Требуется активация будет заменена на кнопку **Лицензия** (см. рисунок 73).

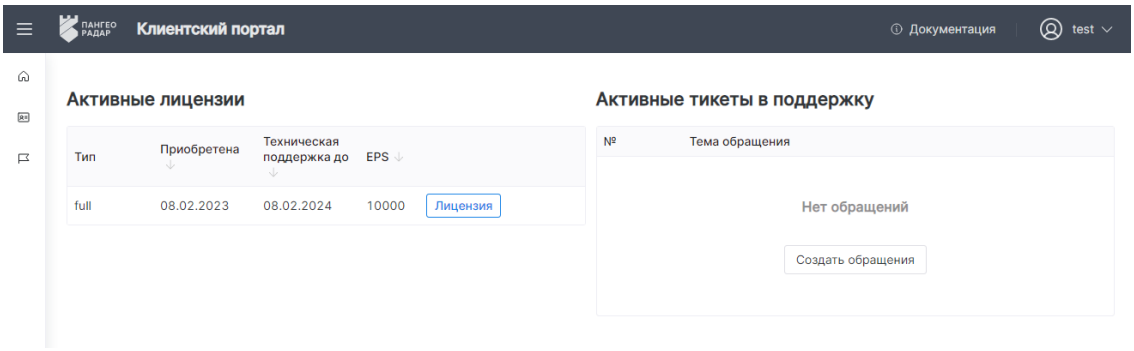

Рисунок 73 - Кнопка получения лицензии

4. Нажмите на кнопку **Лицензия**, после чего откроется окно с кодом лицензии (см. рисунок 74). Скопируйте код лицензии в буфер обмена кнопкой *Скопировать в буфер*.

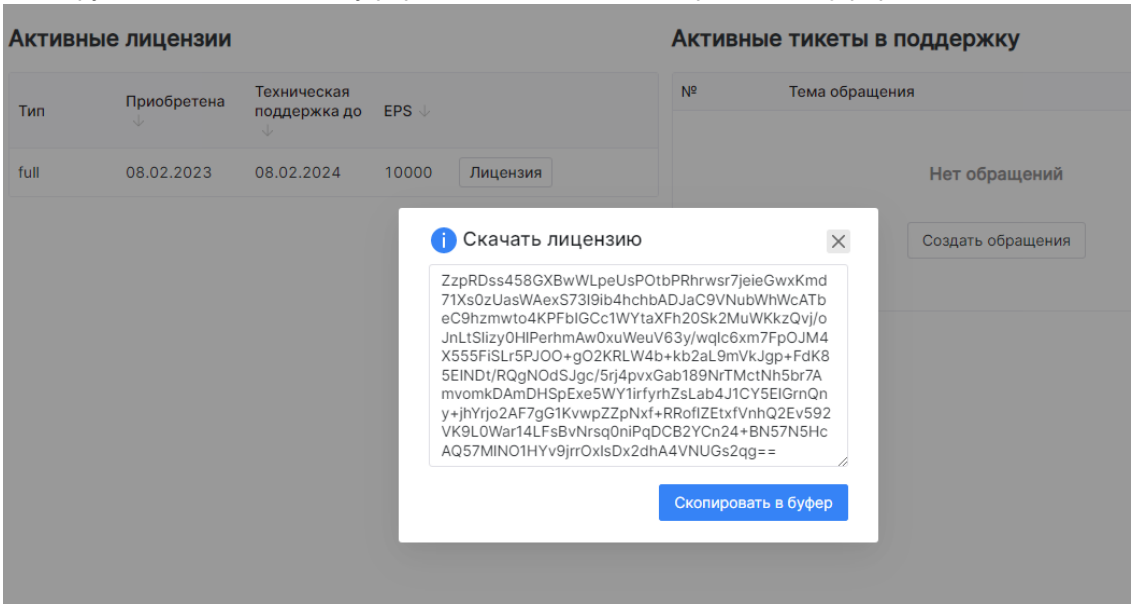

Рисунок 74 - Скачивание лицензии

5. Вернитесь к окну установки (см. рисунок 71). Вставьте код лицензии в окно **Лицензия** и нажмите кнопку **Активировать**. Лицензия будет активирована, а на экране будут

отображены ее параметры (см. рисунок 75).

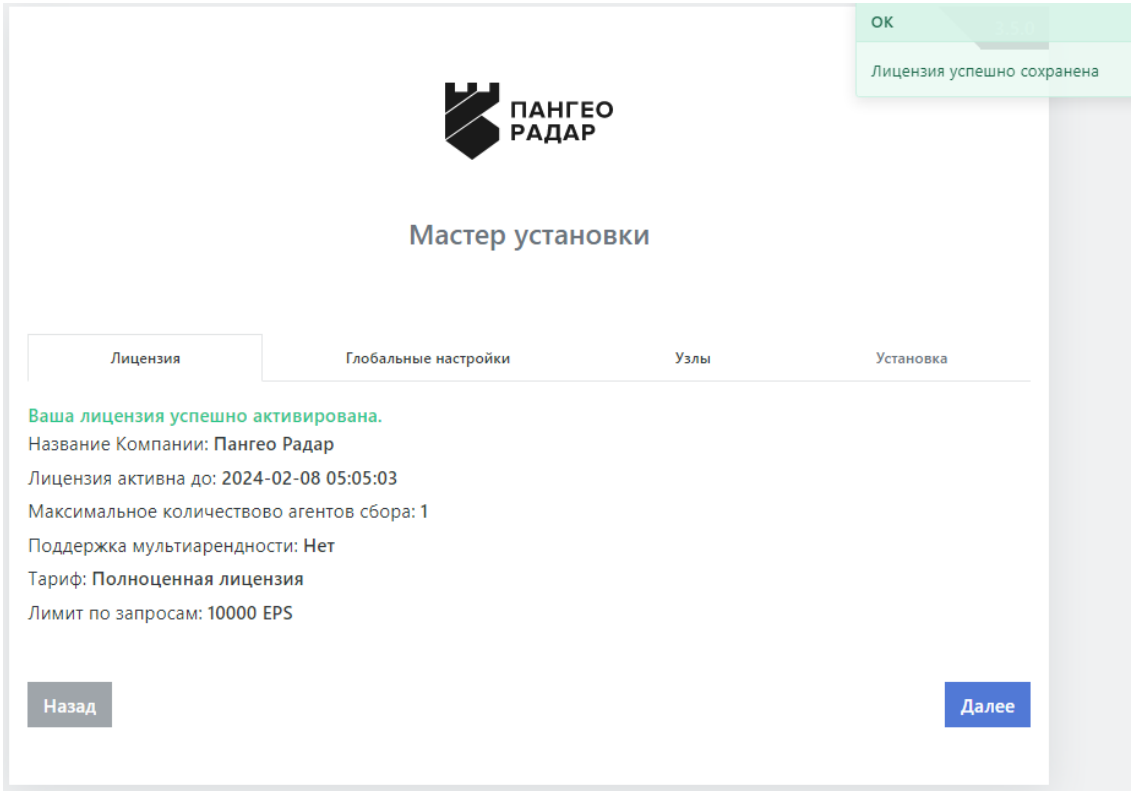

Рисунок 75 - Параметры лицензии

9.2. Просмотр параметров лицензии и повторная активация лицензии

Раздел интерфейса **"Лицензия"** предназначен для управления лицензией и просмотра параметров лицензии.

Вид раздела представлен на рисунке 76.

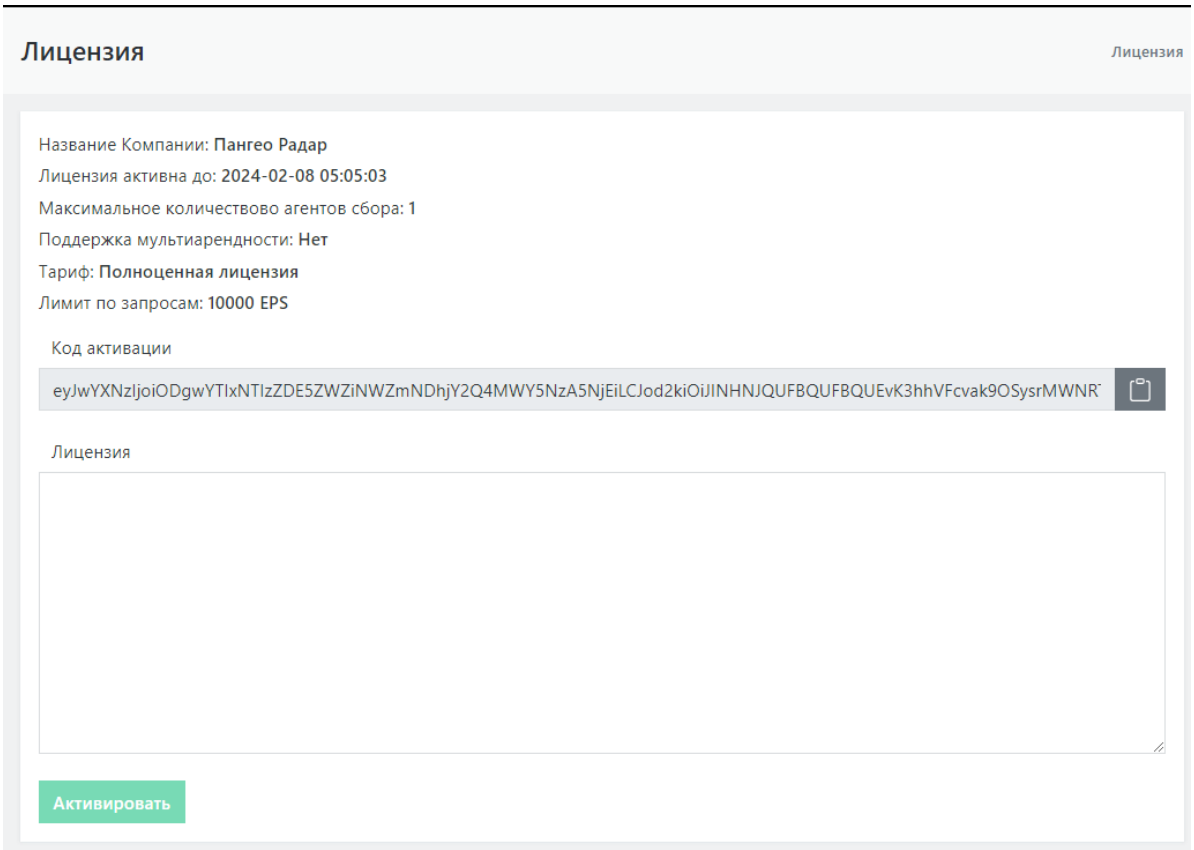

Рисунок 76 - Вид раздела **"Лицензия"**.

В верхней части раздела отображаются параметры лицензии:

- Название компании, которой принадлежит лицензия.
- Срок активности лицензии, по истечении которого, если не будет получена новая лицензия, не будет доступен интерфейс **Платформы Радар**, за исключением текущего раздела.
- Максимальное количество агентов сбора логов.
- Наличие режима мультиарендности и максимальное количество экземпляров **Платформы Радар**.
- Тип тарифа.
- Лимит по количеству запросов в EPS (количество событий в секунду).

В поле *Код активации* указан код, который использовался при установке **Платформы Радар**.

В случае, если активация лицензии будет недоступна (например, срок действия лицензии закончился или **Платформа Радар** была скопирована или перемещена на другой физический или виртуальный сервер), **Платформа Радар** продолжит свою работу, но интерфейс будет недоступен.
Из доступных страниц останется только страница управления лицензией.

Для повторной активации лицензии скопируйте код активации в буфер обмена кликом по иконке  и обратитесь в службу технической поддержки **Платформы Радар**. Сделать это можно из клиентского портала **Платформы Радар** (см. рисунок 77).

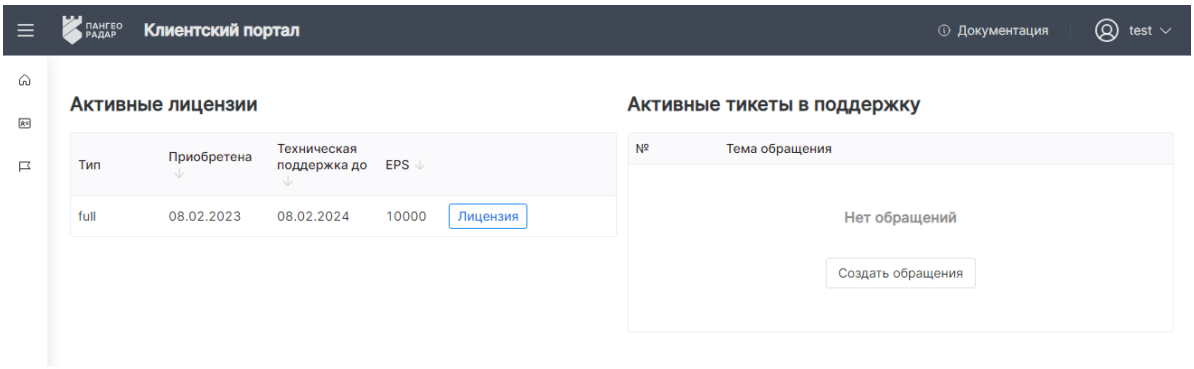

Рисунок 77 - Клиентский портал **Платформы Радар**

Нажмите кнопку *Создать обращение*. В обращении опишите проблему и вставьте ранее скопированный код активации. Для решения проблемы с активацией лицензии дождитесь ответа от службы технической поддержки **Платформы Радар**.

После получения лицензии вставьте ее код в окно *Лицензия* (см. рисунок 76) и нажмите кнопку *Активировать*.

10. Диагностика состояния Платформы Радар

Диагностика состояния **Платформы Радар** осуществляется с помощью специального скрипта диагностики. Скрип диагностики (cluster_diagnostic.sh) обеспечивает проверку состояния всех сервисов и компонентов **Платформы Радар**. Скрипт проводит диагностику как установок на один сервер, так и распределенную (кластер).

В случае обнаружения ошибок скрипт собирает данные диагностики, относящие к данному сервису и окружению узла, на котором обнаружены ошибки работы, при этом не собирая данные с других узлов кластера или узлов, не относящихся к проблеме.

Скрипт не собирает данные диагностики, относящиеся к работе коллектора, как Linux так и Windows.

10.1. Параметры командной строки скрипта

- -h - вывести список доступных параметров
- --diag - собрать данные диагностики по всем сервисам и узлам кластера Пангео Радар
- --elastic-err - выгрузить в архив ошибки парсинга. В случае использования ключа --diag данные так же выгружаются.
- --export-rule - экспортирует активные правила корреляции
- --export-prometheus - экспортирует данные диагностики в архив

10.2. Перечень сведений выгружаемых скриптом диагностики

10.2.1. Сервисы

- Статус сервиса (systemctl status)
- Журнал работы (journalctl)
- Доступность портов

Дополнительные журналы по сервисам (ролям):

- Data - Журналы работы ноды (`/var/log/elasticsearch/`)
- Data - Ошибки парсинга и нормализации (при использовании соответствующих параметров)
- Worker - Журналы работы и ошибки
- Correlator - Журналы работы (без журналов работы правил корреляции)
- Веб-сервер - Журналы доступа и ошибки
- Infra (MQ корреляции) - Журналы работы
- Master (База данных) - Журналы работы и ошибки
- Infra (RMCA) - Журналы доступа и ошибки

10.2.2. Сбор данных на узле с ролью master

- Доступность серверов и их IP адреса
- Список ролей и их IP адреса
- Список подключенных источников
- Контрольные суммы установленных пакетов платформы радар
- Параметры настройки Платформы Радар
- Шаблоны файлов конфигурации Платформы Радар
- SSH список известных хостов (known_hosts)
- Состояние (размер очереди) уведомлений правил корреляции
- Открытые ключи доступа SSH (закрытые ключи не затрагиваются)

10.2.3. Окружение для всех узлов

- Информация о используемом процессоре
- Информация об оперативной памяти и ее использовании
- Файлы конфигурации сервисов Платформы Радар
- Файлы конфигурации системы (`/etc/`)
- Журналы работы (journalctl)
- Список активных процессов
- Версию операционной системы
- Журнал установки компонентов Платформы Радар
- Список примонтированных устройств и файловой системе
- Историю выполняемых команд
- Журналы установки пакетов (APT, DPKG)
- Список установленных пакетов
- Текущие маршруты (route)
- Настройки сети
- Доступную память
- Информацию о дисковом пространстве и именах дисков
- Журналы авторизации
- Информациz о настройках окружения (env)
- Ошибки работы скрипта диагностики (в случае использования параметра --diag)
- Список подключенных репозиториев Debian (etc/apt/sources.list)
- Настройки ядра Linux (sysctl)
- Список запланированных задач (Cron)

11. Пример настройки службы синхронизации времени в ОС Debian

Для настройки службы синхронизации времени необходимо выполнить следующие настройки:

> Все команды выполняются под привилегированным пользователем

1. Добавить адрес NTP сервера в файл конфигурации службы:

```
echo 'NTP=<адрес NTP сервера>'>> /etc/systemd/timesyncd.conf
```

2. Перезапустить службу:

```
systemctl restart systemd-timesyncd.service
```

3. Проверка синхронизации:

```
timedatectl status
```

4. Проверка состояния службы:

```
systemctl status systemd-timesyncd.service
```

5. Добавление службы в атозапуск:

```
systemctl enable --now systemd-timesyncd.service
```

12. Выпуск и установка сертификата TLS для Nginx с использованием MS CA

Если в организации используется собственный корпоративный удостоверяющий центр, его можно использовать для выпуска сертификата веб-сервера **Платформы Радар**.

В данном примере рассмотрен выпуск сертификата с использованием Microsoft Certification Authority.

12.1. Выпуск сертификата

1. Сначала необходимо создать файл закрытого ключа. Для этого необходимо запустить утилиту openssl и указать имя создаваемого файла, а также используемый алгоритм шифрования:

   ```
   # openssl genrsa -out pangeo_custom.key -aes256 2048
   ```

   в результате на экран будет выведено следующее сообщение:

   ```
   Generating RSA private key, 4096 bit long modulus
   ......................++
   ..........................................................................
   .....++
   e is 65537 (0x10001)
   Enter pass phrase for pangeo_custom.key:
   Verifying - Enter pass phrase for pangeo_custom.key:
   ```

   После появления приглашения “Enter pass phrase for radar_custom.key” следует ввести пароль для файла закрытого ключа (дважды). Пароль необходимо запомнить.

2. В текущем каталоге необходимо создать файл openssl.cnf и записать в него следующие данные (пример):

   ```
   [ req ]
   req_extensions = v3_req
   distinguished_name = req_distinguished_name
   promt = yes

   [ req_distinguished_name ]
   countryName = Country Name (2 letter code)
   countryName_default = RU

   stateOrProvinceName = State or Province Name (full name)
   stateOrProvinceName_default = Moscow

   localityName = Locality Name (eg, city)
   localityName_default = Moscow
   ```

```
O.organizationName = Organization Name (eg, company)
O.organizationName_default = Pangeo

organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = ITSec

commonName = Common Name (eg, your name or your server\'s hostname)
commonName_default = radar-353-aio.test.lab

emailAddress = Email Address
emailAddress_default = support@pangeoradar.ru

[ v3_req ]
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = radar-353-aio.test.lab
IP.0 = 192.168.2.147
```

Значения полей: `countryName_default`, `stateOrProvinceName_default`, `localityName_default`, `O.organizationName_default`, `organizationalUnitName_default`, `commonName_default`, `emailAddress_default`, `DNS.0`, `IP.0` необходимо заполнить самостоятельно в соответствии с параметрами инсталляции и инфраструктуры. После внесения изменений файл необходимо сохранить.

3. Необходимо сгенерировать запрос на подпись сертификата, выполнив следующую команду:

```
# openssl req -new -key radar_custom.key -out cert_request.csr -config
openssl.cnf
```

В процессе выполнения команда запросит ввод пароля, указанного в шаге 1.

4. После создания файла запроса (cert_request.csr) необходимо зайти в веб-интерфейс УЦ MS CA и перейти по ссылке “Request a certificate”:

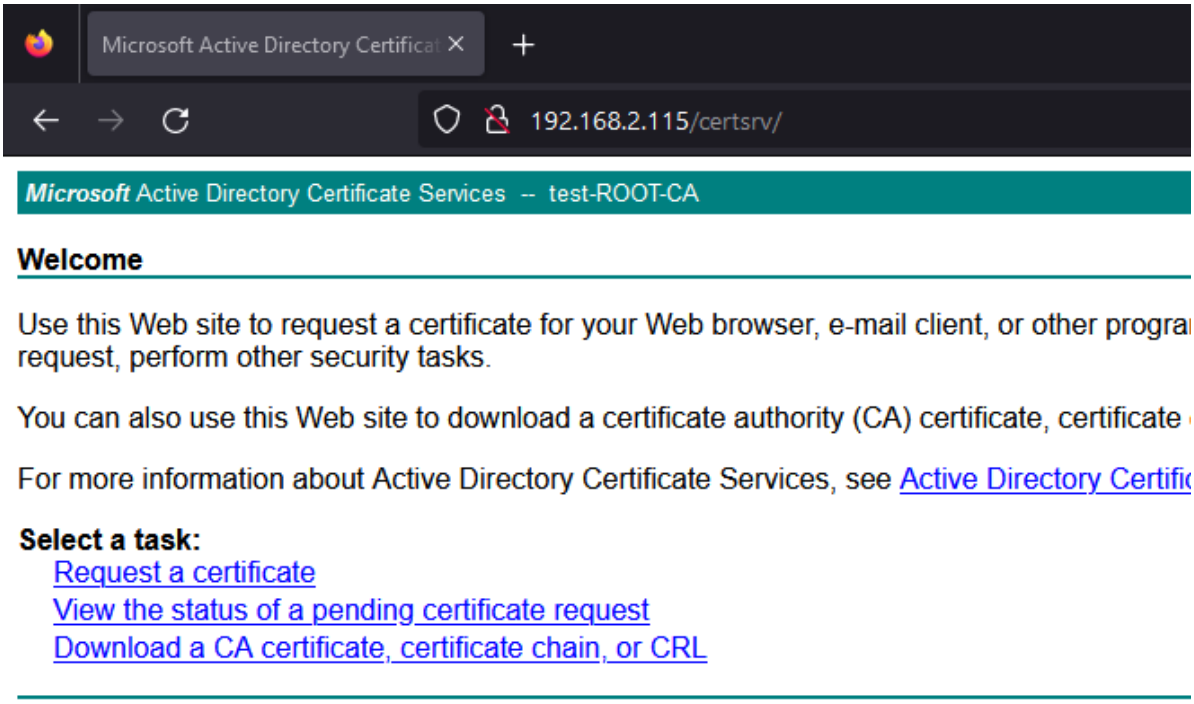

Рисунок 78

5. На следующем этапе необходимо выбрать “advanced certificate request”:

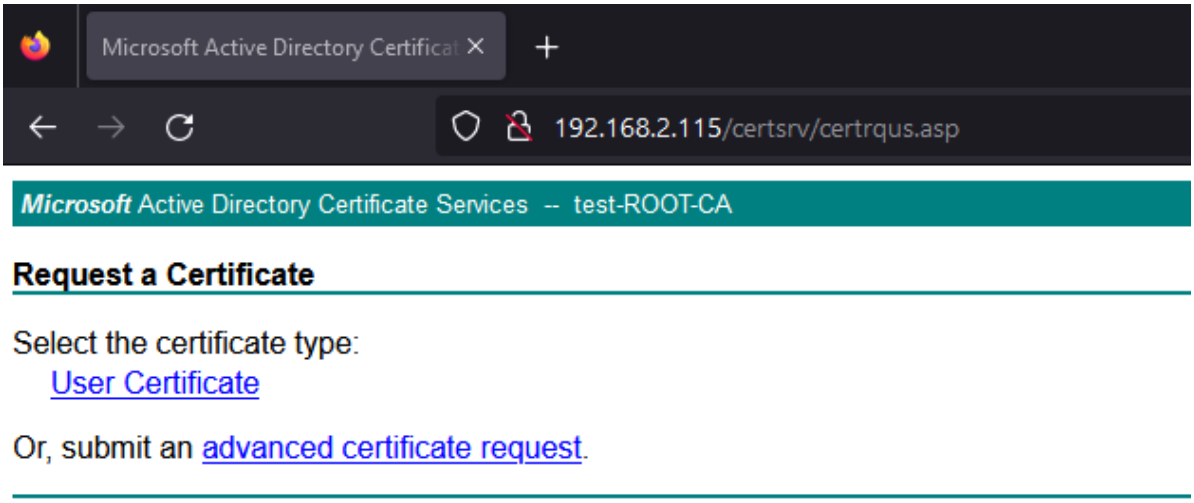

Рисунок 79

6. В поле “Saved Request” необходимо скопировать содержимое файла request.csr, для поля “Certificate Template” выбрать тип “Web Server”. Нажать кнопку “Submit”.

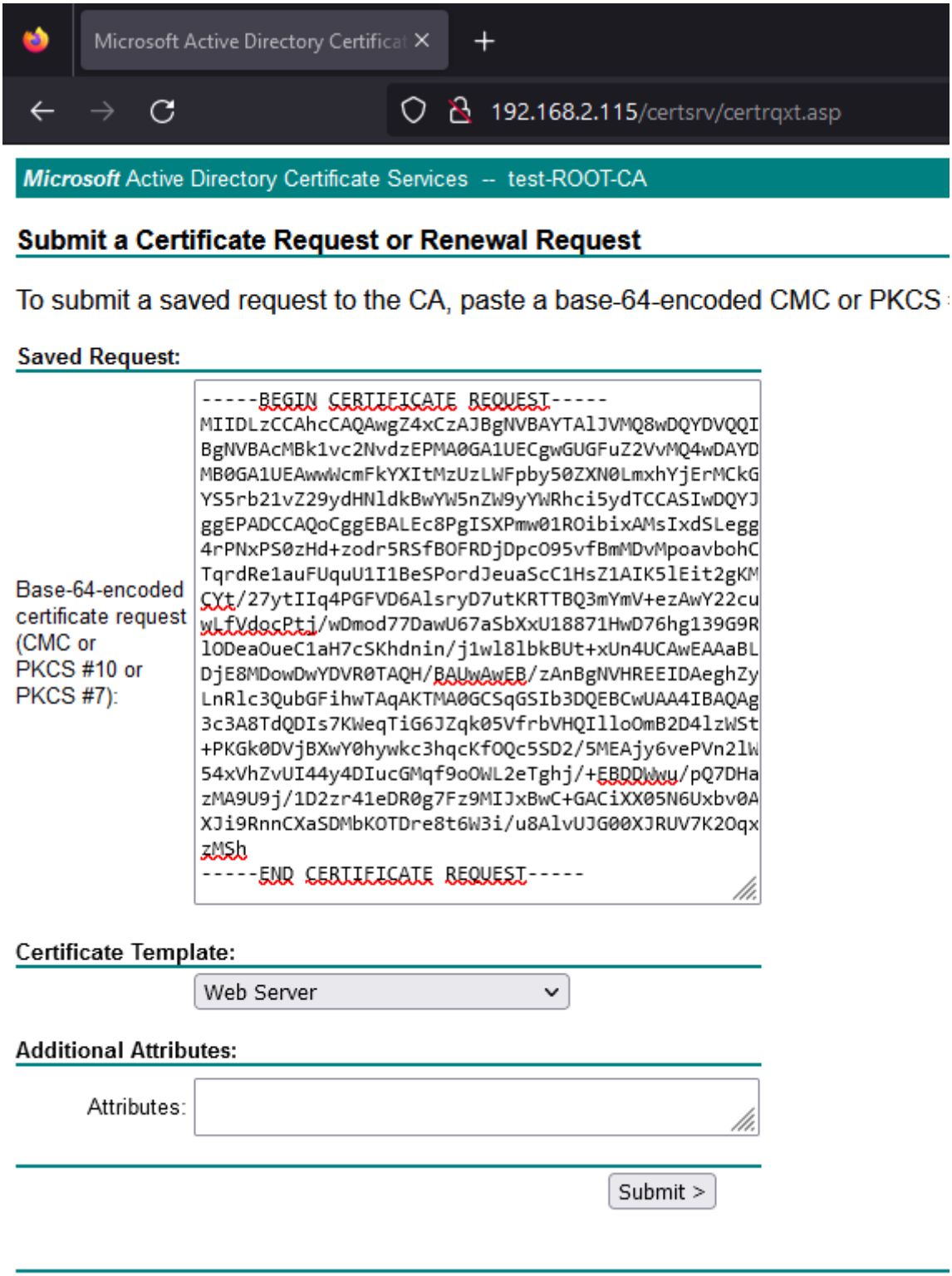

Рисунок 80

7. После успешного выпуска необходимо скачать сертификат (Download certificate) и загрузить файл на сервер, где функционирует служба Nginx.

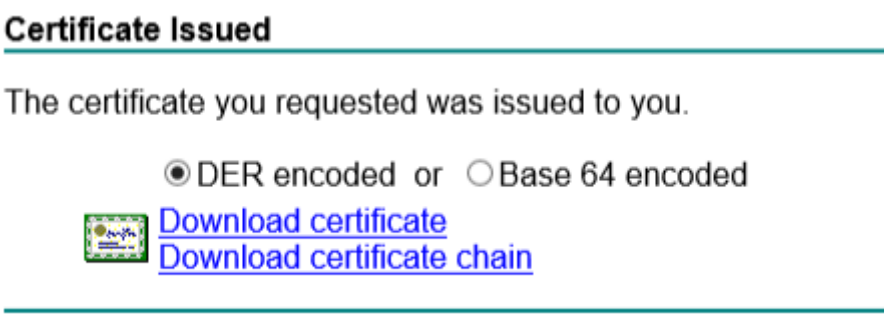

Рисунок 81

12.2. Установка сертификата

К моменту установки сертификата в наличии должны быть следующие файлы (пример):

- *pangeo_custom.key* (файл закрытого ключа);
- *pangeo_custom.cer* (файл сертификата).

Далее:

1. Сконвертируйте файл *.cer в *.crt.

   Если сертификат скачивался в формате DER:

   ```
   openssl x509 -inform DER -in pangeo_custom.cer -out pangeo_custom.crt
   ```

   Если сертификат скачивался в формате PEM (Base64):

   ```
   openssl x509 -inform PEM -in pangeo_custom.cer -out pangeo_custom.crt
   ```

2. Далее удалите пароль для файла закрытого ключа (команда потребует ввод пароля):

   ```
   openssl rsa -in pangeo_custom.key -out pangeo_custom_unencrypted.key
   ```

3. Затем, файлы pangeo_custom.crt и pangeo_custom_unencrypted.key скопируйте в директорию `/opt/pangeoradar/certs/`:

   ```
   # cp pangeo_custom_unencrypted.key /opt/pangeoradar/certs/
   # cp pangeo_custom.crt /opt/pangeoradar/certs/
   # chmod 644 /opt/pangeoradar/certs/pangeo_custom_unencrypted.key
   # chmod 644 /opt/pangeoradar/certs/pangeo_custom.crt
   ```

4. В разделе “Управление конфигурацией” для Nginx укажите использование нестандартных сертификатов, выполните сохранение и применение настроек:

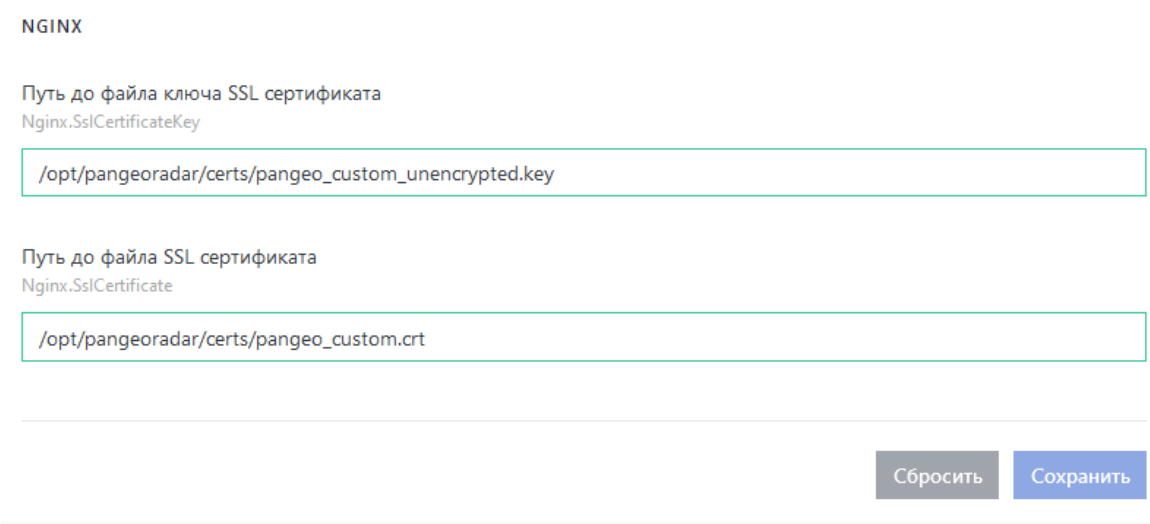

Рисунок 82

5. Для подмены сертификата в Keycloak отредактируйте файл шаблона `/opt/pangeoradar/bin/service_config_templates/ui.nginx.tmpl`, раскомментировав вторую секцию конфигурации:

```
server {
    location /fonts  {
        alias /opt/pangeoradar/bin/dist/fonts;
    }
    location / {
        proxy_pass http://{{.Ui.Ip}}:{{ .Ui.Port }};
    }{{ if .DNS.DomainName | IsDomain }}
    server_name {{ .DNS.UiDomain}};{{ end }}
{{ if .DNS.DomainName | IsIp }}    listen 443 ssl default_server;{{ else }}
   listen 443 ssl;{{ end }}
    ssl on;
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_prefer_server_ciphers on;
    ssl_certificate {{ .Nginx.SslCertificate }};
    ssl_certificate_key {{ .Nginx.SslCertificateKey }};
}

server {
    location /fonts  {
        alias /opt/pangeoradar/bin/dist/fonts;
    }
    location / {
        proxy_pass http://127.0.0.1:{{ .Ui.Port }};
    }
    listen 8080 ssl default_server;
    ssl on;
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_prefer_server_ciphers on;
    ssl_certificate {{ .Nginx.SslCertificate }};
    ssl_certificate_key {{ .Nginx.SslCertificateKey }};
}
```

6. Перезапустите службу nginx и проверьте результат:

```
# systemctl restart nginx
```

На этом, установка сертификата веб-интерфейса завершена. Для Grafana на порте 6630/TCP сертификат будет заменен автоматически.

13. Интеграционный слой

Внутри поставки имеется гибкий инструмент для организации интеграции между Платформой Радар и любой другой системой, с которой можно коммуниципировать через Json API.

13.1. Концепция интеграционного слоя

Основной логикой является наблюдение за изменением данных в структуре хранения информации Платформы PostgreSQL и запуск некоторых действий при наступлении того или иного изменения.

13.1.1. Наблюдение за изменениями

Основной для реагирования на изменение является секция `radar-tables-trigger`. По сути является перечнем наблюдателей, реагирующих на изменения в базе данных.

```
radar-tables-trigger: &radar-tables-trigger
  - name: create_incident
    table: service_asset_findings
    fields: [ ]
    kind: insert
    sql: "SELECT ..."
    sql_vars:
      id: float64toInt64
    outputs:
      - *rvision_insert
```

Доступные триггеры, поле `kind`:

- insert
- update
- delete

При срабатывании тригера на выбранной таблице указанной в секции `table` запускается `sql` скрипт собирающий основной объект для передачи запуска сборки объекта отправляемого в интегрируемую системы. Если `sql` скрипт не указан будет взята строка из наблюдаемой таблицы.

Также есть поле `fields`, заполнив которое можно указать те поля, при изменении которых должен запускать триггер.

поле `sql_vars` необходимо для приведения типов:

- bool
- int
- int32
- int64
- string

- float32
- float64
- float64toInt64

поле `outputs` указывает необходимые каналы для дальнейшей интеграции с внешними системами.

13.1.2. Отправка изменений

Для организации канала отправки объекта соответствия, сформированного после срабатывания триггера, необходимо создать секцию, в которую направить вывод в поле `outputs`

Секция имеет следующую структуру:

```
rvision_update: &rvision_update
  type: http
  url: "https://IP/api/v2/incidents"
  method: POST
  content_type: "application/json"
  headers:
    PgrApiKey: "test"
  prepend:
    - type: http
      url: "https://IP/api/v2/incidents"
      method: GET
      content_type: "application/json"
      query:
        token: "SECRET"
        fields: "identifier"
        filter: '[{"operator":"=","value":%d,"property":"id_siem"}]'
      query_vars_from_trigger:
        filter:
          field: "id"
          type: "float64toInt64"
      append_to_mapping:
        identifier: "data.result.0.identifier"
  mappging: *rvision_mapping
```

- `type` - транспорт, на данны момент поддерживается только `http`
- `url` - адрес ендпоинта для отправки запроса
- `method` - тип запроса (GET, POST, PUT)
- `content_type` - значение заголовка content-type
- `headers` - дополнительные заголовки в формате `ключ: значение`
- `mapping` - объект соответствия
- `prepend` - дополнительная секция, которая будет выполнена перед отправкой основного запроса. Полезна, если нужно сделать запрос на получение доп. информации и обогащения объекта соответствия перед отправкой.

В секции `prepend` доступны те же основные поля, что и в основной. В дополнении к ней доступны опции:

- `query` - строка запроса
- `query_vars_from_trigger` - шаблонизация для строки запроса

- `append_to_mapping` - обогащение объекта соответствия по ключу и значению из ответа

13.1.3. Объект соответствия

Объект соответствия - это объект, который будет собран после срабатывания триггера и передан в канал на отправку.

Структура объекта:

```
rvision_mapping: &rvision_mapping
  token:
    type: "manual"
    value: "SECRET_KEY"
  status_siem:
    type: "map"
    value: "status"
  STATUS:
    type: "active_map"
    value: "status"
    map:
      new: "Создан"
      risk_accepted: "Зарегистрирован"
      assigned_customer: "Назначен"
      working_customer: "Обработка"
      feedback_required: "Раследование"
      closed: "Закрыт"
```

`type` - тип соответствия, доступны:

- `manual` - заданное ручное значение в ключе `value`
- `map` - ключу объекта будет соответствовать поле указанного в значение ключа `value` из триггера изменений
- `active_map` - ключу объекта будет соответствовать значение из объекта `map`, найденного при совпадении ключа, и значение поля из триггера изменений, указанного в ключе `value`

13.2. Пример интеграции с SOAR RVision

Ниже представлен конфигурационный файл `/opt/pangeoradar/configs/pangeoradar-pgr-wal-listener.yaml`, настроенный на обмен информацией об инцидентах с SOAR RVision.

```
---

global:
  force_replica_identity: true
  log_level: warning

# Mappings
rvision_mapping: &rvision_mapping
  token:
    type: "manual"
    value: "SECRET_KEY"
  category:
    type: "manual"
    value: "Инцидент из Пагео Радар"
```

```
info_source:
  type: "manual"
  value: "SIEM Пангео"
type:
  type: "manual"
  value: "Инцидент полученный из Пангео Радар"
id_siem:
  type: "map"
  value: "id"
DESCRIPTION:
  type: "map"
  value: "DESCRIPTION"
risk_impact:
  type: "map"
  value: "risk_impact"
solution:
  type: "map"
  value: "solution"
mitigation:
  type: "map"
  value: "mitigation"
status_siem:
  type: "map"
  value: "status"
STATUS:
  type: "active_map"
  value: "status"
  map:
    new: "Создан"
    risk_accepted: "Зарегистрирован"
    assigned_customer: "Назначен"
    working_customer: "Обработка"
    feedback_required: "Раследование"
    closed: "Закрыт"
risklevel:
  type: "map"
  value: "risklevel"
service_asset_id:
  type: "map"
  value: "service_asset_id"
DETECTION_DATE:
  type: "map"
  value: "created_at"
UPDATE:
  type: "map"
  value: "updated_at"
finding_id:
  type: "map"
  value: "finding_id"
analysis_output:
  type: "map"
  value: "analysis_output"
synopsis:
  type: "map"
  value: "synopsis"
```

```
  title:
    type: "map"
    value: "title"
  risk:
    type: "map"
    value: "risk"
  OCCUR_DATE:
    type: "map"
    value: "acknowledged_at"
  alert_type:
    type: "map"
    value: "alert_type"
  client_note:
    type: "map"
    value: "client_note"
  internal_note:
    type: "map"
    value: "internal_note"
  external:
    type: "map"
    value: "external"
  immediate_action_score:
    type: "map"
    value: "immediate_action_score"
  throughput_period:
    type: "map"
    value: "throughput_period"
  throughput_period_change:
    type: "map"
    value: "throughput_period_change"
  customer_created:
    type: "map"
    value: "customer_created"
  c_visible_since:
    type: "map"
    value: "c_visible_since"
  c_visible_since_in_days:
    type: "map"
    value: "c_visible_since_in_days"
  c_reopened_count:
    type: "map"
    value: "c_reopened_count"
  c_last_customer_status_change:
    type: "map"
    value: "c_last_customer_status_change"
  c_customer_retention_time:
    type: "map"
    value: "c_customer_retention_time"
  logmule_identifier:
    type: "map"
    value: "logmule_identifier"
  c_remote_exploitable:
    type: "map"
    value: "c_remote_exploitable"
  c_occurrence_count:
```

```
    type: "map"
    value: "c_occurrence_count"
  last_occurrence_id:
    type: "map"
    value: "last_occurrence_id"
  itsm_last_synced_at:
    type: "map"
    value: "itsm_last_synced_at"
  itsm_sync_status:
    type: "map"
    value: "itsm_sync_status"
  external_id:
    type: "map"
    value: "external_id"
  itsm_sync_error:
    type: "map"
    value: "itsm_sync_error"
  user_id:
    type: "map"
    value: "user_id"
  updated_by:
    type: "map"
    value: "updated_by"
  group_id:
    type: "map"
    value: "group_id"
  acknowledged_by:
    type: "map"
    value: "acknowledged_by"
  created_by_customer:
    type: "map"
    value: "created_by_customer"
  edited_by:
    type: "map"
    value: "edited_by"
  active_name:
    type: "map"
    value: "active_name"
  IP:
    type: "map_from_json"
    value: "ip"
    from: "inet"
  fqdn:
    type: "map_form_json"
    value: "fqdn"
    from: "varchar_array"


# Outputs
rvision_insert: &rvision_insert
  type: http
  url: "https://IP/api/v2/incidents"
  method: POST
  content_type: "application/json"
  headers:
```

```
    PgrApiKey: "test"
  mappging: *rvision_mapping

rvision_update: &rvision_update
  type: http
  url: "https://IP/api/v2/incidents"
  method: POST
  content_type: "application/json"
  headers:
    PgrApiKey: "test"
  prepend:
    - type: http
      url: "https://IP/api/v2/incidents"
      method: GET
      content_type: "application/json"
      query:
        token: "SECRET"
        fields: "identifier"
        filter: '[{"operator":"=","value":%d,"property":"id_siem"}]'
      query_vars_from_trigger:
        filter:
          field: "id"
          type: "float64toInt64"
      append_to_mapping:
        identifier: "data.result.0.identifier"
  mappging: *rvision_mapping


radar-tables-trigger: &radar-tables-trigger
  - name: create_incident
    table: service_asset_findings
    fields: [ ]
    kind: insert
    sql: "SELECT t.id, CASE WHEN t.description ISNULL THEN f.description ELSE
t.description END, CASE WHEN t.risk_impact ISNULL THEN f.risk_impact ELSE
t.risk_impact END, CASE WHEN t.solution ISNULL THEN f.solution ELSE t.solution
END, t.mitigation, CASE WHEN t.solution ISNULL THEN f.solution ELSE t.solution
END, t.status, t.risklevel, t.service_asset_id, t.created_at, t.updated_at,
t.finding_id, t.analysis_output, t.synopsis, CASE WHEN t.synopsis ISNULL THEN
f.synopsis ELSE t.synopsis END, t.title, CASE WHEN t.title ISNULL THEN f.title
ELSE t.title END, t.risk, t.acknowledged_at, t.alert_type, t.client_note,
t.internal_note, t.external, t.immediate_action_score, t.throughput_period,
t.throughput_period_change, t.customer_created, t.c_visible_since,
t.c_visible_since_in_days, t.c_reopened_count, t.c_last_customer_status_change,
t.c_customer_retention_time, t.logmule_identifier, t.c_remote_exploitable,
t.c_occurrence_count, t.last_occurrence_id, t.itsm_last_synced_at,
t.itsm_sync_status, t.external_id, t.itsm_sync_error, t.user_id, t.updated_by,
t.group_id, t.acknowledged_by, t.created_by_customer, t.edited_by, s.name as
active_name, ni.ip as ip, ni.fqdn as fqdn FROM public.service_asset_findings t
left join findings f on t.finding_id = f.id left join service_assets s on
t.service_asset_id = s.id left join network_interfaces ni on s.id =
ni.service_asset_id where t.id = $1"
    sql_vars:
      id: float64toInt64
    outputs:
```

```
      - *rvision_insert

  - name: update_incident
    table: service_asset_findings
    fields: [ ]
    kind: update
    sql: "SELECT t.id, CASE WHEN t.description ISNULL THEN f.description ELSE
t.description END, CASE WHEN t.risk_impact ISNULL THEN f.risk_impact ELSE
t.risk_impact END, CASE WHEN t.solution ISNULL THEN f.solution ELSE t.solution
END, t.mitigation, CASE WHEN t.solution ISNULL THEN f.solution ELSE t.solution
END, t.status, t.risklevel, t.service_asset_id, t.created_at, t.updated_at,
t.finding_id, t.analysis_output, t.synopsis, CASE WHEN t.synopsis ISNULL THEN
f.synopsis ELSE t.synopsis END, t.title, CASE WHEN t.title ISNULL THEN f.title
ELSE t.title END, t.risk, t.acknowledged_at, t.alert_type, t.client_note,
t.internal_note, t.external, t.immediate_action_score, t.throughput_period,
t.throughput_period_change, t.customer_created, t.c_visible_since,
t.c_visible_since_in_days, t.c_reopened_count, t.c_last_customer_status_change,
t.c_customer_retention_time, t.logmule_identifier, t.c_remote_exploitable,
t.c_occurrence_count, t.last_occurrence_id, t.itsm_last_synced_at,
t.itsm_sync_status, t.external_id, t.itsm_sync_error, t.user_id, t.updated_by,
t.group_id, t.acknowledged_by, t.created_by_customer, t.edited_by, s.name as
active_name, ni.ip as ip, ni.fqdn as fqdn FROM public.service_asset_findings t
left join findings f on t.finding_id = f.id left join service_assets s on
t.service_asset_id = s.id left join network_interfaces ni on s.id =
ni.service_asset_id where t.id = $1"
    sql_vars:
      id: float64toInt64
    outputs:
      - *rvision_update


connections:
  - database: radar
    username: user
    password: secret
    host: 127.0.0.1
    port: 5432
    triggers: *radar-tables-trigger
```

14. Подготовка дисковой подсистемы для реализации роли DATA

Действия, описанные в данной инструкции, выполняются на хосте, который планируется ввести в состав кластера elasticsearch с ролью data (см. раздел "Подготовка дисковой системы").

При развертывании операционной системы необходимо выполнить следующие действия по разметке дисковой подсистемы:

1. Разметить основной диск, на который будет устанавливаться операционная система и дополнительное программное обеспечение для функционирования компонентов

Платформы. Размеры разделов для основного диска выбираются исходя из объема жесткого диска. Основная рекомендация по разметке диска для ОС - размер раздела /var должен быть не менее 75 Gb, т.к. в нем будут размещать все необходимые для работы модуля данные .

2. Разметить дополнительные физические диски.

На рисунке 83 показан вариант разметки основного диска и три не размеченных физических диска.

Чтобы провести разметку дисковой системы необходимо выполнить следующие действия:

1. Выбрать диск и нажать кнопку «Continue» (см. рисунок 83).

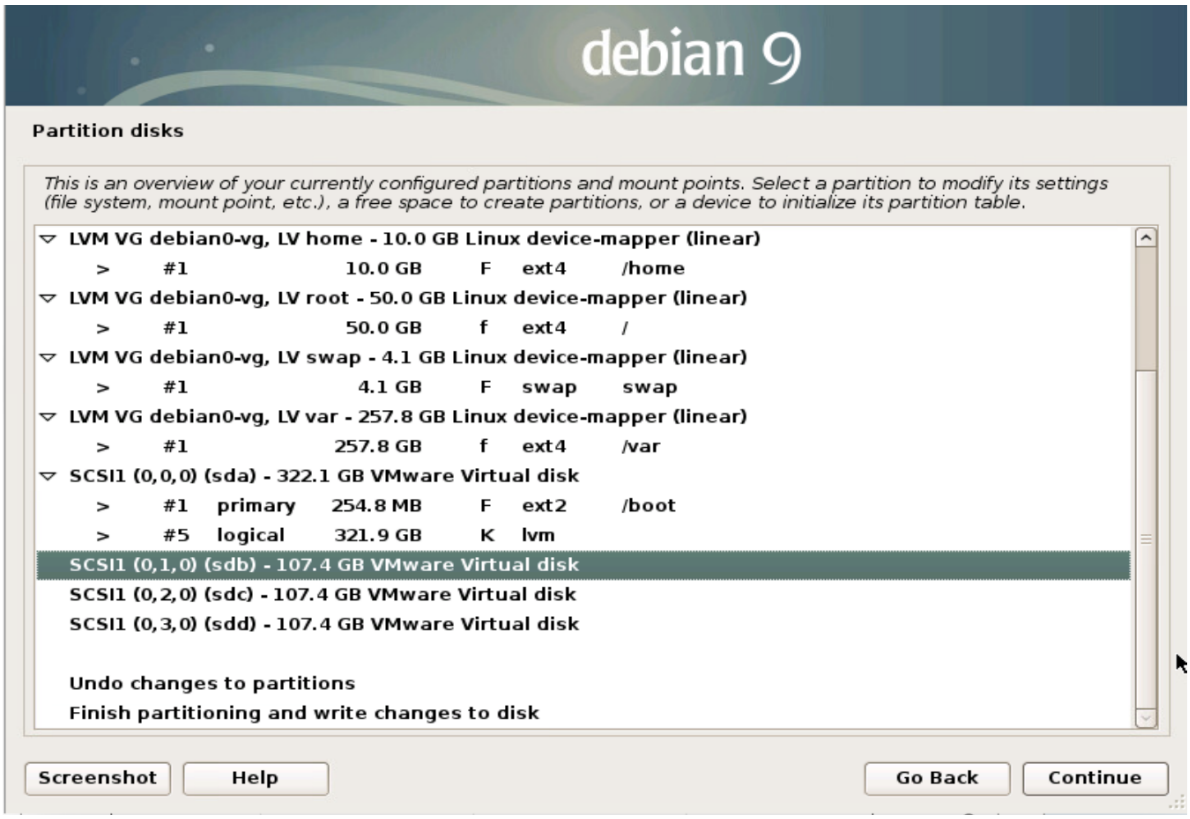

Рисунок 83 - Вариант разметки основного диска

2. Выбирать пункт «Yes» и нажать кнопку «Continue» (см. рисунок 84).

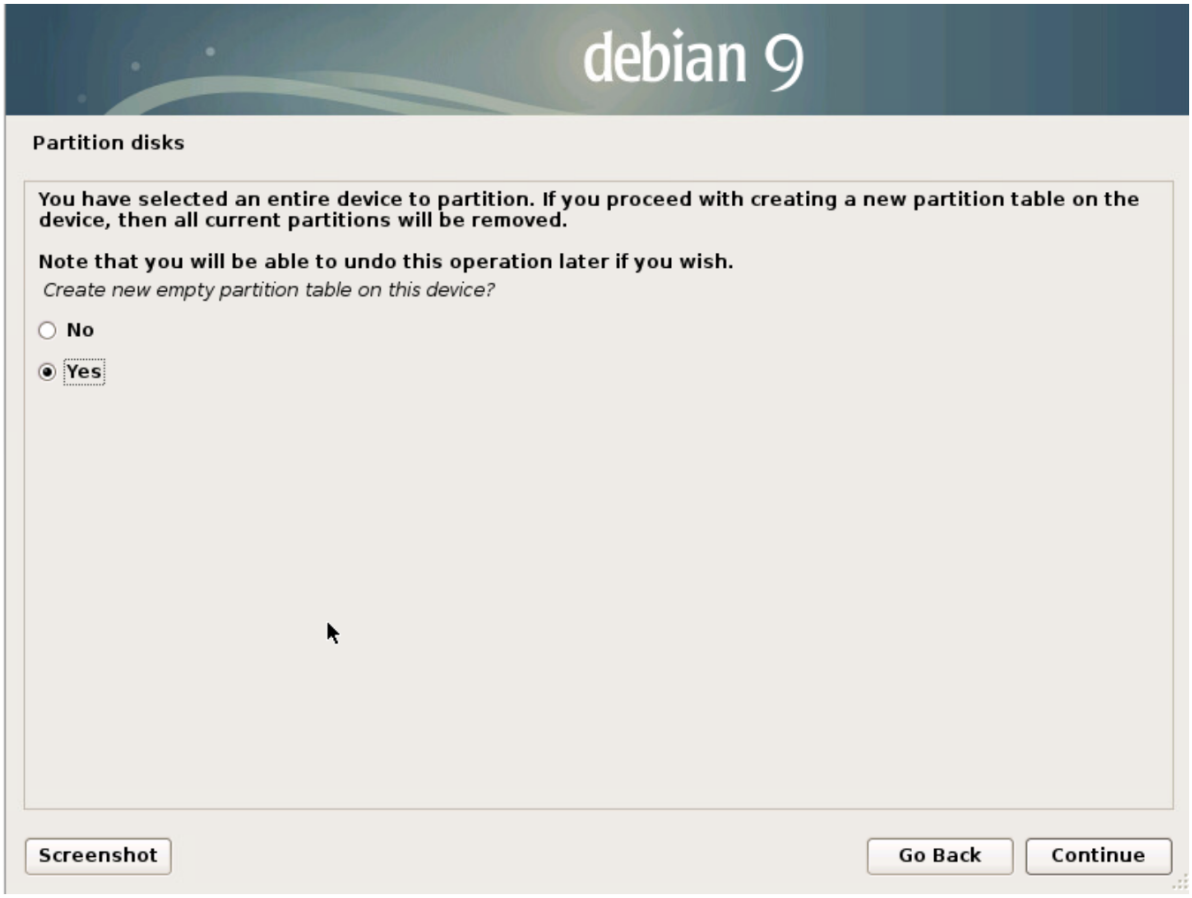

Рисунок 84 - Создание таблицы разделов

3. Выбрать вновь созданный пустой раздел на дополнительном диске (см. рисунок 85).

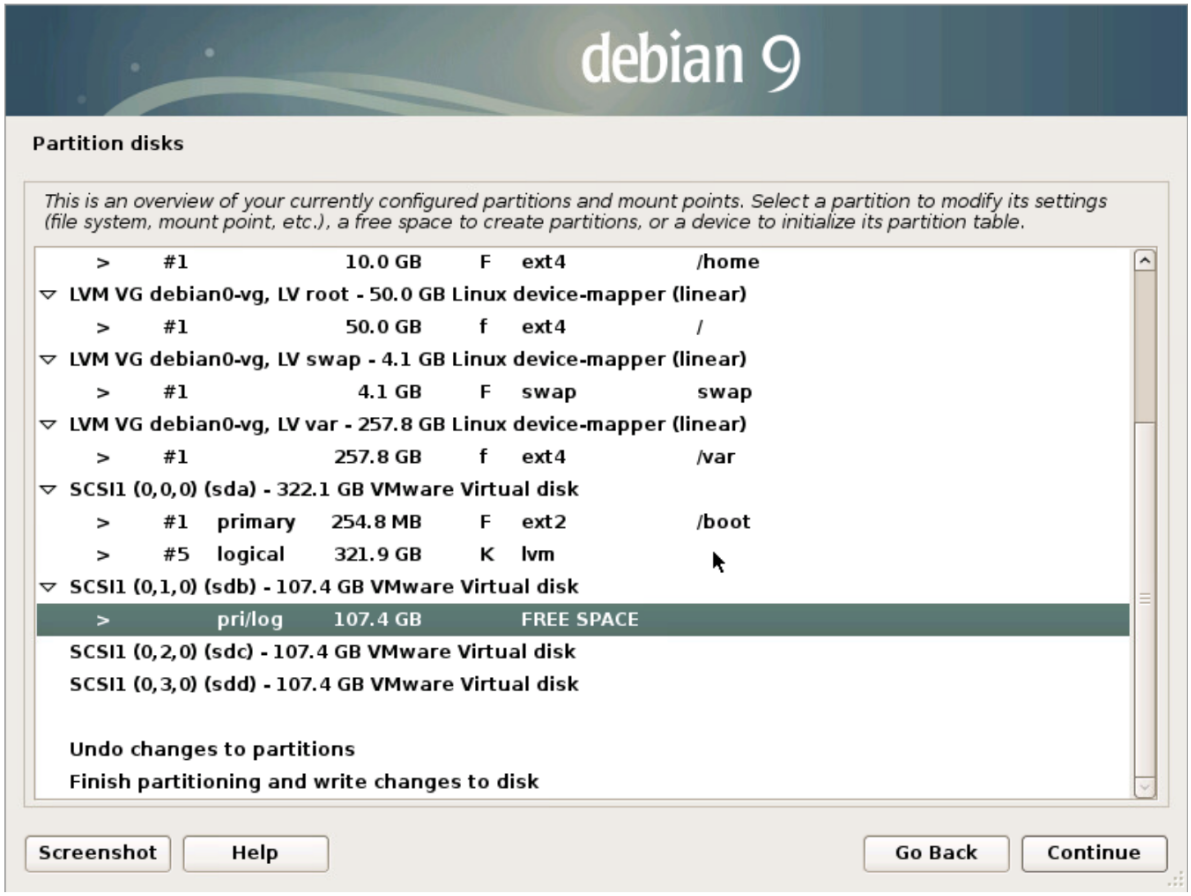

Рисунок 85 - Пустой раздел

4. Выбрать пункт «Create a new partition» и нажать кнопку «Continue» (см. рисунок 86).

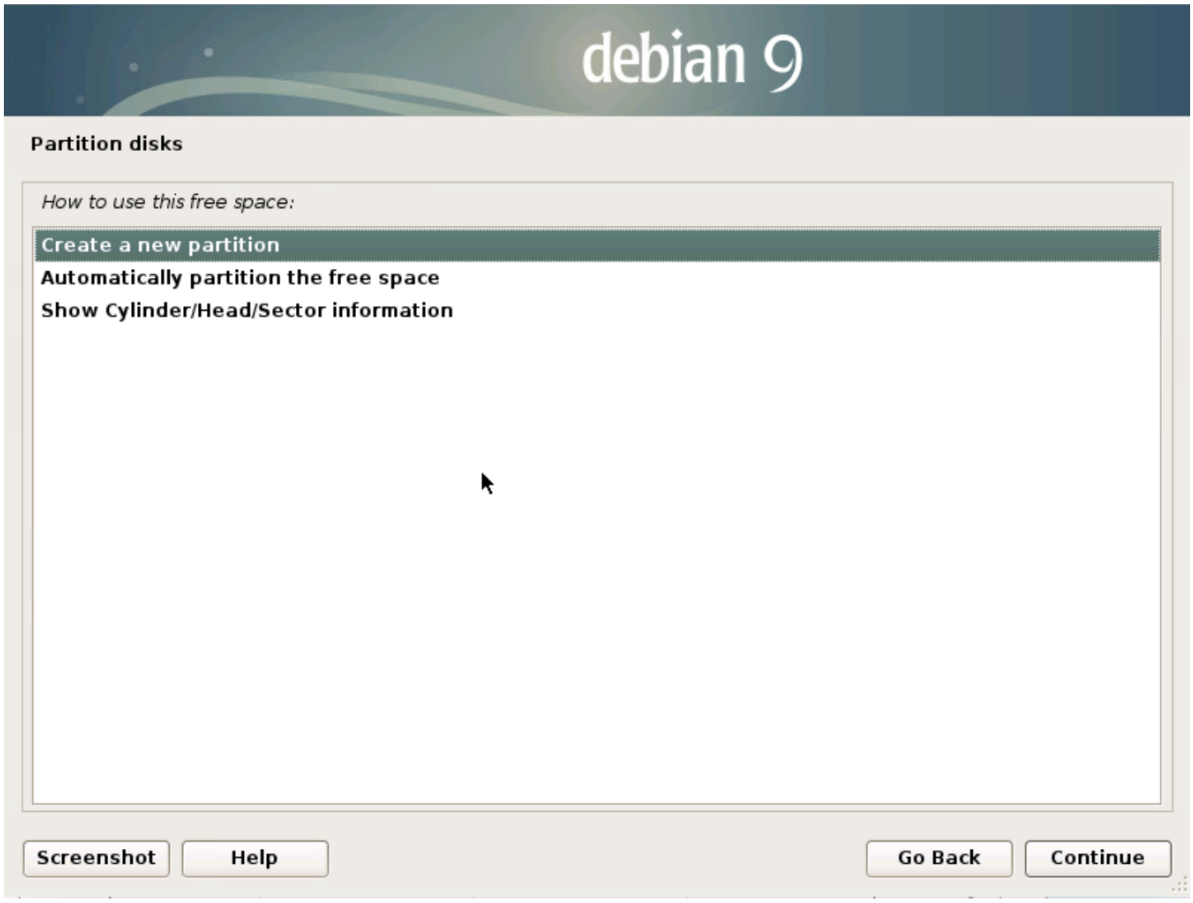

Рисунок 86 - Выбор действий

5. Указать объем раздела и нажать кнопку «Continue» (см. рисунок 87).

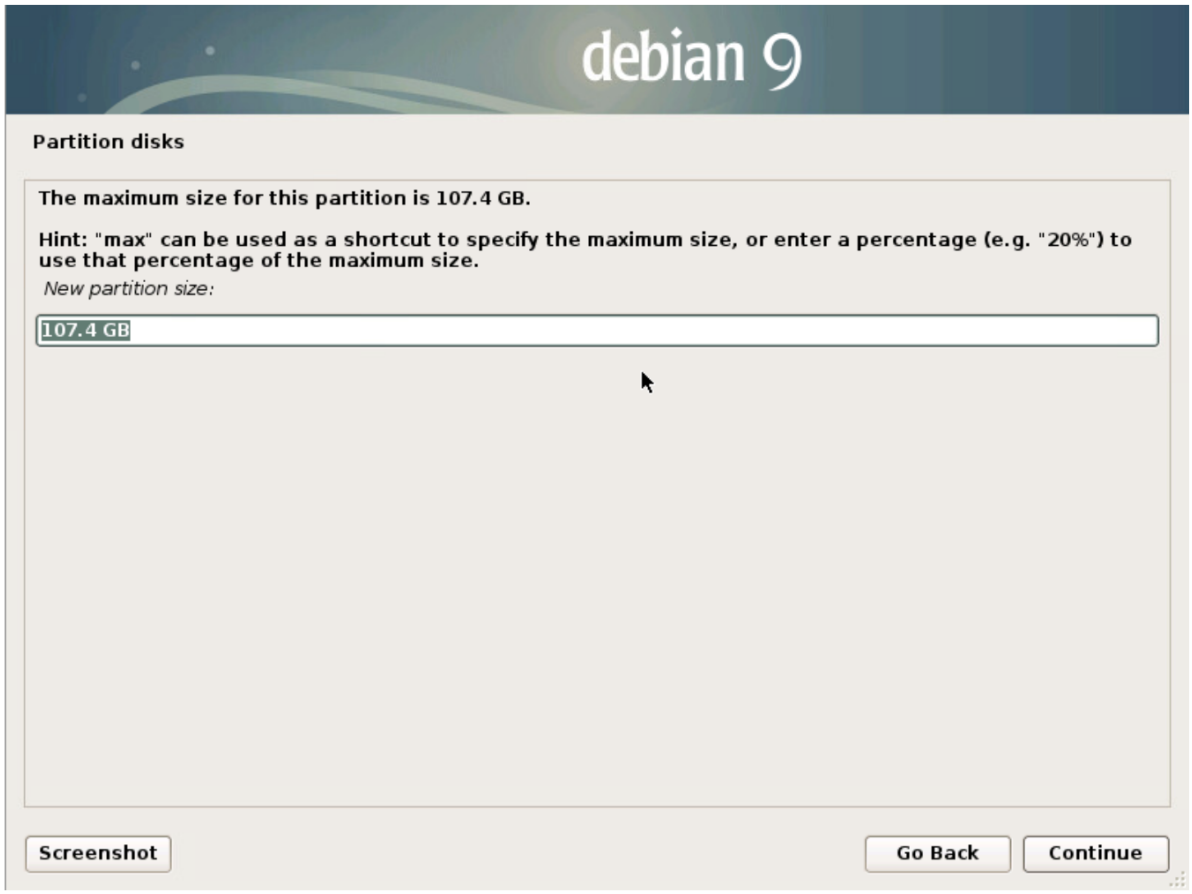

Рисунок 87 - Определение объема раздела

6. Выбрать тип раздела «Primary» и нажать кнопку «Continue» (см. рисунок 88).

Рисунок 88 - Определение типа раздела

7. Далее необходимо настроить параметры раздела (см. рисунок 89). Основные параметры:
    - «Use as» - установить «Ext4 journaling file system»;
    - «Mount point» - ввести «/dataN», где N - порядковый номер дополнительного физического диска, начиная с 1.
    - Выбрать пункт «Done setting up the partition» и нажать кнопку «Continue».

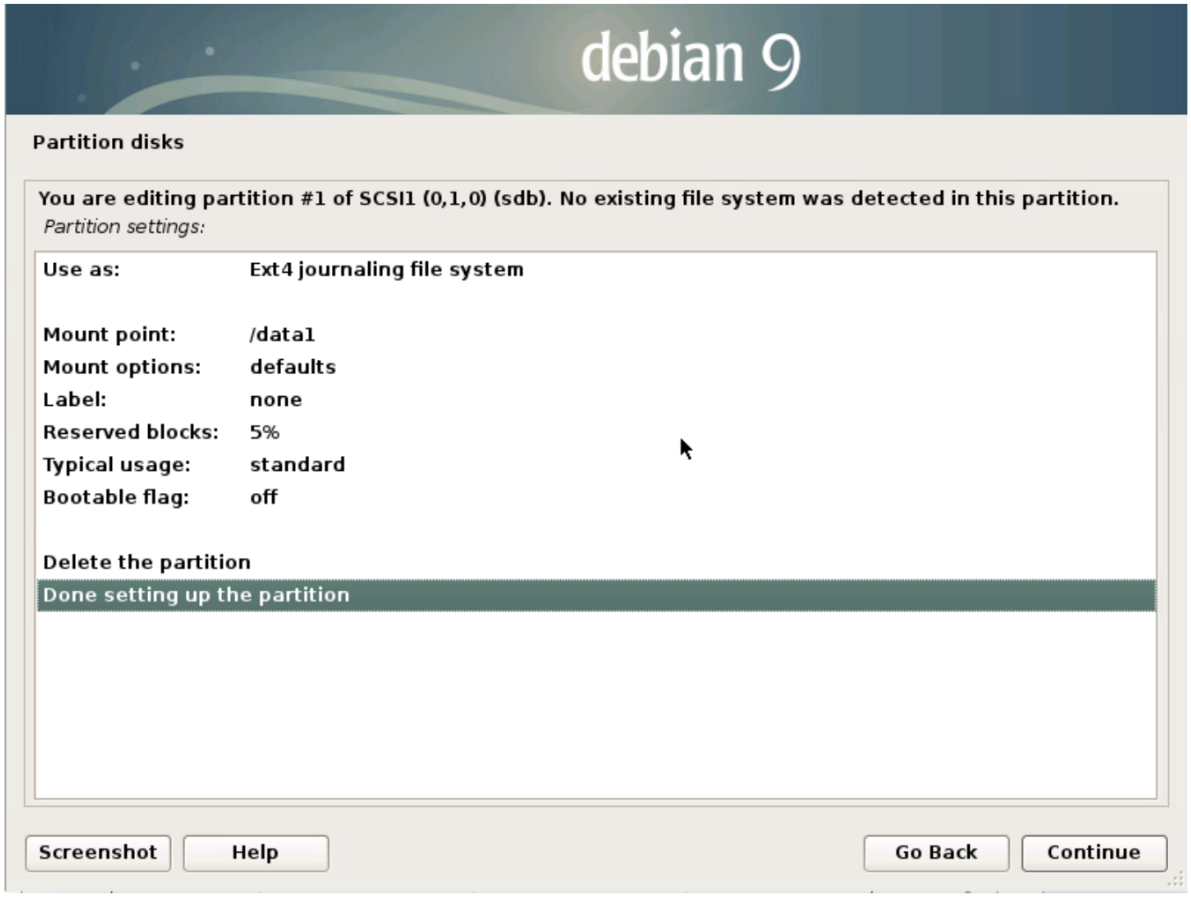

Рисунок 89 - Определение параметров раздела

8. Если дополнительных дисков более одного, то необходимо повторить все выше перечисленные действия для всех дополнительных физических дисков (см. рисунок 90).

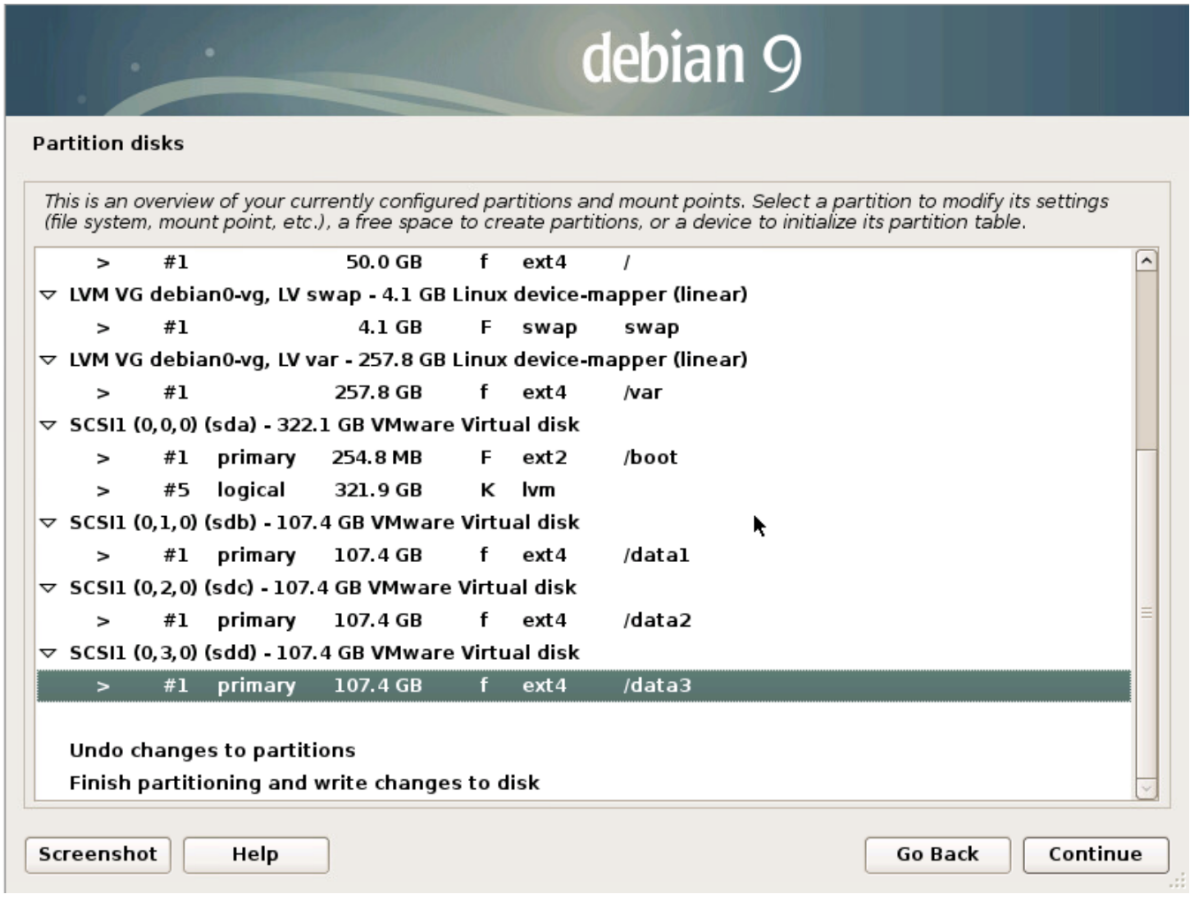

Рисунок 90 - Финальный вариант разметки

15. Перечень используемых Платформой портов

15.1. Централизованная установка Платформы

Ниже приведен перечень используемых портов при централизованной установке Платформы Радар:

Исходящий	Входящий	Порты	Описание
Log-Collector	Master	1500-5000, 9997-9999, 15403, 15404TCP/UDP	Передача данных от сборщика в балансировщик и менеджер очередей
Log-Collector	Источники событий	21, 22, 135, 445, 1443, 3306, 5432, 5601	Активный сбор событий
Log-Collector	Log-Collector	4813	Взаимодействие между двумя сборщиками
Log-Collector	Master	9000	Запрос конфигурационных данных
Master	Log-Collector	4805 4806	Мониторинг и сбор статистики. Управление сборщиком событий API
Источники событий	Log-Collector	162 SNMP trap 4807 UDP receiver 4808 TCP receiver 4809 TCP receiver SSL/TLS 4810 HTTP receiver 4811 HTTPS receiver 4812 NetFlow reciever	Пассивный сбор событий
Пользователи Платформы	Master	8080 9000 6676 6677	Доступ к интерфейсу платформы, проверка API ключей

15.2. Распределенная установка Платформы

Ниже приведенн перечень используемых портов при распределенной установке Платформы Радар (независимо от вариантов распределенной установки):

Исходящий	Входящий	Порты	Описание

Исходящий	Входящий	Порты	Описание
Correlator	Master	5672	Чтение нормализованных событий из очереди для корреляции
Correlator	Master	8086	Передача результатов корреляции
Log-Collector	Balancer	1500-5000, 9997-9999, 15403, 15404TCP/UDP	Передача данных от сборщика в балансировщик и менеджер очередей
Log-Collector	Источники событий	21, 22, 135, 445, 1443, 3306, 5432, 5601	Активный сбор событий
Log-Collector	Log-Collector	4813	Взаимодействие между двумя сборщиками
Log-Collector	Master	9000	Запрос конфигурационных данных
Master	Data	9200	Работа с сырыми событиями
Master	Correlator	2092	Управление правилами корреляции
Master	Log-Collector	4805 4806	Мониторинг и сбор статистики. Управление сборщиком событий API
Master	Balancer Correlator Data Worker	6676	Управление агентами кластера
Master	Balancer Correlator Data Worker	9100	Мониторинг и сбор статистики
Master	Balancer	9292, 9308	Мониторинг и сбор статистики
Master	Data	9114	Мониторинг и сбор статистики
Worker	Balancer	9092	Чтения событий из менеджера очередей для их обработки
Worker	Master	5672	Передача нормализованных событий в очередь на корреляцию
Worker	Data	9200	Передача событий на хранение

Исходящий	Входящий	Порты	Описание
Источники событий	Log-Collector	162 SNMP trap; 4807 UDP receiver; 4808 TCP receiver; 4809 TCP receiver SSL/TLS; 4810 HTTP receiver; 4811 HTTPS receiver; 4812 NetFlow reciever	Пассивный сбор событий
Пользователи Платформы	Master	8080 9000 6676 6677	Доступ к интерфейсу платформы, проверка API ключей
Data (с ролью Master)	Data (с ролью Data)	9300	Взаимодействие между нодами в кластере хранилища данных

16. Список доступных таймзон

Africa/Abidjan	America/Indiana/Winamac	Asia/Ho_Chi_Minh
Africa/Accra	America/Indianapolis	Asia/Hong_Kong
Africa/Addis_Ababa	America/Inuvik	Asia/Hovd
Africa/Algiers	America/Iqaluit	Asia/Irkutsk
Africa/Asmara	America/Jamaica	Asia/Istanbul
Africa/Asmera	America/Jujuy	Asia/Jakarta
Africa/Bamako	America/Juneau	Asia/Jayapura
Africa/Bangui	America/Kentucky/Louisville	Asia/Jerusalem
Africa/Banjul	America/Kentucky/Monticello	Asia/Kabul
Africa/Bissau	America/Knox_IN	Asia/Kamchatka
Africa/Blantyre	America/Kralendijk	Asia/Karachi
Africa/Brazzaville	America/La_Paz	Asia/Kashgar
Africa/Bujumbura	America/Lima	Asia/Kathmandu
Africa/Cairo	America/Los_Angeles	Asia/Katmandu
Africa/Casablanca	America/Louisville	Asia/Khandyga
Africa/Ceuta	America/Lower_Princes	Asia/Kolkata
Africa/Conakry	America/Maceio	Asia/Krasnoyarsk

Africa/Abidjan	America/Indiana/Winamac	Asia/Ho_Chi_Minh
Africa/Dakar	America/Managua	Asia/Kuala_Lumpur
Africa/Dar_es_Salaam	America/Manaus	Asia/Kuching
Africa/Djibouti	America/Marigot	Asia/Kuwait
Africa/Douala	America/Martinique	Asia/Macao
Africa/El_Aaiun	America/Matamoros	Asia/Macau
Africa/Freetown	America/Mazatlan	Asia/Magadan
Africa/Gaborone	America/Mendoza	Asia/Makassar
Africa/Harare	America/Menominee	Asia/Manila
Africa/Johannesburg	America/Merida	Asia/Muscat
Africa/Juba	America/Metlakatla	Asia/Nicosia
Africa/Kampala	America/Mexico_City	Asia/Novokuznetsk
Africa/Khartoum	America/Miquelon	Asia/Novosibirsk
Africa/Kigali	America/Moncton	Asia/Omsk
Africa/Kinshasa	America/Monterrey	Asia/Oral
Africa/Lagos	America/Montevideo	Asia/Phnom_Penh
Africa/Libreville	America/Montreal	Asia/Pontianak
Africa/Lome	America/Montserrat	Asia/Pyongyang
Africa/Luanda	America/Nassau	Asia/Qatar
Africa/Lubumbashi	America/New_York	Asia/Qyzylorda
Africa/Lusaka	America/Nipigon	Asia/Rangoon
Africa/Malabo	America/Nome	Asia/Riyadh
Africa/Maputo	America/Noronha	Asia/Saigon
Africa/Maseru	America/North_Dakota/Beulah	Asia/Sakhalin
Africa/Mbabane	America/North_Dakota/Center	Asia/Samarkand
Africa/Mogadishu	America/North_Dakota/New_Salem	Asia/Seoul
Africa/Monrovia	America/Ojinaga	Asia/Shanghai
Africa/Nairobi	America/Panama	Asia/Singapore
Africa/Ndjamena	America/Pangnirtung	Asia/Srednekolymsk
Africa/Niamey	America/Paramaribo	Asia/Taipei
Africa/Nouakchott	America/Phoenix	Asia/Tashkent
Africa/Ouagadougou	America/Port	au
Africa/Porto	Novo	America/Port_of_Spain
Africa/Sao_Tome	America/Porto_Acre	Asia/Tel_Aviv
Africa/Timbuktu	America/Porto_Velho	Asia/Thimbu
Africa/Tripoli	America/Puerto_Rico	Asia/Thimphu

Africa/Abidjan	America/Indiana/Winamac	Asia/Ho_Chi_Minh
Africa/Tunis	America/Punta_Arenas	Asia/Tokyo
Africa/Windhoek	America/Rainy_River	Asia/Tomsk
America/Adak	America/Rankin_Inlet	Asia/Ujung_Pandang
America/Anchorage	America/Recife	Asia/Ulaanbaatar
America/Anguilla	America/Regina	Asia/Ulan_Bator
America/Antigua	America/Resolute	Asia/Urumqi
America/Araguaina	America/Rio_Branco	Asia/Ust
America/Argentina/Buenos_Aires	America/Rosario	Asia/Vientiane
America/Argentina/Catamarca	America/Santa_Isabel	Asia/Vladivostok
America/Argentina/ComodRivadavia	America/Santarem	Asia/Yakutsk
America/Argentina/Cordoba	America/Santiago	Asia/Yangon
America/Argentina/Jujuy	America/Santo_Domingo	Asia/Yekaterinburg
America/Argentina/La_Rioja	America/Sao_Paulo	Asia/Yerevan
America/Argentina/Mendoza	America/Scoresbysund	Atlantic/Azores
America/Argentina/Rio_Gallegos	America/Shiprock	Atlantic/Bermuda
America/Argentina/Salta	America/Sitka	Atlantic/Canary
America/Argentina/San_Juan	America/St_Barthelemy	Atlantic/Cape_Verde
America/Argentina/San_Luis	America/St_Johns	Atlantic/Faeroe
America/Argentina/Tucuman	America/St_Kitts	Atlantic/Faroe
America/Argentina/Ushuaia	America/St_Lucia	Atlantic/Jan_Mayen
America/Aruba	America/St_Thomas	Atlantic/Madeira
America/Asuncion	America/St_Vincent	Atlantic/Reykjavik
America/Atikokan	America/Swift_Current	Atlantic/South_Georgia
America/Atka	America/Tegucigalpa	Atlantic/St_Helena
America/Bahia	America/Thule	Atlantic/Stanley
America/Bahia_Banderas	America/Thunder_Bay	Australia/ACT
America/Barbados	America/Tijuana	Australia/Adelaide
America/Belem	America/Toronto	Australia/Brisbane
America/Belize	America/Tortola	Australia/Broken_Hill
America/Blanc	Sablon	America/Vancouver
America/Boa_Vista	America/Virgin	Australia/Currie
America/Bogota	America/Whitehorse	Australia/Darwin
America/Boise	America/Winnipeg	Australia/Eucla
America/Buenos_Aires	America/Yakutat	Australia/Hobart
America/Cambridge_Bay	America/Yellowknife	Australia/LHI

Africa/Abidjan	America/Indiana/Winamac	Asia/Ho_Chi_Minh
America/Campo_Grande	Antarctica/Casey	Australia/Lindeman
America/Cancun	Antarctica/Davis	Australia/Lord_Howe
America/Caracas	Antarctica/DumontDUrville	Australia/Melbourne
America/Catamarca	Antarctica/Macquarie	Australia/NSW
America/Cayenne	Antarctica/Mawson	Australia/North
America/Cayman	Antarctica/McMurdo	Australia/Perth
America/Chicago	Antarctica/Palmer	Australia/Queensland
America/Chihuahua	Antarctica/Rothera	Australia/South
America/Coral_Harbour	Antarctica/South_Pole	Australia/Sydney
America/Cordoba	Antarctica/Syowa	Australia/Tasmania
America/Costa_Rica	Antarctica/Troll	Australia/Victoria
America/Creston	Antarctica/Vostok	Australia/West
America/Cuiaba	Arctic/Longyearbyen	Australia/Yancowinna
America/Curacao	Asia/Aden	Brazil/Acre
America/Danmarkshavn	Asia/Almaty	Brazil/DeNoronha
America/Dawson	Asia/Amman	Brazil/East
America/Dawson_Creek	Asia/Anadyr	Brazil/West
America/Denver	Asia/Aqtau	CET
America/Detroit	Asia/Aqtobe	CST6CDT
America/Dominica	Asia/Ashgabat	Canada/Atlantic
America/Edmonton	Asia/Ashkhabad	Canada/Central
America/Eirunepe	Asia/Atyrau	Canada/Eastern
America/El_Salvador	Asia/Baghdad	Canada/Mountain
America/Ensenada	Asia/Bahrain	Canada/Newfoundland
America/Fort_Nelson	Asia/Baku	Canada/Pacific
America/Fort_Wayne	Asia/Bangkok	Canada/Saskatchewan
America/Fortaleza	Asia/Barnaul	Canada/Yukon
America/Glace_Bay	Asia/Beirut	Chile/Continental
America/Godthab	Asia/Bishkek	Chile/EasterIsland
America/Goose_Bay	Asia/Brunei	Cuba
America/Grand_Turk	Asia/Calcutta	EET
America/Grenada	Asia/Chita	EST
America/Guadeloupe	Asia/Choibalsan	EST5EDT
America/Guatemala	Asia/Chongqing	Egypt
America/Guayaquil	Asia/Chungking	Eire

Africa/Abidjan	America/Indiana/Winamac	Asia/Ho_Chi_Minh
America/Guyana	Asia/Colombo	Etc/GMT
America/Halifax	Asia/Dacca	Etc/GMT+0
America/Havana	Asia/Damascus	Etc/GMT+1
America/Hermosillo	Asia/Dhaka	Etc/GMT+10
America/Indiana/Indianapolis	Asia/Dili	Etc/GMT+11
America/Indiana/Knox	Asia/Dubai	Etc/GMT+12
America/Indiana/Marengo	Asia/Dushanbe	Etc/GMT+2
America/Indiana/Petersburg	Asia/Famagusta	Etc/GMT+3
America/Indiana/Tell_City	Asia/Gaza	Etc/GMT+4
America/Indiana/Vevay	Asia/Harbin	Etc/GMT+5
America/Indiana/Vincennes	Asia/Hebron	Etc/GMT+6
Europe/Amsterdam	GB	Etc/GMT+7
Europe/Andorra	GB-Eire	Etc/GMT+8
Europe/Astrakhan	GMT	Etc/GMT+9
Europe/Athens	GMT+0	Etc/GMT-0
Europe/Belfast	GMT-0	Etc/GMT-1
Europe/Belgrade	GMT0	Etc/GMT-10
Europe/Berlin	Greenwich	Etc/GMT-11
Europe/Bratislava	HST	Etc/GMT-12
Europe/Brussels	Hongkong	Etc/GMT-13
Europe/Bucharest	Iceland	Etc/GMT-14
Europe/Budapest	Indian/Antananarivo	Etc/GMT-2
Europe/Busingen	Indian/Chagos	Etc/GMT-3
Europe/Chisinau	Indian/Christmas	Etc/GMT-4
Europe/Copenhagen	Indian/Cocos	Etc/GMT-5
Europe/Dublin	Indian/Comoro	Etc/GMT-6
Europe/Gibraltar	Indian/Kerguelen	Etc/GMT-7
Europe/Guernsey	Indian/Mahe	Etc/GMT-8
Europe/Helsinki	Indian/Maldives	Etc/GMT-9
Europe/Isle_of_Man	Indian/Mauritius	Etc/GMT0
Europe/Istanbul	Indian/Mayotte	Etc/Greenwich
Europe/Jersey	Indian/Reunion	Etc/UCT
Europe/Kaliningrad	Iran	Etc/UTC
Europe/Kiev	Israel	Etc/Universal
Europe/Kirov	Jamaica	Etc/Zulu

Africa/Abidjan	America/Indiana/Winamac	Asia/Ho_Chi_Minh
Europe/Lisbon	Japan	Pacific/Norfolk
Europe/Ljubljana	Kwajalein	Pacific/Noumea
Europe/London	Libya	Pacific/Pago_Pago
Europe/Luxembourg	MET	Pacific/Palau
Europe/Madrid	MST	Pacific/Pitcairn
Europe/Malta	MST7MDT	Pacific/Pohnpei
Europe/Mariehamn	Mexico/BajaNorte	Pacific/Ponape
Europe/Minsk	Mexico/BajaSur	Pacific/Port_Moresby
Europe/Monaco	Mexico/General	Pacific/Rarotonga
Europe/Moscow	NZ	Pacific/Saipan
Europe/Nicosia	NZ	CHAT
Europe/Oslo	Navajo	Pacific/Tahiti
Europe/Paris	PRC	Pacific/Tarawa
Europe/Podgorica	PST8PDT	Pacific/Tongatapu
Europe/Prague	Pacific/Apia	Pacific/Truk
Europe/Riga	Pacific/Auckland	Pacific/Wake
Europe/Rome	Pacific/Bougainville	Pacific/Wallis
Europe/Samara	Pacific/Chatham	Pacific/Yap
Europe/San_Marino	Pacific/Chuuk	Poland
Europe/Sarajevo	Pacific/Easter	Portugal
Europe/Saratov	Pacific/Efate	ROC
Europe/Simferopol	Pacific/Enderbury	ROK
Europe/Skopje	Pacific/Fakaofo	Singapore
Europe/Sofia	Pacific/Fiji	Turkey
Europe/Stockholm	Pacific/Funafuti	UCT
Europe/Tallinn	Pacific/Galapagos	US/Alaska
Europe/Tirane	Pacific/Gambier	US/Aleutian
Europe/Tiraspol	Pacific/Guadalcanal	US/Arizona
Europe/Ulyanovsk	Pacific/Guam	US/Central
Europe/Uzhgorod	Pacific/Honolulu	US/East
Europe/Vaduz	Pacific/Johnston	US/Eastern
Europe/Vatican	Pacific/Kiritimati	US/Hawaii
Europe/Vienna	Pacific/Kosrae	US/Indiana
Europe/Vilnius	Pacific/Kwajalein	US/Michigan
Europe/Volgograd	Pacific/Majuro	US/Mountain

Africa/Abidjan	America/Indiana/Winamac	Asia/Ho_Chi_Minh
Europe/Warsaw	Pacific/Marquesas	US/Pacific
Europe/Zagreb	Pacific/Midway	US/Pacific
Europe/Zaporozhye	Pacific/Nauru	US/Samoa
Europe/Zurich	Pacific/Niue	UTC

17. Включение режима распределенной корреляции

Для включения режима распределенной корреляции необходимо добавить узел в кластер платформы и назначить этому узлу роль **Correlator**. После этого выполнить настройку всех экземпляров коррелятора.

17.1. Настройка экземпляров коррелятора

Включение функции распределенной корреляции осуществляется на всех экземплярах коррелятора в конфигурационном файле `/opt/pangeoradar/configs/logmule/conf.yaml`.

1. Зайдите в раздел «**Администрирование**» — «**Кластер**» — «**Узлы**», найдите узлы с ролями **Correlator** и узнайте их IP-адреса.
2. Подключитесь к узлу по SSH и добавьте параметр **shared_instance** в конфигурационный файл узла с помощью команды:

   `nano /opt/pangeoradar/configs/logmule/conf.yaml`
3. Для включения в конфигурационный файл нужно добавить следующую строку: `shared_instance: true`. Сохраните изменения.
4. Если необходимо, подключитесь ко следующему узлу аналогично пункту 2.
5. Тогда для первого узла коррелятора выставите значение `shared_instance: false`. Для второго узла — `shared_instance: true`.
6. Сохраните конфигурационные файлы и перезапустите службу с помощью команды:

   `service pangeoradar-logmule restart`

17.2. Настройка правила для работы с несколькими корреляторами

Для переключения правила в режим распределенной корреляции нужно сделать следующее:

1. В веб-интерфейсе перейдите в раздел «**Коррелятор**» — «**Правила**».
2. Нажмите на пиктограмму карандаша у правила, которое необходимо переключить в режим распределенной корреляции.
3. В режиме редактирования правила создайте новое хранилище значений с названием **shared_memory** (переменные можно оставить пустыми).
4. Добавьте хранилище **shared_memory** к правилу, как изображено на рисунке 91.
5. Сохраните изменения.

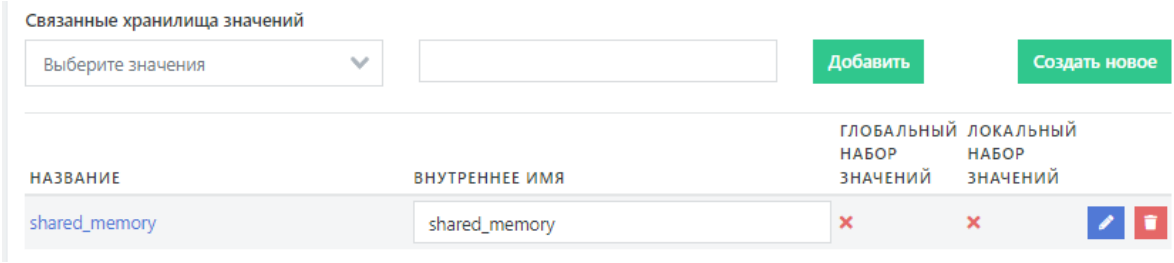

Рисунок 91 - Добавление хранилища shared_memory

Для проверки работы режима распределенной корреляции необходимо перейти в раздел «**Коррелятор**» — «**Правила**».

При переключении между экземплярами коррелятора правило, в которое было добавлено хранилище **shared_memory**, будет помечено как активное.

Для переключения между экземплярами коррелятора необходимо нажать на выпадающее меню с названием экземпляра, как изображено на рисунке 92.

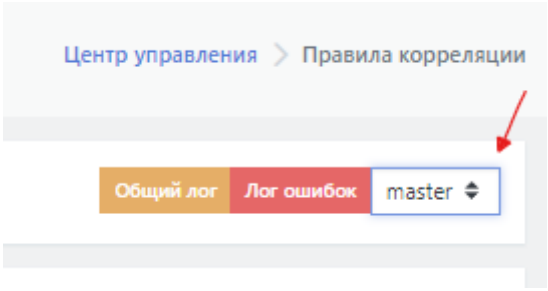

Рисунок 92 - Переключение между экземплярами коррелятора

17.3. Проверка работы правила

Для проверки работы правила при распределенной коммутации необходимо сгенерировать ситуацию, для которой выбранное для проверки правило будет срабатывать. Например, для выбранного для проверки правила **Account_added_and_removed_from_a_group_in_short_period_of_time** необходимо выполнить следующие действия:

1. Подключиться по RDP к лог-коллектору.
2. Запустить командную строку от имени Администратора.
3. Выполнить попытку добавление нового пользователя в Платформу, выполнив команду:

   `C:\Log-collector\user_add_to_group.cmd`

После завершения выполнения команды перейти в веб-интерфейс Платформы в раздел «**Инциденты**». При правильной отработке правила в данном разделе в списке инцидентов отобразится инцидент с названием «**MS-WIN – Пользователь добавлен в локальную группу или удален из нее**» и IP-адресом лог-коллектора.

18. Настройка интеграции со службой Active Directory

В **Платформе Радар** предусмотрена возможность использования доменных учетных записей посредством интеграции с Active Directory.

Для настройки интеграции необходимо:

- указать адрес LDAP сервера,
- указать аккаунт и пароль для поиска по LDAP в настройках KeyCloak.

Если на контроллере(ах) домена LDAP ранее не настраивался, то необходимо установить **Microsoft Identity Management for UNIX Role Service** (см. рисунок 93).

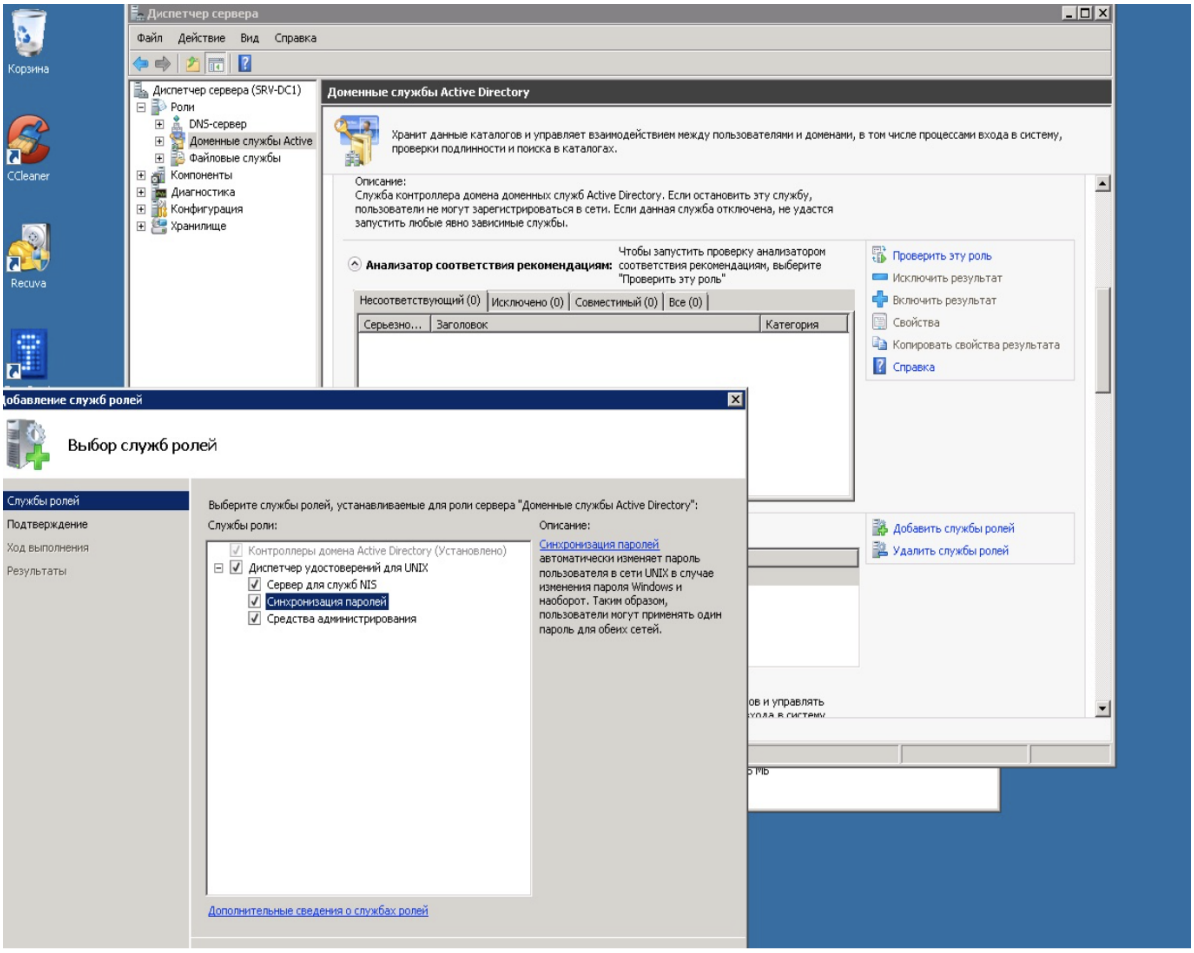

Рисунок 93 - Выбор служб ролей в Microsoft Identity Management for UNIX Role Service

> Данная настройка необходима на контроллерах домена под управлением Windows Server 2008 и ниже. На контроллерах домена под управлением Windows Server 2012 и выше установка **Microsoft Identity Management for UNIX Role Service** не требуется.

18.1. Настройка LDAP

После установки службы перейдите в KeyCloak и начните настройку LDAP, выполнив следующие действия:

1. Откройте консоль администрирования **KeyCloak** (<адрес Платформы Радар>:8180) и перейдите в пункт меню "**Федерация пользователей**" (см. рисунок 94).
2. Откройте список "**Добавить поставщика**" (см. рисунок 94).

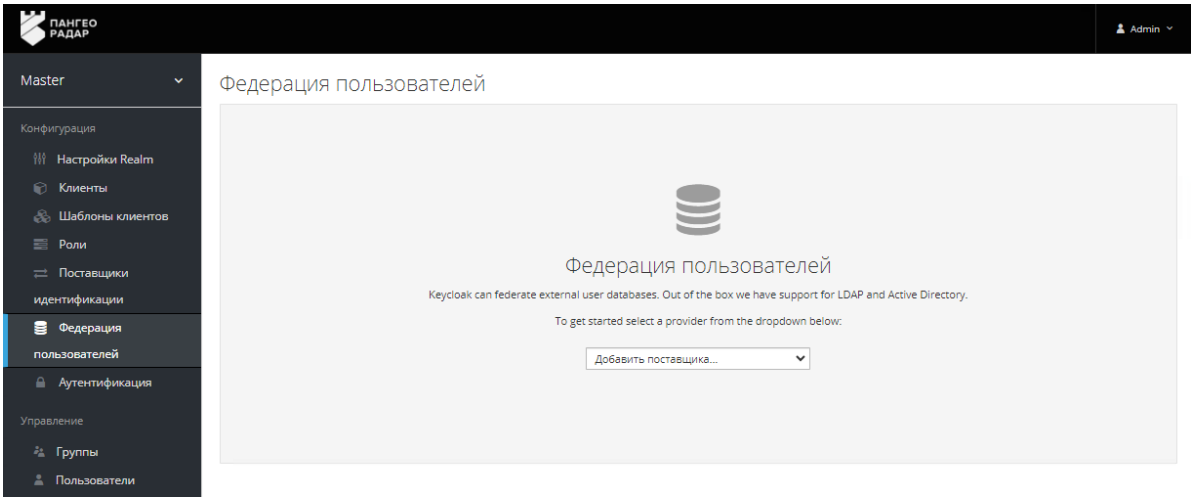

Рисунок 94 - Консоль администрирования KeyCloak, раздел меню "Федерация пользователей", список "Добавить поставщика"

3. В открывшемся списке "**Добавить поставщика**" выберите раздел "**LDAP**" и заполните на вкладке "Требуемые настройки" предоставленные программой поля (см. рисунок 95). Следующие поля обязательны для заполнения:
    - `Включено` - значение ВКЛ (устанавливается по умолчанию);
    - `Наименование в консоли` - ldap (устанавливается по умолчанию);
    - `Приоритет` - 0 (устанавливается по умолчанию);
    - `Импортировать пользователей` - значение ВКЛ (устанавливается по умолчанию);
    - `Режим редактирования` - READ_ONLY (выбрать из списка);
    - `Синхронизировать регистрации` - значение ВЫК (устанавливается по умолчанию);
    - `Поставщик` - указать Active Directory;
    - `Атрибут Username в LDAP` - указать sAMAccountName или cn;
    - `Атрибут RDN в LDAP` - значение cn (установлено по умолчанию);
    - `Атрибут UUID в LDAP` - значение objectGUID (установлено по умолчанию);
    - `Классы объектов пользователя` - значения person, organizationPerson, user (установлены по умолчанию);
    - `URL соединения` - указать IP-адрес сервера Active Directory, например - ldap://srv-dc2.youdomain.local ;
    - `Пользователи DN` - в соответствии с примером `DC=youdomain,DC=local` ;
    - `Пользовательский фильтр LDAP пользователей` - оставить пустым, если не требуется фильтрация списка пользователей;
    - `Поиск области` - выберите One level;
    - `Тип аутентификации` - выбрать Simple;
    - `Сопоставление DN` - указать системный аккаунт в Active Director для чтения данных из LDAP (например, ldap-ro-user@youdoman.local) ;
    - `Сопоставление учетных данных` - пароль системного аккаунта.

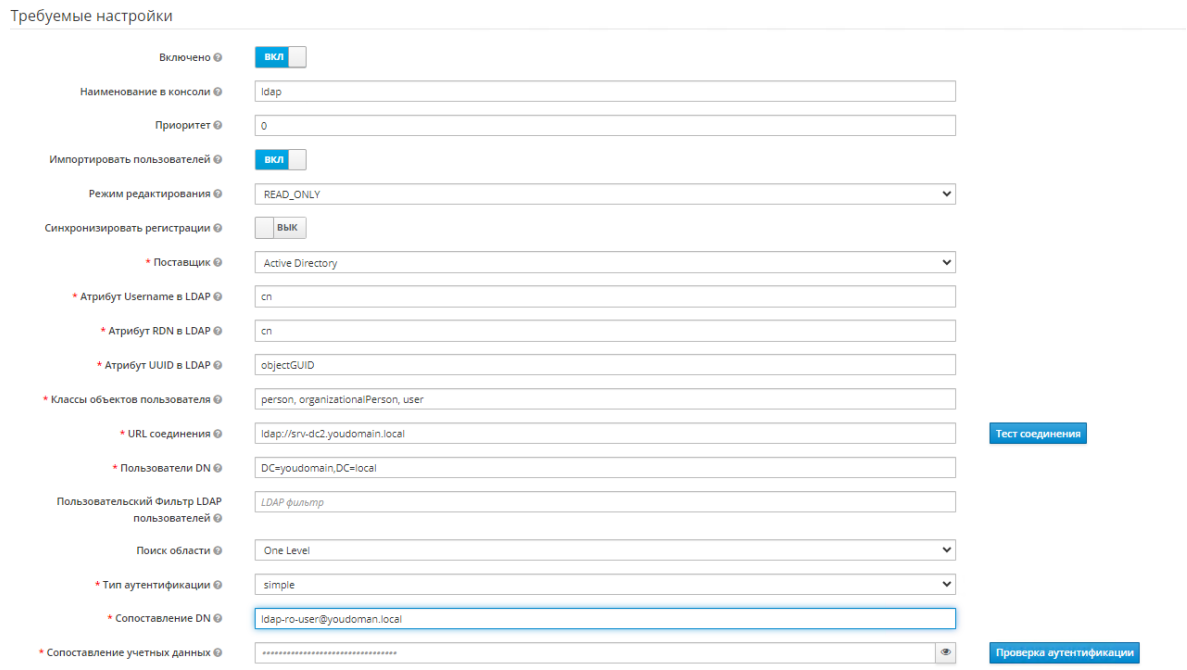

Рисунок 95 - Заполнение данных по LDAP

4. При необходимости можно протестировать введенные параметры LDAP, нажав последовательно кнопки "**Тест соединения**" и "**Проверка аутентификации**" (см. рисунок 95).
5. Для сохранения введённых настроек LDAP нажмите кнопку **Сохранить**, расположенную в самом низу экрана.

После сохранения отобразятся кнопки синхронизации пользователей. Нажмите кнопку **Синхронизировать всех пользователей** (см. рисунок 96), чтобы загрузить список пользователей из домена.

Рисунок 96 - Синхронизация пользователей

18.2. Определение возможных причин сбоя при синхронизации

Если синхронизация пользователей не произошла, то для определения причины сбоя в первую очередь надо смотреть лог плагина `/opt/wildfly/standalone/log/keycloak.log`. В логе следует просмотреть события, зафиксированные в момент нажатия тестовых кнопок или кнопок синхронизации пользователей.

19. Служба уведомлений Toller

19.1. Назначение ПО

Данный программный модуль предназначен для формирования уведомлений от Платформы Радар и пересылки сформированных уведомлений пользователям и администраторам.

19.2. Конфигурация Toller

Конфигурация Toller располагается в меню администрирования Кластер - Управление конфигурацией - Toller (см. рисунок 97).

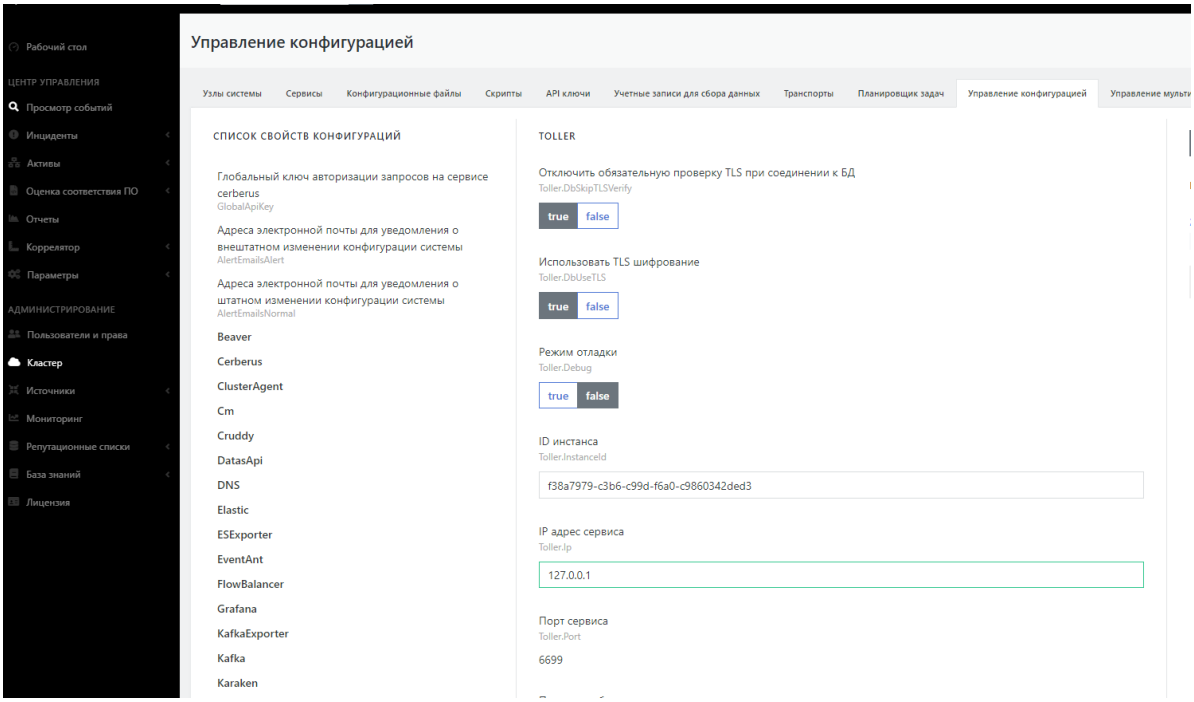

Рисунок 97 - Настройки Toller

19.3. Настройка пользователей

Для настройки получения уведомлений от Платформы Радар конкретными пользователями необходимо выполнить следующие шаги:

1. Зайти в интерфейс Платформы Радар с правами администратора
2. Перейти в раздел "Администрирование", "Пользователи и права", как изображено на рисунке 98;

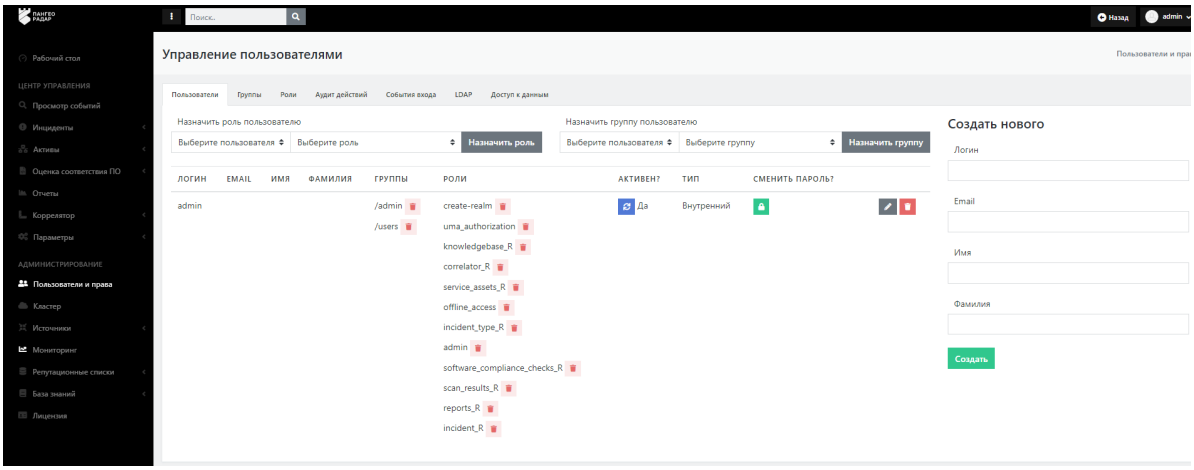

Рисунок 98 - Пользователи и права

3. Найти или создать нужного пользователя и нажать на кнопку редактирования  в строке данного пользователя;

   В правой части страницы откроется форма редактирования параметров пользователя, как изображено на рисунке 99;

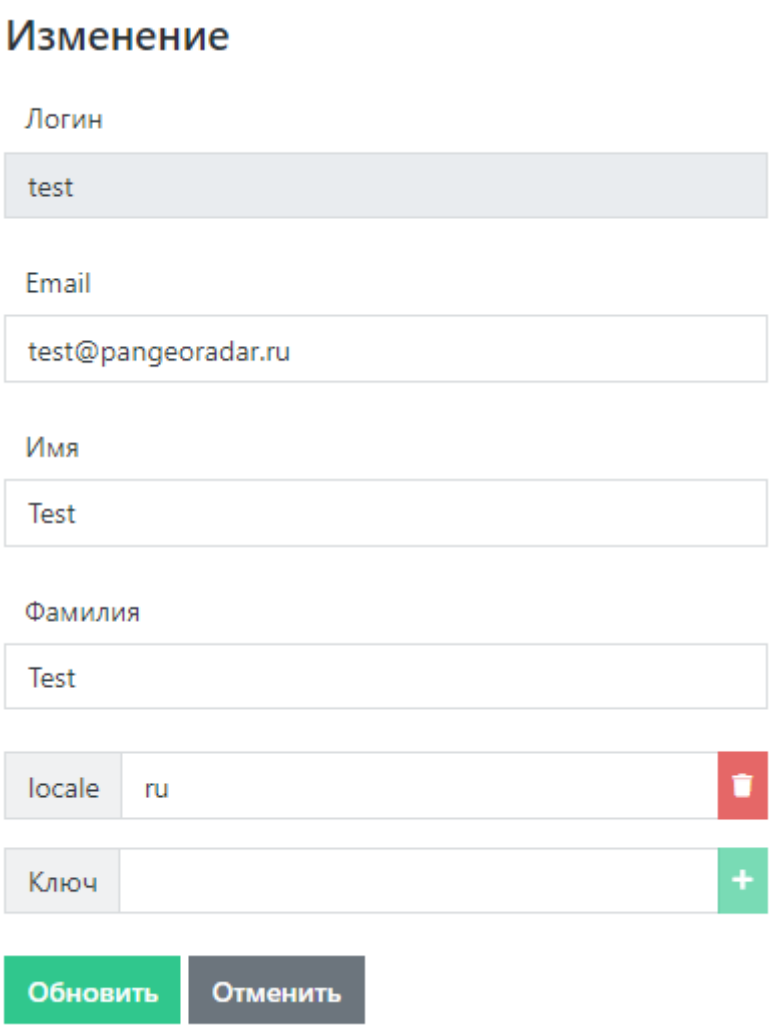

Рисунок 99 - Параметры пользователя

4. Указать актуальный "Email" пользователя, на который предусмотрена отправка уведомлений;
5. Нажать кнопку "Обновить" для сохранения введённых настроек;
6. Авторизоваться под только что созданным\отредактированным пользователем;
7. Перейти в настройки профиля данного пользователя, нажав на имя пользователя в правом верхнем углу интерфейса и нажав на кнопку "Профиль";
8. Произвести необходимые настройки оповещений, как изображено на рисунке 100;

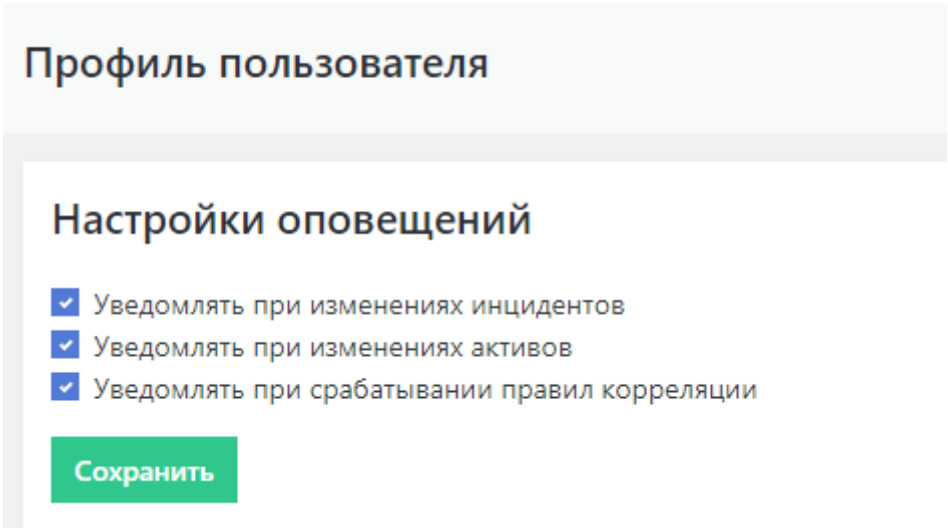

Рисунок 100 - Настройки оповещений

9. Нажать кнопку "Сохранить" для сохранения настроек.

При корректном выполнении вышеописанных действий данный пользователь будет получать уведомления Платформы Радар на указанный в параметрах учетной записи почтовый адрес.

19.4. Настройка оповещений о работе сервисов

Для настройки оповещений о работе сервисов необходимо сделать следующее (все действия необходимо выполнять под привилегированным пользователем):

1. Произвести настройку службы node_exporter;

   Расположение конфигурационного файла: `/etc/systemd/system/node_exporter.service`

   В конец строки ExecStart добавить `--collector.systemd`

   После чего конфигурационный файл должен выглядеть следующим образом:

   ```
   [Unit]
   Description=Node Exporter
   Wants=network-online.target
   After=network-online.target

   [Service]
   User=node_exporter
   Group=node_exporter
   Type=simple
   ExecStart=/opt/pangeoradar/node_exporter/node_exporter --web.listen-
   address=":9101" --collector.systemd

   [Install]
   WantedBy=multi-user.target
   ```

2. Далее необходимо выполнить команду `sudo systemctl daemon-reload`
3. После чего, перезапустить службу node_exporter командой `sudo service node_exporter restart`

> "Оповещения будут отправляться на адрес, указанный в параметре SmtpDefaultTo" конфигурационного файла `/opt/pangeoradar/configs/pangeoradar-toller.yaml`"

20. Резервное копирование

20.1. Способы для снятия резервной копии ElasticSearch

Ниже представлен один из способов работы со снятием резервных копий индексов ElasticSearch путем архивирования индексов. Важно помнить, что для корректной работы потребуется curator версии старше 5.0.

20.1.1. Архивирование индексов

В файле `/etc/elasticsearch/elasticsearch.yml` прописан путь до файлового репозитория:

```
path.repo: /opt/elasticsearch/snapshots
```

Если такой строки нет, необходимо прописать и перезагрузить elasticsearch.

Далее необходимо создать репозиторий, в котором будут размещены снапшоты:

```
mkdir -p /opt/elasticsearch/snapshots/repository
curl -k -XPUT 'https://localhost:9200/_snapshot/repository' -H 'Content-Type:
application/json' -d '{
    "type": "fs",
    "settings": {
        "location": "repository",
        "compress": true
    }
}'
```

Также необходимо создать ещё один репозиторий с именем «recovery», который понадобится для восстановления индексов:

```
mkdir -p /opt/elasticsearch/snapshots/recovery
curl -k -XPUT 'https://localhost:9200/_snapshot/recovery' -H 'Content-Type:
application/json' -d '{
    "type": "fs",
    "settings": {
        "location": "recovery",
        "compress": true
    }
}'
```

Далее представлен пример скрипта для архивирования индексов.

Логика работы скрипта описана в комментариях. Не забудьте поправить значения переменных, если ваши настройки будут отличаться от дефолтных.

```
#!/bin/bash

DAYS=31 #Количество дней, от текущей даты, старше которого индексы будут
архивироваться
SNAPSHOT_DIRECTORY="/opt/elasticsearch/snapshots"
BACKUP_DIR="/opt/elasticsearch/elasticsearch_backup"
REPOSITORY="repository"
LOG="/var/log/elasticsearch/elasticsearch_backup.log"
DATE=`date`

#Проверим существование папки для архивов и если нет, создадим её
if ! [ -d $BACKUP_DIR ]; then
  mkdir -p $BACKUP_DIR
fi

#Получаем массив индексов, которые старше $DAYS
```

```
INDICES=`curator_cli --config /etc/elasticsearch/curator-config.yml --host
localhost --port 9200 show_indices --filter_list "
[{\"filtertype\":\"age\",\"source\":\"creation_date\",\"direction\":\"older\",\"
unit\":\"days\",\"unit_count\":\"$DAYS\"},
{\"filtertype\":\"kibana\",\"exclude\":\"True\"},
{\"filtertype\":\"pattern\",\"kind\":\"regex\",\"value\":\"elastalert_status\",\
"exclude\":\"True\"}]"`

#Проверим, не пустой ли список
TEST_INDICES=`echo $INDICES | grep -q -i "error" && echo 1 || echo 0`

if [ $TEST_INDICES == 1 ]
then
  echo "$DATE Не найдено индексов для обработки" >> $LOG
  exit
else
# Составляем цикл для каждого индекса в массиве $INDICES
for i in $INDICES
  do
    # Создаём снапшот для индекса $i
    curator_cli --config /etc/elasticsearch/curator-config.yml --timeout 600 --
host localhost --port 9200 snapshot --repository $REPOSITORY --filter_list "
{\"filtertype\":\"pattern\",\"kind\":\"regex\",\"value\":\"$i\"}"

    # Заносим в переменную имя снапшота для индекса $i
    SNAPSHOT=`curator_cli --config /etc/elasticsearch/curator-config.yml --host
localhost --port 9200 show_snapshots --repository $REPOSITORY`

    # Архивируем папку репозитория и складываем архив в хранилище
    cd $SNAPSHOT_DIRECTORY/$REPOSITORY && tar cjf $BACKUP_DIR"/"$i".tar.bz" ./*

    # Удаляем snapshot
    curator_cli --config /etc/elasticsearch/curator-config.yml --host localhost
--port 9200 delete_snapshots --repository $REPOSITORY --filter_list "
{\"filtertype\":\"pattern\",\"kind\":\"regex\",\"value\":\"$SNAPSHOT\"}"

    # Удаляем индекс
    curator_cli --config /etc/elasticsearch/curator-config.yml --host localhost
--port 9200 delete_indices --filter_list "
{\"filtertype\":\"pattern\",\"kind\":\"regex\",\"value\":\"$i\"}"

    # Очищаем папку репозитория
    rm -rf $SNAPSHOT_DIRECTORY/$REPOSITORY/*
  done
fi
```

20.1.2. Удаление устаревших архивов

Ниже представлен скрипт для удаления устаревших архивов индексов.

```
#!/bin/bash

# Удаление бекапов старше $DAYS дней
# ВАЖНО! В имени файла архива может быть только один знак "-" перед датой. Дата
должна быть в формате "yyyy.mm.dd".
```

```
# Например: aaa_bbb.ccc-yyyy.mm.dd.tar.bz

DAYS=91
BACKUP_DIR="/opt/elasticsearch/elasticsearch_backup"

#Определяем пороговую дату для удаления архивов
THRESHOLD=$(date -d "$DAYS days ago" +%Y%m%d)

#echo "THRESHOLD=$THRESHOLD"

FILES=`ls -1 $BACKUP_DIR`

TODELETE=`for i in $FILES; do echo $i | awk -F- '{printf "%s\n",$2 ;}' | awk -F.
'{printf "%s%s%s \n",$1,$2,$3 ;}' | sed "s/$/$i/"; done`

echo -e "$TODELETE" |\
while read DATE FILE
  do
     [[ $DATE -le $THRESHOLD ]] && rm -rf $BACKUP_DIR/$FILE
  done
```

Как правило, удалять устаревшие копии необходимо регулярно, и обычно это делается в периоды наименьшей нагрузки на сервер. Вы можете задать команду на запуск выше представленного скрипта как задачу планировщика (cron).

20.1.3. Восстановление индексов из архива

Ниже представлен скрипт для восстановления индекса из архива. Скрипт принимает первым аргументом путь до архива.

```
#!/bin/bash

#Зададим переменные
ARCHIVE=$1
BACKUP_DIR="/opt/elasticsearch/elasticsearch_backup"
RECOVERY_DIR="/opt/elasticsearch/snapshots/recovery/"

# На всякий случай очищаем папку репозитория
rm -rf $RECOVERY_DIR/*

# Разархивируем индекс в папку репозитория
tar xjf $BACKUP_DIR/$ARCHIVE -C $RECOVERY_DIR

# Заносим в переменную $SNAPSHOT имя снапшота в репозитории
SNAPSHOT=`curl -s -XGET "localhost:9200/_snapshot/recovery/_all?pretty" | jq
'.snapshots[0].snapshot' | sed 's/\"//g'`

# Восстанавливаем индекс из снапшота
curl -XPOST "localhost:9200/_snapshot/recovery/$SNAPSHOT/_restore?pretty"

# Нужно выставить небольшую задержку, чтобы Elasticsearch не ругался на удаление
восстанавливаемого снапшота
sleep 30

# Удалим снапшот из репозитория
```

```
curl -XDELETE "localhost:9200/_snapshot/recovery/$SNAPSHOT?pretty"

# Очистим папку репозитория
rm -rf $RECOVERY_DIR/*
```

20.2. Утилиты для снятия резервной копии MongoDB

MongoDB использует для хранения информации форматы JSON и BSON (двоичный JSON). JSON - это удобный для прочтения человеком формат, идеально подходящий для экспорта и импорта данных. Вы сможете управлять экспортированными данными в этом формате с помощью любого инструмента, поддерживающего JSON, включая простой текстовый редактор.

Для создания резервных копий и восстановления, лучше использовать двоичный формат BSON.

Согласованность информации может представлять проблему, если у вас загруженный сервер MongoDB, где информация может изменяться при экспорте или резервном копировании базы данных. Одно из возможных решений этой проблемы — репликация, и вы можете использовать его, когда лучше освоитесь с MongoDB.

Чтобы создать резервную копию данных, вам следует использовать команду `mongodump`. Для восстановления используйте команду `mongorestore`.

Для установки утилит `mongodump` и `mongorestore` используйте скрипт:

```
#Предварительная подготовка к установке
sudo apt update && sudo apt upgrade
sudo apt install gnupg2

#Импорт ключей GPG для MongoDB
wget -nc https://www.mongodb.org/static/pgp/server-6.0.asc

cat server-6.0.asc | gpg --dearmor | sudo tee /etc/apt/keyrings/mongodb.gpg
>/dev/null

#Добавление репозитория MongoDB
sudo sh -c 'echo "deb [ arch=amd64,arm64 signed-by=/etc/apt/keyrings/mongodb.gpg]
https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/6.0 multiverse" >>
/etc/apt/sources.list.d/mongo.list'
sudo apt update

#Установка MongoDB и запуск службы mongod
sudo apt install mongodb-org
sudo systemctl start mongod
```

20.2.1. Утилита mongodump

создайте каталог `/var/backups/mongobackups`:

```
sudo mkdir /var/backups/mongobackups
```

Затем запустите команду `mongodump`:

```
mongodump --db newdb --out /var/backups/mongobackups/`date +"%m-%d-%y"`
```

Результат должен выглядеть следующим образом:

```
Output
2020-10-29T19:22:36.886+0000    writing newdb.restaurants to
2020-10-29T19:22:36.969+0000    done dumping newdb.restaurants (25359 documents)
```

Теперь у вас имеется полная резервная копия базы данных newdb в каталоге `/var/backups/mongobackups/10-29-20/newdb/`.

Как правило, резервное копирование выполняется регулярно, и обычно это делается в периоды наименьшей нагрузки на сервер. Вы можете задать команду mongodump как задачу планировщика (cron).

20.2.2. Утилита mongorestore

Используя аргумент `--drop` мы обеспечим предварительное отбрасывание целевой базы данных так, чтобы резервная копия была восстановлена в чистой базе данных.

```
sudo mongorestore --db newdb --drop /var/backups/mongobackups/10-29-20/newdb/
```

Результат должен выглядеть следующим образом:

```
Output
2020-10-29T19:25:45.825+0000    the --db and --collection args should only be
used when restoring from a BSON file. Other uses are deprecated and will not
exist in the future; use --nsInclude instead
2020-10-29T19:25:45.826+0000    building a list of collections to restore from
/var/backups/mongobackups/10-29-20/newdb dir
2020-10-29T19:25:45.829+0000    reading metadata for newdb.restaurants from
/var/backups/mongobackups/10-29-20/newdb/restaurants.metadata.json
2020-10-29T19:25:45.834+0000    restoring newdb.restaurants from
/var/backups/mongobackups/10-29-20/newdb/restaurants.bson
2020-10-29T19:25:46.130+0000    no indexes to restore
2020-10-29T19:25:46.130+0000    finished restoring newdb.restaurants (25359
documents)
2020-10-29T19:25:46.130+0000    done
```

При восстановлении базы данных MongoDB из предыдущей резервной копии вы получите точную копию информации MongoDB на определенный момент времени, включая все индексы и типы данных.

20.3. Утилиты для снятия резервной копии PostgreSQL

20.3.1. Утилита pg_dumpall

Утилита *pg_dumpall* реализует резервное копирование всего экземпляра (кластера или инстанса) базы данных без указания конкретной базы данных на инстансе. По принципу схожа с *pg_dump*. Добавим, что только утилиты *pg_dump* и *pg_dumpall* предоставляют возможность создания логической копии данных, остальные утилиты, рассматриваемые в этой статье, позволяют создавать только бинарные копии.

```
# pg_dumpall > /tmp/instance.bak
```

Чтобы сразу сжать резервную копию экземпляра базы данных, нужно передать вывод на архиватор *gzip*:

```
# pg_dumpall | gzip > /tmp/instance.tar.gz
```

Ниже приведены параметры, с которыми может вызываться утилита *pg_dumpall*:

-d <имя*бд*>, —*dbname=имя*бд — имя базы данных.

-h <сервер>, —host=сервер — имя сервера.

-p <порт>, —port=порт — TCP-порт, на который принимаются подключения.

-U <пользователь>, —username=пользователь — имя пользователя для подключения.

-w, —no-password — деактивация требования ввода пароля.

-W, —password — активация требования ввода пароля.

—role=<имя роли> — роль, от имени которой генерируется резервная копия.

-a, —data-only — создание резервной копии без схемы данных.

-c, —clean — добавление операторов DROP перед операторами CREATE.

-f <имя*файла*>, —*file=имя*файла — активация направления вывода в указанный файл.

-g, —globals-only — выгрузка глобальных объектов без баз данных.

-o, —oids — выгрузка идентификаторов объектов (OIDs) вместе с данными таблиц.

-O, —no-owner — деактивация генерации команд, устанавливающих принадлежность объектов, как в исходной базе данных.

-r, —roles-only — выгрузка только ролей без баз данных и табличных пространств.

-s, —schema-only — выгрузка только схемы без самих данных.

-S <имя*пользователя*>, —*superuser=имя*пользователя — привилегированный пользователь, используемый для отключения триггеров.

-t, —tablespaces-only — выгрузка табличных пространства без баз данных и ролей.

-v, —verbose — режим подробного логирования.

-V (—version — вывод версии утилиты pg_dumpall.

20.3.2. Утилита pg_restore

Утилита позволяет восстанавливать данные из резервных копий. Например, чтобы восстановить только определенную БД (в нашем примере zabbix), нужно запустить эту утилиту с параметром *-d*:

```
# pg_restore -d zabbix /tmp/zabbix.bak
```

Чтобы этой же утилитой восстановить определенную таблицу, нужно использовать ее с параметром *-t*:

```
# pg_restore -a -t history /tmp/zabbix.bak
```

Также утилитой pg_restore можно восстановить данные из бинарного или архивного файла. Соответственно:

```
# pg_restore -Fc zabbix.bak
# pg_restore -Ft zabbix.tar
```

При восстановлении можно одновременно создать новую базу:

```
# pg_restore -Ft -C zabbix.tar
```

Восстановить данные из дампа также возможно при помощи *psql*:

```
# psql zabbix < /tmp/zabbix.dump
```

Если для подключения нужно авторизоваться, вводим следующую команду:

```
# psql -U zabbix -W zabbix < /tmp/zabbix.dump
```

Ниже приведен синтаксис утилиты *pg_restore*.

-h <сервер>, —host=сервер — имя сервера, на котором работает база данных.

-p <порт>, —port=порт — TCP-порт, через база данных принимает подключения.

-U <пользователь>, —username=пользователь — имя пользователя для подключения..

-w, —no-password — деактивация требования ввода пароля.

-W, —password — активация требования ввода пароля.

—role=имя роли — роль, от имени которой выполняется восстановление резервная копия.

<имя_файла> — расположение восстанавливаемых данных.

-a, —data-only — восстановление данных без схемы.

-c, —clean — добавление операторов DROP перед операторами CREATE.

-C, —create — создание базы данных перед запуском процесса восстановления.

-d <имя*бд*>, —*dbname=имя*бд — имя целевой базы данных.

-e, —exit-on-error — завершение работы в случае возникновения ошибки при выполнении SQL-команд.

-f <имя*файла*>, —*file=имя*файла — файл для вывода сгенерированного скрипта.

-F <формат>, —format=формат — формат резервной копии. Допустимые форматы:

- p, plain — формирует текстовый SQL-скрипт;
- c, custom — формирует резервную копию в архивном формате;
- d, directory — формирует копию в directory-формате;
- t, tar — формирует копию в формате tar.

-I <индекс>, —index=индекс — восстановление только заданного индекса.

-j <число-заданий>, —jobs=число-заданий — запуск самых длительных операций в нескольких параллельных потоках.

-l, —list) — активация вывода содержимого архива.

-L <файл-список>, —use-list=файл-список — восстановление из архива элементов, перечисленных в файле-списке в соответствующем порядке.

-n <пространство_имен>, —schema=схема — восстановление объектов в указанной схеме.

-O, —no-owner — деактивация генерации команд, устанавливающих владение объектами по образцу исходной базы данных.

-P <имя-функции(тип-аргумента[, ...])>, —function=имя-функции(тип-аргумента[, ...]) — восстановление только указанной функции.

-s, —schema-only — восстановление только схемы без самих данных.

-S <пользователь>, —superuser=пользователь — учетная запись привилегированного пользователя, используемая для отключения триггеров.

-t <таблица>, —table=таблица — восстановление определенной таблицы.

-T <триггер>, —trigger=триггер — восстановление конкретного триггера.

-v, —verbose — режим подробного логирования.

-V, —version — вывод версии утилиты pg_restore.

20.3.3. Утилита pg_basebackup

Утилитой *pg_basebackup* можно выполнять резервное копирования работающего кластера баз данных PostgreSQL. Результирующий бинарный файл можно использовать для репликации или восстановления на определенный момент в прошлом. Утилита создает резервную копию всего экземпляра базы данных и не дает возможности создавать слепки данных отдельных сущностей. Подключение pg_basebackup к PostgreSQL выполняется при помощи протокола репликации с полномочиями суперпользователя или с правом REPLICATION.

Для выполнения резервного копирования локальной базы данных достаточно передать утилите *pg_basebackup* параметр *-D*, обозначающий директорию, в которой будет сохранена резервная копия:

```
# pg_basebackup -D /tmp
```

Чтобы создать сжатые файлы из табличных пространств, добавим параметры *-Ft* и *-z*:

```
# pg_basebackup -D /tmp -Ft -z
```

То же самое, но со сжатием bzip2 и для экземпляра базы с общим табличным пространством:

```
# pg_basebackup -D /tmp -Ft | bzip2 > backup.tar.bz2
```

Ниже приведен синтаксис утилиты *pg_basebackup.*

-d <строка*подключения*>, —*dbname*=*строка*подключения — определение базы данных в виде строки для подключения.

-h <сервер>, —host=сервер — имя сервера с базой данных.

-p <порт>, —port=порт — TCP-порт, через база данных принимает подключения.

-s <интервал>, —status-interval=интервал — количество секунд между отправками статусных пакетов.

-U <пользователь>, —username=пользователь — установка имени пользователя для подключения.

-w, —no-password — отключение запроса на ввод пароля.

-W, —password — принудительный запрос пароля.

-V, —version — вывод версии утилиты *pg_basebackup*.

-?, —help — вывод справки по утилите pg_basebackup.

-D каталог, —pgdata=каталог — директория записи данных.

-F <формат>, —format=формат — формат вывода. Допустимые варианты:

- **p, plain** — значение для записи выводимых данных в текстовые файлы;
- **t, tar** — значение, указывающее на необходимость записи в целевую директорию в формате tar.

-r <скорость*передачи*>, —*max-rate*=*скорость*передачи — предельная скорость передачи данных в Кб/с.

-R, —write-recovery-conf — записать минимальный файл *recovery.conf* в директорию вывода.

-S <имя*слота*>, —*slot*=*имя*слота — задание слота репликации при использовании WAL в режиме потоковой передачи.

-T <каталог*1*=*каталог*2>, —tablespace-mapping=каталог*1*=*каталог*2 — активация миграции табличного пространства из одного каталога в другой каталог при копировании.

—xlogdir=каталог_xlog — директория хранения журналов транзакций.

-X <метод>, —xlog-method=метод — активация вывода файлов журналов транзакций WAL в резервную копию на основе следующих методов:

- **f, fetch** — включение режима сбора файлов журналов транзакций при окончании процесса копирования;
- **s, stream** — включение передачи журнала транзакций в процессе создания резервной копии.

-z, —gzip — активация gzip-сжатия результирующего tar-файла.

-Z <уровень>, —compress=уровень — определение уровня сжатия механизмом gzip.

-c , —checkpoint=fast|spread — активация режима реперных точек.

-l <метка>, —label=метка — установка метки резервной копии.

-P, —progress — активация в вывод отчета о прогрессе.

-v, —verbose — режим подробного логирования.

21. Настройка сессий пользователя

Перейдите в административный раздел управления сервисом авторизации

https://auth.domain.ltd

http://ip:8180

Там перейдите в раздел - Настройки Realm / Токены

Есть две настройки:

1. Таймаут сессии SSO.
   По умолчанию 30 минут.

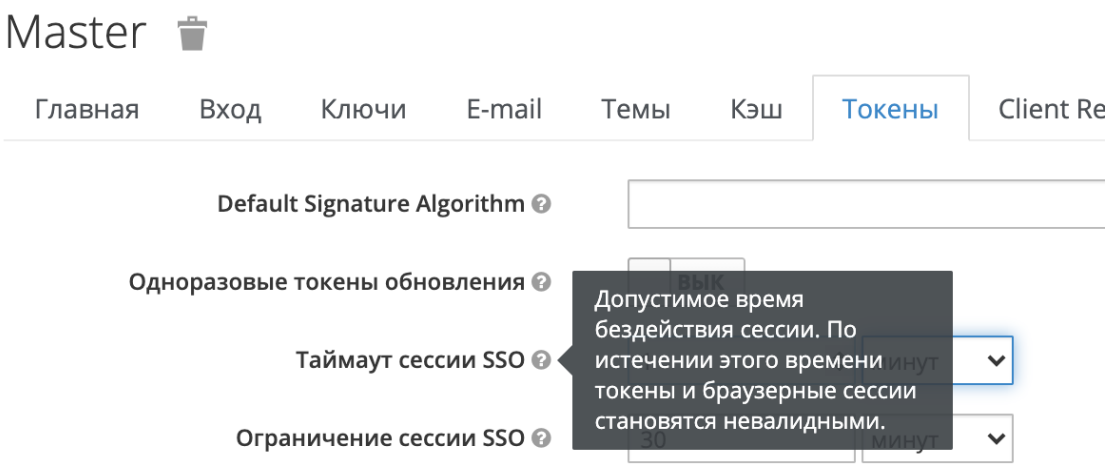

Рисунок 101

2. Ограничение сессии SSO.
   По умолчанию 10 часов.

22. Миграция индексов базы Elasticsearch

На рисунке 102 представлена схема миграции индексов базы Elasticsearch.

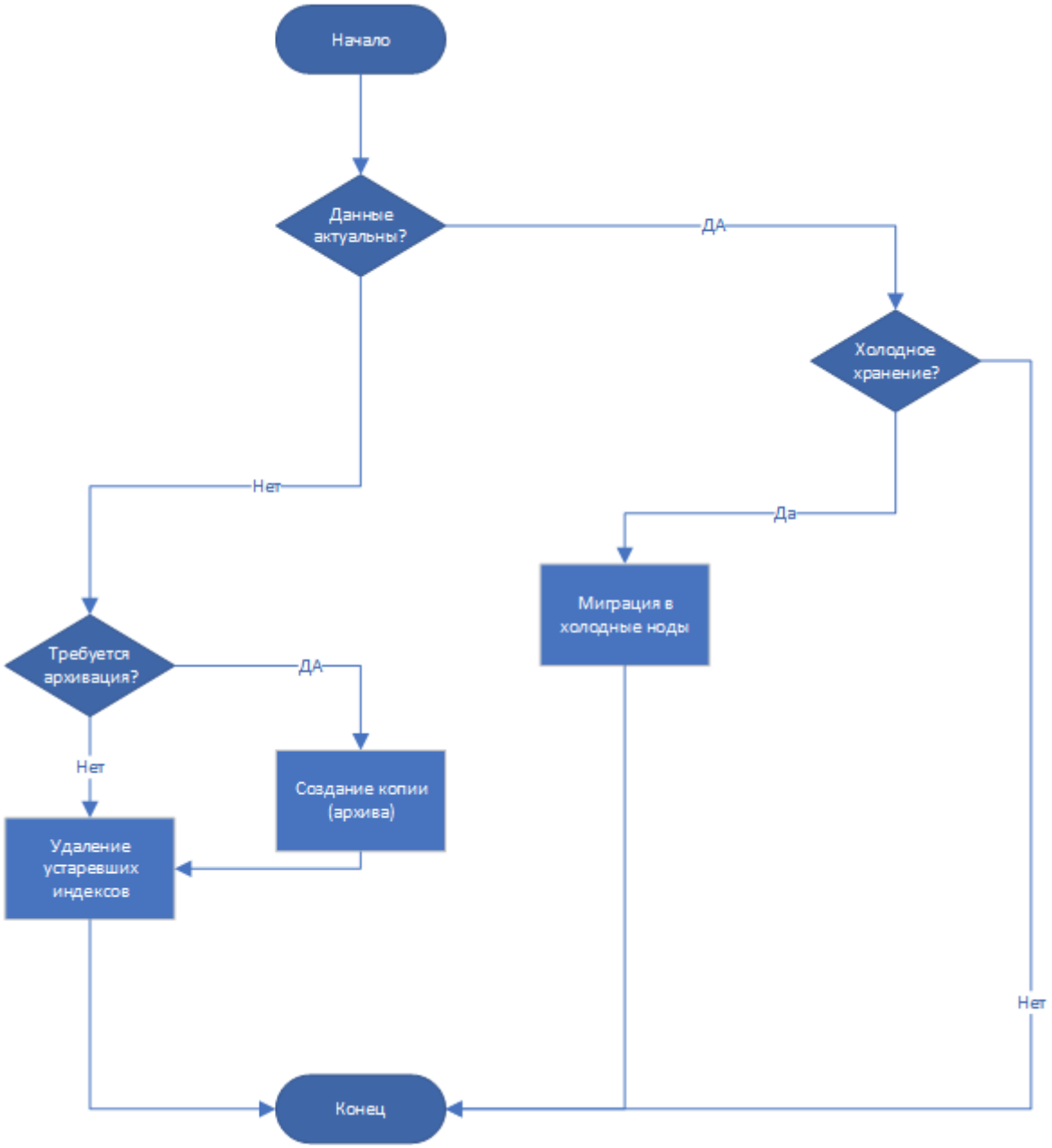

Рисунок 102 - Схема миграции

22.1. Настройка миграции

Настройка миграции производится на одной из нод кластера Elasticsearch.

Для работы скрипта миграции необходимо установить программный компонент `elasticdump`, для этого нужно выполнить команду: `bash /opt/pangeoradar/support_tools/elasticdump/install.sh`

После установки нужно произвести настройку ноды, выполнив команду: `bash /opt/pangeoradar/support_tools/elastic/es_config.sh`

На рисунке 103 изображен этап включения дополнительных параметров, рекомендуется использовать все.

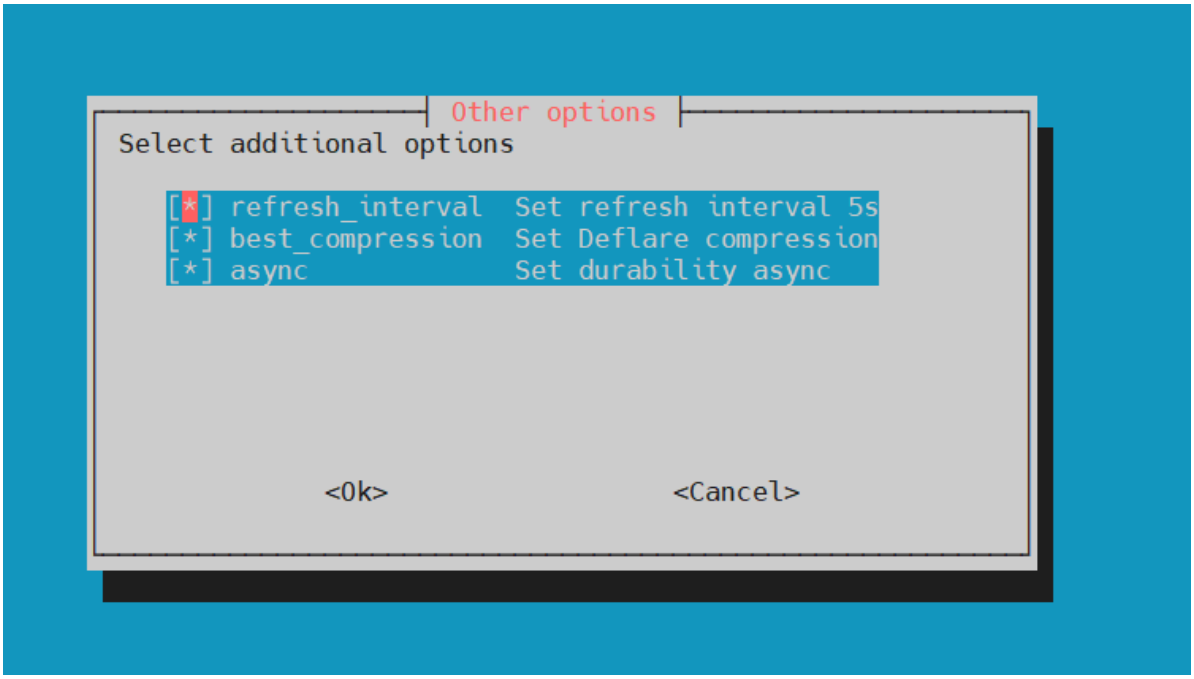

Рисунок 103 - Настройка дополнительных параметров

Далее необходимо произвести настройку самой миграции в конфигурационном файле: `/opt/pangeoradar/support_tools/elastic/indices_route.sh`

Основные настройки и их описания представлены ниже:

```
SNAPSHOT_DIRECTORY="/data/archive"  # путь сохранения архивированных индексов

es_proto="https"                    # протокол по которому осуществляется
подключение к базе
es_host="127.0.0.1"                 # IP адрес сервера ES
es_port=9200                        # порт подключения к ES
hot_cold=1                          # включить\отключить функционал миграции в
"холодное" хранилище
archive=1                           # включить\отключить создание архива
индексов
archive_error=1                     # включить\отключить архивацию индексов
ошибок
cold_day=1                          # количество дней, после которых индексы
перемещаются в "холодное" хранилище
delete_error_day=1                  # количество дней, после которых индексы
ошибок удаляются
delete_day=2                        # количество дней, после которых индексы
удаляются
archive_day=90                      # количество дней хранения архива индексов,
после которых они будут удалены
```

После чего необходимо добавить задачу на ежедневное выполнение. Для этого нужно выполнить команду: `crontab -e`

Удалить из планировщика задач строку:

```
0 4 * * * /usr/bin/curator --config /etc/curator/config.yml
/etc/curator/action.yml
```

Добавить следующую строку:

```
0 4 * * * /bin/bash /opt/pangeoradar/support_tools/elastic/indices_route.sh
```

После чего настройку миграции можно считать завершенной.

22.2. Восстановление индексов из архива

Для восстановления индексов из архива необходимо выполнить команду: `bash /opt/pangeoradar/support_tools/elastic/restore.sh`

После выполнения должно появиться окно с фильтрацией индексов, изображенное на рисунке 104.

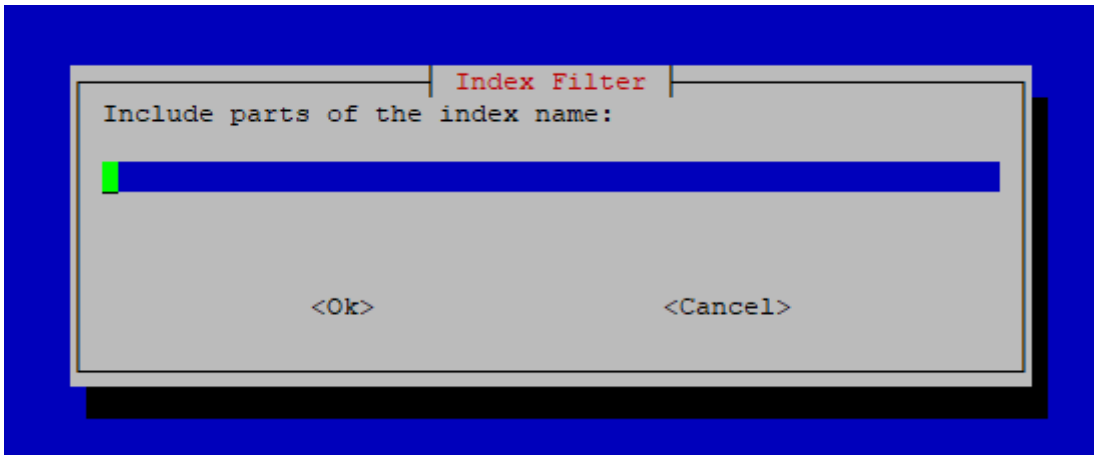

Рисунок 104 - Фильтрация архивированных индексов

В качестве аргументов можно использовать часть имени индекса. Примеры:

- 'firewall' - все архивные индексы межсетевого экрана;
- '2021.11.23' - все архивные индексы за 23 ноября 2021 года;
- '2021.12' - все архивные индексы за декабрь 2021 года.

> Если не указывать аргументы, будут отображены все архивированные индексы.

После чего необходимо выбрать индексы, которые необходимо разархивировать, как изображено на рисунке 105.

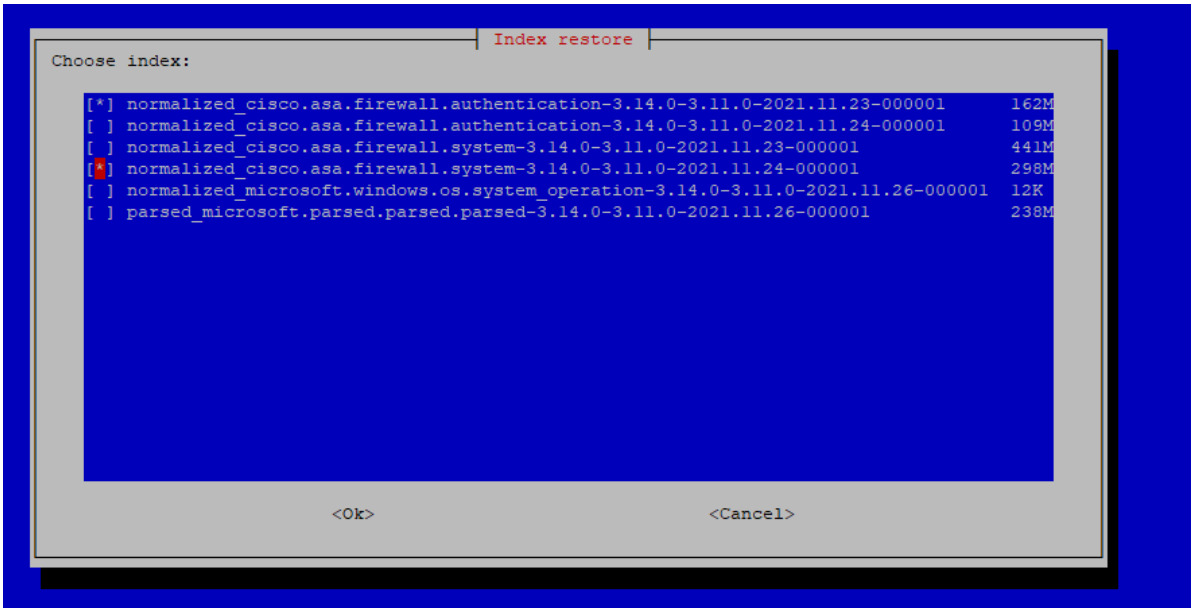

Рисунок 105 - "Выбор индексов для разархивации"

> Возможно восстановление нескольких индексов

Процесс разархивации индексов фиксируется в журнале: `/var/log/restore.log`

23. Исходные ("сырые") события

23.1. Включение\выключение исходных ("сырых") событий

Общий алгоритм для включения\выключения исходных ("сырых") событий:

1. Подключитесь по SSH к узлу обработки событий Платформы (Worker).
2. Выберите какие исходные ("сырые") события вы хотите включить: для всех источников или для определенного источника.
3. Перейдите в настройку конфигурации Termite (подробнее в следующих подразделах) и внесите изменения.
4. Сохраните конфигурацию и перезапустите сервис.

23.1.1. Для всех источников

Включение\выключение исходных ("сырых") событий **для всех источников** осуществляется в разделе Кластер - Управление конфигурацией - Termite - Output (см. рисунок 106).

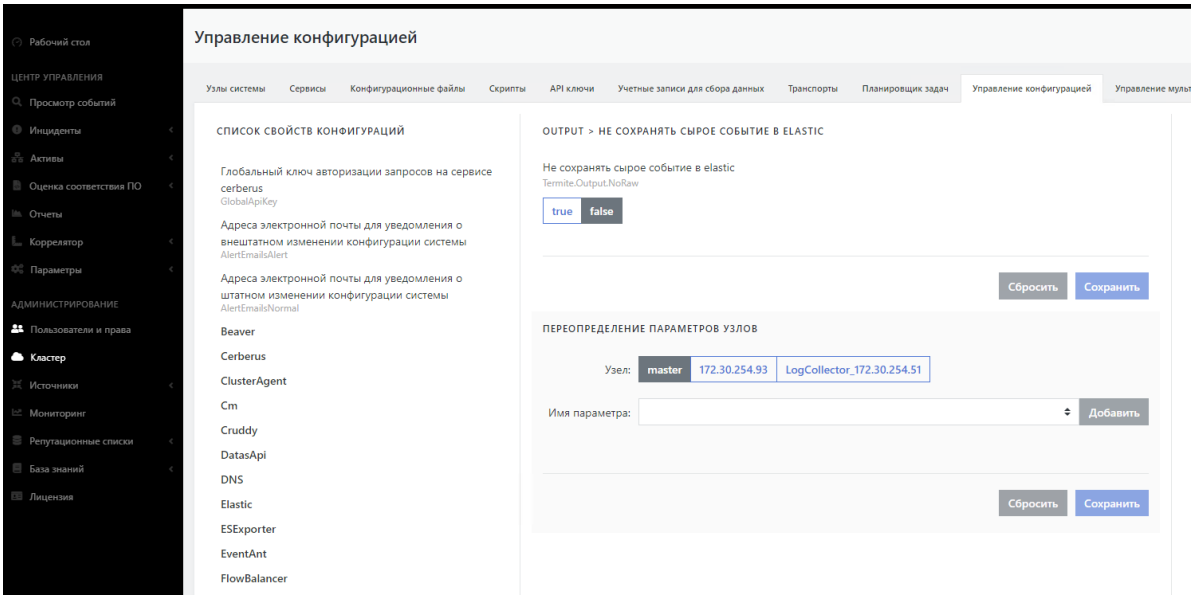

Рисунок 106 - Настройка отправки "сырых" событий

> Перевод данного параметра в состояние 'false' приведет к добавлению "сырой" части событий для всех входящих событий.

23.1.2. Для определенного источника

Включение\выключение исходных ("сырых") событий **для определенного источника** осуществляется в файле `/opt/pangeoradar/configs/termite/inputs-kafka.yaml` путем добавления строки `no_raw: true` в блоке с источником, для которого требуется включение\выключение "сырой" части события.

Пример изменения в конфигурационном файле для источника **Microsoft-Windows-Eventlog**:

```
1514-Microsoft-Windows-Eventlog:
  input: kafka
  encoding: utf-8
  kafka-config:
    enable.ssl.certificate.verification: false
    security.protocol: SSL
    ssl.ca.location: /opt/pangeoradar/certs/pgr.crt
  message-type: microsoft_windows
  servers: ['<IP-адрес-Kafka>:9992']
  topics: ['1514-Microsoft-Windows-Eventlog']
  timezone: Europe/Moscow
  no_raw: true
```

> **Важно!** При проведении "Синхронизации" источников, включение\выключение "сырой" части события для определенного источника необходимо производить повторно.

23.2. Просмотр сохраненных исходных ("сырых") событий

Для просмотра сохраненных исходных (сырых) событий необходимо выполнить следующие действия:

1. В веб-интерфейс Платформы зайдите в раздел **"Просмотр событий"**.
2. Задайте временной интервал в поле **Время**.
3. При необходимости введите или выберите в раскрывающемся списке нужный индекс в поле **Индекс**.
4. Обновите данные на экране согласно заданным параметрам, нажав  .
5. В левой части экрана в области "**Доступные поля**" найдите поле **raw** и нажмите  .

Поле **raw** добавится в область "**Выбранные поля**". В правой части экрана под графиком отобразятся сырые события в формате JSON (см. рисунок 107).

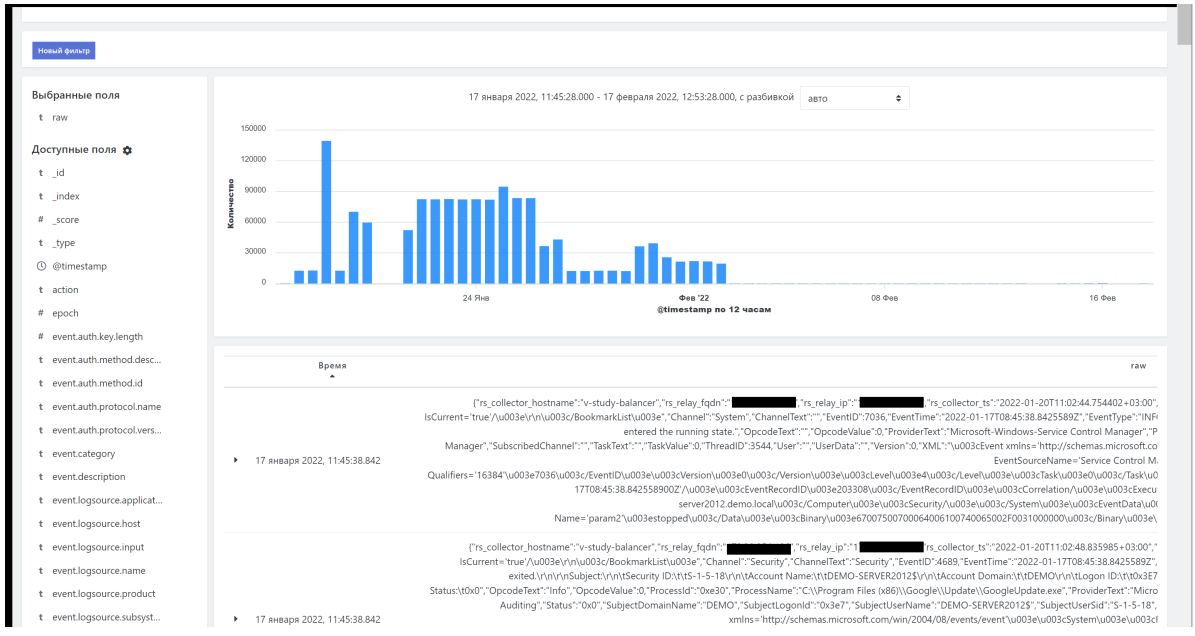

Рисунок 107 - Отображение исходных (сырых) событий в разделе "Просмотр событий"

24. Корректировка времени источника

Корректировка времени источника осуществляется в файле `/opt/pangeoradar/configs/termite/time-fix.yaml`

```
#test-type:
#  hosts:
#    - address: 1.1.1.1
#      lookup: 'initiator.host.ip'
#      timedelta: 1000
#    - address: 2.2.2.2
#      lookup: 'initiator.host.ip'
#      timedelta: -1000
```

в поле `timedelta` укажите число секунд сдвига времени, значение может быть как положительным, так и отрицательным.

в поле `lookup` необходимо указать поле нормализации из которого будет происходить сравнение с полем `address`

> Также при подключении источника возможно указать его таймзону, что приведет к автоматической конвертации её в указанную из нормализованного поля `@timestamp`.

25. Настройка архивации событий

25.1. Проверка текущих настроек политики архивации устаревших событий

В Платформе предусмотрена возможность архивации устаревших событий.

Для проверки текущего состояния политики архивации выполните следующие действия:

1. Зайдите по SSH на сервер архивации событий (узел платформы с ролью **DATA**).
2. Откройте конфигурационный файл /opt/pangeoradar/scripts/indices_route.sh командой:

   `nano/opt/pangeoradar/scripts/indices_route.sh`
3. Посмотрите значения параметров **cold_day** и **delete_day**. По умолчанию они должны иметь значение 27 (27 дней оперативного хранения).

Для проверки работы политики архивации выполните следующие действия:

1. В веб-интерфейсе Платформы перейдите в раздел «**Просмотр событий**».
2. Для формирования отчета выставите в области задания временного интервала промежуток времени длиннее чем заданный промежуток в политиках архивации, например, 30 дней считая от сегодняшнего.

На экране в статистике по событиям не должны отображаться события старше 27 дней.

25.2. Изменение политики архивации устаревших событий

Для изменения политики архивации выполните следующие действия:

1. Зайдите по SSH на сервер архивации событий (узел платформы с ролью **DATA**).
2. Откройте конфигурационный файл узла /opt/pangeoradar/scripts/indices_route.sh командой:

`nano /opt/pangeoradar/scripts/indices_route.sh`

3. Установите для параметров **cold_day** и **delete_day** новое значение оперативного хранения данных.
4. Принудительно запустите архивацию, выполнив команду:

   `bash /usr/bin/bash /opt/pangeoradar/scripts/indices_route.sh`
5. Дождитесь окончания выполнения скрипта.

Для проверки введённых изменений выполните следующие действия:

1. В веб-интерфейсе Платформы перейдите в раздел «**Просмотр событий**».
2. Проверьте, что нет индексов старше 20 дней (см. алгоритм проверки описан в предыдущем подразделе).
3. Вернитесь в терминал сервера архивации событий (узел **DATA**).
4. Перейдите в директорию **/data/archive**.
5. Выведите листинг директории командой:

   `ls -lah`
6. Убедитесь в появлении новых архивов.
7. Для просмотра запланированных заданий выполните команду:

   `crontab -l`
8. Убедитесь в наличии запланированного задания по ротированию и архивации событий.

В результате проведенных действий в веб-интерфейсе платформы должны отсутствовать записи об индексах и событиях старше заданного количества дней в политике архивации.

Должны быть созданы новые архивы с названиями индексов, экспортированных из системы для архивации и долгосрочного хранения.

25.3. Восстановление данных из архива и обращения к восстановленным событиям

В Платформе предусмотрена возможность обращения к устаревшим событиям, находящимся на архивном хранении.

Для того, чтобы получить доступ к архивным данным, необходимо сначала выполнить восстановление данных из архива:

1. Зайдите по SSH на сервер архивации событий (узел платформы с ролью **DATA**).
2. Запустите скрипт восстановления данных командой:

   `bash /opt/pangeoradar/scripts/elastic_restore.sh`
3. В появившемся окне укажите фильтр ***** и нажмите **ОК**.
4. Выберите интересующий индекс из списка, выделите напротив него чекбокс (запомните имя восстанавливаемого индекса) и нажмите **ОК**.
5. Дождитесь окончания восстановления (восстановление осуществляется в фоновом режиме).

Для просмотра восстановленных данных необходимо:

1. Перейдите в веб-интерфейс Платформы в раздел «Просмотр событий».

2. В поле **Время** укажите временной диапазон восстанавливаемого индекса (см. Рисунок 108).
3. В поле **Индекс** укажите имя восстанавливаемого индекса (см. Рисунок 108).
4. Нажмите кнопку **Поиск**.

На экран должен быть выведен список событий (включая диаграмму), относящийся к восстанавливаемому индексу и указанному временному периоду (см. рисунок 108).

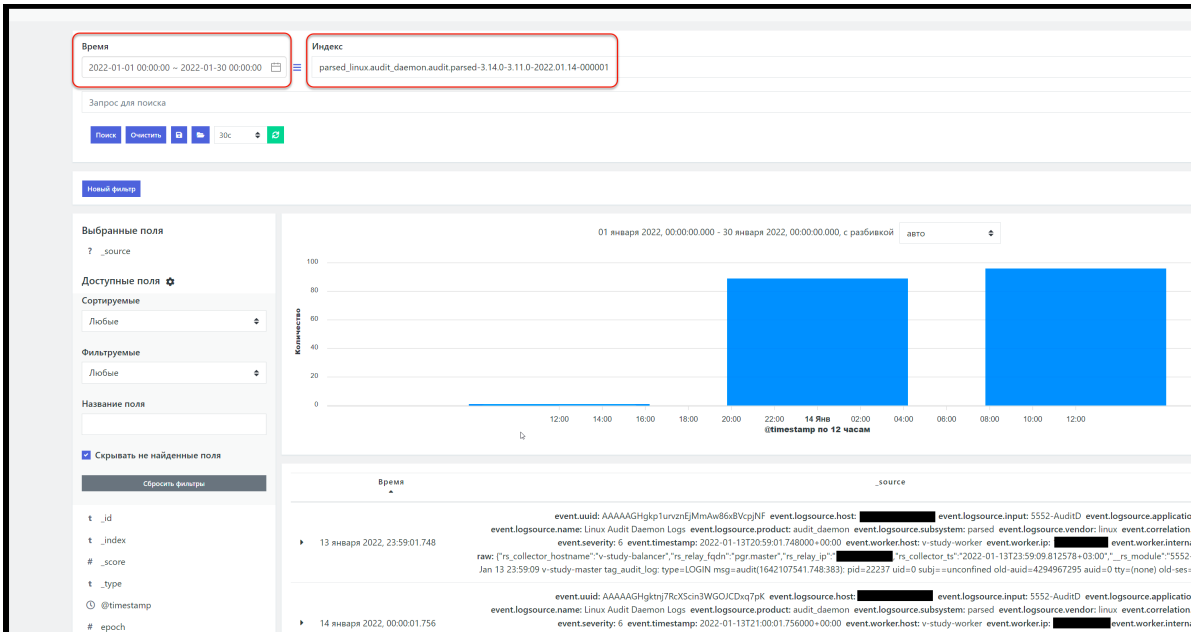

Рисунок 108 - Просмотр данных, восстановленных из архива

26. Настройка и проверка интеграции через API

В Платформе Радар реализована интеграция посредством API с IRP-системами - R-Vision и Security Vision.

26.1. Настройка и проверка передачи через API информации об инциденте во внешнюю систему

Для настройки интеграции с внешними системами через API необходимой выполнить следующие действия:

1. Подключитесь по SSH к узлу платформы с ролью **Master**.
2. Внесите следующие изменения в конфигурационный файл узла **/opt/pangeoradar/configs/pangeoradar-pgr-wal-listener.yaml**:
    - Добавьте реквизиты интегрируемой системы (R-Vision) — ключ доступа к API R-Vision и IP-адрес R-Vision;

- Измените схему соответствия полей согласно требованиям интеграции.

3. Запустите сервис **pangeoradar-pgr-wal-listener**:

   `service pangeordar-pgr-wal-listener start`

Для проверки проведенного подключения выполнить следующие действия:

1. Зайдите в веб-интерфейс Платформы (с правами администратора).
2. Зайдите в раздел «**Инциденты**» — «**Инциденты**».
3. Создайте инцидент вручную, нажав кнопку **Создать инцидент**.

При настроенном API новый инцидент передается во внешнюю систему в автоматическом режиме в процессе создания. Созданный инцидент автоматически создан в IRP.

26.2. Генерация ключа для доступа к API. Использование ключа

Для работы по API необходимо сгенерировать ключ для доступа к API. Для этого выполните следующие действия:

1. Перейдите в веб-интерфейс Платформы в подраздел "Кластер"->"API ключи" (см. рисунок 109).

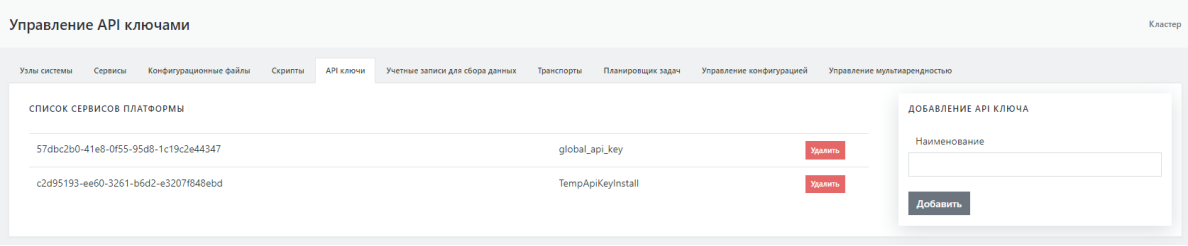

Рисунок 109 - Настройка ключей для работы через API

2. Добавьте ключ, введя значение параметра в поле **Наименование** ключа (например, integration) и нажав кнопку **Добавить**.
3. Подключитесь по SSH к узлу платформы с ролью **Master**.
4. Выполните с использованием ключа **integration**, который был сгенерирован на этапе предварительных действий в данной проверке, следующую команду:

   `curl -k -H "PgrApiKey:<ключ, сгенерированный на шаге 2 >" "https://10.170.9.22:9000/cruddy/public/api/v1/incidents?page=1&per_page=1&order=id%20DESC"`

На экран будут выведена запись по одному инциденту в формате JSON.

27. Настройка политики противодействия попыткам подбора пароля

Платформа обладает встроенными механизмами противодействия попыткам подбора пароля (BruteForce атаки) на базе открытого ПО **Keycloak** (идентификационный брокер).

Для настройки политики противодействия попыткам подбора пароля выполните следующие действия:

1. С правами администратора войдите в специализированный веб-интерфейс **Keycloak** платформы `https://<адрес платформы>:8180` (см. рисунок 110).

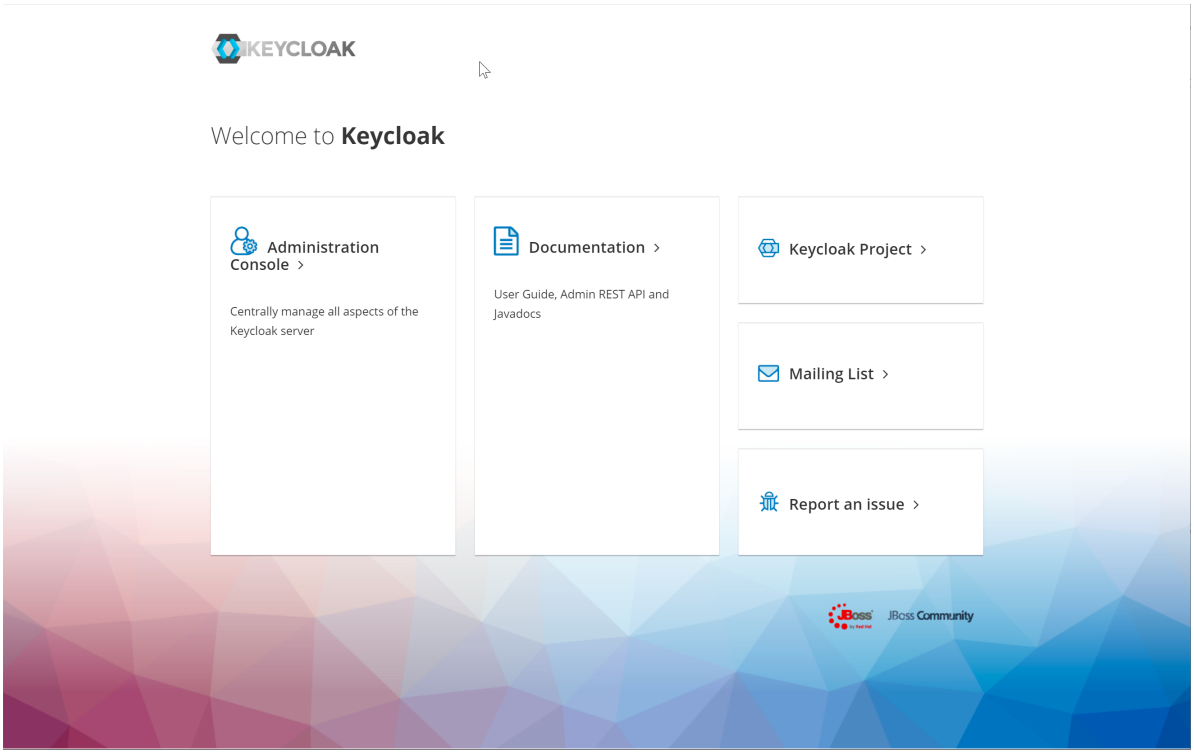

Рисунок 110 - Интерфейс "идентификационного брокера" **Keycloak**

2. Перейдите в раздел "Administration Console" -> "Защита безопасности" -> "Определение Brute Force" (см. рисунок 111).

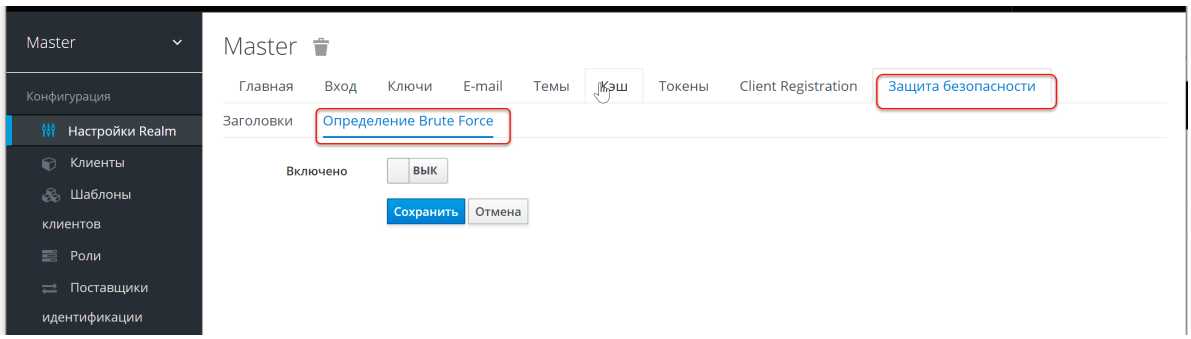

Рисунок 111 - Раздел "Определение Brute Force" при отключенных политиках.

3. Включите политику Определение Brute Force, установив переключатель в поле **Включено** в положение **вкл**. Откроются параметры настройки политики (см. рисунок 112).

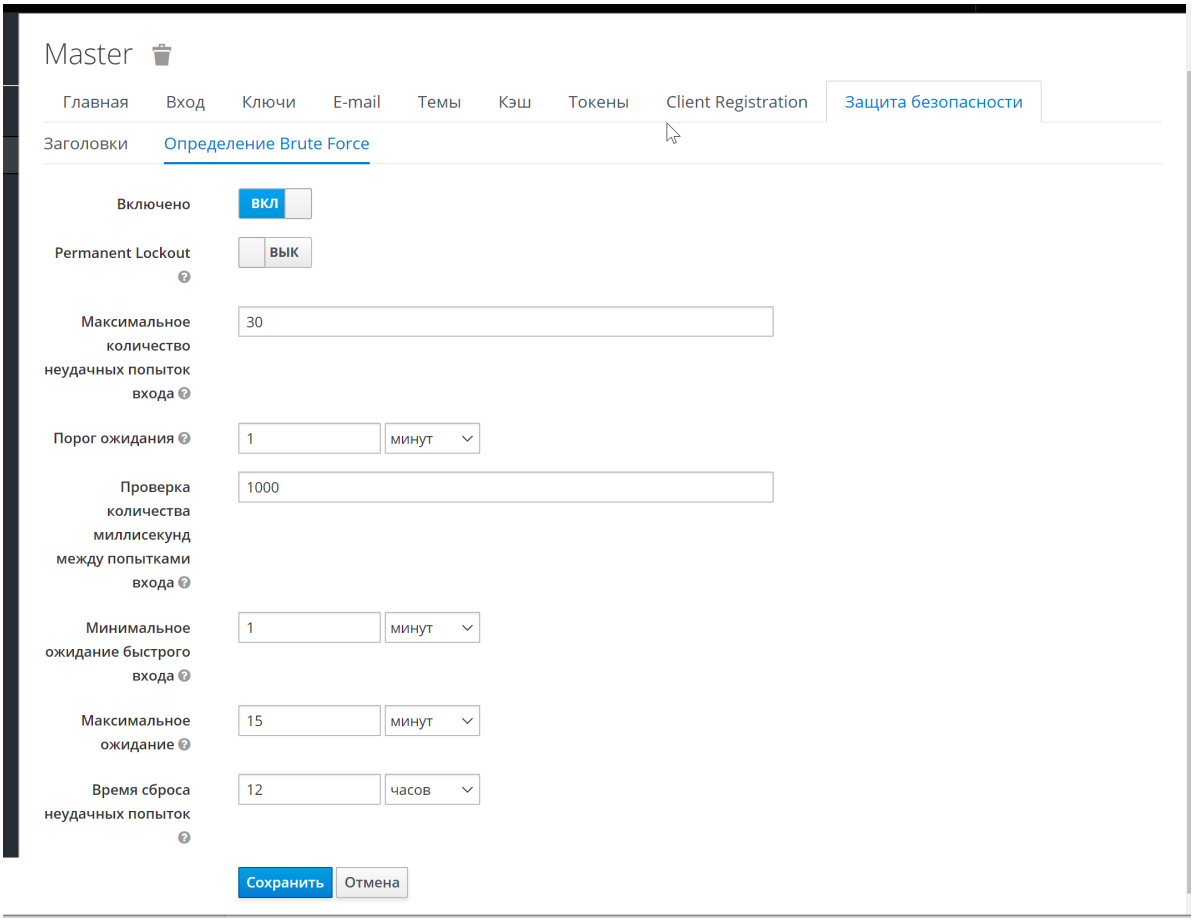

Рисунок 112 - Параметры настройки политики

4. При необходимости установите следующие параметры:
    - максимальное количество неудачных попыток входа (основная настройка) — количество неудачных попыток входа до блокировки пользователя;
    - порог ожидания (основная настройка) — если порог ошибок превышен, сколько времени пользователь будет заблокирован;
    - проверка количества миллисекунд между попытками входа — если попытки аутентификации происходят слишком часто, то пользователя необходимо заблокировать;
    - минимальное ожидание быстрого входа — как долго ждать после неудачной попытки быстрого входа;
    - максимальное ожидание — максимальное время, на которое пользователь будет заблокирован;
    - время сброса неудачных попыток — через какое время счетчик неудачных попыток будет сброшен.
5. Сохраните настройки, нажав кнопку **Сохранить**.

28. Процедура обновления

Процедура обновления отличается у разных версий Платформы, а также зависит от конкретной архитектуры при распределённой установке. Инструкции по обновлению входят в комплект пакетов обновления.

Обновление Платформы не приводит к потере накопленной информации из баз данных. При обновлении сохраняются собранные события, инциденты, база активов и база знаний со всеми пользовательскими изменениями.

Пакеты обновлений могут быть доставлены на серверы Платформы как на съёмных носителях информации (оптические диски, флеш-карты, переносные HDD/SSD накопители), так и с помощью сетевого хранилища при наличии сетевого доступа с серверов Платформы.

Обновления базы знаний с пополнением правил корреляции, правил разбора и нормализации без обновления основных пакетов Платформы могут быть предоставлены отдельно по запросу Заказчика.

29. Проведение централизованного обновления конфигурации и перезапуска сервисов компонентов Платформы

Рассмотрим проведение централизованного (через веб-интерфейс Платформы) обновления конфигурации и перезапуска сервисов компонентов платформы на примере сервиса **rsyslog**, функционирующего в составе узла Платформы с ролью **Balancer** (обновление конфигурации и перезапуск других сервисов Платформы проводится аналогичным образом).

Для проведения централизованного обновления конфигурации и перезапуска сервиса **rsyslog** выполните следующие действия:

1. Зайдите в веб-интерфейс Платформы (с правами администратора).
2. Зайдите в раздел "Кластер"->"Узлы системы"->"Карта кластера" (или "Узлы").
3. Выберите узел с ролью **Balancer** и зафиксировать его IP-адрес (см. рисунок 113).

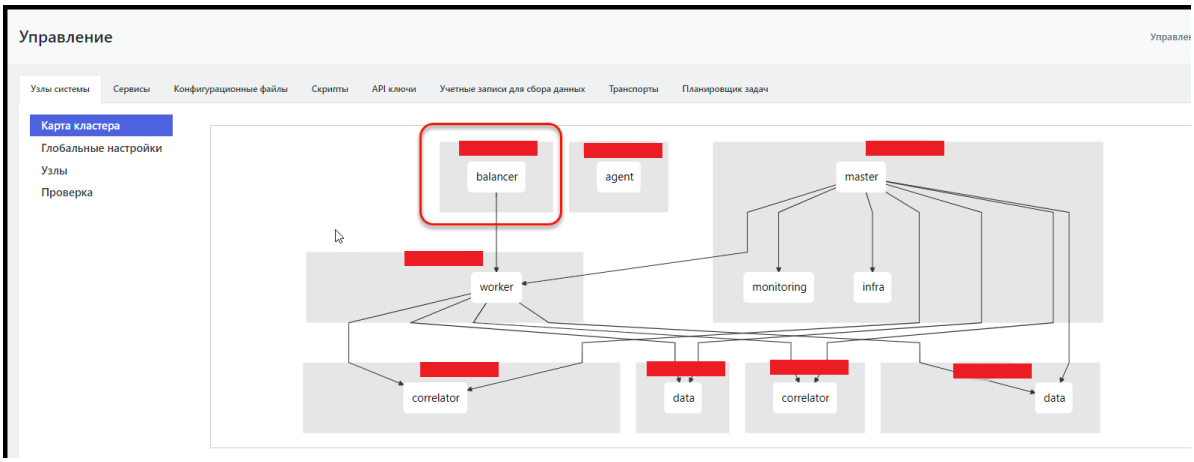

Рисунок 113 - Фиксация IP-адреса узла с ролью Balancer через "Карту кластера"

4. Перейдите в подраздел "Проверка", в списке узлов найти по IP-адресу узел **Balancer** и нажмите кнопку **Настройки** рядом с адресом узла (см. рисунок 114).

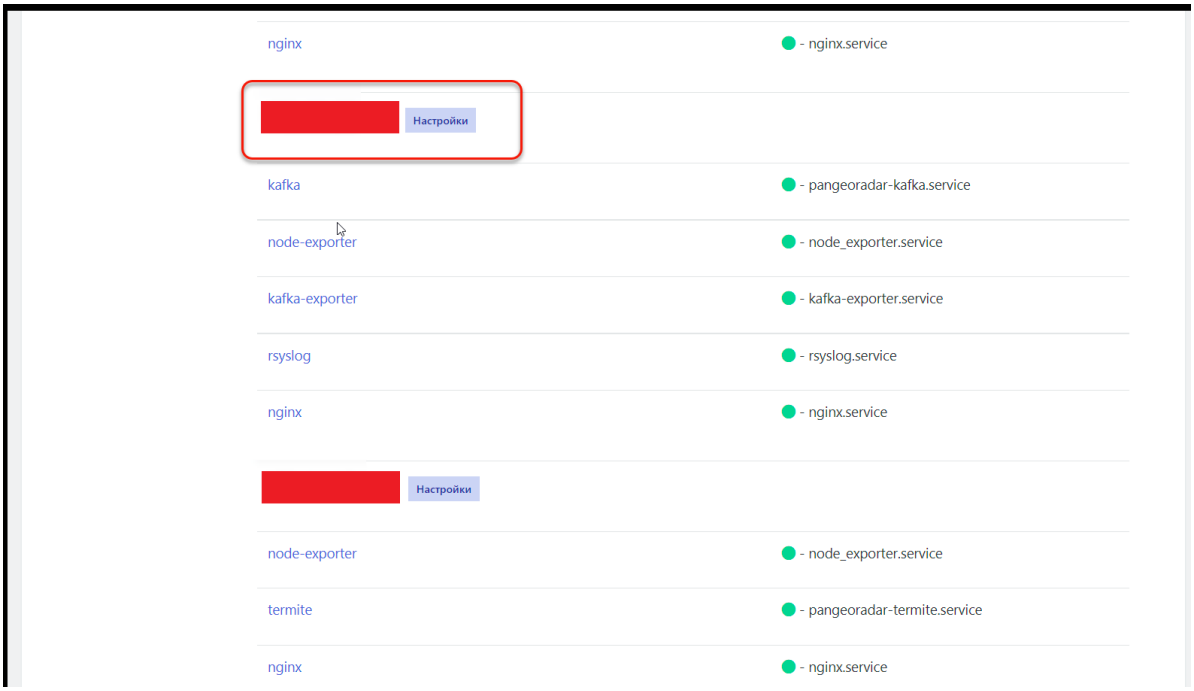

Рисунок 114 - Функция настройки узла Balancer

5. На открывшейся странице настроек узла выберите сервис **rsyslog** и проверьте его текущее состояние — посмотрите статус (см. рисунок 115) и журнал логов сервиса. Сервис должен находится в статусе **Active**.

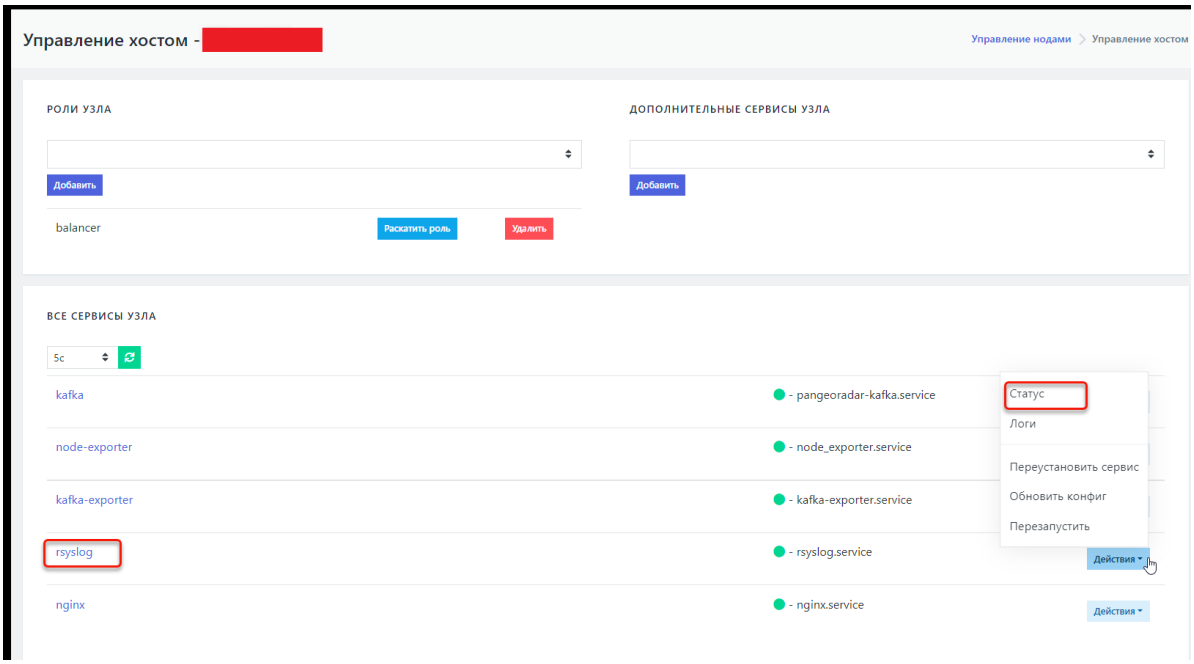

Рисунок 115 - Проверка статуса сервиса rsyslog

6. Перейдите на вкладку "Кластер"->"Конфигурационные файлы".
7. В списке конфигурационных файлов найдите для сервиса **rsyslog** конфигурационный файл **rsyslog-kafka.conf** и щелкните по названию файла. Откроется текст конфигурационного файла (см. рисунок 116).

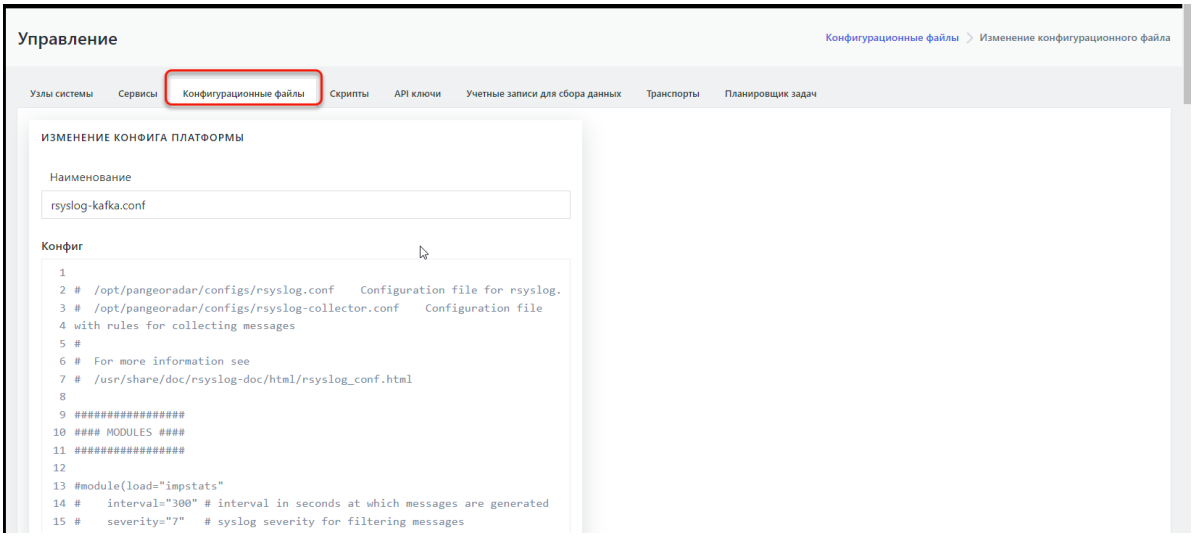

Рисунок 116 - Открытие текста конфигурационного файла для редактирования

8. Внесите в конфигурационный файл необходимые изменения. Например, в конце конфигурационного файла добавьте запись:

   `auth,authpriv.* @10.170.9.21:2671`

9. Нажмите кнопку **Изменить**.
10. Вернитесь в подраздел "Кластер"->"Узлы системы"->"Проверка" и откройте настройки соответствующего узла **Balancer** (см. шаги 4 и 5 данного алгоритма).
11. Для сервиса **rsyslog** в раскрывающемся меню "Действия" выберите пункт **Обновить конфиг**. Появится модальное окно с сообщением об успешном обновлении конфигурационного файла (см. рисунок 117).

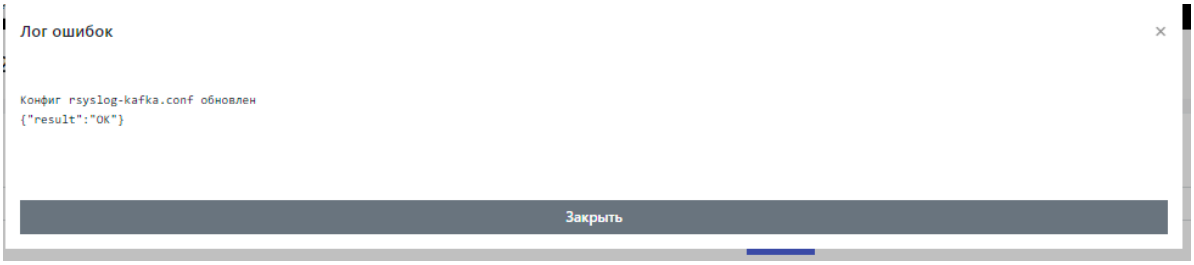

Рисунок 117 - Системное сообщение об успешном обновлении конфигурационного файла

12. Для сервиса **rsyslog** в раскрывающемся меню "Действия" выберите пункт **Перезапустить**. Дождитесь сообщения об успешном перезапуске сервиса (см. рисунок 118).

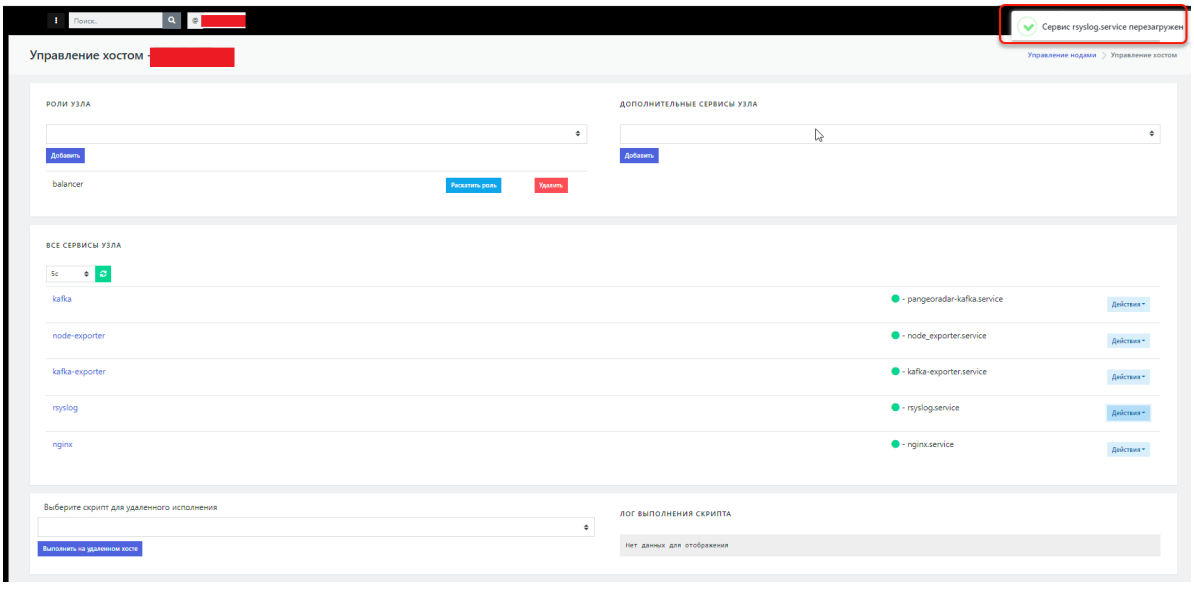

Рисунок 118 - сообщение об успешной перезагрузке сервиса

После проведения перезапуска сервиса при необходимости можно проверить статус сервиса (см. шаги 4 и 5). Также можно подключиться к узлу **Balancer** по SSH и выполнить для проверки изменений, следующую команду:

```
cat /opt/pangeoradar/configs/rsyslog-kafka.conf
```

---

30. Управление конфигурацией Платформы

Конфигурация Платформы и ее модулей осуществляется с помощью отдельных конфигурационных файлов.

Для удобства администратора настройки Платформы и ее модулей сохраняются в БД Платформы. При внесении изменений в настройки конфигурационные файлы формируются автоматически, поэтому администратору нет необходимости вносить изменения непосредственно в конфигурационные файлы.

30.1. Управление конфигурацией кластера

Для доступа к настройкам перейдите в раздел Платформы **Администрирование** - **Кластер**. Далее откройте вкладку **Управление конфигурацией**.

На вкладке в левой части отображается перечень параметров и модулей Платформы, в средней части - выбранные параметры, в правой части - история изменений конфигурации (см. рисунок 119).

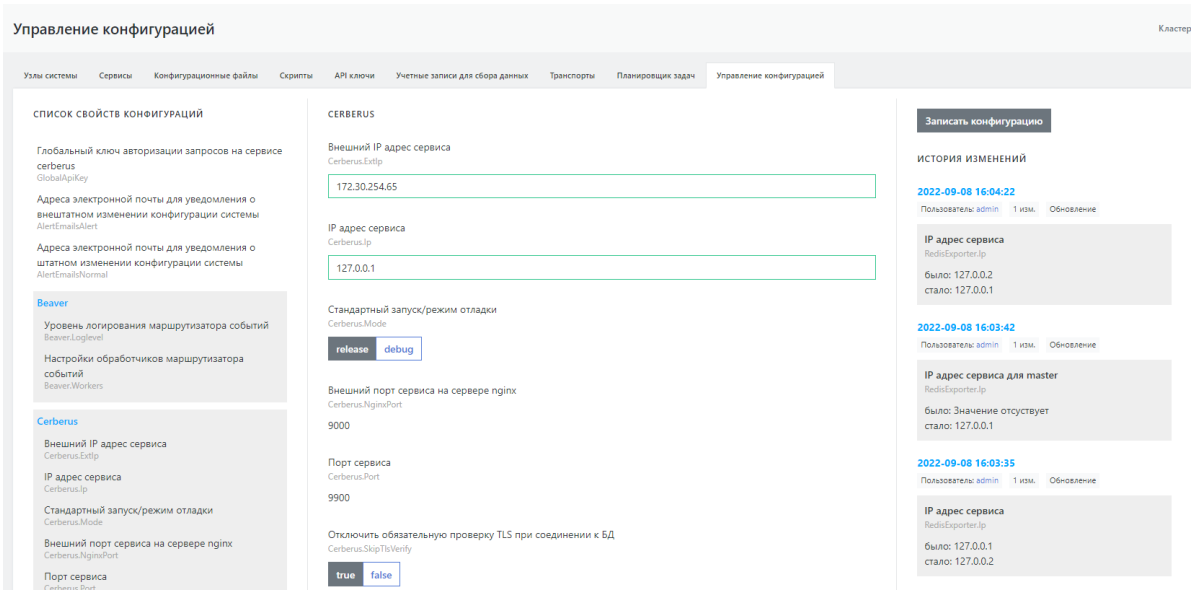

Рисунок 119 - Управление конфигурацией.

Для управления параметрами Платформы выберите один из параметров:

- **Глобальный ключ авторизации запросов на сервисе cerberus**. Представляет из себя глобальнй ключ для API.
- **Адреса электронной почты для уведомления о внештатном изменении конфигурации системы**. Адрес электронной почты о внештатном изменении конфигурации Платформы (например, прямая правка конфигурационных файлов).
- **Адреса электронной почты для уведомления о штатном изменении конфигурации системы**. Адрес электронной почты о штатном изменении конфигурации Платформы (например, другим администратором с помощью панели управления конфигурацией).

Для просмотра и редактирования параметров отдельного модуля кликните по его имени в левой части. Будут отображены все параметры модуля (см. рисунок 120).

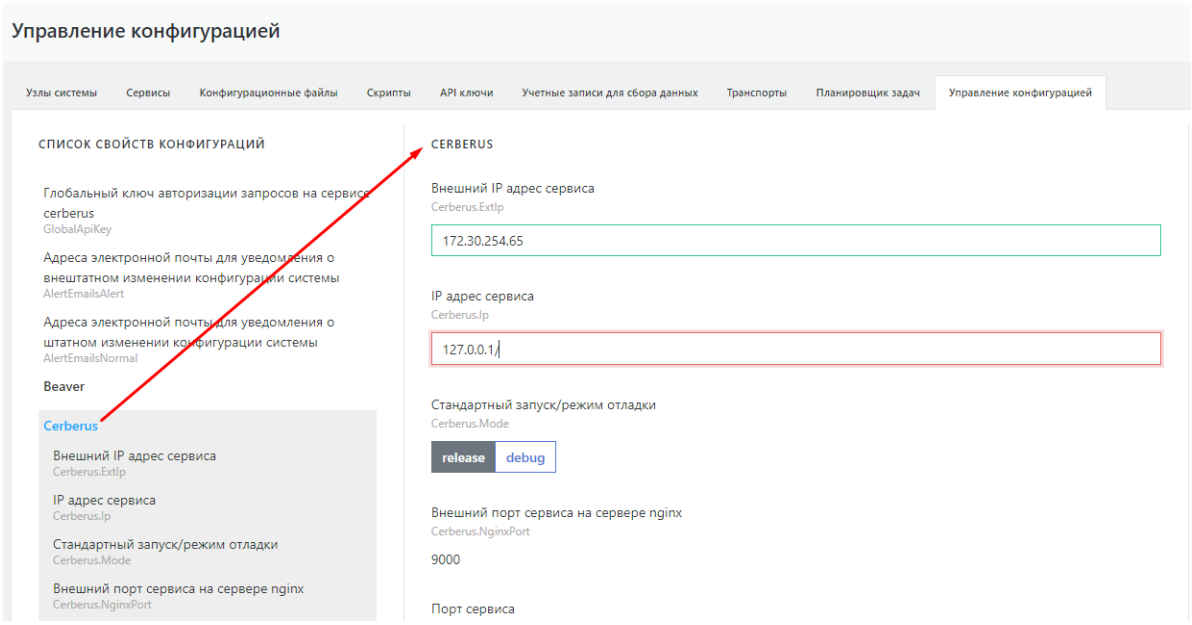

Рисунок 120 - Просмотр и редактирование параметров модуля.

Если в списке выбрать отдельный параметр, то отображен будет только он (см. рисунок 121).

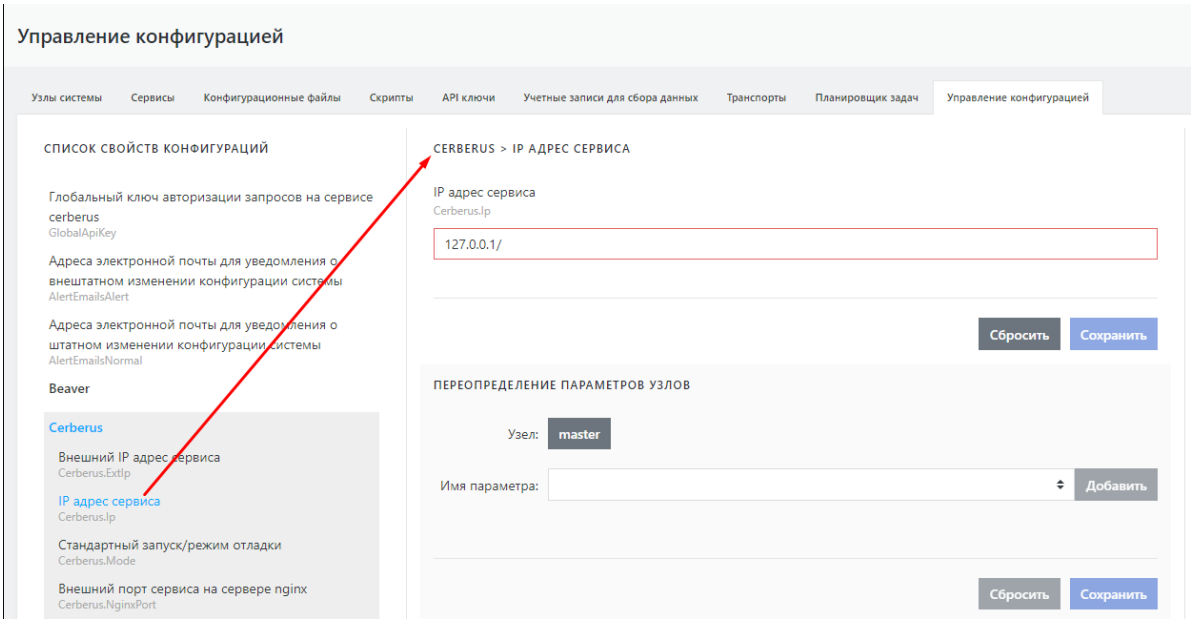

Рисунок 121 - Просмотр и редактирование отдельного параметра.

Для редактирования составных параметров (например, **Termite.DNS.InMemory**) необходимо выбрать группу параметров или отдельный параметр (см. рисунок 122).

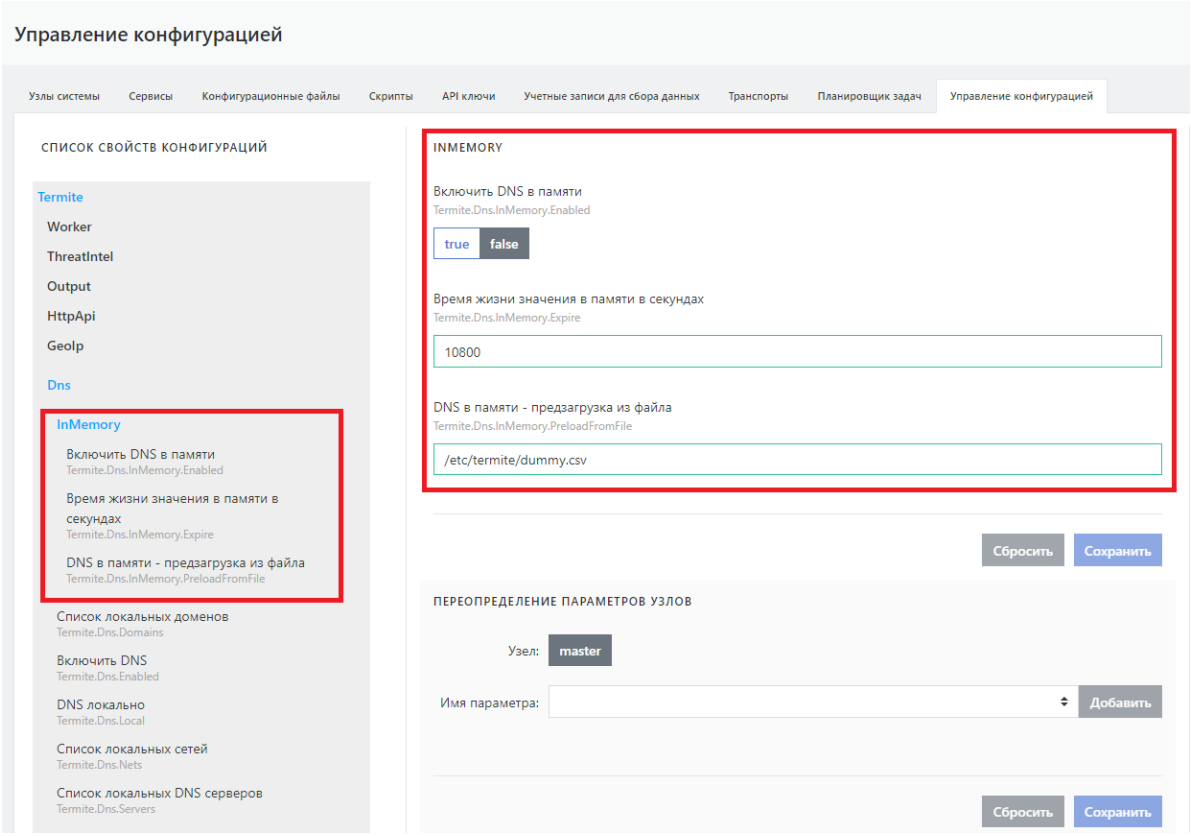

Рисунок 122 - Просмотр и редактирование составных параметров.

> Параметры, содержащие пароли (тип password), не отображаются в открытом виде. Для их маскирования применяется символ *.

После изменения параметров обязательно нажмите кнопку "**Сохранить**", чтобы сохранить измененные параметры. При этом внесенные изменения будут сохранены в БД Платформы и в конфигурационные файлы.

Клик по кнопке "**Сбросить**" вернет прежние значения.

Проверка изменения конфигурации и конфигурационных файлов осуществляется раз в минуту. Платформа сравнивает предыдущее и текущее значение хэш-суммы конфигурационных файлов и параметров. При их несовпадении Платформа вносит изменения, отправляет соответствующее уведомление и перезапускает сервисы с изменившимися параметрами.

Чтобы не ждать проверки изменения конфигурации и применить настройки немедленно кликните кнопку "**Записать конфигурацию**". После этого конфигурация будет перезаписана и соответствующие сервисы будут перезапущены автоматически.

30.2. Переопределение параметров узлов {#nodes}

Вносимые изменения параметров применяются на всех узлах Платформы, однако для отдельных узлов можно установить собственные значения параметров. Для этого при редактировании всех параметров предусмотрена область **Переопределение параметров узлов** (см. рисунок 123).

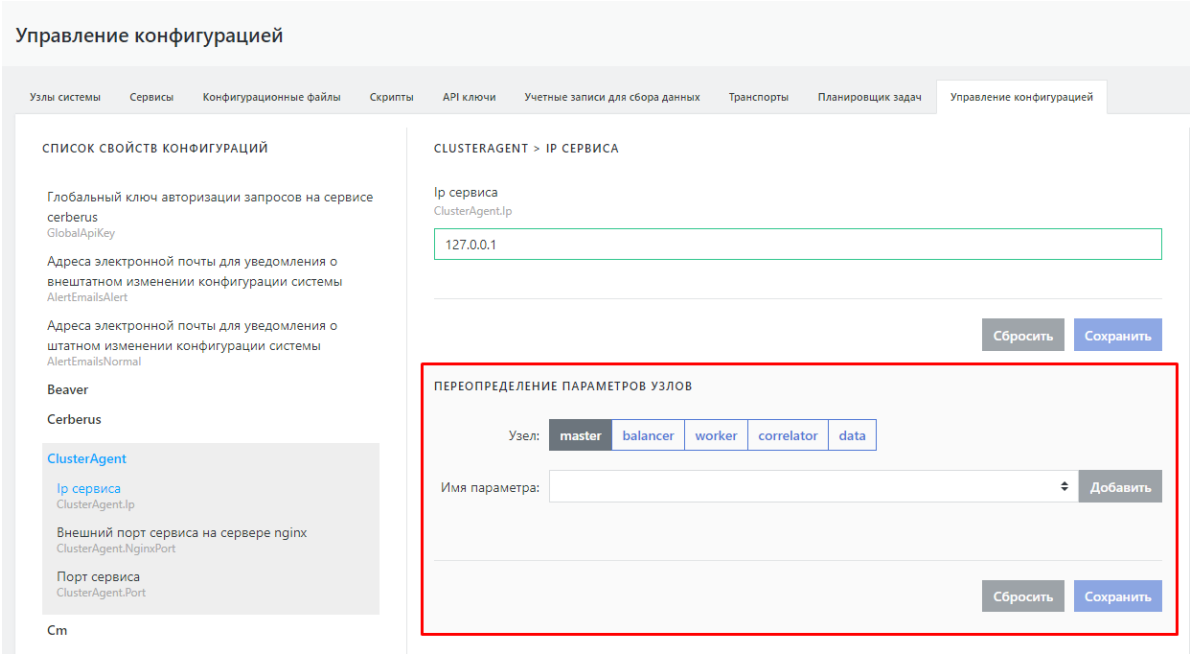

Рисунок 123 - Переопределение параметров узлов.

Выберите узел, для которого необходимо определить параметр, далее из списка выберите параметр, который необходимо определить для этого узла (см. рисунок 124) и нажмите кнопку **Добавить**.

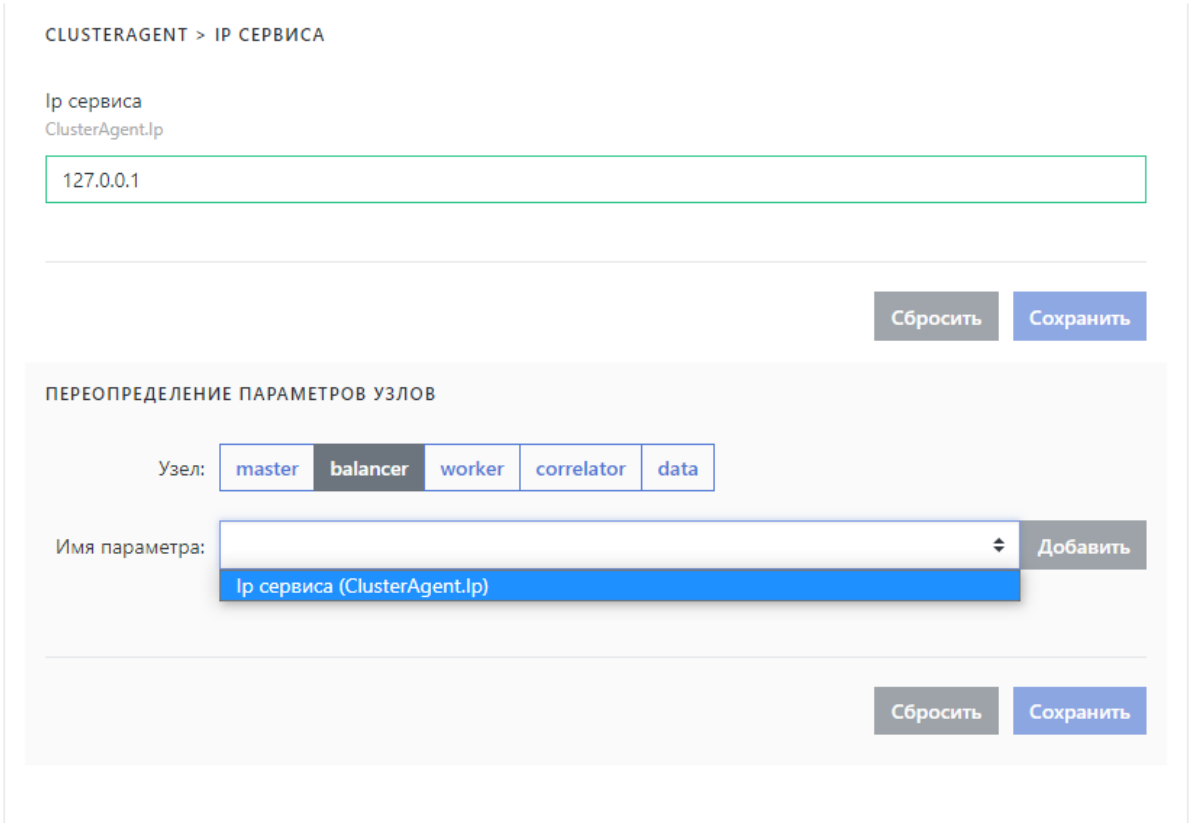

Рисунок 124 - Выбор параметра для узла.

Задайте значение параметра и нажмите кнопку "**Сохранить**". После применения изменений всех параметров запишите конфигурацию кликом по кнопке "**Записать конфигурацию**".

> Переопределение параметров узлов имеет смысл, если выполнена распределенная установка. Если Платформа установлена на один сервер, то переопределение параметра для единственного узла **Master** имеет смысл, если в дальнейшем планируется добавление дополнительных узлов с общими параметрами.

> При переопределении параметров для узла **Master** будут действовать переопределенные значения параметров, а не общие.

30.3. Перезапись параметров из консоли {#console}

В случае, если работоспособность Платформы при неправильном задании параметров нарушена, существует возможность просмотреть и изменить значения параметров Платформы и ее модулей с помощью консоли (на узле **Master**).

Перейдите в каталог `/opt/pangeoradar/bin` командой `cd /opt/pangeoradar/bin`.

Для чтения и задания параметров используются следующие команды консоли:

1. Чтение всех не перезаписанных параметров:

   `./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param`

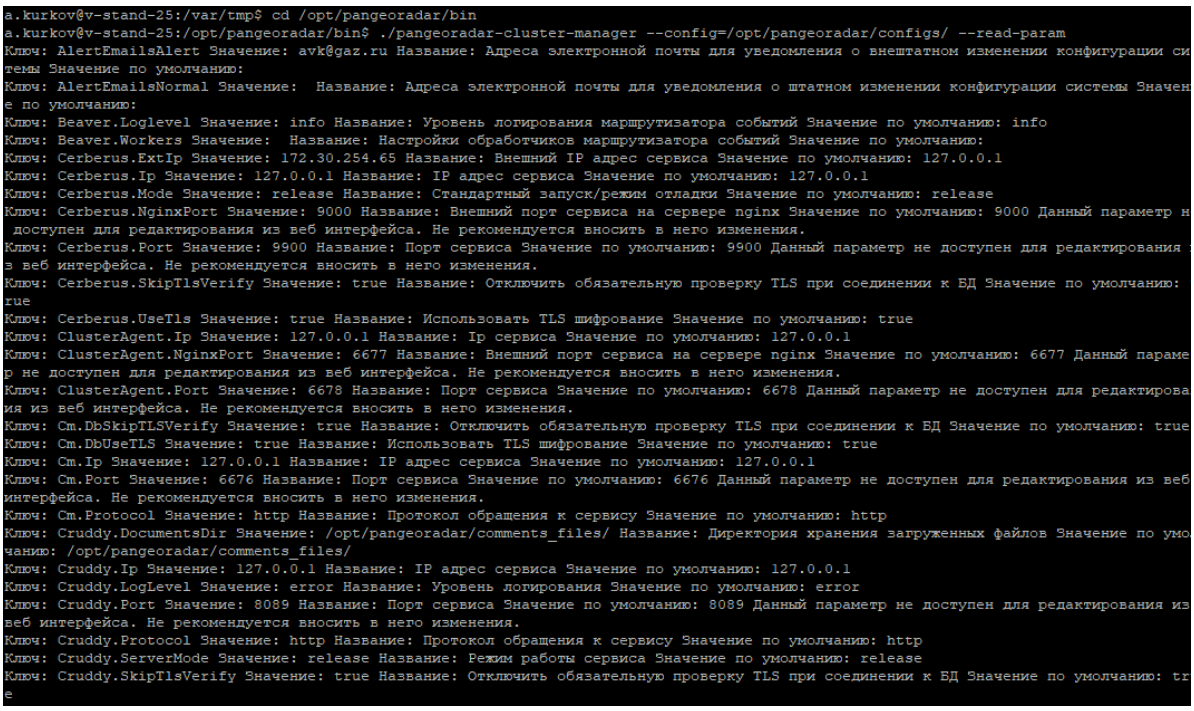

Рисунок 125

2. Чтение всех перезаписанных параметров:

   `./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param --for-overrides`

3. Чтение параметра (ключ из запроса 1 выше):

   `./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param --param-key=<ключ>`

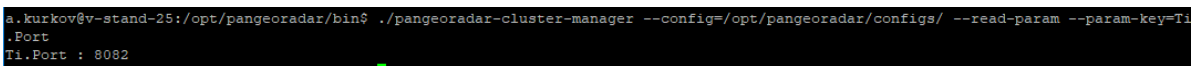

Рисунок 126

4. Чтение перезаписанного параметра (ключ из запроса 2 выше вида название*параметра* > *id*ноды):

   `./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param --for-overrides --param-key="<ключ>"`

5. Запись параметра:

`./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --write-param --param-key=<ключ> --param-value=<значение>`

```
a.kurkov@v-stand-25:/opt/pangeoradar/bin$ ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --write-param --param-key=T
i.Port --param-value=8082
Для Ti.Port установлено значение
```

Рисунок 127

6. Запись перезаписанного параметра (ключ из запроса 2 выше вида название*параметра* > *id*ноды):

   `./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --write-param --param-key="<ключ>" --param-value=<значение> --for-overrides`

7. Перезапись конфигурационных файлов в БД:

   `./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --refresh-param-files`

8. Перезапись конфигурационных файлов в БД для перезаписанных параметров:

   `./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --refresh-param-files --for-overrides`

30.4. Подключение нового инстанса к управляющему инстансу

Перейдите в консоль администратора на **управляющем инстансе** и выполните команду:

```
/opt/pangeoradar/bin/pangeoradar-karaken  create-instance --name=<ip подчиненного  инстанса> --url=https://<ip  подчиненного  инстанса>:9000 --order=1 --conf=/opt/pangeoradar/configs/
```

Перейдите в веб-интерфейс подчиненного инстанса, который необходимо подключить к управляющему инстансу.

В разделе «Кластер» - «Управление конфигурацией» в свойствах «DNS» измените «Адрес сервиса авторизации» указанный url-адрес на url-адрес управляющего инстанса в формате `https://<ip-адрес управляющего инстанса>:8180`

Нажмите «Сохранить» и «Записать конфигурацию».

Перейдите в консоль администратора на подчиненном инстансе и перезапустите сервисы следующими командами:

```
service pangeoradar-cluster-manager restart
service pangeoradar-cluster-agent restart
service pangeoradar-cerberus restart
service pangeoradar-toller restart
```

Перейдите в веб-интерфейс управляющего инстанса и проверьте доступность подчиненного инстанса. В верхнем панели интерфейса должен появиться переключатель инстансов.