Аудит действий пользователя в Почте

Инструкция для администраторов

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Назначение документа

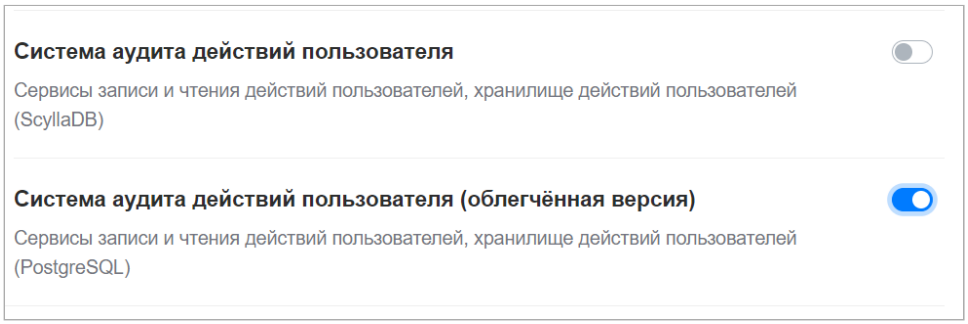
В документе описаны предусмотренные в Почте системы аудита действий пользователя и их отличия. Описано как включить сбор статистики по IP и настроить отправку событий во внешние хранилища.

Документ нужен системным администраторам организации.

Системы аудита

В Почте предусмотрены 2 системы аудита действий пользователей:

- Основанная на БД ScyllaDB — включается по умолчанию. Контейнер с базой данных: **beccasc***. Контейнер с API: **becca***.
- Основанная на БД PostgreSQL. Контейнер с базой данных: **rebeccapg***. Контейнер с API: **rebecca***.



Отличия систем аудита

1. Система на ScyllaDB имеет возможность дублировать действия пользователя во внешние хранилища.
2. Система на PostgreSQL позволяет искать события без привязки к пользователю, то есть просматривать все события из определенной группы. Система на ScyllaDB позволяет искать только действия конкретного пользователя.
3. Система на PostgreSQL потребляет меньше оперативной памяти, поэтому и называется «облегчённой версией».

Описание событий

Действия пользователя в системе сопровождаются отправкой событий. События делятся на следующие группы:

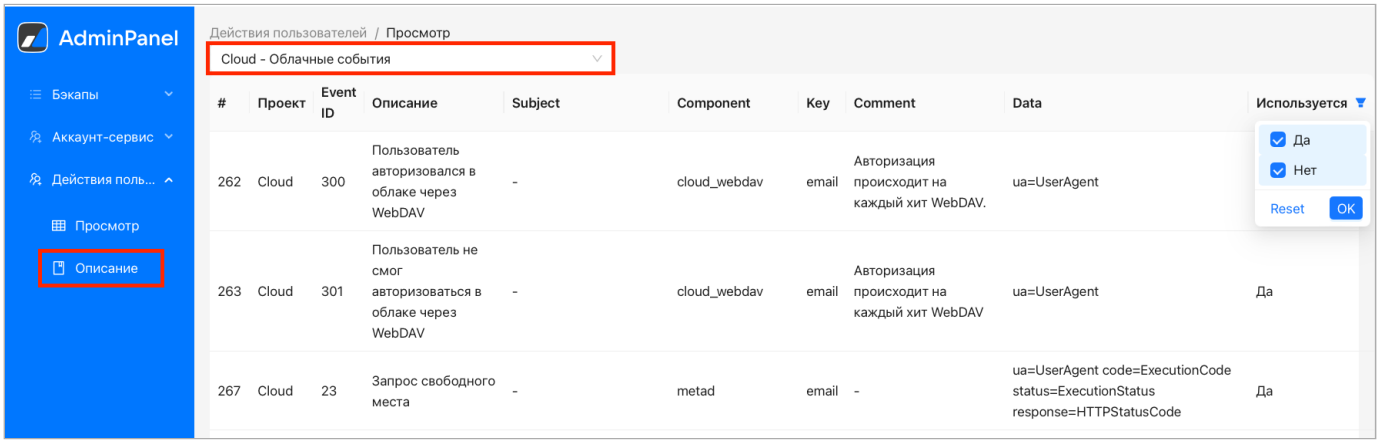
- MailAdmin – действия администратора в Почте.
- Calendar – события Календаря.
- Becca – внутренние события системы аудита на ScyllaDB.
- Mail – события почты и авторизации.
- Cloud – события Диска.
- SpammerDB.
- Alias – события алиасов почтовых ящиков.

Чтобы посмотреть список всех событий и подробное описание каждого события:

1. Перейдите на страницу `https://biz.<mail_domain>` и авторизуйтесь в панели администратора.
2. Перейдите по URL-адресу `https://biz.<mail_domain>/oper/becca/docs`.

Здесь по каждому событию вы найдете:

- Проект, к которому относится событие и идентификатор события.
- Описание события и комментарий к нему.
- Компонент и параметры события.
- Используется ли событие.

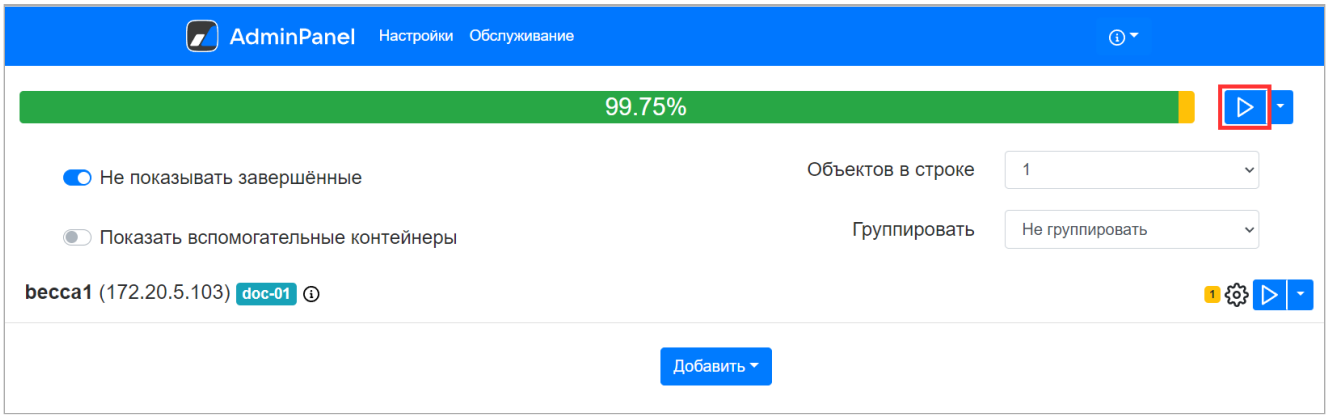


Включить сбор статистики по IP

Сбор статистики нужно включать только для системы на ScyllaDB. Для системы на PostgreSQL она включена по умолчанию.

1. Откройте веб-интерфейс установщика `http://<server-address>:8888`.

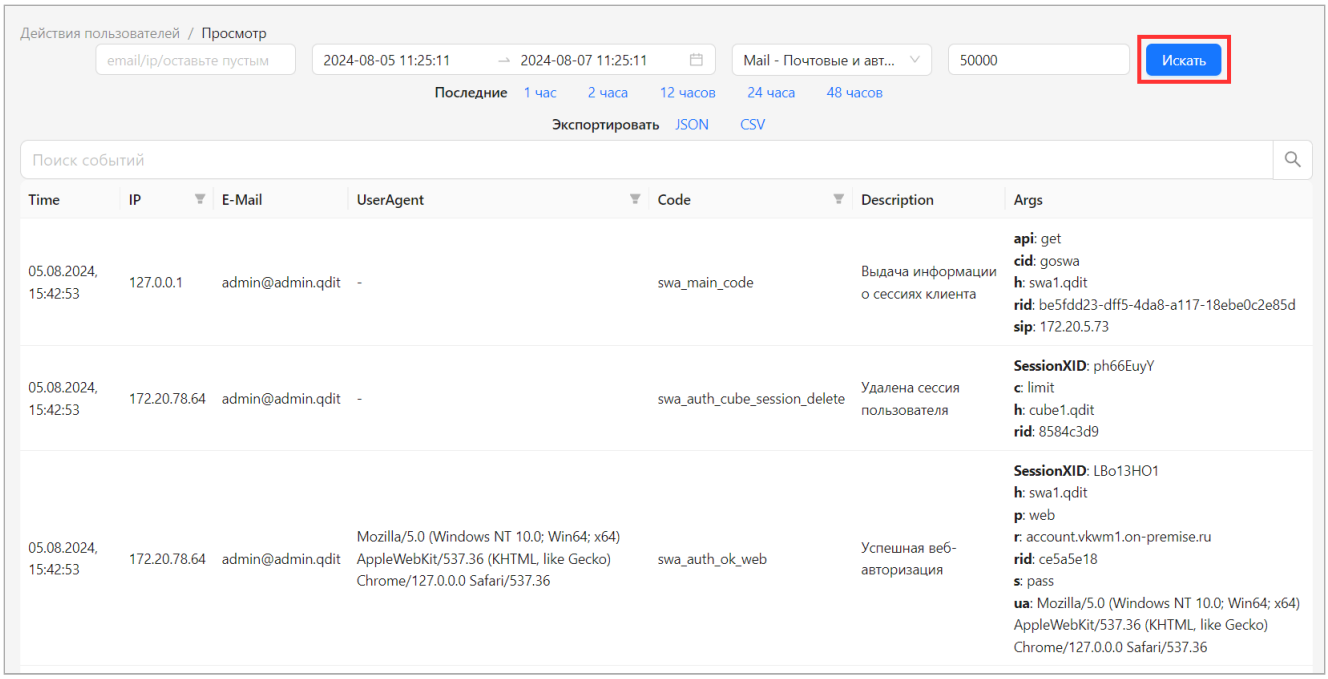
2. Перейдите на вкладку **Настройки → Настройки компонентов → Система учета действий пользователя**.
3. Нажмите кнопку редактировать .
4. Включите опцию **Включить статистику по IP**.
5. Задайте **Время хранения событий по IP** в секундах. По умолчанию устанавливается 3 месяца.
6. Кликните по кнопке **Сохранить**.
7. Перейдите на вкладку **AdminPanel** и запустите автоматическую установку.



8. Подтвердить запуск автоматической установки, нажав на кнопку **Запустить** во всплывающем окне.

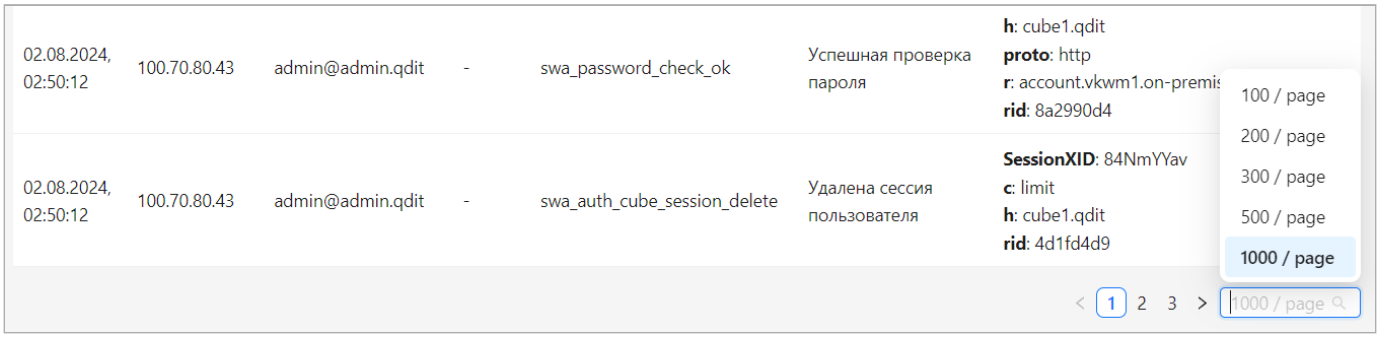
Посмотреть действия пользователя в системе

1. Перейдите на страницу `https://biz.<mail_domain>` и авторизуйтесь в панели администратора.
2. Перейдите по URL-адресу `https://biz.<mail_domain>/oper/` .
3. В меню слева, в разделе **Действия пользователя**, выберите **Просмотр**.
4. Укажите email или IP пользователя. Если пользуетесь системой на PostgreSQL, то поле можно оставить пустым.
5. Задайте период для вывода событий или воспользуйтесь одним из готовых фильтров.
6. Выберите группу событий.
7. Задайте выводимое количество событий.
8. Нажмите на кнопку **Искать**.



Результаты поиска можно экспортировать в .json или .csv файлы.

В самом низу страницы можно переключаться между страницами и управлять количеством событий выводимых на одной странице.

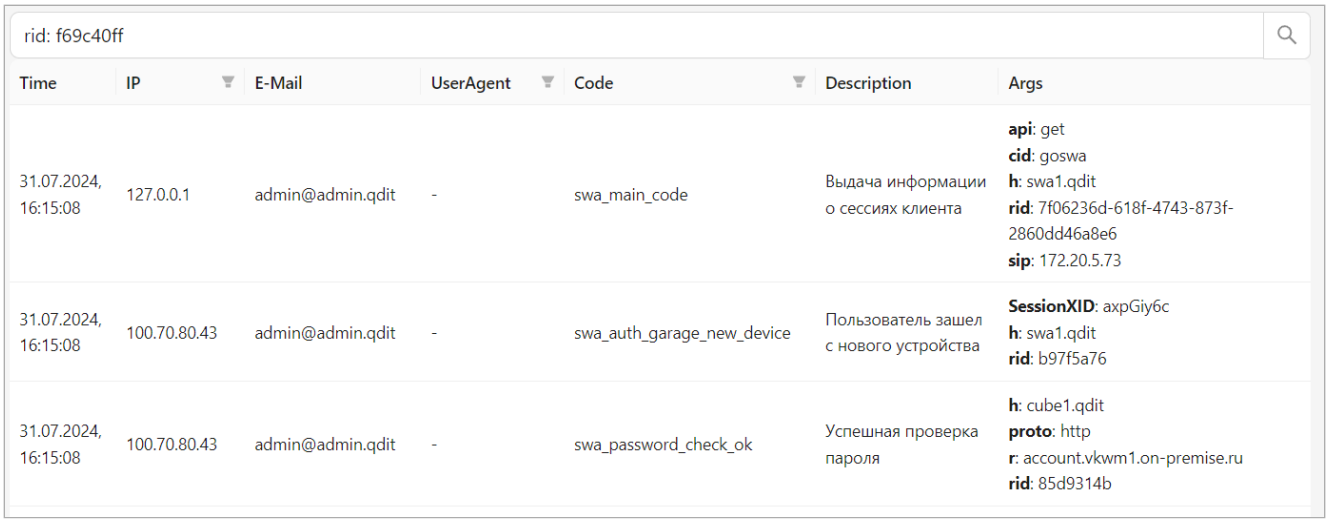


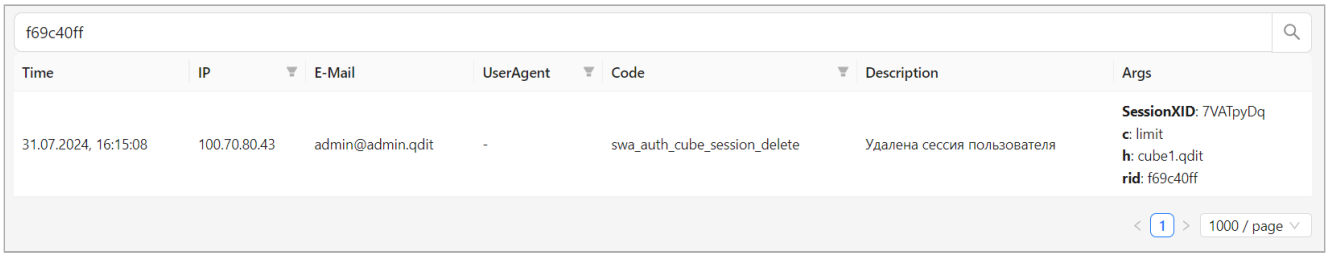
Поиск событий

Поиск событий производится по содержимому в столбце **Args**. В каждой ячейке столбца **Args** перечислены названия и значения полей. Названия полей выделены жирным шрифтом.

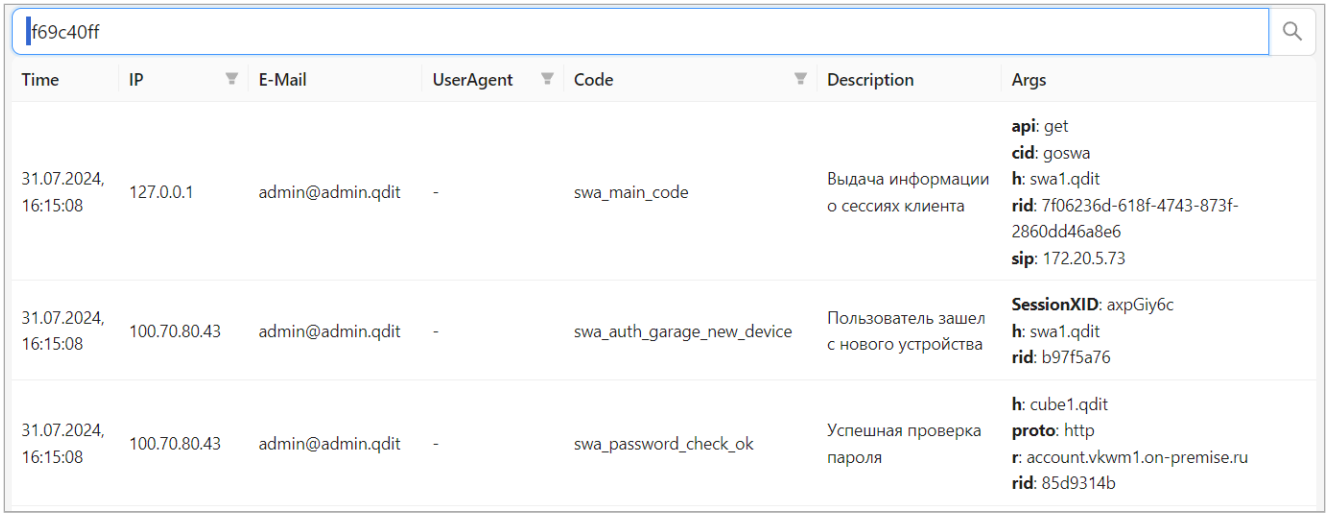
Особенности работы поиска:

- Поиск производится только по значениям полей. То есть запрос `rid: f69c40ff` не выдаст нужное событие, в отличии от `f69c40ff`.





- Поиск чувствителен к пробелам. Если перед запросом `f69c40ff` поставить пробел, то поиск не выдаст нужное событие.



- Поисковой запрос влияет на экспорт событий в .json или .csv файлы.

  Пример экспорта в .csv файл, для запроса `f69c40ff`:

```
time;ip;email;ua;projectDescription;code;eventDescription;arguments
"""31.07.2024, 16:15:08""";100.70.80.43;admin@admin.qdit;-;Почтовые и авторизационные
события;swa_auth_cube_session_delete;Удалена сессия пользователя;SessionXID,
7VATpyDq,c,limit,h,cube1.qdit,rid,f69c40ff
```

Настроить отправку событий во внешние хранилища

1. Откройте веб-интерфейс установщика `http://server-adress:8888`.
2. Перейдите на вкладку **Настройки → Интеграции → Дублирование действий пользователей во внешние хранилища**.
3. Нажмите кнопку редактировать .
4. Включите флаг того хранилища, которое вы планируете использовать: MySQL, Logstash и rsyslog. Есть возможность включения TLS-шифрования.
5. Заполните необходимые поля:

   MySQL

   Предварительно создайте таблицу, в которую будут сохраняться логи.

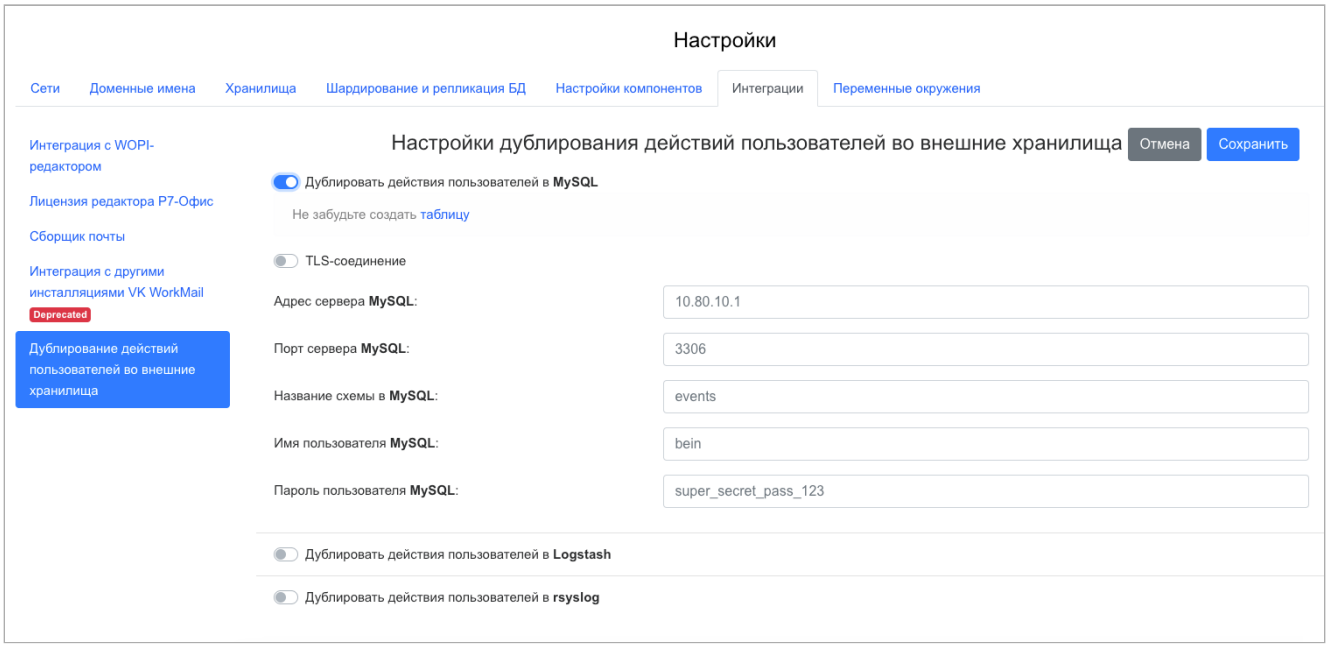
   Адрес сервера MySQL — введите адрес сервера MySQL, на котором будут храниться логи.

   Порт сервера MySQL — порт, открытый в вашей БД для VK Workspace.

   Название схемы в MySQL — тип архитектуры (схемы) вашей БД.

   Имя пользователя MySQL — пользователь БД, имеющий права на запись.

   Пароль пользователя MySQL — введите пароль пользователя, указанного в поле выше.

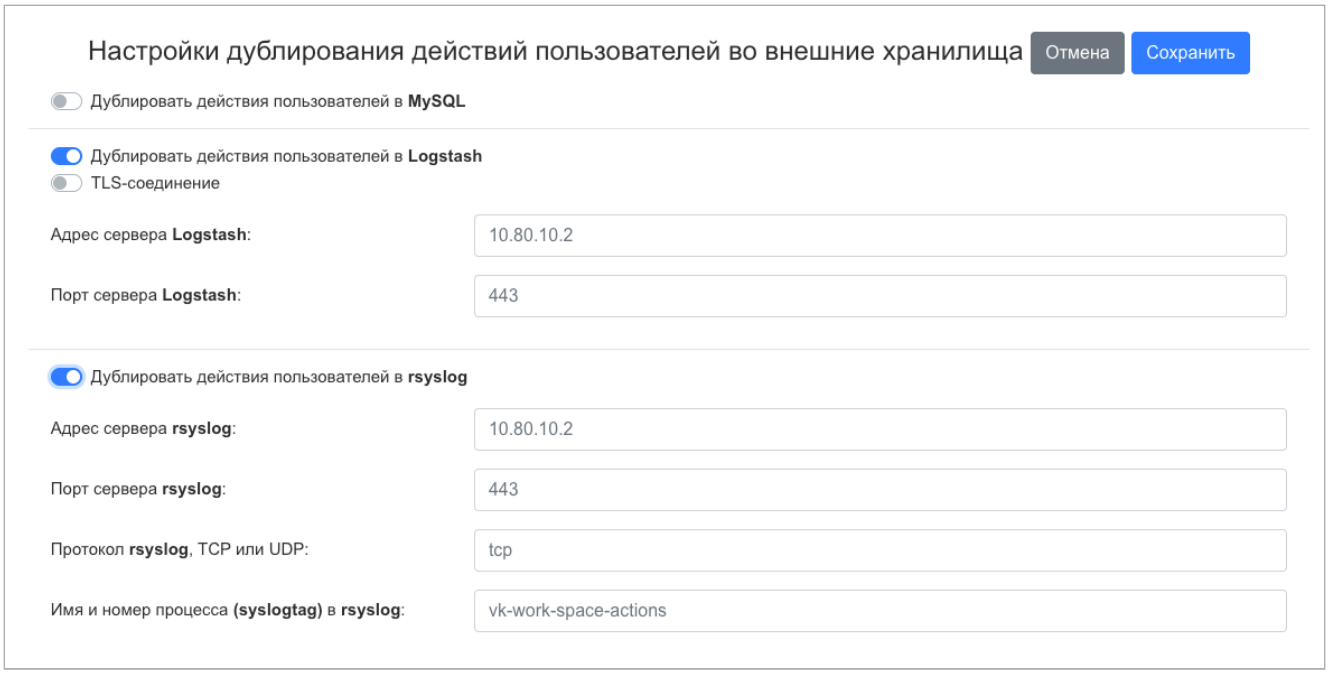


   Logstash

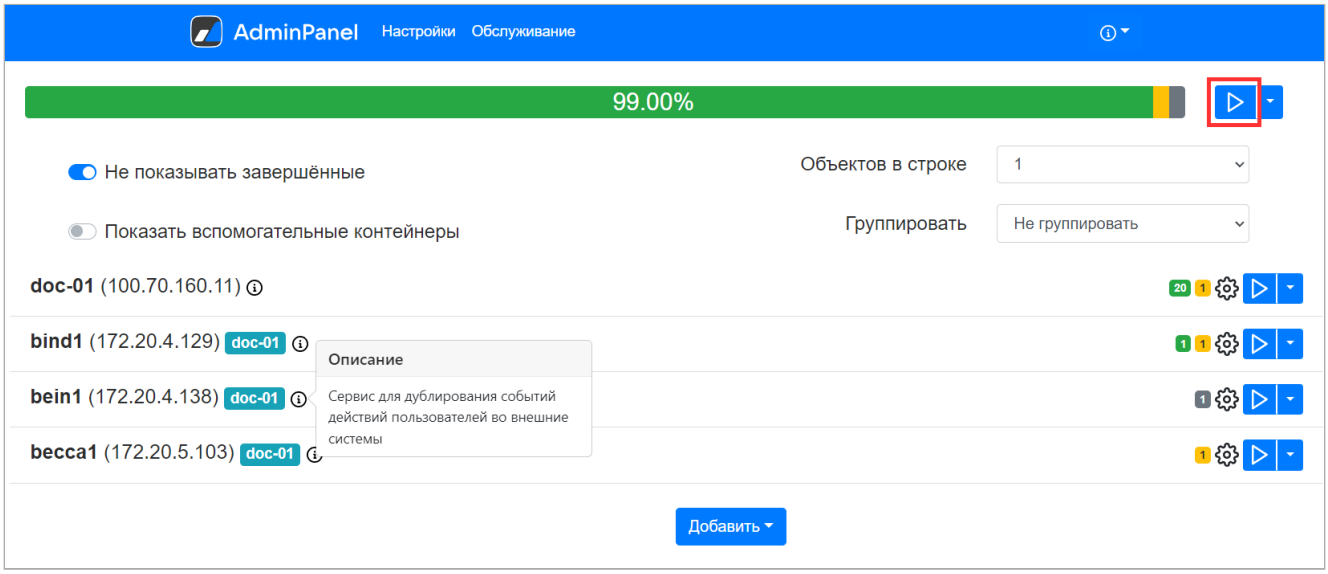
   Введите адрес сервера и порт.

   rsyslog

   Чтобы передавать данные в **rsyslog**, введите адрес сервера, его порт, протокол подключения и syslogtag.



6. Кликните по кнопке **Сохранить**.
7. В случае кластерной установки распределите контейнеры **bein*** и **becca*** по гипервизорам с типом фронт.
8. Перейдите на вкладку **AdminPanel** и запустите автоматическую установку.



9. Подтвердить запуск автоматической установки, нажав на кнопку **Запустить** во всплывающем окне.

Аудит почтовых ящиков для версии Почты 1.16 и ниже

> **Важно**
>
> Для версий выше 1.17 представленная ниже информация не актуальна.

Описание

Отслеживаются входы в почтовый ящик и действия, выполняемые владельцем ящика. Записи об активности пользователей попадают в выделенное хранилище BECCA.

Состояние по умолчанию

Аудит почтовых ящиков включен, веб-интерфейс BECCA выключен.

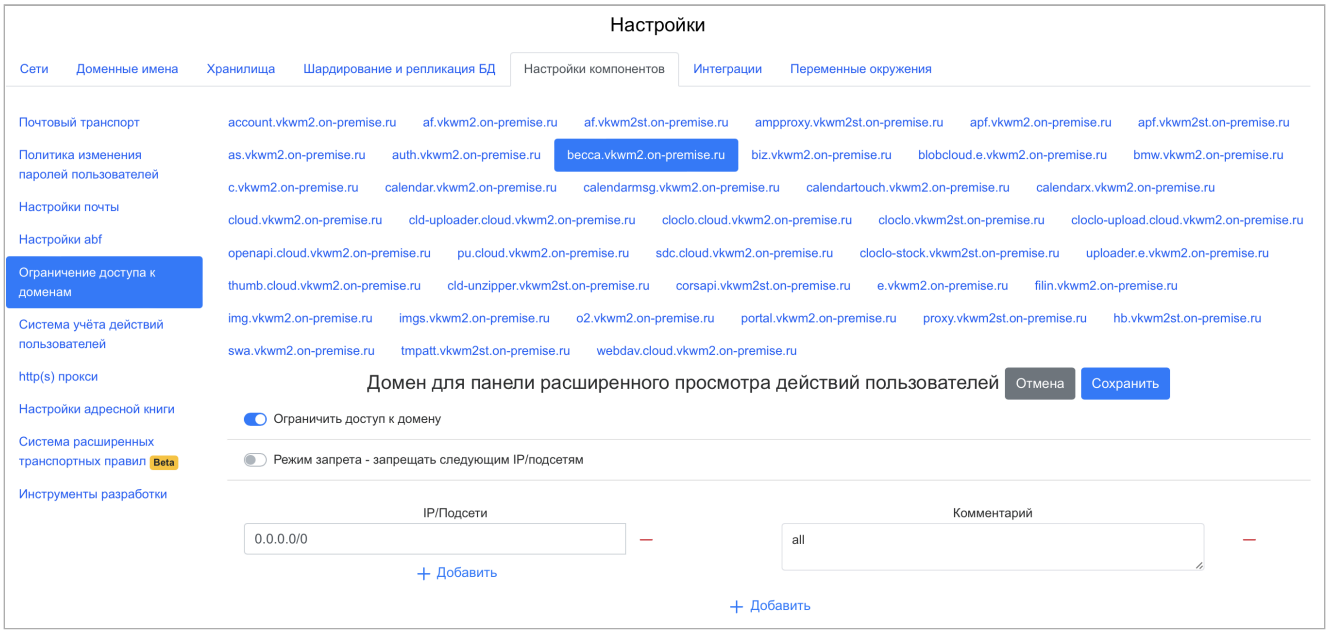
Рекомендуемое состояние

Аудит почтовых ящиков включен, веб-интерфейс BECCA включен.

Настройка доступа к веб-интерфейсу BECCA

Веб-интерфейс BECCA находится по адресу `https://becca.<mail_domain>`. Чтобы получить доступ выполните ряд настроек в веб-интерфейсе установщика `http://server-address:8888`:

1. Включите флаг **Включить статистику по IP** на вкладке **Настройки** в разделе **Настройки компонентов → Система учета действий пользователей**
2. Укажите IP/подсети, для которых будет разрешен доступ к домену `becca.<mail_domain>`, в разделе **Настройки → Настройки компонентов → Ограничение доступа к доменам**.
3. Нажмите на синюю кнопку **Сохранить**, чтобы сохранить изменения.



4. Перейдите на вкладку **AdminPanel** и запустить автоматическую установку, нажав на зеленую кнопку **Play**.

Автор: Груздев Никита

31 июля 2025 г.