

Аудит действий пользователя в Почте

Инструкция для администраторов

Оглавление

Назначение документа	3
Системы аудита	3
Отличия систем аудита	3
Описание событий	4
Включить сбор статистики по IP	4
Посмотреть действия пользователя в системе	5
Поиск событий	6
Настроить отправку событий во внешние хранилища	8
Аудит почтовых ящиков для версии Почты 1.16 и ниже	9

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***.

Система аудита действий пользователя	<input type="checkbox"/>
Сервисы записи и чтения действий пользователей, хранилище действий пользователей (ScyllaDB)	
Система аудита действий пользователя (облегчённая версия)	<input checked="" type="checkbox"/>
Сервисы записи и чтения действий пользователей, хранилище действий пользователей (PostgreSQL)	

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:

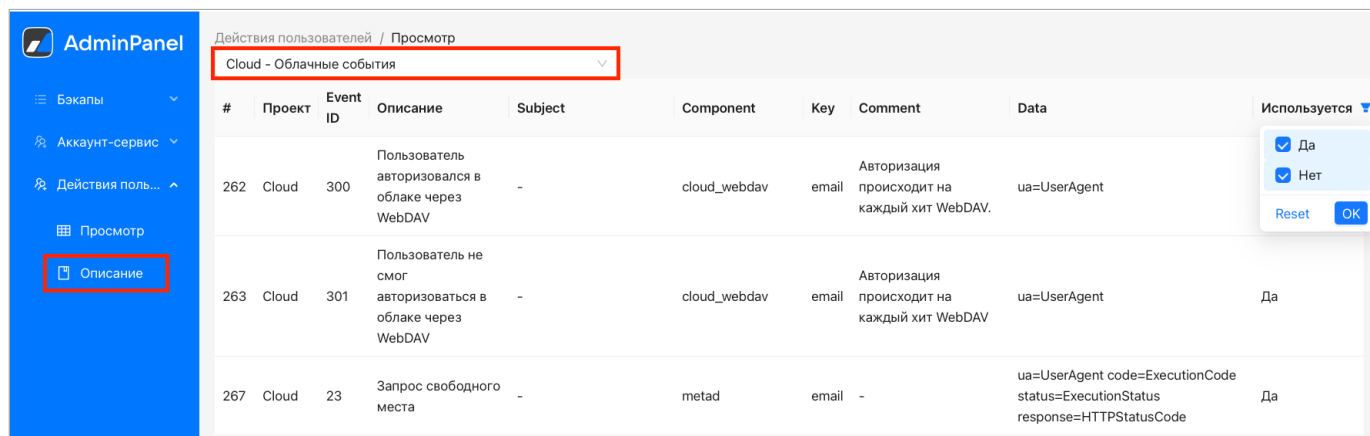
- MailAdmin – действия администратора в Почте.
- Calendar – события Календаря.
- Весса – внутренние события системы аудита на ScyllaDB.
- Mail – события почты и авторизации.
- Cloud – события Диска.
- SpammerDB.
- Alias – события алиасов почтовых ящиков.

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 комментариев к нему.
- Компонент и параметры события.
- Используется ли событие.




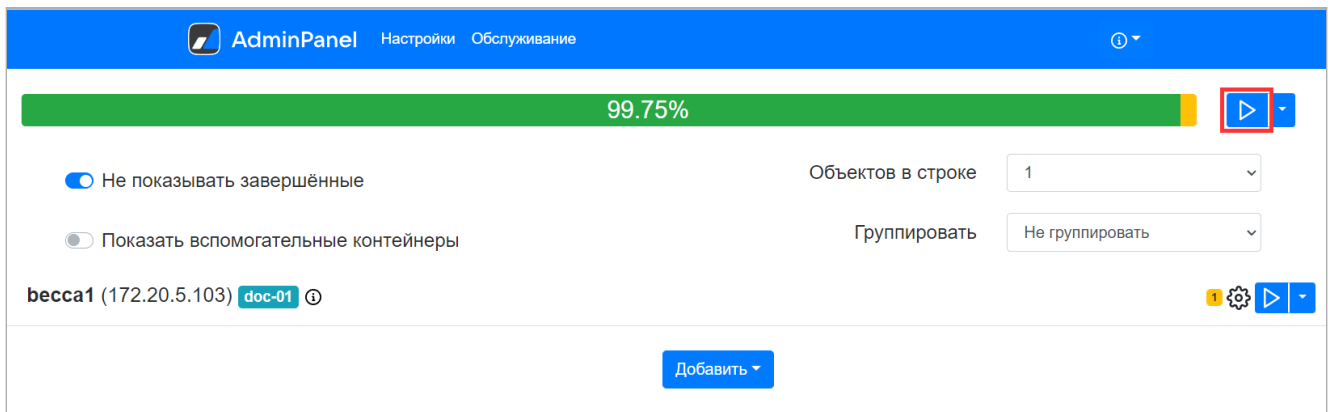
#	Проект	Event ID	Описание	Subject	Component	Key	Comment	Data	Используется
262	Cloud	300	Пользователь авторизовался в облаке через WebDAV	-	cloud_webdav	email	Авторизация происходит на каждый хит WebDAV.	ua=UserAgent	<input checked="" type="checkbox"/> Да <input checked="" type="checkbox"/> Нет
263	Cloud	301	Пользователь не смог авторизоваться в облаке через WebDAV	-	cloud_webdav	email	Авторизация происходит на каждый хит WebDAV	ua=UserAgent	Да
267	Cloud	23	Запрос свободного места	-	metad	email	-	ua=UserAgent code=ExecutionCode status=ExecutionStatus response=HTTPStatusCode	Да

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. Подтвердите 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**.

Действия пользователей / Просмотр

email/ip/оставьте пустым 2024-08-05 11:25:11 → 2024-08-07 11:25:11 Mail - Почтовые и авт... 50000 Искать

Последние 1 час 2 часа 12 часов 24 часа 48 часов

Экспортировать JSON CSV

Поиск событий

Time	IP	E-Mail	UserAgent	Code	Description	Args
05.08.2024, 15:42:53	127.0.0.1	admin@admin.qdit	-	swa_main_code	Выдача информации о сессиях клиента	api: get cid: goswa h: swa1.qdit rid: be5fdd23-dff5-4da8-a117-18ebe0c2e85d sip: 172.20.5.73
05.08.2024, 15:42:53	172.20.78.64	admin@admin.qdit	-	swa_auth_cube_session_delete	Удалена сессия пользователя	SessionXID: ph66EuyY c: limit h: cube1.qdit rid: 8584c3d9
05.08.2024, 15:42:53	172.20.78.64	admin@admin.qdit	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	swa_auth_ok_web	Успешная веб-авторизация	SessionXID: lBo13HO1 h: swa1.qdit p: web r: account.vkwm1.on-premise.ru rid: ce5a5e18 s: pass ua: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36

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.

02.08.2024, 02:50:12	100.70.80.43	admin@admin.qdit	-	swa_password_check_ok	Успешная проверка пароля	h: cube1.qdit proto: http r: account.vkwm1.on-premise.ru rid: 8a2990d4
02.08.2024, 02:50:12	100.70.80.43	admin@admin.qdit	-	swa_auth_cube_session_delete	Удалена сессия пользователя	SessionXID: 84NmYYav c: limit h: cube1.qdit rid: 4d1fd4d9

100 / page
 200 / page
 300 / page
 500 / page
1000 / page

< 1 2 3 > 1000 / page

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`.

rid: f69c40ff

Time	IP	E-Mail	UserAgent	Code	Description	Args
31.07.2024, 16:15:08	127.0.0.1	admin@admin.qdit	-	swa_main_code	Выдача информации о сессиях клиента	api: get cid: goswa h: swa1.qdit rid: 7f06236d-618f-4743-873f-2860dd46a8e6 sip: 172.20.5.73
31.07.2024, 16:15:08	100.70.80.43	admin@admin.qdit	-	swa_auth_garage_new_device	Пользователь зашел с нового устройства	SessionXID: axpGiy6c h: swa1.qdit rid: b97f5a76
31.07.2024, 16:15:08	100.70.80.43	admin@admin.qdit	-	swa_password_check_ok	Успешная проверка пароля	h: cube1.qdit proto: http r: account.vkwm1.on-premise.ru rid: 85d9314b

f69c40ff

Time	IP	E-Mail	UserAgent	Code	Description	Args
31.07.2024, 16:15:08	100.70.80.43	admin@admin.qdit	-	swa_auth_cube_session_delete	Удалена сессия пользователя	SessionXID: 7VATpyDq c: limit h: cube1.qdit rid: f69c40ff

< 1 > 1000 / page

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

f69c40ff


Time	IP	E-Mail	UserAgent	Code	Description	Args
31.07.2024, 16:15:08	127.0.0.1	admin@admin.qdit	-	swa_main_code	Выдача информации о сессиях клиента	api: get cid: goswa h: swa1.qdit rid: 7f06236d-618f-4743-873f-2860dd46a8e6 sip: 172.20.5.73
31.07.2024, 16:15:08	100.70.80.43	admin@admin.qdit	-	swa_auth_garage_new_device	Пользователь зашел с нового устройства	SessionXID: axpGiy6c h: swa1.qdit rid: b97f5a76
31.07.2024, 16:15:08	100.70.80.43	admin@admin.qdit	-	swa_password_check_ok	Успешная проверка пароля	h: cube1.qdit proto: http r: account.vkwm1.on-premise.ru rid: 85d9314b

- 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-address: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.

Настройки

Сети Доменные имена Хранилища Шардирование и репликация БД Настройки компонентов Интеграции Переменные окружения

Настройки дублирования действий пользователей во внешние хранилища

[Отмена](#) [Сохранить](#)

Дублировать действия пользователей в **MySQL**

Не забудьте создать [таблицу](#)

TLS-соединение

Адрес сервера **MySQL**:

Порт сервера **MySQL**:

Название схемы в **MySQL**:

Имя пользователя **MySQL**:

Пароль пользователя **MySQL**:

Дублировать действия пользователей в **Logstash**

Дублировать действия пользователей в **rsyslog**

Logstash

Введите адрес сервера и порт.

rsyslog

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

Настройки дублирования действий пользователей во внешние хранилища

Отмена Сохранить

Дублировать действия пользователей в **MySQL**

Дублировать действия пользователей в **Logstash**

TLS-соединение

Адрес сервера **Logstash**:

Порт сервера **Logstash**:

Дублировать действия пользователей в **rsyslog**

Адрес сервера **rsyslog**:

Порт сервера **rsyslog**:

Протокол **rsyslog**, TCP или UDP:

Имя и номер процесса (**syslogtag**) в **rsyslog**:

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.

The screenshot shows the AdminPanel interface with a blue header. A green progress bar at the top indicates 99.00% completion. Below the progress bar, there are settings for 'Не показывать завершённые' (checked) and 'Показать вспомогательные контейнеры' (unchecked). On the right, there are dropdowns for 'Объектов в строке' (set to 1) and 'Группировать' (set to 'Не группировать'). A list of containers is shown with columns for name, IP, and status. The containers listed are doc-01 (100.70.160.11), bind1 (172.20.4.129), bein1 (172.20.4.138), and becca1 (172.20.5.103). A tooltip for bein1 shows its description: 'Сервис для дублирования событий действий пользователей во внешние системы'. A blue play button icon is highlighted with a red box in the top right corner of the container list area. A 'Добавить' button is at the bottom.

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.

Настройки

Сети Доменные имена Хранилища Шардирование и репликация БД **Настройки компонентов** Интеграции Переменные окружения

Почтовый транспорт account.vkwm2.on-premise.ru af.vkwm2.on-premise.ru af.vkwm2st.on-premise.ru ampproxy.vkwm2st.on-premise.ru apf.vkwm2.on-premise.ru apf.vkwm2st.on-premise.ru

Политика изменения паролей пользователей as.vkwm2.on-premise.ru auth.vkwm2.on-premise.ru **becca.vkwm2.on-premise.ru** biz.vkwm2.on-premise.ru blobcloud.e.vkwm2.on-premise.ru bml.vkwm2.on-premise.ru

c.vkwm2.on-premise.ru calendar.vkwm2.on-premise.ru calendarmsg.vkwm2.on-premise.ru calendartouch.vkwm2.on-premise.ru calendarx.vkwm2.on-premise.ru

Настройки почты cloud.vkwm2.on-premise.ru cld-uploader.cloud.vkwm2.on-premise.ru cloclo.cloud.vkwm2.on-premise.ru cloclo.vkwm2st.on-premise.ru cloclo-upload.cloud.vkwm2.on-premise.ru

Настройки abf openapi.cloud.vkwm2.on-premise.ru pu.cloud.vkwm2.on-premise.ru sdc.cloud.vkwm2.on-premise.ru cloclo-stock.vkwm2st.on-premise.ru uploader.e.vkwm2.on-premise.ru

Ограничение доступа к доменам thumb.cloud.vkwm2.on-premise.ru cld-unzipper.vkwm2st.on-premise.ru corsapi.vkwm2st.on-premise.ru e.vkwm2.on-premise.ru filin.vkwm2.on-premise.ru

Система учёта действий пользователей img.vkwm2.on-premise.ru imgs.vkwm2.on-premise.ru o2.vkwm2.on-premise.ru portal.vkwm2.on-premise.ru proxy.vkwm2st.on-premise.ru hb.vkwm2st.on-premise.ru

swa.vkwm2.on-premise.ru tmpatt.vkwm2st.on-premise.ru webdav.cloud.vkwm2.on-premise.ru

http(s) прокси Домен для панели расширенного просмотра действий пользователей Отмена Сохранить

Ограничить доступ к домену

Режим запрета - запрещать следующим IP/подсетям

IP/Подсети 0.0.0.0/0 + Добавить

Комментарий all + Добавить

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

Автор: Груздев Никита

31 июля 2025 г.