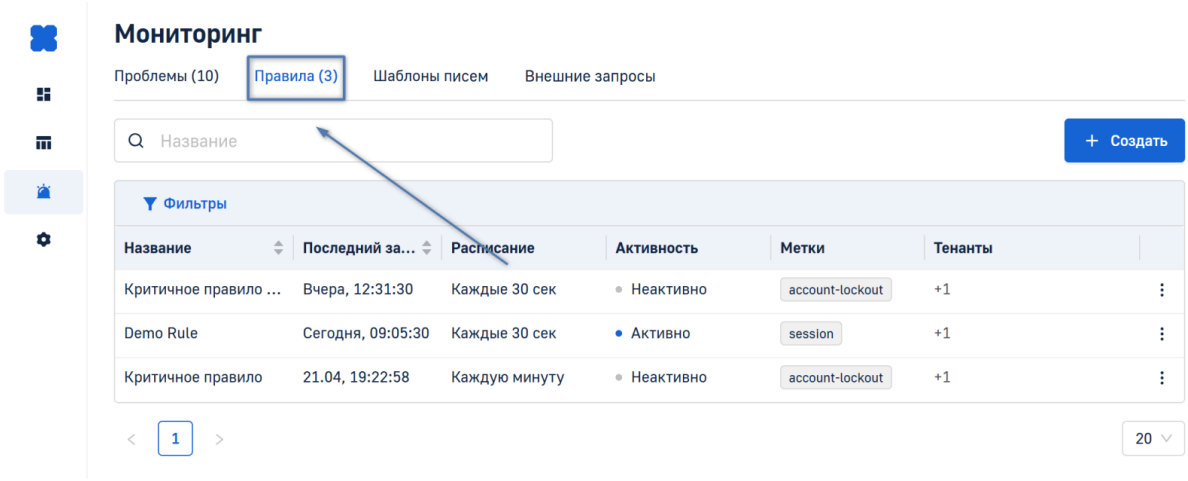
Управление правилами оповещений

В данной статье описано взаимодействие с правилами оповещений в Системе: как их добавить, просмотреть, найти, отредактировать, копировать, активировать/деактивировать и удалить.

Общие сведения

Система позволяет создавать и конфигурировать правила, по которым будут регистрироваться оповещения об определенных событиях.

Для управления правилами необходимо перейти на вкладку **Мониторинг → Правила**.



На вкладке **Правила** расположена таблица со списком всех существующих правил.

Таблица содержит следующие поля:

- **Название** — имя созданного правила;
- **Последний запуск** — дата последнего запуска правила;
- **Расписание** — периодичность запуска проверки событий по правилу;
- **Активность** — состояние активности правила:
  - **Активно** — система осуществляет проверку событий на соответствие условиям правила по расписанию;
  - **Деактивировано** — система не осуществляет проверку.
- **Метки** — метки для классификации правил и оповещений. Возможные значения:
  - **account-lockout**;
  - **asset**;
  - **database**;
  - **endpoint**;
  - **file**;
  - **session**;
  - **web**.
- **Тенанты** — тенанты базы данных, для которых будет срабатывать правило.

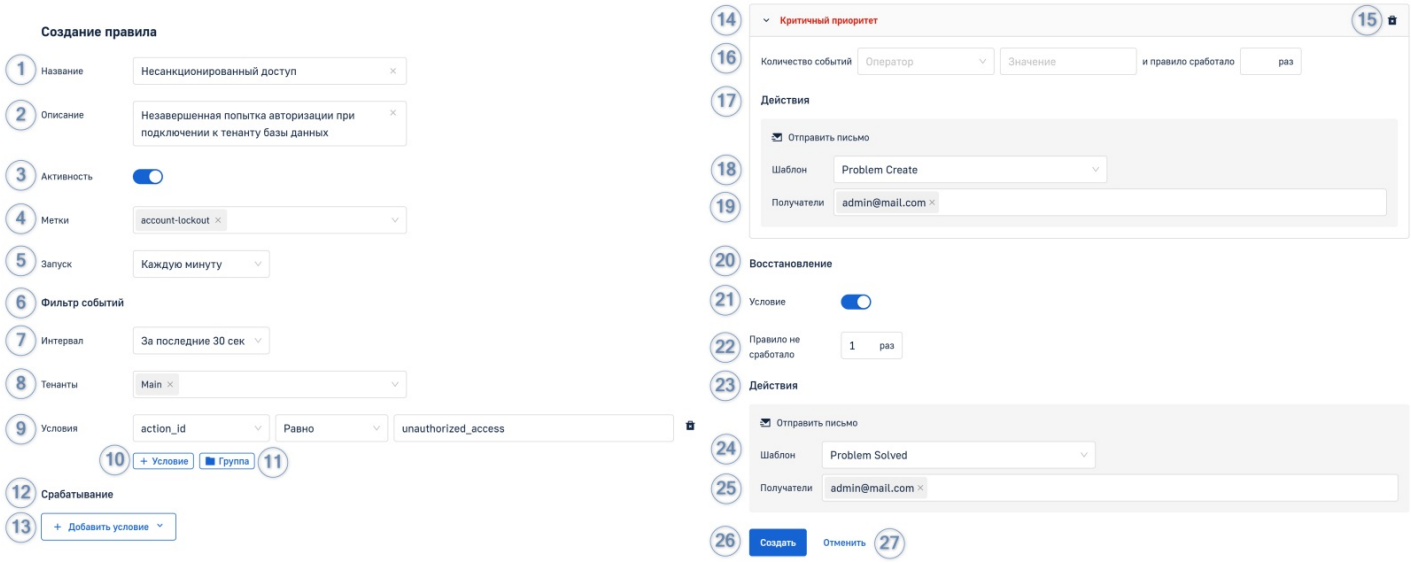
Управление таблицей

По умолчанию на странице отображается 20 записей, однако вы можете выбрать отображение 10, 20 и 50 записей на странице. Для этого нажмите на поле в правом верхнем углу списка и выберите в выпадающем списке необходимое количество для отображения.

Вы можете отсортировать таблицу по **названию** и **дате последнего запуска** правила в порядке возрастания или убывания с помощью значка  . По умолчанию все записи в таблице отображаются в порядке возрастания по дате создания правила.

Для переключения между страницами используйте блок в левом нижнем углу списка:

Добавление правила



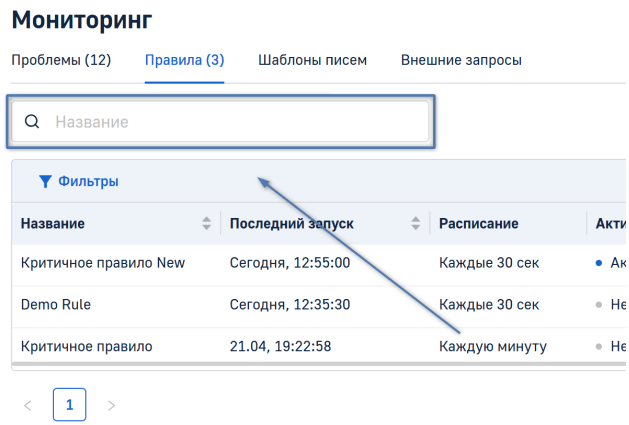
Для того, чтобы добавить новое правило, нажмите кнопку **Создать** в правом верхнем углу страницы и в выпадающем списке выберите **Создать**. При нажатии будет открыто окно со следующими параметрами:

1. **Название** — название правила, которое будет отображаться в списке правил, списке оповещений и самих оповещениях;
2. **Описание** — описание правила, которое будет отображаться в подробной информации об оповещении;
3. **Активность** — состояние активности правила:
   - **Активно** — система осуществляет проверку событий на соответствие условиям правила по расписанию;
   - **Деактивировано** — система не осуществляет проверку.
4. **Метки** — метки для классификации правил и оповещений. Возможные значения:
   - **account-lockout**;
   - **asset**;
   - **database**;
   - **endpoint**;
   - **file**;
   - **session**;
   - **web**.
5. **Запуск** — периодичность запуска проверки событий по правилу;
6. **Фильтр событий** — раздел, в котором задаются параметры выборки событий для проверки;
7. **Интервал** — интервал времени выборки событий для проверки;
8. **Тенанты** — тенанты, в которых будут проверяться события;
9. **Условия** — в данной строке вы можете выбрать поле, оператор и значение в событии, которые будут подпадать под проверку;
10. **Условие** — добавить условия попадания событий в выборку. Если вы добавили более одного условия, вы можете выбрать оператор для этих условий;
11. **Группа** — добавить группу условий попадания событий в выборку. Если вы добавили более одного условия, вы можете выбрать оператор для этих групп условий;
12. **Срабатывание** — раздел, в котором задаются приоритеты оповещений, условия их создания, а также действия, которые при этом совершит система;
13. **Добавить условие** — добавить условие срабатывания правила. При нажатии будет доступен выбор приоритета оповещения:
    - **Критичный**;
    - **Высокий**;
    - **Средний**;
    - **Низкий**;
    - **Информационный**.
14. **Поле условия** — в данном разделе вы можете задать параметры для срабатывания оповещения;
15. **Удалить условие** — нажмите на иконку, чтобы удалить условие для оповещения;
16. **Условия оповещения** — в данной строке вы можете задать количество событий и срабатываний правил для создания оповещения;
17. **Действия** — в данном разделе вы можете настроить действия, которые будут выполняться при создании оповещения. На данный момент доступна только отправка уведомления по электронной почте;
18. **Шаблон** — шаблон электронного письма, которое будет отправлено при создании оповещения;
19. **Получатели** — электронная почта получателей уведомления;
20. **Восстановление** — раздел, в котором задаются условия закрытия оповещения, а также действия, которые при этом совершит система;
21. **Условие** — данный параметр отвечает за активацию автоматического закрытия оповещения при соблюдении указанных ниже условий;
22. **Правило не сработало** — в данном поле вы можете указать количество раз подряд, когда правило не сработало и уязвимость можно считать закрытой;
23. **Действия** — в данном разделе вы можете настроить действия, которые будут выполняться при закрытии оповещения. На данный момент доступна только отправка уведомления по электронной почте;
24. **Шаблон** — шаблон электронного письма, которое будет отправлено при закрытии оповещения;
25. **Получатели** — электронная почта получателей уведомления;
26. **Создать** — нажмите кнопку, чтобы создать правило;
27. **Отменить** — нажмите кнопку, чтобы отменить изменения.

Правило может иметь не более пяти условий срабатывания — по одному условию на каждый уровень приоритета.

Поиск и фильтрация правил

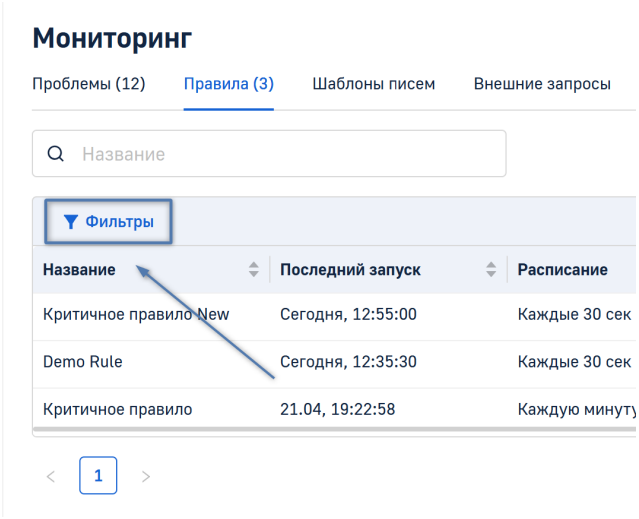
Для того, чтобы найти определенное правило в списке, нажмите на форму поиска в левом верхнем углу таблицы и введите ключевое слово.



В качестве ключевых слов для поиска могут быть использованы:

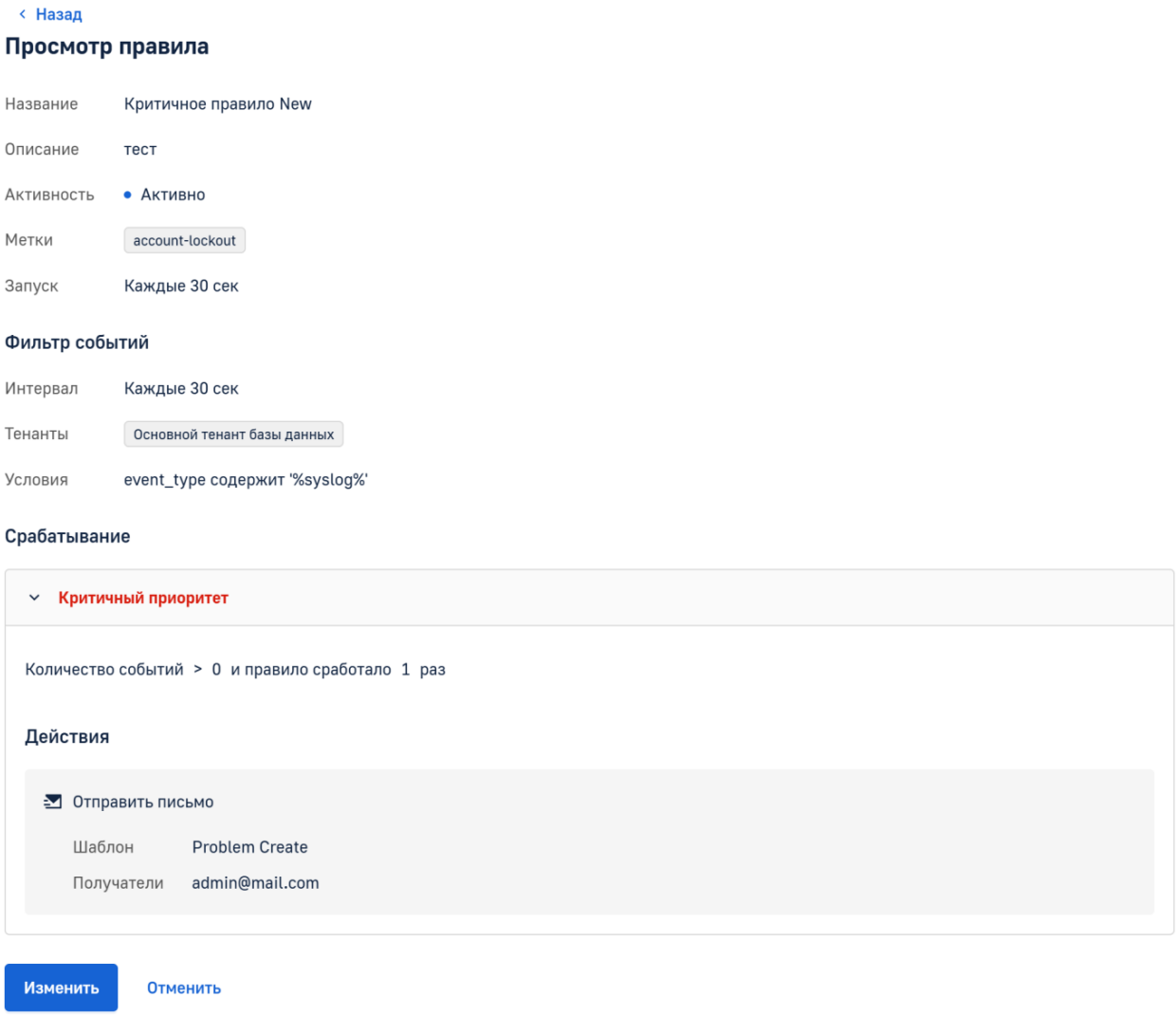
- Имя правила;
- Метки.

Вы также можете отфильтровать список правил по их статусу, тенантам и меткам. Для этого нажмите на иконку фильтра и выберите параметры для фильтрации списка.



Просмотр правил

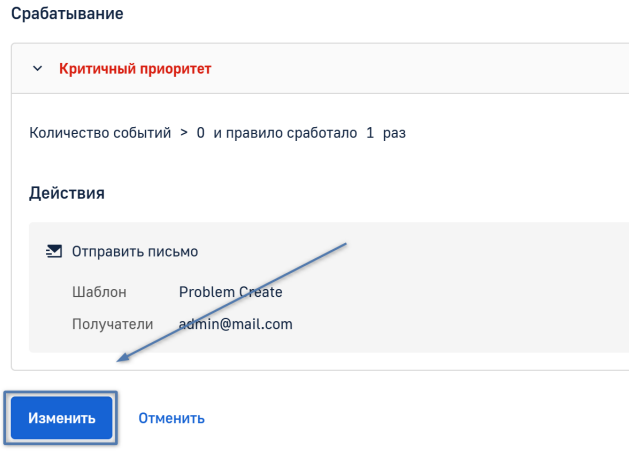
Для того, чтобы просмотреть подробную информацию о параметрах правила, нажмите на него в списке, после чего откроется страница со всеми доступными данными.



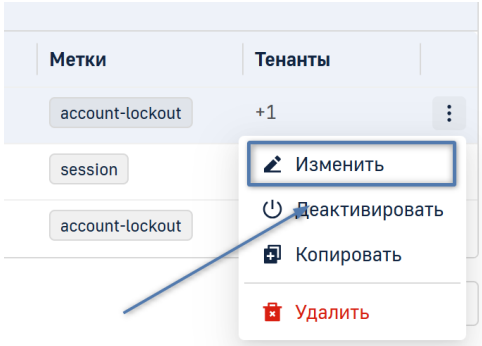
Редактирование правила

Для того, чтобы отредактировать ранее добавленное правило:

- Нажмите на правило в списке, после чего нажмите кнопку **Изменить** в левом нижнем углу открывшейся страницы;



- Нажмите на три точки справа от правила в списке, после чего в выпадающем списке выберите **Изменить**.



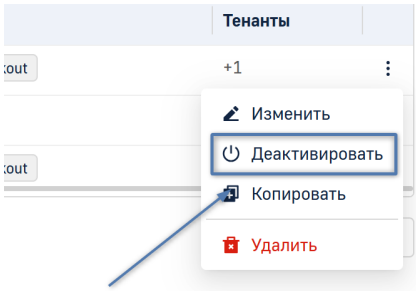
При нажатии будет открыта страница редактирования правила.

Чтобы сохранить изменения, нажмите кнопку **Сохранить** в левом нижнем углу страницы. После этого вы будете автоматически перенаправлены на страницу со списком всех добавленных правил.

Нажмите кнопку **Отменить**, чтобы сбросить все внесенные изменения.

Деактивация/активация правила

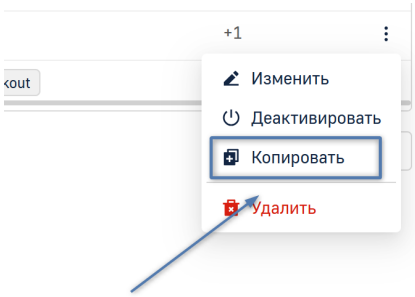
Деактивация правила позволяет остановить работу правила в Системе, не удаляя его полностью. Для того, чтобы деактивировать правило, нажмите на три точки справа от правила в списке, после чего выберите в выпадающем списке **Деактивировать**.



Для активации правила нажмите на три точки справа от правила в списке и выберите**Активировать**.

Копирование правила

Копирование позволяет позволяет создать дубликат правила для последующего редактирования. Для того, чтобы скопировать правило, нажмите на три точки справа от правила в списке, после чего выберите в выпадающем списке **Копировать**.



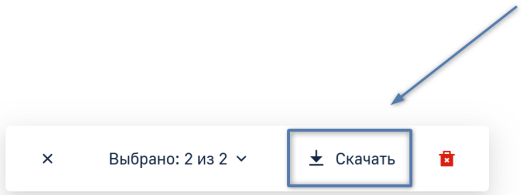
После этого откроется страница редактирования скопированного правила. Для сохранения копии нажмите **Изменить** после внесения всех изменений.

Экспорт/импорт правил

При необходимости вы можете экспортировать и импортировать сконфигурированные правила оповещений. Это позволяет вам создать резервную копию правила, которую вы позже можете импортировать в любую инсталляцию.

Экспорт правил

Для того, чтобы выполнить экспорт одного или нескольких правил, отметьте необходимые для экспорта правила. Чтобы выбрать все правила в списке, нажмите на селектор в шапке таблицы. После этого в появившемся всплывающем окне нажмите **Скачать**.

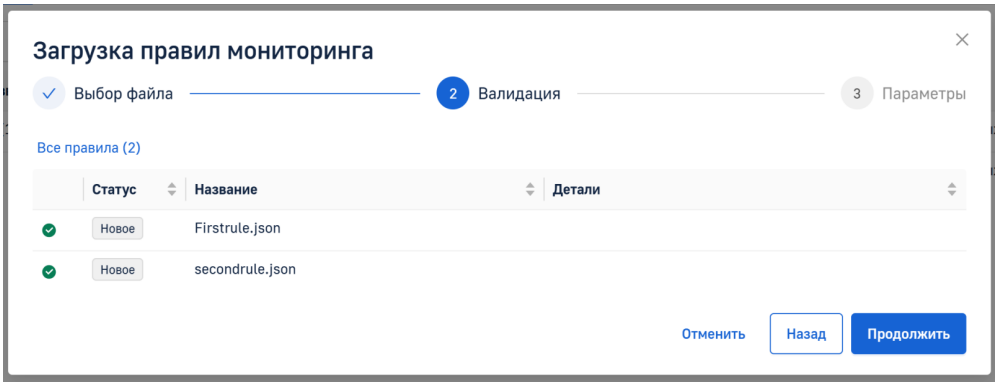


При экспорте одного правила, на АРМ, с которого вы подключились к веб-интерфейсу будет загружен файл**имя_правила.json**. При экспорте нескольких правил, на АРМ, с которого вы подключились к веб-интерфейсу будет загружен ZIP-архив со всеми файлами правил.

Импорт правил

Для того, чтобы импортировать правила в Систему, нажмите **Создать** в правом верхнем углу страницы и в выпадающем списке выберите **Загрузить**. После этого откроется окно, в котором вы сможете выполнить загрузку необходимых правил. Вы можете загрузить одно правило в формате **.json** или сразу несколько в ZIP-архиве. Максимальный допустимый размер ZIP-архива для одной загрузки составляет 1 ГБ.

После того, как вы загрузили правила, нажмите **Продолжить**. Вам будет предложено проверить загружаемые правила в окне валидации.

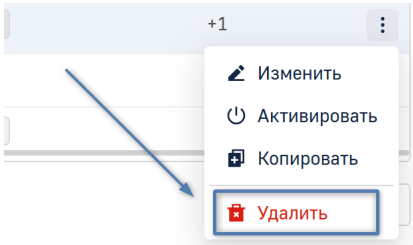


В данном окне вы можете увидеть, удалось ли загрузить правила, являются данные правила новыми или копиями уже существующих в Системе, а также дополнительную информацию, в случае, если правило не удалось загрузить. После проверки нажмите **Продолжить**.

На финальном этапе загрузки вам будет предложено два варианта: импортировать все загруженные правила или только новые (не являющиеся копиями). Для завершения процедуры импорта нажмите **Загрузить**. После этого таблица со списком правил обновится и в ней отобразятся импортированные правила.

Удаление правила

Для того, чтобы удалить правило, нажмите на три точки справа от правила в списке, после чего выберите в выпадающем списке**Удалить**.



После этого, во всплывающем окне нажмите кнопку **Да, удалить** для подтверждения удаления. Если вы передумали удалять правило, нажмите кнопку **Отменить**.

Для того, чтобы удалить несколько правил, отметьте необходимые для удаления правила. Чтобы выбрать все правила в списке, нажмите на селектор в шапке таблицы. После этого в появившемся всплывающем окне нажмите на иконку удаления.

ID статьи: 1372
Последнее обновление: 15 авг., 2025
Обновлено от: Егоров В.
Ревизия: 1
База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.6.0 -> LogIQ. Руководство администратора -> Мониторинг и оповещения -> Управление правилами оповещений

https://docs.axel.pro/entry/1372/