

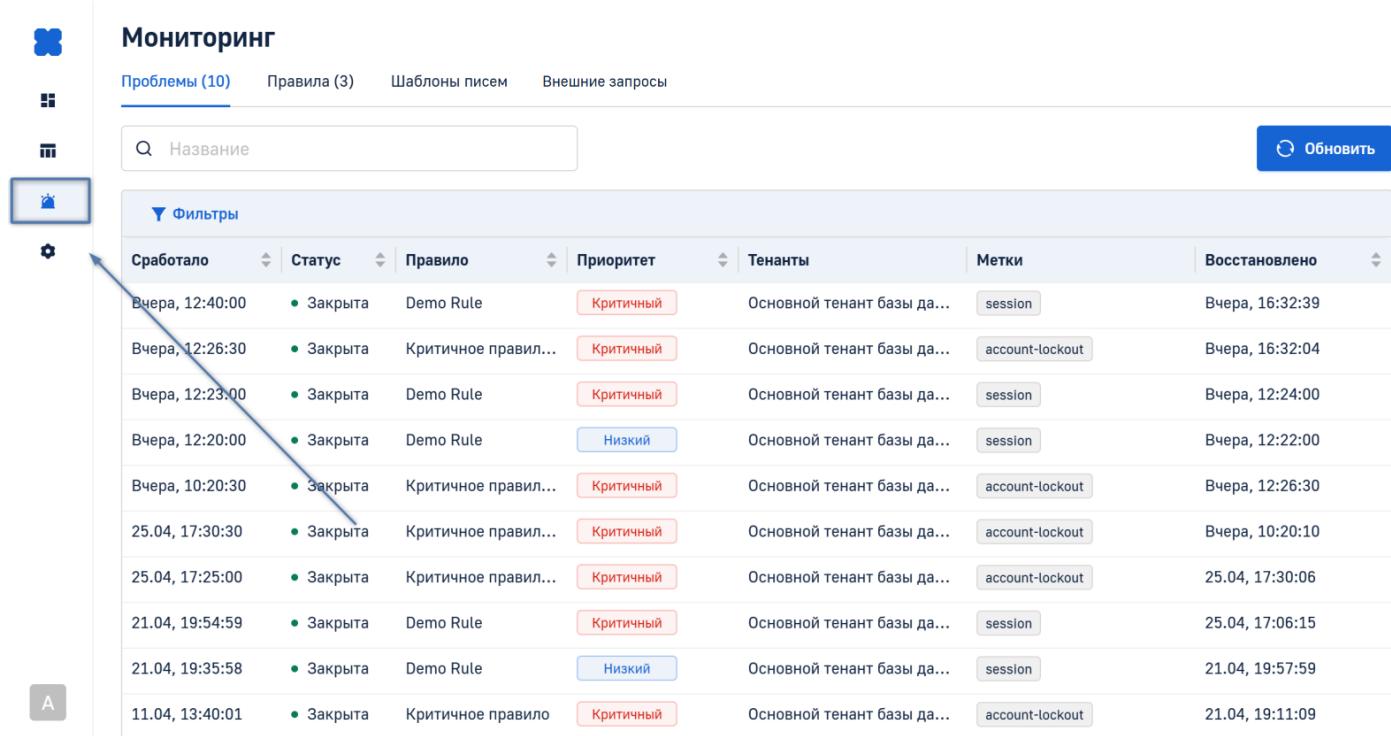
# Работа с оповещениями

В данной статье описано взаимодействие с оповещениями о проблемах, обнаруженных Системой: как их просмотреть, исследовать, найти, отсортировать и изменить статус.

## Общие сведения

Система создает оповещения при получении последовательности событий, которые удовлетворяют заданным правилам оповещения. Каждому оповещению присваивается приоритет в зависимости от приоритета условия срабатывания в правиле оповещения.

Для просмотра оповещений необходимо перейти на вкладку **Мониторинг → Проблемы**.



Сработало	Статус	Правило	Приоритет	Тенанты	Метки	Восстановлено
Вчера, 12:40:00	• Закрыта	Demo Rule	Критичный	Основной тенант базы да...	session	Вчера, 16:32:39
Вчера, 12:26:30	• Закрыта	Критичное правил...	Критичный	Основной тенант базы да...	account-lockout	Вчера, 16:32:04
Вчера, 12:23:00	• Закрыта	Demo Rule	Критичный	Основной тенант базы да...	session	Вчера, 12:24:00
Вчера, 12:20:00	• Закрыта	Demo Rule	Низкий	Основной тенант базы да...	session	Вчера, 12:22:00
Вчера, 10:20:30	• Закрыта	Критичное правил...	Критичный	Основной тенант базы да...	account-lockout	Вчера, 12:26:30
25.04, 17:30:30	• Закрыта	Критичное правил...	Критичный	Основной тенант базы да...	account-lockout	Вчера, 10:20:10
25.04, 17:25:00	• Закрыта	Критичное правил...	Критичный	Основной тенант базы да...	account-lockout	25.04, 17:30:06
21.04, 19:54:59	• Закрыта	Demo Rule	Критичный	Основной тенант базы да...	session	25.04, 17:06:15
21.04, 19:35:58	• Закрыта	Demo Rule	Низкий	Основной тенант базы да...	session	21.04, 19:57:59
11.04, 13:40:01	• Закрыта	Критичное правило	Критичный	Основной тенант базы да...	account-lockout	21.04, 19:11:09

Во вкладке **Проблемы** расположена таблица со списком зарегистрированных оповещений.

Таблица содержит следующие поля:

- **Сработало** — дата и время срабатывания правила;
- **Статус** — статус проблемы:
  - **Открыта** — проблема является актуальной и еще не сработало условие ее закрытия;
  - **Закрыта** — проблема закрыта автоматически или вручную.
- **Правило** — имя правила, по которому сработало оповещение;
- **Приоритет** — приоритет оповещения, зависящий от значения, установленного в правиле. Может принимать следующие значения:
  - **Критичный**;
  - **Высокий**;
  - **Средний**;
  - **Низкий**;
  - **Информационный**.
- **Тенанты** — тенанты баз данных для которых сработало оповещение;
- **Метки** — метки правила, по которому сработало оповещение;
- **Восстановлено** — дата и время перехода оповещения в статус **Закрыта**.

## 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 любой колонке в порядке алфавитного возрастания или убывания с помощью значка . По умолчанию все записи в таблице отображаются в порядке возрастания по колонке **Сработало**.

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

## Поиск и фильтрация оповещений

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

Проблемы (10) Правила (3) Шаблоны писем Внешние запросы

Фильтры				
Сработало	Статус	Правило	Приоритет	
Вчера, 12:40:00	● Закрыта	Demo Rule	Критичный	
Вчера, 12:26:30	● Закрыта	Критичное правил...	Критичный	

В качестве ключевых слов для поиска могут быть использованы:

- Имя правила, по которому сработало оповещение;
- Метка правила, по которому сработало оповещение.

Вы также можете отфильтровать список оповещений по статусу, приоритету, тенанту, меткам и правилам. Для этого нажмите на иконку фильтра и выберите параметры для фильтрации списка.

Проблемы (10) Правила (3) Шаблоны писем Внешние запросы

Фильтры				
Сработало	Статус	Правило	Приоритет	
Вчера, 12:40:00	● Закрыта	Demo Rule	Критичный	
Вчера, 12:26:30	● Закрыта	Критичное правил...	Критичный	
Вчера, 12:23:00	● Закрыта	Demo Rule	Критичный	

## Просмотр оповещения

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

[← Назад](#)

## Проблема Критичное правило

[Закрыть](#)

Статус • Открыта Приоритет Критичный

[Детали](#) [События](#) [История срабатываний](#)

Правило Критичное правило Тенанты Основной тенант базы данных  
Сработало 11.04, 13:40:01 Метки account-lockout  
Восстановлено – Описание Неудачная попытка подключения к тенанту базы данных

### Срабатывание

Если count > 0 Где action\_name содержит '%action%' и сработало 1 раз То Отправить письмо: Problem Create Кому: admin@mail.com

### Восстановление

Если не сработало 1 раз То Отправить письмо: Problem Solved admin@mail.com

На данной странице вы можете выполнить следующие действия:

- Просмотреть подробное описание проблемы;
- Просмотреть события связанные с проблемой;
- Просмотреть историю срабатывания оповещений по заданному правилу;
- Изменить статус оповещения.

## Просмотр подробного описания проблемы

При открытии оповещения будет автоматически открыта вкладка **Детали**, на которой вы можете просмотреть подробные данные об этом оповещении:

- Правило, вызвавшее данное оповещение;
- Дата срабатывания правила;
- Дата закрытия проблемы (если проблема находится в статусе **Закрыта**);
- Тенант, для которого создано оповещение;
- Метка правила, вызвавшего оповещение;
- Описание правила, вызвавшего оповещение;
- Условия срабатывания правила;
- Условия автоматического закрытия проблемы, вызвавшей оповещение.

## Просмотр связанных событий

Для того, чтобы просмотреть все события, связанные с данным оповещением, перейдите на вкладку **События**.

[← Назад](#)

## Проблема Критичное правило

[Возобновить](#)Статус • Закрыта    Приоритет Критичный

Детали

**События**

История срабатываний

[Открыть в таблице событий](#)

timestamp

message

Вчера, 12:26:01

pfconnector-server-docker-wrappet=2025-04-29T05:26:00+0000 lvl=dbug msg="Resource is not valid anymore. Was loaded at 2025-04-29 05:25:45.287280781 +0000 UTC m=+502386.892675930" pid=1

uuid: c1133216-f2a7-40bb-85b3-e89951e9f...    event\_type: syslog    action\_id: 3  
 action\_name: system    key: Informational    registered\_process: null    msgid: 6    id: null  
 category\_generic: null    category\_high: null    category\_low: null    assigned\_src\_host: null  
 assigned\_src\_ip: null    assigned\_src\_port: null    src\_asset: null    src\_fqdn: null  
 src\_geo\_asn: null    +161

Вчера, 12:26:01

pfconnector-server-docker-wrappet=2025-04-29T05:26:00+0000 lvl=dbug msg="Resource is not valid anymore. Was loaded at 0001-01-01 00:00:00 +0000 UTC" pid=1

uuid: 56d00f1f-21f0-4b03-871b-378c457a1...    event\_type: syslog    action\_id: 3  
 action\_name: system    key: Informational    registered\_process: null    msgid: 6    id: null  
 category\_generic: null    category\_high: null    category\_low: null    assigned\_src\_host: null  
 assigned\_src\_ip: null    assigned\_src\_port: null    src\_asset: null    src\_fqdn: null

На данной вкладке вы можете просмотреть дату регистрации события и его содержимое.

Для того, чтобы просмотреть данный список в таблице событий, нажмите **Открыть в таблице событий** в правом верхнем углу. После этого откроется страница **События**, на которой будет применен соответствующий SQL-запрос.

## Просмотр истории срабатывания и изменения статуса оповещения

Для того, чтобы просмотреть историю изменения статуса оповещения, перейдите на вкладку **История срабатываний**.

[← Назад](#)

## Проблема Критичное правило

[Возобновить](#)Статус • Закрыта    Приоритет Критичный

Детали

**События****История срабатываний**

Дата	Статус	Приоритет	Источник	Интервал поиска	Количество
Вчера, 16:32:04	Закрыт	Критичный	admin	—	—
Вчера, 12:26:30	Открыт	Критичный	Система	29.04.25, 12:26:00 - 29.04.25, 12:26:30	783

&lt; 1 &gt;

10 ▾

На данной вкладке вы можете просмотреть следующие данные:

- Дата срабатывания правила или изменения статуса;
- Статус проблемы;
- Приоритет;
- Источник (пользователь, выполнивший действие, либо раздел системы);
- Интервал поиска событий для срабатывания правила;
- Количество событий, попадающих под данное правило.

## Изменение статуса оповещения

Для того, чтобы вручную изменить статус оповещения нажмите **Возобновить** или **Закрыть** в правом верхнем углу страницы:

◀ Назад  
**Проблема Критичное правило**

Статус • Открыта Приоритет Критичный

Детали События История срабатываний

Закрыть

◀ Назад  
**Проблема Критичное правило**

Статус • Закрыта Приоритет Критичный

Детали События История срабатываний

Возобновить

ID статьи: 1374

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 -> Работа с оповещениями

<https://docs.axel.pro/entry/1374/>