

Синхронизация правил нормализации

Данные о последней успешной синхронизации правил нормализации в SIEM и правила нормализации в системе логирования отображаются на странице **Настройки → Компоненты системы → Правила нормализации**.

Правила корреляции

Правила нормализации

▶ Запустить синхронизацию

Последний запуск: Сегодня, 04:00:45 | Статус: Синхронизация завершена

ID брокера	ID SIEM	Изменено	Статус	Описание
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:34	Успешно	
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:34	Успешно	
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:34	Успешно	
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:34	Успешно	
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:34	Успешно	
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:34	Успешно	
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:34	Ошибка	Возникла с
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:33	Ошибка	Возникла с
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:33	Ошибка	Возникла с
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:33	Ошибка	Возникла с
siem_normalization_rules.rb	Базовый пакет/normalizat...	25.12.2024, 00:54:33	Ошибка	Возникла с

Выполнение синхронизации правил нормализации происходит автоматически раз в сутки, однако администратор может запустить синхронизацию в ручном режиме.

Для ручного запуска синхронизации необходимо нажать на кнопку **Запустить синхронизацию**. Поле **Последний запуск** обновится и будет отображаться таблица результатов процесса синхронизации.

Таблица содержит следующие поля:

- **ID брокера** — идентификатор брокера, в котором хранится правило;
- **ID SIEM** — имя события, которому соответствует правило в SIEM;
- **Изменено** — дата последнего изменения правила;
- **Статус** — статус правила нормализации. Может принимать следующие значения:
 - **Успешно** — правило нормализации успешно загружено;
 - **Ошибка** — не удалось загрузить правило нормализации.
- **Описание** — описание ошибки из-за которой не удалось загрузить правило нормализации.

По умолчанию, на странице отображается до 20 записей. Для того, чтобы увеличить число отображаемых записей на странице, нажмите на количество записей в правом нижнем углу страницы и выберите одно из значений:

Успешно

Успешно

Успешно

10

20

50

20 ▾

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.

Правила корреляции

Правила нормализации

Последний запуск Сегодня, 04:00:45 Статус Синхронизации

ID или описание		🔍	🔼 Фильтры
ID брокера	ID SIEM		
siem_normalization_rules.rb	Базовый пакет/normalizat...		

В качестве ключевых слов для поиска могут быть использованы:

- ID брокера;
- ID SIEM;
- Описание ошибки.

Вы также можете отфильтровать список правил по их статусу и дате изменения. Для этого нажмите на иконку фильтра и выберите параметр для фильтрации списка.

Правила корреляции

Правила нормализации

Последний запуск Сегодня, 04:00:45 Статус Синхронизация за

ID или описание		🔍	🔼 Фильтры
ID брокера	ID SIEM		
siem_normalization_rules.rb	Базовый пакет/normalizat...		
siem_normalization_rules.rb	Базовый пакет/normalizat...		

Статус: Все >

Изменено: Не изменено

ID статьи: 429

Последнее обновление: 29 апр., 2025

Обновлено от: Егоров В.

Ревизия: 4

База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.4.0 -> LogIQ. Руководство администратора -> Синхронизация компонентов системы -> Синхронизация правил нормализации

<https://docs.axel.pro/entry/429/>