

Общие сведения

В данной статье приведены общие сведения о Системе.

Назначение Системы

Система предназначена для сбора, обработки, передачи, а также долговременного хранения и анализа Событий.

Ключевые возможности Системы

Система обеспечивает реализацию следующего ключевого функционала:

- Сбор Событий из различных источников, таких как операционные системы, сетевые устройства, базы данных и т.д.;
- Нормализация, агрегация, обогащение и фильтрация Событий;
- Эффективное долговременное хранение большого количества Событий с высоким коэффициентом сжатия;
- Интеграция с внешними системами, такими как системы класса SIEM, IRP и т.д.;
- Автоматическая конвертация правил нормализации и корреляции из MP SIEM;
- Формирование запросов и представление выборки Событий в виде таблицы;
- Построение графиков для анализа и визуализации Событий с гибкой настройкой отображения;
- Формирование и отправка оповещений по срабатыванию настраиваемых триггеров.

Требования к рабочему месту Разработчика

На рабочей станции Разработчика должны быть установлены:

1. Дистрибутив ОС;
2. Веб-браузер для работы с Системой.

Требования к квалификации Разработчика

Разработчик должен обладать следующими навыками:

- знание языка SQL;
- знание особенностей написания SQL-запросов в СУБД **ClickHouse**;
- знание одного из языков для работы с конфигурационными файлами:
 - Ruby;
 - Logstash (JRuby).
- навыки работы в дистрибутивах ОС рабочей станции и сервера;
- навыки работы с утилитами **bash** и **docker**.

Требования к серверу Системы

Сервер, где будет располагаться Система, должен работать по управлению ОС Astra Linux Special Edition версии не ниже 1.7.5.

Также должен быть настроен доступ к сети и к репозиторию Системы.

ID статьи: 215

Последнее обновление: 2 апр., 2025

Обновлено от: Егоров В.

Ревизия: 3

База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.3.0 -> LogIQ. Руководство разработчика -> Введение -> Общие сведения

<https://docs.axel.pro/entry/215/>