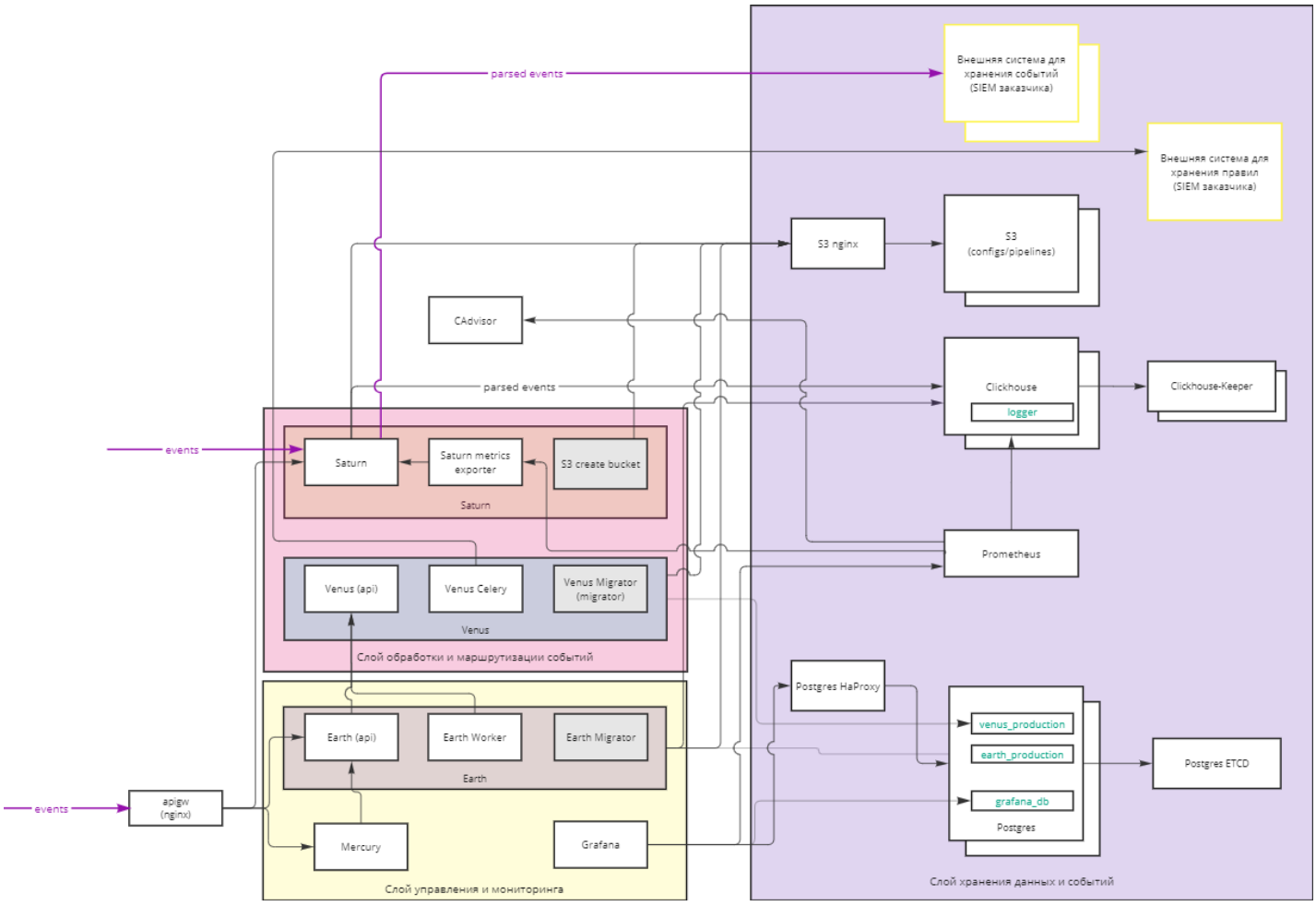
Логикор. Архитектура программного обеспечения

Общие сведения

ПО Логикор представляет собой систему долговременного хранения и фильтрации событий информационной безопасности (далее СДХ). Основное предназначение системы — получение, обработка, сохранение и передача событий информационной безопасности. Далее будет рассмотрена архитектура решения.



В архитектуре Логикор существует условное разделение на 3 основных слоя:

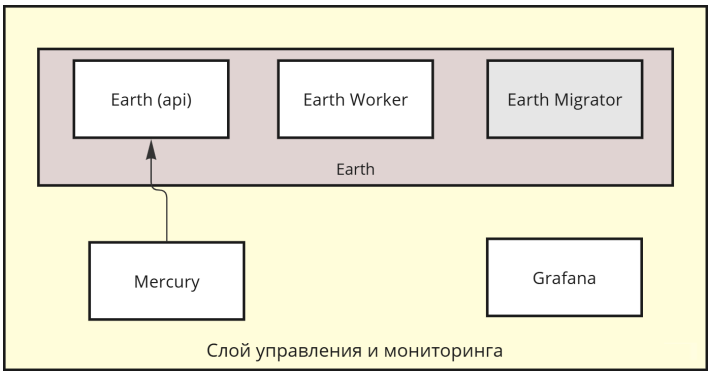
- Слой управления и мониторинга;
- Слой обработки и маршрутизации событий;
- Слой хранения данных и событий.

Глобально, система работает следующим образом:

1. Данные поступают в шлюз для доступа к сервисам, который их направляет в блок **Logstash** слоя обработки и маршрутизации событий.
2. В данном блоке события обрабатываются, после чего, по умолчанию, они отправляются в компонент **ClickHouse** слоя хранения данных и событий.
3. Параллельно события, отфильтрованные по правилам, полученным из блока **Venus**, отправляются во внешние системы хранения событий (SIEM заказчика).

Рассмотрим каждый из слоев более подробно.

Слой управления и мониторинга

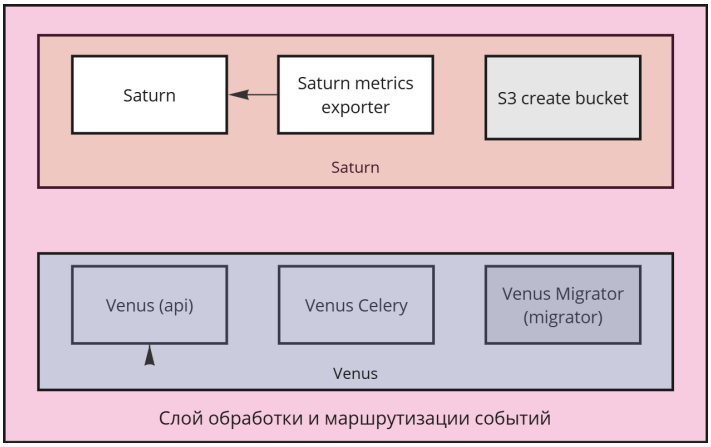


В слое управления и мониторинга производится конфигурация правил обработки и фильтрации данных, а также отображение метрик, передаваемых отдельными компонентами системы. Для управления и мониторинга используется веб-интерфейс, по умолчанию доступный по порту **5555**. Данный слой состоит из следующих блоков и компонентов:

- **Mercury:** данный компонент отвечает за внешнюю оболочку (Frontend) веб-интерфейса и передаёт необходимые команды в блок **Earth**;
- **Earth:** данный блок отвечает за функционирование веб-интерфейса (Backend) и общую конфигурацию системы. Блок **Earth** включает следующие компоненты:
  - **Earth (API):** данный компонент является REST API, используемым для функционирования компонента **Mercury** (веб-интерфейса);
  - **Earth Worker:** данный компонент отвечает за постановку задач по расписанию, необходимых для функционирования систем. Задачи передаются в компонент **Venus (API)** блока **Venus** в слое обработки и маршрутизации событий;
  - **Earth Migrator:** данный компонент отвечает за первичное заполнение базы данных **earth_production** кластера **Postgres** в слое хранения данных и событий (обновление схемы данных, заполнение БД предустановленными значениями). **Earth Migrator** активируется только при первом запуске СДХ.
- **Grafana:** данный компонент отвечает за отображение в реальном времени отслеживаемых внутренних метрик СДХ (таких как загруженность компонентов по

CPU/RAM/HDD, нагрузка и метрики компонентов **Logstash**, а также метрики кластера **ClickHouse**). Веб-интерфейс мониторинга доступен по порту **3000**.

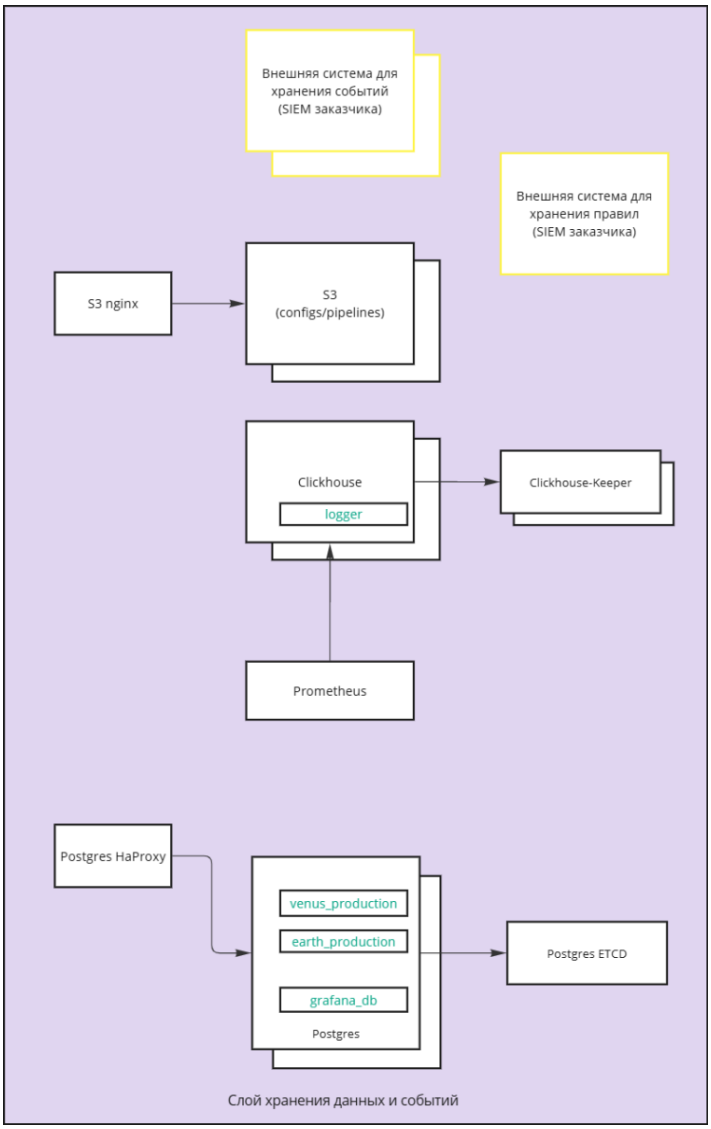
Слой обработки и маршрутизации событий



В слое обработки и маршрутизации производится получение, обработка, фильтрация и маршрутизация данных, поступающих из шлюза доступа к сервисам, а также конвертация правил корреляции и нормализации. Данный слой состоит из следующих блоков:

- **Venus:** данный блок отвечает за конвертацию правил корреляции и нормализации из формата в котором они хранятся в SIEM заказчика, в формат, понятный компоненту **Saturn**. Блок **Venus** включает следующие компоненты:
  - **Venus (API):** данный компонент является REST API, используемым для функционирования блока **Venus** (доступ к данным, постановка задач);
  - **Venus Celery:** данный компонент отвечает за получение правил корреляции и нормализации, их конвертацию в синтаксис конфигурации блока **Logstash**, с последующим сохранением этих правил в общую файловую папку (компонент **S3** в слое хранения данных и событий);
  - **Venus Migrator:** данный компонент отвечает за первичное заполнение базы данных **venus_production** кластера **Postgres** в слое хранения данных и событий (обновление схемы данных, заполнение БД предустановленными значениями). **Venus Migrator** активируется только при первом запуске СДХ.
- **Saturn:** данный блок производит сбор, преобразование, сохранение и маршрутизацию полученных данных. В блока **Saturn** находится решение с открытым исходным кодом **Logstash**, отвечающее непосредственно за получение, обработку, агрегацию, фильтрацию и маршрутизацию данных. События обрабатываемые в рамках этого блока, сохраняются в компоненте **ClickHouse** слоя хранения данных и событий и, при соответствующей настройке, могут быть направлены на внешние системы хранения данных, такие как **RabbitMQ**, **Kafka**, Агенты SIEM-систем и т.д. В рамках маршрутизации и фильтрации данных, отправляемых во внешние системы, могут быть использованы правила корреляции и нормализации, определенные во внешней SIEM-системе. Данный блок включает следующие компоненты:
  - **Saturn:** данный компонент управляет сбором, обработкой, фильтрацией, сохранением и маршрутизацией данных в системе;
  - **Saturn metrics exporter:** данный компонент отвечает за сбор статистики работы компонента **Saturn**, с последующим сохранением этих метрик в БД **Prometheus**;
  - **S3 create bucket:** данный компонент за первичное заполнение компонента **S3** конфигурацией по умолчанию. После того, как общая файловая папка (компонент **S3** в слое хранения данных и событий) создана и в нее загружена конфигурация по умолчанию, компонент перестает работать.

Слой хранения данных и событий



В слое хранения данных и событий производится хранение и передача данных, конфигураций, правил и событий в системе. Данный слой состоит из следующих блоков и компонентов:

- **Postgres:** данный блок представлен объектно-реляционной системой управления базами данных с открытым исходным кодом (ОРСУБД) PostgreSQL, которая распространяется под лицензией PostgreSQL License. Данный блок обеспечивает высокую производительность, надёжность и широкий спектр возможностей и используется для хранения служебной информации СДХ.
  - **Postgres:** данный компонент отвечает за хранение информации о пользовательском интерфейсе. Компонент **Postgres** обычно представляет отказоустойчивый кластер из трех и более узлов;
  - **Postgres HaProxy:** данный компонент отвечает за распределение данных между узлами кластера **Postgres**;
  - **Postgres ETCD:** данный компонент отвечает за определение мастер-узла и ведомых узлов в кластере **Postgres**, хранение этих данных и определение кворума для отказоустойчивости кластера;
- **Prometheus:** данный компонент отвечает за мониторинг и сбор метрик, который используется для отслеживания и анализа производительности приложений и инфраструктуры. **Prometheus** собирает данные с помощью считывания временных рядов, которые затем используются для генерации предупреждений и оповещений, а также для построения графиков и дашбордов;
- **ClickHouse:** данный компонент представлен бесплатной системой управления базами данных с открытым исходным кодом, которая была разработана компанией Яндекс. Она предназначена для быстрого анализа больших наборов данных в режиме реального времени и поддерживает как простые запросы, так и сложные аналитические запросы. В Логикор данная система отвечает за хранение всех событий, поступивших в блок Logstash в слое обработки и маршрутизации событий;
- **ClickHouse-Keeper:** данный компонент отвечает за сборку кластера **ClickHouse**, управление хранением данных, отказоустойчивость кластера **ClickHouse**;
- **S3:** данный компонент отвечает за хранение конфигураций и правил корреляции нормализации, используемых в слое обработки и маршрутизации событий;
- **S3 nginx:** данный компонент является шлюзом для распределения данных из компонента S3.

Для обеспечения отказоустойчивого развертывания СДХ рекомендуется использовать сервисы HaProxy, KeepAliveD или VRRP. Подробное описание доступно в руководстве по развертыванию кластера.

Вспомогательные компоненты

В СДХ Логикор интегрирован вспомогательный компонент **CAdvisor**. Это инструмент для мониторинга ресурсов контейнеров Docker. Он собирает информацию о использовании CPU, памяти, сети и диска контейнерами Docker и передаёт эти метрики в компонент **Grafana** слоя управления и мониторинга. **CAdvisor** может быть использован для обнаружения проблем с производительностью, оптимизации использования ресурсов и диагностики проблем с контейнерами.

ID статьи: 134
Последнее обновление: 20 мар., 2026
Обновлено от: Егоров В.
Ревизия: 9
База знаний Логикор -> Документация -> Логикор. Архитектура программного обеспечения
https://docs.axel.pro/entry/134/