2023

АО «АМТ-ГРУП»

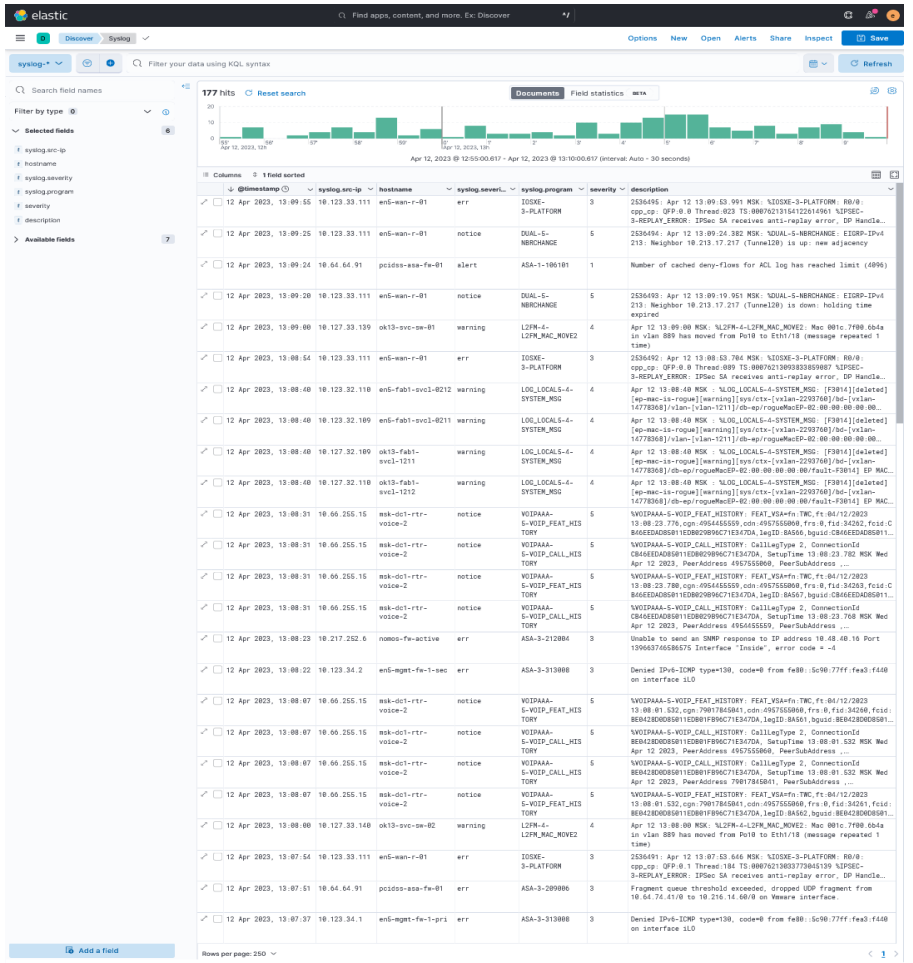
Система сбора логов на базе Elastic Stack

Назначение и преимущества системы

Система предназначена для централизованного сбора, хранения и анализа логов

Преимущества:

- Поддержка множества различных источников данных
- Обработка получаемых данных в удобный для работы формат «на лету»
- Быстрый полнотекстовый поиск интересующих событий и метрик
- Развитый функционал визуализации и анализа
- Распределение данных и отказоустойчивость



AMT GROUP

Основные функции системы

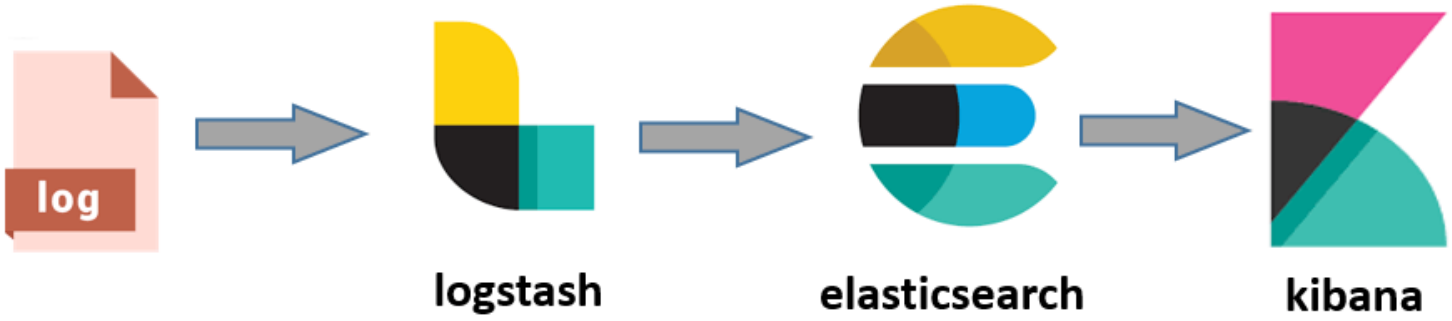
- Массовый, потоковый и непрерывный сбор логов и метрик с оборудования, систем и приложений заказчика
- Возможность предобработки получаемых сообщений в соответствии с настроенными шаблонами
- Пересылка исходных или предобработанных сообщений сторонним коллекторам данных
- Управление хранением и приоритизация доступа к собранным данным
- Поиск и гибкая фильтрация по массиву собранных данных
- Возможность создания интерактивных графиков и диаграмм
- Поддержка кластерной конфигурации для повышения производительности и отказоустойчивости

AMT GROUP

Основные компоненты системы

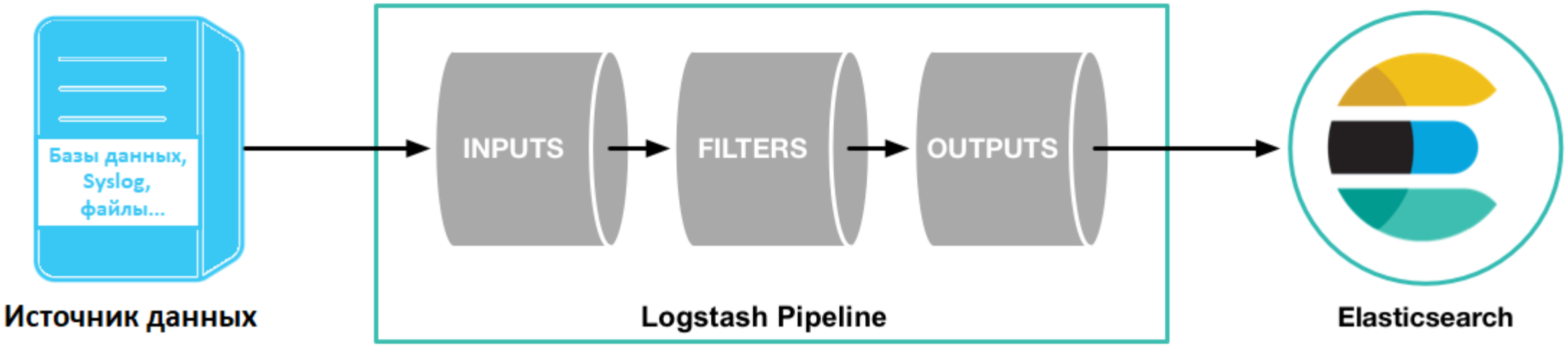
Предлагаемая нами система сбора и работы с логами базируется на решении **Elastic Stack**, которое включает в себя три основных компонента:

- **Logstash** – утилита сбора и обработки исходных данных
- **Elasticsearch** – поисковая система, обеспечивающая хранение проиндексированных данных и доступ к ним
- **Kibana** – средство визуализации и анализа собранных данных



Основные компоненты системы

Logstash — инструмент в составе Elastic Stack, который отвечает за первичное получение сообщений от их источников и поддерживает множество различных типов данных. Получаемые сообщения можно фильтровать, менять формат данных содержимого, а также перенаправлять в другие системы. Обработанные данные Logstash отправляет в конечное хранилище — Elasticsearch.



Основные компоненты системы

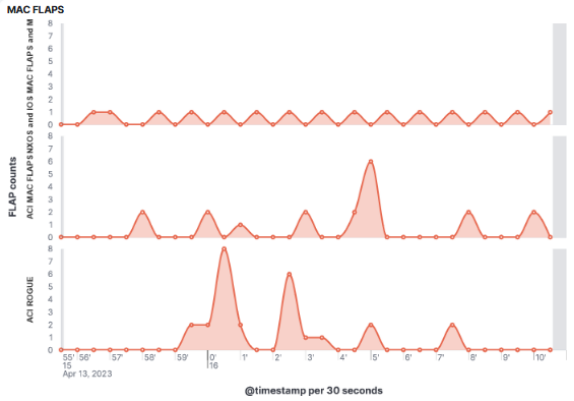
Elasticsearch — сердце Elastic Stack, это распределенная RESTful-система на основе JSON, совмещающая в себе функции поисковой системы и NoSQL-базы данных. Elasticsearch получает от Logstash, индексирует и хранит все собранные и обработанные данные.

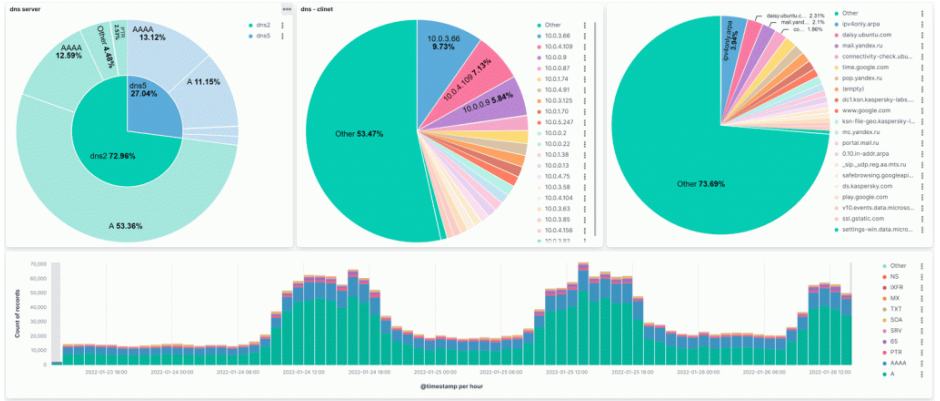
Elasticsearch — это большое, быстрое и хорошо масштабируемое нереляционное хранилище данных, являющееся отличным инструментом для поиска и аналитики журналов событий. Система может быстро обрабатывать большие объемы журналов, индексировать системные логи по мере поступления и выполнять запросы к ним в режиме реального времени.

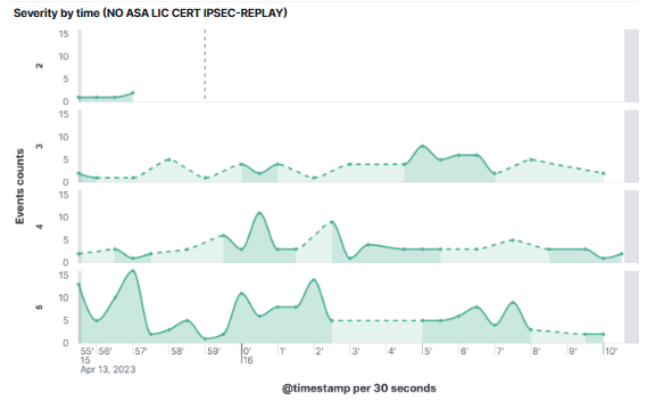
Основные компоненты системы

Kibana — центр визуализации сохранённых в Elasticsearch данных, представляющий их в удобном для восприятия виде, что упрощает их последующий анализ.

Kibana это пользовательский графический интерфейс, реализованный в виде web-панели, отображающий результаты поиска как в интерактивной сводной таблице, так и в виде графиков и диаграмм. Этот инструмент позволяет выполнять сложную аналитику и красочно визуализировать ее.







Преимущества внедрения системы сбора логов от АО «АМТ-ГРУП»

- Гибкость:
  - система может быть доработана под требования заказчика
  - возможность интеграции с другими системами
- Штат высококвалифицированных ИТ-специалистов
- Возможность получения дополнительных услуг:
  - техническая поддержка
  - обновление компонентов системы
  - услуги интеграции
  - обучение специалистов заказчика

Технологии разработки системы

Гибкое и универсальное решение на основе свободно распространяемого ПО:

Elastic Stack

syslog-ng®
by ONE IDENTITY