#### Компонент ведения журнала

#### Требования

Требуется реализовать компонент ведения журнала, обладающий следующими свойствами:

1. распределённая система сбора сообщений от источников различного вида, запущенных на разных компьютерах
2. централизованное хранилище сообщений с широким набором возможностей по обработке данных
3. удобная система визуализации, не требующая от администратора комплекса, подключающегося к управляющему компьютеру по сетевому интерфейсу установки специализрованного ПО

#### Реализация

С учётом особенностей структуры системы поиска и сбора информации, для реализации компонента ведения журнала выбрана распределенная архитектура. Все экземпляры модулей на каждом компьютере системы, а также система управления, используют для ведения журнала унифицированный интерфейс, основанный на библиотеке Boost::Log. Модули, реализованные на языке python, используют python-обертку над этим интерфейсом, реализованную при помощи инструмента Boost::Python.

1. Каждое сообщение содержит следующие данные:
2. Метку времени
3. Тип сообщения (информационное, предупреждение, ошибка)
4. Источник сообщения
5. Текст сообщения
6. Компьютер, на котором запущен источник сообщения

Для идентификации источника сообщения в журнале используются полные строковые имена экземпляров модулей (с учётом их вложенности в конкретные экземпляры трактов). Для идентификации компьютеров используются их строковые имена и IP-адреса.

Принимающие компьютеры, находящиеся под управлением ОС Linux, используют в качестве локального преобразователя сообщений демон Rsyslog, являющийся стандартом де-факто для Linux-систем. Rsyslog обрабатывает сообщения от модулей, в том числе, группирует одинаковые сообщения для уменьшения нагрузки на канал. После обработки, Rsyslog перенаправляет сообщения на управляющий компьютер, где их преобразует и приводит к унифицированному виду менеджер журналов Logstash.

В отличие от принимающих, обрабатывающие компьютеры, находящиеся под управлением ОС Windows, не используют Rsyslog: на каждом из них запущен свой менеджер Logstash.

Logstash посылает преобразованные сообщения в централизованное хранилище журналов Elasticsearch. Elasticsearch предоставляет широкий спектр возможностей по управлению журналом, включая фильтрацию, полнотекстовый поиск. Администратор комплекса получает доступ к собранным Elasticsearch сообщениям при помощи web-интерфейса Kibana, интегрированного в web-интерфейс комплекса и реализующего богатый функционал по настройке отображения сообщений, включающий, в частности, визуализацию интенсивности потоков сообщений разоичного типа с привязкой к временной шкале.

Схема реализованного компонента приведена на рис. 3.22.

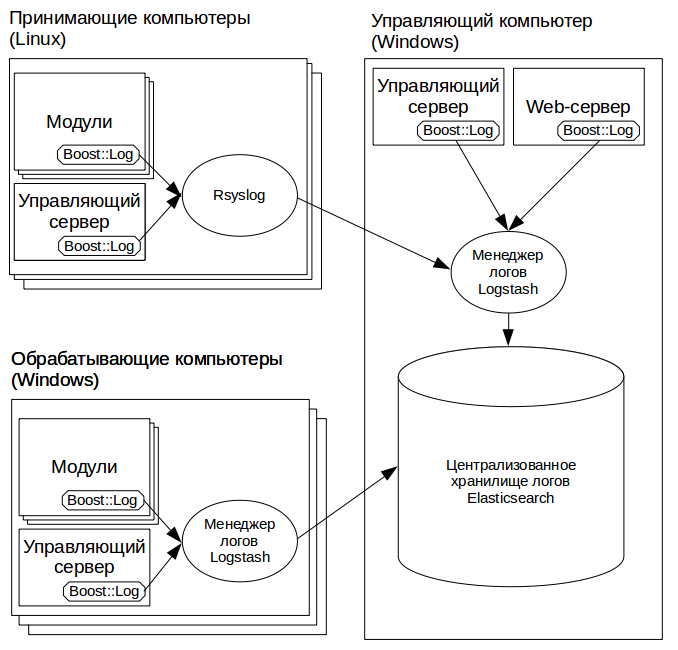
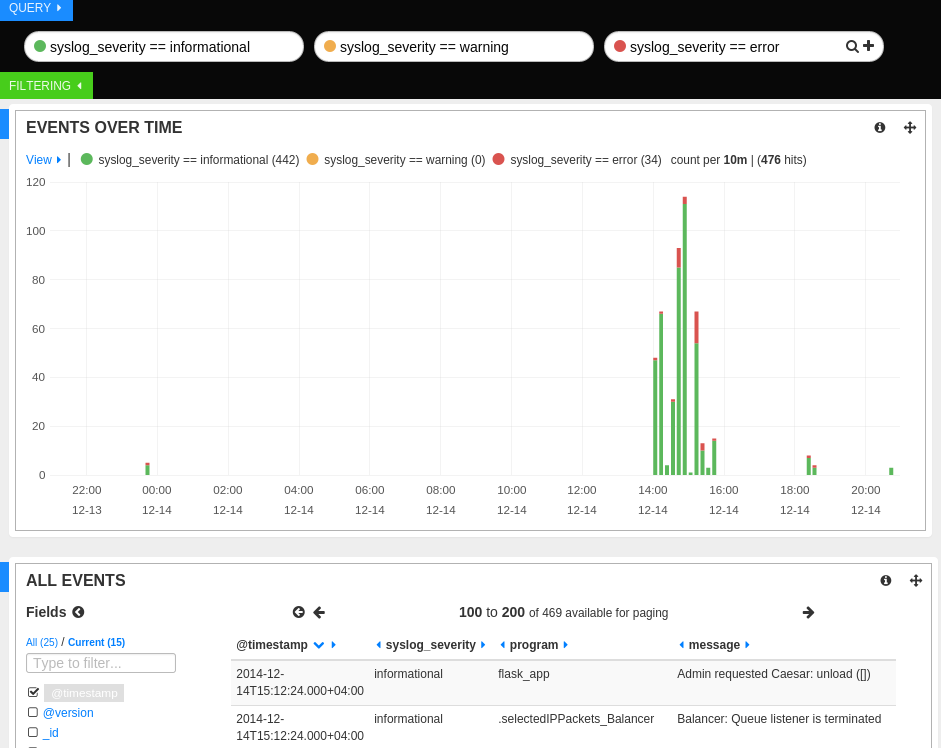


Рисунок 3.22 - Схема компонента ведения журнала

Пример визуализации собранных сообщений приведён на рис. 3.23.

Основные возможности пользователя по управлению отображением сообщений включают:

1. показ/скрытие временного графика
2. показ/скрытие списка сообщений
3. сортировка сообщений по значениям любого поля
4. выбор набора полей для отображения
5. фильтрация списка сообщений по заданному в виде логического выражения признаку
6. выбор групп данных для отображения на графике
7. сохранение/загрузка настроенных конфигураций



*Рисунок 3.23 - Пример визуализации собранных сообщений*