



ROSA Log Viewer

Руководство пользователя

Версия 0.3.0

Введение

Программа ROSA Central Panel Log Viewer предназначена для обзора логов централизованной системы хранения логов

1. Внешний вид программы

На рисунке 1 приведён внешний вид пользовательского интерфейса програм-мы.

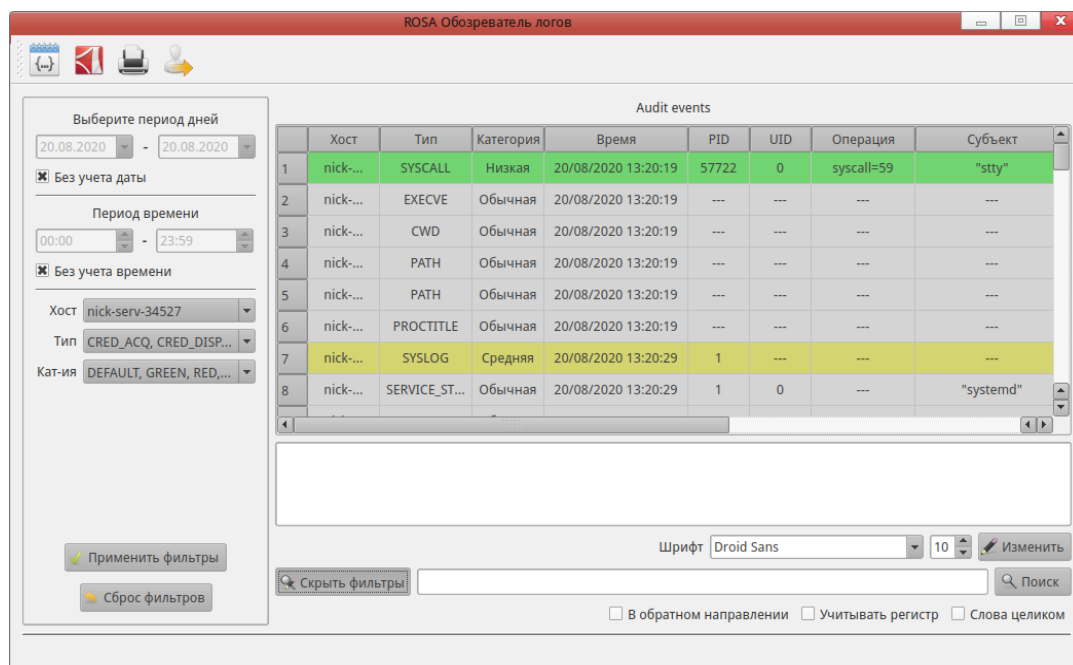


Рисунок 1 - Внешний вид программы

Ниже будут описаны компоненты рабочего окна программы.

2. Описание элементов интерфейса

В верхней части окна расположена панель дополнительных действий, которые будут добавлены в следующей версии. Описание иконок слева на право:

- 1) Экспорт в CVF-файл. (ведется разработка)
- 2) Экспорт в PDF-файл. (ведется разработка)
- 3) Печать (ведется разработка)
- 4) Выход

Слева расположен блок фильтров. Возможно 4 комбинации фильтров времени:

- 1) Все флажки установлены. При нажатии на «Применить фильтр», будет запрошен интервал времени текущего дня от 00:00 до 23:59
- 2) Все флажки сняты. При нажатии на кнопку «Применить фильтр», будет запрошен интервал времени составленный из введенных данных. Начальная точка времени будет составлена из первого поля даты и первого поля времени. Конечная точка времени будет составлена из второго поля даты и второго поля времени. Например: Если в блоке «Выберите период дней» выбраны даты 05/08/2020 и 10/08/2020, а в блоке «период времени» выбрано время 14:00 и 11:00, в таком случае интервал времени составит от 05/08/2020-14:00 до 10/08/2020-11:00.

3) Установлен только флажок «без учета даты». При нажатии на кнопку «Применить фильтры» будет запрошен интервал времени как в пункте 2, за исключением того, что дата будет равняться текущему дню.

4) Установлен только флажок «без учета времени». При нажатии на кнопку «Применить фильтры» будет запрошен интервал времени как в пункте 2, за исключением того, что время начала интервала будет установлено в 00:00, а время конца интервала будет установлено в 23:00.

Под фильтрами времени есть так же три фильтра по полям «хост», «тип» и «Категория». Данные фильтры представляют собой список с возможностью множественного выбора. Для исключения из результатов какого-нибудь значения, достаточно снять галочку напротив этого значения в соответствующем списке, и нажать на кнопку «Применить фильтр».

В центре находится таблица, представляющая события аудита. События можно фильтровать с помощью блока фильтров (если он не отображается, достаточно нажать на кнопке «Показать фильтры»), так же их можно сортировать по любому столбцу. При первом клике левой кнопкой мыши на заголовке столбца произойдет сортировка показанных событий по возрастанию. При повторном клике левой кнопкой мыши, произойдет сортировка показанных событий по убыванию. Сортировка производится лексикографически.

При выборе события левым кликом мыши, в поле под таблицей отобразиться не форматированная строка события.

В нижней части расположены элементы интерфейса для управления шрифтом отображаемых событий, и поиска по отображаемым событиям.

3. Работа с программой

Запуск программы требует пароль администратора! Это необходимо по причине наличия ограниченных прав доступа к файлам логов из директории /var/log.

Шрифт и размер шрифта а так же, время последнего отображенного события красной категории и адрес и порт сервера сохраняются в конфигурационном файле «/etc/rosa-central-panel-logviewer.conf». При последующих запусках программы настройки будут загружаться из него.

При возникновении события красной категории, с временной меткой позднее, чем сохраненное в файле конфигурации, будет выведено сообщение в системном трее.

В случае возникновения ошибок в процессе работы программы, они будут отображаться в статусной строке внизу окна. Длительность отображения одного сообщения составляет 10 секунд.

4. **О программе**

Авторы: Ерёменко Сергей, Моисеев Игорь

Версия: 0.3.0

Лицензия: BSD

Copyright (c) 2019, ООО «НТЦ ИТ РОСА»