Гарда БД

Руководство администратора

Модуль анализа сетевого трафика

Дата выпуска:	18.11.2022
Статус документа:	Released
Версия ПО:	4.21

Содержание

1. Введение

1.1. Аннотация

Данный документ представляет собой Руководство администратора к программному модулю анализа сетевого трафика, входящего в состав программного обеспечения «Гарда БД» (далее Система, Комплекс).

1.2. Типографические соглашения

Обозначения и типографические соглашения, использованные в данном документе, приведены ниже.

Соглашения и обозначения

Пример	Обозначение
***Примечание**: текст*	Важная информация, требующая особого внимания
N	Ссылка на документ
Registration	Названия конфигурационных параметров, вкладок и кнопок в граф. интерфейсе
http://www.example.com/	Гиперссылки

1.3. Использование имен, номеров телефонов, сетевых адресов

Все регистрационные имена пользователей, а также номера телефонов, имена и другие данные абонентов, используемые в Руководстве, являются вымышленными, а IP-адреса не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4. О компании

«Гарда Технологии» – российский разработчик систем защиты от внутренних и внешних угроз информационной безопасности, противодействия мошенничеству и расследования инцидентов.

Решения «Гарда Технологии» занимают лидирующие позиции на российских рынках решений информационной безопасности:

- защиты от DDoS-атак операторского класса.
- защиты баз данных.
- фрод-мониторинга порядка пропуска трафика операторов связи.
- DLP-систем.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Исследовательский центр компании обладает 5 патентами на уникальные технологии. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, операторах связи и государственных структурах России и СНГ. Подробнее – на gardatech.ru

1.5. Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по Московскому времени).
- Email: gbd.support@gardatech.ru.

2. Назначение модуля

Модуль анализа сетевого трафика (далее модуль «Анализатор», анализатор) предназначен для аудита и съема трафика в соответствии с критериями фильтрации. Средствами модуля выполняется анализ на соответствие настроенным политикам, передача перехваченных в соответствии с политиками событий в модули хранения и обработки данных.

3. Установка и обновление модуля

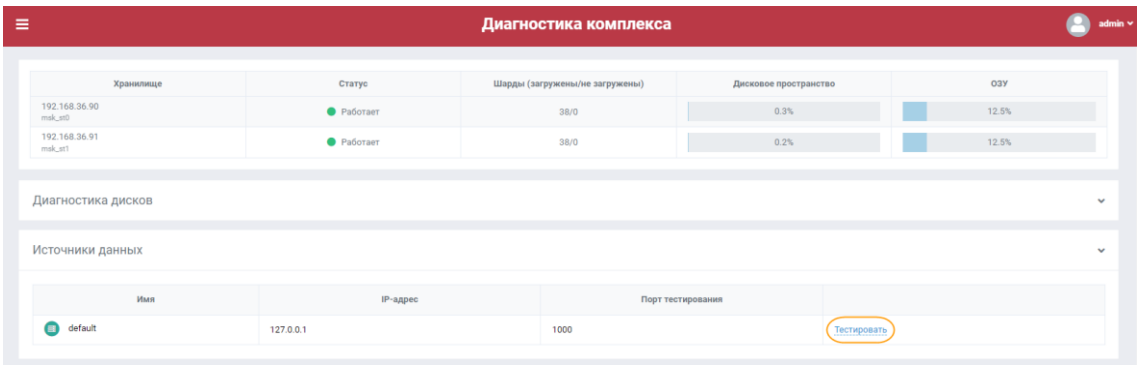
Установка и обновление модуля «Анализатор» описана в соответствующем руководстве, которое можно запросить в Службе технической поддержки.

4. Проблемы с анализатором

4.1. Поступление данных с анализатора

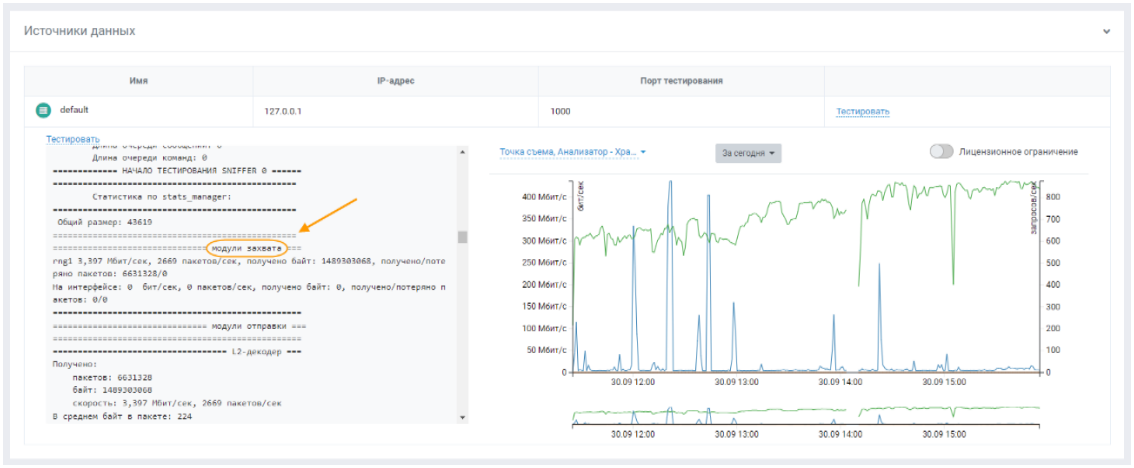
Для проверки поступления данных с анализатора выполните следующее:

1. В веб-интерфейсе системы перейдите в раздел **Диагностика**.
2. В блоке **Источники данных** выберите соответствующий анализатор и нажмите **Тестировать**, как показано на рис. ниже.



Диагностика анализатора

3. В выводе команды в разделе **модули захвата** отображается объем данных, поступающих на анализатор (см. рис. ниже).



Тестирование анализатора

4. Если данные тестирования не выводятся, подключитесь к серверу, на котором запущен анализатор и перезапустите следующий сервис: `service sniffer restart`

5. Если в тестировании анализатора значение объема поступающих данных равно нулю, перейдите к диагностике модуля meteor. Для этого обратитесь в Службу технической поддержки.