ГАРДА

Модуль «Активная защита БД»

Руководство пользователя

gardatech.ru

2023

Тип документа:	Руководство пользователя
Дата выпуска:	09.08.2023
Статус документа:	Released
Версия:	4.23

Содержание

1 Введение 4
1.1 Аннотация 4
1.2 Типографические соглашения 4
1.3 Использование имен, номеров телефонов, сетевых адресов 4
1.4 О компании 4
1.5 Техническая поддержка 5
2 Назначение модуля 6
3 Работа с Модулем 7

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство пользователя к программному модулю «Активная защита БД», входящему в состав программного обеспечения «Гарда БД» (далее Система, Комплекс).

1.2 Типографические соглашения

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

Пример	Обозначение
Примечание: *текст*	Важная информация, требующая особого внимания
См. Руководство администратора	Ссылка на документ
Войти	Названия элементов веб-интерфейса и конфигурационных параметров.
http://www.example.com/	Гиперссылки

1.3 Использование имен, номеров телефонов, сетевых адресов

Приведенные в настоящем документе сведения о юридических и физических лицах, включая любые их данные, являются вымышленными, а IP-адреса и номера телефонов не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4 О компании

Гарда Технологии (входит в ГК Гарда) – разработчик семейства продуктов в области защиты данных и сетевой безопасности. Решения Гарда защищают данные крупнейших государственных организаций и корпораций, защищают 50% всего российского интернета от DDoS-атак, обеспечивают защиту цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель холдинга построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и

сертифицированы ФСТЭК.

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 «Активная защита БД» (далее Модуль) предназначен для мониторинга и блокировки локальных и сетевых запросов к базам данных в режиме реального времени. Критерии перехвата и блокировки обращений к серверам БД конфигурируются на Системе.

3 Работа с Модулем

Модуль устанавливается на сервер БД, после чего автоматически регистрируется в Системе. Список установленных агентов отображается в разделе веб-интерфейса **Агенты** → **Настройки**. При выборе агента из списка отображается окно с настройками и основной информацией об агенте.

Агенты обозначаются следующими пиктограммами:

 - включенные (с включенным контролем подключений);

 - остановленные (с выключенным контролем подключений);

 - недоступные;

 - работа агента ограничена

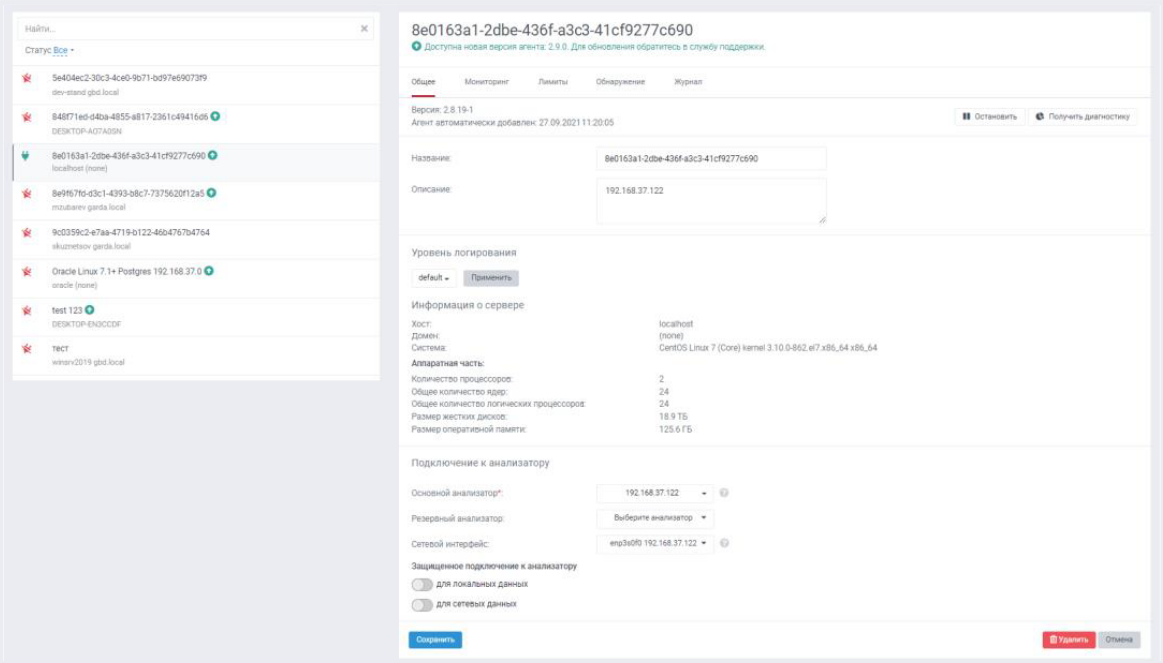
Включение и выключение контроля подключений регулируется при помощи кнопок **Запустить/Остановить** на вкладке **Общее** (см. рисунок ниже). Рядом располагается кнопка **Получить диагностику**, по нажатию на которую формируется диагностическая информация о работе агента.

Информация о сервере, на котором установлен агент, также отображается на вкладке **Общее**.

В разделе также доступен просмотр статистики нагрузки агента на операционную систему, на которую он установлен. Статистика отображается в виде графика, который строится на основе следующих параметров:

- % использования CPU;
- Использование памяти агентом (Кб);
- Использование HDD;
- Скорость передачи данных агентом на анализатор.

Для того чтобы удалить агент из списка, нажмите **Удалить**. Удаление рекомендуется проводить после деинсталляции Модуля с сервера БД.



Для осуществления мониторинга подключений необходимо произвести настройку агентов.

Настройки агентов располагаются в разделе **Агенты** → **Настройки**.

На вкладке **Общее** в поле **Основной анализатор** необходимо выбрать интерфейс анализатора, на который будут отправляться все запросы, перехватываемые агентом.

В поле **Сетевой интерфейс** необходимо выбрать интерфейс сервера БД, через который будут передаваться данные на анализатор. Рекомендуется по возможности выбирать наименее нагруженный интерфейс.

На вкладке **Мониторинг** в поле **Базы данных** необходимо выбрать те базы данных, которые необходимо контролировать.

Для контроля локального перехвата выберите типы соединений локального клиента с локальной БД.

В поле **Правила** можно настроить правила для блокировки трафика или его предварительной фильтрации на стороне агента. Для создания правила необходимо произвести следующие настройки и нажать кнопку **Сохранить**:

1. Введите название правила.
2. Выберите один из следующих типов правил и задайте для него соответствующие критерии:

   Исключение из мониторинга:

- Имя процесса
- Путь до процесса
- Аргументы процесса
- Пользователь ОС
- Логин БД
- Название приложения
- IP-адрес

Примечание: *Критерий* ***IP-адрес*** *не может быть использован одновременно с другими критериями правила.*

Блокировка трафика:

- Имя процесса
- Путь до процесса
- Аргументы процесса
- Пользователь ОС
- Логин БД
- Название приложения
- Таблицы (только для СУБД Oracle и PostgreSQL)
- Операции SQL (только для СУБД Oracle и PostgreSQL)
- IP-адрес

Если по каким-либо причинам указанных критериев блокировки недостаточно, то можно воспользоваться расширенным списком критериев блокировки с применением модуля Анализатор. В данном способе Модуль передает трафик на Анализатор, который в свою очередь посредством DPI производит анализ трафика, принимает решение о блокировке и передает это событие на Модуль.

Для создания правила выполните следующие действия:

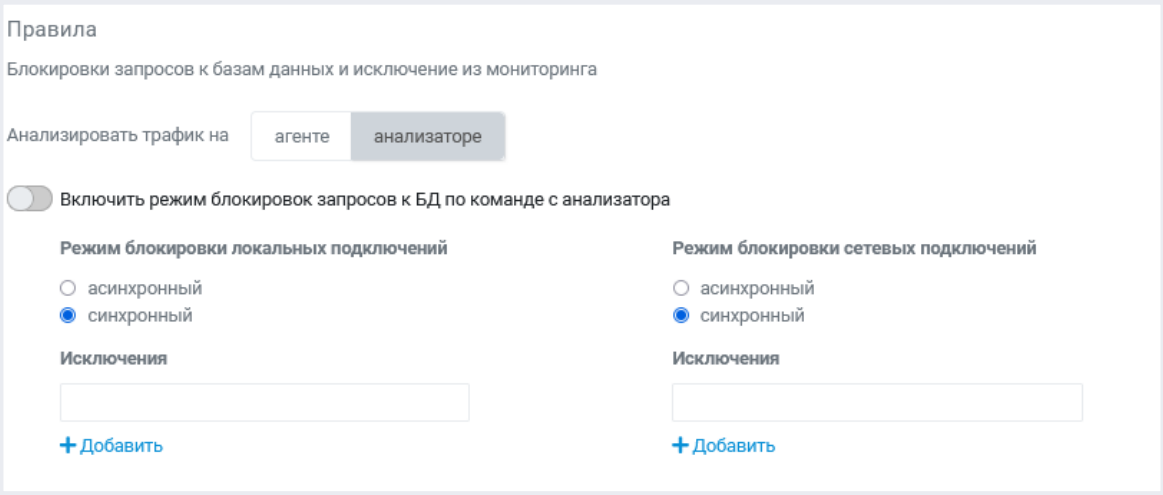
1. Выбрать пункт **Анализировать трафик на Анализаторе**.
2. Включить режим блокировок запросов к БД по команде с Анализатора.
3. Выбрать тип блокировки – **Синхронный** или **Асинхронный**.

Примечание:

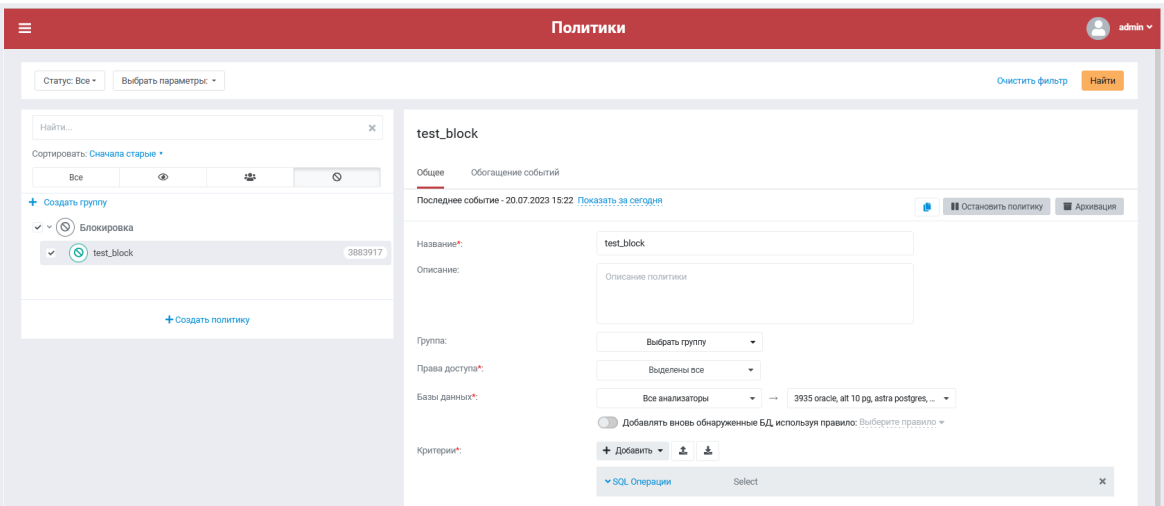
*- **Синхронный режим** означает, что агент перехватывает и*

приостанавливает каждый клиентский запрос, пока не получит подтверждение анализатора. В этом режиме существенно увеличиваются задержки при работе с базой, однако появляется возможность гарантированно заблокировать запросы типа DROP TABLE и DELETE.

*- **Асинхронный режим** означает, что агент не приостанавливает запросы, а просто отправляет перехваченные данные на анализатор и блокирует сессию, если придет команда на блокировку. Т.е. блокировка происходит с задержкой и один-два запрещенных запроса могут успеть выполниться перед тем, как сессия будет разорвана.*



Перейти в раздел **Политики** и создать политику блокировки с необходимыми критериями:



Список критериев

- Дата/Время
- IP адрес:порт
- Логин БД
- Таблица\Объект
- Поле таблицы\объекта
- Логин ОС
- Имя программы
- Имя функции\процедуры
- Экземпляр БД
- Пользователь
- SQL Операции
- Объем запроса
- Объем ответа
- Строк в ответе
- Ключевое слово
- Аутентификация
- Комбинированный
- Регулярные выражения