ГАРДА

Модуль «Активная защита БД»

Функциональная спецификация

gardatech.ru

2023

Тип документа:	Функциональная спецификация
Дата выпуска:	09.08.2023
Статус документа:	Released
Версия:	4.23

Содержание

1 Введение

1.1 Аннотация

Данный документ представляет собой Функциональную спецификацию 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 Функциональные возможности

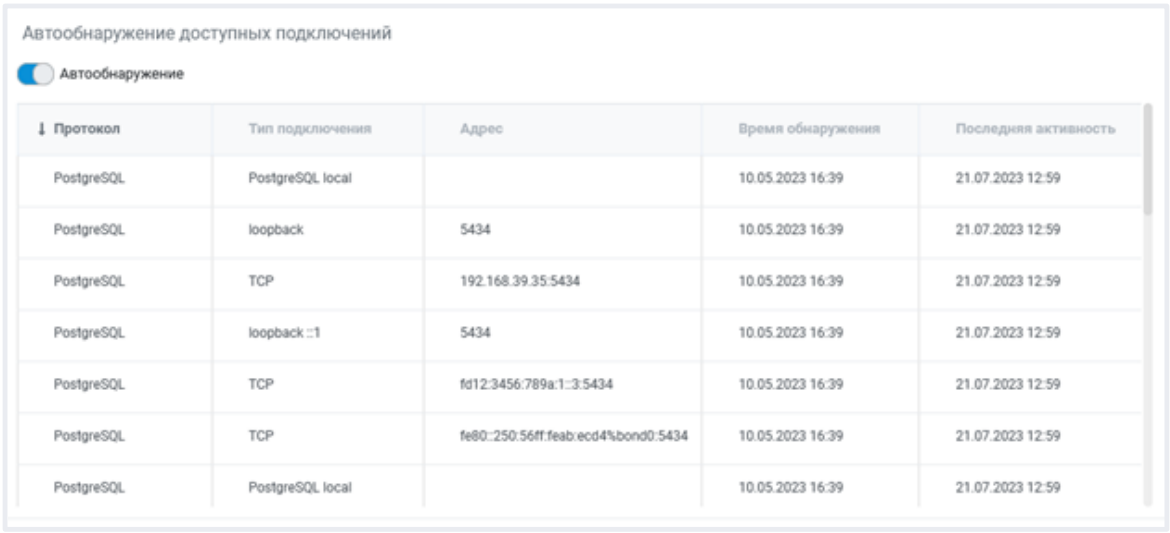
3.1 Мониторинг обращений к серверам БД

Помимо перехвата обращений к серверам БД на сетевых интерфейсах по ipv4/ipv6 Модуль позволяет отслеживать следующие способы взаимодействия с БД:

- Oracle BEQ
- Oracle IPC
- MSSQL named pipe
- MSSQL shared memory
- PostgreSQL local
- MongoDB local
- MySQL local
- MySQL named pipe

3.2 Автообнаружение доступных подключений

Модуль позволяет обнаруживать доступные способы взаимодействия с сервером БД. Найденные подключения сохраняются в таблицу **Автообнаружение доступных подключений**.



3.3 Исключение из мониторинга и блокировка обращений к серверам БД

С помощью Модуля можно исключать из мониторинга и блокировать обращения к серверам БД по критериям, конфигурируемым на Системе.

Список критериев

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

3.4 Блокировка обращений к серверам БД с помощью анализатора трафика

Также существует расширенный список 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.

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

3.5 Список поддерживаемых БД и ОС

ОС	Версия ОС	СУБД	Тип перехвата
RHEL OEL CentOS	5.x	Oracle	TCP External
			TCP Loopback

ОС	Версия ОС	СУБД	Тип перехвата
			Local
		MySQL Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных PostgreSQL Vertica Greenplum Apache Hive Sap Hana Informix ClickHouse	TCP Loopback
			TCP External
RHEL OEL CentOS	6.x 7.x 8.x 9.0	Oracle PostgreSQL Vertica Greenplum MongoDB MySQL	TCP External
			TCP Loopback
			Local
		Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Apache Hive Sap Hana Informix ClickHouse	TCP Loopback
			TCP External
Alt Linux	9.2 10	MySQL	TCP External
			TCP Loopback
			Local

ОС	Версия ОС	СУБД	Тип перехвата
		PostgreSQL Vertica Greenplum MongoDB Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Apache Hive Sap Hana Informix ClickHouse	TCP Loopback TCP External
Windows	5.1 - 5.2	Oracle PostgreSQL Vertica Greenplum MSSQL MySQL Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных PostgreSQL Informix	TCP External
РЕД ОС	7	Oracle PostgreSQL Vertica Greenplum MongoDB	TCP External TCP Loopback Local

ОС	Версия ОС	СУБД	Тип перехвата
		MySQL Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Apache Hive Sap Hana Informix ClickHouse	TCP Loopback
			TCP External
Windows	6.x - 10.x	Oracle MSSQL	TCP External
			TCP Loopback
			Local
		MySQL Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных PostgreSQL Vertica Greenplum Apache Hive Informix	TCP Loopback
			TCP External
AIX	7.1	Oracle	TCP External
			TCP Loopback
			Local
		IBM DB2 Apache Hive	TCP Loopback
			TCP External

ОС	Версия ОС	СУБД	Тип перехвата
Solaris	10.x - 11.x	Oracle	TCP External
			TCP Loopback
			Local
		IBM DB2 Apache Hive	TCP Loopback
			TCP External
OpenSUSE	12.x - 13.x Leap x.x	Oracle MongoDB MySQL	TCP External
			TCP Loopback
			Local
		Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных PostgreSQL Vertica Greenplum Apache Hive Sap Hana Informix ClickHouse	TCP Loopback
			TCP External
SUSE Linux Enterprise Server (SLES)	11	Oracle PostgreSQL	TCP External
			TCP Loopback
			Local

ОС	Версия ОС	СУБД	Тип перехвата
		MySQL Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Vertica Greenplum Apache Hive Sap Hana Informix ClickHouse	TCP Loopback
			TCP External
	12 - 15	Oracle PostgreSQL MongoDB MySQL	TCP External
			TCP Loopback
			Local
		Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Vertica Greenplum Apache Hive Sap Hana Informix ClickHouse	TCP Loopback
			TCP External
	12-15 s390x	Oracle PostgreSQL MongoDB MySQL	TCP External
			TCP Loopback
			Local

ОС	Версия ОС	СУБД	Тип перехвата
		Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Vertica Greenplum Apache Hive Sap Hana Informix ClickHouse	TCP Loopback
			TCP External
Astra Linux Special Edition	1.x – 2.x	Oracle PostgreSQL Greenplum Vertica MongoDB MySQL	TCP External
			TCP Loopback
			Local
		Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Apache Hive Informix ClickHouse	TCP External
			TCP Loopback
Ubuntu	16.04 LTS; 18.04 LTS; 20.04 LTS.	Oracle PostgreSQL Greenplum Vertica MongoDB MySQL	TCP External
			TCP Loopback
			Local

ОС	Версия ОС	СУБД	Тип перехвата
		Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Apache Hive Informix ClickHouse	TCP External
			TCP Loopback
Debian	10	Oracle PostgreSQL Greenplum Vertica MySQL	TCP External
			TCP Loopback
			Local
		Percona Server MariaDB Firebird Interbase Teradata IBM DB2 Ред База Данных Apache Hive Informix ClickHouse	TCP External
			TCP Loopback

3.6 Список поддерживаемых версий ядер

Версия ядра	ОС
4.4.0-87-generic 4.4.0-131-generic 4.4.0-187-generic 4.15.0-112-generic 4.15.0-144-generic 4.15.0-171-generic 4.15.0-180-generic 4.15.0-192-generic 5.4.0-74-generic 5.4.0-77-generic 5.4.0-113-generic 5.4.0-122-generic 5.4.0-128-generic 5.4.0-132-generic 5.15.0-48-generic	Ubuntu
4.15.3-1-generic 4.15.3-2-generic 4.15.3-141-generic 4.15.3-154-generic 5.4.0-71-generic 5.4.0-81-generic 5.4.0-110-generic 5.10.0-1038-generic 5.10.0-1045-generic 5.15.0-33-generic	Astra Linux 1.6, 2.12

Версия ядра	ОС
5.4.0-54-generic 5.4.0-110-generic 5.10.142-1-generic 5.15.0-33-generic 5.15.0-33-lowlatency	Astra Linux 1.7
4.9.79-1.el7.x86_64 4.19.79-1.el7.x86_64 4.19.204-2.el7.x86_64 5.4.53-1.el7.x86_64 5.10.29-1.el7.x86_64 5.14.9-1.el7.x86_64 5.15.5-5.el7.x86_64 5.15.10-1.el7.x86_64 5.15.35-1.el7.3.x86_64 5.15.35-5.el7.3.x86_64 5.15.72-1.el7.3.x86_64 5.15.87-1.el7.3.x86_64	РЕД ОС
2.6.32-279.el6.x86_64 2.6.32-358.el6.x86_64 2.6.32-431.el6.x86_64 2.6.32-504.el6.x86_64 2.6.32-573.el6.x86_64 2.6.32-642.el6.x86_64 2.6.32-696.el6.x86_64 2.6.32-754.el6.x86_64	Red Hat Enterprise Linux 6.0 - 6.10 и CentOS 6.0 - 6.10 Oracle Linux 6.0 - 6.10

Версия ядра	ОС
3.8.13-35.el6uek.x86_64 3.8.13-44.el6uek.x86_64 3.8.13-55.el6uek.x86_64 3.8.13-68.el6uek.x86_64 3.8.13-98.el6uek.x86_64 3.8.13-118.el6uek.x86_64 4.1.12-32.el6uek.x86_64 4.1.12-37.el6uek.x86_64 4.1.12-61.el6uek.x86_64 4.1.12-94.el6uek.x86_64 4.1.12-103.el6uek.x86_64 4.1.12-112.el6uek.x86_64 4.1.12-124.el6uek.x86_64	Oracle Linux 6.0 - 6.10
3.10.0-123.el7.x86_64 3.10.0-229.el7.x86_64	Red Hat Enterprise Linux 7.0 - 7.9 и CentOS 7.0 - 7.9
3.10.0-327.el7.x86_64 3.10.0-514.el7.x86_64 3.10.0-693.el7.x86_64 3.10.0-862.el7.x86_64 3.10.0-957.el7.x86_64 3.10.0-1062.el7.x86_64 3.10.0-1127.el7.x86_64 3.10.0-1160.el7.x86_64 5.4.12-1.el7.elrepo.x86_64	Oracle Linux 7.0 - 7.9

Версия ядра	ОС
3.8.13-35.el7uek.x86_64 3.8.13-44.el7uek.x86_64 3.8.13-55.el7uek.x86_64 3.8.13-68.el7uek.x86_64 3.8.13-98.el7uek.x86_64 3.8.13-118.el7uek.x86_64 4.1.12-32.el7uek.x86_64 4.1.12-37.el7uek.x86_64 4.1.12-61.el7uek.x86_64 4.1.12-94.el7uek.x86_64 4.1.12-103.el7uek.x86_64 4.1.12-112.el7uek.x86_64 4.1.12-124.el7uek.x86_64 4.14.35-1818.el7uek.x86_64 4.14.35-1844.el7uek.x86_64 4.14.35-1902.el7uek.x86_64 4.14.35-2025.el7uek.x86_64 4.14.35-2047.el7uek.x86_64 5.4.17-2011.el7uek.x86_64 5.4.17-2036.el7uek.x86_64 5.4.17-2102.el7uek.x86_64 5.4.17-2136.el7uek.x86_64	Oracle Linux 7.0 - 7.9

Версия ядра	ОС
4.18.0-80.el8.x86_64 4.18.0-80.el8_0.x86_64	Red Hat Enterprise Linux 8.0 - 8.6 и CentOS 8.0 - 8.6
4.18.0-147.el8.x86_64 4.18.0-147.el8_1.x86_64 4.18.0-193.el8.x86_64 4.18.0-193.el8_2.x86_64 4.18.0-240.el8.x86_64 4.18.0-240.el8_3.x86_64 4.18.0-305.el8.x86_64 4.18.0-305.el8_4.x86_64 4.18.0-348.el8.x86_64 4.18.0-348.el8_5.x86_64 4.18.0-372.el8.x86_64 4.18.0-372.el8_6.x86_64 4.18.0-394.el8.x86_64 4.18.0-408.el8.x86_64 4.18.0-425.el8.x86_64 4.18.0-425.el8_7.x86_64 4.18.0-365.el8.x86_64 4.18.0-448.el8.x86_64 5.5.5-1.el8.elrepo.x86_64	Oracle Linux 8.0 - 8.4
5.4.17-2011.el8uek.x86_64; 5.4.17-2036.el8uek.x86_64; 5.4.17-2102.el8uek.x86_64 5.4.17-2136.el8uek.x86_64	Oracle Linux 8.0 - 8.6
5.14.0-70.el9_0.x86_64	Red Hat Enterprise Linux 9 и CentOS 9
5.14.0-124.el9.x86_64 5.14.0-162.6.1.el9_1.x86_64	Oracle Linux 9

Версия ядра	ОС
5.15.0-1.el9uek.x86_64 5.15.0-2.el9uek.x86_64 5.15.0-3.el9uek.x86_64 5.15.0-4.el9uek.x86_64 5.15.0-5.el9uek.x86_64 5.15.0-6.el9uek.x86_64 5.15.0-7.el9uek.x86_64	Oracle Linux 9
4.4.73-5-default 5.3.18-22-default	SUSE Linux Enterprise Server 12-15 s390x
4.12.14-lp151-default 5.3.18-lp152-default 5.3.18-22-default 5.3.18-24-default 5.3.18-57-default 5.3.18-59-default 5.14.21-150400-default	SUSE Linux Enterprise Server 12-15 OpenSUSE 12-15 x64
5.4.214-std-def-alt1 5.10.144-std-def-alt0.c9f.2 5.10.145-std-def-alt1	Alt Linux