ГАРДА

Модуль «Активная защита БД»

Руководство администратора

gardatech.ru

2023

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

Содержание

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство администратора 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 Установка агента на сервер БД

Для установки агента на сервер БД необходимо выполнить следующий действия:

1. Скопировать дистрибутив агента на сервер.
2. Выполнить установку агента одним из следующих способов.

Внимание: *Установка на ОС Linux/AIX/Solaris должна производиться от УЗ root.*

Внимание: *Удалённое обновление агента с PU работает только на версиях >= 2.9.0*

3.1 Centos 5.x/RHEL 5.x/Oracle Linux 5.x

```
[localhost DBS]# rpm -ihv dbs_agent-x.x.x-rhel5-x86_64.rpm
```

3.2 Centos 6.x/RHEL 6.x/Oracle Linux 6.x

```
[localhost DBS]# rpm -ihv dbs_agent-x.x.x-rhel6-x86_64.rpm
```

Установка агента с функцией удалённого обновления с PU:

```
[localhost DBS]# DBS_AGENT_UPGRADE_SERVICE_ENABLED=1 rpm -ihv
dbs_agent-x.x.x-rhel6-x86_64.rpm
```

3.3 OpenSuse 11.x/SLES 11.x

```
[localhost DBS]# rpm -ihv dbs_agent-x.x.x-sles11-x86_64.rpm
```

Установка агента с функцией удалённого обновления с PU:

```
[localhost DBS]# DBS_AGENT_UPGRADE_SERVICE_ENABLED=1 rpm -ihv
dbs_agent-x.x.x-sles11-x86_64.rpm
```

3.4 Centos 7.x/RHEL 7.x/Oracle Linux 7.x

```
[localhost DBS]# rpm -ihv dbs_agent-x.x.x-rhel7-x86_64.rpm
```

Установка агента с функцией удалённого обновления с PU:

```
[localhost DBS]# DBS_AGENT_UPGRADE_SERVICE_ENABLED=1 rpm -ihv
dbs_agent-x.x.x-rhel7-x86_64.rpm
```

3.5 Centos 8.x/RHEL 8.x/Oracle Linux 8.x/REDOS 7.1-7.3

```
[localhost DBS]# rpm -ihv dbs_agent-x.x.x-rhel8-x86_64.rpm
```

Установка агента с функцией удалённого обновления с PU:

```
[localhost DBS]# DBS_AGENT_UPGRADE_SERVICE_ENABLED=1 rpm -ihv
dbs_agent-x.x.x-rhel8-x86_64.rpm
```

3.6 Centos 9.x/RHEL 9.x/Oracle Linux 9.x

```
[localhost DBS]# rpm -ihv dbs_agent-x.x.x-rhel9-x86_64.rpm
```

Установка агента с функцией удалённого обновления с PU:

```
[localhost DBS]# DBS_AGENT_UPGRADE_SERVICE_ENABLED=1 rpm -ihv
dbs_agent-x.x.x-rhel9-x86_64.rpm
```

3.7 Windows Server

Внимание: *Перед установкой агента на Windows Server x86 или x64, необходимо установить патчи безопасности: KB4493730 и KB4474419*

Внимание: *В Windows Server 2008 SP2 x86 сервис агента нужно запускать от администатора*

Внимание: *В Windows Vista/Server 2008 SP2 рекомендуется устанавливать npcap 0.9983-0.9987 или Winpcap.*

Для установки агента на Windows Server выполните следующие действия:

1. Скопировать exe файл агента на сервер.
2. Запустить установку агента `dbs_agent-x.x.x-winXX.exe`.
3. Во время установки агента будет предложено установить дополнительное ПО - Winpcap и Visual C++ Redistributable Packages (если оно не установлено на сервере).
4. Сконфигурировать агент (необходимо задать IP адрес хранилища ПК Гарда БД (веб-сервер) и порты для подключения к анализатору).

5. Конфигурационный файл по умолчанию находится в каталоге установки агента: `C:\Program Files\Garda Database Agent\cfg`. При установке агента путь можно изменить (см. описание конфигурационного файла)
6. После правки конфигурационного файла необходимо зайти в `computer management/services` и перезапустить службу **Garda Technologies database agent**.

3.8 Docker

Чтобы добавить агент Гарда БД в докер-образ, нужно сначала подготовить конфигурационный файл `dbs_agent.cfg` с нужными настройками.

Пример конфигурационного файла:

```
{
"DISK_BUFFER_PATH": "",
"GUID": "17b3da3f-dc06-46c3-9bb8-cca3f4ba733f",
"HTTP_SERVER_URL": "https://ip_адрес_ТВД:5070/Agent/Connect"
"KERNEL_MODULE": false,
"LOGGER_HOST": "",
"LOGGER_LEVEL": "info",
"PROCESS_BLOCKING_MODE": "async",
"SNIFFER_FLEX_PORT": 2201,
"SNIFFER_FLEX_PORT_TLS": 2202
}
```

Также пример конфигурационного файла лежит в архиве с дистрибутивом агента в `/opt/dbs_agent/cfg/dbs_agent.cfg`

Если требуется, чтобы настройки агента на пульте не слетали при каждом перезапуске контейнера, нужно сгенерировать случайный GUID и прописать его в `dbs_agent.cfg`, например:`"GUID" : "8c846be1-7328-48f2-b7f3-4509d9744e98"`

Потом нужно добавить установку агента в Dockerfile.
Пример 1:

```
FROM oraclelinux:8
ARG dbs_agent_ver=dbs_agent-2.11.0-1-docker-x86_64.tar.gz
COPY $dbs_agent_ver /
RUN cd / && tar -xvf $dbs_agent_ver --strip-components 1
RUN rm -rf /$dbs_agent_ver
ADD dbs_agent.cfg /opt/dbs_agent/cfg/
```

```
RUN /opt/dbs_agent/scripts/postinst.sh && /bin/chown
dbs_agent /opt/dbs_agent/cfg/dbs_agent.cfg
```

Если используется non-root контейнер, нужно явно указать, что агент устанавливается от root пользователя, а потом при необходимости вернуть исходного non-root пользователя

Пример 2:

```
FROM docker.io/bitnami/postgresql:latest
ARG dbs_agent_ver=dbs_agent-2.11.0-1-docker-x86_64.tar.gz
USER root
COPY $dbs_agent_ver /
RUN cd / && tar -xvf $dbs_agent_ver --strip-components 1
RUN rm -rf /$dbs_agent_ver
ADD dbs_agent.cfg /opt/dbs_agent/cfg/
RUN /opt/dbs_agent/scripts/postinst.sh && /bin/chown
dbs_agent /opt/dbs_agent/cfg/dbs_agent.cfg
USER 1001
```

Если в процессе установки не будет хватать каких-то пакетов, нужно сначала установить их. Например, если в debian/ubuntu системе нет setcap, то после `ADD dbs_agent.cfg /opt/dbs_agent/cfg/` нужно добавить строчку: `RUN apt-get update && apt-get install -y libcap2-bin`