Dr.WEB

Server Security Suite (Unix)

Руководство администратора



© «Доктор Веб», 2026. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

Ограничение ответственности

Ни при каких обстоятельствах ООО «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

Dr.Web Server Security Suite (Unix)
Версия 11.1
Руководство администратора
07.10.2026

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте.

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение 8

2. Условные обозначения и сокращения 9

3. О продукте 10

3.1. Основные функции Dr.Web Server Security Suite 11

3.2. Структура Dr.Web Server Security Suite 13

3.2.1. Базовые антивирусные компоненты 14

3.2.2. Компоненты поиска угроз 16

3.2.3. Сервисные компоненты 17

3.2.4. Интерфейсные компоненты 19

3.3. Помещение в карантин 21

3.4. Полномочия для работы с файлами 22

3.5. Режимы работы 23

4. Системные требования и совместимость 28

5. Лицензирование 33

6. Установка и удаление 34

6.1. Установка Dr.Web Server Security Suite 35

6.1.1. Установка универсального пакета 36

6.1.1.1. Установка в режиме командной строки 38

6.1.2. Установка из репозитория 39

6.2. Обновление Dr.Web Server Security Suite 43

6.2.1. Получение текущих обновлений 43

6.2.2. Переход на новую версию 44

6.2.3. Обновление без подключения к интернету 47

6.3. Удаление Dr.Web Server Security Suite 49

6.3.1. Удаление универсального пакета 49

6.3.1.1. Удаление в режиме командной строки 50

6.3.2. Удаление Dr.Web Server Security Suite, установленного из репозитория 50

6.4. Дополнительно 53

6.4.1. Пакеты и файлы Dr.Web Server Security Suite 53

6.4.2. Выборочные установка и удаление компонентов 56

6.5. Настройка подсистем безопасности 62

6.5.1. Настройка политик безопасности SELinux 63

6.5.2. Настройка запуска в режиме ЗПС (Astra Linux SE, версии 1.6 и 1.7) 66

7. Начало работы **68**
7.1. Регистрация и активация **68**
7.1.1. Ключевой файл 71
7.2. Проверка работоспособности **72**
7.3. Настройка мониторинга файловой системы **73**
7.4. Интеграция с файловым сервером Samba **75**
7.5. Интеграция с томами NSS **78**
8. Краткие инструкции **80**
9. Компоненты Dr.Web Server Security Suite **86**
9.1. Dr.Web ConfigD **86**
9.1.1. Принципы работы 86
9.1.2. Аргументы командной строки 88
9.1.3. Параметры конфигурации 89
9.2. Dr.Web Ctl **93**
9.2.1. Формат вызова из командной строки 95
9.2.2. Общие опции 95
9.2.3. Команды 95
9.2.3.1. Команды антивирусной проверки 96
9.2.3.2. Команды управления угрозами и карантином 110
9.2.3.3. Команды управления конфигурацией 116
9.2.3.4. Расширенные команды 119
9.2.3.4.1. Команды управления обновлением и работой в режиме централизованной защиты 120
9.2.3.4.2. Информационные команды 122
9.2.4. Примеры использования 127
9.2.5. Параметры конфигурации 130
9.3. Веб-интерфейс управления Dr.Web **131**
9.3.1. Управление компонентами 133
9.3.2. Управление угрозами 134
9.3.3. Управление настройками 136
9.3.3.1. Управление централизованной защитой 142
9.3.4. Проверка локальных файлов 144
9.4. SplDer Guard **148**
9.4.1. Принципы работы 148
9.4.2. Аргументы командной строки 152
9.4.3. Параметры конфигурации 153

9.4.4. Использование модуля ядра для SpIDer Guard 161
9.5. SpIDer Guard для SMB 164
9.5.1. Принципы работы 164
9.5.2. Аргументы командной строки 166
9.5.3. Параметры конфигурации 167
9.5.4. Сборка модуля VFS SMB 175
9.6. SpIDer Guard для NSS 177
9.6.1. Принципы работы 177
9.6.2. Аргументы командной строки 179
9.6.3. Параметры конфигурации 180
9.7. Dr.Web ClamD 186
9.7.1. Принципы работы 186
9.7.2. Аргументы командной строки 187
9.7.3. Параметры конфигурации 188
9.7.4. Интеграция с внешними приложениями 194
9.8. Dr.Web File Checker 195
9.8.1. Принципы работы 195
9.8.2. Аргументы командной строки 196
9.8.3. Параметры конфигурации 197
9.9. Dr.Web Network Checker 199
9.9.1. Принципы работы 199
9.9.2. Аргументы командной строки 201
9.9.3. Параметры конфигурации 202
9.9.4. Организация сканирующего кластера 208
9.10. Dr.Web Scanning Engine 212
9.10.1. Принципы работы 212
9.10.2. Аргументы командной строки 214
9.10.3. Параметры конфигурации 217
9.11. Dr.Web Updater 221
9.11.1. Принципы работы 221
9.11.2. Аргументы командной строки 222
9.11.3. Параметры конфигурации 223
9.12. Dr.Web ES Agent 229
9.12.1. Принципы работы 229
9.12.2. Аргументы командной строки 230
9.12.3. Параметры конфигурации 231

9.13. Dr.Web HTTPD **234**
9.13.1. Принципы работы 234
9.13.2. Аргументы командной строки 235
9.13.3. Параметры конфигурации 236
9.13.4. Описание HTTP API 239
9.14. Dr.Web SNMPD **262**
9.14.1. Принципы работы 262
9.14.2. Аргументы командной строки 264
9.14.3. Параметры конфигурации 265
9.14.4. Интеграция с системами мониторинга 268
9.14.5. Dr.Web SNMP MIB 277
9.15. Dr.Web MeshD **300**
9.15.1. Принципы работы 300
9.15.2. Аргументы командной строки 302
9.15.3. Параметры конфигурации 303
9.16. Dr.Web CloudD **308**
9.17. Dr.Web StatD **313**
9.17.1. Принципы работы 313
9.17.2. Аргументы командной строки 313
9.17.3. Параметры конфигурации 314
10. Приложения **316**
10.1. Приложение А. Виды компьютерных угроз **316**
10.2. Приложение Б. Устранение компьютерных угроз **322**
10.3. Приложение В. Техническая поддержка **325**
10.4. Приложение Г. Конфигурационный файл Dr.Web Server Security Suite **327**
10.4.1. Структура файла 327
10.4.2. Типы параметров 328
10.5. Приложение Д. Генерация сертификатов SSL **333**
10.6. Приложение Е. Описание известных ошибок **336**
10.7. Приложение Ж. Список сокращений **386**

1. Введение

Решение Dr.Web Server Security Suite позволит вам обеспечить надежную защиту вашего сервера от распространения компьютерных угроз всех возможных типов, используя наиболее современные технологии обнаружения и обезвреживания угроз. Это повысит качество услуг, предоставляемых сервером.

Данное руководство предназначено для помощи администраторам серверов, работающих под управлением Unix-подобных ОС, таких как ОС семейства GNU/Linux и FreeBSD (далее в документе будет использовано обозначение Unix), в установке и использовании Dr.Web Server Security Suite.

Если у вас уже установлен Dr.Web Server Security Suite предыдущей версии, и вы желаете обновить его до актуальной версии, выполните на нее переход (см. раздел Переход на новую версию).

2. Условные обозначения и сокращения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Важное замечание или указание
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание
Антивирусная сеть	Новый термин или акцент на термине в описаниях
<IP-address>	Поля для замены функциональных названий фактическими значениями
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса
CTRL	Обозначения клавиш клавиатуры
`/home/user`	Наименования файлов и каталогов, фрагменты программного кода
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы



Команды, которые требуется ввести с клавиатуры в командную строку операционной системы (в терминале или эмуляторе терминала), в руководстве предваряются символом приглашения к вводу `$` или `#`, определяющим, какие полномочия пользователя необходимы для выполнения указанной команды. Стандартным для Unix-систем образом подразумевается, что:

`$` — для выполнения команды достаточно обычных прав пользователя.

`#` — для выполнения команды требуются права суперпользователя (обычно — *root*). Для повышения прав можно использовать команды `su` и `sudo`.

Перечень сокращений приведен в разделе Приложение Ж. Список сокращений.

3. О продукте

Назначение

Dr.Web Server Security Suite создан для защиты файлов аппаратных и виртуальных файловых серверов, работающих под управлением Unix-подобных ОС (GNU/Linux и FreeBSD) от вирусов и всех прочих видов вредоносного программного обеспечения, а также для предотвращения распространения через них угроз для различных платформ. При работе в режиме централизованной защиты Dr.Web Server Security Suite контролируется сервером под управлением Dr.Web Enterprise Security Suite.

Защита данных

Основные компоненты (антивирусное ядро и вирусные базы) являются не только крайне эффективными и нетребовательными к системным ресурсам, но и кросс-платформенными, что позволяет специалистам компании «Доктор Веб» создавать надежные антивирусные решения, обеспечивающие защиту компьютеров, работающих под управлением распространенных операционных систем, от угроз, предназначенных для различных платформ. В настоящее время, наряду с Dr.Web Server Security Suite, в компании «Доктор Веб» разработаны также и другие антивирусные решения для Unix-подобных операционных систем (GNU/Linux и FreeBSD), macOS и Windows. Кроме того, разработаны антивирусные решения, обеспечивающие защиту мобильных устройств, работающих под управлением ОС Android и «Аврора».

Компоненты Dr.Web Server Security Suite постоянно обновляются, а вирусные базы регулярно дополняются новыми записями, что обеспечивает актуальный уровень защищенности файлов аппаратных и виртуальных файловых серверов. Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре, и обращение к облачному сервису Dr.Web Cloud, хранящему информацию о новейших угрозах, сигнатуры которых еще отсутствуют в базах.

Дополнительно:

- Основные функции Dr.Web Server Security Suite
- Структура Dr.Web Server Security Suite
- Помещение в карантин
- Полномочия для работы с файлами
- Режимы работы

3.1. Основные функции Dr.Web Server Security Suite

1. **Поиск и обезвреживание угроз.** Производится поиск как непосредственно вредоносных программ всех возможных типов (различных вирусов, включая вирусы, инфицирующие почтовые файлы и загрузочные записи дисков, а также троянских программ, почтовых червей и т. п.), так и нежелательных программ (рекламных программ, программ-шуток, программ автоматического дозвона). Подробнее о видах угроз см. Приложение А. Виды компьютерных угроз.

   Для обнаружения угроз используются:

   - *сигнатурный анализ* — метод проверки, позволяющий обнаружить уже известные угрозы, информация о которых содержится в вирусных базах;
   - *эвристический анализ* — набор методов проверки, позволяющих обнаруживать угрозы, которые еще неизвестны;
   - *облачные технологии обнаружения угроз* — производится обращение к сервису Dr.Web Cloud, собирающему свежую информацию об актуальных угрозах, рассылаемую различными антивирусными продуктами Dr.Web.

   Эвристический анализатор может ложно реагировать на программное обеспечение, не являющегося вредоносным. Поэтому объекты, содержащие обнаруженные им угрозы, получают специальный статус «подозрительные». Рекомендуется помещать такие файлы в карантин, а также передавать на анализ в антивирусную лабораторию «Доктор Веб». Подробнее о методах обезвреживания угроз см. Приложение Б. Устранение компьютерных угроз.

   При проверке файловой системы по запросу пользователя имеется возможность как полной проверки всех объектов файловой системы, доступных пользователю, так и выборочной проверки только указанных объектов (отдельных каталогов или файлов, соответствующих указанным критериям). Кроме того, доступна возможность отдельной проверки загрузочных записей томов и исполняемых файлов, из которых запущены процессы, активные в системе в данный момент. В последнем случае при обнаружении угрозы выполняется не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него. В системах, реализующих мандатную модель доступа к файлам с набором различных уровней доступа, сканирование файлов, недоступных на текущем уровне доступа, может производиться в специальном режиме автономного экземпляра.

   Все объекты с угрозами, обнаруженные в файловой системе, регистрируются в постоянно хранимом реестре угроз, за исключением тех угроз, которые были обнаружены в режиме автономного экземпляра.

   Утилита управления из командной строки Dr.Web Ctl, входящая в состав Dr.Web Server Security Suite, позволяет также выполнять проверку на наличие угроз файловых систем удаленных узлов сети, предоставляющих удаленный терминальный доступ через SSH или Telnet.

Вы можете использовать удаленное сканирование только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле используйте средства управления, предоставляемые непосредственно этим узлом. Например, на роутерах и прочих «умных» устройствах используйте механизмы обновления прошивки, а на вычислительных машинах — подключитесь к ним (в том числе в удаленном терминальном режиме) и произведите соответствующие операции в их файловой системе (удаление или перемещение файлов и т. п.) или запустите антивирусное программное обеспечение (ПО), установленное на них.

2. **Мониторинг обращений к файлам:**
   - **В файловой системе ОС.** Отслеживаются обращения к файлам с данными и попытки запуска исполняемых файлов. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках инфицирования ими файловой системы сервера. Помимо стандартного режима мониторинга имеется возможность включить усиленный («параноидальный») режим, в котором доступ к файлам будет блокироваться монитором до момента окончания их проверки (это позволяет предотвратить случаи доступа к файлу, когда он содержит угрозу, но результат его проверки становится известным уже после того, как приложение успело получить доступ к файлу). Усиленный режим мониторинга повышает уровень безопасности, но замедляет доступ приложений к еще не проверенным файлам.

     Функция мониторинга файловой системы доступна только для ОС семейства GNU/Linux. Для других ОС из списка поддерживаемых не поставляется компонент, предоставляющий эту возможность.

   - **В разделяемых каталогах Samba.** Отслеживаются обращения локальных и удаленных пользователей файлового сервера к файлам как на запись, так и на чтение. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках сохранения их в хранилище, что предотвращает их дальнейшее распространение по сети.
   - **На томах Novell Storage Services.** Отслеживаются обращения пользователей файлового хранилища NSS к файлам на запись. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках сохранения их в хранилище NSS, что предотвращает их дальнейшее распространение по сети.

     Функция мониторинга томов Novell Storage Services доступна только для Novell Open Enterprise Server SP2 на базе операционной системы SUSE Linux Enterprise Server 10 SP3 или более поздней версии. Для других ОС из списка поддерживаемых компонент, предоставляющий эту возможность, не поставляется.

3. **Надежная изоляция инфицированных или подозрительных объектов**, обнаруженных в файловой системе сервера, в специальном хранилище — карантине, чтобы они не могли нанести ущерба системе. При перемещении объектов в карантин

они специальным образом переименовываются и могут быть восстановлены в исходное место (в случае необходимости) только по команде пользователя.

4. **Автоматическое обновление** антивирусного ядра, содержимого вирусных баз для поддержания высокого уровня надежности защиты от вредоносных программ.
5. **Сбор статистики** проверок и инцидентов, связанных с вредоносным ПО. Ведение журнала обнаруженных угроз. Отправка уведомлений об обнаруженных угрозах по SNMP внешним системам мониторинга и серверу централизованной защиты, если Dr.Web Server Security Suite работает в режиме централизованной защиты, а также облачному сервису Dr.Web Cloud.
6. **Обеспечение работы под управлением сервера централизованной защиты** для применения на сервере единых политик безопасности, принятых в антивирусной сети под управлением Dr.Web Enterprise Security Suite, в состав которой он входит. Это может быть как сеть некоторого предприятия (корпоративная сеть) или частная сеть VPN, так и сеть, организованная провайдером каких-либо услуг, например, доступа в интернет.

3.2. Структура Dr.Web Server Security Suite

Dr.Web Server Security Suite представляет собой программный комплекс, состоящий из набора компонентов, каждый из которых выполняет свой набор функций. В соответствии с задачами, решаемыми компонентами, они разделены на категории:

- Базовые антивирусные компоненты, образующие ядро продукта Dr.Web Server Security Suite. При отсутствии компонентов этой категории продукт не может выполнять сканирование файлов (и иных данных) на предмет наличия вирусов и иных угроз.
- Компоненты поиска угроз. Данные компоненты используются для решения базовых задач Dr.Web Server Security Suite — поиска вредоносных и потенциально опасных объектов. В своей работе компоненты этой категории используют базовые антивирусные компоненты.
- Сервисные компоненты, решающие вспомогательные задачи для поддержки антивирусной защиты (обновление вирусных баз, подключение к серверам централизованной защиты, общая координация работы компонентов Dr.Web Server Security Suite и т. д.).
- Интерфейсные компоненты, предоставляющие (пользователю или сторонним приложениям) интерфейс для управления работой Dr.Web Server Security Suite.

Перечень компонентов, входящих в состав Dr.Web Server Security Suite, перечислен в таблицах ниже.

3.2.1. Базовые антивирусные компоненты

Компонент	Описание
Dr.Web Virus-Finding Engine	Антивирусное ядро. Реализует алгоритмы поиска и распознавания вирусов и прочих вредоносных программ (используя сигнатурный и эвристический анализ). Работает под управлением компонента Dr.Web Scanning Engine Файл библиотеки: `drweb32.dll`. Внутреннее наименование, выводимое в журнал: `CoreEngine`
Dr.Web Scanning Engine	Сканирующее ядро. Компонент, отвечающий за загрузку антивирусного ядра Dr.Web Virus-Finding Engine и вирусных баз. • Передает антивирусному ядру на проверку содержимое файлов и загрузочных записей дисковых устройств. • Организует очередь файлов, ожидающих проверки. • Выполняет лечение тех угроз, для которых данное действие применимо. Может работать как под управлением демона Dr.Web ConfigD, так и в автономном режиме. Используется компонентами Dr.Web File Checker и Dr.Web Network Checker. Также может использоваться компонентом Dr.Web MeshD (в некоторых режимах работы) и внешними (по отношению к Dr.Web Server Security Suite) приложениями, использующими непосредственно API Dr.Web Scanning Engine Исполняемый файл компонента: `drweb-se`. Внутреннее наименование, выводимое в журнал: `ScanEngine`
Вирусные базы	Автоматически обновляемая база данных сигнатур вирусов и прочих угроз, а также алгоритмов распознавания и нейтрализации вредоносного программного обеспечения. Используется антивирусным ядром Dr.Web Virus-Finding Engine и поставляется совместно с ним
Dr.Web File Checker	Компонент проверки объектов файловой системы и менеджер карантина. • Принимает от компонента поиска угроз задания на проверку файлов, находящихся в локальной (по отношению к Dr.Web Scanning Engine) файловой системе. • Обходит каталоги файловой системы согласно заданию, передает файлы на проверку сканирующему ядру Dr.Web Scanning Engine и оповещает компоненты-клиенты о ходе проверки. • Выполняет удаление инфицированных файлов, перемещение их в карантин и восстановление из карантина, управляет каталогами карантина.

Компонент	Описание
	• Организует и содержит в актуальном состоянии кеш, хранящий информацию о ранее проверенных файлах для уменьшения частоты повторных проверок файлов. Используется компонентами, проверяющими объекты файловой системы, такими как SpIDer Guard, SpIDer Guard для SMB, SpIDer Guard для NSS Исполняемый файл компонента: `drweb-filecheck`. Внутреннее наименование, выводимое в журнал: `FileCheck`
Dr.Web Network Checker	Агент сетевой проверки данных. • Используется для передачи на проверку в сканирующее ядро данных, отправленных компонентами программного комплекса через сеть (это такие компоненты, как Dr.Web ClamD). • Позволяет Dr.Web Server Security Suite организовывать распределенную проверку данных: принимать на проверку данные с удаленных узлов сети и передавать локальные данные на проверку на удаленные узлы сети. Для приема и передачи данных на удаленных узлах также должен функционировать антивирусный продукт Dr.Web для операционных систем семейства Unix. В режиме распределенной проверки позволяет автоматически распределять интенсивность антивирусного сканирования по доступным узлам, снижая нагрузку на узлы с большим объемом проверки (например, выполняющих роль почтовых серверов и интернет-шлюзов). При наличии в сети узлов-партнеров, способных принимать данные на проверку, компоненты, использующие Dr.Web Network Checker для проверки, могут не использовать мощности локального сканирующего ядра Dr.Web Scanning Engine. Таким образом, локальное сканирующее ядро Dr.Web Scanning Engine, Dr.Web Virus-Finding Engine и вирусные базы могут отсутствовать. Для обеспечения безопасности при передаче файлов по сети использует SSL Исполняемый файл компонента: `drweb-netcheck`. Внутреннее наименование, выводимое в журнал: `NetCheck`
Dr.Web MeshD	Компонент, осуществляющий подключение продукта Dr.Web Server Security Suite к локальному облаку, позволяющему продуктам Dr.Web для Unix обмениваться обновлениями, результатами проверки файлов, передавать друг другу на проверку файлы, а также предоставлять услуги сканирующего ядра напрямую. При наличии этого компонента в составе продукта и при наличии в составе локального облака, к которому он подключен, узлов, предоставляющих услуги сканирующего ядра, локальное сканирующее ядро Dr.Web Scanning Engine, Dr.Web Virus-Finding Engine и вирусные базы могут отсутствовать

Компонент	Описание
	Исполняемый файл компонента: `drweb-meshd`. Внутреннее наименование, выводимое в журнал: `MeshD`

3.2.2. Компоненты поиска угроз

Компонент	Описание
SplDer Guard	Монитор файловой системы GNU/Linux. Работает в фоновом режиме и отслеживает операции с файлами (такие как создание, открытие, закрытие и запуск файла) в файловых системах GNU/Linux. Посылает компоненту Dr.Web File Checker запросы на проверку содержимого новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ. В зависимости от возможностей ОС использует системный механизм *fanotify* или специализированный модуль ядра, разработанный компанией «Доктор Веб» (LKM-модуль, поставляется совместно с SplDer Guard в отдельном пакете). При работе через системный механизм *fanotify* монитор может работать в усиленном или «параноидальном» режиме, блокируя доступ к файлам, которые еще не проверены, до момента окончания их проверки. По умолчанию используется обычный режим мониторинга. Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Исполняемый файл компонента: `drweb-spider`. Внутреннее наименование, выводимое в журнал: `LinuxSpider`
Загружаемый модуль ядра Linux для SplDer Guard	Загружаемый модуль ядра Linux (LKM-модуль), используемый монитором SplDer Guard для доступа к событиям файловой системы в тех ОС, в которых API fanotify недоступен или реализован с ограниченным набором функций. Компонент поставляется как в скомпилированном виде (для набора ОС, в которых fanotify не реализован или недоступен), так и в виде исходного кода, позволяющего осуществить сборку и установку модуля ядра ОС вручную (инструкция по сборке приведена в разделе Использование модуля ядра для SplDer Guard). Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Для архитектур ARM64, E2K и IBM POWER (ppc64el) работа с модулем ядра не поддерживается.

Компонент	Описание
	Исполняемый файл компонента: `drweb.ko`
SpIDer Guard для SMB	Монитор разделяемых каталогов Samba. Работает в фоновом режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции чтения и записи) в каталогах, отведенных для файловых хранилищ SMB-сервера Samba. Посылает компоненту Dr.Web File Checker запросы на проверку содержимого новых и изменившихся файлов. Для интеграции с файловым сервером использует модули VFS SMB, работающие на стороне сервера Samba Исполняемый файл компонента: `drweb-smbspider-daemon`. Внутреннее наименование, выводимое в журнал: `SMBSpider`
SpIDer Guard для NSS	Монитор томов NSS (Novell Storage Services). Работает в фоновом режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции записи) на томах NSS, смонтированных в указанную точку файловой системы. Посылает компоненту Dr.Web File Checker запросы на проверку содержимого новых и изменившихся файлов. Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Работоспособен только в Novell Open Enterprise Server SP2 на базе операционной системы SUSE Linux Enterprise Server 10 SP3 или более поздних версий. Исполняемый файл компонента: `drweb-nss`. Внутреннее наименование, выводимое в журнал: `NSS`

3.2.3. Сервисные компоненты

Компонент	Описание
Dr.Web CloudD	Компонент взаимодействия с облаком Dr.Web Cloud. Отправляет URL, посещаемые пользователем, а также сведения о проверяемых файлах, в облачный сервис Dr.Web Cloud для их проверки на наличие угроз, информация о которых пока отсутствует в вирусных базах Исполняемый файл компонента: `drweb-cloudd`. Внутреннее наименование, выводимое в журнал: `CloudD`

Компонент	Описание
Dr.Web ConfigD	Демон управления конфигурацией комплекса Dr.Web Server Security Suite. • Управляет активностью (запуск и остановка) других компонентов программного комплекса в зависимости от настроек. • Перезапускает компоненты, завершившие работу в результате сбоя, запускает одни компоненты комплекса по требованию других, информирует компоненты продукта об изменении состава запущенных компонентов. • Хранит и предоставляет всем компонентам информацию об имеющихся лицензионных ключах и настройках. Получает измененные настройки и ключи от уполномоченных компонентов Dr.Web Server Security Suite и оповещает все компоненты об изменении лицензионных ключей и настроек Исполняемый файл компонента: `drweb-configd`. Внутреннее наименование, выводимое в журнал: `ConfigD`
Dr.Web ES Agent	Агент централизованной защиты. Обеспечивает работу программного комплекса в централизованном и мобильном режимах. • Организует связь с сервером централизованной защиты, получает от него лицензионный ключевой файл, обновления вирусных баз и антивирусного ядра. • Передает на сервер информацию о составе и состоянии компонентов Dr.Web Server Security Suite и накопленную статистику инцидентов, связанных с вредоносным ПО Исполняемый файл компонента: `drweb-esagent`. Внутреннее наименование, выводимое в журнал: `ESAgent`
Dr.Web StatD	Компонент для хранения статистики событий компонентов Dr.Web Server Security Suite. Получает и организует хранение событий, поступающих от компонентов программного комплекса, таких как неожиданное завершение работы, обнаружение угрозы и др. Исполняемый файл компонента: `drweb-statd`. Внутреннее наименование, выводимое в журнал: `StatD`
Dr.Web Updater	Компонент обновления. Отвечает за загрузку с серверов обновлений компании «Доктор Веб» обновлений для вирусных баз, антивирусного ядра. Обновления могут загружаться как автоматически, по расписанию, так и непосредственно по команде пользователя (через утилиту Dr.Web Ctl или через веб-интерфейс управления)

Компонент	Описание
	Исполняемый файл компонента: `drweb-update`. Внутреннее наименование, выводимое в журнал: `Update`

3.2.4. Интерфейсные компоненты

Компонент	Описание
Dr.Web HTTPD	Веб-сервер управления компонентами Dr.Web Server Security Suite. Предоставляет специализированный HTTP API для управления компонентами Dr.Web Server Security Suite. Указанный API используется веб-интерфейсом управления. Для обеспечения безопасности при подключении к веб-интерфейсу управления использует протокол HTTPS. Для передачи данных на проверку в Dr.Web Scanning Engine использует Dr.Web Network Checker Исполняемый файл компонента: `drweb-httpd`. Внутреннее наименование, выводимое в журнал: `HTTPD`
Веб-интерфейс управления Dr.Web	Веб-интерфейс управления. Может быть открыт в любом браузере на локальном или удаленном узле сети. Наличие веб-интерфейса управления позволяет продукту не использовать сторонние веб-серверы (такие, например, как Apache HTTP Server) и утилиты удаленного администрирования наподобие Webmin. Работоспособность обеспечивается веб-сервером Dr.Web HTTPD
Dr.Web Ctl	Утилита, обеспечивающая интерфейс управления Dr.Web Server Security Suite из командной строки. Позволяет осуществлять запуск проверки файлов, просматривать содержимое карантина и управлять им, запускать обновление вирусных баз, подключать Dr.Web Server Security Suite к серверу централизованной защиты и отключаться от него, просматривать и изменять значения параметров конфигурации программного комплекса Исполняемый файл компонента: `drweb-ctl`. Внутреннее наименование, выводимое в журнал: `Ctl`
Dr.Web SNMPD	Представляет собой SNMP-агент. Предназначен для интеграции Dr.Web Server Security Suite с внешними системами мониторинга посредством протокола SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов комплекса, а также собирать статистику обнаружения и нейтрализации угроз.

Компонент	Описание
	Поддерживает протоколы SNMP v2c и v3 Исполняемый файл компонента: `drweb-snmpd`. Внутреннее наименование, выводимое в журнал: `SNMPD`
Dr.Web ClamD	Компонент, эмулирующий интерфейс антивирусного демона `clamd` (компонент антивирусного продукта ClamAV®). Позволяет прозрачно использовать Dr.Web Server Security Suite для антивирусной проверки любым приложениям, которые могут использовать антивирусный продукт ClamAV®. Для передачи данных на проверку в Dr.Web Scanning Engine, в зависимости от режима, использует Dr.Web File Checker или Dr.Web Network Checker Исполняемый файл компонента: `drweb-clamd`. Внутреннее наименование, выводимое в журнал: `ClamD`

На рисунке ниже показана структура Dr.Web Server Security Suite и его взаимодействия с внешними приложениями.

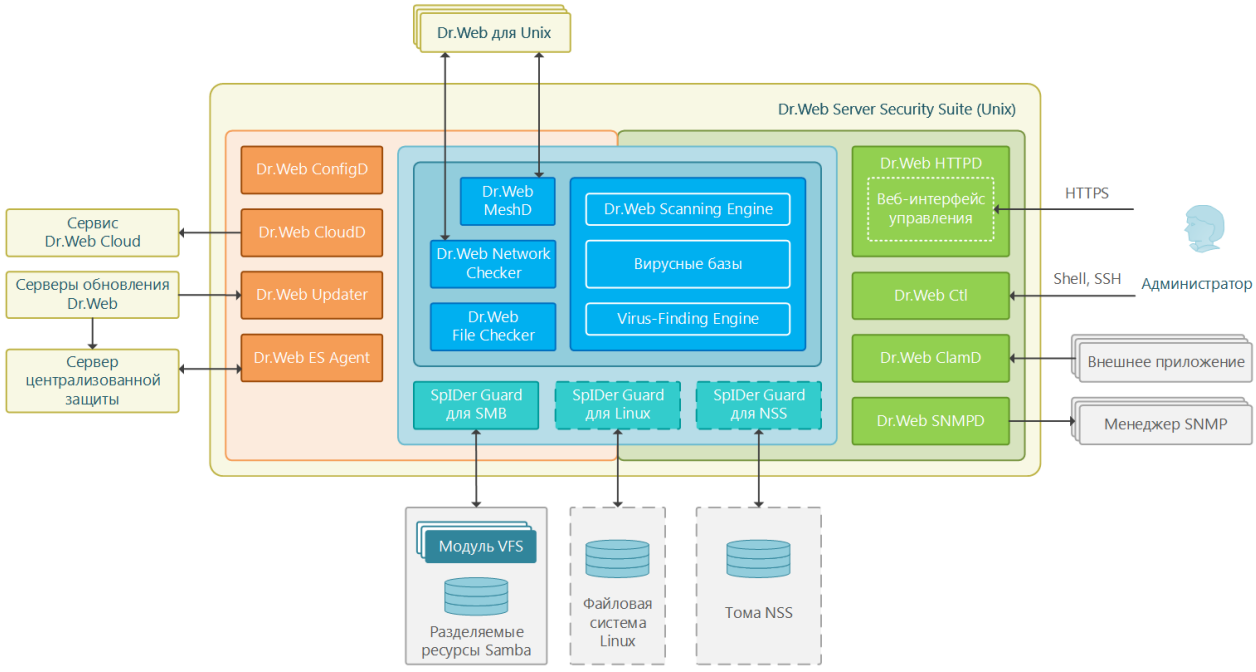


Рисунок 1. Структура Dr.Web Server Security Suite

На приведенном рисунке использованы следующие обозначения:

	Dr.Web Server Security Suite в целом и внешние по отношению к нему программные продукты Dr.Web, не входящие непосредственно в его состав
	Внешние по отношению к Dr.Web Server Security Suite программы и программные комплексы, с которыми он интегрируется

	Сервисные компоненты, решающие конкретные задачи в рамках антивирусной защиты (обновление вирусных баз, подключение к серверам централизованной защиты, общая координация работы и т. д.)
	Компоненты, предоставляющие (пользователю или сторонним приложениям) интерфейс для управления работой Dr.Web Server Security Suite
	Компоненты, используемые для антивирусной проверки
	Базовые антивирусные компоненты, образующие ядро Dr.Web Server Security Suite. Используются компонентами, осуществляющими проверку файлов и данных

Компоненты, обозначенные пунктирной границей, могут отсутствовать, в зависимости от поставки или сценария использования Dr.Web Server Security Suite.

Более подробно компоненты Dr.Web Server Security Suite описаны в разделе Компоненты Dr.Web Server Security Suite.

3.3. Помещение в карантин

Карантин Dr.Web Server Security Suite представляет собой систему каталогов, предназначенных для надежной изоляции файлов, содержащих выявленные угрозы, которые в данный момент не могут быть обезврежены по каким-либо причинам. Например, обнаруженная угроза может быть неизлечимой, потому что еще неизвестна Dr.Web Server Security Suite (например, она была обнаружена эвристическим анализатором, а в вирусных базах ее сигнатура, а следовательно, и метод лечения, отсутствует), или при попытке ее лечения возникают ошибки. Кроме того, файл может быть перемещен в карантин непосредственно по желанию пользователя, если он выбрал соответствующее действие в списке обнаруженных угроз или указал его как реакцию на угрозы определенного типа.

Когда файл, содержащий угрозу, перемещается в карантин, он специальным образом переименовывается, чтобы предотвратить возможность его идентификации пользователями и программами, и затруднить доступ к нему, минуя инструменты работы с карантином, реализованные в Dr.Web Server Security Suite. Кроме того, при перемещении файла в карантин у него всегда сбрасывается бит исполнения для предотвращения запуска.

Каталоги карантина размещаются:

- *в домашнем каталоге пользователя* (если на данном компьютере имеется несколько учетных записей разных пользователей, то в домашнем каталоге каждого из этих пользователей может быть создан свой собственный каталог карантина);
- *в корневом каталоге каждого логического тома,* смонтированного в файловой системе.

Каталоги карантина Dr.Web Server Security Suite всегда имеют имя `.com.drweb.quarantine` и создаются по мере необходимости в тот момент, когда к

какой-либо угрозе применяется действие «**В карантин**» (`QUARANTINE`), другими словами, до тех пор, пока угроз не обнаружено, каталоги карантина не создаются. При этом всегда создается только тот каталог карантина, который требуется для изоляции файла. Для определения, в какой из каталогов требуется изолировать файл, используется имя владельца файла. Если при движении к корню файловой системы `/` от каталога, содержащего файл, достигается домашний каталог владельца, файл изолируется в каталог карантина, находящийся в нем. В противном случае файл будет изолирован в каталог карантина, созданный в корне тома, содержащего файл (корневой каталог тома необязательно совпадет с корнем файловой системы). Таким образом, любой инфицированный файл, помещаемый в карантин, всегда остается на том томе, на котором он был обнаружен. Это обеспечивает корректную работу карантина при наличии в системе съемных накопителей и других томов, которые могут монтироваться в файловой системе периодически и в различные точки.

Пользователь может управлять содержимым карантина из командной строки, используя утилиту Dr.Web Ctl или через веб-интерфейс управления. При этом всегда обрабатывается консолидированный карантин, объединяющий в себе все каталоги с изолированными объектами, доступные в данный момент. С точки зрения пользователя, просматривающего содержимое консолидированного карантина, каталог карантина, располагающийся в его домашнем каталоге, называется *Пользовательским* карантином, а все остальные каталоги карантина считаются *Системным* карантином.



Работа с карантином возможна даже тогда, когда отсутствует активная лицензия, но в этом случае становится невозможным лечение изолированных объектов.

Не все антивирусные компоненты Dr.Web Server Security Suite используют карантин для изоляции угроз. Например, его не использует компонент Dr.Web ClamD.

3.4. Полномочия для работы с файлами

При сканировании объектов файловой системы и нейтрализации угроз Dr.Web Server Security Suite (точнее, пользователь, от имени которого он запущен) должен обладать следующими полномочиями:

Действие	**Требуемые полномочия**
Вывод всех обнаруженных угроз	Без ограничений. Специальных полномочий не требуется.
Вывод содержимого контейнера (архива, почтового файла и т. п.) (Отображение только элементов, которые	Без ограничений. Специальных полномочий не требуется.

Действие	Требуемые полномочия
содержат ошибку или угрозу)	
Перемещение в карантин	Без ограничений. Пользователь может отправлять в карантин все инфицированные файлы, независимо от наличия у него прав на чтение и запись для перемещаемого файла.
Удаление угроз	Пользователь должен иметь права на запись в удаляемый файл. Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т. п.), вместо удаления выполняется перемещение контейнера в карантин.
Лечение файлов	Без ограничений. После выполнения лечения остается вылеченный файл с исходными правами доступа и владельцем. Файл может быть удален, если удаление является методом лечения обнаруженной в нем угрозы.
Восстановление файла из карантина	Пользователь должен иметь разрешение на чтение восстанавливаемого файла и иметь разрешение выполнять запись в каталог восстановления.
Удаление файла из карантина	Пользователь должен иметь разрешение на запись в исходный файл, который был перемещен в карантин.

Для запуска утилиты управления из командной строки Dr.Web Ctl с правами суперпользователя (обычно *root*) используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

3.5. Режимы работы

В этом разделе

- Принципы централизованной защиты
- Подключение к серверу централизованной защиты
- Отключение от сервера централизованной защиты

Dr.Web Server Security Suite может работать как в автономном режиме, так и в составе корпоративной или частной *антивирусной сети*, управляемой каким-либо *сервером централизованной защиты*. Такой режим работы называется *режимом централизованной защиты*. Использование этого режима не требует установки дополнительного программного обеспечения, переустановки или удаления Dr.Web Server Security Suite.

- В *автономном режиме* защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационный и лицензионный ключевой файлы находятся на локальных дисках, а Dr.Web Server Security Suite полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов обновлений компании «Доктор Веб».
- В *режиме централизованной защиты* защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки Dr.Web Server Security Suite могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты, принятой в антивирусной сети. В этом режиме на компьютере используется особый лицензионный ключевой файл, полученный от выбранного сервера централизованной защиты, к которому подключен Dr.Web Server Security Suite. Лицензионный или демонстрационный ключевой файл пользователя, если он имеется на локальном компьютере, не используется. На сервер централизованной защиты отсылается статистика работы Dr.Web Server Security Suite, включая статистику инцидентов, связанных с вредоносным ПО. Обновление вирусных баз также выполняется с сервера централизованной защиты. Настройка режима централизованной защиты описана в Руководстве администратора Dr.Web Enterprise Security Suite по управлению Dr.Web Server Security Suite.
- В *мобильном режиме* Dr.Web Server Security Suite получает обновления вирусных баз с серверов обновлений компании «Доктор Веб», но использует локально хранящиеся настройки и особый лицензионный ключевой файл, полученные от сервера централизованной защиты.

Возможность настройки монитора файловой системы SplDer Guard, а также его включения и выключения при работе Dr.Web Server Security Suite под управлением сервера централизованной защиты зависит от разрешений, заданных на сервере.

Принципы централизованной защиты

Решения компании «Доктор Веб» по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (см. иллюстрацию ниже).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз *локальными антивирусными компонентами* (в данном случае продуктом Dr.Web Server Security Suite), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.



Рисунок 2. Логическая структура антивирусной сети

Обновление и конфигурация локальных компонентов производится через *сервер централизованной защиты*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и сервером централизованной защиты может быть весьма значительным, поэтому предусматривается возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

Все необходимые обновления загружаются на сервер централизованной защиты с серверов обновлений компании «Доктор Веб».

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется сервером централизованной защиты по указанию администраторов

антивирусной сети. Администраторы управляют конфигурацией сервера централизованной защиты и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также, при необходимости, задают настройки работы конкретных локальных антивирусных компонентов.



Локальные антивирусные компоненты несовместимы с антивирусным программным обеспечением как других компаний, так и антивирусными решениями Dr.Web, не поддерживающими режим централизованной защиты (например, антивирус Dr.Web версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы или потере важных данных.

В режиме централизованной защиты возможен экспорт и сохранение отчетов о функционировании Dr.Web Server Security Suite с помощью сервера централизованной защиты. Поддерживается экспорт и сохранение отчетов в форматах HTML, CSV, PDF и XML.

Подключение к серверу централизованной защиты

Dr.Web Server Security Suite может быть подключен к серверу централизованной защиты антивирусной сети при помощи команды `esconnect` утилиты управления из командной строки `drweb-ctl`.



Для верификации сервера централизованной защиты используется сертификат, соответствующий уникальному открытому ключу шифрования, используемому сервером. По умолчанию агент централизованной защиты Dr.Web ES Agent не позволит произвести подключение к серверу, если вы не укажете файл сертификата сервера, к которому производится подключение. Файл сертификата необходимо предварительно получить у администратора антивирусной сети, обслуживаемой сервером, к которому вы хотите подключить Dr.Web Server Security Suite.

Если Dr.Web Server Security Suite подключен к серверу централизованной защиты, то имеется возможность перевести его в мобильный режим и вернуть назад в режим централизованной защиты. Включение и выключение мобильного режима регулируется параметром конфигурации `MobileMode` компонента Dr.Web ES Agent.



Возможность перехода Dr.Web Server Security Suite в мобильный режим работы зависит от разрешений, заданных на используемом сервере централизованной защиты.

Отключение от сервера централизованной защиты

Dr.Web Server Security Suite может быть отключен от сервера централизованной защиты антивирусной сети при помощи команды `esdisconnect` утилиты управления из командной строки `drweb-ctl`.

4. Системные требования и совместимость

В этом разделе

- Системные требования
- Перечень поддерживаемых версий операционных систем
  - GNU/Linux
  - FreeBSD
- Требуемые дополнительные пакеты и компоненты
- Ограничения совместимости
- Поддерживаемые файловые серверы
  - Файловая служба Samba
  - Файловая служба NSS
- Совместимость с подсистемами безопасности

Системные требования

Использование Dr.Web Server Security Suite возможно на компьютере, удовлетворяющем следующим требованиям:

Параметр	Требования
Платформа	Поддерживаются процессоры следующих архитектур и систем команд: • Intel/AMD: 32-бит (*IA-32*, *x86*); 64-бит (*x86-64*, *x64*, *amd64*); • ARM64; • E2K (*Эльбрус*); • IBM POWER9, Power10 (*ppc64el*)
Оперативная память	Не менее 500 МБ свободной оперативной памяти (рекомендуется 1 ГБ и более)
Место на жестком диске	Не менее 2 ГБ свободного дискового пространства на томе, на котором размещаются каталоги устанавливаемого продукта
Операционная система	GNU/Linux (на основе ядра версии 2.6.37 или более поздней, использующая библиотеку `glibc` версии 2.13 или более поздней, систему инициализации `systemd` версии 209 или более позднюю), FreeBSD. Перечень поддерживаемых версий операционных систем приведен ниже. Операционная система должна поддерживать механизм аутентификации PAM
Прочее	Наличие сетевого подключения: • подключение к интернету для обновления вирусных баз и компонентов антивирусного продукта;

Параметр	Требования
	• при работе в режиме централизованной защиты достаточно только подключения к используемому серверу в рамках локальной сети, доступ в интернет не требуется

Для обеспечения правильной работы Dr.Web Server Security Suite должны быть открыты следующие порты:

Назначение	Направление	Номера портов
Для получения обновлений	исходящий	80
Для соединения с облачным сервисом Dr.Web Cloud	исходящий	2075 (в том числе для UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

Перечень поддерживаемых версий операционных систем

GNU/Linux

Платформа	Поддерживаемые версии GNU/Linux
x86_64	• Astra Linux Common Edition (Орел) 2.12; • Astra Linux Special Edition 1.6 (с кумулятивным патчем 20200722SE16), 1.7, 1.8; • CentOS 7, 8; • Debian 9, 10, 11, 12, 13; • Fedora 37, 38; • Red Hat Enterprise Linux 7, 8, 9; • SUSE Linux Enterprise Server 12 SP3; • Ubuntu 18.04, 20.04, 22.04, 24.04; • Альт 8 СП; • Альт Рабочая станция 9, 10, 11; • Альт Сервер 9, 10, 11; • Гослинукс IC6; • РЕД ОС 7.2 МУРОМ, РЕД ОС 7.3 МУРОМ, РЕД ОС 8
x86	• CentOS 7; • Debian 10; • Альт 8 СП; • Альт Рабочая станция 9, 10

Платформа	Поддерживаемые версии GNU/Linux
ARM64	• Astra Linux Special Edition (Новороссийск) 4.7; • CentOS 7, 8; • Debian 11, 12; • Ubuntu 18.04; • Альт 8 СП; • Альт Рабочая станция 9, 10, 11; • Альт Сервер 9, 10, 11
E2K	• Astra Linux Special Edition (Ленинград) 8.1 (с кумулятивным патчем 20200429SE81); • Альт 8 СП; • Альт Рабочая станция 10; • Альт Сервер 10; • ОПО ВК Эльбрус-8.32 ТВГИ.00311-28; • Эльбрус-Д МЦСТ 1.4
ppc64el	• CentOS 8; • Ubuntu 20.04



В ОС Альт 8 СП, Эльбрус-Д МЦСТ 1.4 и Гослинукс IC6 работа с мандатными уровнями доступа не поддерживается.

Для прочих версий GNU/Linux, соответствующих описанным требованиям, полная совместимость с Dr.Web Server Security Suite не гарантируется. При возникновении проблем с совместимостью с вашим дистрибутивом обратитесь в техническую поддержку.

FreeBSD

Платформа	Поддерживаемые версии FreeBSD
x86	11, 12, 13, 14
x86_64	11, 12, 13, 14, 15



Для ОС FreeBSD установка Dr.Web Server Security Suite возможна только из универсального пакета.

Для корректной работы Dr.Web Server Security Suite в ОС FreeBSD 13, 14 и 15 необходимо установить пакет совместимости `compat12x`.

Требуемые дополнительные пакеты и компоненты

Dr.Web Server Security Suite не требует установки дополнительных пакетов и компонентов ОС (кроме программного обеспечения защищаемого серверного решения, см. ниже).

Для удобной работы с Dr.Web Server Security Suite из командной строки рекомендуется включить автодополнение команд в используемой командной оболочке, если оно не включено.

В случае возникновения проблем с установкой требуемых дополнительных пакетов и компонентов обратитесь к справочным руководствам используемой вами версии операционной системы.

Ограничения совместимости

- Работа SpIDer Guard с использованием модуля ядра (LKM-модуля) *не поддерживается* для ОС, запущенных в среде гипервизора Xen. Попытка загрузки модуля ядра SpIDer Guard при работе ОС в среде Xen может привести к критической ошибке ядра ОС (т. н. ошибка *«Kernel panic»*).
- Работа SpIDer Guard с использованием модуля ядра (LKM-модуля) *не поддерживается* для архитектур ARM64, E2K и IBM POWER (ppc64el).
- Работа SpIDer Guard в усиленном («параноидальном») режиме с предварительной блокировкой доступа к еще не проверенным файлам возможна *только* через fanotify и при условии, что ядро ОС собрано с активной опцией `CONFIG_FANOTIFY_ACCESS_PERMISSIONS`.

Поддерживаемые файловые серверы

Файловая служба Samba

Для интеграции с файловой службой Samba требуется установленный и настроенный сервер Samba одной из следующих версий: 3.6–4.24.

Монитор SpIDer Guard для SMB, входящий в состав Dr.Web Server Security Suite, использует для интеграции с Samba специальный модуль VFS SMB. Совместно с компонентом SpIDer Guard для SMB поставляется несколько версий модуля VFS SMB, собранных для различных версий Samba, однако они могут оказаться несовместимы с версией Samba, установленной на вашем файловом сервере, например, если установленный у вас сервер Samba использует опцию `CLUSTER_SUPPORT`.

В случае несовместимости поставляемых модулей VFS SMB с вашим сервером Samba, в процессе установки Dr.Web Server Security Suite на экран *будет выдано соответствующее сообщение*. В этом случае перед интеграцией необходимо выполнить процедуру сборки модуля VFS SMB для вашего сервера Samba, включая поддержку опции `CLUSTER_SUPPORT`, если это требуется.

Процедура сборки модуля VFS SMB из исходного кода описана в разделе Сборка модуля VFS SMB.

Файловая служба NSS

Для интеграции с файловой службой Novell Storage Services (NSS) требуется Novell Open Enterprise Server SP2 на базе операционной системы SUSE Linux Enterprise Server 10 SP3 или более поздних версий (11 SP1, SP2).

Совместимость с подсистемами безопасности

При настройках по умолчанию Dr.Web Server Security Suite не совместим с подсистемой безопасности SELinux. Кроме того, по умолчанию Dr.Web Server Security Suite работает в режиме ограниченной функциональности в системах GNU/Linux, использующих мандатные модели доступа (например, в системах, оснащенных подсистемой мандатного доступа PARSEC, основанной на присвоении пользователям и файлам различных уровней привилегий, называемых мандатными уровнями).

В случае необходимости установки Dr.Web Server Security Suite в системы с SELinux (а также в системы, использующие мандатные модели доступа) необходимо выполнить дополнительные настройки подсистемы безопасности для снятия ограничений в функционировании Dr.Web Server Security Suite. Подробнее см. в разделе Настройка подсистем безопасности.

5. Лицензирование

Права пользователя на использование копии Dr.Web Server Security Suite подтверждаются и регулируются лицензией, приобретенной пользователем у компании «Доктор Веб» или ее партнеров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением, условия которого принимаются пользователем при установке Dr.Web Server Security Suite на свой компьютер. В лицензии фиксируется информация о пользователе и продавце, а также параметры использования приобретенной копии продукта, в частности:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование Dr.Web Server Security Suite;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать приобретенную копию Dr.Web Server Security Suite).

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а на локальном компьютере с лицензией связывается специальный файл, регулирующий работу компонентов Dr.Web Server Security Suite в соответствии с параметрами лицензии. Он называется *лицензионным ключевым файлом*.

Для предварительного ознакомления с возможностями продукта вы можете активировать *демонстрационный период*. При активации демонстрационного периода вы получаете право на полноценное использование установленной копии Dr.Web Server Security Suite в течение всего этого периода, если не нарушены условия его активации. При этом также автоматически формируется специальный ключевой файл, называемый *демонстрационным*.

При отсутствии действующей лицензии или активированного демонстрационного периода (в том числе, если срок действия ранее приобретенной лицензии или демонстрационный период истек), антивирусные функции Dr.Web Server Security Suite блокируются, кроме того, сервис регулярных обновлений вирусных баз Dr.Web с серверов обновлений компании «Доктор Веб» становится недоступным. Однако имеется возможность активировать Dr.Web Server Security Suite, подключив его к серверу централизованной защиты антивирусной сети предприятия или антивирусной сети, организованной интернет-провайдером. В этом случае управление антивирусными функциями и обновлениями копии продукта, установленной на компьютере в составе антивирусной сети, возлагается на сервер централизованной защиты.

6. Установка и удаление

В этом разделе описываются процедуры установки и удаления Dr.Web Server Security Suite, а также процедура получения текущих обновлений и процедура перехода на новую версию, если на вашем компьютере уже установлен Dr.Web Server Security Suite более ранней версии.

Кроме этого, в этом разделе описана процедура выборочной установки и удаления компонентов Dr.Web Server Security Suite (например, для устранения ошибок, возникших в процессе эксплуатации Dr.Web Server Security Suite, или для установки продукта с ограниченным набором функций) и настройка расширенных подсистем безопасности (таких как SELinux), что может потребоваться при установке или в процессе эксплуатации Dr.Web Server Security Suite.

Для осуществления этих операций необходимы права суперпользователя (обычно пользователя *root*). Для получения прав суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.



Не гарантируется совместимость Dr.Web Server Security Suite с антивирусными программами других производителей. Так как установка двух антивирусов на один компьютер может привести к ошибкам в работе операционной системы и потере важных данных, перед установкой Dr.Web Server Security Suite настоятельно рекомендуется удалить с компьютера антивирусные программы других производителей.

Если на вашем компьютере уже имеется другой антивирусный продукт Dr.Web, установленный из универсального пакета (`.run`), и вы желаете установить еще один антивирусный продукт Dr.Web (например, у вас из универсального пакета установлен продукт Dr.Web Desktop Security Suite, и вы хотите в дополнение к нему установить Dr.Web Server Security Suite), то предварительно убедитесь, что версия уже установленного продукта совпадает с версией Dr.Web Server Security Suite, которую вы планируете установить. Если версия, которую вы собираетесь установить, новее, чем версия продукта, который уже установлен на вашем компьютере, перед началом установки дополнительного продукта обновите уже установленный продукт до версии Dr.Web Server Security Suite, которую вы хотите установить дополнительно.

Для ОС FreeBSD установка Dr.Web Server Security Suite возможна только из универсального пакета.

Дополнительно:

- Установка Dr.Web Server Security Suite
- Обновление Dr.Web Server Security Suite
- Удаление Dr.Web Server Security Suite
- Настройка подсистем безопасности
- Пакеты и файлы Dr.Web Server Security Suite

- Выборочные установка и удаление компонентов

6.1. Установка Dr.Web Server Security Suite

Вы можете установить Dr.Web Server Security Suite одним из двух способов:

1. Загрузив с сайта компании «Доктор Веб» установочный файл, представляющий собой универсальный пакет для Unix-систем, снабженный программой установки в режиме командной строки. Для ее работы в режиме графического рабочего стола необходимо наличие эмулятора терминала.
2. Выполнив установку Dr.Web Server Security Suite в виде набора нативных пакетов (для этого потребуется подключиться к соответствующему репозиторию пакетов компании «Доктор Веб»).



Для ОС FreeBSD установка Dr.Web Server Security Suite возможна только из универсального пакета.

Для корректной работы Dr.Web Server Security Suite в ОС FreeBSD 13, 14 и 15 необходимо установить пакет совместимости `compat12x`.

В Альт 8 СП и других ОС, использующих устаревшие версии пакетного менеджера, рекомендуется устанавливать Dr.Web Server Security Suite из универсального пакета.

После установки Dr.Web Server Security Suite подсистема IMA/EVM ОС Альт 8 СП 11100-01 может выдавать предупреждение о возможном нарушении целостности. Чтобы избежать этого предупреждения, после установки Dr.Web Server Security Suite выполните команду:

```
# integalert fix
```

ОС Альт 8 СП 11100-02 и ОС Альт 8 СП 11100-03 не подвержены этой проблеме.



После установки Dr.Web Server Security Suite любым из указанных в этом руководстве способов в начале работы вам потребуется активировать лицензию или установить ключевой файл. Кроме того, вы можете подключить Dr.Web Server Security Suite к серверу централизованной защиты (подробнее см. раздел Лицензирование). До тех пор, пока вы этого не сделаете, *функции антивирусной защиты будут отключены.* Кроме того, в ряде случаев необходимо выполнить основную настройку базовой функциональности Dr.Web Server Security Suite, как описано в разделе Начало работы.

В процессе работы программы установки (как из универсального пакета `.run`, так и из нативных пакетов при помощи пакетного менеджера), на локальный почтовый адрес `root@localhost` отправляются сообщения электронной почты, содержащие результаты установки Dr.Web Server Security Suite.

Dr.Web Server Security Suite, установленный любым из рассмотренных в этом разделе способов, вы можете впоследствии удалить или обновить при наличии исправлений для входящих в него компонентов или выходе новой версии Dr.Web Server Security Suite. При необходимости выполните также настройку подсистем безопасности GNU/Linux для корректной работы Dr.Web Server Security Suite. При возникновении проблем с функционированием отдельных компонентов вы можете выполнить их выборочную установку и удаление, не удаляя Dr.Web Server Security Suite целиком.

6.1.1. Установка универсального пакета

Универсальный пакет Dr.Web Server Security Suite распространяется в виде установочного файла с именем `drweb-<версия>-av-srv-<ОС>-<платформа>.run`, где <*ОС*> — Unix-подобная операционная система, а <*платформа*> — строка, указывающая тип платформы, для которой предназначен Dr.Web Server Security Suite (для 32-битных платформ — `x86`, для 64-битных платформ — `amd64`, `arm64`, `e2s` и `ppc64el`), например:

```
drweb-11.1.0-av-srv-linux-amd64.run
```

Далее в данном разделе руководства имя установочного файла, соответствующее формату, указанному выше, обозначается как <*имя файла .run*>, а путь к этому файлу — как <*путь к файлу .run*>.

Версия Dr.Web Server Security Suite определяется первыми двумя числами, разделенными точкой, в имени универсального пакета.

Чтобы установить компоненты Dr.Web Server Security Suite

1. Если у вас отсутствует установочный файл (универсальный пакет), загрузите его с официального сайта компании «Доктор Веб».
2. Сохраните установочный файл на жесткий диск компьютера в любой доступный для записи каталог (например, `/home/`<*username*>, где <*username*> — имя текущего пользователя).
3. Разрешите исполнение файла, например, командой:

   ```
   # chmod +x <путь к файлу .run>
   ```

4. Запустите его на выполнение командой:

   ```
   # <путь к файлу .run>
   ```

   или воспользуйтесь стандартным файловым менеджером вашей графической оболочки как для изменения свойств файла (прав доступа), так и для его запуска.



В случае установки Dr.Web Server Security Suite в среде ОС Astra Linux SE версий 1.6 и 1.7, работающей в режиме *замкнутой программной среды* (ЗПС), может произойти отказ в запуске программы установки из-за отсутствия открытого ключа компании «Доктор Веб» в списке доверенных ключей. В этом случае необходимо выполнить предварительную настройку режима ЗПС (см. Настройка запуска в режиме ЗПС (Astra Linux SE, версии 1.6 и 1.7)), после чего запустить программу установки повторно.

При этом будет проверена целостность архива, затем файлы, содержащиеся в архиве, будут распакованы во временный каталог и автоматически запустится программа установки. Если запуск был осуществлен не с правами суперпользователя, то программа установки автоматически попытается повысить свои права, запросив пароль (используется утилита `sudo`). Если попытка повышения прав окончится неудачей, установка будет отменена.



Если раздел файловой системы, содержащий временный каталог, не имеет достаточного количества свободного места для распаковки дистрибутива, процесс установки будет завершен после выдачи соответствующего сообщения. В этом случае повторите распаковку, изменив значение системной переменной окружения `TMPDIR` таким образом, чтобы она указывала на каталог в разделе файловой системы, имеющем достаточное количество свободного места. Также вы можете воспользоваться ключом распаковки в указанный каталог `--target` (см. раздел Выборочные установка и удаление компонентов).

После этого запустится программа установки для режима командной строки (для ее работы в режиме графического рабочего стола необходимо наличие эмулятора терминала).

5. Следуйте инструкциям программы установки.

Имеется возможность запустить программу установки в полностью автоматическом режиме, выполнив команду:

```
# <путь к файлу .run> -- --non-interactive
```

В этом случае программа установки будет запущена в полностью автоматическом режиме, без показа диалогов программы установки для режима командной строки.

Использование этой опции означает, что вы соглашаетесь с условиями Лицензионного соглашения Dr.Web. Ознакомиться с текстом Лицензионного соглашения после установки Dr.Web Server Security Suite вы можете, прочитав файл `/opt/drweb.com/share/doc/LICENSE` для GNU/Linux или `/usr/local/libexec/drweb.com/share/doc/LICENSE` для FreeBSD. Расширение файла указывает язык, на котором написан текст Лицензионного соглашения. Файл `LICENSE` (без расширения) хранит текст Лицензионного соглашения Dr.Web на английском языке. Если вы не согласны с условиями Лицензионного соглашения, вам следует удалить Dr.Web Server Security Suite после установки.

Запуск программы установки в полностью автоматическом режиме требует наличия прав суперпользователя (обычно пользователя *root*). Для повышения прав вы можете использовать команду `su` или `sudo`.

Если ваш дистрибутив GNU/Linux оснащен подсистемой безопасности SELinux, то возможно возникновение ситуации, когда работа программы установки будет прервана подсистемой безопасности. В этом случае вам необходимо временно перевести SELinux в *разрешающий (Permissive)* режим, для чего выполните команду:

```
# setenforce 0
```

После этого перезапустите программу установки. Также в этом случае по окончании процесса установки необходимо выполнить настройку политик безопасности SELinux, чтобы в дальнейшем антивирусные компоненты работали корректно.

Все установочные файлы, извлеченные из архива, будут автоматически удалены по окончании установки.

Рекомендуется сохранить файл `.run`, из которого производилась установка, для возможной переустановки Dr.Web Server Security Suite или его компонентов в последующем, без обновления его версии.

6.1.1.1. Установка в режиме командной строки

После запуска программы установки, работающей в режиме командной строки, на экране появится текст приглашения к установке.

1. Для начала установки ответьте `Yes` или `Y` на запрос «Вы хотите продолжить?». Чтобы отказаться от установки, введите `No` или `N`. В этом случае работа программы установки будет завершена.
2. Далее перед началом установки вам необходимо ознакомиться с текстом Лицензионного соглашения компании «Доктор Веб», который будет выведен на экран. Для перелистывания текста соглашения пользуйтесь клавишами ENTER (перелистывание текста на одну строчку вниз) и ПРОБЕЛ (перелистывание текста вниз на экран).

Перелистывание текста Лицензионного соглашения назад (вверх) не предусмотрено.

3. После прочтения Лицензионного соглашения вам будет предложено принять его условия. Введите `Yes` или `Y`, если вы принимаете условия, и `No` или `N`, если вы не согласны с условиями Лицензионного соглашения. В случае отказа от принятия условий Лицензионного соглашения работа программы установки будет завершена.
4. После принятия условий Лицензионного соглашения автоматически будет запущен процесс установки на компьютер компонентов Dr.Web Server Security Suite. При этом на экран будет выводиться информация о ходе установки (журнал установки), включающая в себя перечень устанавливаемых компонентов.
5. В случае успешного окончания процесса установки на экране появится информационное сообщение, содержащее инструкции по способам управления работой Dr.Web Server Security Suite.

В случае возникновения ошибки на экран будет выведено соответствующее сообщение с описанием ошибки, после чего работа программы установки будет завершена. Если установка была прервана из-за ошибки, устраните проблемы, вызвавшие ошибку установки, и повторите процесс установки заново.

6.1.2. Установка из репозитория

Нативные пакеты Dr.Web Server Security Suite находятся в официальном репозитории Dr.Web. После добавления репозитория Dr.Web в список репозиториев, используемых менеджером пакетов вашей операционной системы, вы сможете устанавливать его в виде нативных пакетов для операционной системы так же, как и любые другие программы из репозиториев вашей операционной системы. Необходимые зависимости будут разрешаться автоматически. Кроме того, при установке Dr.Web Server Security Suite из подключенного репозитория пакетный менеджер ОС обнаруживает обновления всех компонентов Dr.Web и предлагает их установку.

Для доступа к репозиторию Dr.Web требуется подключение к интернету.

Все нижеприведенные команды для подключения репозиториев, импортирования ключей, установки и удаления пакетов должны быть выполнены с правами суперпользователя (обычно пользователя *root*). Для получения соответствующих прав используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Для ОС FreeBSD установка Dr.Web Server Security Suite возможна только из универсального пакета.

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

- Astra Linux, Debian, Mint, Ubuntu (apt);

- Альт (apt-rpm);
- Mageia, OpenMandriva Lx (urpmi);
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf);
- SUSE Linux (zypper).

Astra Linux, Debian, Mint, Ubuntu (apt)

1. Репозиторий для этих ОС защищен цифровой подписью «Доктор Веб». Для доступа к репозиторию импортируйте и добавьте в хранилище пакетного менеджера ключ цифровой подписи, выполнив команду:

```
# wget https://repo.drweb.com/drweb/drweb.gpg -O /etc/apt/trusted.gpg.d/drweb.gpg
```

> Ключ цифровой подписи «Доктор Веб» ранее устанавливался с помощью утилиты `apt-key`, которая признана устаревшей и не рекомендуется для использования. Кроме того, теперь для хранения ключей подписи разработчики ОС рекомендуют использовать каталог `/etc/apt/trusted.gpg.d` вместо файла `/etc/apt/trusted.gpg`. Ввиду этого при выполнении установки Dr.Web Server Security Suite из репозитория, если ключ подписи установлен в каталог `/etc/apt/trusted.gpg`, команда `apt-get update` (см. ниже) выдаст следующее предупреждение: `Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.` Установка Dr.Web Server Security Suite при этом продолжится в обычном режиме, а функциональность продукта не пострадает. Чтобы предупреждение больше не выводилось при установке или переустановке продуктов «Доктор Веб», установите ключ подписи как указано выше.

2. Чтобы подключить репозиторий, выполните команду:

```
# echo "deb https://repo.drweb.com/drweb/debian 11.1 non-free" > /etc/apt/sources.list.d/drweb.list
```

> Вы можете выполнить пункты 1 и 2, загрузив специальный DEB-пакет и установив его.

3. Для установки Dr.Web Server Security Suite из репозитория выполните команды:

```
# apt-get update
# apt-get install drweb-file-servers
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, Synaptic или aptitude). Кроме того, альтернативные менеджеры, такие как aptitude, рекомендуется использовать для разрешения конфликта пакетов, если он возникнет.

Альт (apt-rpm)

1. Чтобы подключить репозиторий, добавьте следующую строку в файл `/etc/apt/sources.list.d/drweb-apt-rpm-<arch>.list`:

```
rpm http://repo.drweb.com/drweb/altlinux 11.1/<arch> drweb
```

где <*arch*> — обозначение используемой архитектуры пакетов:

- для 32-разрядной версии: `i386`;
- для архитектуры AMD64: `x86_64`;
- для архитектуры ARM64: `aarch64`;
- для архитектуры E2K: `e2s`;
- для архитектуры IBM POWER (ppc64el): `ppc64le`.

2. Перед установкой Dr.Web Server Security Suite на компьютере архитектуры E2K под управлением ОС Альт добавьте в файл `/etc/rpmrc` следующие строки:

```
arch_compat: e2kv4: e2s
arch_compat: e2k: e2s
arch_compat: e2s: noarch
```

3. Чтобы установить Dr.Web Server Security Suite из репозитория, выполните команды:

```
# apt-get update
# apt-get install drweb-file-servers
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, Synaptic или aptitude).

Mageia, OpenMandriva Lx (urpmi)

1. Подключите репозиторий с помощью команды:

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/linux/11.1/<arch>/
```

где <*arch*> — обозначение используемой архитектуры пакетов:

- для 32-разрядной версии: `i386`;
- для 64-разрядной версии: `x86_64`.

2. Для установки Dr.Web Server Security Suite из репозитория выполните команду:

```
# urpmi drweb-file-servers
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, rpmdrake).

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

1. Добавьте файл `drweb.repo` со следующим содержимым в каталог `/etc/yum.repos.d`:

```
[drweb]
name=DrWeb - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

Если планируется записать вышеуказанное содержимое в файл при помощи команды типа `echo` с перенаправлением вывода, символ `$` следует экранировать: `\$`.

Вы можете выполнить пункт 1, загрузив специальный RPM-пакет и установив его.

2. Для установки Dr.Web Server Security Suite из репозитория выполните команду:

```
# yum install drweb-file-servers
```

В ОС Fedora, начиная с версии 22, рекомендуется вместо менеджера `yum` использовать менеджер `dnf`, например:

```
# dnf install drweb-file-servers
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, PackageKit или Yumex).

SUSE Linux (zypper)

1. Чтобы подключить репозиторий, выполните команду:

```
# zypper ar https://repo.drweb.com/drweb/linux/11.1/\$basearch/ drweb
```

2. Для установки Dr.Web Server Security Suite из репозитория выполните команды:

```
# zypper refresh
# zypper install drweb-file-servers
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, YaST).

6.2. Обновление Dr.Web Server Security Suite

Предусмотрено два режима обновления Dr.Web Server Security Suite:

1. Получение текущих обновлений пакетов и компонентов, выпущенных в рамках эксплуатации актуальной версии Dr.Web Server Security Suite (как правило, такие обновления содержат исправления ошибок и мелкие улучшения в функционировании компонентов).
2. Переход на новую версию. Этот способ обновления используется, если компания «Доктор Веб» выпустила новую версию Dr.Web Server Security Suite, отличающуюся новыми возможностями.



Dr.Web Server Security Suite позволяет обновлять вирусные базы и антивирусное ядро даже при отсутствии доступа в интернет на защищаемом сервере.

6.2.1. Получение текущих обновлений

После установки Dr.Web Server Security Suite любым из способов, описанных в соответствующем разделе, происходит автоматическое подключение менеджера пакетов к репозиторию пакетов Dr.Web:

- Если установка производилась из универсального пакета (файл `.run`), а в системе используются пакеты в формате DEB (например, ОС Astra Linux, Debian, Mint, Ubuntu), или в системе не имеется менеджера пакетов (FreeBSD), для работы с пакетами Dr.Web используется отдельная версия менеджера пакетов `zypper`, автоматически установленная в рамках установки Dr.Web Server Security Suite.

  Чтобы получить и установить обновленные пакеты Dr.Web этим менеджером, перейдите в каталог `/opt/drweb.com/bin` для GNU/Linux или `/usr/local/libexec/drweb.com/bin` для FreeBSD и выполните команды:

  ```
  # ./zypper refresh
  # ./zypper update
  ```

  В ОС FreeBSD версии 11.x для платформы `amd64` при обновлении с использованием менеджера `zypper` может возникнуть ошибка обновления репозитория. В этом случае установите пакет совместимости `compat10x-amd64` и повторите попытку обновления.

  Для установки пакета выполните команду:

  ```
  # pkg install compat10x-amd64
  ```

- Во всех остальных случаях используйте команды обновления пакетного менеджера, используемого в вашей ОС, например:
  - в Red Hat Enterprise Linux и CentOS используйте команду `yum`;

- в Fedora используйте команду `yum` или `dnf`;
- в SUSE Linux используйте команду `zypper`;
- в Mageia и OpenMandriva Lx используйте команду `urpmi`;
- в Альт, Astra Linux, Debian, Mint, Ubuntu используйте команду `apt-get`.

Вы также можете использовать альтернативные менеджеры пакетов, разработанные для вашей операционной системы. При необходимости обратитесь к справочному руководству по используемому вами менеджеру пакетов.

В случае выпуска новой версии Dr.Web Server Security Suite, пакеты, содержащие его компоненты, помещаются в раздел репозитория Dr.Web, соответствующий новой версии. В этом случае для обновления необходимо переключить менеджер пакетов на новый раздел репозитория Dr.Web (см. раздел Переход на новую версию).

6.2.2. Переход на новую версию

В этом разделе

- Предварительные замечания
- Обновление предыдущих версий
  - Обновление установкой универсального пакета
  - Обновление из репозитория
  - Перенос ключевого файла
  - Повторное подключение к серверу централизованной защиты

Предварительные замечания



Перед тем, как выполнить переход на новую версию, убедитесь, что ваш сервер отвечает системным требованиям новой версии.

Поддерживается процедура обновления предыдущих версий Dr.Web Server Security Suite до новой версии. Переход на новую версию Dr.Web Server Security Suite выполняйте тем же способом, каким была установлена версия Dr.Web Server Security Suite, подлежащая обновлению:

- Если версия Dr.Web Server Security Suite, подлежащая обновлению, была установлена из репозитория, то переход на новую версию выполняйте путем обновлением из репозитория.
- Если версия Dr.Web Server Security Suite, подлежащая обновлению, была установлена из универсального пакета, то для перехода на новую версию установите универсальный пакет, содержащий новую версию.

Чтобы уточнить способ, которым была установлена версия Dr.Web Server Security Suite, подлежащая обновлению, проверьте наличие в каталоге исполняемых файлов Dr.Web Server Security Suite скрипта программы удаления `uninst.sh`. Если этот файл присутствует, текущая версия Dr.Web Server Security Suite была установлена из универсального пакета, а в противном случае — из репозитория.

Для ОС FreeBSD установка Dr.Web Server Security Suite возможна только из универсального пакета.

Если вы не имеете возможности обновить Dr.Web Server Security Suite тем же способом, каким он был установлен изначально, то предварительно удалите текущую версию, а потом выполните установку новой версии любым доступным для вас способом. Способы установки и удаления предыдущих версий Dr.Web Server Security Suite аналогичны способам установки и удаления, рассмотренным в этом руководстве. Для дополнительной информации обратитесь к Руководству администратора по установленной у вас версии Dr.Web Server Security Suite.

Если версия Dr.Web Server Security Suite, подлежащая обновлению, работает под управлением сервера централизованной защиты, то перед началом обновления рекомендуется сохранить адрес этого сервера. Например, для получения адреса сервера централизованной защиты, к которому подключен Dr.Web Server Security Suite с версией новее 6.0.2, выполните команду:

```
$ drweb-ctl appinfo
```

Из присутствующей в выводе команды строчки вида

```
ESAgent; <PID>; RUNNING 1; Connected <адрес>, on-line
```

сохраните часть *<адрес>* (может выглядеть как строка вида `tcp://<IP-адрес>:<порт>`, например: `tcp://10.20.30.40:1234`). Кроме того, рекомендуется сохранить файл сертификата сервера.

В случае возникновения затруднений с получением параметров текущего подключения обратитесь к Руководству администратора по установленной версии Dr.Web Server Security Suite, а также к администратору вашей антивирусной сети.

Обновление предыдущих версий

Обновление установкой универсального пакета

Выполните установку новой версии Dr.Web Server Security Suite из универсального пакета. В случае необходимости в процессе установки вам будет предложено автоматически удалить имеющиеся компоненты старой версии Dr.Web Server Security Suite.



Если в процессе обновления вам необходимо выполнить удаление имеющейся версии Dr.Web Server Security Suite и на вашем сервере одновременно установлено несколько серверных продуктов Dr.Web (например, Dr.Web Server Security Suite, Dr.Web Mail Security Suite и Dr.Web Gateway Security Suite), то для сохранения работоспособности продуктов, не подлежащих обновлению (Dr.Web Mail Security Suite и Dr.Web Gateway Security Suite), следует отметить для удаления только следующие пакеты:

- `drweb-file-servers-doc`,
- `drweb-smbspider`.

Обновление из репозитория



Вы не сможете обновить Dr.Web для файловых серверов UNIX версии 6.0.2 до новой версии из репозитория, если на вашем сервере установлено одновременно несколько серверных продуктов Dr.Web версии 6.0.2 (например, для файловых серверов, для почтовых серверов и интернет-шлюзов). В этом случае вам следует установить новую версию Dr.Web Server Security Suite на отдельную машину.

Чтобы обновить текущую версию Dr.Web Server Security Suite, установленную из репозитория компании «Доктор Веб»

В зависимости от типа используемых пакетов, выполните следующие действия:

- **В случае использования пакетов RPM (yum, dnf):**

1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов новой версии).



Имя репозитория, хранящего пакеты новой версии, см. в разделе Установка из репозитория. Для уточнения способа смены репозиториев обратитесь к справочным руководствам используемого вами дистрибутива операционной системы.

2. Установите новую версию Dr.Web Server Security Suite из репозитория, выполнив команду:

```
# yum update
```

или, если используется менеджер dnf (как, например, в ОС Fedora версии 22 и более поздних):

```
# dnf update
```



Если в процессе обновления пакетов возникнет ошибка, то выполните удаление и последующую повторную установку Dr.Web Server Security Suite. При необходимости см. разделы Удаление Dr.Web Server Security Suite, установленного из репозитория и Установка из репозитория (пункты, соответствующие используемой вами ОС и менеджеру пакетов).

- **В случае использования пакетов DEB (apt-get)**:
  1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов новой версии).
  2. Обновите пакеты Dr.Web Server Security Suite, выполнив команды:

```
# apt-get update
# apt-get dist-upgrade
```

Перенос ключевого файла

При любом способе обновления Dr.Web Server Security Suite уже имеющийся у вас лицензионный ключевой файл будет автоматически установлен в надлежащее место для использования новой версией Dr.Web Server Security Suite.



В случае возникновения проблем с автоматической установкой лицензионного ключевого файла вы можете выполнить его установку вручную. Dr.Web Server Security Suite хранит ключевой файл в каталоге `/etc/opt/drweb.com/` для GNU/Linux или `/usr/local/etc/drweb.com/` для FreeBSD. В случае утраты действующего лицензионного ключевого файла обратитесь в службу технической поддержки компании «Доктор Веб».

Повторное подключение к серверу централизованной защиты

Если это возможно, то после обновления (если обновляемая версия была подключена к серверу централизованной защиты) подключение будет восстановлено автоматически. Если подключение не восстановилось автоматически, для подключения обновленной версии Dr.Web Server Security Suite к антивирусной сети выполните команду:

```
$ drweb-ctl esconnect <адрес сервера> --Certificate <путь к файлу сертификата сервера>
```

В случае возникновения затруднений с подключением обратитесь к администратору вашей антивирусной сети.

6.2.3. Обновление без подключения к интернету

В условиях повышенных требований к безопасности, когда подключение к интернету отсутствует или ограничено, обновление вирусных баз и антивирусного ядра можно выполнять без подключения к интернету. В этом случае обновления загружаются на компьютер, подключенный к интернету, копируются на USB-накопитель или сетевой диск, после чего устанавливаются на другой, не подключенный к интернету компьютер. Процедура обновления выполняется через командную строку.

Чтобы получить обновления

1. На компьютере, подключенном к интернету, выполните команду:

```
$ drweb-ctl update --Path <путь к каталогу для загрузки обновлений>
```

2. Скопируйте полученные обновления на USB-накопитель или сетевой диск.
3. Примонтируйте сетевой диск или накопитель на компьютере, на который требуется установить обновления. Если вы получаете обновления с USB-накопителя, для этого потребуется выполнить команды:

```
# mkdir /mnt/usb
# mount <путь к устройству> /mnt/usb
```

4. Установите обновления с помощью команды:

```
$ drweb-ctl update --From /mnt/usb
```

6.3. Удаление Dr.Web Server Security Suite

В зависимости от способа установки, вы можете удалить Dr.Web Server Security Suite одним из двух способов:

- запустив программу удаления универсального пакета для режима командной строки;
- удалив пакеты, установленные из репозитория компании «Доктор Веб», используя системный менеджер пакетов.

После удаления Dr.Web Server Security Suite вам необходимо вручную удалить из каталога сервера Samba ссылку на модуль VFS SMB Dr.Web и отредактировать файл конфигурации Samba (`smb.conf`), удалив из секций параметров разделяемых каталогов строку `vfs objects = smb_spider` (где `smb_spider` — имя символической ссылки на модуль VFS SMB Dr.Web).

6.3.1. Удаление универсального пакета

Удаление Dr.Web Server Security Suite, установленного из универсального пакета, выполняется при помощи командной строки (в графическом режиме необходимо наличие эмулятора терминала).

Программа удаления удалит не только Dr.Web Server Security Suite, но и *все другие* продукты Dr.Web, установленные на вашем компьютере.

Если на вашем компьютере, кроме Dr.Web Server Security Suite, установлены и другие продукты Dr.Web, для удаления только Dr.Web Server Security Suite вместо запуска программы удаления воспользуйтесь процедурой выборочной установки и удаления компонентов.

Удаление Dr.Web Server Security Suite из командной строки

Чтобы запустить программу удаления для режима командной строки, выполните команду:

```
# /opt/drweb.com/bin/uninst.sh
```

для GNU/Linux или

```
# /usr/local/libexec/drweb.com/bin/uninst.sh
```

для FreeBSD. Процедура удаления Dr.Web Server Security Suite рассмотрена в разделе Удаление в режиме командной строки.

Чтобы запустить программу удаления в полностью автоматическом режиме без показа интерфейса пользователя (включая диалоги программы удаления для режима командной строки), выполните команду:

```
# env DRWEB_NON_INTERACTIVE=yes /opt/drweb.com/bin/uninst.sh
```



В Альт 8 СП и других ОС, использующих устаревшие версии пакетного менеджера, во время удаления на консоль могут выводиться сообщения вида:

```
/etc/init.d/drweb-configd: Нет такого файла или каталога
```

На работу системы эти сообщения никак не влияют. Процедура удаления выполняется корректно.

6.3.1.1. Удаление в режиме командной строки

После запуска программы удаления, работающей в режиме командной строки, на экране появится текст приглашения к удалению.

1. Для начала удаления ответьте `Yes` или `Y` на запрос «Вы хотите продолжить?». Чтобы отказаться от удаления продуктов Dr.Web с вашего компьютера, введите `No` или `N`. В этом случае работа программы удаления будет завершена.
2. После подтверждения удаления запустится процедура удаления всех установленных пакетов Dr.Web. При этом на экран будут выдаваться записи, фиксируемые в журнал и отражающие ход процесса удаления.
3. По окончании процесса программа удаления завершит свою работу автоматически.

6.3.2. Удаление Dr.Web Server Security Suite, установленного из репозитория

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

- Astra Linux, Debian, Mint, Ubuntu (apt);
- Альт (apt-rpm);
- Mageia, OpenMandriva Lx (urpme);
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf);
- SUSE Linux (zypper).



Все нижеприведенные команды для удаления пакетов должны быть выполнены с правами суперпользователя (обычно пользователя *root*). Для этого используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Astra Linux, Debian, Mint, Ubuntu (apt)

Чтобы удалить корневой метапакет Dr.Web Server Security Suite, выполните команду:

```
# apt-get remove drweb-file-servers
```

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить корневой метапакет вместе со всеми зависимостями, выполните команду:

```
# apt-get remove drweb-file-servers --autoremove
```

При этом будут удалены все более не требуемые пакеты (а не только пакеты Dr.Web Server Security Suite), которые были автоматически установлены для удовлетворения зависимостей других пакетов.

Если корневой метапакет уже был удален, то чтобы автоматически удалить из системы все более не используемые пакеты, выполните команду:

```
# apt-get autoremove
```

Вы также можете удалить пакеты Dr.Web Server Security Suite с помощью альтернативных менеджеров (например, Synaptic или aptitude).

Альт (apt-rpm)

Удаление Dr.Web Server Security Suite в данном случае выполняется так же, как в ОС Debian и Ubuntu (см. выше).

Вы также можете удалить пакеты Dr.Web Server Security Suite с помощью альтернативных менеджеров (например, Synaptic или aptitude).



В ОС Альт 8 СП во время удаления на консоль могут выводиться сообщения вида:

```
/etc/init.d/drweb-configd: Нет такого файла или каталога
```

На работу системы эти сообщения никак не влияют. Процедура удаления выполняется корректно.

Mageia, OpenMandriva Lx (urpme)

Чтобы удалить корневой метапакет Dr.Web Server Security Suite, выполните команду:

```
# urpme drweb-file-servers
```

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить корневой метапакет вместе со всеми зависимостями, выполните команду:

```
# urpme --auto-orphans drweb-file-servers
```

При этом будут удалены все более не требуемые пакеты (а не только пакеты Dr.Web Server Security Suite), которые были автоматически установлены для удовлетворения зависимостей других пакетов.

Вы также можете удалить пакеты Dr.Web Server Security Suite с помощью альтернативных менеджеров (например, `rpmdrake`).

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

Чтобы удалить все установленные пакеты Dr.Web, выполните команду (в некоторых системах символ `*` требуется экранировать: `\*`):

```
# yum remove drweb*
```

В ОС Fedora, начиная с версии 22, вместо менеджера `yum` рекомендуется использовать менеджер `dnf`, например:

```
# dnf remove drweb*
```



Эти команды удалят из системы все пакеты, название которых начинается на `drweb` (стандартное наименование для пакетов программных продуктов Dr.Web). Будут удалены все пакеты с таким именем, а не только пакеты Dr.Web Server Security Suite.

Вы также можете удалить пакеты Dr.Web Server Security Suite с помощью альтернативных менеджеров (например, PackageKit или Yumex).

SUSE Linux (zypper)

Чтобы удалить корневой метапакет Dr.Web Server Security Suite, выполните команду:

```
# zypper remove drweb-file-servers
```

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить все установленные пакеты Dr.Web, выполните команду (в некоторых системах символ `*` требуется экранировать: `\*`):

```
# zypper remove drweb*
```



Эта команда удалит из системы все пакеты, название которых начинается на `drweb` (стандартное наименование для пакетов программных продуктов Dr.Web). Будут удалены все пакеты с таким именем, а не только пакеты Dr.Web Server Security Suite.

Вы также можете удалить пакеты Dr.Web Server Security Suite с помощью альтернативных менеджеров (например, YaST).

6.4. Дополнительно

6.4.1. Пакеты и файлы Dr.Web Server Security Suite

В этом разделе

- Пакеты
- Файлы

Пакеты

Dr.Web Server Security Suite состоит из следующих пакетов:

Пакет	Содержимое
`drweb-bases`	Файлы вирусных баз
`drweb-boost`	Библиотеки Boost
`drweb-clamd`	Файлы компонента Dr.Web ClamD
`drweb-cloudd`	Файлы компонента Dr.Web CloudD
`drweb-common`	Основной конфигурационный файл `drweb.ini`, основные библиотеки, документация и структура каталогов Dr.Web Server Security Suite, утилита сбора данных о конфигурации продукта и системном окружении. В процессе установки данного пакета также будут созданы пользователь `drweb` и группа `drweb`
`drweb-configd`	Файлы компонента Dr.Web ConfigD
`drweb-configure`	Файлы вспомогательной утилиты настройки Dr.Web Server Security Suite
`drweb-ctl`	Файлы компонента Dr.Web Ctl
`drweb-documentation`	Файлы документации в формате HTML по продуктам Dr.Web для Unix

Пакет	Содержимое
drweb-engine	Файлы антивирусного ядра Dr.Web Virus-Finding Engine
drweb-esagent	Файлы компонента Dr.Web ES Agent
drweb-filecheck	Файлы компонента Dr.Web File Checker
drweb-file-servers-doc	Документация в формате PDF
drweb-file-servers	Корневой метапакет Dr.Web Server Security Suite
drweb-httpd	Файлы компонента Dr.Web HTTPD и веб-интерфейса управления (метапакет)
drweb-httpd-bin	Файлы компонента Dr.Web HTTPD
drweb-httpd-webconsole	Файлы веб-интерфейса управления
drweb-icu	Библиотеки поддержки интернационализации и Unicode
drweb-libs	Файлы основных библиотек
drweb-netcheck	Файлы компонента Dr.Web Network Checker
drweb-nss	Файлы компонента SplDer Guard для NSS
drweb-openssl	Библиотеки OpenSSL
drweb-protobuf	Библиотеки Google Protobuf
drweb-se	Файлы компонента Dr.Web Scanning Engine
drweb-smbspider-daemon	Файлы компонента SplDer Guard для SMB (демон мониторинга SMB)
drweb-smbspider	Файлы компонента SplDer Guard для SMB
drweb-smbspider-modules	Файлы компонента SplDer Guard для SMB (модули VFS SMB)
drweb-smbspider-modules-src	Файлы компонента SplDer Guard для SMB (исходный код модуля VFS SMB)
drweb-snmpd	Файлы компонента Dr.Web SNMPD
drweb-spider	Файлы компонента SplDer Guard
drweb-spider-kmod	Файлы загружаемого модуля ядра Linux для работы SplDer Guard в режиме *LKM*
drweb-update	Файлы компонента Dr.Web Updater

В разделе Выборочные установка и удаление компонентов приведены типовые наборы компонентов для выборочной установки, обеспечивающие решение типовых задач Dr.Web Server Security Suite.

Файлы

Файлы Dr.Web Server Security Suite размещаются в каталогах `/opt`, `/etc` и `/var` дерева файловой системы.

Структура используемых каталогов:

Каталог	Содержимое
• Для GNU/Linux: `/etc/init.d/` • Для FreeBSD: `/usr/local/etc/rc.d/`	Управляющий скрипт `drweb-configd` для демона управления конфигурацией Dr.Web ConfigD
• Для GNU/Linux: `/etc/opt/drweb.com/` • Для FreeBSD: `/usr/local/etc/drweb.com/`	Общий конфигурационный файл `drweb.ini` и ключевой файл `drweb32.key`. Кроме этого, содержит:
`certs/`	– файлы используемых сертификатов.
• Для GNU/Linux: `/opt/drweb.com/` • Для FreeBSD: `/usr/local/libexec/drweb.com/`	Основной каталог Dr.Web Server Security Suite. Содержит в себе:
`bin/`	– исполняемые файлы всех компонентов (за исключением Dr.Web Virus-Finding Engine);
`include/`	– заголовочные файлы используемых библиотек;
`lib/`	– используемые библиотеки;
`man/`	– файлы системной справки `man`;
`share/`	– вспомогательные файлы, в том числе:
`doc/`	▫ документация Dr.Web Server Security Suite (текст Лицензионного соглашения и руководства администратора, если пакеты с документацией установлены),
`drweb-bases/`	▫ файлы вирусных баз Dr.Web (исходные образы, поставляемые при установке),

Каталог	Содержимое
drweb-spider-kmod/	▫ файлы модуля ядра для работы компонента SpIDer Guard (исходный код для ручной сборки),
scripts/	▫ файлы вспомогательных скриптов.
• Для GNU/Linux: /var/opt/drweb.com/ • Для FreeBSD: /var/drweb.com/	Вспомогательные и временные файлы, в том числе:
bases/	– файлы вирусных баз Dr.Web (актуальная обновленная версия);
cache/	– кеш обновлений;
drl/	– списки используемых серверов обновлений;
lib/	– антивирусное ядро Dr.Web Virus-Finding Engine в виде динамически загружаемой библиотеки drweb32.dll и настройки режима работы с сервером централизованной защиты;
update/	– каталог для временного хранения обновлений в процессе их получения.

6.4.2. Выборочные установка и удаление компонентов

В этом разделе

- Типовые комплекты компонентов для выборочной установки
- Установка и удаление компонентов Dr.Web Server Security Suite, установленного из репозитория
- Установка и удаление компонентов Dr.Web Server Security Suite, установленного из универсального пакета
  - Распаковка установочного файла
  - Выборочная установка компонентов
  - Выборочное удаление компонентов

В случае необходимости вы можете выполнить выборочную установку и удаление отдельных компонентов Dr.Web Server Security Suite, установив или удалив соответствующие пакеты. Выборочную установку и удаление следует производить тем же способом, каким был установлен Dr.Web Server Security Suite.

Для переустановки какого-либо компонента вы можете сначала удалить его, а потом установить заново.

Типовые комплекты компонентов для выборочной установки

Если требуется установить Dr.Web Server Security Suite с ограниченной функциональностью, вместо установки корневого метапакета из репозитория или из универсального пакета, вы можете установить только пакеты компонентов, обеспечивающих необходимую функциональность. Пакеты, требуемые для разрешения зависимостей, будут установлены автоматически. В таблице ниже приведены комплекты компонентов, предназначенные для решения типовых задач Dr.Web Server Security Suite. В столбце **Пакеты для установки** перечислены пакеты, которые необходимо установить для получения указанного комплекта компонентов.

Выборочный комплект компонентов	**Пакеты для установки**	**Будут установлены**
Минимальный комплект для консольного сканирования	• `drweb-filecheck`, • `drweb-se`	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Scanning Engine, • Dr.Web Updater, • Вирусные базы
Комплект для мониторинга файловой системы GNU/Linux	• `drweb-se`, • `drweb-spider`	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Scanning Engine, • Dr.Web Updater, • SpIDer Guard, • Вирусные базы
Комплект для мониторинга разделяемых каталогов Samba	• `drweb-se`, • `drweb-smbspider`	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Scanning Engine, • Dr.Web Updater, • SpIDer Guard для SMB, • Вирусные базы
Комплект для мониторинга томов NSS	• `drweb-nss`, • `drweb-se`	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Scanning Engine, • Dr.Web Updater, • SpIDer Guard для NSS, • Вирусные базы

Выборочный комплект компонентов	Пакеты для установки	Будут установлены
Комплект для эмуляции ClamAV (`clamd`)	• `drweb-clamd`, • `drweb-se`	• Dr.Web ClamD, • Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Network Checker, • Dr.Web Scanning Engine, • Dr.Web Updater, • Вирусные базы

Установка и удаление компонентов Dr.Web Server Security Suite, установленного из репозитория

Если Dr.Web Server Security Suite был установлен из репозитория, для установки или удаления отдельного компонента используйте соответствующую команду менеджера пакетов вашей ОС, например:

1. Чтобы удалить компонент Dr.Web Network Checker (пакет `drweb-netcheck`) из состава Dr.Web Server Security Suite, установленного в ОС CentOS, выполните команду:

   ```
   # yum remove drweb-netcheck
   ```

2. Чтобы добавить компонент Dr.Web Network Checker (пакет `drweb-netcheck`) в состав Dr.Web Server Security Suite, установленного в ОС Ubuntu, выполните команду:

   ```
   # apt-get install drweb-netcheck
   ```

При необходимости воспользуйтесь справкой по менеджеру пакетов вашей ОС.

Установка и удаление компонентов Dr.Web Server Security Suite, установленного из универсального пакета

Если Dr.Web Server Security Suite был установлен из универсального пакета, и вы хотите дополнительно установить или переустановить пакет какого-либо компонента, вам понадобится установочный файл (с расширением `.run`), из которого был установлен Dr.Web Server Security Suite. Если вы не сохранили этот файл, загрузите его с сайта компании «Доктор Веб».

Распаковка установочного файла

При запуске файла `.run` вы можете использовать следующие параметры командной строки:

`--noexec` — распаковать установочные файлы Dr.Web Server Security Suite вместо запуска процесса установки;

`--keep` — не удалять установочные файлы Dr.Web Server Security Suite и журнал установки по окончании установки;

`--target` *<каталог>* — распаковать установочные файлы Dr.Web Server Security Suite в указанный каталог *<каталог>*.

С полным перечнем параметров командной строки, которые могут быть использованы для установочного файла, можно ознакомиться, выполнив команду:

```
$ ./<имя файла .run> --help
```

Для выборочной установки компонентов Dr.Web Server Security Suite предварительно распакуйте содержимое установочного файла. Для этого выполните команду:

```
$ ./<имя файла .run> --noexec --target <каталог>
```

Выборочная установка компонентов

Установочный файл `.run` содержит пакеты всех компонентов, из которых состоит Dr.Web Server Security Suite (в формате RPM), а также вспомогательные файлы. Файлы пакетов каждого компонента имеют вид:

```
<имя_компонента>_<версия>~linux_<платформа>.rpm
```

где *<версия>* — это строка, включающая в себя версию и дату выпуска пакета, а *<платформа>* — строка, указывающая тип платформы, для которой предназначен Dr.Web Server Security Suite. Имена всех пакетов, содержащих компоненты Dr.Web Server Security Suite, начинаются с префикса `drweb`.

Для установки пакетов в состав установочного комплекта включен менеджер пакетов `zypper`. Для выборочной установки используйте служебный скрипт `installpkg.sh`. Для этого предварительно распакуйте содержимое установочного файла в любой каталог, доступный для записи.



Для установки пакетов необходимы права суперпользователя (обычно пользователя *root*). Для получения прав суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Чтобы выполнить установку пакета компонента, перейдите в каталог, содержащий распакованный установочный файл, и выполните в командной строке или эмуляторе терминала команду:

```
# ./scripts/installpkg.sh <имя_пакета>
```

Например:

```
# ./scripts/installpkg.sh drweb-netcheck
```

Если требуется установить Dr.Web Server Security Suite целиком, запустите скрипт установки, выполнив команду:

```
$ ./install.sh
```

Кроме этого, вы можете установить все пакеты Dr.Web Server Security Suite (в том числе, чтобы установить недостающие компоненты, или компоненты, удаленные по ошибке), запустив установку корневого метапакета:

```
# ./scripts/installpkg.sh drweb-file-servers
```

Выборочное удаление компонентов

Если в вашей ОС используется формат пакетов RPM, для выборочного удаления пакета какого-либо компонента выполните соответствующую команду удаления менеджера пакетов вашей операционной системы:

- в Red Hat Enterprise Linux и CentOS выполните команду `yum remove <имя_пакета>`;
- в Fedora выполните команду `yum remove <имя_пакета>` или `dnf remove <имя_пакета>`;
- в SUSE Linux выполните команду `zypper remove <имя_пакета>`;
- в Mageia, OpenMandriva Lx выполните команду `urpme <имя_пакета>`;
- в Альт выполните команду `apt-get remove <имя_пакета>`.

Например, для Red Hat Enterprise Linux:

```
# yum remove drweb-netcheck
```

Если ваша ОС использует пакеты формата DEB, либо если в составе системы не имеется менеджера пакетов (FreeBSD), для выборочного удаления воспользуйтесь менеджером пакетов `zypper`, поставляемым с Dr.Web Server Security Suite. Для этого перейдите в каталог `/opt/drweb.com/bin` для GNU/Linux или `/usr/local/libexec/drweb.com/bin` для FreeBSD и выполните команду:

```
# ./zypper remove <имя_пакета>
```

Например:

```
# ./zypper remove drweb-netcheck
```

Если вы хотите удалить Dr.Web Server Security Suite целиком, запустите скрипт удаления, выполнив команду:

```
# ./uninst.sh
```

Для переустановки какого-либо компонента вы можете сначала удалить его, а потом установить, запустив выборочную или полную установку.

6.5. Настройка подсистем безопасности

Наличие в составе ОС подсистемы обеспечения дополнительной безопасности SELinux, а также использование систем мандатного управления доступом (в отличие от классической дискреционной модели Unix), таких как PARSEC, приводит к проблемам в функционировании Dr.Web Server Security Suite при настройках по умолчанию. Для обеспечения корректной работы Dr.Web Server Security Suite в этом случае необходимо внести дополнительные изменения в настройки подсистемы безопасности и/или Dr.Web Server Security Suite.



Настройка разрешений системы мандатного доступа PARSEC для Dr.Web Server Security Suite позволит его компонентам обходить ограничения установленных политик безопасности и получать доступ к файлам разных уровней привилегий.

Даже если вы не настроите разрешения системы мандатного доступа PARSEC для Dr.Web Server Security Suite, то вы все равно сможете запускать проверку файлов непосредственно из командной строки. Для этого используйте команду `drweb-ctl` в автономном режиме работы, указав при запуске параметр `--Autonomous`.

В режиме автономного экземпляра будет возможна проверка файлов, для доступа к которым необходим уровень привилегий не выше уровня, с которым работает пользователь, запустивший сеанс проверки. Данный режим имеет следующие особенности:

- Для запуска в режиме автономного экземпляра необходимо наличие действующего ключевого файла, работа под управлением сервера централизованной защиты не поддерживается (имеется возможность установить ключевой файл, экспортированный с сервера централизованной защиты). При этом, даже если Dr.Web Server Security Suite подключен к серверу централизованной защиты, автономный экземпляр *не сообщает* серверу централизованной защиты об угрозах, обнаруженных при запуске в режиме автономного экземпляра.
- Все вспомогательные компоненты, обслуживающие работу автономного экземпляра, будут запущены от имени текущего пользователя и будут работать со специально сформированным файлом конфигурации.
- Все временные файлы и сокеты Unix, используемые для взаимодействия компонентов между собой, будут создаваться только в каталоге с уникальным именем. Этот каталог создается запущенным автономным экземпляром в каталоге временных файлов (указанном в системной переменной окружения `TMPDIR`).
- Пути к файлам вирусных баз, антивирусного ядра и исполняемым файлам сервисных компонентов заданы по умолчанию.
- Число одновременно работающих автономных экземпляров не ограничено.
- При завершении работы автономно запущенного экземпляра комплект обслуживающих его сервисных компонентов также завершает работу.

6.5.1. Настройка политик безопасности SELinux

В этом разделе

- Проблемы при установке универсального пакета
- Проблемы функционирования Dr.Web Server Security Suite

Если используемый вами дистрибутив GNU/Linux оснащен подсистемой безопасности SELinux (*Security-Enhanced Linux — Linux с улучшенной безопасностью*), то, чтобы служебные компоненты Dr.Web Server Security Suite (такие как сканирующее ядро) работали корректно после установки компонентов, вам, возможно, потребуется внести изменения в политики безопасности, используемые SELinux.

Проблемы при установке универсального пакета

При включенном SELinux установка Dr.Web Server Security Suite в виде универсального пакета из установочного файла (`.run`) может окончиться неудачей, поскольку будет заблокирована попытка создания в системе специального пользователя *drweb*, с полномочиями которого работают компоненты Dr.Web Server Security Suite.

Если попытка установки Dr.Web Server Security Suite из установочного файла (`.run`) была прервана из-за невозможности создания пользователя *drweb*, проверьте режим работы SELinux, для чего выполните команду `getenforce`. Эта команда выводит на экран текущий режим защиты:

- `Enforcing` — защита активна, используется запрещающая стратегия: действия, нарушающие политики безопасности, регистрируются в журнале аудита и блокируются;
- `Permissive` — защита активна, но используется разрешающая стратегия: действия, нарушающие политики безопасности, не запрещаются, а только фиксируются в журнале аудита;
- `Disabled` — SELinux установлен, но неактивен.

Если SELinux работает в режиме *Enforcing*, временно (на период установки Dr.Web Server Security Suite) переведите ее в режим *Permissive*. Для этого выполните команду:

```
# setenforce 0
```

Указанная команда временно (до первой перезагрузки системы) переведет SELinux в режим *Permissive*.



Какой бы режим защиты вы ни установили при помощи команды `setenforce`, после перезагрузки операционной системы SELinux вернется в режим защиты, заданный в ее настройках (обычно файл настроек SELinux находится в каталоге `/etc/selinux`).

После успешной установки Dr.Web Server Security Suite из установочного файла, но до его запуска и активации верните режим *Enforcing*, для чего выполните команду:

```
# setenforce 1
```

Проблемы функционирования Dr.Web Server Security Suite

В некоторых случаях при работающем SELinux отдельные компоненты Dr.Web Server Security Suite (такие как `drweb-se` и `drweb-filecheck`) не смогут запуститься, вследствие чего сканирование объектов и мониторинг файловой системы станут невозможны. Признаком того, что эти компоненты не могут быть запущены, является появление сообщений об ошибках 119 и 120 в системном журнале, который ведет служба `syslog` (обычно этот журнал расположен в каталоге `/var/log/`).

В случае срабатывания системы безопасности SELinux информация об отказах фиксируется также в системном журнале аудита. В общем случае, при использовании в системе демона audit, журнал аудита хранится в файле `/var/log/audit/audit.log`. В противном случае сообщения о запрете операции записываются в общий файл журнала (`/var/log/messages` или `/var/log/syslog`).

Если установлено, что компоненты сканирования не функционируют из-за того, что они блокируются SELinux, скомпилируйте для них специальные *политики безопасности*.



В некоторых дистрибутивах GNU/Linux указанные ниже утилиты могут быть по умолчанию не установлены. В этом случае вам, возможно, потребуется установить их дополнительно.

Чтобы настроить политики безопасности SELinux

1. Создайте новый файл с исходным кодом политики SELinux (файл с расширением `.te`). Данный файл определяет ограничения, относящиеся к описываемому модулю. Исходный файл политики может быть создан двумя способами:
   1) С помощью утилиты `audit2allow`. Это наиболее простой способ, поскольку данная утилита генерирует разрешающие правила на основе сообщений об отказе в доступе в файлах системных журналов. Возможно задать автоматический поиск сообщений в файлах журналов или указать путь к файлу журнала вручную.

Этот способ можно использовать только в том случае, когда в системном журнале аудита уже зарегистрированы инциденты нарушения политик безопасности SELinux компонентами Dr.Web Server Security Suite. Если это не так, дождитесь таких инцидентов в процессе работы Dr.Web Server Security Suite или создайте разрешающие политики принудительно, воспользовавшись утилитой `policygentool` (см. ниже).

Утилита `audit2allow` находится в пакете `policycoreutils-python` или `policycoreutils-devel` (для ОС Red Hat Enterprise Linux, CentOS, Fedora, в зависимости от версии) или в пакете `python-sepolgen` (для ОС Debian, Ubuntu).

Пример использования `audit2allow`:

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

В данном примере утилита `audit2allow` производит поиск в файле `/var/log/audit/audit.log` сообщений об отказе в доступе для компонента `drweb-se`.

В результате работы утилиты создаются два файла: исходный файл политики `drweb-se.te` и готовый к установке модуль политики `drweb-se.pp`.

Если подходящих инцидентов в системном журнале не обнаружено, утилита вернет сообщение об ошибке.

В большинстве случаев вам не потребуется вносить изменения в файл политики, созданный утилитой `audit2allow`, поэтому рекомендуется сразу переходить к пункту 4 для установки полученного модуля политики `drweb-se.pp`.

По умолчанию утилита `audit2allow` в качестве результата своей работы выводит на экран готовый вызов команды `semodule`. Скопировав его в командную строку и выполнив, вы выполните пункт 4. Перейдите к пункту 2, только если вы хотите внести изменения в политики, автоматически сформированные для компонентов Dr.Web Server Security Suite.

2) С помощью утилиты `policygentool`. Для этого укажите в качестве параметров имя компонента, работу с которым вы хотите настроить, и полный путь к его исполняемому файлу.

Утилита `policygentool`, входящая в состав пакета `selinux-policy` для ОС Red Hat Enterprise Linux и CentOS, может работать некорректно. В таком случае воспользуйтесь утилитой `audit2allow`.

Пример создания политик при помощи `policygentool`:

- для компонента `drweb-se`:

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- для компонента `drweb-filecheck`:

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

Вам будет предложено указать несколько общих характеристик домена, после чего для каждого компонента будут созданы три файла, определяющих политику:

<module_name>`.te`, *<module_name>*`.fc` и *<module_name>*`.if`.

2. При необходимости отредактируйте сгенерированный исходный файл политики *<module_name>.te*, а затем, используя утилиту `checkmodule`, создайте бинарное представление (файл с расширением `.mod`) исходного файла локальной политики.



Для успешной работы этой команды в системе должен быть установлен пакет `checkpolicy`.

Пример использования:

```
# checkmodule -M -m -o drweb-se.mod drweb-se.te
```

3. Создайте устанавливаемый модуль политики (файл с расширением `.pp`) с помощью утилиты `semodule_package`.

Пример:

```
# semodule_package -o drweb-se.pp -m drweb-se.mod
```

4. Для установки созданного модуля политики воспользуйтесь утилитой `semodule`.

Пример:

```
# semodule -i drweb-se.pp
```

Для получения дополнительной информации о принципах работы и настройки SELinux обратитесь к документации по используемому вами дистрибутиву GNU/Linux.

6.5.2. Настройка запуска в режиме ЗПС (Astra Linux SE, версии 1.6 и 1.7)

В ОС Astra Linux SE поддерживается особый режим *замкнутой программной среды* (ЗПС). В этом режиме запускаются только приложения, исполняемые файлы которых подписаны цифровой подписью разработчика, чей открытый ключ добавлен в перечень ключей, которым доверяет ОС.

Начиная с версии 1.6, в ОС Astra Linux SE механизм подписи был изменен. Запуск Dr.Web Server Security Suite в режиме ЗПС требует предварительной настройки Astra Linux SE 1.6 и 1.7.

Чтобы настроить Astra Linux SE версий 1.6 и 1.7 для запуска Dr.Web Server Security Suite в режиме ЗПС

1. Установите пакет `astra-digsig-oldkeys`, если он еще не установлен, с установочного диска ОС.

2. Поместите открытый ключ компании «Доктор Веб» в каталог `/etc/digsig/keys/legacy/keys` (в случае отсутствия каталога его необходимо создать):

```
# cp /opt/drweb.com/share/doc/digsig.gost.gpg /etc/digsig/keys/legacy/keys
```

3. Выполните команду:

```
# update-initramfs -k all -u
```

4. Перезагрузите систему.

7. Начало работы

1. Выполните активацию Dr.Web Server Security Suite.
2. Проверьте его работоспособность.
3. Интегрируйте Dr.Web Server Security Suite с требуемыми файловыми службами (см. инструкцию для Samba, см. инструкцию для NSS).
4. При необходимости настройте параметры мониторинга областей файловой системы GNU/Linux, находящихся вне томов NSS и вне разделяемых каталогов Samba.
5. Проверьте состав запущенных компонентов и при необходимости включите дополнительные компоненты, которые по умолчанию отключены, если они необходимы для защиты вашего сервера (например, SpIDer Guard, Dr.Web ClamD или Dr.Web SNMPD).

   Для корректной работы дополнительных компонентов может оказаться недостаточно только их включения. Возможно также потребуется внести изменения в их настройки, заданные по умолчанию.

   Для просмотра перечня установленных и запущенных компонентов, а также их настройки, используйте:

   - утилиту управления из командной строки Dr.Web Ctl (используйте команды `drweb-ctl appinfo`, `drweb-ctl cfshow` и `drweb-ctl cfset`);
   - веб-интерфейс управления Dr.Web Server Security Suite (по умолчанию доступ через браузер осуществляется по адресу `https://127.0.0.1:4443`).

7.1. Регистрация и активация

В этом разделе

- Приобретение и регистрация лицензии
- Активация Dr.Web Server Security Suite
  - Запрос демонстрационного периода
  - Установка ключевого файла
- Повторная регистрация

Приобретение и регистрация лицензии

При приобретении лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов обновлений компании «Доктор Веб», а также получать стандартную техническую поддержку компании «Доктор Веб» и ее партнеров.

Приобрести любой антивирусный продукт Dr.Web или серийный номер для него вы можете у наших партнеров или через интернет-магазин. Дополнительную информацию о возможных вариантах лицензий можно найти на официальном сайте компании «Доктор Веб».

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем Dr.Web Server Security Suite, и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки.

Активация Dr.Web Server Security Suite

Приобретенная лицензия может быть активирована непосредственно на сайте компании «Доктор Веб».

При активации или продлении лицензии требуется указать серийный номер. Этот номер может поставляться вместе с Dr.Web Server Security Suite или по электронной почте, при покупке или продлении лицензии онлайн.

Запрос демонстрационного периода

Вы можете использовать команду `license` утилиты командной строки Dr.Web Ctl (`drweb-ctl`), которая позволяет автоматически получить демонстрационный ключевой файл или лицензионный ключевой файл для серийного номера зарегистрированной лицензии. Для получения демонстрационного периода на использование Dr.Web Server Security Suite следует обратиться к мастеру запроса демо на официальном сайте компании «Доктор Веб». После выбора продукта и заполнения анкеты вы получите по электронной почте серийный номер или ключевой файл для активации демонстрационного периода.



Демонстрационный период использования Dr.Web Server Security Suite может быть выдан повторно для того же компьютера только по истечении определенного периода времени.

Установка ключевого файла

Если уже имеется ключевой файл, соответствующий действующей лицензии на этот продукт (например, он был получен от продавца по электронной почте после регистрации или Dr.Web Server Security Suite переносится на другой сервер), имеется возможность активировать Dr.Web Server Security Suite, просто указав путь к имеющемуся ключевому файлу. Это можно сделать следующим образом:

- Вручную, для этого:
  1. Распакуйте ключевой файл, если он был вами получен в архиве.

2. Далее выполните любое из указанных ниже действий.
   - Скопируйте его в каталог `/etc/opt/drweb.com` для GNU/Linux или `/usr/local/etc/drweb.com` для FreeBSD и переименуйте в `drweb32.key`.
   - В файле конфигурации Dr.Web Server Security Suite установите значение параметра `KeyPath` таким образом, чтобы он указывал на ключевой файл. В этом случае название ключа может отличаться от `drweb32.key`.
3. Перезагрузите конфигурацию Dr.Web Server Security Suite, выполнив команду:

```
# drweb-ctl reload
```

для применения внесенных изменений.

Вы также можете выполнить команду:

```
# drweb-ctl cfset Root.KeyPath <путь к ключевому файлу>
```

В последнем случае дополнительно перезагружать конфигурацию Dr.Web Server Security Suite не требуется. Ключевой файл не будет скопирован в каталог `/etc/opt/drweb.com` для GNU/Linux или `/usr/local/etc/drweb.com` для FreeBSD, а останется в исходном каталоге.



Если ключевой файл не скопирован в каталог `/etc/opt/drweb.com` для GNU/Linux или `/usr/local/etc/drweb.com` для FreeBSD, пользователь сам несет ответственность за его сохранность. Такой способ установки ключевого файла не рекомендуется из-за возможности его случайного удаления (например, если он был размещен в каталоге, подвергающемся автоматической очистке системой). Помните, что в случае утраты вы можете запросить ключевой файл повторно, но количество запросов на его получение ограничено.

Повторная регистрация

Повторная регистрация может потребоваться в случае утраты лицензионного ключевого файла при наличии активной лицензии. При повторной регистрации укажите те же персональные данные, которые вы ввели при первой регистрации лицензии. Допускается использовать другой адрес электронной почты — в таком случае лицензионный ключевой файл будет выслан по новому адресу.

Получить лицензионный ключевой файл с помощью команды управления лицензией можно ограниченное количество раз. Если это число превышено, то ключевой файл можно получить, подтвердив регистрацию своего серийного номера на сайте компании «Доктор Веб». Ключевой файл будет выслан на адрес электронной почты, который был указан при первой регистрации.

После получения ключевого файла по электронной почте вам необходимо выполнить процедуру его установки.

7.1.1. Ключевой файл

Ключевой файл — это специальный файл, который хранится на локальном компьютере и соответствует приобретенной лицензии или активированному демонстрационному периоду для Dr.Web Server Security Suite. В ключевом файле фиксируются параметры использования продукта в соответствии с приобретенной лицензией или активированным демонстрационным периодом.

Ключевой файл имеет расширение `.key` и является действительным при одновременном выполнении следующих условий:

- Срок действия лицензии или демонстрационного периода, которым он соответствует, не истек.
- Разрешение, определяемое лицензией или активным демонстрационным периодом, распространяется на все используемые модули.
- Целостность файла не нарушена.

При нарушении любого из этих условий ключевой файл становится недействительным.



При работе Dr.Web Server Security Suite ключевой файл по умолчанию должен находиться в каталоге `/etc/opt/drweb.com` для GNU/Linux или `/usr/local/etc/drweb.com` для FreeBSD и называться `drweb32.key`.

Компоненты Dr.Web Server Security Suite регулярно проверяют наличие и корректность ключевого файла. Его содержимое защищено от редактирования при помощи механизма электронной цифровой подписи, поэтому редактирование делает ключевой файл недействительным. Не рекомендуется открывать ключевой файл в текстовых редакторах во избежание случайной порчи его содержимого.

При отсутствии действительного ключевого файла (лицензионного или демонстрационного), а также по истечении срока его действия, антивирусные функции всех компонентов блокируются до установки действующего ключевого файла.

Рекомендуется сохранять имеющийся лицензионный ключевой файл до истечения срока его действия. В этом случае при переустановке Dr.Web Server Security Suite или переносе его на другой сервер повторная регистрация серийного номера лицензии не потребуется, и вы сможете использовать лицензионный ключевой файл, полученный при первом прохождении процедуры регистрации.



По электронной почте ключевые файлы Dr.Web обычно передаются запакованными в архивы `.zip`. Архив, содержащий ключевой файл для активации Dr.Web Server Security Suite, обычно имеет имя `agent.zip`. Если в сообщении электронной почты содержится *несколько* архивов, то нужно использовать именно архив `agent.zip`. Перед установкой ключевого файла вы должны распаковать архив любым удобным для вас способом и извлечь из него ключевой файл, сохранив его в любой доступный каталог (например, в домашний каталог или на съемный носитель USB flash).

7.2. Проверка работоспособности

Для проверки работоспособности антивирусных программ, использующих сигнатурные методы обнаружения угроз, используется тест *EICAR (European Institute for Computer Anti-Virus Research)*, разработанный одноименной организацией. Этот тест разработан для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении угрозы.

Программа, используемая для теста *EICAR*, не является вредоносной, но специально определяется большинством антивирусных программ как вирус. Антивирусные продукты Dr.Web называют этот «вирус» следующим образом: *EICAR Test File (NOT a Virus!)*. Примерно так его называют и другие антивирусные программы. Тестовая программа EICAR представляет собой последовательность из 68 байт, образующую тело исполняемого файла `.com` для ОС MS-DOS/Windows, в результате исполнения которого в консоль или на экран эмулятора терминала выводится текстовое сообщение:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

Тело тестовой программы состоит только из текстовых символов, которые формируют следующую строку:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Если вы создадите текстовый файл, состоящий из приведенной выше строки, то в результате получится программа, которая и будет описанным «вирусом».

В случае корректной работы Dr.Web Server Security Suite этот файл должен обнаруживаться при проверке объектов файловой системы любым доступным способом, с уведомлением об обнаружении угрозы EICAR Test File (NOT a Virus!).

Пример команды для проверки работоспособности Dr.Web Server Security Suite при помощи тестовой программы EICAR:

```
$ echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*' > testfile
&& drweb-ctl scan testfile && rm testfile
```

Данная команда записывает строку, представляющую собой тело тестовой программы EICAR, в файл `testfile` в текущий каталог, выполняет проверку полученного файла, после чего удаляет созданный файл.



Для успешного проведения вышеуказанного теста вы должны иметь права записи в текущий каталог. Кроме того, убедитесь, что в нем отсутствует файл с именем `testfile` (при необходимости измените имя файла в команде).

В случае успешного обнаружения тестового «вируса» на экран будет выдано следующее сообщение:

```
<путь к текущему каталогу>/testfile - infected with EICAR Test File (NOT a Virus!)
```

Если при проверке будет получено сообщение об ошибке, обратитесь к описанию известных ошибок.



Если в системе работает монитор файловой системы SplDer Guard, при обнаружении угрозы файл может быть тут же удален или перемещен в карантин (в зависимости от настроек компонента). В этом случае после сообщения об обнаружении угрозы команда `rm` сообщит об отсутствии файла. Эта ситуация не является ошибкой, а сигнализирует о корректной работе монитора.

7.3. Настройка мониторинга файловой системы

В этом разделе

- Основные настройки мониторинга файлов
- Изменение режима мониторинга файлов

Для настройки мониторинга файловой системы GNU/Linux монитором SplDer Guard необходимо задать значения ряда параметров, находящихся в секции настроек `[LinuxSpider]` конфигурационного файла.

Основные настройки мониторинга файлов

- Установите для параметра `Start` значение `Yes`, чтобы включить монитор.
- Укажите режим взаимодействия монитора с файловой системой в параметре `Mode` (рекомендуется использовать значение `Auto`).
- В параметре `ExcludedProc` при необходимости перечислите пути к исполняемым файлам доверенных приложений, то есть приложений, доступ которых к файлам не будет контролироваться монитором.
- В параметре `ExcludedFilesystem` при необходимости перечислите имена файловых систем (например, `cifs`), файлы которых не будут контролироваться монитором.
- Определите область наблюдения в файловой системе, задав набор защищаемых пространств. Каждое защищаемое пространство задается отдельной секцией `[LinuxSpider.Space.<`*имя пространства*`>]`. Для каждого пространства в параметре `Path` задайте путь к каталогу, в котором расположены файлы, подлежащие наблюдению, и установите параметр `Enable` в значение `Yes`, чтобы добавить защищаемое пространство к области наблюдения монитора.
- В параметре `ExcludedPath` (для всей файловой системы совместно, или для каждого защищаемого пространства индивидуально) определите область исключения (перечни путей к объектам, подлежащим и не подлежащим контролю монитором). В частности, если некоторые пути находятся под управлением файлового сервера Samba или являются томами NSS, эти пути следует добавить в область исключения во избежание конфликтов при проверке разными мониторами.

- Задайте параметры проверки файлов и реакции монитора на обнаружение угроз различных типов (в том числе, при необходимости, определите их индивидуально для каждого защищаемого пространства в области наблюдения монитора).

Изменение режима мониторинга файлов



Режимы усиленного мониторинга файлов с их предварительной блокировкой доступны только если SplDer Guard работает в режиме `FANOTIFY`, а ядро ОС собрано со включенной опцией `CONFIG_FANOTIFY_ACCESS_PERMISSIONS`.

Для переключения режимов работы SplDer Guard необходимо обладать правами суперпользователя. Для получения прав суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

- Чтобы переключить SplDer Guard в режим работы `FANOTIFY`, выполните команду:

```
# drweb-ctl cfset LinuxSpider.Mode FANOTIFY
```

- Чтобы изменить режим мониторинга, выполните команду:

```
# drweb-ctl cfset LinuxSpider.BlockBeforeScan <режим>
```

где *<режим>* определяет режим блокировки:

- `Off` — блокировка доступа не производится, SplDer Guard осуществляет обычный (не блокирующий) режим мониторинга;
- `Executables` — производится блокировка доступа к исполняемым файлам, SplDer Guard осуществляет усиленный контроль исполняемых файлов;
- `All` — производится блокировка доступа к любым файлам, SplDer Guard осуществляет «параноидальный» режим мониторинга.

- Чтобы изменить срок актуальности результатов проверки файлов, хранимых Dr.Web File Checker в кеше, выполните команду:

```
# drweb-ctl cfset FileCheck.RescanInterval <период>
```

где *<период>* определяет период актуальности предыдущих результатов проверки, находящихся в кэше. Допустимо значение от `0s` до `1m`. Если указан период менее 1 секунды, то сканирование будет осуществляться при каждом запросе.

После внесения изменений в настройки перезагрузите конфигурацию Dr.Web Server Security Suite с помощью команды:

```
# drweb-ctl reload
```

Вы также можете перезапустить Dr.Web Server Security Suite, перезапустив демон управления конфигурацией Dr.Web ConfigD с помощью команды:

```
# service drweb-configd restart
```

7.4. Интеграция с файловым сервером Samba

В этом разделе

- Шаги по интеграции с Samba
- Утилита конфигурирования

Монитор SpIDer Guard для SMB использует для интеграции с Samba специальный модуль VFS SMB. Совместно с монитором SpIDer Guard для SMB поставляется несколько версий модуля VFS SMB, собранных для различных версий Samba, однако они могут оказаться несовместимы с версией Samba, установленной на вашем файловом сервере, например, если установленный у вас сервер Samba использует опцию `CLUSTER_SUPPORT`.

В случае несовместимости поставляемых модулей VFS SMB с вашим сервером Samba, в процессе установки Dr.Web Server Security Suite на экран *будет выдано соответствующее сообщение*. В этом случае перед интеграцией необходимо выполнить процедуру сборки модуля VFS SMB для вашего сервера Samba, включая поддержку опции `CLUSTER_SUPPORT`, если это требуется.

Для получения информации о процедуре сборки модуля VFS SMB из исходного кода см. раздел Сборка модуля VFS SMB.

Шаги по интеграции с Samba

Для интеграции SpIDer Guard для SMB с файловым сервером Samba необходимо выполнить следующее:

1. В каталоге VFS-модулей сервера Samba (по умолчанию для GNU/Linux — `/usr/lib/<`*архитектура*`>-linux-gnu/samba/`) создать символическую ссылку `smb_spider.so`, указывающую на модуль VFS SMB компании «Доктор Веб», соответствующий используемой версии сервера Samba.

   Модули VFS SMB, поставляемые компанией «Доктор Веб», расположены в каталоге с библиотеками `/opt/drweb.com/lib/<`*архитектура*`>-linux-gnu/samba/` (в Debian, Ubuntu, Mint) или `/opt/drweb.com/lib64/samba/`.

   Файлы модулей имеют имя вида `libsmb_spider.so.<`*ver*`>`, где <*ver*> — версия сервера Samba, с которой работает модуль.

   Например, `/opt/drweb.com/lib/x86_64-linux-gnu/samba/libsmb_spider.so.4.13.0` — модуль VFS SMB для сервера Samba версии 4.13.0 для GNU/Linux, архитектура `x86_64`.

2. В файле конфигурации сервера Samba `smb.conf` (по умолчанию для GNU/Linux в каталоге `/etc/samba`) создайте секции для разделяемых каталогов. Секция разделяемого каталога должна иметь вид:

```
[<имя ресурса>]
comment = <комментарий>
path = <путь к защищаемому каталогу>
vfs objects = smb_spider
writeable = yes
browseable = yes
guest ok = yes
public = yes
```

где *<имя ресурса>* — любое имя разделяемого ресурса, а *<комментарий>* — произвольная строка-комментарий (не обязательно). Имя объекта, указанное в параметре `vfs objects`, должно совпадать с именем файла символической ссылки (`smb_spider` в данном случае).

После этого каталог, указанный в параметре `path`, будет находиться под наблюдением монитора SpIDer Guard для SMB. При этом взаимодействие SpIDer Guard для SMB с модулем VFS SMB будет производиться через Unix-сокет `/<samba chroot path>/var/run/.com.drweb.smb_spider_vfs`. Путь к этому Unix-сокету по умолчанию задан в настройках SpIDer Guard для SMB, а также модуля VFS SMB.

Подключить SpIDer Guard для SMB к уже настроенным в файле конфигурации сервера Samba разделяемым каталогам вы можете, используя утилиту конфигурирования `drweb-configure`.

3. Если требуется изменить путь к сокету, то его необходимо задать не только в настройках SpIDer Guard для SMB (параметр `SmbSocketPath`), но и в файле конфигурации Samba `smb.conf`. Для этого в секцию `[<имя ресурса>]` необходимо добавить строку:

```
smb_spider:socket = <путь к сокету>
```

где *<путь к сокету>* должен быть абсолютным путем к Unix-сокету, относительно корня, заданного для сервера Samba через `chroot` (*<samba chroot path>*).

4. При необходимости вы можете исключать объекты в защищаемых разделямых каталогах (как каталоги из проверки, так и отдельные файлы). Для этого укажите пути к этим объектам в качестве значений параметра `ExcludedPath`. В качестве значений параметра `IncludedPath` вы можете указать пути к объектам, которые обязательно должны быть включены в проверку.



Параметр `IncludedPath` имеет приоритет над параметром `ExcludedPath`: если один и тот же файл или каталог добавлен в значения обоих параметров, он будет включен в список для обязательной проверки.

5. Если требуется задать индивидуальные настройки проверки для данного разделяемого каталога, отличные от настроек по умолчанию (для всех модулей), то необходимо задать тег-идентификатор для модуля VFS SMB, контролирующего этот каталог:

   ```
   smb_spider:tag = <имя ресурса>
   ```

   Далее индивидуальные настройки контроля этого разделяемого каталога задаются в настройках SpIDer Guard для SMB в виде отдельной секции `[SMBSpider.Share.<имя ресурса>]`.

   Чтобы добавить новую секцию параметров с тегом *<имя ресурса>* при помощи утилиты управления Dr.Web Ctl, выполните команду `drweb-ctl cfset SmbSpider.Share.<имя ресурса>.<параметр> <значение>`, например:

   ```
   # drweb-ctl cfset SmbSpider.Share.AccountingFiles.OnAdware Quarantine
   ```

   Данная команда добавит в файл конфигурации секцию `[SMBSpider.Share.AccountingFiles]`. Эта секция будет содержать все параметры проверки каталога, причем значения всех параметров, кроме параметра `OnAdware`, указанного в команде, будут совпадать со значениями параметров из общей секции `[SMBSpider]`.

6. Включите SpIDer Guard для SMB, задав для параметра `Start` значение `Yes`.

После внесения изменений в настройки перезапустите сервер Samba, а также перезагрузите конфигурацию Dr.Web Server Security Suite, выполнив команду:

```
# drweb-ctl reload
```

Вы также можете перезапустить Dr.Web Server Security Suite, перезапустив демон управления конфигурацией Dr.Web ConfigD с помощью команды:

```
# service drweb-configd restart
```



Для предотвращения возможных конфликтов между SpIDer Guard для SMB и SpIDer Guard при проверке файлов в разделяемых каталогах Samba, рекомендуется дополнительно настроить SpIDer Guard, выполнив одно из следующих действий:

- добавить разделяемые каталоги Samba в область исключения (перечислить эти каталоги в параметре `ExcludedPath`);
- добавить процесс Samba (`smbd`) в список игнорируемых процессов (указать `smbd` в параметре `ExcludedProc`).

Утилита конфигурирования

Для удобства интеграции SpIDer Guard для SMB с настроенными в конфигурации файлового сервера Samba разделяемыми каталогами (подключения к ним и отключения) разработана специальная вспомогательная утилита `drweb-configure`. Для настройки подключения SpIDer Guard для SMB к имеющимся разделяемым каталогам или отключения от них, выполните команду:

```
# drweb-configure samba [<параметры>]
```

В качестве параметров можно указать:

- `+`*<ресурс Samba>* — имя разделяемого ресурса Samba (как оно указано в файле конфигурации `smb.conf`), который следует добавить под защиту SpIDer Guard для SMB;
- `-`*<ресурс Samba>* — имя разделяемого ресурса Samba (как оно указано в файле конфигурации `smb.conf`), который следует исключить из-под защиты SpIDer Guard для SMB;
- `+/all` — добавить под защиту SpIDer Guard для SMB все разделяемые ресурсы Samba, указанные в файле конфигурации `smb.conf`;
- `-/all` — исключить из-под защиты SpIDer Guard для SMB все разделяемые ресурсы Samba, указанные в файле конфигурации `smb.conf`;
- `add_symlink` — создать символическую ссылку `smb_spider.so`, указывающую на модуль VFS SMB Dr.Web (путь к исходному файлу может различаться в зависимости от используемой версии Samba);
- `remove_symlink` — удалить символическую ссылку `smb_spider.so`;
- *<файл конфигурации>* — путь к файлу конфигурации файлового сервера Samba (`smb.conf`), который следует обработать. Если этот параметр опустить, утилита `drweb-configure` попытается автоматически обнаружить актуальный файл `smb.conf`.



Получить справку по модулю настройки интеграции SpIDer Guard для SMB с разделяемыми каталогами Samba можно с помощью команды:

```
$ drweb-configure --help samba
```

7.5. Интеграция с томами NSS

Для интеграции Dr.Web Server Security Suite с томами Novell Storage Services необходимо задать значения ряда параметров, находящихся в секции `[NSS]` конфигурационного файла:

- В параметре `ProtectedVolumes` перечислите имена томов файловой системы NSS, находящихся в точке монтирования томов NSS и подлежащих защите. Если параметр оставить пустым, то защите будут подлежать все тома, присутствующие в точке монтирования томов NSS.

- При необходимости, задавая значения параметров `ExcludedPath` и `IncludedPath`, определите пути к объектам, находящимся на защищаемых томах, которые должны быть исключены из проверки и, наоборот, проверяться монитором SplDer Guard для NSS. Допускается указание путей как к каталогам, так и к отдельным файлам. Если указан каталог, то будет пропускаться или проверяться все содержимое этого каталога, включая вложенные файлы и каталоги.

  Параметр `IncludedPath` имеет приоритет над параметром `ExcludedPath`, т. е. если один и тот же объект (файл или каталог) включен в оба параметра, то он будет проверен.

  Параметры `IncludedPath` и `ExcludedPath` допускают использование файловых масок (*wildcards*). Регистрозависимость путей, указываемых в этих параметрах, определяется настройками NSS.

- Включите компонент SplDer Guard для NSS, задав для параметра `Start` значение `Yes`.

После внесения изменений в настройки перезагрузите конфигурацию Dr.Web Server Security Suite, выполнив команду:

```
# drweb-ctl reload
```

Вы также можете перезапустить Dr.Web Server Security Suite, перезапустив демон управления конфигурацией Dr.Web ConfigD с помощью команды:

```
# service drweb-configd restart
```

8. Краткие инструкции

В этом разделе

- Работа с файловыми хранилищами:
  - Как настроить мониторинг файловой системы GNU/Linux
  - Как подключить Dr.Web Server Security Suite к серверу Samba
  - Как добавить новый разделяемый каталог SMB
  - Как подключить Dr.Web Server Security Suite к Novell Storage Services
  - Как добавить новый защищаемый том NSS
- Общие вопросы по управлению Dr.Web Server Security Suite:
  - Как перезапустить Dr.Web Server Security Suite
  - Как подключиться к серверу централизованной защиты
  - Как отключиться от сервера централизованной защиты
  - Как активировать Dr.Web Server Security Suite
  - Как обновить версию Dr.Web Server Security Suite
  - Как добавить или удалить компонент Dr.Web Server Security Suite
  - Как управлять работой компонентов Dr.Web Server Security Suite
  - Как просмотреть журнал Dr.Web Server Security Suite

Как подключить Dr.Web Server Security Suite к серверу Samba

Следуйте инструкции, представленной в разделе Интеграция с файловым сервером Samba.

Как подключить Dr.Web Server Security Suite к Novell Storage Services

Следуйте инструкции, представленной в разделе Интеграция с томами NSS.

Как настроить мониторинг файловой системы GNU/Linux

Следуйте инструкции, представленной в разделе Настройка мониторинга файловой системы.

Как перезапустить Dr.Web Server Security Suite

Для перезапуска уже работающего Dr.Web Server Security Suite вы можете использовать управляющий скрипт демона управления конфигурацией Dr.Web ConfigD. Запуск, останов и перезапуск этого демона приводит, соответственно, к запуску, останову и перезапуску всех компонентов Dr.Web Server Security Suite.

Скрипт для управления Dr.Web ConfigD располагается в стандартном для ОС каталоге (`/etc/init.d/` для GNU/Linux или `/usr/local/etc/rc.d/` для FreeBSD) и называется `drweb-configd`. Скрипт имеет следующие управляющие параметры:

Параметр	Описание
`start`	Запустить Dr.Web ConfigD, если он еще не запущен. При запуске Dr.Web ConfigD запустит все необходимые компоненты Dr.Web Server Security Suite.
`stop`	Завершить работу Dr.Web ConfigD, если он запущен. При завершении работы Dr.Web ConfigD завершит работу всех компонентов Dr.Web Server Security Suite.
`restart`	Перезапустить (завершить и запустить) Dr.Web ConfigD, который завершит и запустит все компоненты Dr.Web Server Security Suite. Если Dr.Web ConfigD не был запущен, равносильно `start`.
`condrestart`	Перезапустить Dr.Web ConfigD только в том случае, если он был запущен.
`reload`	Послать Dr.Web ConfigD сигнал HUP, если он запущен. Dr.Web ConfigD перешлет этот сигнал всем компонентам Dr.Web Server Security Suite. Используется для инициации процесса перечитывания конфигурации всеми компонентами Dr.Web Server Security Suite.
`status`	Вывести на консоль текущее состояние Dr.Web ConfigD.

Например, для перезапуска Dr.Web Server Security Suite (или запуска, если он не был запущен) в ОС семейства GNU/Linux выполните команду:

```
# /etc/init.d/drweb-configd restart
```

Как подключиться к серверу централизованной защиты

1. Получите от администратора антивирусной сети адрес сервера централизованной защиты и файл его сертификата, а также, при необходимости, дополнительные параметры, такие как идентификатор станции и пароль, или идентификаторы основной и тарифной группы.
2. Используйте команду `esconnect` утилиты управления Dr.Web Server Security Suite из командной строки Dr.Web Ctl.

   Для подключения обязательно используйте параметр `--Certificate`, указав путь к файлу сертификата сервера. Дополнительно вы можете указать идентификатор узла («станции», с точки зрения сервера централизованной защиты) и пароль для

аутентификации на сервере, если они вам известны, используя параметры `--Login` и `--Password`. Если эти параметры заданы, то подключение к серверу будет успешным только при указании правильной пары идентификатор/пароль. Если эти параметры не указаны, то подключение к серверу будет успешным только в случае его одобрения на сервере (автоматически или администратором антивирусной сети, в зависимости от настроек сервера).

Кроме того, вы можете использовать параметр `--Newbie` (подключиться как «новичок»). Если этот режим подключения разрешен на сервере, то, после одобрения подключения, сервер автоматически сгенерирует для хоста уникальную пару идентификатор/пароль, которая в дальнейшем будет использоваться для его подключения к этому серверу.



При подключении как «новичок», новая учетная запись для хоста будет сгенерирована сервером централизованной защиты даже в том случае, если ранее он уже имел учетную запись на этом сервере.

Типовой пример команды подключения Dr.Web Server Security Suite к серверу централизованной защиты:

```
# drweb-ctl esconnect <адрес сервера> --Certificate <путь к файлу сертификата сервера>
```

После успешного подключения к серверу централизованной защиты Dr.Web Server Security Suite будет работать в режиме централизованной защиты или в мобильном режиме, в зависимости от разрешений, установленных на сервере и значения параметра конфигурации `MobileMode` компонента Dr.Web ES Agent. Для принудительного использования мобильного режима установите этот параметр в значение `On`. Для работы в режиме централизованной защиты установите параметр в значение `Off`.

Типовой пример команды перевода Dr.Web Server Security Suite, подключенного к серверу централизованной защиты, в мобильный режим:

```
# drweb-ctl cfset ESAgent.MobileMode On
```



Если используемый сервер централизованной защиты не поддерживает или запрещает мобильный режим работы, то изменение значения параметра конфигурации `MobileMode` не переведет Dr.Web Server Security Suite в мобильный режим.

Как отключиться от сервера централизованной защиты

Для отключения Dr.Web Server Security Suite от сервера централизованной защиты и перевода его в автономный режим используйте команду `esdisconnect` утилиты управления Dr.Web Server Security Suite из командной строки Dr.Web Ctl:

```
# drweb-ctl esdisconnect
```

Для успешной работы Dr.Web Server Security Suite в автономном режиме необходимо иметь действующий лицензионный ключевой файл. В противном случае антивирусные функции Dr.Web Server Security Suite после перехода в автономный режим *будут заблокированы*.

Как активировать Dr.Web Server Security Suite

1. Пройдите регистрацию на сайте компании «Доктор Веб».
2. Получите на указанный при регистрации адрес электронной почты (или загрузите непосредственно с сайта после окончания регистрации) архив, содержащий действительный лицензионный ключевой файл.
3. Выполните процедуру установки ключевого файла.

Как добавить новый разделяемый каталог SMB

1. Отредактируйте конфигурационный файл сервера Samba `smb.conf`, добавив в него секцию описания разделяемого каталога. Секция разделяемого каталога должна иметь вид:

```
[<имя ресурса>]
comment = <комментарий>
path = <путь к защищаемому каталогу>
vfs objects = smb_spider
writeable = yes
browseable = yes
guest ok = yes
public = yes
```

   где *<имя ресурса>* — любое имя разделяемого ресурса, а *<комментарий>* — необязательная произвольная строка-комментарий.
2. Если требуется задать для добавленного разделяемого каталога настройки проверки, отличающиеся от заданных для SpIDer Guard для SMB по умолчанию, воспользуйтесь пунктами 3 и 4 инструкции, приведенной в разделе Интеграция с файловым сервером Samba.
3. Перезапустите сервер Samba и Dr.Web Server Security Suite.

Как добавить новый защищаемый том NSS

1. Укажите имя тома, подлежащего защите, в параметре `ProtectedVolumes` (находится в секции `[NSS]` конфигурационного файла). Если параметр сделать пустым, то защите будут подлежать все тома, присутствующие в каталоге монтирования томов NSS.
2. Перезапустите Dr.Web Server Security Suite.

Как обновить версию Dr.Web Server Security Suite

Обновите версии компонентов или выполните переход на новую версию.

Вам может быть предложено удалить текущую версию Dr.Web Server Security Suite.

Как добавить или удалить компонент Dr.Web Server Security Suite

Воспользуйтесь процедурой выборочной установки и удаления компонентов.

При установке или удалении компонента для удовлетворения зависимостей могут быть дополнительно установлены или удалены другие компоненты Dr.Web Server Security Suite.

Как управлять работой компонентов Dr.Web Server Security Suite

Для просмотра состояния компонентов Dr.Web Server Security Suite и управления их работой используйте:

- Утилиту управления из командной строки Dr.Web Ctl. Используйте команды `drweb-ctl appinfo`, `drweb-ctl cfshow` и `drweb-ctl cfset`. Чтобы просмотреть перечень доступных команд управления, выполните команду `drweb-ctl --help`.
- Веб-интерфейс управления Dr.Web Server Security Suite. По умолчанию доступ через браузер осуществляется по адресу `https://127.0.0.1:4443`.

Как просмотреть журнал Dr.Web Server Security Suite

При настройках по умолчанию общий журнал всех компонентов Dr.Web Server Security Suite выводится в `syslog` (файл, в который записывает сообщения системный компонент `syslog`, зависит от системы и находится в каталоге `/var/log`). Общие настройки ведения журнала задаются в конфигурационном файле в секции `[Root]` (параметры `Log` и `DefaultLogLevel`). Для каждого из компонентов в его секции настроек доступны параметры `Log` и `LogLevel`, задающие место хранения журнала и уровень подробности сообщений, выводимых компонентом в журнал.

Также вы можете выполнить команду `drweb-ctl log`.

Чтобы изменить настройки ведения журнала, используйте утилиту управления из командной строки Dr.Web Ctl или веб-интерфейс управления Dr.Web Server Security Suite.

Чтобы облегчить идентификацию ошибок, настройте вывод общего журнала всех компонентов в отдельный файл и разрешите вывод расширенной отладочной информации. Для этого выполните команды:

```
# drweb-ctl cfset Root.Log <путь к файлу журнала>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

Чтобы вернуть настройки ведения общего журнала всех компонентов по умолчанию, выполните команды:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

9. Компоненты Dr.Web Server Security Suite

В разделе перечислены компоненты, входящие в состав Dr.Web Server Security Suite. Для каждого компонента указаны его назначение, принципы функционирования, а также параметры, которые он хранит в файле конфигурации.

9.1. Dr.Web ConfigD

Демон управления конфигурацией Dr.Web ConfigD — это центральный управляющий компонент Dr.Web Server Security Suite. Он обеспечивает централизованное хранение настроек для всех компонентов Dr.Web Server Security Suite, управляет активностью всех компонентов и организует доверительный обмен данными между ними.

Dr.Web ConfigD выполняет следующие функции:

- запуск и остановка компонентов Dr.Web Server Security Suite в зависимости от настроек;
- автоматический перезапуск компонентов в случае сбоев;
- запуск компонентов по запросу от других компонентов;
- оповещение компонентов об изменении настроек;
- предоставление возможности централизованного управления конфигурационными параметрами;
- предоставление компонентам информации из используемого ключевого файла;
- получение лицензионной информации от компонентов;
- получение новой лицензионной информации от специализированных компонентов;
- оповещение запущенных компонентов об изменении лицензионной информации.

9.1.1. Принципы работы

Демон управления конфигурацией Dr.Web ConfigD всегда запускается с правами суперпользователя (*root*). Он запускает остальные компоненты Dr.Web Server Security Suite и связывается с ними через предварительно открытый сокет. Демон управления конфигурацией принимает подключения от прочих компонентов Dr.Web Server Security Suite через информационный сокет (доступен публично) и административный сокет (доступен только компонентам, запущенным с правами суперпользователя). Демон загружает параметры конфигурации и лицензионные данные из файлов или обеспечивает их получение от используемого сервера централизованной защиты через агент Dr.Web ES Agent, а также подстановку корректных значений по умолчанию для параметров конфигурации. К моменту старта любого компонента или отсылки ему сигнала SIGHUP демон управления конфигурацией всегда имеет целостный непротиворечивый набор настроек всех компонентов Dr.Web Server Security Suite.

При получении сигнала SIGHUP Dr.Web ConfigD перечитывает параметры конфигурации и данные из лицензионного ключевого файла. В случае необходимости демон также рассылает компонентам уведомления, чтобы они перечитали собственные параметры конфигурации.

При получении сигнала SIGTERM Dr.Web ConfigD сначала завершает работу всех компонентов, а потом сам завершает работу. Dr.Web ConfigD обеспечивает удаление всех временных файлов компонентов после того, как они завершат работу.

Принципы взаимодействия с другими компонентами

1. При запуске все компоненты получают от Dr.Web ConfigD параметры конфигурации и лицензионную информацию. В дальнейшей работе компоненты используют только эти полученные настройки.
2. Dr.Web ConfigD обеспечивает сбор сообщений от всех запущенных под его управлением компонентов в единый журнал. Dr.Web ConfigD собирает все сообщения, выводимые компонентами в *stderr*, и помещает в общий журнал Dr.Web Server Security Suite с отметкой, у какого компонента и в какой момент произошла ошибка.
3. Все управляемые компоненты завершают работу с определенным кодом. Если код завершения отличен от `101`, `102` и `103`, компонент будет перезапущен, а соответствующее сообщение из *stderr* будет зафиксировано в журнале Dr.Web Server Security Suite.
   - Завершение работы с кодом 101 означает, что компонент не может функционировать с предоставленной лицензией. Компонент будет перезапущен только при изменении параметров лицензии.
   - Завершение работы с кодом 102 означает, что он не может функционировать с текущими параметрами конфигурации. Dr.Web ConfigD предпримет попытку перезапустить компонент, когда будет изменены какие-либо параметры конфигурации.
   - Завершение работы с кодом `103` происходит в результате длительного отсутствия обращений к компонентам, запускаемым Dr.Web ConfigD по требованию (Dr.Web Scanning Engine и Dr.Web File Checker). Период, по истечении которого компонент завершает работу с кодом `103`, указывается в настройках соответствующего компонента (параметр `IdleTimeLimit`).
   - Если новые значения параметров конфигурации, полученные компонентом от Dr.Web ConfigD, не могут быть применены «на лету», компонент завершает работу с кодом `0`, чтобы Dr.Web ConfigD перезапустил его.
   - Если компонент не может подключиться к Dr.Web ConfigD или происходит ошибка протокола взаимодействия, компонент отправляет соответствующее сообщение в *stderr* и завершает работу с кодом `1`.

4. Организован обмен сигналами.
   - Чтобы компонент применил измененные параметры конфигурации, Dr.Web ConfigD отправляет ему сигнал SIGHUP.
   - Чтобы компонент завершил работу, Dr.Web ConfigD отправляет ему сигнал SIGTERM. Компонент должен завершить работу в течение 30 секунд после получения сигнала.
   - Если компонент не завершает работу в течение положенных 30 секунд, Dr.Web ConfigD отправляет ему сигнал SIGKILL для принудительного завершения работы.

9.1.2. Аргументы командной строки

Чтобы запустить демон управления конфигурацией Dr.Web ConfigD из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-configd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-configd [<параметры>]
```

Dr.Web ConfigD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет
`--config`	Назначение: Использовать при работе указанный конфигурационный файл. Краткий вариант: `-c` Аргументы: <*путь к файлу*> — путь к используемому конфигурационному файлу.
`--daemonize`	Назначение: Запустить компонент в режиме демона, т. е. без доступа к терминалу. Краткий вариант: `-d` Аргументы: Нет
`--pid-file`	Назначение: Использовать при работе указанный PID-файл. Краткий вариант: `-p` Аргументы: <*путь к файлу*> — путь к файлу, в котором следует сохранить идентификатор процесса (PID).

Пример:

```
$ /opt/drweb.com/bin/drweb-configd -d -c /etc/opt/drweb.com/drweb.ini
```

Приведенная команда запустит Dr.Web ConfigD в режиме демона, заставив его использовать конфигурационный файл `/etc/opt/drweb.com/drweb.ini`.

Замечания о запуске

Для обеспечения работоспособности Dr.Web Server Security Suite компонент должен быть запущен в режиме демона. В штатном режиме Dr.Web ConfigD запускается при старте операционной системы, для чего он оснащен скриптом управления с именем `drweb-configd`, размещенным в системном каталоге (`/etc/init.d` для GNU/Linux или `/usr/local/etc/rc.d` для FreeBSD). Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки (запускается командой `drweb-ctl`).



Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-configd`.

9.1.3. Параметры конфигурации

Демон управления конфигурацией Dr.Web ConfigD использует параметры, указанные в секции `[Root]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента Dr.Web ConfigD. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала демона управления конфигурацией, а также метод ведения журнала для тех компонентов, у которых не указан свой собственный метод ведения журнала.

Параметр	Описание
	При начальной загрузке, пока конфигурационный файл еще не прочитан, демон управления конфигурацией будет использовать следующие значения этого параметра: • в режиме демона (если был запущен с параметром `-d`) — `SYSLOG:Daemon`; • в ином случае — `Stderr`. Если компонент работает в фоновом режиме (запущен с параметром командной строки `-d`), значение `Stderr` *не может* быть использовано для данного параметра. Значение по умолчанию: `SYSLOG:Daemon`
`PublicSocketPath` *{путь к файлу}*	Путь к сокету, используемому для взаимодействия всех компонентов Dr.Web Server Security Suite. Значение по умолчанию: `/var/run/.com.drweb.public`
`AdminSocketPath` *{путь к файлу}*	Путь к сокету, используемому для взаимодействия компонентов Dr.Web Server Security Suite, обладающих повышенными (административными) привилегиями. Значение по умолчанию: `/var/run/.com.drweb.admin`
`DebugIpc` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC (взаимодействие демона управления конфигурацией с другими компонентами). Значение по умолчанию: `No`
`UseCloud` *{логический}*	Использовать или не использовать сервис Dr.Web Cloud для получения сведений о вредоносности файлов и URL. Значение по умолчанию: `No`
`UseMesh` *{логический}*	Использовать или не использовать для проверки компонент Dr.Web MeshD. Если этот параметр выключен, для проверки вместо Dr.Web MeshD используется Dr.Web Scanning Engine. Возможные значения: • `On`, `Yes`, `True` — использовать Dr.Web MeshD; • `Off`, `No`, `False` — не использовать Dr.Web MeshD. Если компонент Dr.Web MeshD не установлен, то вне зависимости от указанного значения будет использоваться компонент Dr.Web Scanning Engine. Если ни один из компонентов не установлен, то проверка завершается с ошибкой x119. Значение по умолчанию: `No`

Параметр	Описание
`UseVxcube` *{логический}*	Использовать или не использовать Dr.Web vxCube при проверке почтовых вложений в режиме внешнего фильтра, подключенного к MTA. Значение по умолчанию: `No`
`KeyPath` *{путь к файлу}*	Путь к ключевому файлу (лицензионному или демонстрационному). Значение по умолчанию: • для GNU/Linux: `/etc/opt/drweb.com/drweb32.key` • для FreeBSD: `/usr/local/etc/drweb.com/drweb32.key`
`CoreEnginePath` *{путь к файлу}*	Путь к динамической библиотеке антивирусного ядра Dr.Web Virus-Finding Engine. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/lib/drweb32.dll` • для FreeBSD: `/var/drweb.com/lib/drweb32.dll`
`VirusBaseDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы вирусных баз. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/bases` • для FreeBSD: `/var/drweb.com/bases`
`VersionDir` *{путь к каталогу}*	Путь к каталогу, в котором хранится информация о текущих версиях используемых компонентов Dr.Web Server Security Suite. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/version` • для FreeBSD: `/var/drweb.com/version`
`CacheDir` *{путь к каталогу}*	Путь к каталогу кеша (используется как для кеша обновлений, так и для кеша проверенных файлов). Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/cache` • для FreeBSD: `/var/drweb.com/cache`
`TempDir` *{путь к каталогу}*	Путь к каталогу для хранения временных файлов. Значение по умолчанию: *Путь, извлеченный из системной переменной окружения* `TMPDIR`, `TMP`, `TEMP` или `TEMPDIR` (переменные перебираются в указанном порядке). Если ни одна из них не обнаружена, то используется `/tmp`.
`RunDir` *{путь к каталогу}*	Путь к каталогу, в котором находятся PID-файлы запущенных компонентов и сокеты, используемые для взаимодействия компонентов Dr.Web Server Security Suite. Значение по умолчанию: `/var/run`

Параметр	Описание
`VarLibDir` *{путь к каталогу}*	Путь к каталогу библиотек, используемых компонентами Dr.Web Server Security Suite. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/lib` • для FreeBSD: `/var/drweb.com/lib`
`AdminGroup` *{имя группы | GID}*	Группа пользователей, обладающих административными правами в рамках Dr.Web Server Security Suite. Данные пользователи, наряду с суперпользователем (пользователем *root*), могут повышать привилегии компонентов Dr.Web Server Security Suite до привилегий суперпользователя. Значение по умолчанию: *Определяется автоматически* в момент установки Dr.Web Server Security Suite
`VersionNotification` *{логический}*	Уведомлять или не уведомлять пользователя о наличии обновлений для текущей установленной версии Dr.Web Server Security Suite. Значение по умолчанию: `Yes`
`DefaultLogLevel` *{уровень подробности}*	Уровень подробности ведения журнала *для всех компонентов* Dr.Web Server Security Suite по умолчанию. Используется, если в конфигурации какого-либо из компонентов не указан свой уровень подробности ведения журнала. Значение по умолчанию: `Notice`
`VxcubeApiAddress` *{строка}*	Доменное имя (FQDN) или IP-адрес узла, на котором находится сервер API Dr.Web vxCube. Значение по умолчанию: *(не задано)*
`VxcubeApiKey` *{строка}*	Ключ API Dr.Web vxCube. Значение по умолчанию: *(не задано)*
`VxcubeProxyUrl` *{адрес подключения}*	Адрес прокси-сервера, который используется для подключения к Dr.Web vxCube. Поддерживаются только HTTP-прокси без авторизации. Возможные значения: <*адрес подключения*> — параметры подключения к прокси-серверу в формате `http://`<*хост*>`:`<*порт*>, где: • <*хост*> — адрес узла, на котором работает прокси-сервер (IP-адрес или имя домена, т. е. FQDN); • <*порт*> — используемый порт. Значение по умолчанию: *(не задано)*

9.2. Dr.Web Ctl

В этом разделе

- Общие сведения
- Удаленная проверка узлов

Общие сведения

Имеется возможность управлять работой Dr.Web Server Security Suite из командной строки. Для этого в его состав входит специальная утилита Dr.Web Ctl (`drweb-ctl`). С ее помощью вы можете выполнять из командной строки следующие действия:

- запуск проверки файлов, загрузочных записей дисков и исполняемых файлов активных процессов;
- запуск проверки файлов на удаленных узлах сети (см. примечание);
- запуск обновления антивирусных компонентов (вирусных баз, антивирусного ядра, и прочих, в зависимости от поставки);
- просмотр и изменение параметров конфигурации Dr.Web Server Security Suite;
- просмотр состояния компонентов Dr.Web Server Security Suite и статистики обнаруженных угроз;
- просмотр карантина и управление его содержимым (через компонент Dr.Web File Checker);
- подключение к серверу централизованной защиты или отключение от него.

Чтобы команды управления, вводимые пользователем, имели эффект, должен быть запущен демон управления конфигурацией Dr.Web ConfigD (по умолчанию он автоматически запускается при старте операционной системы).



Для выполнения некоторых управляющих команд требуются полномочия суперпользователя.

Для получения полномочий суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Утилита `drweb-ctl` поддерживает стандартное автодополнение команд управления Dr.Web Server Security Suite, если функция автодополнения включена в используемой вами командной оболочке. В случае если командная оболочка не поддерживает автодополнение, вы можете настроить ее при необходимости. Для этого обратитесь к справочному руководству по используемому вами дистрибутиву операционной системы.

При завершении работы утилита возвращает код выхода в соответствии с соглашением для POSIX-совместимых систем: 0 (нуль) — если операция выполнена успешно, и не нуль — в противном случае.

Ненулевой код выхода утилита возвращает только в том случае, когда произошла внутренняя ошибка (например: утилита не смогла подключиться к некоторому компоненту, запрошенная операция не может быть выполнена и т. п.). Если утилита обнаруживает (и, возможно) нейтрализует некоторую угрозу, она возвращает код выхода 0, так как запрошенная операция (такая как `scan` и т. п.) выполнена успешно. Если необходимо установить перечень обнаруженных угроз и примененных к ним действий, то проанализируйте сообщения, которые утилита выводит на консоль.

Коды всех имеющихся ошибок приведены в разделе Приложение Е. Описание известных ошибок.

Удаленная проверка узлов

Dr.Web Server Security Suite позволяет проверять на наличие угроз файлы, находящиеся на удаленных узлах сети. В качестве таких узлов могут выступать не только полноценные вычислительные машины (рабочие станции и серверы), но и роутеры, ТВ-приставки и прочие «умные» устройства, образующие так называемый «интернет вещей». Для выполнения удаленной проверки требуется, чтобы удаленный узел предоставлял возможность удаленного доступа к нему через *SSH* (*Secure Shell*) или *Telnet*. Для доступа к устройству вы должны знать его IP-адрес или доменное имя, имя и пароль пользователя, который может совершить удаленный доступ к системе через *SSH* или *Telnet*. Указанный пользователь должен иметь права доступа к проверяемым файлам (как минимум — право на их чтение).

Данная функция может быть использована только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Устранение угроз (то есть изоляция их в карантин, удаление или лечение вредоносных объектов) средствами удаленной проверки невозможно. Для устранения обнаруженных угроз на удаленном узле воспользуйтесь средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров и прочих «умных» устройств вы можете обновить прошивку, а для вычислительных машин — подключиться к ним (в том числе в удаленном терминальном режиме) и произвести соответствующие операции в их файловой системе (удаление или перемещение файлов и т. п.) или запустить установленное на них антивирусное ПО.

Удаленная проверка реализуется только через утилиту управления из командной строки `drweb-ctl` (используется команда `remotescan`).

9.2.1. Формат вызова из командной строки

Утилита управления работой Dr.Web Server Security Suite имеет следующий формат вызова:

```
$ drweb-ctl [<общие опции> | <команда> [<аргумент>] [<опции команды>]]
```

где:

- *<общие опции>* — опции, которые могут быть использованы при запуске без указания команды или для любой из команды. Не являются обязательными для запуска.
- *<команда>* — команда, которая должна быть выполнена Dr.Web Server Security Suite (например, запустить проверку файлов, вывести содержимое карантина и т. п.).
- *<аргумент>* — аргумент команды. Зависит от указанной команды. У некоторых команд аргументы отсутствуют.
- *<опции команды>* — опции, управляющие работой указанной команды. Зависят от команды. У некоторых команд опции отсутствуют.

9.2.2. Общие опции

Доступны следующие общие опции:

Опция	Описание
`-h, --help`	Вывести на экран краткую общую справку и завершить работу. Для вывода справки по любой команде используйте вызов: `$ drweb-ctl <команда> -h`
`-v, --version`	Вывести на экран версию модуля и завершить работу
`-d, --debug`	Предписывает выводить на экран расширенные диагностические сообщения во время выполнения указанной команды. Не имеет смысла без указания команды. Используйте вызов: `$ drweb-ctl <команда> -d`

9.2.3. Команды

В этом разделе

- Команды антивирусной проверки
- Команды управления угрозами и карантином
- Команды управления конфигурацией
- Расширенные команды
  - Команды управления обновлением и работой в режиме централизованной защиты

- Информационные команды

9.2.3.1. Команды антивирусной проверки

Доступны следующие команды антивирусной проверки файловой системы:

Команда	Описание
`scan <путь>`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker указанного файла или каталога. **Аргументы** *<путь>* — путь к файлу или каталогу, который нужно проверить (может быть относительным). Этот аргумент может быть опущен в случае использования опции `--stdin` или `--stdin0`. Для проверки перечня файлов, выбираемых по некоторому условию, рекомендуется использовать утилиту `find` (см. Примеры использования) и опцию `--stdin` или `--stdin0`. **Опции** `-a [--Autonomous]` — запустить автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. ⚠ Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`, также о них не будет сообщено серверу централизованной защиты, если Dr.Web Server Security Suite работает под его управлением. `--Report <тип>` — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout <интервал времени>` — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--FollowSymlinks` — автоматически разрешать символические ссылки. `--PackerMaxLevel <число>` — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite,

Команда	Описание
	ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Значение должно быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <*число*> — ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (*b, kb, mb, gb*). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *(не задано)*. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`.

Команда	Описание
	`--Exclude` <*путь*> — путь, исключаемый из проверки. Может быть относительным и включать в себя файловую маску (содержащую символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`). Необязательная опция; может быть указана более одного раза. `--OnKnownVirus` <*действие*> — действие, которое нужно выполнить, если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnIncurable` <*действие*> — действие, которое нужно выполнить, если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnSuspicious` <*действие*> — действие, которое нужно выполнить, если эвристический анализ обнаружит подозрительный объект. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnAdware` <*действие*> — действие, которое нужно выполнить, если обнаружена рекламная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnDialers` <*действие*> — действие, которое нужно выполнить, если обнаружена программа дозвона. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnJokes` <*действие*> — действие, которое нужно выполнить, если обнаружена программа-шутка. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnRiskware` <*действие*> — действие, которое нужно выполнить, если обнаружена потенциально опасная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnHacktools` <*действие*> — действие, которое нужно выполнить, если обнаружена программа взлома. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`.

Команда	Описание
	Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т. п.), вместо удаления (`DELETE`) выполняется перемещение контейнера в карантин (`QUARANTINE`). `--stdin` — получить список путей для проверки из стандартного потока ввода (*stdin*). Пути в списке должны быть разделены символом новой строки (`\n`). `--stdin0` — получить список путей для проверки из стандартного потока ввода (*stdin*). Пути в списке должны быть разделены нулевым символом NUL (`\0`). При использовании опций `--stdin` и `--stdin0` пути в списке не должны содержать шаблонов. Предпочтительное использование опций `--stdin` и `--stdin0` — обработка в команде `scan` списка путей, сформированного внешней программой, например, `find` (см. Примеры использования).
`bootscan` *<устройство>* | `ALL`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker загрузочной записи на указанных дисковых устройствах. Проверяются как записи MBR, так и записи VBR. **Аргументы** *<устройство>* — путь к блочному файлу дискового устройства, загрузочная запись на котором подлежит проверке. Может быть указано несколько дисковых устройств через пробел. Обязательный аргумент. Если вместо файла устройства указано `ALL`, будут проверены все загрузочные записи на всех доступных дисковых устройствах. **Опции** `-a [--Autonomous]` — запустить автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`, также о них не будет сообщено серверу централизованной защиты, если Dr.Web Server Security Suite работает под его управлением. `--Report` *<тип>* — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет;

Команда	Описание
	• `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--Cure` <*Yes*|*No*> — требуется ли делать попытки лечения обнаруженных угроз. Если указано `No`, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: `No`. `--ShellTrace` — включить вывод дополнительной отладочной информации при проверке загрузочной записи
`procscan`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker содержимого исполняемых файлов, содержащих код процессов, запущенных в системе. При обнаружении угрозы выполняется не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него. **Аргументы**: Нет. ⚠ Эта команда предназначена только для дистрибутивов Dr.Web Server Security Suite, работающих под управлением ОС семейства GNU/Linux. **Опции** `-a [--Autonomous]` — запустить автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. ⚠ Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`, также о них не будет сообщено серверу централизованной защиты, если Dr.Web Server Security Suite работает под его управлением. `--Report` <*тип*> — тип отчета о проверке.

Команда	Описание
	Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--Exclude` <*путь*> — путь, исключаемый из проверки. Может включать в себя файловую маску (содержащую символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`). Путь (в том числе содержащий маску) должен быть абсолютным. Необязательная опция; может быть указана более одного раза. `--OnKnownVirus` <*действие*> — действие, которое нужно выполнить, если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnIncurable` <*действие*> — действие, которое нужно выполнить, если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`.

Команда	Описание
	Значение по умолчанию: `REPORT`. `--OnSuspicious` <*действие*> — действие, которое нужно выполнить, если эвристический анализ обнаружит подозрительный объект. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnAdware` <*действие*> — действие, которое нужно выполнить, если обнаружена рекламная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnDialers` <*действие*> — действие, которое нужно выполнить, если обнаружена программа дозвона. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnJokes` <*действие*> — действие, которое нужно выполнить, если обнаружена программа-шутка. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnRiskware` <*действие*> — действие, которое нужно выполнить, если обнаружена потенциально опасная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnHacktools` <*действие*> — действие, которое нужно выполнить, если обнаружена программа взлома. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`.  При обнаружении угроз в исполняемом файле все запущенные из него процессы принудительно завершаются Dr.Web Server Security Suite.
`memscan --Cure` <*логическое значение*>	**Назначение**: Инициировать проверку процессов. В отличие от [команды] `procscan`, проверка осуществляется только в оперативной памяти. **Аргументы**: Нет. **Опции** `--Cure` <*логическое значение*> — лечить угрозу при ее обнаружении. Обязательный параметр. Возможные значения: • `On`, `Yes`, `True` — лечить угрозу при ее обнаружении; • `Off`, `No`, `False` — не лечить угрозу при ее обнаружении.

Команда	Описание
	`--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного процесса в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `-d [--Debug]` — вывести на экран расширенные диагностические сообщения во время выполнения указанной команды.
`netscan [`<*путь*>`]`	**Назначение**: Инициировать распределенную проверку указанного файла или каталога через агент сетевой проверки данных Dr.Web Network Checker. Если настроенные соединения с другими узлами, на которых имеется продукт Dr.Web для Unix, поддерживающий функцию распределенной проверки, отсутствуют, то будет произведена проверка с использованием сканирующего ядра, доступного локально (аналогично команде `scan`). **Аргументы** <*путь*> — путь к файлу или каталогу, который нужно проверить. Если этот аргумент опущен, то производится сканирование данных, поступающих через входной поток stdin. **Опции** `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие

Команда	Описание
	запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Значение должно быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <*число*> — ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (*b, kb, mb, gb*). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *(не задано)*. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--Cure` <*Yes*|*No*> — требуется ли делать попытки лечения обнаруженных угроз.

Команда	Описание
	Если указано `No`, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: `No`
`rawscan <путь>`	**Назначение**: Инициировать «сырую» проверку указанного файла или каталога с использованием сканирующего ядра Dr.Web Scanning Engine напрямую, без использования компонента проверки файлов Dr.Web File Checker.  Угрозы, обнаруженные при «сыром» сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`. Рекомендуется использовать эту команду только для отладки функционирования Dr.Web Scanning Engine. Команда имеет следующую особенность: она выводит заключение «cured» (вылечен), если нейтрализована, по меньшей мере, *одна* из угроз, обнаруженных в файле (не обязательно *все* из них). Таким образом, *не рекомендуется* использовать эту команду, если требуется надежное сканирование файлов. Вместо этого для проверки файлов и каталогов рекомендуется использовать команду `scan`. **Аргументы** <*путь*> — путь к файлу или каталогу, который нужно проверить. **Опции** `--ScanEngine` <*путь*> — путь к Unix-сокету сканирующего ядра Dr.Web Scanning Engine. Если не указан, то для проверки будет запущен автономный экземпляр сканирующего ядра (будет завершен после окончания проверки). `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным

Команда	Описание
	объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <*число*> — ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (*b, kb, mb, gb*). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *(не задано)*. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке.

Команда	Описание
	Значение по умолчанию: `On`. `--Cure` <*Yes*|*No*> — требуется ли делать попытки лечения обнаруженных угроз. Если указано `No`, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: `No`. `--ListCleanItem` — включить вывод списка чистых файлов при проверке контейнера. `--ShellTrace` — включить вывод дополнительной отладочной информации при проверке файла. `--Output` <*путь к файлу*> — дублировать вывод команды в указанный файл
`remotescan` <*узел*> <*путь*>	**Назначение**: Инициировать проверку указанного файла или каталога на указанном удаленном узле, подключившись к нему через *SSH* или *Telnet*. ⚠ Угрозы, обнаруженные при удаленном сканировании, не будут нейтрализованы, более того, они не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats`. Вы можете использовать эту команду только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров, ТВ-приставок и прочих «умных» устройств вы можете воспользоваться механизмом обновления прошивки, а для вычислительных машин — выполнив подключение к ним (в том числе — в удаленном терминальном режиме) и произведя соответствующие операции в их файловой системе (удаление или перемещение файлов и т. п.) или запустив антивирусное ПО, установленное на них. **Аргументы** • <*узел*> — IP-адрес или доменное имя узла, к которому необходимо подключиться для проверки. • <*путь*> — путь к файлу или каталогу, который нужно проверить (должен быть абсолютным).

Команда	Описание
	Опции `-l [--Login]` <*имя*> — логин (имя пользователя) для авторизации на удаленном узле через выбранный протокол. Если имя пользователя не указано, будет произведена попытка подключиться к удаленному узлу от имени пользователя, запустившего команду. `-i [--Identity]` <*путь к файлу*> — файл закрытого ключа для аутентификации указанного пользователя через выбранный протокол. Команда `remotescan` предназначена для сканирования маршрутизаторов SOHO (Small Office / Home Office). Ключ в формате, используемом по умолчанию утилитой `ssh-keygen`, не поддерживается. Для проверки удаленного узла по SSH требуется ключ в формате PEM, который можно сгенерировать командой: `$ ssh-keygen -t rsa -m PEM -f rsa_pem` `-m [--Method]` <*SSH|Telnet*> — метод (протокол) подключения к удаленному узлу. Если метод не указан, будет использован SSH. `-p [--Port]` <*число*> — номер порта на удаленном узле для подключения через выбранный протокол. Значение по умолчанию: Порт по умолчанию для выбранного протокола (`22` — для SSH, `23` — для Telnet). `--UseChannels` <*число*> — число каналов передачи данных. Значение по умолчанию: `5`. `--Password` <*пароль*> — пароль для аутентификации указанного пользователя через выбранный протокол. Пароль передается в открытом виде. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено.

Команда	Описание
	Значение по умолчанию: `0`. `--PackerMaxLevel <число>` — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel <число>` — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel <число>` — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel <число>` — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio <степень>` — максимально допустимая степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract <число>` — ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (*b, kb, mb, gb*). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *(не задано)*.

Команда	Описание
	`--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--Exclude` <*путь*> — путь, исключаемый из проверки. Может включать в себя файловую маску (содержащую символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`). Путь (в том числе содержащий маску) должен быть абсолютным. Необязательная опция; может быть указана более одного раза. `--TransferListenAddress` <*адрес*> — адрес, прослушиваемый для приема файлов, передаваемых на проверку удаленным устройством. Необязательная опция. Если не указана, используется произвольный адрес. `--TransferListenPort` <*порт*> — порт, прослушиваемый для приема файлов, передаваемых на проверку удаленным устройством. Необязательная опция. Если не указана, используется случайный порт. `--TransferExternalAddress` <*адрес*> — адрес для передачи файлов на проверку, сообщаемый удаленному устройству. Необязательная опция. Если не указана, используется значение опции `--TransferListenAddress`, либо исходящий адрес уже установленной сессии. `--TransferExternalPort` <*порт*> — порт для передачи файлов на проверку, сообщаемый удаленному устройству. Необязательная опция. Если не указана, используется порт, определенный автоматически. `--ForceInteractive` — использовать интерактивную сессию SSH (только для метода подключения SSH). *Необязательная опция.*

9.2.3.2. Команды управления угрозами и карантином

Доступны следующие команды управления угрозами и карантином:

Команда	Описание
`threats` [<*действие*> <*объект*>]	**Назначение**: Выполнить указанное действие с обнаруженными ранее угрозами по их идентификаторам. Тип действия определяется указанной опцией команды. Если действие не указано, то вывести на экран информацию об обнаруженных, но не обезвреженных угрозах. Информация об угрозах выводится в соответствии с форматом, заданным необязательной опцией `--Format`. Если опция `--Format` не указана, то для каждой угрозы выводится следующая информация: • идентификатор, присвоенный угрозе (порядковый номер);

Команда	Описание
	• полный путь к инфицированному файлу; • информация об угрозе (имя, тип по классификации компании «Доктор Веб»); • информация о файле: размер, пользователь-владелец, дата последнего изменения; • история действий с инфицированным файлом: обнаружение, применявшиеся действия и т. п. **Аргументы**: Нет. **Опции** `--Format "<`*строка формата*`>"` — выводить информацию об угрозах в указанном формате. Описание строки формата приведено ниже. Если эта опция указана совместно с любой из опций-действий, она игнорируется. `-f [--Follow]` — ожидать поступления новых сообщений об угрозах и выводить их сразу при поступлении (CTRL+C прерывает ожидание). Если эта опция указана совместно с любой из опций-действий, она игнорируется. `--Cure <`*список угроз*`>` — выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Quarantine <`*список угроз*`>` — выполнить перемещение в карантин перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Delete <`*список угроз*`>` — выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Ignore <`*список угроз*`>` — игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую). Если требуется применить действие ко всем обнаруженным угрозам, вместо *<список угроз>* укажите `All`. Например, команда: `$ drweb-ctl threats --Quarantine All` перемещает в карантин все обнаруженные объекты с угрозами. `--Directory <`*список каталогов*`>` — выводить только те угрозы, которые были обнаружены в файлах в каталогах из *<списка каталогов>*. Если эта опция указана совместно с любой из опций-действий, она игнорируется.

Команда	Описание
`quarantine [<действие> <объект>]`	**Назначение**: Применить действие к указанному объекту, находящемуся в карантине. Если действие не указано, то вывести на экран информацию об объектах, находящихся в карантине, с указанием их идентификаторов и краткой информации об исходных файлах, перемещенных в карантин. Информация об изолированных объектах выводится в соответствии с форматом, заданным необязательной опцией `--Format`. Если опция `--Format` не указана, то для каждого изолированного объекта выводится следующая информация: • идентификатор, присвоенный изолированному объекту в карантине; • исходный путь к файлу, перемещенному в карантин; • дата перемещения файла в карантин; • информация о файле: размер, пользователь-владелец, дата последнего изменения; • информация об угрозе (имя, тип по классификации компании «Доктор Веб»). **Аргументы**: Нет. **Опции** `--Format "<строка формата>"` — выводить информацию об объектах, находящихся в карантине, в указанном формате. Описание строки формата приведено ниже. Если эта опция указана совместно с любой из опций-действий, она игнорируется. `-f [--Follow]` — ожидать поступления новых сообщений об угрозах и выводить их сразу при поступлении (CTRL+C прерывает ожидание). Если эта опция указана совместно с любой из опций-действий, она игнорируется. `-a [--Autonomous]` — запустить автономный экземпляр компонента проверки файлов Dr.Web File Checker для выполнения заданного действия с карантином, завершив работу компонента после окончания действия. Эта опция может быть применена совместно с любой из опций, указанных ниже. `--Discovery [<список каталогов>,]` — произвести поиск каталогов карантина в указанном списке каталогов и добавить их к консолидированному карантину в случае обнаружения. Если `<список каталогов>` не указан, то произвести поиск каталогов карантина в стандартных местах файловой системы (точки монтирования томов и домашние каталоги пользователей).

Команда	Описание

	Эта опция может быть указана совместно не только с опцией `-a` (`--Autonomous`) (см. выше), но и с любой из опций-действий, перечисленных ниже. Более того, если команда `quarantine` запускается в режиме автономного экземпляра, т. е. с опцией `-a` (`--Autonomous`), но без опции `--Discovery`, то это равносильно вызову:
	`quarantine --Autonomous --Discovery`
	`--Delete` <*объект*> — удалить указанный объект, помещенный в карантин.
	Удаление объекта, помещенного в карантин — необратимая операция.
	`--Restore` <*объект*> — восстановить указанный объект из карантина в исходное место.
	Для выполнения этого действия может потребоваться, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). Восстановить файл из карантина можно, даже если он инфицирован.
	`--Cure` <*объект*> — попытаться вылечить указанный объект в карантине.
	Даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина воспользуйтесь опцией восстановления `--Restore`.
	`--TargetPath` <*путь*> — восстановить объект из карантина в указанное место: как файл с указанным именем, если <*путь*> — это путь к файлу, или в указанный каталог (если <*путь*> — это путь к каталогу). Может быть указан как абсолютный путь, так и относительный (относительно текущего каталога).
	Опция применяется только совместно с опцией восстановления `--Restore`.
	В качестве <*объект*> используется идентификатор объекта в карантине. Если требуется применить действие ко всем объектам, находящимся в карантине, вместо <*объект*> укажите `All`. Например, команда
	`$ drweb-ctl quarantine --Restore All --TargetPath test`

Команда	Описание
	восстанавливает из карантина все имеющиеся в нем объекты, помещая их в подкаталог `test`, находящийся в текущем каталоге, из которого запущена команда `drweb-ctl`. Если для варианта `--Restore All` указана дополнительная опция `--TargetPath`, то она должна задавать путь к каталогу, а не к файлу.

Если в настройках SpIDer Guard для NSS для некоторого типа угроз указано действие `QUARANTINE`, то при восстановлении угрозы этого типа из карантина на том NSS при помощи команды `quarantine`, она будет снова незамедлительно перемещена в карантин. Например, настройки по умолчанию:

```
NSS.OnKnownVirus = CURE
NSS.OnIncurable = QUARANTINE
```

помещают все неизлечимые объекты в карантин. Поэтому, при восстановлении неизлечимого объекта из карантина на том NSS при помощи команды `quarantine`, он будет снова незамедлительно перемещен в карантин.

Форматированный вывод данных для команд threats и quarantine

Формат вывода задается строкой формата, указанной в качестве аргумента необязательной опции `--Format`. Строка формата обязательно указывается в кавычках. Строка формата может включать в себя как обычные символы (будут выведены на экран «как есть»), так и специализированные маркеры, которые при выводе будут заменены на соответствующую информацию. Доступны следующие маркеры:

1. Общие для команд `threats` и `quarantine`:

Маркер	Описание
`%{n}`	Перевод строки
`%{t}`	Табуляция
`%{threat_name}`	Имя обнаруженной угрозы по классификации компании «Доктор Веб»
`%{threat_type}`	Тип угрозы («known virus» и т. д.) по классификации компании «Доктор Веб»
`%{size}`	Размер исходного файла

Маркер	Описание
`%{origin}`	Полное имя исходного файла с путем
`%{path}`	Синоним `%{origin}`
`%{ctime}`	Дата/время модификации исходного файла в формате "*%Y-%b-%d %H:%M:%S*" (например, "`2018-Jul-20 15:58:01`")
`%{timestamp}`	То же, что и `%{ctime}`, но в формате времени *Unix timestamp*
`%{owner}`	Пользователь-владелец исходного файла
`%{rowner}`	Удаленный пользователь-владелец исходного файла (если не применимо или значение неизвестно — заменяется на `?`)

2. Специфические для команды `threats`:

Маркер	Описание
`%{hid}`	Идентификатор записи об угрозе в реестре истории событий, связанных с угрозой
`%{tid}`	Идентификатор угрозы
`%{htime}`	Дата/время события, связанного с угрозой
`%{app}`	Идентификатор компонента Dr.Web Server Security Suite, обработавшего угрозу
`%{event}`	Последнее событие, связанное с угрозой: • `FOUND` — угроза была обнаружена; • `CURE` — угроза была вылечена; • `QUARANTINE` — файл с угрозой был перемещен в карантин; • `DELETE` — файл с угрозой был удален; • `IGNORE` — угроза была проигнорирована; • `RECAPTURED` — угроза была обнаружена другим компонентом
`%{err}`	Текст сообщения об ошибке (если ошибки нет — заменяется на пустую строку)

3. Специфические для команды `quarantine`:

Маркер	Описание
`%{qid}`	Идентификатор объекта в карантине
`%{qtime}`	Дата/время перемещения объекта в карантин
`%{curetime}`	Дата/время попытки лечения объекта, перемещенного в карантин (если не применимо или значение неизвестно — заменяется на `?`)

Маркер	Описание
`%{cureres}`	Результат попытки лечения объекта, перемещенного в карантин: • `cured` — угроза вылечена; • `not cured` — угроза не вылечена либо попыток лечения не производилось

Пример

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%{n}}"
```

Данная команда выведет содержимое карантина в виде записей следующего вида:

```
{
 <путь к файлу>: <имя угрозы> - <дата перемещения в карантин>
}
...
```

9.2.3.3. Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
`cfset` <*секция*>`.`<*параметр*> <*значение*>	**Назначение**: Изменить активное значение указанного параметра текущей конфигурации Dr.Web Server Security Suite. **Аргументы** • <*секция*> — имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент. • <*параметр*> — имя изменяемого параметра. Обязательный аргумент. • <*значение*> — новое значение параметра. Обязательный аргумент.

Команда	Описание
	Для задания значения параметров всегда используется формат <*секция*>.<*параметр*> <*значение*>, знак присваивания = не используется. Если вы хотите задать несколько значений параметра, то нужно повторить вызов команды `cfset` столько раз, сколько значений параметра вы хотите добавить. При этом для добавления нового значения в список значений параметра необходимо использовать опцию `-a` (см. ниже). Нельзя указывать в качестве аргумента последовательность <*параметр*> <*значение 1*>, <*значение 2*>, так как строка "<*значение 1*>, <*значение 2*>" будет считаться единым значением параметра <*параметр*>. Описание конфигурационного файла доступно в разделе Приложение Г. Конфигурационный файл Dr.Web Server Security Suite, а также в документации `man 5 drweb.ini`. **Опции** `-a [--Add]` — не заменять текущее значение параметра, а добавить указанное значение в список значений параметра (допустимо только для параметров, которые могут иметь список значений). Также эту опцию необходимо использовать для добавления новых групп параметров с тегом. `-e [--Erase]` — не заменять текущее значение параметра, а удалить указанное значение из его списка (допустимо только для параметров, которые имеют список значений). `-r [--Reset]` — сбросить параметр в значение по умолчанию. <*значение*> в этом случае в команде не указывается, а если указано — игнорируется. Опции не являются обязательными. Если они не указаны, то текущее значение параметра (в том числе список значений) заменяется на указанное значение. Для секций, описывающих индивидуальные параметры точек подключения компонента Dr.Web ClamD и разделяемых каталогов для монитора SpIDer Guard для SMB, применение опции `-r` приводит к замене значения параметра в

Команда	Описание

	индивидуальной секции на значение, указанное у соответствующего «родительского» параметра в секции настроек компонента.
	
	Если требуется добавить новую точку подключения <*point*> для Dr.Web ClamD или секцию параметров для разделяемого каталога Samba с тегом <*tag*>, выполните команду
	
	`cfset ClamD.Endpoint.<point> -a`
	
	например:
	
	`cfset ClamD.Endpoint.point1 -a`
	
	`cfset SmbSpider.Share.<tag> -a`
	
	например:
	
	`cfset SmbSpider.Share.AccountingFiles -a`
	
	Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды `su` или `sudo`.

`cfshow [<секция>[.<параметр>]]`	**Назначение**: Вывести на экран параметры текущей конфигурации Dr.Web Server Security Suite. Для вывода параметров по умолчанию используется формат <*секция*>.<*параметр*> = <*значение*>. Секции и параметры не установленных компонентов по умолчанию не выводятся. **Аргументы** • <*секция*> — имя секции конфигурационного файла, параметры которой нужно вывести на экран. Необязательный аргумент. Если не указан, то на экран выводятся параметры всех секций конфигурационного файла. • <*параметр*> — имя выводимого параметра. Необязательный аргумент. Если не указан, выводятся все параметры указанной секции, в противном случае выводится только этот параметр. Если указан без имени секции, то выводятся все вхождения этого параметра во все секции конфигурационного файла.

Команда	Описание
	Опции `--Uncut` — вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. Если не указано, то выводятся только те параметры, которые используются имеющимися компонентами. `--Changed` — вывести только те параметры, значения которых отличаются от значений по умолчанию. `--Ini` — вывести значения параметров в формате файла `.ini`: сначала в отдельной строке выводится имя секции, заключенное в квадратные скобки, после чего параметры, принадлежащие секции, перечисляются в виде пар <*параметр*> = <*значение*> (по одному в строке). `--Value` — вывести только значение указанного параметра. В этом случае аргумент <*параметр*> обязателен.
`reload`	**Назначение**: Перезагрузить конфигурацию Dr.Web Server Security Suite. При этом демон управления конфигурацией Dr.Web ConfigD выполняет следующие действия: • перечитывает конфигурацию и рассылает ее изменения всем компонентам Dr.Web Server Security Suite; • переоткрывает журнал Dr.Web Server Security Suite; • запускает компоненты, использующие вирусные базы (включая антивирусное ядро); • пытается запустить компоненты, работа которых была нештатно завершена. **Аргументы**: Нет. **Опции**: Нет

9.2.3.4. Расширенные команды

В этом разделе

- Команды управления обновлением и работой в режиме централизованной защиты
- Информационные команды

9.2.3.4.1. Команды управления обновлением и работой в режиме централизованной защиты

Доступны следующие команды управления обновлением и работой в режиме централизованной защиты:

Команда	Описание
`update`	**Назначение**: Инициировать процесс обновления антивирусных компонентов (вирусных баз, антивирусного ядра и прочих, в зависимости от поставки) с серверов обновлений компании «Доктор Веб», прервать уже запущенный процесс обновления или откатить результаты последнего обновления, восстановив предыдущие версии обновленных файлов. Команда не имеет эффекта, если Dr.Web Server Security Suite работает под управлением сервера централизованной защиты. **Аргументы**: Нет. **Опции** `--Stop` — прервать уже идущий процесс обновления. `--Rollback` — откатить последнее обновление и восстановить последние сохраненные копии обновленных файлов. `--From` <*путь*> — выполнить обновление из указанного каталога без подключения к интернету. `--Path` <*путь*> — сохранить в указанный каталог файлы, которые будут использоваться для обновления без подключения к интернету. Если в этот каталог уже были загружены файлы, то они будут обновлены.
`esconnect` <*сервер*>`[:`<*порт*>`]`	**Назначение**: Подключить Dr.Web Server Security Suite к указанному серверу централизованной защиты. О режимах работы см. в разделе Режимы работы. **Аргументы** • <*сервер*> — IP-адрес или имя узла в сети, на котором располагается сервер централизованной защиты. Обязательный аргумент. • <*порт*> — номер порта, используемого сервером централизованной защиты. Необязательный аргумент, указывается только в случае, если сервер централизованной защиты использует нестандартный порт. **Опции** `--Certificate` <*путь*> — путь к файлу сертификата сервера централизованной защиты, к которому производится подключение.

Команда	Описание
	`--Login` <*ID*> — логин (идентификатор рабочей станции) для подключения к серверу централизованной защиты. `--Password` <*пароль*> — пароль для подключения к серверу централизованной защиты. `--Compress` <*On*|*Off*> — принудительно инициировать сжатие передаваемых данных (`On`) или запретить его (`Off`). Если опция не указана, использование сжатия определяется сервером. `--Encrypt` <*On*|*Off*> — принудительно инициировать шифрование передаваемых данных (`On`) или запретить его (`Off`). Если опция не указана, использование шифрования определяется сервером. `--Newbie` — подключиться как «новичок» (получить новую учетную запись на сервере). `--Group` <*ID*> — идентификатор группы на сервере, в которую следует поместить рабочую станцию при подключении. Указывается только совместно с опцией `--Password`. `--Rate` <*ID*> — идентификатор тарифной группы, которую следует применить к рабочей станции при ее включении в группу на сервере централизованной защиты. Указывается только совместно с опцией `--Group`. `--CfgFile` <*путь*> — подключиться к серверу централизованной защиты, используя конфигурационный файл с настройками соединения. Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`esdisconnect`	**Назначение**: Отключить Dr.Web Server Security Suite от сервера централизованной защиты и перевести его в автономный режим работы. Команда не имеет эффекта, если Dr.Web Server Security Suite уже работает в автономном режиме. **Аргументы**: Нет. **Опции**: Нет. Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды `su` или `sudo`.

9.2.3.4.2. Информационные команды

Доступны следующие информационные команды:

Команда	Описание
`appinfo`	**Назначение**: Вывести на экран информацию о работающих компонентах Dr.Web Server Security Suite. Для каждого запущенного компонента выводится следующая информация: • внутреннее имя; • идентификатор процесса GNU/Linux (PID); • состояние (запущен, остановлен и т. п.); • код ошибки, если работа компонента завершена вследствие ошибки; • дополнительная информация (опционально); Для демона управления конфигурацией (`drweb-configd`) в качестве дополнительной информации выводятся: • перечень установленных компонентов — *Installed*; • перечень компонентов, запуск которых должен быть обеспечен демоном — *Should run*. **Аргументы**: Нет. **Опции** `-f [--Follow]` — ожидать поступления новых сообщений об изменении состояния модулей и выводить их на экран сразу при поступлении (CTRL+C прерывает ожидание)
`baseinfo`	**Назначение**: Вывести на экран информацию о текущей версии антивирусного ядра и состоянии вирусных баз. Выводится следующая информация: • версия антивирусного ядра; • дата и время выпуска используемых вирусных баз; • число доступных записей об угрозах; • момент последнего успешного обновления вирусных баз и антивирусного ядра; • момент следующего запланированного автоматического обновления. **Аргументы**: Нет. **Опции** `-l [--List]` — вывести полный список загруженных файлов вирусных баз данных и число записей об угрозах в каждом файле

Команда	Описание
`events`	**Назначение**: Просмотреть события Dr.Web Server Security Suite. Кроме этого, команда позволяет выполнить управление событиями (отметка как «прочитанные», удаление). **Аргументы**: Нет. **Опции** `--Report` <*тип*> — тип отчета о событиях. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. `-f [--Follow]` — ожидать поступления новых событий и выводить их на экран сразу при поступлении (нажатие CTRL+C прерывает ожидание). `--ShowSeen` — показать также и уже прочитанные события; `-s [--Since]` <*дата, время*> — показывать события, произошедшие не ранее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-u [--Until]` <*дата, время*> — показывать события, произошедшие не позднее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-t [--Types]` <*список типов*> — показывать события только перечисленных типов (типы событий перечисляются через запятую). Доступен следующий тип событий: `UnexpectedAppTermination` — неожиданное завершение работы какого-либо компонента. Для вывода событий всех типов используйте `All`. `--Show` <*список событий*> — вывести на экран перечисленные события (идентификаторы событий перечисляются через запятую); `--Delete` <*список событий*> — удалить перечисленные события (идентификаторы событий перечисляются через запятую); `--MarkAsSeen` <*список событий*> — отметить перечисленные события как «прочитанные» (идентификаторы событий перечисляются через запятую).

Команда	Описание
	Если требуется отметить как «прочитанные» или удалить все события, вместо <*список событий*> укажите `All`. Например, команда `$ drweb-ctl events --MarkAsSeen All` отметит как «прочитанные» все имеющиеся события
`report` <*тип*>	**Назначение**: Сформировать отчет о событиях Dr.Web Server Security Suite в виде страницы HTML (тело страницы выводится в указанный файл). **Аргументы** <*тип*> — тип событий, для которых формируется отчет (указывается один тип). Возможные значения см. в описании опции `--Types` команды `events`. Обязательный аргумент. **Опции** `-o [--Output]` <*путь к файлу*> — сохранить отчет в указанный файл. Обязательная опция. `-s [--Since]` <*дата, время*> — включить в отчет события, произошедшие не ранее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-u [--Until]` <*дата, время*> — включить в отчет события, произошедшие не позднее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `--TemplateDir` <*путь к каталогу*> — путь к каталогу, в котором находятся файлы шаблонов HTML-страницы отчета. Опции `-s`, `-u` и `--TemplateDir` являются необязательными.
`license`	**Назначение**: Вывести на экран информацию об активной лицензии, получить демонстрационную лицензию или получить ключевой файл для уже зарегистрированной лицензии (например, на сайте компании). Если не указана ни одна опция, то выводится следующая информация (если используется лицензия для автономного режима работы): • номер лицензии, • дата и время окончания действия лицензии. Если используется лицензия, выданная сервером централизованной защиты (для работы в режиме централизованной защиты или в мобильном режиме), выводится соответствующая информация. **Аргументы**: Нет.

Команда	Описание
	Опции `--GetDemo` — запросить демонстрационный ключ сроком на месяц и получить его, если не нарушены условия получения демонстрационного периода. `--GetRegistered` <*серийный номер*> — получить лицензионный ключевой файл для указанного серийного номера, если не нарушены условия получения нового ключевого файла (например, программа не находится в режиме централизованной защиты, когда лицензией управляет сервер централизованной защиты). `--NetworkTimeout` <*интервал времени*> — тайм-аут в миллисекундах на сетевые операции при использовании команды `license`. Используется для продолжения активации в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то активация будет продолжена. Если указан `0`, то тайм-аута нет. Значение по умолчанию: `0`. `--Proxy http://`<*имя пользователя*>`:`<*пароль*>`@`<*адрес сервера*>`:`<*номер порта*> — получить лицензионный ключ через прокси-сервер (используется только совместно с одной из предыдущих опций — `--GetDemo` или `--GetRegistered`). *Если серийный номер не является серийным номером демонстрационного периода, то он должен быть предварительно зарегистрирован на сайте компании.* Подробнее о лицензировании продуктов Dr.Web см. раздел Лицензирование. Для регистрации серийного номера и для получения демонстрационного периода требуется наличие подключения к интернету.
`log`	**Назначение**: Вывести в консоль (поток *stdout*) последние записи журнала Dr.Web Server Security Suite (аналогично команде `tail`). **Аргументы**: Нет. **Опции** `-s [--Size]` <*число*> — число последних записей журнала, которые нужно вывести на экран. `-c [--Components]` <*список компонентов*> — список идентификаторов компонентов, записи которых будут выведены. Указываются через пробел. Если параметр не указан, выводятся

Команда	Описание
	все доступные последние записи, отправленные в журнал любым из компонентов. Актуальные идентификаторы установленных компонентов (т. е. внутренние имена компонентов, выводимые в журнал) вы можете узнать, используя команду `appinfo`. `-f [--Follow]` — ожидать поступления новых записей в журнал и выводить их на экран сразу при поступлении (нажатие CTRL+C прерывает ожидание).  Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (обычно пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`stat`	**Назначение**: Вывести на экран статистику работы компонентов, обрабатывающих файлы, либо агента сетевой проверки данных Dr.Web Network Checker (нажатие CTRL+C или Q прерывает отображение статистики). В статистике отображается: • имя компонента, инициировавшего проверку файлов; • PID компонента; • усредненное количество файлов, обрабатываемых в секунду за последнюю минуту, 5 минут, 15 минут; • процент использования кеша проверенных файлов; • среднее количество ошибок проверки в секунду. Для агента распределенной проверки на экран выводится: • перечень локальных клиентов, инициировавших сканирование; • перечень удаленных узлов, которым переданы файлы на сканирование; • перечень удаленных узлов, от которых получены файлы на сканирование. Для локальных клиентов агента распределенной проверки указывается имя и PID, а для удаленных — адрес и порт узла. Для каждого клиента, как локального, так и удаленного выводится: • среднее за секунду количество проверенных файлов; • среднее за секунду количество переданных и полученных байт; • среднее за секунду количество ошибок. **Аргументы**: Нет.

Команда	Описание
	Опции `-n [--Netcheck]` — вывести на экран статистику работы агента сетевой проверки данных

9.2.4. Примеры использования

В этом разделе

- Проверка объектов
  - Простые команды проверки
  - Проверка файлов, отобранных по критериям
  - Проверка дополнительных объектов
- Управление конфигурацией
- Управление угрозами
- Пример работы в режиме автономного экземпляра

Проверка объектов

Простые команды проверки

1. Выполнить проверку каталога `/home` с параметрами по умолчанию:

```
$ drweb-ctl scan /home
```

2. Выполнить проверку списка путей к файлам, перечисленным в файле `daily_scan` (по одному пути в строке файла):

```
$ drweb-ctl scan --stdin < daily_scan
```

3. Выполнить проверку загрузочной записи на дисковом устройстве *sda*:

```
$ drweb-ctl bootscan /dev/sda
```

4. Выполнить проверку запущенных процессов:

```
$ drweb-ctl procscan
```

Проверка файлов, отобранных по критериям

В нижеприведенных примерах для формирования выборки файлов, подлежащих проверке, используется результат работы утилиты `find`. Полученный перечень файлов передается команде `drweb-ctl scan` с параметром `--stdin` или `--stdin0`.

1. Выполнить проверку списка файлов, возвращенных утилитой `find`, и разделенных символом NUL (`\0`):

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. Проверить все файлы всех каталогов, начиная с корневого, находящихся на одном разделе файловой системы:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. Проверить все файлы всех каталогов, начиная с корневого, кроме файлов `/var/log/messages` и `/var/log/syslog`:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog | drweb-ctl scan
--stdin
```

4. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователю *root*:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям *root* и *admin*:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям с UID из диапазона 1000–1005:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. Проверить файлы во всех каталогах, начиная с корневого, но находящихся не более чем на пятом уровне вложенности относительно корневого каталога:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. Проверить файлы в корневом каталоге, не заходя во вложенные каталоги:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. Проверить файлы во всех каталогах, начиная с корневого, при этом следовать по встречающимся символическим ссылкам:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. Проверить файлы во всех каталогах, начиная с корневого, при этом не следовать по встречающимся символическим ссылкам:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. Проверить во всех каталогах, начиная с корневого, файлы, созданные не позже, чем 1 мая 2017 года:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

Проверка дополнительных объектов

Проверка объектов каталога `/tmp` на удаленном узле *192.168.0.1* при подключении к нему через SSH как пользователь *user* с паролем *passw*:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

Управление конфигурацией

1. Вывести на экран информацию о запущенных компонентах Dr.Web Server Security Suite:

```
$ drweb-ctl appinfo
```

2. Вывести на экран все параметры из секции `[Root]`:

```
$ drweb-ctl cfshow Root
```

3. Задать значение `No` для параметра `Start` в секции `[LinuxSpider]` (это приведет к остановке работы монитора файловой системы SpIDer Guard):

```
# drweb-ctl cfset LinuxSpider.Start No
```

Для этого требуются полномочия суперпользователя. Пример вызова этой же команды с использованием `sudo` для временного повышения полномочий:

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Выполнить принудительное обновление антивирусных компонентов Dr.Web Server Security Suite:

```
$ drweb-ctl update
```

5. Выполнить перезагрузку конфигурации для компонентов Dr.Web Server Security Suite:

```
# drweb-ctl reload
```

Для этого требуются полномочия суперпользователя. Пример вызова этой же команды с использованием `sudo` для временного повышения полномочий:

```
$ sudo drweb-ctl reload
```

6. Подключить Dr.Web Server Security Suite к серверу централизованной защиты, работающему на узле *192.168.0.1*, при условии, что сертификат сервера располагается в файле `/home/user/cscert.pem`:

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. Подключить Dr.Web Server Security Suite к серверу централизованной защиты, используя файл настроек подключения `install.cfg`:

```
$ drweb-ctl esconnect --CfgFile <путь к файлу install.cfg>
```

8. Отключить Dr.Web Server Security Suite от сервера централизованной защиты:

```
# drweb-ctl esdisconnect
```

Для этого требуются полномочия суперпользователя. Пример вызова этой же команды с использованием `sudo` для временного повышения полномочий:

```
$ sudo drweb-ctl esdisconnect
```

9. Просмотреть последние записи, внесенные компонентами `drweb-update` и `drweb-configd` в журнал Dr.Web Server Security Suite:

```
# drweb-ctl log -c Update ConfigD
```

Управление угрозами

1. Вывести на экран информацию об обнаруженных угрозах:

```
$ drweb-ctl threats
```

2. Переместить все файлы, содержащие необезвреженные угрозы, в карантин:

```
$ drweb-ctl threats --Quarantine All
```

3. Вывести на экран список файлов, перемещенных в карантин:

```
$ drweb-ctl quarantine
```

4. Восстановить все файлы из карантина:

```
$ drweb-ctl quarantine --Restore All
```

Пример работы в режиме автономного экземпляра

Проверить файлы и обработать карантин в режиме автономного экземпляра:

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=QUARANTINE
$ drweb-ctl quarantine -a --Delete All
```

Первая команда проверит файлы в каталоге `/home/user` в режиме автономного экземпляра, и файлы, содержащие известные угрозы, будут помещены в карантин. Вторая команда обработает содержимое карантина (также в режиме автономного экземпляра) и удалит все содержащиеся в нем объекты.

9.2.5. Параметры конфигурации

Утилита управления из командной строки Dr.Web Ctl не имеет собственной секции параметров в объединенном конфигурационном файле Dr.Web Server Security Suite. Утилита использует параметры, указанные в секции `[Root]`.

9.3. Веб-интерфейс управления Dr.Web

В этом разделе

- Назначение
- Системные требования веб-интерфейса
- Доступ к управлению через веб-интерфейс
- Главное меню

Назначение

Веб-интерфейс управления Dr.Web Server Security Suite позволяет выполнять следующие действия:

- просматривать состояние компонентов Dr.Web Server Security Suite, запускать и останавливать работу некоторых из них;
- просматривать состояние обновлений и запускать обновление вручную при необходимости;
- просматривать состояние лицензии и загружать лицензионный ключ при необходимости;
- просматривать перечень обнаруженных угроз и управлять содержимым карантина (отображаются только угрозы, обнаруженные в файлах локальной файловой системы компонентом Dr.Web File Checker);
- выполнять редактирование настроек компонентов Dr.Web Server Security Suite;
- подключать Dr.Web Server Security Suite к серверу централизованной защиты или переводить его в автономный режим работы;
- запускать проверку локальных файлов по требованию (в том числе перетаскиванием их на страницу, открытую в браузере).

Системные требования веб-интерфейса

Корректная работа веб-интерфейса управления гарантируется в следующих браузерах:

- Microsoft Internet Explorer версии 11 и более поздней;
- Mozilla Firefox версии 25 и более поздней;
- Google Chrome версии 30 и более поздней.

Доступ к управлению через веб-интерфейс

Для доступа к веб-интерфейсу необходимо в адресной строке браузера ввести адрес вида:

```
https://<хост_drweb>:<порт>/
```

где *<xocm_drweb>* — IP-адрес или имя узла, на котором работает Dr.Web Server Security Suite, в составе которого функционирует сервер веб-интерфейса Dr.Web HTTPD, а *<nopm>* — порт на этом узле, прослушиваемый Dr.Web HTTPD. Для доступа к компонентам Dr.Web Server Security Suite, работающего на локальном узле, достаточно использовать IP-адрес `127.0.0.1` или имя `localhost`. При настройках по умолчанию используется порт `4443`.

Таким образом, для доступа к веб-интерфейсу на локальном компьютере при настройках по умолчанию необходимо ввести адрес:

```
https://127.0.0.1:4443/
```

В случае успешного подключения к серверу управления на экране появится стартовая страница, содержащая форму аутентификации. Для доступа к управлению необходимо пройти аутентификацию, введя в соответствующие поля формы логин и пароль пользователя, обладающего административными полномочиями на узле, на котором функционирует Dr.Web Server Security Suite.

При необходимости вы можете обеспечить авторизацию на веб-интерфейсе по личному сертификату пользователя. Для этого:

1. Создайте личный сертификат, подписанный сертификатом удостоверяющего центра.
2. Импортируйте подписанный сертификат в качестве удостоверяющего сертификата пользователя в браузер, через который осуществляется подключение к веб-интерфейсу управления.
3. В настройках компонента Dr.Web HTTPD (параметр `AdminSslCA`) укажите путь к файлу сертификата удостоверяющего центра, которым подписан ваш личный сертификат.

При авторизации на веб-интерфейсе по личному сертификату пользователя форма авторизации не показывается при начале работы с веб-интерфейсом, а пользователь авторизуется как пользователь *root*.

При необходимости обратитесь к информации в разделе Приложение Д. Генерация сертификатов SSL.

Главное меню

В левой части страниц веб-интерфейса управления, открывающихся после успешного прохождения аутентификации, расположено главное меню, состоящее из следующих пунктов:

- **Главная** — открывает главную страницу, на которой отображается перечень установленных компонентов Dr.Web Server Security Suite и их состояние.
- **Угрозы** — открывает страницу, отображающую все угрозы, обнаруженные на сервере. В этом разделе вы можете осуществлять управление обнаруженными угрозами, в том

числе, перемещать инфицированные объекты в карантин, осуществлять повторную проверку, лечение или удаление вредоносных объектов.

- **Настройки** — открывает страницу управления настройками компонентов Dr.Web Server Security Suite, установленных на сервере.
- **Информация** — открывает страницу просмотра краткой информации о версии веб-интерфейса и состоянии вирусных баз.
- **Справка** — открывает в новой вкладке браузера справку по продуктам Dr.Web для Unix.
- **Проверить файл** — показывает панель оперативной проверки файлов, которая будет доступна поверх любой страницы веб-интерфейса до момента закрытия панели.
- **Выйти** — завершает сеанс работы текущего пользователя с веб-интерфейсом управления (недоступно, если используется авторизация по личному сертификату пользователя).

9.3.1. Управление компонентами

Просмотр перечня компонентов, входящих в состав Dr.Web Server Security Suite, и управление их работой осуществляются на странице **Главная**.

Отображаемые компоненты Dr.Web Server Security Suite разделены на две части: основные, выполняющие обнаружение угроз, и сервисные, обеспечивающие корректную работу Dr.Web Server Security Suite в целом. Перечень основных компонентов (зависит от поставки) отображается в виде таблицы, расположенной в верхней части страницы. Для каждого компонента указывается:

1. **Название**. Нажмите название, чтобы перейти к странице настроек компонента.
2. **Состояние**. Состояние, в котором находится компонент, иллюстрируется переключателем и текстовой подписью, отображающей текущее состояние, в котором он находится. Чтобы запустить компонент или приостановить его работу, нажмите переключатель. Возможные состояния переключателя:

	Компонент отключен и не используется.
	Компонент включен и корректно функционирует.
	Компонент включен, но не функционирует вследствие произошедшей ошибки.

   Если в работе компонента произошла ошибка, вместо состояния выводится сообщение об ошибке. Нажмите , чтобы открыть всплывающее окно с подробной информацией о произошедшей ошибке и рекомендациями по ее устранению.
3. **Нагрузка**. Среднее число файлов, обработанных компонентом за секунду в течение последней минуты, 5 минут, 15 минут (три числа, разделенных косой чертой).
4. **Ошибки**. Среднее число ошибок за секунду, произошедших в работе компонента в течение последней минуты, 5 минут, 15 минут (три числа, разделенных косой чертой).

Наведите указатель на ?, чтобы получить всплывающую подсказку.

Под таблицей основных компонентов в виде набора плиток перечисляются сервисные компоненты Dr.Web Server Security Suite (такие как Dr.Web Scanning Engine, Dr.Web File Checker и др.). Для них также указываются состояние и статистика их работы. Нажмите название компонента, чтобы открыть страницу его настроек. Как правило, эти компоненты запускаются и завершаются автоматически, по мере необходимости. Если какой-либо из них может быть запущен или остановлен пользователем вручную, то, кроме названия и статистики работы, в плитке сервисного компонента доступен выключатель для управления его запуском.

В нижней части страницы указывается информация о вирусных базах и лицензии. Кнопка **Обновить** позволяет начать принудительное обновление вирусных баз, а кнопка **Продлить** (или **Активировать лицензию**, в зависимости от текущего состояния лицензии) — продлить или активировать лицензию путем загрузки на сервер действующего ключевого файла, подходящего для Dr.Web Server Security Suite.

9.3.2. Управление угрозами

Обзор перечня обнаруженных угроз и управление ими осуществляются на странице **Угрозы**.

На этой странице приводится полный перечень угроз, обнаруженных компонентами Dr.Web Server Security Suite, выполняющими мониторинг и проверку файловой системы. В верхней части страницы располагается меню, позволяющее отфильтровать угрозы по категориям:

- **Все** — отобразить в списке все обнаруженные угрозы (в том числе активные и те, которые были помещены в карантин);
- **Активные** — отобразить в списке только активные угрозы, т. е. такие, которые были обнаружены, но все еще не нейтрализованы;
- **Заблокированные** — отобразить в списке угрозы, которые не нейтрализованы, но файлы, содержащие их, были заблокированы для доступа пользователей (актуально только для файловых хранилищ, контролируемых SpIDer Guard для SMB);
- **В карантине** — отобразить в списке угрозы, перемещенные в карантин;
- **Ошибки** — отобразить в списке угрозы, при попытке обработки которых произошла ошибка.

Справа от названия каждой категории в меню отображается число, показывающее количество обнаруженных угроз, соответствующих данной категории. Для отображения в списке угроз требуемой категории нажмите ее название в меню.

В списке угроз для каждой угрозы выводится следующая информация:

- **Файл** — имя файла, содержащего вредоносный объект (путь к файлу не указывается);
- **Владелец** — имя пользователя, являющегося владельцем файла, содержащего угрозу;

- **Компонент** — имя компонента, обнаружившего угрозу;
- **Угроза** — имя вредоносного объекта, обнаруженного в файле, по классификации компании «Доктор Веб».

Для объекта, выделенного в списке, справа от списка выводится подробная информация:

- имя угрозы (выводится в виде ссылки, при нажатии которой в новой вкладке браузера открывается страница Вирусной библиотеки Dr.Web с описанием угрозы);
- размер файла в байтах;
- имя компонента, обнаружившего угрозу;
- дата и время обнаружения угрозы;
- дата и время последнего изменения файла;
- имя пользователя-владельца файла с угрозой;
- имя группы, которой принадлежит пользователь-владелец;
- имя удаленного пользователя, поместившего файл в хранилище (актуально только для файловых хранилищ, контролируемых SpIDer Guard для SMB);
- идентификатор файла с угрозой в карантине, если файл уже был помещен в карантин;
- полный путь к файлу в исходном месте (там, где в нем была обнаружена угроза).

Чтобы выделить объект в списке, нажмите соответствующую строку списка. Чтобы выделить более одного объекта, установите флажки в строках выделяемых объектов. Чтобы за один раз выделить все объекты или снять выделение со всех объектов в списке, установите или снимите флажок, расположенный в поле **Файл** в заголовке списка угроз.

Для применения действий к объектам, выделенным в списке угроз, необходимо нажать соответствующую кнопку на панели инструментов, расположенной непосредственно над списком угроз. В панели инструментов доступны следующие кнопки:

	Удалить отмеченные файлы.
	Восстановить отмеченные файлы из карантина в исходное место.
	Применить дополнительное действие к отмеченным файлам (выбирается из выпадающего списка). Доступны следующие дополнительные действия: • **В карантин** — переместить файлы с угрозами в карантин; • **Лечить** — попытаться вылечить угрозы; • **Игнорировать** — игнорировать угрозы, обнаруженные в отмеченных файлах, и удалить их из списка обнаруженных угроз.



Некоторые из кнопок могут быть недоступны в зависимости от типа выделенных угроз.

Для работами с угрозами, обнаруженными на томах NSS, требуется, чтобы был установлен и запущен SpIDer Guard для NSS.

Если в настройках монитора SpIDer Guard для NSS для некоторого типа угроз указано действие **В карантин**, то при восстановлении файла с угрозой этого типа из карантина на том NSS он будет снова незамедлительно перемещен в карантин. Например, настройки монитора по умолчанию помещают все неизлечимые объекты в карантин, поэтому при восстановлении неизлечимого объекта из карантина на том NSS этот объект будет снова незамедлительно перемещен в карантин.

На странице **Угрозы** также доступна панель фильтрации списка угроз на основании поискового запроса. Чтобы отфильтровать список угроз, оставив в нем только те объекты, в описании которых присутствует заданная строка, воспользуйтесь строкой поиска. Она расположена в правой части панели инструментов и отмечена значком . Для фильтрации списка следует ввести произвольное слово в строку поиска, при этом из списка угроз будут скрыты все объекты, не содержащие в своем названии или описании указанного слова (поиск выполняется без учета регистра букв). Чтобы очистить результаты поиска и вернуться к исходному списку, нажмите в строке поиска или удалите поисковое слово.

9.3.3. Управление настройками

В этом разделе

- Просмотр и изменение настроек компонента в табличной форме
- Просмотр и изменение настроек компонента в редакторе ini
- Дополнительно

Просмотр и изменение текущих параметров конфигурации компонентов, входящих в состав Dr.Web Server Security Suite и перечисленных на главной странице, производятся на странице **Настройки**. Кроме того, на этой странице вы можете переключить Dr.Web Server Security Suite в режим *централизованной защиты* или в *автономный* режим работы (подробнее о режимах работы см. раздел Режимы работы).

В левой части страницы располагается меню, в котором перечисляются все компоненты Dr.Web Server Security Suite, настройки которых доступны для просмотра и редактирования. Чтобы просмотреть и изменить настройки компонента, выберите его в меню, нажав его имя. Имя компонента, настройки которого в данный момент просматриваются в редакторе, выделяется в меню слева.

- Пункт меню **Централизованная защита** позволяет перейти на страницу управления работой в режиме централизованной защиты.
- Пункт меню **Общие настройки** соответствует настройкам Dr.Web ConfigD, обеспечивающего общую работу Dr.Web Server Security Suite.

Если компонент имеет кроме основной секции настроек также и дополнительные, специфичные секции настроек (например, такие секции имеются у компонента эмуляции интерфейса ClamAV® Dr.Web ClamD — в каждой из них задаются индивидуальные параметры проверки для клиентов, использующих определенный адрес подключения), то слева от имени компонента в меню выводится значок сворачивания/разворачивания дополнительных (подчиненных) секций настроек этого компонента. Если этот значок имеет вид ▸, то дополнительные секции скрыты. Если же этот значок имеет вид ▾, то дополнительные секции также отображаются в меню по одной строке на дополнительную секцию. Чтобы свернуть или развернуть список подчиненных секций компонента, нажмите значок сворачивания/разворачивания сбоку от имени нужного компонента в меню.

- Дополнительные секции настроек компонента отображаются с отступом вправо. Чтобы просмотреть или отредактировать параметры дополнительной секции, нажмите ее название.
- Чтобы добавить для компонента новую подчиненную секцию параметров, если он допускает такую возможность, нажмите +. Этот значок расположен справа от имени компонента и появляется при наведении указателя мыши на имя компонента. Далее укажите уникальное имя (тег) дополнительной секции параметров и нажмите **ОК**. Чтобы отказаться от добавления новой секции, нажмите **Отменить**.
- Чтобы удалить подчиненную секцию параметров, нажмите ×. Этот значок расположен справа от имени (тега) секции и появляется при наведении указателя мыши на имя компонента. Далее подтвердите удаление выбранной секции, нажав **Да**, или откажитесь от удаления, нажав **Нет**.

В верхней части страницы просмотра настроек располагается меню, управляющее режимом просмотра настроек. Доступны следующие режимы:

- **Все** — отобразить в табличном редакторе все параметры конфигурации компонента, доступные для просмотра и изменения;
- **Измененные** — отобразить в табличном редакторе для просмотра и изменения только те параметры конфигурации компонента, которые имеют значения, отличные от значений по умолчанию;
- **Редактор ini** — отобразить параметры конфигурации компонента, которые имеют значения, отличные от значений по умолчанию, в редакторе параметров файла конфигурации (в виде пар `параметр = значение`).

На странице управления настройками доступна также панель фильтрации списка отображаемых параметров на основании поискового запроса. Чтобы отфильтровать список параметров, оставив в нем только те параметры, в описании которых присутствует заданная строка, необходимо воспользоваться строкой поиска. Она расположена в правой части меню, управляющего режимом просмотра, и отмечена значком 🔍. Чтобы отфильтровать список параметров, введите произвольное слово в строку поиска, при этом из списка параметров будут скрыты все параметры, не содержащие в своем описании указанного слова (поиск выполняется без учета регистра

букв). Чтобы очистить результаты поиска и вернуться к исходному списку параметров, нажмите в строке поиска или удалите поисковое слово.

Фильтрация списка параметров работает только при просмотре списка параметров в табличной форме (режим **Все** или **Измененные**).

Просмотр и изменение настроек компонента в табличной форме

При просмотре списка параметров в табличной форме (режим **Все** или **Измененные**) каждая строка таблицы содержит имя и описание параметра (слева) и его текущее значение (справа). Для параметров логического типа (имеющих только два допустимых значения — «Да» и «Нет») вместо значения параметра отображается флажок (включенное состояние соответствует заданному значению «Да», а выключенное — значению «Нет»).

> В режиме просмотра всех параметров, а не только измененных, значения, отличные от значений, определенных для этих параметров по умолчанию, выделены в списке жирным шрифтом.

Общий список параметров разбит на разделы, такие как **Основные**, **Дополнительные** и т. д. Чтобы свернуть или развернуть раздел таблицы, нажмите заголовок раздела. Если раздел свернут, а параметры, входящие в него, не указаны в таблице, то слева от имени раздела отображается . Если раздел развернут и входящие в него параметры указаны в таблице, слева от имени раздела отображается .

Чтобы изменить параметр, нажмите его текущее значение в таблице (для параметра логического типа — установите или снимите соответствующий флажок). Если параметр имеет строго ограниченный набор значений, то при нажатии значения откроется выпадающий список, в котором необходимо выбрать требуемое значение. Если значение параметра — число, то при нажатии оно будет доступно в поле редактирования прямо в таблице. В этом случае следует указать новое требуемое значение и нажать ENTER. Во всех этих случаях измененное значение параметра сразу же фиксируется в настройках компонента.

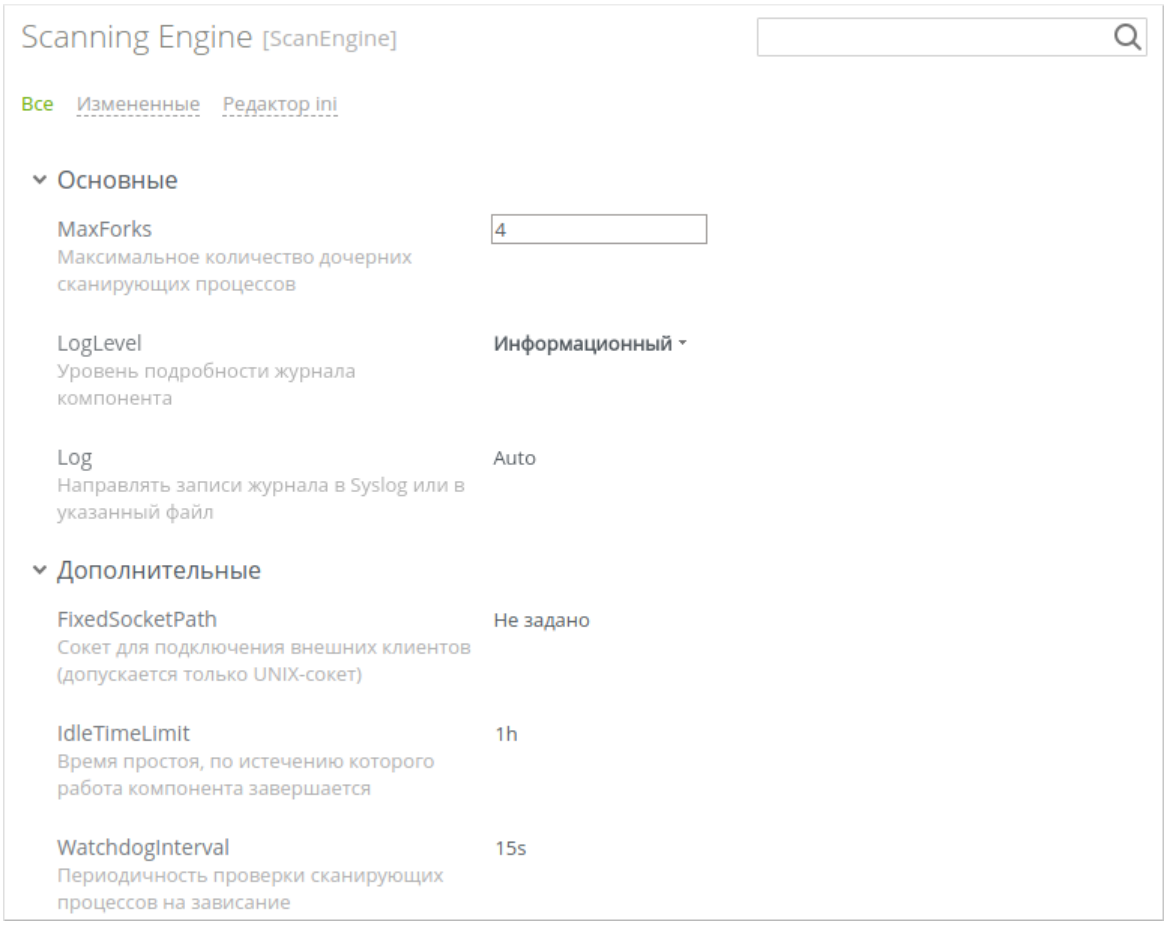


Рисунок 3. Представление настроек компонента в табличной форме

Если параметр принимает строковое значение или список произвольных значений, то при нажатии текущего значения параметра на экране появляется всплывающее окно, в котором можно отредактировать текущее значение параметра. Если параметр принимает список значений, то элементы списка выводятся в многострочном поле редактирования по одному в строке, как показано на рисунке ниже. Чтобы отредактировать элементы списка, измените, удалите или добавьте требуемые строки в поле редактирования.

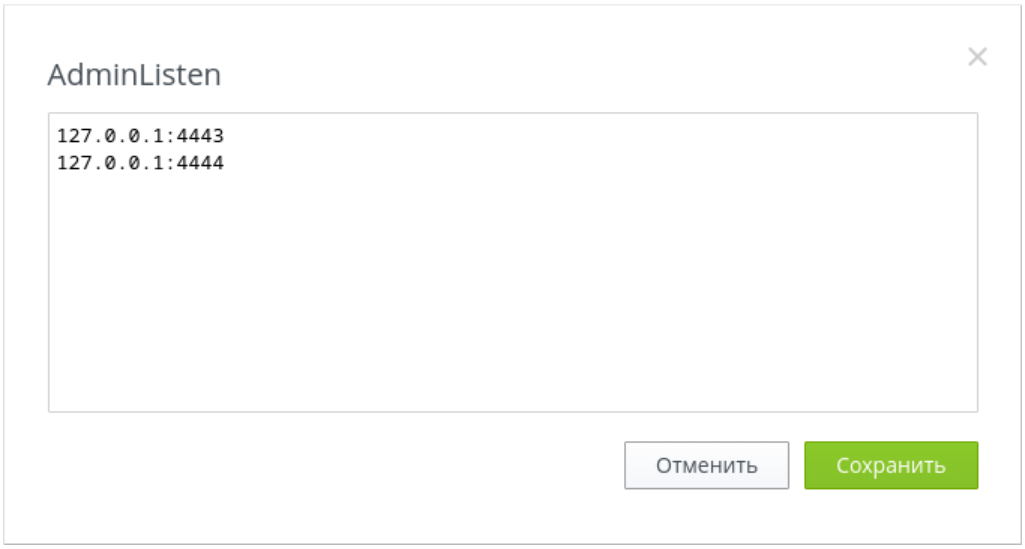


Рисунок 4. Редактирование списка значений

Чтобы сохранить внесенные изменения и закрыть окно, после редактирования значения параметра нажмите **Сохранить**. Чтобы закрыть окно без сохранения внесенных изменений, нажмите **Отменить** или ✕ в верхнем правом углу всплывающего окна.

Просмотр и изменение настроек компонента в редакторе ini

При просмотре параметров в режиме **Редактор ini** они отображаются в редакторе параметров файла конфигурации (в виде пар `параметр = значение`), где `параметр` — имя параметра, задаваемое непосредственно в секции настроек компонента в конфигурационном файле. В этом режиме отображаются только те параметры конфигурации, значения которых отличаются от значений, определенных по умолчанию (т. е. те параметры, значения которых в таблице **Все** выводятся жирным шрифтом). Пример отображения параметров в виде пар показан на рисунке ниже.

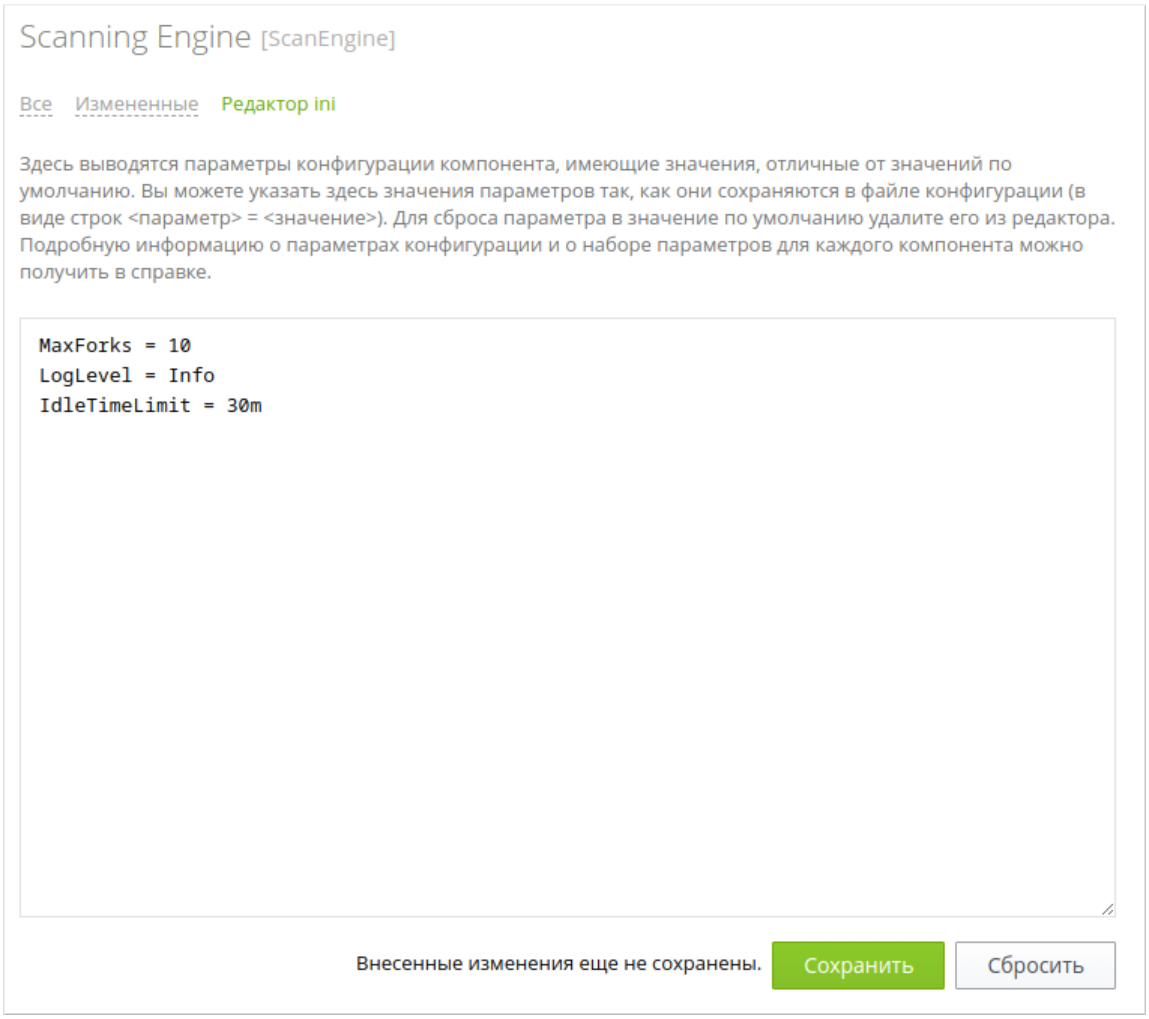


Рисунок 5. Редактирование настроек в формате файла конфигурации

Для внесения изменений необходимо отредактировать текст, учитывая правила формирования файла конфигурации (всегда редактируется только секция файла конфигурации, относящаяся к компоненту, выделенному в меню слева). При необходимости вы можете указать в редакторе любой из параметров, доступных для компонента. В этом случае его значение, установленное по умолчанию, будет заменено на значение, указанное вами в редакторе. Если требуется сбросить параметр в значение по умолчанию, достаточно удалить его строчку из редактора. В этом случае после сохранения изменений параметру будет присвоено значение по умолчанию.

Чтобы сохранить внесенные изменения после редактирования, нажмите **Сохранить**. Чтобы отменить внесенные изменения, нажмите **Отменить**.

При нажатии **Сохранить** выполняется проверка корректности текста, введенного в редакторе: проверяется, что не указаны несуществующие параметры, а также, что все указанные значения параметров допустимы. В случае обнаружения ошибок на экран выдается соответствующее сообщение.

Подробно ознакомиться с общим описанием файла конфигурации, его структурой и особенностями задания значений параметров можно в разделе Приложение Г. Конфигурационный файл Dr.Web Server Security Suite.

Дополнительно

- Параметры конфигурации компонента Dr.Web ConfigD (общие настройки).
- Параметры конфигурации компонента SpIDer Guard.
- Параметры конфигурации компонента SpIDer Guard для NSS.
- Параметры конфигурации компонента SpIDer Guard для SMB.
- Параметры конфигурации компонента Dr.Web ES Agent.
- Параметры конфигурации компонента Dr.Web Updater.
- Параметры конфигурации компонента Dr.Web ClamD.
- Параметры конфигурации компонента Dr.Web File Checker.
- Параметры конфигурации компонента Dr.Web Scanning Engine.
- Параметры конфигурации компонента Dr.Web Network Checker.
- Параметры конфигурации компонента Dr.Web SNMPD.
- Параметры конфигурации компонента Dr.Web CloudD.
- Параметры конфигурации компонента Dr.Web StatD.
- Управление централизованной защитой.

9.3.3.1. Управление централизованной защитой

Вы можете подключить Dr.Web Server Security Suite к серверу централизованной защиты или отключиться от него, переведя продукт в автономный режим работы. Для перехода на страницу управления централизованной защитой выберите пункт **Централизованная защита** в меню настроек на странице **Настройки**.

Чтобы подключить Dr.Web Server Security Suite к серверу централизованной защиты или отключиться от него, используйте соответствующий флажок на этой странице.

Подключение к серверу централизованной защиты

При попытке подключения к серверу централизованной защиты на экране появится всплывающее окно, в котором требуется указать параметры подключения к серверу.

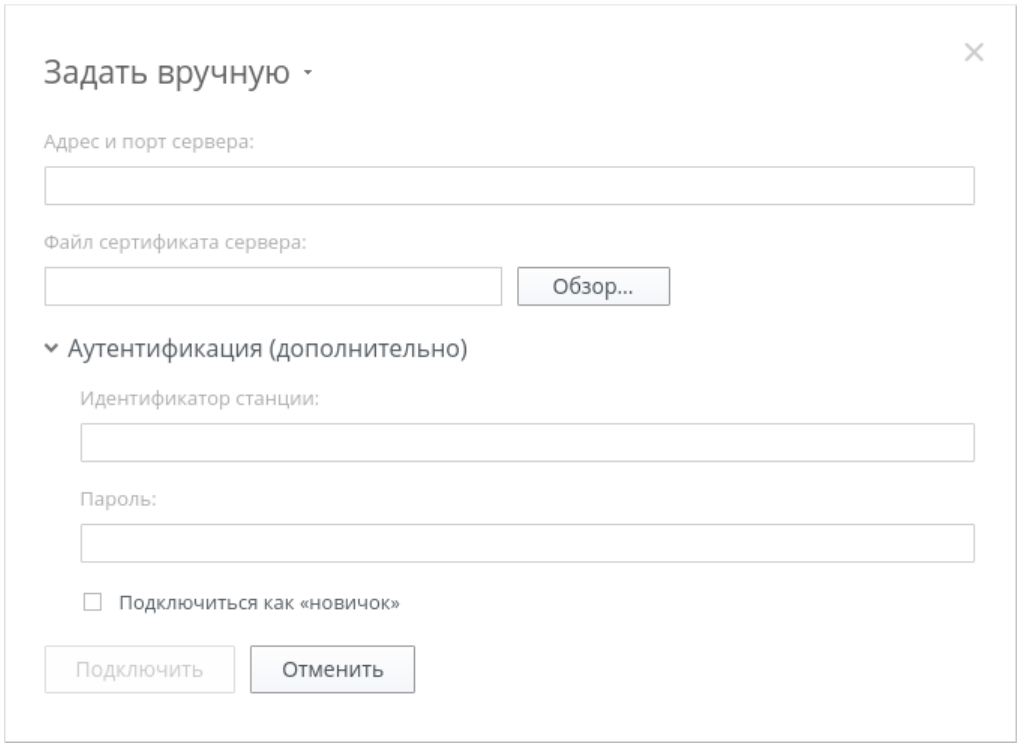


Рисунок 6. Подключение к серверу централизованной защиты

В выпадающем списке, расположенном в верхней части окна, выберите способ подключения к серверу. Доступно три способа:

- *Загрузить из файла*,
- *Задать вручную*,
- *Определить автоматически*.

Если вы выбрали вариант *Загрузить из файла*, укажите в соответствующем поле окна путь к файлу настроек подключения к серверу, предоставленному вам администратором антивирусной сети. При выборе варианта *Задать вручную* следует указать адрес и порт для подключения к серверу централизованной защиты. Кроме того, для способов подключения *Задать вручную* и *Определить автоматически* вы можете также указать путь к файлу публичного ключа сервера, если он у вас имеется (обычно этот файл предоставляется администратором антивирусной сети или провайдером).

Дополнительно, в разделе **Аутентификация (дополнительно)**, вы можете указать идентификатор рабочей станции и пароль для аутентификации на сервере, если они вам известны. Если эти поля заполнены, то подключение к серверу будет успешным только при указании правильной пары идентификатор/пароль. Если эти поля оставить пустыми, то подключение к серверу будет успешным только в случае его одобрения на сервере (автоматически или администратором антивирусной сети, в зависимости от настроек сервера).

Кроме того, вы можете установить флажок **Подключиться как «новичок»**. Если режим «новичок» для подключения станций разрешен на сервере, то после одобрения подключения он автоматически сгенерирует уникальную пару идентификатор/пароль,

которая в дальнейшем будет использоваться для подключения вашего компьютера к этому серверу.

При подключении как «новичок» новая учетная запись для вашего компьютера будет сгенерирована сервером централизованной защиты даже в том случае, если ранее он уже имел учетную запись на этом сервере.

Параметры подключения следует задавать в строгом соответствии с инструкциями, предоставленными администратором антивирусной сети или провайдером.

Для подключения к серверу после указания всех параметров нажмите **Подключить** и дождитесь окончания процесса подключения. Чтобы закрыть окно без подключения к серверу, нажмите **Отменить**.

После того, как вы подключили Dr.Web Server Security Suite к серверу централизованной защиты, он будет работать под управлением сервера до тех пор, пока вы его не переведете в автономный режим. Подключение к серверу будет происходить автоматически каждый раз при запуске Dr.Web Server Security Suite.

9.3.4. Проверка локальных файлов

В этом разделе

- Открытие панели проверки локальных файлов и настройка параметров проверки
- Запуск проверки локальных файлов

Веб-интерфейс предоставляет возможность оперативной проверки на наличие угроз файлов, находящихся на локальном компьютере, с которого осуществляется доступ к веб-интерфейсу управления. При проверке используется сканирующее ядро, входящее в состав Dr.Web Server Security Suite. Проверяемые файлы загружаются на сервер по протоколу HTTP, но после проверки, даже в случае обнаружения угроз, они не сохраняются на сервере и не перемещаются в карантин. Пользователь, отправивший файлы на проверку, будет только проинформирован о ее результате.

Открытие панели проверки локальных файлов и настройка параметров проверки

Выбор и загрузка файлов для проверки осуществляются на панели проверки локальных файлов, которая отображается при выборе пункта **Проверить файл** в главном меню веб-интерфейса. Активированная панель отображается в нижнем правом углу страницы веб-интерфейса. Внешний вид панели проверки локальных файлов показан на рисунке ниже.

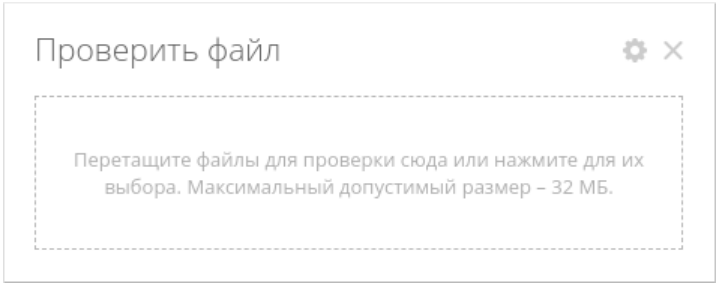


Рисунок 7. Панель проверки локальных файлов

Для закрытия панели нажмите ✕ в верхнем правом углу панели. Нажмите ⚙, чтобы перейти к настройкам проверки локальных файлов, где вы можете указать максимальное время, отведенное на проверку файла (не считая времени его загрузки на север с локального компьютера), разрешить или запретить эвристический анализ, а также указать максимальную степень сжатия для сжатых объектов и глубину вложенности для объектов, упакованных в контейнеры (такие как архивы).

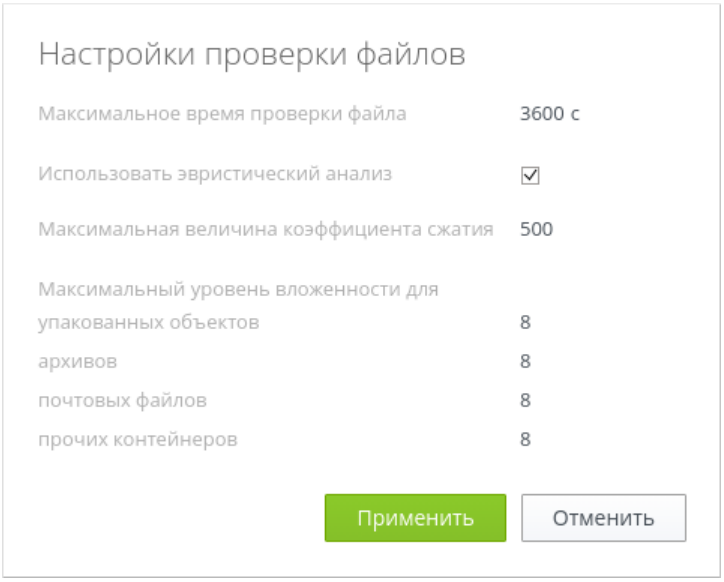


Рисунок 8. Настройка параметров проверки локальных файлов

Для применения измененных настроек и возврата к режиму выбора файлов для проверки нажмите **Применить**. Для возврата к выбору файлов без изменения настроек нажмите **Отменить**.

Запуск проверки локальных файлов

Для начала проверки файлов нажмите надпись-мишень **Перетащите файлы для проверки сюда или нажмите для их выбора**, при этом откроется стандартное окно выбора файлов файлового менеджера. Вы можете выбрать одновременно несколько файлов для проверки.

Выбор каталогов для проверки не допускается.

Вы также можете перетащить выбранные для проверки файлы мышью непосредственно на мишень из окна файлового менеджера. После указания проверяемых файлов начнется их загрузка на сервер с Dr.Web Server Security Suite и проверка по мере загрузки. В процессе загрузки и проверки файлов панель проверки отображает общий прогресс процесса проверки.

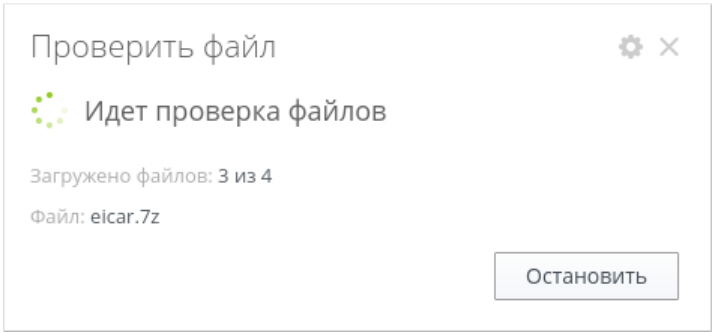


Рисунок 9. Проверка локальных файлов

В случае необходимости вы можете прервать процесс загрузки и проверки файлов, нажав **Остановить**. По окончании проверки на панели отображается отчет о проверке загруженных файлов.

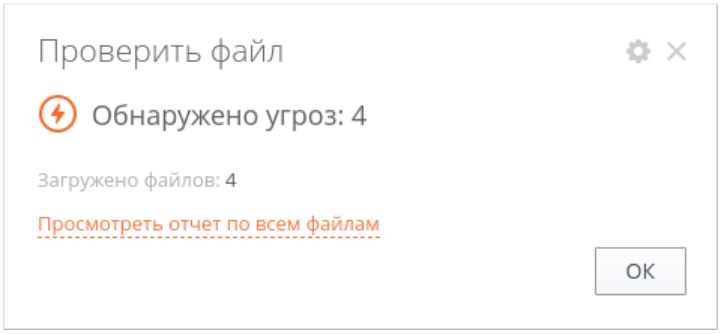


Рисунок 10. Результат проверки локальных файлов

Если вами было загружено более одного файла, будет доступен расширенный отчет о проверке файлов. Чтобы просмотреть расширенный отчет, нажмите **Просмотреть отчет по всем файлам**.

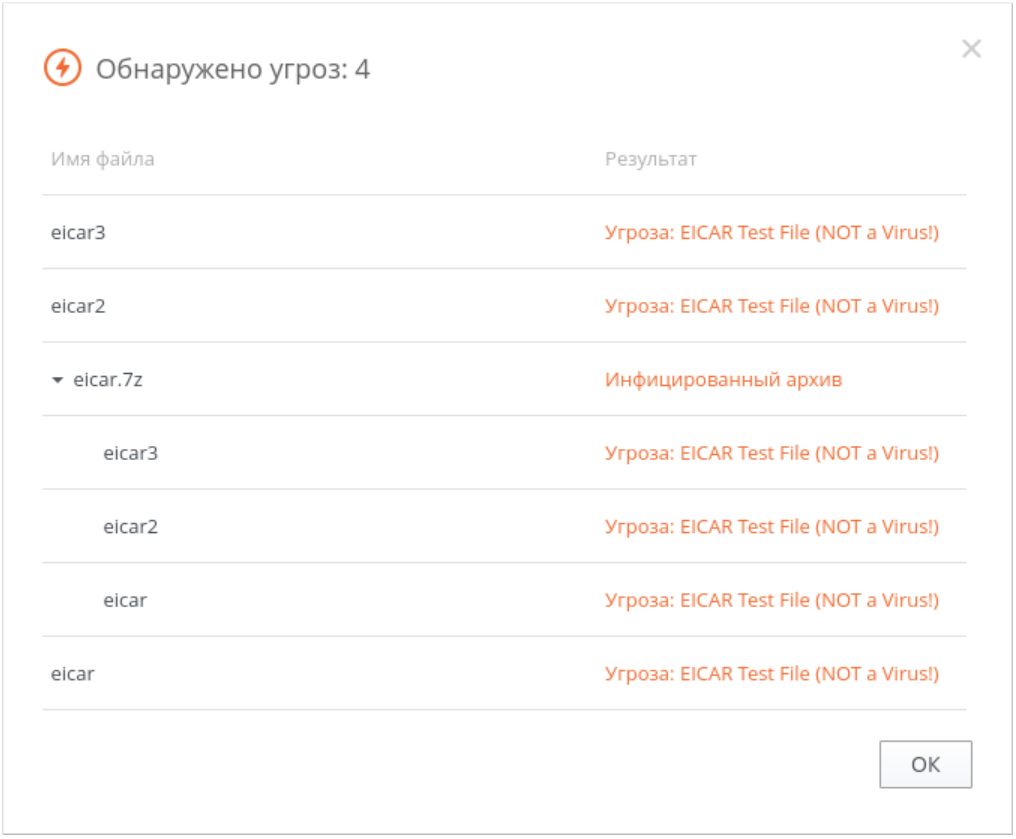


Рисунок 11. Расширенный отчет о проверке локальных файлов

Чтобы закрыть отчет и перевести панель в состояние готовности к выбору новых файлов для проверки, нажмите **OK**.

Запуск проверки локальных файлов с текущими настройками возможен даже тогда, когда панель проверки файлов закрыта. Для начала загрузки и проверки локальных файлов просто перетащите их мышью из окна файлового менеджера на открытую в браузере страницу веб-интерфейса управления.

9.4. SpIDer Guard



Компонент поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Монитор файловой системы SpIDer Guard предназначен для мониторинга файловой активности на томах файловой системы операционных систем GNU/Linux. Компонент работает в режиме резидентного монитора и отслеживает основные события файловой системы, связанные с изменением файлов (их создание, открытие, закрытие). При перехвате этих событий монитор проверяет, был ли изменен файл, и в этом случае формирует для компонента проверки файлов Dr.Web File Checker задание на проверку содержимого измененного файла сканирующим ядром Dr.Web Scanning Engine.

Кроме того, монитор файловой системы SpIDer Guard отслеживает попытки запуска исполняемых файлов. Если программа, содержащаяся в исполняемом файле, по результатам проверки будет признана вредоносной, все процессы, запущенные из этого файла, будут принудительно завершены.

9.4.1. Принципы работы

В этом разделе

- Общие сведения
- Определение областей файловой системы, подлежащих наблюдению
- Режим усиленного мониторинга файлов

Общие сведения

Монитор файловой системы SpIDer Guard работает в пользовательском пространстве (*user mode*), используя для контроля событий файловой системы системный механизм fanotify или специальный *загружаемый модуль ядра* Linux (*LKM — Loadable Kernel Module*), разработанный компанией «Доктор Веб». В настройках рекомендуется использовать *автоматический режим* (`Auto`), который позволит компоненту при старте определить и использовать наилучший режим работы, поскольку не все версии ядра Linux поддерживают механизм fanotify, использующийся монитором. Если компонент не может использовать указанный в настройках режим интеграции, он завершается сразу после старта. Если указан автоматический режим, то компонент попытается использовать сначала fanotify, а затем модуль ядра LKM. Если не получится использовать ни один из этих режимов, компонент завершит работу.

Для ряда ОС модуль ядра поставляется совместно с SpIDer Guard уже в скомпилированном виде. Если для ОС, в которой используется SpIDer Guard, модуль ядра не поставляется в скомпилированном виде, используйте исходный код модуля, предоставляемый компанией «Доктор Веб» для сборки и установки модуля ядра вручную (инструкция по сборке приведена в разделе Использование модуля ядра для SpIDer Guard).

При обнаружении новых или измененных файлов монитор отправляет задание на их проверку компоненту проверки файлов Dr.Web File Checker, который, в свою очередь, инициирует их проверку сканирующим ядром Dr.Web Scanning Engine. При работе через системный механизм fanotify монитор может блокировать доступ к файлам (всех типов или только к исполняемым файлам — PE, ELF, скриптам с преамбулой `#!`), которые еще не проверены, до момента окончания их проверки (см. ниже).

SpIDer Guard автоматически распознает моменты монтирования и отмонтирования новых томов файловой системы (например, на накопителях USB-flash и CD/DVD, массивы RAID и т. п.) и корректирует список наблюдаемых областей по мере необходимости.

Определение областей файловой системы, подлежащих наблюдению

Для оптимизации проверки файловой системы, монитор файловой системы SpIDer Guard контролирует обращение только к тем файлам, которые находятся в областях файловой системы, указанных в конфигурации. Каждая такая область определяется как путь к некоторому каталогу дерева файловой системы и называется *защищаемым пространством (protected space)*. Совокупность всех защищаемых пространств образует в файловой системе единую *область наблюдения*, контролируемую монитором. Помимо области наблюдения, в настройках компонента можно задать также совокупность каталогов файловой системы, которые требуется исключить из мониторинга (*область исключения*). Если в настройках компонента не указано ни одного защищаемого пространства, область наблюдения охватывает собой все дерево каталогов файловой системы. Таким образом, наблюдению подвергаются только те файлы, пути к которым принадлежат области наблюдения, но не принадлежат области исключения.

Использование исключений бывает необходимо, например, если некоторые файлы часто изменяются, что порождает их постоянную перепроверку и тем самым нагружает систему. Если точно известно, что частое изменение файлов в некотором каталоге не является следствием вредоносной активности, а следствием работы некоторой доверенной программы, то можно добавить путь к этому каталогу, или изменяемым файлам в нем, в список исключений. В этом случае монитор файловой системы SpIDer Guard не будет реагировать на изменения этих файлов, даже если они принадлежат области наблюдения. Кроме того, имеется возможность указать и саму программу,

работающую с файлами, в списке доверенных программ (параметр конфигурации `ExcludedProc`), тогда файловые операции, производимые этой программой, также не будут приводить к проверкам файлов, даже если эти файлы находятся в области наблюдения. Аналогично, при необходимости, можно запретить мониторинг и проверку файлов, находящихся в других файловых системах, примонтированных к локальной файловой системе (например, примонтированные через CIFS каталоги с внешних файловых серверов). Для указания файловых систем, файлы на которых не должны проверяться, используется параметр `ExcludedFilesystem`.

Защищаемые пространства, как части области наблюдения с указанными для них параметрами проверки, задаются в настройках компонента как именованные секции, содержащие в своем имени произвольный уникальный идентификатор, присвоенный защищаемому пространству. Каждая секция, описывающая пространство, содержит параметр `Path`, определяющий путь в файловой системе, хранящий каталоги этого защищаемого пространства (т. е. фрагмент дерева файловой системы, находящийся под наблюдением в рамках данного пространства), а также параметр `ExcludedPath`, определяющий локальную (т. е. относительно `Path`) область исключения внутри защищаемого пространства. Параметр `ExcludedPath` может содержать в себе стандартные файловые маски (т. е. содержать символы `*` и `?`). Кроме локальных областей исключения, в настройках может быть задана и глобальная область исключения, при помощи параметра `ExcludedPath`, указанного вне секций, описывающих защищаемые пространства. Все каталоги, попавшие в эту область, в том числе и каталоги защищаемых пространств, будут исключены из проверки. К каждому защищаемому пространству применяется только глобальная и собственная области исключения: если одно пространство вложено в другое, то к вложенному пространству не применяются настройки исключения, указанные для включающего его защищаемого пространства. Кроме того, в настройках каждого защищаемого пространства имеется логический параметр `Enable`, определяющий, включено или нет наблюдение за файлами, находящимися в области наблюдения данного пространства. Если этот параметр установлен в значение `No`, то содержимое данного пространства не контролируется монитором. Кроме того, защищаемое пространство не контролируется монитором, если параметр `Path` имеет пустое значение.



Если у всех защищаемых пространств, указанных в настройках монитора, наблюдение отключено, или их пути не заданы, то SplDer Guard работает вхолостую, поскольку ни один файл дерева файловой системы не будет находиться под наблюдением. Если необходимо контролировать всю файловую систему как единое защищаемое пространство, следует удалить из настроек все именованные секции защищаемых пространств.

Рассмотрим пример настроек областей наблюдения и исключения. Пусть в настройках компонента заданы следующие параметры:

```
[LinuxSpider]
ExcludedPath = /directory1/tmp
...

[LinuxSpider.Space.space1]
```

```
Path = /directory1
ExcludedPath = "*.tmp"
...

[LinuxSpider.Space.space2]
Path = /directory1/directory2
...

[LinuxSpider.Space.space3]
Path = /directory3
Enable = No
...
```

Это означает, что под наблюдением находятся файлы, расположенные в каталоге `/directory1`, и его подкаталогах, за исключением каталога `/directory1/tmp`. Кроме того, исключаются из наблюдения файлы, чье полное имя соответствует маске `/directory1/*.tmp` (это не касается вложенной области `/directory1/directory2`, на которую данная маска не распространяется, не смотря на то, что эта область вложена в защищаемое пространство *space1*). Файлы, находящиеся в каталоге `/directory3`, не контролируются.

Режим усиленного мониторинга файлов

SpIDer Guard может использовать три режима мониторинга:

- *Обычный* (установлен по умолчанию) — отслеживаются операции доступа к файлам (создание, открытие, закрытие и запуск файла). Запрашивается проверка файла, доступ к которому был осуществлен. По результатам проверки к файлу могут быть применены действия по нейтрализации угрозы, если она в нем обнаружена. До окончания проверки доступ к файлу со стороны приложений, запросивших доступ, не ограничивается.
- *Усиленный контроль исполняемых файлов* — для файлов, не считающихся исполняемыми, — так же, как и в обычном режиме. SpIDer Guard блокирует запрошенную операцию доступа к исполняемому файлу до тех пор, пока не станут известны результаты его проверки на наличие угроз.

  Исполняемыми файлами считаются двоичные файлы форматов PE и ELF, а также текстовые файлы скриптов, содержащие преамбулу «`#!`».

- *«Параноидальный» режим* — SpIDer Guard блокирует запрошенную операцию доступа к любому файлу до тех пор, пока не станут известны результаты его проверки на наличие угроз.

Dr.Web File Checker в течение определенного времени сохраняет результаты проверки файлов в специальном кэше, поэтому при повторном доступе к тому же файлу, при наличии информации в кэше, повторное сканирование файла не производится, в качестве результата проверки этого файла используется результат, извлеченный из кэша. Несмотря на это, использование «параноидального» режима мониторинга приводит к существенному замедлению работы при доступе к файлам.

Для настройки режима мониторинга измените значение параметра `BlockBeforeScan` в настройках компонента.



Подробнее о настройке SplDer Guard и режимах мониторинга файлов см. в разделе Настройка мониторинга файловой системы.

9.4.2. Аргументы командной строки

Чтобы запустить компонент SplDer Guard из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-spider [<параметры>]
```

SplDer Guard допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-spider --help
```

Данная команда выведет на экран краткую справку компонента SplDer Guard.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при загрузке операционной системы. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-spider`.

9.4.3. Параметры конфигурации

В этом разделе

- Параметры компонента
- Настройка индивидуальных параметров мониторинга защищаемых пространств

Компонент использует параметры конфигурации, заданные в секции `[LinuxSpider]` объединенного конфигурационного файла Dr.Web Server Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-spider`
`Start` *{логический}*	Компонент запускается демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: Зависит от того, в составе какого продукта Dr.Web работает компонент.
`[*] ExcludedPath` *{путь к файлу или каталогу}*	Путь к объекту, который должен быть пропущен при мониторинге файловых операций. Допускается указание пути как к отдельному файлу, так и к каталогу в целом. Если указан каталог, то будут исключены из наблюдения все файлы и подкаталоги (включая вложенные) этого каталога. Допускается использовать файловые маски (содержащие символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`).

<table>
<tr><th>Параметр</th><th>Описание</th></tr>
<tr><td></td><td>
Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).

Пример: Добавить в список файл <code>/etc/file1</code> и каталог <code>/usr/bin</code>.

• Добавление значений с помощью команды <code>drweb-ctl cfset</code>:
<pre># drweb-ctl cfset LinuxSpider.ExcludedPath -a /etc/file1
drweb-ctl cfset LinuxSpider.ExcludedPath -a /usr/bin</pre>
• Добавление значений в файл конфигурации.
○ Два значения в одной строке:
<pre>[LinuxSpider]
ExcludedPath = "/etc/file1", "/usr/bin"</pre>
○ Две строки (по одному значению в строке):
<pre>[LinuxSpider]
ExcludedPath = /etc/file1
ExcludedPath = /usr/bin</pre>
Чтобы изменения вступили в силу, перезагрузите конфигурацию Dr.Web Server Security Suite с помощью команды:
<pre># drweb-ctl reload</pre>
Нет смысла указывать здесь пути к символическим ссылкам, поскольку при проверке файла всегда анализируется прямой путь к нему.

Значение по умолчанию: <code>/proc, /sys</code>
</td></tr>
<tr><td><code>Mode</code>

{LKM | FANOTIFY | AUTO}</td><td>
Режим работы SplDer Guard.

Возможные значения:
• <code>LKM</code> — работа через LKM-модуль Dr.Web, установленный в ядро операционной системы (LKM — Loadable Kernel Module);
• <code>FANOTIFY</code> — работа через системный механизм fanotify;
• <code>AUTO</code> — автоматическое определение оптимального режима работы.
</td></tr>
</table>

Параметр	Описание
	 Изменять значения этого параметра следует производить с крайней осторожностью, поскольку ядра Linux в разной мере поддерживают тот и другой режим работы. Настоятельно рекомендуется оставлять этот параметр в значении `AUTO`, чтобы при запуске был выбран оптимальный режим интеграции с диспетчером файловой системы. При этом компонент сначала пытается использовать режим `FANOTIFY`, потом, в случае неудачи, — `LKM`. Если не удалось использовать ни один из режимов, работа компонента завершается. При необходимости вы можете собрать LKM-модуль Dr.Web из исходного кода и установить его в систему, следуя инструкции в разделе Использование модуля ядра для SplDer Guard. Значение по умолчанию: `AUTO`

`ExcludedProc`
 	
{путь к файлу или список путей}
	Список процессов, файловая активность которых не контролируется. Если файловая операция была совершена любым из процессов, указанных в значении параметра, то измененный или созданный файл не будет проверяться.
	
	Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Допускается использовать файловые маски (содержащие символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`).
	
	Пример: Добавить в список процессы `wget` и `curl`.
	• Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset LinuxSpider.ExcludedProc -a /usr/bin/wget`
	`# drweb-ctl cfset LinuxSpider.ExcludedProc -a /usr/bin/curl`
	• Добавление значений в файл конфигурации.

Параметр	Описание

	○ Два значения в одной строке:
	`[LinuxSpider]`
	`ExcludedProc = "/usr/bin/wget",`
	`"/usr/bin/curl"`
	○ Две строки (по одному значению в строке):
	`[LinuxSpider]`
	`ExcludedProc = /usr/bin/wget`
	`ExcludedProc = /usr/bin/curl`
	Чтобы изменения вступили в силу, перезагрузите конфигурацию Dr.Web Server Security Suite с помощью команды:
	`# drweb-ctl reload`
	Значение по умолчанию: *(не задано)*

`BlockBeforeScan` *{Off | Executables | All}*	Блокировать файлы при обращении к ним до проверки монитором (усиленный или «параноидальный» режим мониторинга). Допустимые значения: • `Off` — не блокировать доступ к файлам, даже если они не проверены. • `Executables` — блокировать доступ к исполняемым файлам (форматов PE и ELF и скриптов, содержащих преамбулу `#!`), не проверенным монитором. • `All` — блокировать доступ ко всем файлам, не проверенным монитором. Файлы блокируются только в режиме `FANOTIFY`. Значение по умолчанию: `Off`
`ExcludedFilesystem` *{имя файловой системы}*	Файловая система, доступ к файлам которой контролироваться не будет. Данная функция доступна только в режиме `FANOTIFY`. Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список файловые системы `cifs` и `nfs`.

Параметр	Описание

	• Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset LinuxSpider.ExcludedFilesystem -a cifs`
	`# drweb-ctl cfset LinuxSpider.ExcludedFilesystem -a nfs`
	• Добавление значений в файл конфигурации.
	○ Два значения в одной строке:
	`[LinuxSpider]`
	`ExcludedFilesystem = "cifs", "nfs"`
	○ Две строки (по одному значению в строке):
	`[LinuxSpider]`
	`ExcludedFilesystem = cifs`
	`ExcludedFilesystem = nfs`
	Чтобы изменения вступили в силу, перезагрузите конфигурацию Dr.Web Server Security Suite с помощью команды:
	`# drweb-ctl reload`
	Значение по умолчанию: `cifs`

`[*] OnKnownVirus` *{действие}*	Действие при обнаружении в проверяемом файле известной угрозы (вируса и т. д.). Допустимые значения: `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `CURE`
`[*] OnIncurable` *{действие}*	Действие в случае невозможности излечения угрозы. Допустимые значения: `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnSuspicious` *{действие}*	Действие при обнаружении в проверяемом с помощью эвристического анализа файле неизвестной угрозы (или подозрения на угрозу). Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnAdware` *{действие}*	Действие при обнаружении в проверяемом файле рекламной программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnDialers` *{действие}*	Действие при обнаружении в проверяемом файле программы автоматического дозвона.

Параметр	Описание
	Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnJokes` *{действие}*	Действие при обнаружении в проверяемом файле программы-шутки. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`[*] OnRiskware` *{действие}*	Действие при обнаружении в проверяемом файле потенциально опасной программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`[*] OnHacktools` *{действие}*	Действие при обнаружении в проверяемом файле в проверяемом файле хакерской программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`[*] ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `30s`
`[*] HeuristicAnalysis` *{On | Off}*	Использовать или не использовать эвристический анализ для поиска возможных неизвестных угроз. Эвристический анализ повышает надежность проверки, но увеличивает ее длительность. Действие на срабатывание эвристического анализатора задается параметром `OnSuspicious`. Допустимые значения: • `On` — использовать эвристический анализ при проверке. • `Off` — не использовать эвристический анализ. Значение по умолчанию: `On`
`[*] PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает

Параметр	Описание
	предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[*] ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `0`
`[*] MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `0`
`[*] ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов с вложениями (например, страницы HTML, файлы `.jar` и т. п.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[*] MaxCompressionRatio` *{целое число}*	Максимально допустимая степень сжатия проверяемых объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`

Параметр	Описание
`DebugAccess` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о доступе к файлам. Значение по умолчанию: `No`

Настройка индивидуальных параметров мониторинга защищаемых пространств

Для каждого защищаемого пространства файловой системы в конфигурационном файле, наряду с секцией `[LinuxSpider]`, хранящей все параметры работы монитора, задается отдельная секция, определяющая путь к наблюдаемой области файловой системы и параметры ее мониторинга. Каждая индивидуальная секция защищаемого пространства должна иметь имя вида `[LinuxSpider.Space.`<*имя пространства*>`]`, где <*имя пространства*> — уникальный идентификатор защищаемого пространства.

Индивидуальная секция пространства должна включать в себя следующие параметры, отсутствующие в общей секции `[LinuxSpider]`:

Параметр	Описание
`Path` *{путь к каталогу}*	Определяет путь к каталогу, хранящему файлы, которые должны находиться под наблюдением (включая вложенные каталоги). По умолчанию данный параметр имеет пустое значение, поэтому при добавлении защищаемого пространства к области наблюдения обязательно следует задать данный параметр. Значение по умолчанию: *(не задано)*
`Enable` *{логический}*	Содержимое защищаемого пространства, расположенное внутри пути `Path`, должно находиться под наблюдением монитора. Установка данного параметра в `No` предписывает монитору исключить содержимое данного защищаемого пространства из объединенной области наблюдения. Значение по умолчанию: `Yes`



Если у всех защищаемых пространств, указанных в настройках монитора, наблюдение отключено, или их пути не заданы, то SplDer Guard работает вхолостую, поскольку ни один файл дерева файловой системы не будет находиться под наблюдением. Если необходимо контролировать всю файловую систему как единое защищаемое пространство, следует удалить из настроек все именованные секции защищаемых пространств.

Кроме указанных выше, индивидуальные секции защищаемых пространств могут включать в себя список параметров из общей секции настроек компонента, отмеченных обозначением `[*]` в таблице выше, и переопределяющих параметр, заданный для защищаемого пространства (например, действие при обнаружении угрозы, максимальную глубину проверки архивов и т. п.). Если для защищаемого пространства не указан какой-либо из параметров, то мониторинг файлов в этом пространстве регулируется значениями соответствующих параметров из секции `[LinuxSpider]`.

Чтобы добавить новую секцию параметров для защищаемого пространства с тегом *<имя пространства>* при помощи утилиты управления Dr.Web Ctl (запускается командой `drweb-ctl`), выполните команду:

```
# drweb-ctl cfset LinuxSpider.Space -a <имя пространства>
```

Пример:

```
# drweb-ctl cfset LinuxSpider.Space -a Space1
# drweb-ctl cfset LinuxSpider.Space.Space1.Path /home/user1
```

Первая команда добавит в файл конфигурации секцию `[LinuxSpider.Space.Space1]`, а вторая задаст для нее значение параметра `Path`, указав путь к наблюдаемой области файловой системы. Все прочие параметры в данной секции будут совпадать со значениями параметров из общей секции `[LinuxSpider]`.

9.4.4. Использование модуля ядра для SplDer Guard

В этом разделе

- Общие сведения
- Инструкция по сборке модуля ядра
- Возможные ошибки сборки

Общие сведения

Если операционная система не предоставляет механизм fanotify, используемый SplDer Guard для мониторинга действий с объектами файловой системы, он может использовать специальный загружаемый LKM-модуль, работающий в пространстве ядра (кроме того, модуль ядра может использоваться в тех случаях, когда механизм fanotify реализован с ограничениями по доступу к файловой системе).

По умолчанию в составе SplDer Guard поставляется скомпилированный модуль ядра для всех ОС, указанных в разделе Системные требования и совместимость. Кроме этого совместно с компонентом SplDer Guard поставляется архив в формате `.tar.bz2`, содержащий исходные файлы загружаемого модуля ядра, чтобы его можно было собрать вручную.

Загружаемый модуль ядра (LKM), используемый SpIDer Guard, предназначен для работы с ядрами Linux версий 2.6.* и более поздней.

Работа с LKM не поддерживается для архитектур ARM64, E2K и IBM POWER (ppc64el).

Архив с исходным кодом загружаемого модуля ядра располагается в каталоге `/opt/drweb.com/share/drweb-spider-kmod/src/` и имеет имя вида `drweb-spider-kmod-<версия>-<дата>.tar.bz2`.

Также в каталоге `drweb-spider-kmod` имеется файл скрипта `check-kmod-install.sh`, исполнив который, вы получите информацию, поддерживает ли используемая вами операционная система предварительно скомпилированные версии ядра, уже включенные в состав Dr.Web Server Security Suite. Если нет, то на экран будет выведена рекомендация выполнить ручную сборку.

В случае отсутствия каталога `drweb-spider-kmod` по указанному пути, выполните установку пакета `drweb-spider-kmod` (из репозитория или выборочной установкой из универсального пакета, в зависимости от способа, которым установлен Dr.Web Server Security Suite).

Для выполнения ручной сборки загружаемого модуля ядра из исходного кода необходимо обладать правами суперпользователя (пользователя *root*). Для получения прав суперпользователя при сборке используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Инструкция по сборке модуля ядра

1. Распакуйте архив с исходным кодом в любой каталог. Например, команда

   ```
   # tar -xf drweb-spider-kmod-<версия>-<дата>.tar.bz2
   ```

   распакует архив непосредственно в каталог, содержащий сам архив, создав в нем подкаталог с именем файла архива.

2. Перейдите в созданный каталог с исходным кодом и выполните команду:

   ```
   # make
   ```

   В случае возникновения ошибок на этапе `make` следует их устранить и выполнить компиляцию повторно.

3. После успешного окончания этапа `make` выполните команды:

   ```
   # make install
   # depmod
   ```

4. После успешной сборки модуля ядра и его регистрации в системе, выполните дополнительно настройку SpIDer Guard, указав ему режим работы с модулем ядра, выполнив команду:

   ```
   # drweb-ctl cfset LinuxSpider.Mode LKM
   ```

Также допускается установка значения `AUTO` вместо значения `LKM`. В этом случае SpIDer Guard будет пробовать использовать не только модуль ядра, но и системный механизм fanotify. Для получения дополнительной информации выполните команду:

```
$ man 1 drweb-spider
```

Возможные ошибки сборки

На этапе выполнения сборки `make` могут возникать ошибки. В случае возникновения ошибок проверьте следующее.

- Для успешной сборки требуется наличие Perl и компилятора GCC. Если они отсутствуют, установите их.
- В некоторых ОС может потребоваться предварительная установка пакета `kernel-devel`.
- В некоторых ОС сборка может завершиться ошибкой из-за неправильно определенного пути к каталогу исходного кода ядра. В этом случае используйте команду `make` с параметром `KDIR=`*<путь к исходным кодам ядра>*. Обычно файлы исходного кода размещаются в каталоге `/usr/src/kernels/`*<версия ядра>*.



Версия ядра, выдаваемая командой `uname -r`, может не совпадать с именем каталога *<версия ядра>*.

9.5. SpIDer Guard для SMB

SpIDer Guard для SMB — это монитор каталогов файловой системы, используемых как разделяемые каталоги файловым SMB-сервером Samba. Этот компонент предназначен для мониторинга действий с файлами в разделяемых каталогах Samba. Он работает в режиме резидентного монитора и контролирует основные действия в файловой системе, относящиеся к файлам и каталогам (создание, открытие, закрытие, а также операции чтения и записи), содержащимся в защищаемых каталогах. Когда компонент перехватывает такое событие, он проверяет, был ли файл изменен, и если да, то он создает задачу на проверку этого файла, которую отправляет компоненту проверки файлов Dr.Web File Checker. Если запрашиваемый файл действительно требует проверки, Dr.Web File Checker, в свою очередь, инициирует проверку содержимого файла сканирующим ядром Dr.Web Scanning Engine. Если в файле обнаружена угроза, файл блокируется для доступа на период, указанный в настройках, до момента применения к нему действия по нейтрализации угрозы. Также в настройках компонента может быть задано предписание блокировать файл в случае ошибки его проверки (в том числе если отсутствует действующая лицензия).



Для предотвращения возможных конфликтов между SpIDer Guard и SpIDer Guard для SMB при проверке файлов в разделяемых каталогах Samba, рекомендуется дополнительно настроить SpIDer Guard, выполнив одно из следующих действий:

- добавить разделяемые каталоги Samba в область исключения (перечислить эти каталоги в параметре `ExcludedPath`);
- добавить процесс Samba (`smbd`) в список игнорируемых процессов (указать значение `smbd` в параметре `ExcludedProc`).



Монитор SpIDer Guard для SMB использует для интеграции с Samba специальный модуль VFS SMB. Совместно с монитором SpIDer Guard для SMB поставляется несколько версий модуля VFS SMB, собранных для различных версий Samba, однако они могут оказаться несовместимы с версией Samba, установленной на вашем файловом сервере, например, если установленный у вас сервер Samba использует опцию `CLUSTER_SUPPORT`.

В случае несовместимости поставляемых модулей VFS SMB с вашим сервером Samba необходимо выполнить сборку модуля VFS SMB для вашего сервера Samba, включая поддержку опции `CLUSTER_SUPPORT`, если это требуется. Процедура сборки модуля VFS SMB из исходного кода описана в разделе Сборка модуля VFS SMB.

9.5.1. Принципы работы

В этом разделе

- Общие сведения
- Задание областей файловой системы, подлежащих наблюдению

Общие сведения

Монитор SpIDer Guard для SMB работает в режиме демона (обычно запускается демоном управления конфигурацией Dr.Web ConfigD при запуске системы). После запуска он работает в качестве сервера, к которому подключаются специальные плагины (модули VFS SMB), работающие на стороне сервера Samba и контролирующие активность пользователей в разделяемых каталогах. При обнаружении новых или измененных файлов монитор запрашивает их проверку компонентом проверки файлов Dr.Web File Checker.

Когда в файле, проверенном по запросу от монитора, обнаруживается неизлечимая угроза, или если для данного типа угрозы в настройках было указано действие «Блокировать» (`BLOCK`), монитор дает команду модулю VFS SMB, контролирующему разделяемый каталог, блокировать этот файл для пользователей (т. е. запретить чтение файла, запись в него и его исполнение). Также, если это не отключено в настройках, рядом с заблокированным файлом создается специальный текстовый файл, содержащий описание причины блокировки файла. Это делается для того, чтобы предотвратить для пользователя эффект «неожиданного исчезновения файла», который мог бы возникать в случае, если к файлу было автоматически применено действие «Удалить» (`DELETE`) или «В карантин» (`QUARANTINE`). Это позволяет предотвратить множественные попытки пользователя (или программы-червя, заразившей компьютер пользователя) заново создать перемещенный или удаленный файл. Кроме того, это действие является способом проинформировать пользователя, что его компьютер, вероятно, инфицирован какой-либо вредоносной программой. Получив такую информацию, пользователь может выполнить антивирусную проверку компьютера, обнаружить и обезвредить локальные угрозы. Дополнительно файл (в зависимости от значения соответствующего параметра конфигурации) может быть заблокирован при ошибке проверки, в том числе, если отсутствует активная лицензия, обеспечивающая работу SpIDer Guard для SMB.

Задание областей файловой системы, подлежащих наблюдению

Вы можете запретить компоненту наблюдать за указанными каталогами и файлами, находящимися внутри контролируемых разделяемых каталогов сервера Samba. Это может понадобиться, если какие-либо файлы изменяются слишком часто, что заставляет монитор столь же часто их проверять и может привести к большой нагрузке на систему. Если при этом точно известно, что для некоторых файлов в хранилище частое изменение — это нормальное поведение, то рекомендуется исключить такие файлы из-под наблюдения монитора. В этом случае он не будет реагировать на их изменение и не будет инициировать их проверку компонентом проверки файлов.

Для определения каталогов, подлежащих и не подлежащих наблюдению, монитор файловых хранилищ Samba SpIDer Guard для SMB использует два параметра конфигурации:

- `IncludedPath` — список путей, подлежащих мониторингу («область наблюдения»);
- `ExcludedPath` — список путей для исключения из мониторинга («область исключения»).

Стандартно в качестве области наблюдения рассматривается весь разделяемый каталог. В случае указания областей наблюдения и исключения, наблюдению подвергаются только те файлы из разделяемого каталога, пути к которым не относятся к исключениям из списка `ExcludedPath` или принадлежат области наблюдения, определяемой списком `IncludedPath`. При этом, если один и тот же путь указан в обоих списках, то параметр `IncludedPath` имеет приоритет — объекты, расположенные по данному пути, будут находиться под контролем монитора SpIDer Guard для SMB. Таким образом, вы можете использовать параметр `IncludedPath` для включения в область наблюдения отдельных каталогов и файлов, находящихся внутри области исключения.

Вы можете задать различные параметры защиты для разных разделяемых каталогов Samba, находящихся под защитой монитора SpIDer Guard для SMB, включая разные области наблюдения и исключения, а также реакции на обнаруженные угрозы. Это достигается заданием в секции конфигурации монитора SpIDer Guard для SMB индивидуальных настроек для модулей VFS SMB, контролирующих эти разделяемые каталоги.



Об интеграции Dr.Web Server Security Suite с файловой службой см. раздел Интеграция с файловым сервером Samba.

9.5.2. Аргументы командной строки

Чтобы запустить компонент SpIDer Guard для SMB из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-smbspider-daemon [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-smbspider-daemon [<параметры>]
```

SpIDer Guard для SMB допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента.

	Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-smbspider-daemon --help
```

Данная команда выведет на экран краткую справку компонента SpIDer Guard для SMB.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при загрузке операционной системы. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-smbspider-daemon`.

9.5.3. Параметры конфигурации

В этом разделе

- Параметры компонента
- Настройка индивидуальных параметров мониторинга

Компонент использует параметры конфигурации, заданные в секции `[SMBSpider]` объединенного конфигурационного файла Dr.Web Server Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента.

Параметр	Описание
	Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-smbspider-daemon` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-smbspider-daemon`
`Start` *{логический}*	Компонент запускается демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно запустить компонент, а установка в значение `No` — немедленно завершить его работу. Значение по умолчанию: `No`

`[*] ExcludedPath`
 	
{путь к файлу или каталогу}
	Путь к объекту внутри разделяемого каталога, который должен быть пропущен при проверке вместе со всеми подкаталогами и вложенными файлами. Допускается указание пути относительно корневого каталога файлового хранилища SMB (см. параметр `SambaChrootDir`) как к отдельному файлу, так и к каталогу в целом. Допускается использовать файловые маски, содержащие символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`.
	
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	
	Пример: Добавить в список файл `etc/file1` и каталог `usr/bin`.
	
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[SMBSpider]`
	`ExcludedPath = "etc/file1", "usr/bin"`
	• Две строки (по одному значению в строке):
	`[SMBSpider]`
	`ExcludedPath = etc/file1`
	`ExcludedPath = usr/bin`

Параметр	Описание

	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset SMBSpider.ExcludedPath -a etc/file1`
	`# drweb-ctl cfset SMBSpider.ExcludedPath -a usr/bin`
	Если указан каталог, то будет пропущено все содержимое этого каталога.
	Значение по умолчанию: *(не задано)*

`[*] IncludedPath`
{путь к файлу или каталогу}
	Путь к объекту внутри разделяемого каталога, который должен обязательно проверяться. Допускается указание пути относительно корневого каталога файлового хранилища SMB (см. параметр `SambaChrootDir`) как к отдельному файлу, так и к каталогу в целом. Допускается использовать файловые маски, содержащие символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`.
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	Пример: Добавить в список файл `etc/file1` и каталог `usr/bin`.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[SMBSpider]`
	`IncludedPath = "etc/file1", "usr/bin"`
	• Две строки (по одному значению в строке):
	`[SMBSpider]`
	`IncludedPath = etc/file1`
	`IncludedPath = usr/bin`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset SMBSpider.IncludedPath -a etc/file1`
	`# drweb-ctl cfset SMBSpider.IncludedPath -a usr/bin`
	Если указан каталог, то будут проверены все содержащиеся в этом каталоге файлы и подкаталоги.
	Данный параметр имеет приоритет над параметром `ExcludedPath`, т. е. если один и тот же объект (файл или каталог) включен в оба параметра, то он будет проверен.
	Значение по умолчанию: *(не задано)*

Параметр	Описание
`[*] AlertFiles` *{логический}*	Создавать или не создавать для заблокированного файла текстовый файл с описанием причин блокировки. Создаваемый файл будет иметь имя *<имя заблокированного файла>*`.drweb.alert.txt`. Допустимые значения: • `Yes` — создавать файлы причин блокировки; • `No` — не создавать такие файлы. Значение по умолчанию: `Yes`
`[*] OnKnownVirus` *{действие}*	Действие при обнаружении известной угрозы. Допустимые значения: `BLOCK`, `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `CURE`
`[*] OnIncurable` *{действие}*	Действие в случае неудачной попытки излечения угрозы. Допустимые значения: `BLOCK`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnSuspicious` *{действие}*	Действие при обнаружении подозрительного объекта. Допустимые значения: `PASS`, `REPORT`, `BLOCK`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`[*] OnAdware` *{действие}*	Действие при обнаружении рекламной программы. Допустимые значения: `PASS`, `REPORT`, `BLOCK`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `PASS`
`[*] OnDialers` *{действие}*	Действие при обнаружении программы автоматического дозвона. Допустимые значения: `PASS`, `REPORT`, `BLOCK`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `PASS`
`[*] OnJokes` *{действие}*	Действие при обнаружении программы-шутки. Допустимые значения: `PASS`, `REPORT`, `BLOCK`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `PASS`
`[*] OnRiskware` *{действие}*	Действие при обнаружении потенциально опасной программы.

Параметр	Описание
	Допустимые значения: `PASS`, `REPORT`, `BLOCK`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `PASS`
`[*] OnHacktools` *{действие}*	Действие при обнаружении хакерской программ. Допустимые значения: `PASS`, `REPORT`, `BLOCK`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `PASS`
`[*] BlockOnError` *{логический}*	Блокировать или не блокировать файл для доступа, если в процессе его проверки произошла ошибка, либо если отсутствует действующая лицензия, разрешающая проверку файлов монитором SplDer Guard для SMB.  Если этот параметр установлен в значение `Yes`, то при отсутствии действующей лицензии SplDer Guard для SMB будет блокировать все файлы, помещаемые в защищаемый им разделяемый каталог. Допустимые значения: • `Yes` — блокировать доступ к файлу; • `No` — не блокировать доступ к файлу. Значение по умолчанию: `Yes`
`[*] ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `30s`
`[*] HeuristicAnalysis` *{On | Off}*	Использовать или не использовать эвристический анализ для поиска возможных неизвестных угроз. Эвристический анализ повышает надежность проверки, но увеличивает ее длительность. Параметр `OnSuspicious` определяет действие при срабатывании эвристического анализатора. Допустимые значения: • `On` — использовать эвристический анализ при проверке; • `Off` — не использовать эвристический анализ. Значение по умолчанию: `On`
`[*] PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Под запакованным объектом понимается

Параметр	Описание
	исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Все объекты, уровень вложенности которых больше указанного, будут пропускаться при проверке, инициированной по запросу SplDer Guard для SMB. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[*] ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `0`
`[*] MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[*] ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов с вложениями (например, страницы HTML, файлы `.jar` и т. п.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`

Параметр	Описание
`[*] MaxCompressionRatio` *{целое число}*	Максимально допустимая степень сжатия проверяемых объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, то он будет пропущен при проверке, инициированной по запросу SpIDer Guard для SMB. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`
`SmbSocketPath` *{путь к файлу}*	Путь к файлу сокета для взаимодействия SpIDer Guard для SMB с модулям VFS SMB. Этот путь всегда является относительным и дополняет путь, указанный в значении параметра `SambaChrootDir` (в случае пустого значения дополняется путь к корню файловой системы `/`). Значение по умолчанию: `var/run/.com.drweb.smb_spider_vfs`
`SambaChrootDir` *{путь к каталогу}*	Путь к корневому каталогу файлового хранилища SMB (переопределяется через `chroot` файловым сервером). Используется как префикс, подставляемый в начало всех путей к файлам и каталогам, находящимся в файловом хранилище, и описывает путь к ним относительно корня локальной файловой системы. Если этот путь не указан, то используется путь к корню файловой системы `/`. Значение по умолчанию: *(не задано)*
`ActionDelay` *{интервал времени}*	Величина задержки, которую SpIDer Guard для SMB нужно выдержать между моментом обнаружения угрозы и применением действия к инфицированному объекту. В течение этого периода файл будет блокирован. Значение по умолчанию: `1d`
`MaxCacheSize` *{размер}*	Размер кеша, отводимого модулям VFS SMB на хранение информации о проверенных файлах в контролируемых ими каталогах SMB. Если указано `0`, то кеш не используется. Значение по умолчанию: `10MB`

Настройка индивидуальных параметров мониторинга

В конфигурационном файле SMB-сервера Samba (обычно это файл `smb.conf`) можно задать уникальный тег для каждого модуля VFS SMB, контролирующего каждый разделяемый каталог (хранилище). Уникальные теги для модулей VFS SMB в файле `smb.conf` задаются строкой вида:

```
smb_spider:tag = <имя>
```

где <*имя*> — это уникальный тег (имя), присвоенный сервером Samba модулю VFS SMB, контролирующему некоторый разделяемый каталог.

Если для какого-либо модуля VFS SMB определен уникальный тег <*имя*>, то имеется возможность добавить в конфигурационный файл Dr.Web Server Security Suite, наряду с секцией `[SMBSpider]`, хранящей все параметры работы с SMB, отдельную секцию, регулирующую только параметры проверки конкретного хранилища. Такое хранилище защищается модулем VFS SMB, имеющим присвоенный тег. Данная секция должна иметь имя вида `[SMBSpider.Share.<имя>]`.

Индивидуальные секции для модулей VFS SMB могут включать в себя список параметров, отмеченных символом `[*]` в таблице выше. Остальные параметры не могут быть указаны в индивидуальных секциях, поскольку они всегда определяются сразу для всех модулей VFS SMB, с которыми работает монитор каталогов SMB SpIDer Guard для SMB.

Модуль VFS SMB будет брать значения всех параметров, не указанных в индивидуальной секции `[SMBSpider.Share.<имя>]`, которую он использует, из общей секции `[SMBSpider]`. Таким образом, если вовсе не задавать индивидуальных секций, помеченных тегами, то все модули VFS SMB будут использовать одинаковые настройки защиты контролируемых разделяемых каталогов. При этом, если из секции `[SMBSpider.Share.<имя>]` удалить какой-либо параметр, то для этой секции (и соответствующего каталога с тегом <*имя*>) будет применяться не значение параметра по умолчанию, а значение, указанное в соответствующем одноименном «родительском» параметре (из общей секции `[SMBSpider]`).

Чтобы добавить новую секцию параметров для разделяемого каталога Samba с тегом <*имя*> при помощи утилиты управления Dr.Web Server Security Suite из командной строки Dr.Web Ctl (запускается командой `drweb-ctl`), выполните команду:

```
# drweb-ctl cfset SmbSpider.Share -a <имя>
```

Пример:

```
# drweb-ctl cfset SmbSpider.Share -a AccountingFiles
# drweb-ctl cfset SmbSpider.Share.AccountingFiles.OnAdware QUARANTINE
```

Первая команда добавит в файл конфигурации секцию `[SMBSpider.Share.AccountingFiles]`, а вторая изменит в ней значение параметра

`OnAdware`. Таким образом, добавленная секция будет содержать все параметры, отмеченные символом `[*]` в таблице выше, причем значения всех параметров, кроме параметра `OnAdware`, указанного в команде, будут совпадать со значениями параметров из общей секции `[SMBSpider]`.

9.5.4. Сборка модуля VFS SMB

В этом разделе

- Общие сведения
- Инструкция по сборке модуля VFS SMB

Общие сведения

Если версия Samba на вашем файловом сервере не совместима ни с одной из имеющихся в наличии версий вспомогательного модуля VFS SMB, используемого монитором SpIDer Guard для SMB, вам потребуется собрать этот модуль из исходного кода.

Исходный код вспомогательного модуля VFS SMB, используемого SpIDer Guard для SMB, поставляется в отдельном пакете `drweb-smbspider-modules-src` и запакован в архив формата `tar.gz`. При установке пакета `drweb-smbspider-modules-src` архив с исходным кодом располагается в каталоге `/usr/src/` и имеет имя `drweb-smbspider-11.1.src.tar.gz`. В случае отсутствия этого архива по указанному пути выполните установку пакета (из репозитория или выборочной установкой из универсального пакета, в зависимости от способа, которым установлен Dr.Web Server Security Suite).

Кроме исходного кода модуля VFS SMB, используемого SpIDer Guard для SMB, вам также потребуется исходный код используемой вами версии сервера Samba. В случае отсутствия исходного кода загрузите его. Для определения, какая версия Samba у вас используется, выполните команду:

```
$ smbd -V
```

Вспомогательный модуль VFS SMB, используемый SpIDer Guard для SMB, должен быть собран с использованием исходного кода той версии Samba, которая работает на вашем файловом сервере, в противном случае работоспособность SpIDer Guard для SMB не гарантируется.

Для выполнения сборки из исходного кода необходимо обладать правами суперпользователя (обычно пользователя *root*). Для получения прав суперпользователя при сборке используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Инструкция по сборке модуля VFS SMB

1. Распакуйте архив с исходным кодом модуля в любой каталог. Например, команда

   ```
   # tar -xf drweb-smbspider-11.1.src.tar.gz
   ```

   распакует архив непосредственно в каталог, содержащий сам архив, создав в нем подкаталог с именем файла архива.

2. Уточните версию используемого вами сервера Samba и загрузите его исходный код, если этого еще не было сделано.

3. Уточните, использует ли установленный у вас сервер Samba опцию `CLUSTER_SUPPORT`, выполнив команду:

   ```
   $ smbd -b | grep CLUSTER_SUPPORT
   ```

   Если опция `CLUSTER_SUPPORT` используется установленным у вас сервером Samba, в результате выполнения указанной команды на экран будет выдана строка `CLUSTER_SUPPORT`.

4. Перейдите в каталог с исходным кодом Samba и выполните конфигурирование (`./configure`) и сборку (`make`) сервера. При конфигурировании укажите актуальное значение опции, отвечающей за использование `CLUSTER_SUPPORT`. В случае проблем с конфигурированием и сборкой исходного кода Samba, обратитесь к документации разработчика.

   > Сборка Samba из исходного кода нужна только для последующей правильной сборки модуля VFS SMB, используемого SplDer Guard для SMB. Замены установленного у вас сервера Samba на собранный из исходного кода не потребуется.

5. После успешного окончания сборки Samba перейдите в каталог с исходным кодом модуля VFS SMB и выполните команду:

   ```
   # ./configure --with-samba-source=<путь к каталогу исходного кода Samba> && make
   ```

   где *<путь к каталогу исходного кода Samba>* — это путь к каталогу, в котором производилась сборка Samba на предыдущем шаге.

6. После успешной сборки модуля VFS SMB, скопируйте полученный файл `libsmb_spider.so` из созданного в результате сборки подкаталога `.libs` в каталог VFS-модулей сервера Samba (по умолчанию для GNU/Linux — `/usr/lib/<архитектура>-linux-gnu/samba/`) с переименованием файла в `smb_spider.so`, выполнив, например, команду:

   ```
   # cp ./.libs/libsmb_spider.so /usr/lib/x86_64-linux-gnu/samba/smb_spider.so
   ```

7. После копирования собранного модуля VFS SMB, каталоги, в которых производилась сборка модуля и сервера Samba, можно удалить.

Далее необходимо выполнить интеграцию Dr.Web Server Security Suite с сервером Samba, как это описано в соответствующем разделе Руководства администратора. В данном случае на первом шаге интеграции не требуется создавать символической ссылки `smb_spider.so` в каталоге VFS-модулей сервера Samba.

9.6. SpIDer Guard для NSS



Компонент поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux, и работает только в Novell Open Enterprise Server SP2 на базе операционной системы SUSE Linux Enterprise Server 10 SP3 или более поздней.

Монитор томов SpIDer Guard для NSS предназначен для мониторинга файловой активности на томах файловой системы NSS (Novell Storage Services). Компонент работает в режиме резидентного монитора и отслеживает основные события файловой системы, связанные с изменением файлов (создание, открытие, закрытие). При перехвате этих событий монитор проверяет, было ли изменено содержимое файла, и если да, то формирует задание компоненту проверки файлов Dr.Web File Checker на проверку содержимого измененного файла.

9.6.1. Принципы работы

В этом разделе

- Общие сведения
- Задание путей к проверяемым объектам

Общие сведения

Монитор SpIDer Guard для NSS работает в режиме демона (обычно запускается демоном управления конфигурацией Dr.Web ConfigD при запуске системы). Он выполняет наблюдение только тех томов файловой системы NSS, которые указаны в настройках монитора (параметр `ProtectedVolumes`). Точка файловой системы, в которую производится монтирование томов NSS, определяется автоматически. Автоматической корректировки списка наблюдаемых томов NSS по мере их монтирования или отмонтирования не производится. При обнаружении новых или измененных файлов на томах NSS монитор запрашивает их проверку компонентом проверки файлов Dr.Web File Checker.



Особенностью работы монитора томов NSS является то, что если угроза обнаруживается в файле при его копировании (как на защищаемый том, так и внутри тома NSS), то SplDer Guard для NSS отметит наличие угрозы только в файле-копии, но оставит не обнаруженной угрозу в файле-источнике. Файл-источник в этом случае будет считаться безопасным до тех пор, пока к нему не будет осуществлена отдельная попытка доступа, причем, если он расположен на томе NSS, то проверен он будет только в случае его изменения.

Если в настройках монитора томов NSS для какого-либо типа угроз указано действие `QUARANTINE`, при восстановлении объекта с угрозой этого типа из карантина на том NSS этот объект будет снова незамедлительно перемещен в карантин. Например, настройки по умолчанию:

```
NSS.OnKnownVirus = CURE
NSS.OnIncurable = QUARANTINE
```

помещают все неизлечимые объекты в карантин. Поэтому, при восстановлении неизлечимого объекта из карантина на том NSS он будет снова незамедлительно перемещен в карантин.

Задание путей к проверяемым объектам

Монитор томов SplDer Guard для NSS будет проверять только те объекты файловой системы, которые находятся на защищаемых томах NSS (параметр `ProtectedVolumes`) и пути к которым на этих томах не соответствуют путям, указанным в параметре `ExcludedPath`, и соответствуют путям, указанным в параметре `IncludedPath`. При этом параметр `IncludedPath` имеет приоритет над параметром `ExcludedPath`: если путь к объекту содержится в обоих этих параметрах, то он проверяется. Использование исключений может быть необходимо, если файлы в каком-либо каталоге часто изменяются, что порождает их постоянную перепроверку и тем самым нагружает систему. Если точно известно, что частое изменение файлов в каком-либо каталоге является не следствием вредоносной активности, а следствием работы какой-либо доверенной программы, вы можете добавить путь к этому каталогу или этим файлам в список исключений. В этом случае монитор томов SplDer Guard для NSS не будет реагировать на изменения этих файлов. Параметр `IncludedPath` разумно использовать, если нужно обеспечить проверку каких-либо объектов, находящихся внутри пути, указанном в параметре `ExcludedPath`.

Рассмотрим пример настроек:

```
ProtectedVolumes =
ExcludedPath = vol1/path1, vol1/path2, vol2/sys
IncludedPath = vol1/path1, vol1/path2/incl, vol2/doc
```

При указанных настройках монитор будет проверять все файлы на томе `vol3` (не наложено никаких ограничений на проверку), все файлы на томе `vol2`, за исключением файлов, находящихся в каталоге `/sys` и всех его подкаталогах. На томе `vol1` будут игнорироваться только файлы в каталоге `/path2`, но при этом будут проверяться файлы

во всех прочих каталогах этого тома, которые не находятся в каталоге `/path2`, а также объекты, содержащиеся в каталоге `/path2/incl`.

> Указание одного и того же пути (в данном примере — `vol1/path`) в обоих списках бессмысленно, поскольку это равносильно отсутствию ограничений на проверку этого пути. Кроме того, указание пути `vol2/doc` в параметре `IncludedPath` также бессмысленно, поскольку зона исключений, заданная для тома `vol2`, содержит только каталог `/sys`.

Параметры `IncludedPath` и `ExcludedPath` допускают использование файловых масок (*wildcards*). Например, настройка:

```
ExcludedPath = vol1/*.txt
```

исключает из проверки на томе `vol1` (томе, смонтированном в каталог `vol1` точки монтирования томов NSS) все файлы, соответствующие маске `*.txt`. Регистрозависимость путей, указываемых в параметрах `IncludedPath` и `ExcludedPath`, определяется настройками NSS.

> Об интеграции Dr.Web Server Security Suite с файловой службой см. в разделе Интеграция с томами NSS.

9.6.2. Аргументы командной строки

Чтобы запустить компонент SpIDer Guard для NSS из командной строки, выполните команду:

```
$ /opt/drweb.com/bin/drweb-nss [<параметры>]
```

SpIDer Guard для NSS допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-nss --help
```

Данная команда выведет на экран краткую справку компонента SpIDer Guard для NSS.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при загрузке операционной системы. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-nss`.

9.6.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[NSS]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: `/opt/drweb.com/bin/drweb-nss`
`Start` *{логический}*	Компонент запускается демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: `No`

Параметр	Описание
`LogProtocol` *{логический}*	Сохранять или не сохранять сообщения протокола в журнал монитора томов NSS SplDer Guard для NSS. Возможные значения: • `Yes` — сохранять; • `No` — не сохранять. Значение по умолчанию: `No`

`ProtectedVolumes`
{имя тома}
	Имена томов файловой системы NSS, находящихся в точке монтирования томов NSS и подлежащих защите. Если параметр пуст, то защите подлежат все тома, присутствующие в точке монтирования томов NSS.
	
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	
	Пример: Добавить в список тома `vol1` и `vol2`.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[NSS]`
	`ProtectedVolumes = "vol1", "vol2"`
	• Две строки (по одному значению в строке):
	`[NSS]`
	`ProtectedVolumes = vol1`
	`ProtectedVolumes = vol2`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset NSS.ProtectedVolumes -a vol1`
	`# drweb-ctl cfset NSS.ProtectedVolumes -a vol2`
	Значение по умолчанию: *(не задано)*

`ExcludedPath` *{путь к файлу или каталогу}*	Путь к объекту (файлу или каталогу), который должен быть пропущен при проверке. Если указан каталог, то будет пропущено все содержимое этого каталога, включая подкаталоги и вложенные файлы, за исключением объектов, пути к которым указаны в параметре `IncludedPath` — эти объекты *будут проверяться*. Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список файл `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации.

Параметр	Описание

	• Два значения в одной строке:
	`[NSS]`
	`ExcludedPath = "/etc/file1", "/usr/bin"`
	• Две строки (по одному значению в строке):
	`[NSS]`
	`ExcludedPath = /etc/file1`
	`ExcludedPath = /usr/bin`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset NSS.ExcludedPath -a /etc/file1`
	`# drweb-ctl cfset NSS.ExcludedPath -a /usr/bin`
	Параметр допускает использование файловых масок (*wildcards*). Регистрозависимость указываемых путей определяется настройками NSS.
	Пути в списке *указываются относительными* — относительно точки монтирования томов NSS.
	Значение по умолчанию: *(не задано)*

`IncludedPath`
{путь к файлу или каталогу}
	Путь к объекту (файлу или каталогу), который должен быть обязательно проверен. Если указан каталог, то будут проверены все содержащиеся в этом каталоге файлы и подкаталоги.
	Этот параметр используется при необходимости проверки отдельных объектов (файлов или подкаталогов), путь к которым указан в параметре `ExcludedPath`. Если путь к объекту указан в значениях параметров `IncludedPath` и `ExcludedPath` одновременно, то этот объект будет проверен.
	Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	Пример: Добавить в список файл `/etc/file1` и каталог `/usr/bin`.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[NSS]`
	`IncludedPath = "/etc/file1", "/usr/bin"`
	• Две строки (по одному значению в строке):
	`[NSS]`
	`IncludedPath = /etc/file1`
	`IncludedPath = /usr/bin`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset NSS.IncludedPath -a /etc/file1`
	`# drweb-ctl cfset NSS.IncludedPath -a /usr/bin`

Параметр	Описание
	Параметр допускает использование файловых масок (*wildcards*) и может быть чувствительным к регистру (в зависимости от настроек NSS). Пути в списке *указываются относительными* — относительно точки монтирования томов NSS. Значение по умолчанию: *(не задано)*
`OnKnownVirus` *{действие}*	Действие при обнаружении известной угрозы. Допустимые значения: `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `CURE`
`OnIncurable` *{действие}*	Действие в случае неудачной попытки лечения угрозы. Допустимые значения: `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`OnSuspicious` *{действие}*	Действие в случае обнаружения неизвестной угрозы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `QUARANTINE`
`OnAdware` *{действие}*	Действие в случае обнаружения рекламной программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`OnDialers` *{действие}*	Действие в случае обнаружения программы автоматического дозвона. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`OnJokes` *{действие}*	Действие в случае обнаружения программы-шутки. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`OnRiskware` *{действие}*	Действие в случае обнаружения потенциально опасной программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`OnHacktools` *{действие}*	Действие в случае обнаружения хакерской программы. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`

Параметр	Описание
`OnError` *{действие}*	Действие в случае ошибки во время проверки файла. Допустимые значения: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
`ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла по запросу от монитора томов NSS. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `30s`
`HeuristicAnalysis` *{On | Off}*	Использовать или не использовать эвристический анализ для поиска возможных неизвестных угроз при проверке по запросу от монитора томов NSS. Использование эвристического анализа повышает надежность проверки, но увеличивает ее длительность. Действие при срабатывании эвристического анализатора задается параметром `OnSuspicious`. Возможные значения: • `On` — использовать эвристический анализ при проверке; • `Off` — не использовать эвристический анализ. Значение по умолчанию: `On`
`PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `0`

Параметр	Описание
`MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов с вложениями (например, страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MaxCompressionRatio` *{целое число}*	Максимально допустимая степень сжатия проверяемых объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, то он будет пропущен при проверке, инициированной по запросу монитора томов NSS. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`



Если в настройках монитора томов NSS для одного или нескольких типов угроз указано действие `QUARANTINE`, то при восстановлении угрозы этого типа из карантина на том NSS она будет снова незамедлительно перемещена в карантин. Например, настройки по умолчанию

```
NSS.OnKnownVirus = CURE
NSS.OnIncurable = QUARANTINE
```

помещают все неизлечимые объекты в карантин. Поэтому при восстановлении неизлечимого объекта из карантина на том NSS он будет снова незамедлительно перемещен в карантин.

9.7. Dr.Web ClamD

Компонент Dr.Web ClamD предназначен для эмуляции интерфейса антивирусного демона `clamd`, являющегося центральным компонентом антивирусного продукта Clam AntiVirus (ClamAV®) от Sourcefire, Inc. Этот интерфейс позволяет внешним приложениям, которые могут использовать антивирусный продукт ClamAV®, проверять файлы с помощью Dr.Web Server Security Suite.

9.7.1. Принципы работы

Компонент Dr.Web ClamD позволяет выполнять по запросу от внешних приложений проверку на наличие угроз как содержимого файлов, расположенных в локальной файловой системе, так и непосредственно потоков данных, передаваемых внешним приложением через сокет. Кроме того, компонент может проверять содержимое файлов, для которых внешнее приложение передало отрытый дескриптор через сокет.



Проверка файла по переданному дескриптору осуществляется только через локальный Unix-сокет.

Если внешнее приложение предоставило путь к файлу в локальной файловой системе, компонент передает задание на проверку этого файла компоненту проверки файлов Dr.Web File Checker, иначе он передает данные, полученные от приложения через сокет, агенту распределенной проверки Dr.Web Network Checker.

По умолчанию компонент не запускается автоматически при старте Dr.Web Server Security Suite. Чтобы обеспечить запуск компонента, необходимо выполнить не только его включение настройкой `Start`, но и определить не менее одной точки подключения. После запуска компонент ожидает поступления запросов от внешних приложений на проверку указанных файлов или потоков передаваемых данных. В настройках можно определить набор различных точек подключения внешних приложений, указав для каждой свои собственные настройки проверки.

В качестве внешних приложений могут выступать и непосредственно серверы файловых служб (такие как Samba и ProFTPd), если они оснащены модулем интеграции с Dr.Web ClamD. Подробнее см. в разделе Интеграция с внешними приложениями.



Обнаруженные угрозы *не нейтрализуются* средствами Dr.Web Server Security Suite, внешнему приложению только возвращается результат проверки. Таким образом, внешнее приложение само несет ответственность за нейтрализацию обнаруженной угрозы.

9.7.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web ClamD из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-clamd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-clamd [<параметры>]
```

Dr.Web ClamD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-clamd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web ClamD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости (обычно при загрузке операционной системы). Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-clamd`.

9.7.3. Параметры конфигурации

В этом разделе

- Параметры компонента
- Особенность настроек компонента

Компонент использует параметры конфигурации, заданные в секции `[ClamD]` объединенного конфигурационного файла Dr.Web Server Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-clamd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-clamd`
`Start` *{логический}*	Компонент запускается демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: `No`
`Endpoint.<тег>.ClamdSocket` *{IP-адрес | Unix-сокет}*	Точка подключения с именем *<тег>* и сокет (адрес IPv4 или адрес сокета Unix) для клиентов, желающих проверять файлы на наличие угроз.

Параметр	Описание
	Для одной точки <*тег*> может быть задан только один сокет. Значение по умолчанию: не задано
`[Endpoint.<тег>.]ReadTimeout` *{интервал времени}*	Тайм-аут на ожидание данных от клиента. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки <*тег*>, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `5s`
`[Endpoint.<тег>.]StreamMaxLength` *{размер}*	Максимальный размер данных, которые могут быть получены от клиента (при передаче данных для проверки в виде потока байтов). Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки <*тег*>, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `25mb`
`[Endpoint.<тег>.]ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла или одной порции данных, поступивших от клиента. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки <*тег*>, иначе оно определено для всех точек, у которых значение этого параметра не задано. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `3m`
`[Endpoint.<тег>.]HeuristicAnalysis` *{On | Off}*	Использовать эвристический анализ при проверке. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки <*тег*>, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `On`
`[Endpoint.<тег>.]PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Запакованные объекты представляют собой исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Они могут включать другие запакованные объекты, а те, в свою очередь, также могут включать

Параметр	Описание
	запакованные объекты, и т. д. Максимальный уровень вложенности — это предельный уровень, после которого запакованные объекты внутри запакованных объектов не проверяются. Если указан префикс `Endpoint.`<*тег*>, то значение параметра определено только для точки <*тег*>, иначе оно определено для всех точек, у которых значение этого параметра не задано. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[Endpoint.`<*тег*>`.]ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.). Архивы могут содержать другие архивы, а те, в свою очередь, также могут содержать архивы, и т. д. Максимальный уровень вложенности — это предельный уровень, после которого архивы внутри архивов не проверяются. Если указан префикс `Endpoint.`<*тег*>, то значение параметра определено только для точки <*тег*>, иначе оно определено для всех точек, у которых значение этого параметра не задано. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[Endpoint.`<*тег*>`.]MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень, после которого объекты внутри объектов не будут проверяться. Если указан префикс `Endpoint.`<*тег*>, то значение параметра определено только для точки <*тег*>, иначе оно определено для всех точек, у которых значение этого параметра не задано. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`

Параметр	Описание
`[Endpoint.<тег>.]ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов, содержащих вложенные объекты (например, страницы HTML или файлы `.jar`). Эти объекты могут содержать другие вложенные объекты, которые, в свою очередь, также могут содержать вложенные объекты, и т. д. Максимальный уровень вложенности — это предельный уровень, после которого объекты внутри объектов не проверяются. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[Endpoint.<тег>.]MaxCompressionRatio` *{целое число}*	Максимально допустимая степень сжатия запакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`
`[Endpoint.<тег>.]DetectSuspicious` *{логический}*	Сообщать о подозрительных файлах, обнаруженных эвристическим анализатором. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `Yes`
`[Endpoint.<тег>.]DetectAdware` *{логический}*	Сообщать о файлах, содержащих рекламные программы. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано.

Параметр	Описание
	Значение по умолчанию: `Yes`
`[Endpoint.<тег>.]DetectDialers` *{логический}*	Сообщать о файлах, содержащих программы дозвона. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `Yes`
`[Endpoint.<тег>.]DetectJokes` *{логический}*	Сообщать о файлах, содержащих программы-шутки. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `No`
`[Endpoint.<тег>.]DetectRiskware` *{логический}*	Сообщать о файлах, содержащих потенциально опасные программы. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `No`
`[Endpoint.<тег>.]DetectHacktools` *{логический}*	Сообщать о файлах, содержащих программы взлома. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `No`
`[Endpoint.<тег>.] ReportPasswordProtected` *{целое число}*	Сообщать об ошибке, если проверяемые файлы защищены паролем. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `No`

Особенность настроек компонента

Параметры, отмеченные необязательным префиксом `Endpoint.<тег>`, могут быть сгруппированы. Каждая такая группа определяет *точку подключения* (*endpoint*) с задаваемым уникальным идентификатором *<тег>*, используемую клиентами для подключения к компоненту. Все параметры проверки, включенные в одну группу, определяют параметры, которые будут применяться при проверке данных от клиентов, подключившихся к этой точке. Если параметр указан без префикса `Endpoint.<тег>`, то он определяет значение, применяемое для всех точек подключения. Если из точки подключения удалить параметр, то для точки подключения будет применяться не значение параметра по умолчанию, а значение, указанное в соответствующем одноименном «родительском» параметре (без префикса `Endpoint.<тег>`).



Параметр `ClamdSocket` должен обязательно задаваться с префиксом `Endpoint.<тег>`, поскольку он не только определяет прослушиваемый сокет, но и определяет группу (точку подключения), к которой этот сокет привязывается.

Пример

Пусть требуется организовать две точки подключения для двух групп внешних приложений (серверов) *servers1* и *servers2*. При этом серверы из группы *servers1* могут подключаться через Unix-сокет, а серверы из группы *servers2* — через сетевое соединение. Кроме того, эвристический анализ должен быть выключен по умолчанию, но для серверов из группы *servers2* его нужно использовать. Пример соответствующих настроек:

1) Для задания в файле конфигурации:

```
[ClamD]
HeuristicAnalysis = Off

[ClamD.Endpoint.servers1]
ClamdSocket = /tmp/srv1.socket

[ClamD.Endpoint.servers2]
ClamdSocket = 127.0.0.1:1234
HeuristicAnalysis = On
```

2) Для задания через утилиту командной строки Dr.Web Ctl:

```
# drweb-ctl cfset ClamD.HeuristicAnalysis Off
# drweb-ctl cfset ClamD.Endpoint -a servers1
# drweb-ctl cfset ClamD.Endpoint -a servers2
# drweb-ctl cfset ClamD.Endpoint.servers1.ClamdSocket /tmp/srv1.socket
# drweb-ctl cfset ClamD.Endpoint.servers2.ClamdSocket 127.0.0.1:1234
# drweb-ctl cfset ClamD.Endpoint.servers2.HeuristicAnalysis On
```



Оба способа задания настроек приведут к одинаковому результату, но при ручной правке файла конфигурации необходимо применить измененные настройки с помощью команды `drweb-ctl reload`.

9.7.4. Интеграция с внешними приложениями

За счет использования интерфейса, эмулирующего интерфейс антивирусного демона `clamd`, входящего в состав антивирусного решения ClamAV, Dr.Web ClamD может быть сопряжен с любыми внешними приложениями, способными подключаться к антивирусному демону `clamd`.

В таблице ниже перечислены примеры приложений, которые могут использовать `clamd` для антивирусной проверки:

Продукт	**Интеграция**
Файловые службы	
FTP-сервер ProFTPd	**Использование clamd** Проверка файлов, загружаемых на сервер по протоколу FTP. **Требование для интеграции** Сборка ProFTPd с дополнительным модулем `mod_clamav`. **Ссылки на документацию** Документация по продукту ProFTPd. Описание и исходный код модуля mod_clamav

В настройке компонента, обращающегося непосредственно к Dr.Web ClamD как к антивирусному демону `clamd`, следует указать в качестве адреса подключения к антивирусному демону `clamd` путь к Unix-сокету или TCP-сокету, прослушиваемому Dr.Web ClamD на одной из созданных в его настройках точек подключения *(endpoint)*.

Пример подключения ProFTPd к Dr.Web ClamD:

1. Настройка Dr.Web ClamD:

```
[ClamD]
Start = yes

[ClamD.Endpoint.ftps]
ClamdSocket = 127.0.0.1:3310
```

2. Настройка ProFTPd:

```
ClamAV on
ClamServer 127.0.0.1
ClamPort 3310
```

9.8. Dr.Web File Checker

Компонент проверки файлов Dr.Web File Checker предназначен для проверки файлов и каталогов файловой системы. Он используется другими компонентами Dr.Web Server Security Suite для проверки объектов файловой системы. Кроме этого, компонент ведет постоянно хранимый реестр всех угроз, обнаруженных в файловой системе, и выполняет функцию менеджера карантина, управляя содержимым каталогов, в которых располагаются изолированные файлы.

9.8.1. Принципы работы

Компонент Dr.Web File Checker запускается с правами суперпользователя (пользователя *root*) и используется для сканирования объектов файловой системы (файлы, каталоги и загрузочные записи).

Dr.Web File Checker индексирует все проверенные файлы и каталоги и сохраняет данные о проверенных объектах в специальном кеше, чтобы не выполнять повторную проверку объектов, которые уже были проверены ранее и не изменялись с момента последней проверки (в этом случае, если заявка о проверке такого объекта поступает повторно, возвращается результат его предыдущей проверки, извлеченный из кеша).

При поступлении запросов на проверку объектов файловой системы от других компонентов Dr.Web File Checker проверяет, требуется ли проверка запрошенного объекта, и если да, то формирует задание на проверку его содержимого для сканирующего ядра Dr.Web Scanning Engine. Если проверенный объект содержит угрозу, то Dr.Web File Checker заносит его в реестр обнаруженных угроз и применяет к нему нейтрализующее действие (лечение, удаление или перемещение в карантин), если это действие задано клиентским компонентом, инициировавшим проверку, в качестве реакции на угрозу. В качестве инициаторов проверки могут выступать различные компоненты Dr.Web Server Security Suite (например, монитор SpIDer Guard для SMB).

В процессе проверки запрошенных объектов файловой системы компонент проверки файлов формирует и отправляет компоненту-клиенту, запросившему проверку, отчеты о результатах проверки и предпринятых действиях по нейтрализации угроз, если они были обнаружены.

Помимо стандартного метода проверки файлов, для внутренних нужд поддерживаются специальные методы проверки файлов:

- *Метод «flow»* — метод потоковой проверки файлов. Компонент, использующий этот метод, один раз инициализирует параметры проверки и обезвреживания угроз, и далее эти параметры будут применяться ко всему потоку заявок на проверку файлов, поступающих от этого компонента. Этот метод проверки используется монитором SpIDer Guard.
- *Метод «proxy»* — метод проверки файлов, заключающийся в том, что компонент проверки файлов выполняет только проверку файлов на наличие угроз, не применяя к

ним никаких действий, в том числе не выполняя регистрацию обнаруженных угроз (эти действия целиком возлагаются на компонент, инициировавший проверку). Этот метод проверки используется монитором SpIDer Guard для SMB и компонентом Dr.Web ClamD.

В процессе своей работы компонент проверки файлов не только ведет реестр угроз и управляет карантином, но и собирает общую статистику проверки файлов, усредняя количество файлов, проверенных в течение секунды за последнюю минуту, последние 5 минут, последние 15 минут.

9.8.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web File Checker из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-filecheck [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-filecheck [<параметры>]
```

Dr.Web File Checker допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-filecheck --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web File Checker.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при поступлении от других компонентов Dr.Web Server Security Suite заявок на проверку объектов файловой системы. Для управления параметрами работы

компонента, а также для проверки файлов по требованию используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для проверки произвольного файла или каталога компонентом Dr.Web File Checker используйте команду `scan` утилиты Dr.Web Ctl:

```
$ drweb-ctl scan <путь к файлу или каталогу>
```

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-filecheck`.

9.8.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[FileCheck]` объединенного конфигурационного файла Dr.Web Server Security Suite.

Эта секция хранит следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-filecheck` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-filecheck`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`

Параметр	Описание
`DebugClientIpc` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC. Значение по умолчанию: `No`
`DebugScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения, поступающие в процессе проверки файлов. Значение по умолчанию: `No`
`DebugFlowScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о проверке файлов методом *«flow»*. Метод *«flow»* обычно используется монитором SpIDer Guard. Значение по умолчанию: `No`
`DebugProxyScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о проверке файлов методом *«proxy»*. Метод *«proxy»* обычно используется монитором SpIDer Guard для SMB и компонентом Dr.Web ClamD. Значение по умолчанию: `No`
`DebugCache` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о состоянии кеша проверенных файлов. Значение по умолчанию: `No`
`MaxCacheSize` *{размер}*	Максимальный разрешенный размер кеша для хранения информации о проверенных файлах. Если указано `0`, то кеширование отключено. Значение по умолчанию: `50mb`
`RescanInterval` *{интервал времени}*	Длительность интервала, в течение которого не производится повторная проверка содержимого файлов, информация о предыдущей проверке которых имеется в кеше (период актуальности кешированной информации). Допустимые значения: от 0 секунд (`0s`) до 1 минуты (`1m`). Если указан интервал менее `1s`, то задержка отсутствует, файл будет проверяться при любом запросе. Значение по умолчанию: `1s`

9.9. Dr.Web Network Checker

Компонент сетевой проверки данных Dr.Web Network Checker предназначен для проверки в сканирующем ядре данных, полученных через сеть, а также для организации распределенной проверки файлов на наличие угроз. Он позволяет организовать соединение между набором узлов сети с установленным на них Dr.Web Server Security Suite с целью приема и передачи данных (например, содержимого файлов) между узлами сети для проверки этих данных. При взаимодействии узлов компонент организует автоматическое распределение задач на проверку данных (передавая и получая их по сети) на все доступные узлы сети, с которыми настроено соединение, обеспечивая балансировку их нагрузки, вызванной проверкой отправленных данных. Если соединения с удаленными узлами не настроены, компонент передает все полученные данные на проверку локальному сканирующему ядру Dr.Web Scanning Engine.



Данный компонент всегда используется для проверки данных, полученных через сетевые соединения, поэтому, если он отсутствует или недоступен, будет нарушена работоспособность компонентов, отправляющих данные на проверку через сетевое соединение (Dr.Web ClamD).

Данный компонент не предназначен для организации распределенной проверки файлов, расположенных в локальной файловой системе, так как не может заменить компонент проверки файлов Dr.Web File Checker. Для организации распределенной проверки локальных файлов используйте компонент Dr.Web MeshD.

В случае большой интенсивности проверки данных, передаваемых через сеть, возможно возникновение проблем с проверкой из-за исчерпания числа доступных файловых дескрипторов. В этом случае необходимо увеличить лимит на число файловых дескрипторов, доступных Dr.Web Server Security Suite.

Обмен проверяемыми данными может производиться как по открытому каналу, так и по защищенному, с использованием SSL/TLS. При использовании защищенного соединения необходимо обеспечить узлы, обменивающиеся файлами, корректными сертификатами и ключами SSL. Для генерации ключей и сертификатов можно воспользоваться утилитой `openssl`. Пример использования утилиты `openssl` для генерации сертификатов и закрытых ключей приведен в разделе Приложение Д. Генерация сертификатов SSL.

9.9.1. Принципы работы

Компонент позволяет передать данные, не представленные в виде файлов в локальной файловой системе, на сканирование в сканирующее ядро Dr.Web Scanning Engine, расположенное на локальном или удаленном узле. С такими данными работают компоненты, отправляющие данные на проверку через сетевое соединение (Dr.Web ClamD).



Эти компоненты всегда используют Dr.Web Network Checker (даже расположенный на локальном узле) для передачи файлов на проверку сканирующему ядру Dr.Web Scanning Engine. Поэтому, если Dr.Web Network Checker недоступен, эти компоненты *не смогут корректно функционировать*.

Кроме этого, Dr.Web Network Checker позволяет организовать соединение Dr.Web Server Security Suite с заданным набором узлов в сети с установленным на них Dr.Web Server Security Suite (или любым другим решением Dr.Web для Unix версии не ниже 10.1) для организации распределенной проверки на наличие данных, не представленных в виде файлов в локальной файловой системе. За счет этого компонент позволять создать и настроить *сканирующий кластер*, представляющий собой набор узлов сети, обменивающихся данными для проверки (на каждом узле должен быть запущен свой экземпляр агента распределенной проверки Dr.Web Network Checker). На каждом узле сети, включенном в сканирующий кластер, Dr.Web Network Checker выполняет автоматическое распределение задач на проверку данных, передавая их по сети на все доступные узлы, с которыми настроено соединение. При этом осуществляется балансировка нагрузки на узлы, вызванной проверкой данных, в зависимости от количества ресурсов, доступных на удаленных узлах. В качестве индикатора количества ресурсов, доступных для нагрузки, выступает количество дочерних сканирующих процессов, порожденных сканирующим ядром Dr.Web Scanning Engine на узле, включенном в кластер. Также оцениваются длины очередей файлов, дожидающихся проверки на каждом используемом узле.

При этом любой узел сети, включенный в сканирующий кластер, может выступать как в роли клиента сканирования, передающего данные на удаленную проверку, так и в роли сервера сканирования, принимающего с указанных узлов сети данные для проверки. При необходимости агент распределенной проверки можно настроить таким образом, чтобы узел выступал только в качестве сервера сканирования или только в качестве клиента сканирования.

Данные, принятые по сети для проверки, сохраняются в локальную файловую системы в виде временных файлов и передаются на проверку сканирующему ядру Dr.Web Scanning Engine, либо, в случае его недоступности или большой нагруженности, на другой узел сканирующего кластера.

Имеющийся в настройках компонента параметр `InternalOnly` позволяет управлять режимом работы Dr.Web Network Checker, определяя, используется ли он для включения Dr.Web Server Security Suite в сканирующий кластер или только для обеспечения внутренних нужд компонентов, работающих локально в составе Dr.Web Server Security Suite.

Вы можете создать свой собственный компонент (внешнее приложение), использующий Dr.Web Network Checker для проверки файлов (в том числе путем распределения проверки по узлам сканирующего кластера). Для этого компонент Dr.Web Network Checker предоставляет специализированный API, основанный на технологии Google Protobuf. Описание API Dr.Web Network Checker, а также примеры кода клиентского приложения, использующего Dr.Web Network Checker, поставляются в составе пакета `drweb-netcheck`.

Пример организации сканирующего кластера приведен в разделе Организация сканирующего кластера.

9.9.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web Network Checker из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-netcheck [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-netcheck [<параметры>]
```

Dr.Web Network Checker допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-netcheck --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Network Checker.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается автоматически демоном управления конфигурацией

Dr.Web ConfigD по мере необходимости (обычно при старте операционной системы). При этом, если в настройках компонента задано значение параметра `FixedSocket`, а параметр `InternalOnly` установлен в значение `No`, то компонент будет запущен демоном управления конфигурацией и постоянно доступен клиентам через Unix-сокет. Для управления параметрами работы компонента, а также для запуска сетевого сканирования (при наличии настроенного соединения с другими узлами сети) используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки. Если соединение с другими узлами сети не настроено, вместо сетевого сканирования будет запущено обычное сканирование на стороне локального сканирующего ядра.



Чтобы запустить утилиту Dr.Web Ctl, используйте команду `drweb-ctl`.

Чтобы проверить произвольный файл или каталог компонентом Dr.Web Network Checker, используйте команду `netscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl netscan <путь к файлу или каталогу>
```

Чтобы получить справку о компоненте из командной строки, выполните команду `man 1 drweb-netcheck`.

9.9.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[NetCheck]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-netcheck`

Параметр	Описание
	• для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-netcheck`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает работу. Если задано значение параметра `LoadBalanceAllowFrom` или `FixedSocket`, то настройка игнорируется (компонент не завершает свою работу по истечении максимального времени простоя). Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`FixedSocket` *{путь к файлу | адрес}*	Сокет фиксированного экземпляра агента Dr.Web Network Checker. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр агента распределенной проверки файлов, доступный клиентам через этот сокет. Возможные значения: • *<путь к файлу>* — путь к файлу локального Unix-сокета; • *<адрес>* — сетевой сокет в виде пары *<IP-адрес>:<порт>*.

Параметр	Описание

	Убедитесь, что каталогу с файлом сокета назначены следующие права доступа:
	`drwxr-xr-x`
	Чтобы просмотреть права доступа, выполните команду:
	`$ ls -ld <путь к каталогу>`
	Значение по умолчанию: *(не задано)*

`InternalOnly` *{логический}*	Режим работы компонента. Если задано значение `Yes`, то компонент используется только для внутренних нужд компонентов Dr.Web Server Security Suite, но не обслуживает сканирующий кластер или внешние (по отношению к Dr.Web Server Security Suite) клиентские приложения вне зависимости от настроек `LoadBalance*` и заданного значения параметра `FixedSocket`. Значение по умолчанию: `No`
`LoadBalanceUseSsl` *{логический}*	Использовать или не использовать SSL/TLS для соединения с другими узлами. Возможные значения: • `Yes` — использовать SSL/TLS; • `No` — не использовать SSL/TLS. Если этот параметр установлен в `Yes`, то для данного узла и для всех узлов, с которыми он взаимодействует, должны быть обязательно заданы соответствующие друг другу сертификат и закрытый ключ (параметры `LoadBalanceSslCertificate` и `LoadBalanceSslKey`). Значение по умолчанию: `No`
`LoadBalanceSslCertificate` *{путь к файлу}*	Путь к файлу сертификата SSL, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS. Файл сертификата и файл закрытого ключа (определяется параметром `LoadBalanceSslKey`) должны соответствовать друг другу. Значение по умолчанию: *(не задано)*

Параметр	Описание
`LoadBalanceSslKey` *{путь к файлу}*	Путь к файлу закрытого ключа, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS. ⚠ Файл сертификата (определяется параметром `LoadBalanceSslCertificate`) и файл закрытого ключа должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`LoadBalanceSslCa` *{путь}*	Путь к каталогу или файлу, в котором располагается перечень доверенных корневых сертификатов. Среди данных сертификатов должен находиться сертификат, удостоверяющий подлинность сертификатов, используемых агентами внутри сканирующего кластера при обмене данными через SSL/TLS. Если значение параметра не задано, то Dr.Web Network Checker, работающий на данном узле, не проверяет подлинность сертификатов взаимодействующих агентов, однако они, в зависимости от заданных для них настроек, могут проверять подлинность сертификата, используемого агентом, работающим на данном узле. Значение по умолчанию: *(не задано)*
`LoadBalanceServerSocket` *{адрес}*	Сетевой сокет (IP-адрес и порт), прослушиваемый Dr.Web Network Checker на данном узле для получения файлов на проверку от удаленных узлов (при работе в качестве сервера сетевого сканирования). Значение по умолчанию: *(не задано)*
`LoadBalanceAllowFrom` *{IP-адрес}*	IP-адрес удаленного узла сети, от которого Dr.Web Network Checker на данном узле может принимать файлы на проверку (как сервер сетевого сканирования). Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список адреса узлов 192.168.0.1 и 10.20.30.45. 1. Добавление значений в файл конфигурации.

Параметр	Описание

	• Два значения в одной строке:
	`[NetCheck]`
	`LoadBalanceAllowFrom = "192.168.0.1", "10.20.30.45"`
	• Две строки (по одному значению в строке):
	`[NetCheck]`
	`LoadBalanceAllowFrom = 192.168.0.1`
	`LoadBalanceAllowFrom = 10.20.30.45`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 192.168.0.1`
	`# drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 10.20.30.45`
	Если параметр пуст, то удаленные файлы на проверку не принимаются (узел не работает в режиме сервера).
	Значение по умолчанию: *(не задано)*

`LoadBalanceSourceAddress` *{IP-адрес}*	IP-адрес сетевого интерфейса, используемого Dr.Web Network Checker на данном узле для передачи файлов на удаленную проверку, если узел работает как клиент сетевого сканирования, и если на узле доступно несколько сетевых интерфейсов. Если указать пустое значение, то используемый сетевой интерфейс будет автоматически выбран ядром ОС. Значение по умолчанию: *(не задано)*

`LoadBalanceTo`
{адрес}
	Сокет (IP-адрес и порт) удаленного узла, на который Dr.Web Network Checker на данном узле может отправлять файлы на удаленную проверку (как клиент сетевого сканирования).
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[NetCheck]`
	`LoadBalanceTo = "192.168.0.1:1234", "10.20.30.45:5678"`

Параметр	Описание

	• Две строки (по одному значению в строке):
	`[NetCheck]`
	`LoadBalanceTo = 192.168.0.1:1234`
	`LoadBalanceTo = 10.20.30.45:5678`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset NetCheck.LoadBalanceTo -a 192.168.0.1:1234`
	`# drweb-ctl cfset NetCheck.LoadBalanceTo -a 10.20.30.45:5678`
	Если параметр пуст, то локальные файлы не передаются на удаленную проверку (узел не работает в режиме клиента сетевого сканирования).
	Значение по умолчанию: *(не задано)*

`LoadBalanceStatusInterval` *{интервал времени}*	Интервал времени между рассылками данным узлом информации о своей загруженности для всех агентов распределенной проверки, перечисленных в параметре `LoadBalanceAllowFrom`. Значение по умолчанию: `1s`
`SpoolDir` *{путь к каталогу}*	Каталог в локальной файловой системе, используемый для хранения файлов, принятых Dr.Web Network Checker по сети от клиентов сканирования для проверки. Значение по умолчанию: `/tmp/com.drweb.ncheck`
`LocalScanPreference` *{дробное число}*	Относительный вес (предпочтительность) узла при выборе места для проверки файла (локального или принятого по сети). Если в некоторый момент времени вес локального узла больше суммарного веса всех доступных узлов-серверов сканирования, файл будет оставлен агентом для локальной проверки. Минимальное значение: `1`. Значение по умолчанию: `1`
`LoadBalanceSslCrl` *{путь}*	Путь к каталогу или файлу с перечнем отозванных сертификатов. Если значение параметра не задано, то Dr.Web Network Checker, работающий на данном узле, не проверяет сертификаты взаимодействующих агентов на актуальность, однако они, в зависимости от заданных для них настроек, могут проверять актуальность сертификата, используемого агентом, работающим на данном узле. Значение по умолчанию: *(не задано)*

9.9.4. Организация сканирующего кластера

В этом разделе

- Вводные замечания
- Пример организации сканирующего кластера
- Настройка узлов кластера
- Проверка работы кластера

Вводные замечания

Для организации сканирующего кластера, позволяющего выполнять распределенную проверку данных (при сканировании файлов или иных объектов), необходимо иметь набор узлов сети с установленным на каждом из них компонентом Dr.Web Network Checker. Чтобы узел кластера мог не только принимать и передавать данные, подлежащие проверке, необходимо, чтобы на узле также было установлено сканирующее ядро Dr.Web Scanning Engine. Таким образом, для организации узла сканирующего кластера необходимо, чтобы на сервере были установлены как минимум следующие компоненты (прочие компоненты Dr.Web Server Security Suite, устанавливаемые автоматически, для обеспечения работоспособности приведенных здесь компонентов, опущены):

1. Dr.Web Network Checker (пакет `drweb-netcheck`) — компонент приема и передачи данных между узлами по сети.
2. Dr.Web Scanning Engine (пакет `drweb-se`) — сканирующее ядро, необходимое для проверки данных, полученных по сети. Может отсутствовать, в этом случае узел будет только передавать данные для проверки на другие доступные узлы сканирующего кластера.

Узлы, составляющие сканирующий кластер, образуют одноранговую (*peer to peer*) сеть, т. е. каждый из них, в зависимости от того, какие настройки заданы у компонента Dr.Web Network Checker на этом узле, может выступать как в роли *клиента сканирования* (передающего данные на проверку в другие узлы), так и в роли *сервера сканирования* (принимающего данные на проверку от других узлов). При соответствующих настройках узел кластера может быть одновременно и клиентом, и сервером сканирования.

Параметры компонента Dr.Web Network Checker, отвечающие за настройку сканирующего кластера, имеют имя, начинающееся с `LoadBalance`.

Пример организации сканирующего кластера

Рассмотрим пример организации сканирующего кластера, показанного на рисунке ниже.

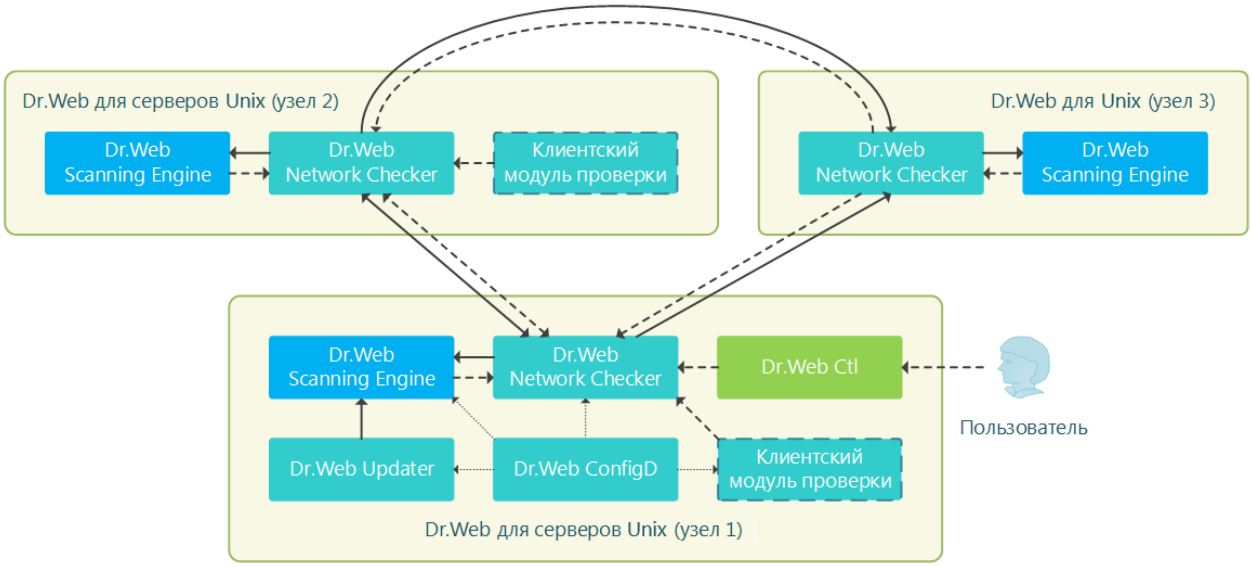


Рисунок 12. Структура сканирующего кластера

В данном случае предполагается, что кластер состоит из трех узлов, обозначенных на рисунке как *узел 1*, *узел 2* и *узел 3*. Узел 1 и узел 2 представляют собой серверы с установленным полноценным продуктом Dr.Web для серверов Unix (например, Dr.Web Gateway Security Suite или Dr.Web Mail Security Suite, тип продукта не имеет значения), а узел 3 используется только для помощи в сканировании файлов, передаваемых с узлов 1 и 2. Поэтому на нем установлен только минимально необходимый комплект компонентов (Dr.Web Network Checker и Dr.Web Scanning Engine, прочие компоненты, устанавливаемые автоматически для обеспечения работоспособности узла, такие как Dr.Web ConfigD, на схеме не обозначены). Узлы 1 и 2 могут функционировать и как серверы, и как клиенты сканирования в отношении друг друга (выполнять взаимное распределение нагрузки, связанной со сканированием), а узел 3 — только в роли сервера, принимая задания с узлов 1 и 2.

«Клиентский модуль проверки» на схеме обозначает компоненты серверов, формирующих компоненту Dr.Web Network Checker на узле задания на проверку, которые будут (в зависимости от соотношения нагрузки) распределены между локальным сканирующим ядром Dr.Web Scanning Engine и узлами-партнерами кластера, выполняющими роль серверов сканирования.



В качестве клиентского модуля проверки могут выступать только компоненты, проверяющие данные, не представленные в виде файла в локальной файловой системе. Это означает, что сканирующий кластер не может быть использован для распределенной проверки файлов монитором файловой системы SpIDer Guard и компонентом проверки файлов Dr.Web File Checker.

Настройка узлов кластера

Для настройки указанной конфигурации кластера необходимо внести изменения в настройки компонента Dr.Web Network Checker на всех трех узлах кластера. Все приведенные ниже фрагменты настроек представлены в формате `.ini` (см. описание формата файла конфигурации).

Узел 1

```
[NetCheck]
InternalOnly = No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <IP-адрес Узла 1>:<Порт Узла 1>
LoadBalanceAllowFrom = <IP-адрес Узла 2>
LoadBalanceSourceAddress = <IP-адрес Узла 1>
LoadBalanceTo = <IP-адрес Узла 2>:<Порт Узла 2>
LoadBalanceTo = <IP-адрес Узла 3>:<Порт Узла 3>
```

Узел 2

```
[NetCheck]
InternalOnly = No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <IP-адрес Узла 2>:<Порт Узла 2>
LoadBalanceAllowFrom = <IP-адрес Узла 1>
LoadBalanceSourceAddress = <IP-адрес Узла 2>
LoadBalanceTo = <IP-адрес Узла 1>:<Порт Узла 1>
LoadBalanceTo = <IP-адрес Узла 3>:<Порт Узла 3>
```

Узел 3

```
[NetCheck]
InternalOnly=No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <IP-адрес Узла 3>:<Порт Узла 3>
LoadBalanceAllowFrom = <IP-адрес Узла 1>
LoadBalanceAllowFrom = <IP-адрес Узла 2>
```

Примечания:

- Прочие (не указанные здесь) параметры Dr.Web Network Checker оставлены без изменения.
- Значения IP-адресов и номеров портов необходимо заменить на актуальные.
- Использование SSL при обмене данными между узлами в данном примере отключено. Чтобы использовать SSL, необходимо задать значение `Yes` для параметра `LoadBalanceUseSsl`, а также задать актуальные значения параметров `LoadBalanceSslCertificate`, `LoadBalanceSslKey` и `LoadBalanceSslCa`.

Проверка работы кластера

Чтобы проверить работу кластера в режиме разделения данных при сканировании, выполните на узлах 1 и 2 команду:

```
$ drweb-ctl netscan <путь к файлу или каталогу>
```

При выполнении этой команды компонент Dr.Web Network Checker проверяет файлы из указанного каталога, распределив нагрузку по настроенным узлам кластера. Чтобы просмотреть статистику сетевой проверки на каждом из узлов, перед началом проверки запустите вывод статистики Dr.Web Network Checker командой:

```
$ drweb-ctl stat -n
```

Чтобы прервать вывод статистики, нажмите CTRL+C или Q.

9.10. Dr.Web Scanning Engine

Сканирующее ядро Dr.Web Scanning Engine предназначено для поиска вирусов и других вредоносных объектов в файлах и загрузочных записях (*MBR — Master Boot Record*, *VBR — Volume Boot Record*) дисковых устройств. Компонент выполняет загрузку в память и запуск антивирусного ядра Dr.Web Virus-Finding Engine и вирусных баз Dr.Web, используемых им для поиска угроз.

Сканирующее ядро работает в режиме демона, в качестве сервиса, принимающего от других компонентов Dr.Web Server Security Suite запросы на проверку объектов файловой системы на наличие угроз (это компоненты Dr.Web File Checker и Dr.Web Network Checker и, возможно, Dr.Web MeshD). При отсутствии или недоступности компонентов Dr.Web Scanning Engine и Dr.Web Virus-Finding Engine антивирусные проверки на данном узле не производятся (за исключением случаев, когда в составе Dr.Web Server Security Suite присутствует компонент Dr.Web MeshD, в настройках которого задано соединение с узлами локального облака, предоставляющими услугу сканирующего ядра).

9.10.1. Принципы работы

Компонент Dr.Web Scanning Engine, работающий в режиме демона, принимает от других компонентов Dr.Web Server Security Suite запросы на проверку объектов файловой системы (файлов, загрузочных записей на дисках) на наличие внедренных угроз, формирует очереди задач на проверку объектов и выполняет проверку запрошенных объектов, используя антивирусное ядро Dr.Web Virus-Finding Engine. Если в проверенном объекте обнаружена угроза, и в задании на проверку стоит указание выполнять лечение, сканирующее ядро пытается выполнять лечение, если это действие может быть применено к проверенному объекту.

Сканирующее ядро, антивирусное ядро Dr.Web Virus-Finding Engine и вирусные базы образуют атомарный комплекс и не могут быть разделены. Сканирующее ядро осуществляет загрузку вирусных баз и обеспечивает среду для функционирования кросс-платформенного антивирусного ядра Dr.Web Virus-Finding Engine. Обновление вирусных баз и антивирусного ядра производится компонентом обновлений Dr.Web Updater, входящим в состав Dr.Web Server Security Suite, но не являющимся частью сканирующего ядра. Компонент обновлений запускается демоном управления конфигурацией Dr.Web ConfigD периодически или принудительно в ответ на поступившую команду пользователя. Кроме того, если Dr.Web Server Security Suite функционирует в режиме централизованной защиты, то функции обновления вирусных баз и антивирусного ядра берет на себя агент централизованной защиты Dr.Web ES Agent, который взаимодействует с сервером централизованной защиты и получает обновления от него.

Dr.Web Scanning Engine может работать как под контролем демона управления конфигурацией Dr.Web ConfigD, так и автономно. В первом случае демон обеспечивает запуск ядра и своевременное обновление вирусных баз, используемых ядром. Во

втором случае запуск ядра и обновление вирусных баз возлагаются на использующее его внешнее приложение. Компоненты Dr.Web Server Security Suite, выполняющие запросы к сканирующему ядру на предмет проверки файлов, используют тот же программный интерфейс, что и внешние приложения.

Вы можете создать свой собственный компонент (внешнее приложение), использующий Dr.Web Scanning Engine для проверки файлов. Для этого компонент Dr.Web Scanning Engine предоставляет специализированный API, основанный на технологии Google Protobuf. Для получения описания API Dr.Web Scanning Engine, а также примеров кода клиентского приложения, использующего Dr.Web Scanning Engine, обратитесь в отдел по работе с партнерами компании «Доктор Веб».

Поступающие задачи на сканирование автоматически распределяются по трем очередям, имеющим различный приоритет (высокий, нормальный и низкий). Очередь, в которую будет помещена задача, определяется исходя из того, какой компонент ее сформировал. Например, задачи, поступающие от мониторов файловых систем, помещаются в очереди высокого приоритета, поскольку при мониторинге важна скорость реакции на действия с объектами файловой системы. Сканирующее ядро ведет статистику своего использования, фиксируя количество поступивших задач на сканирование, а также длины очередей. В качестве показателя средней нагрузки сканирующее ядро определяет среднюю длину очередей в секунду. Этот показатель усредняется для последней минуты, последних 5 минут и последних 15 минут.

Антивирусное ядро Dr.Web Virus-Finding Engine поддерживает как сигнатурный анализ (поиск известных угроз на основе сигнатур, содержащихся в вирусных базах), так и различные технологии эвристического и поведенческого анализа, предназначенные для распознавания потенциальной опасности объекта на основе анализа последовательности содержащихся в нем машинных инструкций и других признаков исполняемого кода.

Эвристический анализатор не гарантирует достоверного распознавания угроз и может допускать следующие ошибки:

- *Ошибки первого рода* — это ложные срабатывания анализатора, когда в качестве вредоносного отмечается безопасный объект.
- *Ошибки второго рода* — это ошибочное признание вредоносного объекта безопасным.

Поэтому угрозы, обнаруженные эвристическим анализатором, отнесены в особую категорию «Подозрительные» (*Suspicious*).

Рекомендуется выполнять перемещение подозрительных объектов в карантин с тем, чтобы в дальнейшем, после обновления вирусных баз, проверить их методами сигнатурного анализа. Для предотвращения ошибок второго рода рекомендуется поддерживать вирусные базы в актуальном состоянии.

Антивирусное ядро Dr.Web Virus-Finding Engine позволяет осуществлять проверку как незапакованных, так и запакованных файлов и объектов, содержащихся в различных контейнерах, таких как архивы, сообщения электронной почты и т. д.

9.10.2. Аргументы командной строки

Чтобы запустить сканирующее ядро Dr.Web Scanning Engine из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-se <сокет> [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-se <сокет> [<параметры>]
```

где обязательный аргумент *<сокет>* указывает адрес сокета, используемого Dr.Web Scanning Engine для обслуживания запросов клиентских компонентов. Может задаваться только в виде пути к файлу (сокет Unix).

Dr.Web Scanning Engine допускает использование следующих параметров:

Параметр	**Описание**
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет
Дополнительные параметры запуска (совпадают с параметрами из конфигурационного файла и замещают их при необходимости):	
`--CoreEnginePath`	Назначение: Путь к файлу библиотеки антивирусного ядра Dr.Web Virus-Finding Engine. Краткий вариант: Нет. Аргументы: *<путь к файлу>* — полный путь к файлу используемой библиотеки.
`--VirusBaseDir`	Назначение: Путь к каталогу, содержащему файлы вирусных баз. Краткий вариант: Нет. Аргументы: *<путь к каталогу>* — полный путь к каталогу вирусных баз.
`--TempDir`	Назначение: Путь к каталогу временных файлов.

	Краткий вариант: Нет. Аргументы: <*путь к каталогу*> — полный путь к каталогу временных файлов.
`--KeyPath`	Назначение: Путь к используемому ключевому файлу. Краткий вариант: Нет. Аргументы: <*путь к файлу*> — полный путь к ключевому файлу.
`--MaxForks`	Назначение: Максимальное разрешенное число дочерних процессов, которые Dr.Web Scanning Engine может породить в процессе проверки. Краткий вариант: Нет. Аргументы: <*число*> — максимальное разрешенное число дочерних процессов.
`--WatchdogInterval`	Назначение: Периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность дочерних процессов, занимающихся проверкой содержимого файлов, для остановки зависших при проверке. Краткий вариант: Нет. Аргументы: <*интервал времени*> — периодичность проверки дочерних процессов.
`--AbortForkOnTimeout`	Назначение: Завершить процессы сканирования при тайм-ауте, послав им сигнал SIGABRT. Краткий вариант: Нет. Аргументы: Нет
`--ShellTrace`	Назначение: Отслеживание оболочки (вывод в журнал расширенной информации о проверке файлов ядром Dr.Web Virus-Finding Engine). Краткий вариант: Нет. Аргументы: Нет
`--LogLevel`	Назначение: Уровень подробности ведения журнала ядром Dr.Web Scanning Engine в процессе работы. Краткий вариант: Нет. Аргументы: <*уровень подробности*>. Возможные значения: • `DEBUG` — самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация. • `INFO` — выводятся все сообщения. • `NOTICE` — выводятся сообщения об ошибках, предупреждения, уведомления. • `WARNING` — выводятся сообщения об ошибках и предупреждения. • `ERROR` — выводятся только сообщения об ошибках.
`--Log`	Назначение: Способ ведения журнала сообщений компонента. Краткий вариант: Нет.

	Аргументы: <*тип журнала*>. Возможные значения:
	• `Stderr[:ShowTimestamp]` — сообщения будут выводиться в стандартный поток ошибок *stderr*.
	Опция `ShowTimestamp` предписывает добавлять к каждому сообщению метку времени.
	• `Syslog[:`<*facility*>`]` — сообщения будут передаваться системной службе журналирования `syslog`.
	Дополнительная метка <*facility*> используется для указания типа журнала, в котором `syslog` будет сохранять сообщения.
	Возможные значения:
	○ `DAEMON` — сообщения демонов;
	○ `USER` — сообщения пользовательских процессов;
	○ `MAIL` — сообщения почтовых программ;
	○ `LOCAL0` — сообщения локальных процессов 0;
	...
	○ `LOCAL7` — сообщения локальных процессов 7.
	• <*path*> — путь к файлу, в который будут сохраняться сообщения журнала.
	Примеры:
	`--Log /var/opt/drweb.com/log/se.log`
	`--Log Stderr:ShowTimestamp`
	`--Log Syslog:DAEMON`

`--ForkMemoryLimit`	Назначение: Максимальный объем оперативной памяти, выделяемый для работы экземпляра сканирующего ядра. Краткий вариант: Нет. Аргументы: <*размер в байтах*> — максимальный объем оперативной памяти. Допустимые значения: от 1073741824 байт (1 Гб) до 4294967296 байт (4 Гб). Значение по умолчанию: `4294967296` (4 Гб) ⚠ Этот параметр не задействуется в 32-разрядных дистрибутивах продукта.
`--EngineDallocLimit`	Назначение: Максимальный объем оперативной памяти, выделяемый для хранения временных файлов. Краткий вариант: Нет. Аргументы: <*размер в байтах*> — максимальный объем оперативной памяти. Допустимые значения: от 52428800 байт (50 Мб) до 1073741824 байт (1 Гб). Значение по умолчанию: `524288000` (500 Мб)

	Настоятельно не рекомендуется менять значение по умолчанию для этого параметра, если вы не уверены, что это действительно необходимо.

Пример:

```
$ /opt/drweb.com/bin/drweb-se /tmp/drweb.ipc/.se --MaxForks=5
```

Данная команда запустит экземпляр сканирующего ядра Dr.Web Scanning Engine, заставив его создать Unix-сокет `/tmp/drweb.ipc/.se` для взаимодействия с клиентскими компонентами и порождать не более 5 сканирующих дочерних процессов при проверке файлов.

Замечания о запуске

При необходимости может быть запущено произвольное количество экземпляров сканирующего ядра Dr.Web Scanning Engine, предоставляющих сервис по проверке файлов на наличие угроз клиентским приложениям (не обязательно только компонентам Dr.Web Server Security Suite). При этом, если в конфигурации компонента задано значение параметра `FixedSocketPath`, то один экземпляр сканирующего ядра всегда будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD и доступен клиентам через Unix-сокет. Экземпляры сканирующего ядра, запускаемые непосредственно из командной строки, будут работать в автономном режиме, без подключения к демону управления конфигурацией, даже если он запущен. Для управления параметрами работы компонента, а также для проверки файлов по требованию используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для сканирования произвольного файла или каталога компонентом Dr.Web Scanning Engine используйте команду `rawscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl rawscan <путь к каталогу или файлу>
```

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-se`.

9.10.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ScanEngine]` объединенного конфигурационного файла Dr.Web Server Security Suite.

Эта секция хранит следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-se` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-se`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Если задано значение параметра `FixedSocketPath`, то настройка игнорируется (компонент не завершает свою работу по истечению максимального времени простоя). Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `1h`

`FixedSocketPath`
{путь к файлу}
	Путь к файлу Unix-сокета фиксированного экземпляра сканирующего ядра Dr.Web Scanning Engine.
	При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр сканирующего ядра, доступный клиентам через этот сокет.
	⚠ Убедитесь, что каталогу с файлом сокета назначены следующие права доступа:
	`drwxr-xr-x`
	Чтобы просмотреть права доступа, выполните команду:
	`$ ls -ld <путь к каталогу>`
	Значение по умолчанию: *(не задано)*

Параметр	Описание
`MaxForks` *{целое число}*	Максимальное разрешенное количество экземпляров дочерних сканирующих процессов, порождаемых сканирующим ядром Dr.Web Scanning Engine, которые могут быть запущены одновременно. Значение по умолчанию: *Автоматически определяется при старте* как удвоенное число доступных процессорных ядер, или `4`, если полученное число меньше 4.
`ForkMemoryLimit` *{целое число}*	Максимальный объем оперативной памяти, выделяемый для работы экземпляра сканирующего ядра. Значение указывается как целое число с суффиксом (*b, kb, mb, gb*). Если суффикс не указан, то значение интерпретируется как размер в байтах. Допустимые значения: от 1 гигабайта (`1GB`) до 4 гигабайт (`4GB`). Значение по умолчанию: `4GB` ⚠ Этот параметр не задействуется в 32-разрядных дистрибутивах Dr.Web Server Security Suite.
`EngineDallocLimit` *{целое число}*	Максимальный объем оперативной памяти, выделяемый для хранения временных файлов. Если указанное значение меньше размера временного файла, то он будет создан на устройстве хранения, что замедлит работу Dr.Web Server Security Suite. Значение указывается как целое число с суффиксом (*b, kb, mb, gb*). Если суффикс не указан, то значение интерпретируется как размер в байтах. Допустимые значения: от 50 мегабайт (`50MB`) до 1 гигабайта (`1GB`). Значение по умолчанию: `500MB` ⚠ Настоятельно не рекомендуется менять значение по умолчанию для этого параметра, если вы не уверены, что это действительно необходимо.
`WatchdogInterval` *{интервал времени}*	Периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность порожденных им дочерних сканирующих процессов для обнаружения зависаний при проверке («сторожевой таймер»). Значение по умолчанию: `15s`
`BufferedIo` *{логическое значение}*	Использовать или не использовать буферизованный ввод-вывод при проверке файлов.

Параметр	Описание
	Использование буферизованного ввода-вывода в ОС семейства GNU/Linux и ОС FreeBSD может увеличить скорость проверки файлов, расположенных на медленных дисковых устройствах. Возможные значения: • `On`, `Yes`, `True` — использовать буферизованный ввод-вывод; • `Off`, `No`, `False` — не использовать буферизованный ввод-вывод. Значение по умолчанию: `Off`
`AbortForkOnTimeout` *{логическое значение}*	Завершать или не завершать процессы сканирования при тайм-ауте, послав им сигнал SIGABRT. Возможные значения: • `On`, `Yes`, `True` — завершать процессы сканирования при тайм-ауте; • `Off`, `No`, `False` — не завершать процессы сканирования при тайм-ауте. Значение по умолчанию: `Off`

9.11. Dr.Web Updater

Компонент обновлений Dr.Web Updater предназначен для получения обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine с серверов обновлений компании «Доктор Веб».

Если Dr.Web Server Security Suite работает в режиме централизованной защиты, то в качестве источника обновлений используется сервер централизованной защиты, причем все обновления получаются с сервера через Dr.Web ES Agent, а Dr.Web Updater для загрузки обновлений не используется.

9.11.1. Принципы работы

Компонент подключается к серверам обновлений компании «Доктор Веб» для проверки наличия и загрузки обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine. Списки серверов, образующих доступную зону обновлений, хранятся в специальном файле, который подписан с целью невозможности его модификации. При подключении к серверам обновлений через прокси-сервер поддерживается только базовая и дайджест-аутентификация.

Если Dr.Web Server Security Suite не подключен к серверу централизованной защиты или подключен к нему в мобильном режиме, то Dr.Web Updater автоматически запускается демоном управления конфигурацией Dr.Web ConfigD с периодичностью, указанной в настройках. Также компонент может быть запущен Dr.Web ConfigD в ответ на поступившую команду пользователя (внеочередное обновление).

При наличии на серверах обновлений доступных обновлений, они загружаются в каталог `/var/opt/drweb.com/cache/` для GNU/Linux или `/var/drweb.com/cache/` для FreeBSD, после чего размещаются в рабочих каталогах Dr.Web Server Security Suite.

По умолчанию все обновления загружаются с зоны обновления, общей для всех продуктов Dr.Web. Перечень используемых по умолчанию серверов, входящих в зону обновления, указывается в файлах, находящихся в каталогах, указанных в параметрах `*DrlDir`. При необходимости по запросу клиента может быть создана особая зона обновления (для каждого вида обновления), список серверов которой указывается в отдельном файле (по умолчанию с именем `update.drl`). Этот файл находится в каталоге, указанном в соответствующем параметре `*CustomDrlDir`. В этом случае компонент обновлений будет загружать обновления только с этих серверов, не используя серверы из зоны по умолчанию.

Для отказа от использования особой зоны обновления достаточно очистить значение соответствующего параметра `*CustomDrlDir` в настройках компонента.

Содержимое файлов списков серверов подписано для невозможности их модификации. Если вам необходимо создать особый перечень серверов обновления, обратитесь в техническую поддержку.

Компонент может выполнять сохранение резервных копий обновляемых файлов для последующего отката обновлений по команде пользователя. Место сохранения резервных копий и глубина хранимой истории обновлений задаются в настройках компонента. Откат обновлений выполняется через утилиту управления Dr.Web Server Security Suite из командной строки Dr.Web Ctl (запускается командой `drweb-ctl`).

9.11.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web Updater из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-update [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-update [<параметры>]
```

Dr.Web Updater допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-update --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Updater.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается демоном управления конфигурацией Dr.Web ConfigD автоматически, по мере необходимости. Для управления параметрами работы компонента, а также для обновления вирусных баз и антивирусного ядра по

требованию пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-update`.

9.11.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[Update]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, то используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-update` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-update`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу.

Параметр	Описание
	Компонент запускается при очередном обновлении по расписанию. По окончании обновления ждет указанный интервал времени, и, если новых запросов не поступает, то завершает свою работу до следующей попытки обновления. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `10m`
`Start` *{логический}*	Запускать или не запускать компонент при загрузке Dr.Web Server Security Suite. Этот параметр имеет приоритет над параметром `DwsUpdateEnabled`. Допустимые значения: • `Yes` — запускать компонент при загрузке Dr.Web Server Security Suite; • `No` — не запускать компонент при загрузке Dr.Web Server Security Suite. Значение по умолчанию: `Yes`
`UpdateInterval` *{интервал времени}*	Частота проверки наличия обновлений на серверах обновления Dr.Web, т. е. период времени, который должен пройти от предыдущей успешной попытки подключения к серверам обновления (автоматического или инициированного пользователем) до следующей попытки выполнить обновление. Значение по умолчанию: `30m`
`NetworkTimeout` *{интервал времени}*	Тайм-аут на сетевые операции компонента при выполнении обновлений с серверов Dr.Web. Используется для ожидания продолжения обновления в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то обновление будет продолжено. Не имеет смысла указывать величину тайм-аута более `75s`, т. к. за это время соединение закроется по тайм-ауту TCP. Минимальное значение: `5s`. Значение по умолчанию: `60s`
`RetryInterval` *{интервал времени}*	Частота повторных попыток выполнить обновление с серверов обновления, если очередная попытка выполнить обновление завершилось неудачей. Допустимые значения: от 1 минуты (`1m`) до 30 минут (`30m`).

Параметр	Описание
	Значение по умолчанию: `3m`
`MaxRetries` *{целое число}*	Количество повторных попыток выполнить обновление с серверов обновления Dr.Web (предпринимаемых через промежутки времени, указанные в параметре `RetryInterval`), если предыдущая попытка обновления закончилась неудачей. Если значение параметра — `0`, то повторные попытки выполнить неудавшееся обновление не производятся (следующее обновление будет производиться через период времени, указанный в параметре `UpdateInterval`). Значение по умолчанию: `3`
`UseHttps` *{Always | ResListOnly | Never}*	Использовать или не использовать протокол HTTPS при скачивании обновлений. Допустимые значения: • `Always` — всегда использовать протокол HTTPS при скачивании обновлений. • `ResListOnly` — использовать протокол HTTPS только при скачивании файла `.lst` со списком файлов обновления. Сами файлы обновления будут скачиваться по протоколу HTTP. • `Never` — всегда использовать протокол HTTP при скачивании обновлений. Значение по умолчанию: `ResListOnly`
`Proxy` *{строка подключения}*	Параметры подключения к прокси-серверу, который используется компонентом обновлений Dr.Web Updater для подключения к серверам обновлений Dr.Web (например, если непосредственное подключение к внешним серверам запрещено политиками безопасности сети). Если значение параметра не задано, то прокси-сервер не используется. Возможные значения: <*строка подключения*> — строка подключения к прокси-серверу. Имеет следующий формат (URL): `[`<*протокол*>`://][`<*пользователь*>`:`<*пароль*>`@]` <*хост*>`:`<*порт*> где: • <*протокол*> — тип используемого протокола (в текущей версии доступен только `http`); • <*пользователь*> — имя пользователя для подключения к прокси-серверу; • <*пароль*> — пароль для подключения к прокси-серверу;

Параметр	Описание

	• <*хост*> — адрес узла, на котором работает прокси-сервер (IP-адрес или имя домена, т. е. FQDN);
	• <*порт*> — используемый порт.
	Части URL <*протокол*> и <*пользователь*>:<*пароль*> могут отсутствовать. Адрес прокси-сервера <*хост*>:<*порт*> является обязательным.
	Если имя пользователя или пароль содержат символы `@`, `%` или `:`, то их следует заменить на соответствующие HEX-коды: `%40`, `%25` и `%3A` соответственно.
	Примеры:
	1. В файле конфигурации:
	• Подключение к прокси-серверу на узле `proxyhost.company.org` на порт `123`:
	`Proxy = proxyhost.company.org:123`
	• Подключение к прокси-серверу на узле `10.26.127.0` на порт `3336`, используя протокол HTTP, от имени пользователя `legaluser` с паролем `passw`:
	`Proxy = http://legaluser:passw@10.26.127.0:3336`
	• Подключение к прокси-серверу на узле `10.26.127.0` на порт `3336` от имени пользователя `user@company.com` с паролем `passw%123`:
	`Proxy = user%40company.com:passw%25123%3A@10.26.127.0:3336`
	2. Задание тех же самых значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset Update.Proxy proxyhost.company.org:123`
	`# drweb-ctl cfset Update.Proxy http://legaluser:passw@10.26.127.0:3336`
	`# drweb-ctl cfset Update.Proxy user%40company.com:passw%25123%3A@10.26.127.0:3336`
	Значение по умолчанию: *(не задано)*

`ExcludedFiles` *{имя файла}*	Имя файла, который не будет обновляться компонентом обновлений Dr.Web Updater. Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список файлы `123.vdb` и `456.dws`.

Параметр	Описание

	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[Update]`
	`ExcludedFiles = "123.vdb", "456.dws"`
	• Две строки (по одному значению в строке):
	`[Update]`
	`ExcludedFiles = 123.vdb`
	`ExcludedFiles = 456.dws`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset Update.ExcludedFiles -a 123.vdb`
	`# drweb-ctl cfset Update.ExcludedFiles -a 456.dws`
	Значение по умолчанию: `drweb32.lst`

`BaseUpdateEnabled` *{логический}*	Разрешить или запретить обновление вирусных баз и антивирусного ядра. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`
`BaseDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам из стандартной зоны обновления, используемым для обновления вирусных баз и антивирусного ядра. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/drl/bases` • для FreeBSD: `/var/drweb.com/drl/bases`
`BaseCustomDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам особой («клиентской») зоны обновления, используемым для обновления вирусных баз и антивирусного ядра. Если в каталоге, на который указывает параметр, имеется непустой подписанный файл списка серверов (файл `.drl`), то обновление ведется только с этих серверов, а серверы основной зоны (см. выше) не используются для обновления вирусных баз и антивирусного ядра. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/custom-drl/bases` • для FreeBSD: `/var/drweb.com/custom-drl/bases`

Параметр	Описание
`VersionUpdateEnabled` *{логический}*	Разрешить или запретить обновление версий компонентов Dr.Web Server Security Suite. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`
`VersionDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам, используемым для обновления версий компонентов Dr.Web Server Security Suite. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/drl/version` • для FreeBSD: `/var/drweb.com/drl/version`
`BackupDir` *{путь к каталогу}*	Путь к каталогу, в который сохраняются старые версии обновляемых файлов для возможности отката обновлений. При каждом обновлении сохраняются резервные копии только обновленных файлов. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/backup` • для FreeBSD: `/var/drweb.com/backup`
`MaxBackups` *{целое число}*	Максимальное количество сохраняемых предыдущих версий обновляемых файлов. При превышении этой величины самая старая копия удаляется при очередном обновлении. Если значение параметра — `0`, то предыдущие версии файлов для восстановления не сохраняются. Значение по умолчанию: `0`

9.12. Dr.Web ES Agent

Агент централизованной защиты Dr.Web ES Agent предназначен для подключения Dr.Web Server Security Suite к серверу централизованной защиты.

Когда Dr.Web Server Security Suite подключен к серверу централизованной защиты, Dr.Web ES Agent синхронизирует лицензионный ключевой файл с ключами, хранящимися на сервере централизованной защиты. Кроме того, Dr.Web ES Agent передает на сервер централизованной защиты, к которому он подключен, статистику инцидентов, связанных с вредоносным ПО, перечень запущенных компонентов и их состояние.

Также Dr.Web ES Agent выполняет обновление вирусных баз Dr.Web Server Security Suite непосредственно с подключенного сервера централизованной защиты, минуя компонент обновления Dr.Web Updater.

9.12.1. Принципы работы

Компонент Dr.Web ES Agent осуществляет подключение к серверу централизованной защиты, который позволяет администратору сети реализовать на всем пространстве сети единую политику безопасности, в частности, настроить на всех рабочих станциях и серверах сети одинаковые стратегии проверки файлов и других объектов файловой системы и реакции на обнаруженные угрозы. Кроме того, сервер централизованной защиты выполняет в рамках защищаемой сети функции внутреннего сервера обновлений, играя роль хранилища актуальных вирусных баз (обновление в этом случае производится через Dr.Web ES Agent, Dr.Web Updater не используется).

При подключении Dr.Web ES Agent к серверу централизованной защиты агент обеспечивает прием от сервера актуальной версии настроек программных компонентов и лицензионного ключевого файла, которые он передает демону управления конфигурацией Dr.Web ConfigD для применения к управляемым компонентам. Кроме того, он может принимать от сервера централизованной защиты задания на проверку объектов файловой системы на рабочей станции (в том числе по расписанию).

Dr.Web ES Agent собирает и отправляет на сервер, к которому он подключен, статистику обнаружения различных угроз и примененных действий.

Для подключения Dr.Web ES Agent к серверу централизованной защиты требуется иметь пароль и идентификатор узла («рабочей станции» в терминах сервера централизованной защиты), а также файл публичного ключа шифрования, используемого сервером для подтверждения его подлинности. Вместо идентификатора станции можно указать при подключении идентификатор основной и тарифной групп, в которые станцию необходимо включить на сервере. Требуемые идентификаторы и файл публичного ключа можно получить у администратора, управляющего антивирусной защитой сети через сервер централизованной защиты.

Кроме того, к серверу централизованной защиты можно подключить защищаемый узел («рабочую станцию») в режиме «новичок», если данная возможность разрешена сервером централизованной защиты. В этом случае после того, как администратор подтвердит заявку на подключение станции, сервер централизованной защиты автоматически сгенерирует для узла новые идентификатор и пароль и отправит их агенту для использования при последующих подключениях.

9.12.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web ES Agent из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-esagent [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-esagent [<параметры>]
```

Dr.Web ES Agent допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-esagent --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web ES Agent.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически, при старте операционной системы, демоном управления конфигурацией Dr.Web ConfigD. Для управления параметрами работы компонента, а также для подключения Dr.Web Server Security Suite к серверу централизованной защиты используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-esagent`.

9.12.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ESAgent]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-esagent` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-esagent`
`MobileMode` *{On | Off | Auto}*	Использовать или не использовать мобильный режим Dr.Web Server Security Suite при подключении к серверу централизованной защиты. Допустимые значения: • `On` — использовать мобильный режим, если он разрешен сервером централизованной защиты (устанавливать обновления с серверов обновлений компании «Доктор Веб» с помощью Dr.Web Updater); • `Off` — не использовать мобильный режим, оставаться в режиме централизованной защиты (всегда получать обновления только с сервера централизованной защиты); • `Auto` — использовать мобильный режим, если он разрешен сервером централизованной защиты, а обновления устанавливать как с серверов обновлений компании «Доктор Веб» с помощью Dr.Web Updater, так и с сервера централизованной защиты, в зависимости от того, какое соединение доступно и качество какого соединения лучше.

Параметр	Описание
	 Поведение данного параметра зависит от разрешений на сервере: если мобильный режим на используемом сервере не разрешен, то параметр не имеет никакого эффекта. Значение по умолчанию: `Auto`
`Discovery` *{On | Off}*	Разрешить или запретить агенту принимать *discovery*-запросы от инспектора сети, встроенного в сервер централизованной защиты (*discovery*-запросы используются инспектором для проверки структуры и состояния антивирусной сети). Допустимые значения: • `On` — разрешать агенту принимать и обрабатывать *discovery*-запросы; • `Off` — запретить агенту принимать и обрабатывать *discovery*-запросы.  Данный параметр имеет приоритет над настройками сервера централизованной защиты: если указано значение `Off`, агент не будет принимать discovery-запросы, даже если эта функция включена на сервере. Значение по умолчанию: `On`
`UpdatePlatform` *{название платформы}*	Обозначение платформы, для которой агент будет получать с сервера централизованной защиты обновления для антивирусного ядра. Допустимые значения: • для GNU/Linux: `unix-linux-32`, `unix-linux-64-engine64`, `unix-linux-aarch64`, `unix-linux-e2k`, `unix-linux-e2k-engine64`, `unix-linux-mips`, `unix-linux-ppc64le`; • для FreeBSD: `unix-freebsd-32`, `unix-freebsd-64-engine64`; • для Darwin: `unix-darwin-32`, `unix-darwin-64-engine64`, `unix-darwin-aarch64`.  Настоятельно не рекомендуется изменять значение параметра, если вы не уверены, что это действительно необходимо. Значение по умолчанию: *Зависит от используемой платформы*
`DebugIpc` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC (взаимодействие Dr.Web ES Agent и демона управления конфигурацией Dr.Web ConfigD). Значение по умолчанию: `No`

Параметр	Описание
`DebugConfig` *{логический}*	Добавлять или не добавлять в журнал информацию о настройках, полученных от сервера централизованной защиты. Значение по умолчанию: `No`
`SrvMsgAutoremove` *{целое число}*	Срок хранения сообщений. По завершении указанного срока сообщения удаляются из базы. Допустимые значения: от 1 недели (`1w`) до 365 дней (`365d`). Значение параметра указывается в виде целого числа с суффиксом `s`, `m`, `h`, `d`, `w`. Значение по умолчанию: `1w`

9.13. Dr.Web HTTPD

Компонент Dr.Web HTTPD обеспечивает инфраструктуру для локального или удаленного взаимодействия с Dr.Web Server Security Suite посредством протокола HTTP (например, через веб-браузер).

Помимо управления Dr.Web Server Security Suite через веб-интерфейс Dr.Web, вы можете использовать непосредственно командный интерфейс (HTTP API) Dr.Web HTTPD для взаимодействия с компонентами Dr.Web Server Security Suite по протоколу HTTPS. Данная возможность позволяет разработать для Dr.Web Server Security Suite собственный управляющий интерфейс.

HTTP API Dr.Web HTTPD описан в соответствующем разделе.

При использовании защищенного соединения HTTPS необходимо обеспечить сервер Dr.Web HTTPD корректным сертификатом и закрытым ключом SSL. По умолчанию для Dr.Web HTTPD серверный сертификат и закрытый ключ SSL генерируются автоматически, в процессе установки, но при необходимости вы можете сгенерировать для сервера собственную пару сертификат/ключ. Также персональный удостоверяющий сертификат пользователя, подписанный доверенным для Dr.Web HTTPD сертификатом удостоверяющего центра, может использоваться для автоматической авторизации клиентов при обращении к Dr.Web HTTPD.

Для генерации ключей и сертификатов можно воспользоваться утилитой `openssl`. Примеры использования утилиты `openssl` для генерации сертификатов и закрытых ключей приведены в разделе Приложение Д. Генерация сертификатов SSL.

9.13.1. Принципы работы

Dr.Web HTTPD представляет собой веб-сервер, специально разработанный для управления работой Dr.Web Server Security Suite, позволяя тем самым не использовать для этих целей как сторонние веб-серверы (такие как Apache HTTP Server и Nginx), так и управляющие сервисы наподобие Webmin. Более того, он может работать с ними на одном узле, не препятствуя их функционированию.

Сервер Dr.Web HTTPD обслуживает запросы, поступающие по протоколам HTTP и HTTPS на сокеты, заданные в его настройках, что позволяет ему не конфликтовать с другими веб-серверами, если они также используются на этом узле. Для управления Dr.Web Server Security Suite используется безопасный протокол HTTPS.



Веб-интерфейс управления Dr.Web не является обязательным для функционирования Dr.Web Server Security Suite и может отсутствовать, поэтому соответствующий блок на схеме обведен пунктирной границей.

Компонент Dr.Web HTTPD формирует управляющие команды к демону управления конфигурацией Dr.Web ConfigD, компоненту проверки файлов Dr.Web File Checker и другим компонентам на основании команд, полученных через HTTP API.

Описание веб-интерфейса управления, использующего Dr.Web HTTPD, приведено в соответствующем разделе.

Если веб-интерфейс управления Dr.Web не включен в состав Dr.Web Server Security Suite, вы можете подключить к продукту любой сторонний интерфейс управления, использующий HTTP API (описан в разделе Описание HTTP API) компонента Dr.Web HTTPD.

9.13.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web HTTPD из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-httpd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-httpd [<параметры>]
```

Dr.Web HTTPD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-httpd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web HTTPD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости (обычно при загрузке

операционной системы). Если компонент запущен, то для управления работой компонентов Dr.Web Server Security Suite достаточно выполнить HTTPS-подключение к одному из адресов, обслуживающих функционирование веб-интерфейса, при помощи любого стандартного браузера. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-httpd`.

9.13.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[HTTPD]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-httpd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-httpd`
`Start` *{логический}*	Запустить или остановить компонент с помощью демона конфигурации Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: *Зависит от того, установлен ли веб-интерфейс управления*

Параметр	Описание
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`

`AdminListen`
 	
{адрес, ...}
	Список сетевых сокетов (каждый сокет определяется парой *<IP-адрес>:<порт>*), прослушиваемых Dr.Web HTTPD в ожидании подключений по HTTPS от клиентов с административными полномочиями. Используется как для подключения к веб-интерфейсу управления, так и для доступа к HTTP API.
	
	Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	
	Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678.
	
	1. Добавление значений в конфигурационный файл.
	• Два значения в одной строке:
	`[HTTPD]`
	`AdminListen = "192.168.0.1:1234", "10.20.30.45:5678"`
	• Две строки (по одному значению в строке):
	`[HTTPD]`
	`AdminListen = 192.168.0.1:1234`
	`AdminListen = 10.20.30.45:5678`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset HTTPD.AdminListen -a 192.168.0.1:1234`
	`# drweb-ctl cfset HTTPD.AdminListen -a 10.20.30.45:5678`
	
	Если не указано ни одного значения, то использование HTTP API и веб-интерфейса управления невозможно.
	
	Значение по умолчанию: `127.0.0.1:4443`

`AdminSslCertificate` *{путь к файлу}*	Путь к файлу серверного сертификата, используемого сервером веб-интерфейса управления для взаимодействия с клиентами, подключающимися к административному сокету по протоколу HTTPS. Файл сертификата генерируется автоматически при установке компонента.

Параметр	Описание
	Файл сертификата и файл закрытого ключа (определяется параметром `AdminSslKey`) должны соответствовать друг другу. Значение по умолчанию: • для GNU/Linux: `/etc/opt/drweb.com/certs/serv.crt` • для FreeBSD: `/usr/local/etc/drweb.com/certs/serv.crt`
`AdminSslKey` *{путь к файлу}*	Путь к файлу закрытого ключа, используемого сервером веб-интерфейса управления для взаимодействия с клиентами, подключающимися к административному сокету по протоколу HTTPS. Файл закрытого ключа генерируется автоматически при установке компонента. Файл сертификата (определяется параметром `AdminSslCertificate`) и файл закрытого ключа должны соответствовать друг другу. Значение по умолчанию: • для GNU/Linux: `/etc/opt/drweb.com/certs/serv.key` • для FreeBSD: `/usr/local/etc/drweb.com/certs/serv.key`
`AdminSslCA` *{путь к файлу}*	Путь к файлу сертификата доверенного центра сертификации для сертификатов, используемых клиентами, подключающимися к административному сокету по протоколу HTTPS. Если сертификат клиента подписан указанным здесь сертификатом, то для клиента не производится аутентификация указанием пары логин-пароль. Более того, этот метод аутентификации запрещается для клиентов, использующих сертификаты, подписанные этим сертификатом. Клиент, прошедший аутентификацию при помощи сертификата, всегда считается суперпользователем (*root*). Значение по умолчанию: *(не задано)*
`PublicListen` *{адрес, ...}*	Список сетевых сокетов (каждый сокет определяется парой *<IP-адрес>:<порт>*), прослушиваемых Dr.Web HTTPD в ожидании подключений по HTTP от клиентов с ограниченными полномочиями. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список). Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678. 1. Добавление значений в конфигурационный файл.

Параметр	Описание

	• Два значения в одной строке:
	`[HTTPD]`
	`PublicListen = "192.168.0.1:1234", "10.20.30.45:5678"`
	• Две строки (по одному значению в строке):
	`[HTTPD]`
	`PublicListen = 192.168.0.1:1234`
	`PublicListen = 10.20.30.45:5678`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset HTTPD.PublicListen -a 192.168.0.1:1234`
	`# drweb-ctl cfset HTTPD.PublicListen -a 10.20.30.45:5678`
	Подключиться к HTTP API с полным набором команд и веб-интерфейсу управления, используя данные адреса, невозможно.
	Значение по умолчанию: *(не задано)*

`WebconsoleRoot` *{путь к каталогу}*	Путь к каталогу с файлами веб-интерфейса управления (аналог каталога `htdocs` для Apache HTTP Server). Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/share/drweb-httpd/webconsole` • для FreeBSD: `/usr/local/libexec/drweb.com/share/drweb-httpd/webconsole`
`HelpRoot` *{путь к каталогу}*	Путь к каталогу с файлами документации, доступной через веб-интерфейс управления. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/share/doc/html` • для FreeBSD: `/usr/local/libexec/drweb.com/share/doc/html`
`AccessLogPath` *{путь к файлу}*	Путь к журналу запросов HTTP/HTTPS, поступающих от клиентов к серверу веб-интерфейса управления. Если параметр не задан, информация о запросах в журнал не сохраняется. Значение по умолчанию: *(не задано)*

9.13.4. Описание HTTP API

В этом разделе

- Общие положения
  - Формат HTTP-ответа на HTTP-запрос
  - Кодировка строк объектов JSON
  - Общие ограничения на передачу данных

- Авторизация и идентификация пользователя
  - С помощью логина и пароля (SCS)
  - Авторизация по личному сертификату
- Управление Dr.Web Server Security Suite
- Проверка объектов
- Управление списком угроз
- Управление карантином
- Примеры использования HTTP API

Общие положения

HTTP API представляет собой инструмент для интеграции Dr.Web Server Security Suite со сторонними приложениями через протокол HTTP (для обеспечения безопасности используется защищенный протокол HTTPS).

Для взаимодействия с API используется протокол HTTP версии 1.0. Во всех запросах используются стандартные методы протокола HTTP — `GET` и `POST`. Все данные, за исключением особо оговоренных случаев, передаются в виде JSON-объектов. При передаче JSON-объекта в теле запроса HTTP POST заголовок `Content-Type:` должен быть установлен в значение `application/json`. Для ясности примеры JSON-объектов, приведенные ниже, снабжены комментариями (начинаются с символов `//`), которые не поддерживаются форматом JSON и при вставке в код должны быть удалены.

Формат HTTP-ответа на HTTP-запрос

- В ответ на все запросы API всегда (за исключением особо оговоренных случаев) возвращает JSON-объект. В случае возникновения ошибки API возвращает JSON-объект Error.
- Если поле ответного JSON-объекта имеет тип «массив», но этот массив не содержит ни одного элемента, то в ответе сервера такое поле опускается.
- Заголовок `Content-Type:` в ответе всегда (за исключением особо оговоренных случаев) имеет значение `application/json`.
- При попытке обращения к несуществующему ресурсу в ответе возвращается JSON-объект Error, в котором поле `code` имеет значение `EC_UNEXPECTED_MESSAGE`.
- Если используется SCS (*Secure Cookie Sessions for HTTP*), то ответы содержат cookie, подтверждающие авторизацию клиента (здесь и далее — *SCS-cookie*).

Кодировка строк объектов JSON

- Строки передаются в кодировке UTF-8 (без BOM). В запросах символы вне таблицы ASCII не экранируются последовательностями типа `\uXXXX`, а передаются в кодировке UTF-8.

- В ответах объекты JSON могут содержать как символы, закодированные в UTF-8, так и экранированные последовательности `\uXXXX`.

Общие ограничения на передачу данных

- В POST-запросах, в теле которых передается JSON-объект, допустимы любые символы, разрешенные RFC 7159.
- В GET-запросах в URI могут использоваться любые символы, разрешенные RFC 1945.
- В любых других частях запроса (заголовки, тела) также могут быть использованы любые символы, разрешенные RFC 1945.

Авторизация и идентификация пользователя

Чтобы начать работу с API, клиент должен быть авторизован сервером. Предусмотрены два способа авторизации:

1. Использование SCS согласно RFC 6896.
2. Использование клиентских сертификатов SSL, удостоверенных сертификатом доверенного ЦС на стороне Dr.Web HTTPD. В этом случае клиент считается авторизованным как суперпользователь (используются клиентские сертификаты X.509).

При авторизации с использованием SCS SCS-cookie передаются в следующих HTTP-заголовках: `Cookie:` — в запросе, `Set-Cookie:` — в ответе.
При авторизации с использованием SSL-сертификатов SCS-cookie не требуются.

При авторизации по SCS работа с API начинается с отправки команды `login`. В случае успешного выполнения этой команды клиент получает SCS-cookie, подтверждающий авторизацию.
При авторизации с помощью клиентского сертификата выполнять команду `login` не требуется; при попытке ее выполнения будет возвращен JSON-объект Error.

С помощью логина и пароля (SCS)

Команды авторизации и идентификации клиента:

Команда API	Описание
`login`	Действие: Выполнить авторизацию клиента по указанным имени пользователя и паролю для дальнейшей работы с HTTP API. В случае успешной аутентификации возвращается SCS-cookie. URI: `/api/10.2/login` Метод HTTP: POST

Команда API	Описание
	Входные параметры: объект AuthOptions Результат успешного исполнения: пустой объект, SCS-cookie
`logout`	Действие: Отозвать (деактивировать) выданный ранее SCS-cookie. В ответе на запрос с отозванным SCS-cookie будет возвращен объект Error с ошибкой `EC_NOT_AUTHORIZED`. URI: `/api/10.2/logout` Метод HTTP: GET Входные параметры: SCS-cookie Результат исполнения: пустой объект
`whoami`	Действие: Получить имя авторизованного пользователя. URI: `/api/10.2/whoami` Метод HTTP: GET Входные параметры: (SCS-cookie)* Результат исполнения: объект whoami, (SCS-cookie)

*) Здесь и далее SCS-cookie заключен в скобки, поскольку он необходим только при авторизации через SCS.



Команды авторизации `login` и `logout` используются только при авторизации через SCS.

Описание используемых объектов

1) `AuthOptions` — объект, содержащий логин и пароль пользователя:

```
{
 "user": <строка>, //Имя пользователя
 "password": <строка> //Пароль пользователя
}
```



Вы можете указать любого пользователя, входящего в группу администраторов (`sudoers` — в Debian и Ubuntu, `wheel` — в CentOS и Fedora, `astra-admin` — в Astra Linux, и т. п.). Если пользователь не является членом группы `sudoers`, в ответе на запрос возвращается ошибка `EC_NOT_AUTHORIZED`.

2) `whoami` — объект, содержащий имя пользователя, авторизованного для работы с HTTP API:

```
{
 "whoami":
 {
 "user": <строка> //Имя пользователя
 }
}
```

3) `Error` — объект, содержащий информацию о произошедшей ошибке:

```
{
 "error":
 {
 "code": <строка>, //Строковый код ошибки вида EC_XXX
 *"what": <строка> //Описание ошибки
 }
}
```

Символом `*` помечен необязательный параметр.



JSON-объект Error, возвращаемый командами HTTP API при ошибках обработки запросов, в поле `code` содержит не числовой код ошибки, а внутренний строковый код, использующийся компонентами Dr.Web Server Security Suite. Этот код представляет собой строку вида `EC_XXX`. Для уточнения числового кода и получения описания ошибки обратитесь к разделу Приложение Е. Описание известных ошибок).

Авторизация по личному сертификату

Этот способ авторизации предполагает использование личного удостоверяющего сертификата, подписанного сертификатом удостоверяющего центра, который указан в настройках Dr.Web HTTPD как доверенный. При авторизации по сертификату все запросы считаются выполняемыми от имени суперпользователя (пользователя *root*).

Чтобы авторизоваться по личному сертификату пользователя

1. Создайте личный сертификат, подписанный сертификатом удостоверяющего центра.
2. В настройках компонента Dr.Web HTTPD (параметр `AdminSslCA`) укажите путь к файлу сертификата удостоверяющего центра, которым подписан ваш личный сертификат.
3. При каждом подключении к Dr.Web HTTPD при установлении соединения используйте подписанный сертификат.

При необходимости обратитесь к информации в разделе Приложение Д. Генерация сертификатов SSL.

Управление Dr.Web Server Security Suite

Команды API для просмотра и изменения текущих значений параметров конфигурации:

Команда API	Описание
Команды управления конфигурацией	
`get_lexmap`	Действие: Получить значения параметров текущей конфигурации («лексическая карта» параметров). URI: `/api/10.2/get_lexmap` Метод HTTP: GET Входные параметры: (SCS-cookie) Результат успешного исполнения: объект LexMaps, (SCS-cookie)
`set_lexmap`	Действие: Установить или сбросить значения указанных параметров текущей конфигурации (переданных в виде «лексической карты» параметров). URI: `/api/10.2/set_lexmap` Метод HTTP: POST Входные параметры: (SCS-cookie), объект LexMap Результат успешного исполнения: объект SetOptionResult, (SCS-cookie)
Команды обновления	
`start_update`	Действие: Запустить обновление. URI: `/api/10.2/start_update` Метод HTTP: POST Входные параметры: (SCS-cookie) Результат успешного исполнения: объект StartUpdate, (SCS-cookie)
`stop_update`	Действие: Остановить активный процесс обновления. URI: `/api/10.2/stop_update` Метод HTTP: POST Входные параметры: (SCS-cookie) Результат успешного исполнения: пустой объект, (SCS-cookie)

Команда API	Описание
`baseinfo`	Действие: Просмотреть информацию о загруженных вирусных базах URI: `/api/10.2/baseinfo` Метод HTTP: GET Входные параметры: (SCS-cookie) Результат успешного исполнения: объект BaseInfoResult, содержащий объект VirusBaseInfo, (SCS-cookie)
Команды управления лицензией	
`install_license`	Действие: Установить указанный ключевой файл. URI: `/api/10.2/install_license` Метод HTTP: POST Входные параметры: (SCS-cookie), тело ключевого файла (или архива, содержащего ключевой файл) Результат успешного исполнения: пустой объект, (SCS-cookie)
Команды подключения к серверу централизованной защиты	
`esconnect`	Действие: Включить режим централизованной защиты. URI: `/api/10.2/esconnect` Метод HTTP: POST Входные параметры: (SCS-cookie), объект ESConnection Результат успешного исполнения: пустой объект, (SCS-cookie)
`esdisconnect`	Действие: Выключить режим централизованной защиты. URI: `/api/10.2/esdisconnect` Метод HTTP: POST Входные параметры: (SCS-cookie) Результат успешного исполнения: пустой объект, (SCS-cookie)

Конфигурация компонентов возвращается и задается в виде так называемой *лексической карты*, то есть в виде последовательности пар «параметр»/«значение». Объект LexMaps всегда содержит три вложенных объекта LexMap, содержащих следующие лексические карты:

- *active* — активные (актуальные на текущий момент) параметры;
- *hardcoded* — значения по умолчанию (применяются для параметров, значения которых не указаны или указаны некорректно);
- *master* — карта значений параметров конфигурации, заданных клиентом для использования.



Команда `get_lexmap` всегда возвращает все три набора значений параметров конфигурации для всех компонентов, которые могут присутствовать в составе Dr.Web Server Security Suite, а не только тех, которые установлены и работают.

Описание используемых объектов JSON

1) `LexMaps` — объект, содержащий активную, предопределенную и определенную пользователем лексические карты параметров:

```
{
 "active": <LexMap>, //Активные значения параметров конфигурации
 "hardcoded": <LexMap>, //Предопределенные значения параметров конфигурации
 "master": <LexMap> //Значения параметров конфигурации, заданные пользователем
}
```

   Каждое из указанных полей является объектом LexMap, который, в свою очередь, содержит массив объектов типа LexOption.

2) `LexMap` — объект, содержащий лексическую карту параметров:

```
{
 "option": [<LexOption>] //Массив опций конфигурации
}
```

3) `LexOption` — объект, содержащий параметр или секцию конфигурации (группу параметров):

```
{
 "key": <строка>, //Имя опции (параметра конфигурации или секции)
 *"value": <LexValue>, //Если данная опция является параметром
 *"map": <LexMap> //Если данная опция является секцией
}
```

   Символом `*` помечены необязательные параметры.

   Объект LexOption представляет собой секцию или параметр конфигурации Dr.Web Server Security Suite. Он обязательно содержит поле `key`, соответствующее имени секции или параметра, а также либо поле `value` (если объект — это параметр), либо поле `map` (если это секция). Секция также представляет собой объект типа LexMap, а значение параметра — объект LexValue, содержащий поле `item`, описывающее значение параметра в строковом виде.

4) `LexValue` — объект, содержащий массив значений параметра:

```
{
 "item": [<строка>] //Массив значений параметра
}
```

Команда `set_lexmap` принимает на вход объект LexMap, который должен содержать те параметры, значения которых необходимо заменить на новые или сбросить в значения по умолчанию. Параметры, которые следует сбросить в значения по умолчанию, не должны содержать поля `value`. Параметры, не упомянутые в лексической карте, переданной команде `set_lexmap`, останутся без изменений. В результате исполнения команда `set_lexmap` возвращает объект SetOptionResult, содержащий измененные значения каждого из указанных в команде параметров.

5) `SetOptionResult` — объект, поле `item` которого содержит массив с измененными значениями параметров:

```
{
 "item": [<SetOptionResultItem>] //Массив результатов
}
```

Объект содержит массив объектов SetOptionResultItem, которые содержат измененные значения каждого из указанных в команде параметров.

6) `SetOptionResultItem` — объект, содержащий информацию об изменении значения параметра:

```
{
 "option": <строка>, //Имя параметра
 "result": <строка>, //Результат изменения значения (код ошибки)
 *"lower_limit": <строка>, //Нижняя допустимая граница значений
 *"upper_limit": <строка> //Верхняя допустимая граница значений
}
```

Символом `*` помечены необязательные параметры.

Поле `option` содержит в себе имя параметра, к которому применялось действие, а `result` — результат попытки изменить его значение. Если новое значение было успешно применено, поле имеет значение `EC_OK`. В случае ошибки в объекте могут присутствовать поля `lower_limit` и `upper_limit`, содержащие наибольшее и наименьшее допустимые значения параметра.

7) `StartUpdate` — объект, содержащий информацию о начатом процессе обновления:

```
{
 "start_update":
  {
    "attempt_id": <число> //Идентификатор запущенного процесса обновления
  }
}
```

8) `ESConnection` — объект, содержащий информацию о подключении к серверу централизованной защиты:

```
{
 *"server": <строка>, //<Адрес узла>:<порт> (без префикса http/https)
 "certificate": <строка>, //Ключ сервера в base64
 *"newbie": <булево значение>, //По умолчанию: false
 *"login": <строка>, //Имя пользователя
```

```
 *"password": <строка> //Пароль
}
```

Символом * помечены необязательные параметры.

Параметры login и password указываются, если newbie = true.
Перед подключением скачайте с сервера централизованной защиты файл сертификата и выполните команду:

```
$ cat certificate.pem | base64
```

Строку, полученную в результате выполнения этой команды, и нужно использовать в качестве значения параметра certificate.

9) BaseInfoResult — объект, содержащий информацию о загруженных вирусных базах:

```
{
 "vdb_base_stamp": <число>, //Временная метка базы
 "vdb_bases": [<VirusBaseInfo>] //Детальная информация о базе
}
```

10) VirusBaseInfo — объект, содержащий подробную информацию о вирусной базе:

```
{
  "path": <строка>, //Путь до файла базы
  "virus_records": <число>, //Количество записей в базе
  "version": <число>, //Версия базы
  "timestamp": <число>, //Временная метка базы
  "md5": <строка>, //MD5-хеш базы
  "load_result": <строка>, //Результат загрузки базы (в случае успешной загрузки — EC_OK)
  *"sha1": <строка> //SHA1-хеш базы
}
```

Символом * помечен необязательный параметр.

Проверка объектов

Команды API для проверки объектов:

Команда API	Описание
Проверка данных (используется вызов компонента Dr.Web Network Checker)	
scan_request	Действие: Запрос на создание подключения (*endpoint*) для проверки данных с необходимыми параметрами. URI: /api/10.2/scan_request Метод HTTP: POST Входные параметры: (SCS-cookie), объект ScanOptions Результат успешного исполнения: объект ScanEndpoint, (SCS-cookie)

Команда API	Описание
`scan_endpoint`	Действие: Запуск проверки данных (например, тела файла) на созданном подключении *endpoint*. URI: `/api/10.2/scan_endpoint/<endpoint>` Метод HTTP: POST Входные параметры: (SCS-cookie), проверяемые данные Результат успешного исполнения: объект ScanResult, (SCS-cookie)
`scan_path`	Действие: Сканирование файла или каталога, расположенного по указанному пути. URI: `/api/10.2/scan_path` Метод HTTP: POST Входные параметры: (SCS-cookie), объект ScanPathOptions Результат успешного исполнения: объект ScanPathResult, (SCS-cookie)
`scan_stat`	Действие: Получение статистики сканирования. URI: `/api/10.2/scan_stat` Метод HTTP: GET Входные параметры: (SCS-cookie), формат статистики (JSON или CSV) Результат успешного исполнения: объект ScanStat (если выбран формат JSON), (SCS-cookie) Если выбран формат CSV, в ответ на запрос будет возвращена таблица, столбцы которой соответствуют полям объекта ScanStat.

Описание используемых объектов JSON

1) `ScanOptions` — объект, содержащий параметры, используемые при создании *endpoint* для проверки файлов:

```
{
 "scan_timeout_ms": <число>, //Тайм-аут на проверку файла в мс
 "cure": <булево значение>, //Применять ли лечение к инфицированному файлу
 "heuristic_analysis": <булево значение>, //Использовать ли эвристический анализ
 "packer_max_level": <число>, //Максимальный уровень вложенности для запакованных
объектов
 "archive_max_level": <число>, //Максимальный уровень вложенности для архивов
 "mail_max_level": <число>, //Максимальный уровень вложенности для почтовых объектов
 "container_max_level": <число>, //Максимальный уровень вложенности для прочих сложных
объектов (контейнеров)
 "max_compression_ratio": <число>, //Максимальная величина коэффициента сжатия архивов
```

```
 "min_size_to_scan": <число>, //Минимальный размер объекта для сканирования
 "max_size_to_scan": <число>, //Максимальный размер объекта для сканирования
 "threat_hash": <булево значение> //Получать ли хеши обнаруженных угроз
}
```

2) `ScanPathOptions` — объект, содержащий параметры сканирования файла или каталога по указанному пути:

```
{
 "path": <строка>, //Абсолютный путь файла или каталога для сканирования
 *"exclude_path": [<строка>], //Список путей, исключенных из сканирования (можно
использовать маски)
 *"scan_timeout_ms": <число>, //Тайм-аут сканирования одного объекта
 *"archive_max_level": <число>, //Максимальный уровень вложенности для архивных
объектов
 *"packer_max_level": <число>, //Максимальный уровень вложенности для запакованных
объектов
 *"mail_max_level": <число>, //Максимальный уровень вложенности для почтовых сообщений
 *"container_max_level": <число>, //Максимальный уровень вложенности для прочих
сложных объектов (контейнеров)
 *"max_compression_ratio": <число>, //Максимальная величина коэффициента сжатия
архивов
 *"heuristic_analysis": <булево значение>, //Использовать ли эвристический анализ (по
умолчанию true)
 *"follow_symlinks": <булево значение>, //Переходить ли по символическим ссылкам
 *"min_size_to_scan": <число>, //Минимальный размер объекта для сканирования
 *"max_size_to_scan": <число>, //Максимальный размер объекта для сканирования
 *"timeout_ms": <число>, //Тайм-аут сканирования всех объектов
 *"threat_hash": <булево значение> //Возвращать ли SHA1- и SHA256-хеши угроз
}
```

Символом `*` помечены необязательные параметры.

3) `ScanPathResult` — объект, содержащий результаты сканирования файла или каталога по указанному пути:

```
{
  //ScanPathResult:
  "results": [<ScanResult>], //Результаты сканирования
  *"error": <строка> //Ошибка, если процесс завершился с ошибкой (например, по тайм-
ауту)
}
```

Символом `*` помечен необязательный параметр.

Если сканирование завершено успешно, строка `error` будет отсутствовать в ответе.

4) `ScanResult` — объект, содержащий результаты сканирования:

```
{
 //ScanResult:
 "scan_report": <ScanReport>, //Отчет о сканировании
 *"sha1": <строка>, //Хеш SHA1 угрозы
 *"sha256": <строка> //Хеш SHA256 угрозы
}
```

Символом `*` помечены необязательные параметры.

5) `ScanReport` — объект, содержащий информацию о файле с обнаруженной угрозой:

```
{
 //ScanReport:
 "object": <строка>, //Строка, имя просканированного объекта
     // Для файла: абсолютный путь, для вложенного объекта — имя файла
```

```
     // Для вызова scan_endpoint будет всегда указывать на временный файл
 *"size": <число>, //Размер объекта
 *"compressed_size": <число>, //Размер объекта в сжатом состоянии
 *"core_fingerprint": <строка>, //Отпечаток движка
 *"packer": [<строка>], //Список упаковщиков, которыми был запакован объект
 *"compression_ratio": <число>, //Коэффициент сжатия архива
 *"archive": <Archive>, //Сведения о типе архива (контейнера), если объект распознан
как таковой
 *"virus": [<Virus>], //Угрозы, обнаруженные в объекте (если найдены)
 *"item": [<ScanReport>], //Отчеты о сканировании вложенных объектов (если они были)
 *"error": <строка>, //Ошибка сканирования (если возникла)
 *"heuristic_analysis": <булево значение>, //Использовался ли эвристический анализ
(true – использовался, false – нет)
 *"cured": <булево значение>, //Вылечен ли объект (true – вылечен, false – нет)
 *"cured_by_deletion": <булево значение>, //Удален ли объект в ходе лечения (true –
удален, false – нет)
 *"new_path": <строка>, //Новый путь к объекту, переименованному в ходе лечения
 *"user_time": <число>, //Время, проведенное в пространстве пользователя
 *"system_time": <число> //Время, проведенное в системных вызовах во время
сканирования
}
```

Символом * помечены необязательные параметры.

Поля `virus` и `error` могут отсутствовать в ответе, если в ходе сканирования не было найдено никаких угроз или не произошло никаких ошибок. Для вызова `scan_endpoint` поле `scan_endpoint` всегда указывает на временный файл, созданный компонентом Dr.Web Network Checker в локальной файловой системе сервера (в этот файл помещаются данные для проверки, отправленные в теле запроса `scan_endpoint`).

6) `ScanEndpoint` — объект, содержащий информацию о созданном *endpoint* для проверки файлов:

```
{
 "endpoint": <строка> //Уникальный идентификатор созданного endpoint
}
```

Возвращенный в теле объекта идентификатор `endpoint` используется для запуска проверки файла командой `scan_endpoint` (как часть URI).

7) `VirusInfo` — объект, содержащий информацию об обнаруженной угрозе:

```
{
 "type": <строка>, //Тип выявленной угрозы
 "name": <строка>  //Название угрозы
}
```

Поле `type` (тип угрозы) — строка вида `SE_XXX`:

- `SE_KNOWN_VIRUS` — известная угроза,
- `SE_VIRUS_MODIFICATION` — модификация известной угрозы,
- `SE_UNKNOWN_VIRUS` — неизвестная угроза (подозрительный объект),
- `SE_ADWARE` — рекламная программа,
- `SE_DIALER` — программа автодозвона,
- `SE_JOKE` — программа-шутка,
- `SE_RISKWARE` — потенциально опасное ПО,

- SE_HACKTOOL — программа взлома.

8) Archive — объект, содержащий информацию об архиве, запакованных объектах, почтовых сообщениях и других контейнерах:

```
{
 "type": <строка> //Тип архива, может принимать одно из значений:
         "SE_ARCHIVE" //Архив
         "SE_MAIL" //Письмо
         "SE_CONTAINER" //Другой тип контейнера
,"name": <строка> //Формат архива
}
```

9) ScanStat — объект, содержащий статистику проверок:

```
{
 "origin": <строка>, //Приложение, по запросу которого было выполнено сканирование
 // Счетчики зараженных объектов:
 "known_virus": <число>, //Количество зараженных известными угрозами объектов
 "virus_modification": <число>, //Количество объектов, зараженных модификацией
известной угрозы
 "unknown_virus": <число>, //Количество зараженных неизвестными угрозами объектов
 "adware": <число>, //Количество объектов с SE_ADWARE
 "dialer": <число>, //Количество объектов с SE_DIALER
 "joke": <число>, //Количество объектов с SE_JOKE
 "riskware": <число>, //Количество объектов с SE_RISKWARE
 "hacktool": <число>, //Количество объектов с SE_HACKTOOL
 "cured": <число>, //Количество вылеченных объектов
 "quarantined": <число>, //Количество объектов, помещенных в карантин
 "deleted": <число> //Количество удаленных объектов
}
```

Управление списком угроз

Для управления списком угроз, обнаруженных при сканировании, доступны следующие команды HTTP API:

Команда API	Описание
threats	Действие: Получить перечень идентификаторов всех обнаруженных угроз. URI: /api/10.2/threats/ Метод HTTP: GET Входные параметры: (SCS-cookie) Результат успешного исполнения: массив идентификаторов угроз
threat_info	Действие: Получить информацию об угрозе с идентификатором <*threat ID*>. URI: /api/10.2/threat_info/<*threat ID*> Метод HTTP: GET

Команда API	Описание
	Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), объект FileThreat
`cure_threat`	Действие: Попытаться вылечить угрозу с идентификатором <*threat ID*>. URI: `/api/10.2/cure_threat/`<*threat ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`delete_threat`	Действие: Удалить файл, содержащий угрозу с идентификатором <*threat ID*>. URI: `/api/10.2/delete_threat/`<*threat ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`ignore_threat`	Действие: Проигнорировать угрозу с идентификатором <*threat ID*>. URI: `/api/10.2/ignore_threat/`<*threat ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`quarantine_threat`	Действие: Переместить в карантин угрозу с идентификатором <*threat ID*>. URI: `/api/10.2/quarantine_threat/`<*threat ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект

У каждой найденной угрозы имеется уникальный целочисленный идентификатор <*threat ID*>. Список идентификаторов всех обнаруженных угроз возвращается командой `threats`. В командах `threat_info`, `cure_threat`, `delete_threat`, `ignore_threat` и `quarantine_threat` можно использовать только идентификаторы угроз из этого списка.

Всю информацию об отдельной угрозе из списка, включая историю действий с ней, возвращает запрос `threat_info` в виде объекта FileThreat.

Описание используемых объектов JSON

1) `FileThreat` — объект, содержащий в себе следующую информацию:

```
{
 "threat_id": <число>, //Идентификатор угрозы
 "detection_time": <Unix-время>, //Дата и время обнаружения угрозы
 "report": <ScanReport>, //Отчет о проверке файла
 "stat": <FileStat>, //Информация о файле
 "origin": <строка>, //Имя компонента, обнаружившего угрозу
 "origin_pid": <число>, //PID компонента, обнаружившего угрозу
 "task_id": <число>, //Идентификатор задачи на проверку в сканирующем ядре
 "history": [<ActionResult>] //История действий с угрозой (массив)
}
```

Поле `report` содержит объект ScanReport; поле `stat` — объект FileStat, а поле `history` — массив объектов ActionResult (история действий по отношению к файлу).

2) `ScanReport` — объект, содержащий информацию о файле с обнаруженной угрозой:

```
{
 "object": <строка>, //Объект файловой системы с угрозой
 "size": <число>, //Размер файла с угрозой в байтах
 "virus": [<VirusInfo>], //Перечень сведений об обнаруженных угрозах
 *"error": <строка>, //Сообщение об ошибке
 "heuristic_analysis": <булево значение> //Использовался ли эвристический анализ (true
– использовался, false – нет)
}
```

Символом `*` помечен необязательный параметр.

Поле `virus` представляет собой массив объектов VirusInfo, содержащих информацию обо всех обнаруженных угрозах. Поле `error` присутствует, только если произошла ошибка.

3) `FileStat` — объект, содержащий статистическую информацию о файле:

```
{
 "dev": <число>, //Устройство
 "ino": <число>, //Индексный дескриптор (inode)
 *"size": <число>, //Размер файла
 *"uid": <User>, //Идентификатор пользователя-владельца
 *"gid": <Group>, //Идентификатор группы владельцев
 *"mode": <число>, //Режим доступа к файлу
 *"mtime": <Unix-время>, //Дата и время модификации файла
 *"ctime": <Unix-время>, //Дата и время создания файла
 *"rsrc_size": <число>,
 *"finder_info": <строка>,
 *"ext_finder_info": <строка>,
 *"uchg": <строка>,
 *"volume_name": <строка>, //Имя тома
 *"volume_root": <строка>, //Корень (точка монтирования) тома
 *"xattr": [<Xattr>] //Расширенная информация о файле
}
```

Символом `*` помечены необязательные параметры.

Поле `xattr` представляет собой массив объектов `Xattr`. Этот объект содержит два строковых поля `name` и `value`. Поля `uid` и `gid` представляют собой объекты `User` и `Group`, хранящие информацию о пользователе-владельце и о группе владельцев соответственно. Они содержат по два поля:

- `uid` (`gid`) — числовой идентификатор пользователя (группы);
- `username` (`groupname`) — строковое имя пользователя (группы).

4) `ActionResult` — объект, содержащий информацию о действии по отношению к файлу и его результате:

```
{
 "action": <строка>, //Применяемое действие
 "action_time": <Unix-время>, //Дата и время применения
 "result": <строка>, //Результат применения
 "cure_report": <ScanReport> //Отчет о применении действия
}
```

Команды `cure_threat`, `delete_threat`, `ignore_threat` и `quarantine_threat` возвращают пустой объект в случае успешного выполнения. Если запрошенное действие с угрозой завершилось ошибкой (например, угрозу не удалось нейтрализовать), то вместо пустого объекта будет возвращен объект Error.

Управление карантином

Для управления содержимым карантина, хранящего угрозы, доступны следующие команды HTTP API:

Команда API	Описание
`quarantine`	Действие: Получить перечень идентификаторов объектов, помещенных в карантин. URI: `/api/10.2/quarantine/` Метод HTTP: GET Входные параметры: (SCS-cookie) Результат успешного исполнения: (SCS-cookie), массив объектов QuarantineId (объектов в карантине)
`qentry_info`	Действие: Получить информацию об изолированном в карантине объекте с идентификатором *<entry ID>*. URI: `/api/10.2/qentry_info/`*<entry ID>* Метод HTTP: GET Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), объект QEntry

Команда API	Описание
`cure_qentry`	Действие: Выполнить попытку лечения объекта с идентификатором *<entry ID>*, находящегося в карантине. URI: `/api/10.2/cure_qentry/`*<entry ID>* Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`delete_qentry`	Действие: Удалить из карантина объект с идентификатором *<entry ID>*. URI: `/api/10.2/delete_qentry/`*<entry ID>* Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`restore_qentry`	Действие: Восстановить (в исходное местоположение) из карантина объект с идентификатором *<entry ID>*. URI: `/api/10.2/restore_qentry/`*<entry ID>* Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект

Команда `quarantine` возвращает массив объектов QuarantineId, в котором каждый объект содержит идентификатор объекта, находящегося в карантине. Идентификатор состоит из двух частей: `chunk_id` и `entry_id`.

Описание используемых объектов JSON

1) `QuarantineId` — объект, содержащий части составного идентификатора изолированного объекта:

```
{
 "chunk_id": <строка>,
 "entry_id": <строка>
}
```

Комбинация этих двух полей в виде *<entry_id>@<chunk_id>* представляет собой идентификатор изолированного объекта, находящегося в карантине. Этот идентификатор указывается во всех запросах на выполнение действий с любым объектом в карантине при помощи команд `qentry_info`, `cure_qentry`, `delete_qentry` и `restore_qentry`. Команда `qentry_info` используется для

получения подробной информации об изолированном объекте по его идентификатору. Она возвращает объект QEntry.

2) `QEntry` — объект, содержащий информацию об изолированном объекте:

```
{
 "entry_id": <строка>, //Части идентификатора
 *"chunk_id": <строка>, //изолированного объекта
 *"quarantine_dir": <строка>, //Каталог карантина
 "restore_path": <строка>, //Путь, куда будет восстановлен объект
 "creation_time": <Unix-время>, //Дата и время помещения в карантин
 "report": <ScanReport>, //Отчет о проверке объекта (см. ScanReport выше)
 "stat": <FileStat>, //Статистическая информация о файле (см. FileStat выше)
 *"history": [<QEntryOperation>], //История манипуляций с объектом
 *"who": <RemoteUser>, //Удаленный владелец файла (если файл был изолирован с
файлового хранилища с сетевым доступом)
 *"detection_time": <Unix-время>, //Дата и время обнаружения угрозы
 *"origin": <строка> //Компонент, обнаруживший угрозу
}
```

Символом `*` помечены необязательные параметры.

Поле `report` содержит объект ScanReport, поле `stat` — объект FileStat, а в поле `history` хранится история действий по отношению к изолированному объекту. Каждая запись о действии описывается объектом QEntryOperation. Необязательное поле `who` содержит информацию об удаленном пользователе в виде объекта RemoteUser.

3) `QEntryOperation` — объект, хранящий информацию об операции по отношению к объекту в карантине:

```
{
 "action": <строка>, //Действие, применявшееся к объекту (см. обозначения ниже)
 "action_time": <Unix-время>, //Дата и время применения действия
 "result": <строка>, //Ошибка применения действия (код вида EC_XXX)
 *"restore_path": <строка>, //Путь восстановления объекта из карантина (если action =
"QENTRY_ACTION_RESTORE")
 *"rescan_report": <ScanReport> //Отчет о повторной проверке (если action =
"QENTRY_ACTION_RESCAN")
}
```

Символом `*` помечены необязательные параметры.

Поле `action` может принимать следующие значения:

- `QENTRY_ACTION_DELETE` — попытка удаления объекта из карантина;
- `QENTRY_ACTION_RESTORE` — попытка восстановления объекта из карантина;
- `QENTRY_ACTION_RESCAN` — попытка повторной проверки объекта в карантине;
- `QENTRY_ACTION_CURE` — попытка лечения объекта в карантине.

4) `RemoteUser` — объект, содержащий информацию об удаленном пользователе-владельце файла (если файл был изолирован с сетевого хранилища):

```
{
 *"ip": <строка>, //IP-адрес пользователя
 *"user": <строка>, //Имя пользователя
 *"domain": <строка> //Домен пользователя
}
```

Символом `*` помечены необязательные параметры.

Команды `cure_qentry`, `delete_qentry` и `restore_qentry` возвращают пустой объект в случае успешного выполнения. Если выполнение команды завершилось ошибкой, в ответе возвращается объект Error.

Примеры использования HTTP API

Для проверки работы HTTP API можно воспользоваться утилитой `curl`. Структуру и формат запроса можно представить следующим образом:

```
$ curl https://<HTTPD.AdminListen>/<HTTP API URI> -k -X <метод HTTP>
 [-H 'Content-Type: application/json' --data-binary '@<файл JSON-объекта>']
 [-c <cookie-файл> [-b <cookie-файл>]] [> <файл результата>]
```

- опция `-k` указывает, что `curl` может не проверять корректность используемого SSL-сертификата;
- опция `-X` используется для указания используемого метода HTTP (GET или POST);
- опция `-H` используется для добавления заголовка `Content-Type: application/json`;
- опция `--data-binary` (или `-d`) используется для присоединения к телу запроса JSON-объекта, взятого из текстового файла;
- если для авторизации используется SCS, файлы, содержащие передаваемый и принимаемый SCS-cookie, указываются в параметрах `-b` и `-c` соответственно.

Подробную информацию об опциях утилиты `curl` можно получить с помощью команд `curl --help` и `man curl`.

1. **Авторизовать клиента** с указанием имени пользователя и пароля (для SCS).

   В файл `user.json` предварительно должен быть записан объект AuthOptions в формате JSON, например:

   ```
   {"user":"<username>","password":"<passphrase>"}
   ```

   Запрос:

   ```
   $ curl https://127.0.0.1:4443/api/10.2/login -k -X POST -H 'Content-Type:
   application/json' --data-binary '@user.json' -c cookie.file
   ```

   Ответ:

   ```
   HTTP/1.0 200 OK
   Content-Type: application/json
   Content-Length: 2
   Set-Cookie: DWToken=6QXy4wn_JGov9A1GohWP_kvMK3dN6ccKegjNgKcmHpb_AqSrHg9cNX_yFJhxPDgr|
   MTQ2Mjg3Mzg4NQ==|cWd4Ow==|GywBUVOhU4w2LF_BKT5frg==|kR_rip5nrpxWjJ2dfZ7Xfmvi3rE=;
   Secure; HttpOnly; Max-Age: 900; Path=/
   Pragma: no-cache

   {}
   ```

Заголовок `Set-Cookie` содержит SCS-cookie, который нужно использовать во всех последующих запросах к HTTP API. В теле объекта в случае успешной аутентификации возвращается пустой объект. Если пользователь не авторизован, возвращается объект Error:

```
HTTP/1.0 403 Forbidden
Content-Type: application/json
Content-Length: 35
Pragma: no-cache

{"error":{"code":"EC_AUTH_FAILED"}}
```

2. **Получить информацию об угрозе** с *ID = 1*:

   Запрос:

   ```
   $ curl https://127.0.0.1:4443/api/10.2/threat_info/1 -k -X GET -c cookie.file -b
   cookie.file
   ```

   Ответ:

   ```
   HTTP/1.0 200 OK
   Content-Type: application/json
   Content-Length: 574
   Set-Cookie: DWToken=<…>;
    Secure; HttpOnly; Max-Age: 900; Path=/
   Pragma: no-cache

   {"threat_id":1,"detection_time":1462881660,
   "report":{"object":"/sites/site1/eicar.com.txt","size":68,"packer":[],
   "virus":[{"type":"SE_KNOWN_VIRUS","name":"EICAR Test File (NOT a Virus!)"}],
   "heuristic_analysis":true,"core_fingerprint":"0D2DD5A869DAB7AE354153A4D5F70F45",
   "item":[],"log":[],"user_time":0,"system_time":0},"stat":{"dev":2049,"ino":898,
   "size":68,"uid":{"uid":1000,"username":"user"},"gid":{"gid":1000,"groupname":"user"},
   "mode":33204,"mtime":1441028214,"ctime":1460738554,"xattr":[]},
   "origin":"APP_COMMAND_LINE_TOOL","origin_pid":2726,"task_id":1,"history":[]}
   ```

3. **Переместить в карантин** угрозу с *ID = 1*:

   Запрос:

   ```
   $ curl -v -c cookie.jar -b cookie.jar -k -X POST -H 'Content-Type:application/json'
   https://127.0.0.1:4443/api/10.2/quarantine_threat/1
   ```

   Ответ:

   ```
   HTTP/1.0 200 OK
   Content-Type: application/json
   Content-Length: 2
   Set-Cookie: DWToken=<…>; Secure; HttpOnly; Max-Age: 900; Path=/
   Pragma: no-cache

   {}
   ```

4. **Просмотреть информацию об изолированном объекте**:

   Запрос:

   ```
   $ curl -v -k -X GET -c cookie.jar -b cookie.jar
   https://127.0.0.1:4443/api/10.2/qentry_info/3070d3ce-7b6e-4143-9d9f-
   89ba3473a781@801:2108d
   ```

Ответ:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 781
Set-Cookie: DWToken=<…>; Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{"entry_id":"3070d3ce-7b6e-4143-9d9f-89ba3473a781","chunk_id":"3830313A3231303864",
"quarantine_dir":"2F686F6D652F757365722F2E636F6D2E64727765622E71756172616E74696E65",
"restore_path":"2E2E2F7473742F65696361722E636F6D2E747874","creation_time":1462888884,
"report":{"object":"/home/user/tst/eicar.com.txt","size":68,"packer":[],
"virus":[{"type":"SE_KNOWN_VIRUS","name":"EICAR Test File (NOT a Virus!)"}],
"heuristic_analysis":true,"core_fingerprint":"467CD4C6D423C55448B71CD5B8152776",
"item":[],"log":[],"user_time":0,"system_time":0},"stat":{"dev":2049,"ino":898,
"size":68,"uid":{"uid":1000,"username":"user"},"gid":{"gid":1000,"groupname":"user"},
"mode":33204,"mtime":1441028214,"ctime":1462888421,"xattr":[]},"history":[],
"detection_time":1462888667,"origin":"APP_COMMAND_LINE_TOOL"}
```

5. **Изменить настройки:** выключить Dr.Web CloudD.

   В файл `lexmap_ls_off.json` предварительно должен быть записан объект LexMap в формате JSON:

   ```
   {"option":[{"key":"Root","map":{"option":
   [{"key":"UseCloud","value":{"item":["no"]}}]}}]}
   ```

   Запрос:

   ```
   $ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type: application/json'
   --data-binary '@lexmap_ls_off.json' https://127.0.0.1:4443/api/10.2/set_lexmap
   ```

   Ответ:

   ```
   HTTP/1.0 200 OK
   Content-Type: application/json
   Content-Length: 58
   Set-Cookie: DWToken=<…>; Secure; HttpOnly; Max-Age: 900; Path=/
   Pragma: no-cache

   {"item":[{"option":"Root.UseCloud","result":"EC_OK"}]}
   ```

6. **Изменить настройки:** включить Dr.Web CloudD.

   В файл `lexmap_ls_on.json` предварительно должен быть записан объект LexMap в формате JSON:

   ```
   {"option":[{"key":"Root","map":{"option":
   [{"key":"UseCloud","value":{"item":["yes"]}}]}}]}
   ```

   Запрос:

   ```
   $ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type: application/json'
   --data-binary '@lexmap_ls_on.json' https://127.0.0.1:4443/api/10.2/set_lexmap
   ```

   Ответ:

   ```
   HTTP/1.0 200 OK
   Content-Type: application/json
   Content-Length: 58
   Set-Cookie: DWToken=<…>; Secure; HttpOnly; Max-Age: 900; Path=/
   Pragma: no-cache
   ```

```
{"item":[{"option":"Root.UseCloud","result":"EC_OK"}]}
```

9.14. Dr.Web SNMPD

Dr.Web SNMPD — это SNMP-агент, предназначенный для интеграции Dr.Web Server Security Suite с системами мониторинга, использующими протокол SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов Dr.Web Server Security Suite, а также собирать статистику обнаружения и нейтрализации угроз. Агент поддерживает предоставление системам мониторинга или любым SNMP-менеджерам следующей информации:

- Состояние любого компонента Dr.Web Server Security Suite.
- Счетчики количества обнаруженных угроз различных типов (в соответствии с классификацией Dr.Web).

Кроме того, агент может рассылать уведомления SNMP trap по факту обнаружения угроз и по факту ошибок при попытках нейтрализации обнаруженных угроз. Агент поддерживает протокол SNMP версий 2c и 3.

Описание информации, которая может быть предоставлена агентом, содержится в специально сформированном компанией «Доктор Веб» разделе MIB (*Management Information Base*). В разделе MIB, определенном для продуктов Dr.Web для Unix-подобных ОС, описывается следующая информация:

1. Форматы оповещений SNMP trap об обнаружении и нейтрализации угроз, а также об ошибках компонентов Dr.Web Server Security Suite.
2. Статистика работы Dr.Web Server Security Suite.
3. Состояние компонентов Dr.Web Server Security Suite.

Подробнее о данных, которые можно получить, используя протокол SNMP, см. в соответствующем разделе.

9.14.1. Принципы работы

В этом разделе

- Общие сведения
- Интеграция с системным SNMP-агентом

Общие сведения

По умолчанию компонент запускается автоматически при старте Dr.Web Server Security Suite. После запуска компонент формирует структуры данных в соответствии со структурой, описанной в Dr.Web SNMP MIB, и начинает ожидать поступление запросов на получение информации от внешних менеджеров SNMP. Компонент получает информацию о статусе компонентов Dr.Web Server Security Suite, а также уведомления об

обнаружении угроз непосредственно от демона управления конфигурацией Dr.Web ConfigD.

Обнаружение угроз сканирующим ядром может происходить при проверках файлов, производящихся по запросам от различных компонентов Dr.Web Server Security Suite. При обнаружении любой угрозы происходит увеличение счетчика количества обнаруженных угроз, соответствующего типу угрозы, а всем менеджерам SNMP, получающим оповещения, рассылается уведомление SNMP trap с информацией об обнаруженной угрозе.



Накопленные значения счетчиков (например, счетчиков обнаруженных угроз) не сохраняются между запусками Dr.Web SNMPD. Таким образом, при перезапуске Dr.Web SNMPD по любой причине (в том числе при общем перезапуске Dr.Web Server Security Suite) накопленные значения счетчиков сбрасываются в ноль.

Интеграция с системным SNMP-агентом

Для корректной работы SNMP-агента Dr.Web в случае, если на сервере уже работает основной системный SNMP-агент `snmpd` (`net-snmp`), необходимо настроить передачу SNMP-запросов по ветке MIB Dr.Web от `snmpd` к Dr.Web SNMPD. Для этого необходимо отредактировать конфигурационный файл `snmpd` (обычно `/etc/snmp/snmpd.conf` для GNU/Linux или `/etc/snmpd.config` для FreeBSD), добавив в него строку следующего вида:

```
proxy -v <версия> -c <community> <адрес>:<порт> <ветвь MIB>
```

Где:

- *<версия>* — используемая версия SNMP (2c, 3);
- *<community>* — «community string», используемая Dr.Web SNMPD;
- *<адрес>:<порт>* — сетевой сокет, прослушиваемый Dr.Web SNMPD;
- *<ветвь MIB>* — OID ветви дерева MIB, содержащей описания переменных и уведомлений SNMP (*trap*), используемых Dr.Web (этот OID равен `.1.3.6.1.4.1.29690`).

При использовании настроек SNMP-агента Dr.Web по умолчанию добавляемая строка имеет следующий вид:

```
proxy -v 2c -c public localhost:50000 .1.3.6.1.4.1.29690
```



Поскольку в этом случае порт 161 будет использоваться стандартным системным `snmpd`, то для Dr.Web SNMPD в параметре `ListenAddress` следует указать другой порт (`50000` в данном примере).

9.14.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web SNMPD из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-snmpd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-snmpd [<параметры>]
```

Dr.Web SNMPD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-snmpd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web SNMPD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости (обычно при загрузке операционной системы). Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-snmpd`.

9.14.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[SNMPD]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, то используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-snmpd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-snmpd`
`Start` *{логический}*	Запускать или не запускать компонент с помощью демона управления конфигурацией Dr.Web ConfigD. Если параметр имеет значение `Yes`, то демон управления конфигурацией немедленно запустит компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: `No`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`SnmpVersion` *{V2c | V3}*	Используемая версия протокола SNMP (*SNMPv2c* или *SNMPv3*).

Параметр	Описание
	Значение по умолчанию: `V2c`
`ListenAddress` *{адрес}*	Адрес (IP-адрес и порт), прослушиваемый агентом Dr.Web SNMPD в ожидании подключений от клиентов (менеджеров SNMP). Для совместной работы с `snmpd` необходимо указать порт, отличный от стандартного (`161`). Кроме того, у `snmpd` необходимо настроить проксирование. Значение по умолчанию: `127.0.0.1:161`

`TrapReceiver`
 	
{список адресов}
	Список адресов (IP-адрес и порт), на которые Dr.Web SNMPD отправляет уведомления *SNMP trap* при обнаружении угроз компонентами Dr.Web Server Security Suite.
	
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	
	Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678.
	
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[SNMPD]`
	`TrapReceiver = "192.168.0.1:1234", "10.20.30.45:5678"`
	• Две строки (по одному значению в строке):
	`[SNMPD]`
	`TrapReceiver = 192.168.0.1:1234`
	`TrapReceiver = 10.20.30.45:5678`
	2. Добавление значений с помощью команды `drweb-ctl cfset`:
	`# drweb-ctl cfset SNMPD.TrapReceiver -a 192.168.0.1:1234`
	`# drweb-ctl cfset SNMPD.TrapReceiver -a 10.20.30.45:5678`
	
	Значение по умолчанию: *(не задано)*

`V2cCommunity` *{строка}*	Строка «SNMP read community» для аутентификации менеджеров SNMP (протокол *SNMPv2c*) при доступе к переменным MIB Dr.Web для чтения.

Параметр	Описание
	Параметр используется, если задано `SnmpVersion = V2c`. Значение по умолчанию: `public`
`V3EngineId` *{строка}*	Строка-идентификатор *Engine ID* для *SNMPv3* (согласно RFC 3411). Значение по умолчанию: `800073FA044452574542`
`V3UserName` *{строка}*	Имя пользователя для аутентификации менеджеров SNMP (протокол *SNMPv3*) для доступа к переменным MIB Dr.Web. Параметр используется, если задано `SnmpVersion = V3`. Значение по умолчанию: `noAuthUser`

`V3Auth`
 	
{SHA(<pwd>) | MD5(<pwd>) | None}
	Метод аутентификации менеджеров SNMP (протокол *SNMPv3*) для доступа к переменным MIB Dr.Web.
	
	Возможные значения:
	• `SHA(<PWD>)` — используется SHA-хеш пароля (строки <*PWD*>);
	• `MD5(<PWD>)` — используется MD5-хеш пароля (строки <*PWD*>);
	• `None` — аутентификация не производится;
	
	где <*PWD*> — пароль в открытом виде (*plain text*).
	
	При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа `\`.
	
	Примеры:
	1. Значение параметра в файле конфигурации:
	`V3Auth = MD5(123456)`
	2. Задание этого же значения из командной строки с помощью команды `drweb-ctl cfset`:
	`drweb-ctl cfset SNMPD.V3Auth MD5\(123456\)`
	
	Параметр используется, если задано `SnmpVersion = V3`.
	
	Значение по умолчанию: `None`

`V3Privacy` *{DES(<secret>) | AES128(<secret>) | None}*	Метод шифрования содержимого SNMP-сообщений (протокол *SNMPv3*).

Параметр	Описание

	Возможные значения:
	• `DES(<secret>)` — используется алгоритм шифрования DES;
	• `AES128(<secret>)` — используется алгоритм шифрования AES128;
	• `None` — шифрование содержимого SNMP-сообщений не производится;
	где *<secret>* — секрет, разделяемый менеджером и агентом (*plain text*).
	При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа `\`.
	Примеры:
	1. Значение параметра в файле конфигурации:
	`V3Privacy = AES128(supersecret)`
	2. Задание этого же значения из командной строки с помощью команды `drweb-ctl cfset`:
	`drweb-ctl cfset SNMPD.V3Privacy AES128\(supersecret\)`
	Параметр используется, если задано `SnmpVersion = V3`.
	Значение по умолчанию: `None`

9.14.4. Интеграция с системами мониторинга

В этом разделе

- Интеграция с системой мониторинга Munin
  - Подключение узла к Munin
- Интеграция с системой мониторинга Zabbix
  - Подключение узла к Zabbix
  - Настройка приема уведомлений SNMP trap для Zabbix
- Интеграция с системой мониторинга Nagios
  - Подключение узла к Nagios
  - Настройка Nagios
  - Настройка приема уведомлений SNMP trap для Nagios

SNMP-агент Dr.Web может выступать поставщиком данных для любой системы мониторинга, использующей протокол SNMP версии *2c* или *3*. Перечень данных,

доступных для мониторинга, и их структура описаны в файле описания MIB Dr.Web `DRWEB-SNMPD-MIB.txt`, поставляемом совместно с Dr.Web Server Security Suite. Этот файл находится в каталоге `/opt/drweb.com/share/drweb-snmpd/mibs` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/mibs` для FreeBSD.

Для удобства настройки совместно с компонентом поставляются необходимые шаблоны настроек для популярных систем мониторинга Munin, Zabbix и Nagios.

Шаблоны настроек для систем мониторинга находятся в каталоге `/opt/drweb.com/share/drweb-snmpd/connectors` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors` для FreeBSD.

Интеграция с системой мониторинга Munin

Система мониторинга Munin состоит из централизованного сервера (мастера) munin, собирающего статистику от клиентов munin-node, располагающихся локально на узлах, подлежащих наблюдению. Каждый клиент мониторинга по запросу от сервера собирает данные о работе наблюдаемого узла, запуская *подключаемые модули* (*plug-ins*), предоставляющие данные для передачи на сервер.

Для подключения Dr.Web SNMPD к системе мониторинга Munin в каталоге `/opt/drweb.com/share/drweb-snmpd/connectors/munin/plugins` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/munin/plugins` для FreeBSD поставляются готовые подключаемые модули сбора данных Dr.Web, используемые munin-node. Эти модули собирают данные для построения следующих графиков:

- количество обнаруженных угроз;
- статистика проверки файлов.

Указанные модули поддерживают использование протокола SNMP версий 1, 2c и 3. На основе этих шаблонных модулей можно создать любые подключаемые модули, опрашивающие состояние Dr.Web Server Security Suite через Dr.Web SNMPD.

В каталоге `/opt/drweb.com/share/drweb-snmpd/connectors/munin` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/munin` для FreeBSD поставляются следующие файлы.

Файл	Описание
`plugins/snmp__drweb_malware`	Подключаемый модуль `munin-node` для опроса Dr.Web SNMPD через SNMP с целью получения количества угроз, обнаруженных Dr.Web Server Security Suite на узле.

Файл	Описание
plugins/snmp__drweb_filecheck	Подключаемый модуль munin-node для опроса Dr.Web SNMPD через SNMP с целью получения статистики проверки файлов Dr.Web Server Security Suite на узле.
plugin-conf.d/drweb.cfg	Пример конфигурации в munin-node значений переменных среды исполнения подключаемых модулей Dr.Web.

Подключение узла к Munin

В данной инструкции предполагается, что система мониторинга Munin уже корректно развернута на сервере мониторинга, а на наблюдаемом узле установлены и корректно функционируют Dr.Web SNMPD (возможно, в режиме прокси совместно с snmpd) и munin-node.

1. Настройка на наблюдаемом узле
   - Скопируйте файлы snmp__drweb_* в каталог библиотек подключаемых модулей munin-node. Этот путь зависит от используемой ОС, например, в Debian и Ubuntu это путь /usr/share/munin/plugins.
   - Настройте munin-node, подключив к нему поставляемые подключаемые модули Dr.Web. Для этого используйте утилиту munin-node-configure, которая поставляется совместно с munin-node.

     Например, команда:

     ```
     $ munin-node-configure --shell --snmp localhost
     ```

     выведет на экран терминала список команд для создания необходимых символических ссылок на подключаемые модули. Скопируйте и выполните их в командной строке. Указанная команда предполагает, что:

     1) munin-node установлена на том же узле в сети, что и Dr.Web SNMPD. Если это не так, то следует указать вместо localhost правильный FQDN или IP-адрес наблюдаемого узла.
     2) Dr.Web SNMPD использует протокол SNMP версии 2c. Если это не так, то следует указать правильную версию протокола SNMP в вызове команды munin-node-configure. Эта команда имеет набор ключей, которые позволяют гибко настроить подключаемые модули, в том числе указать используемую версию протокола SNMP, порт, используемый SNMP-агентом на наблюдаемом узле, строку *community string* и т. п. При необходимости воспользуйтесь справкой по команде munin-node-configure.
   - При необходимости определите или переопределите значения параметров среды, в которой должны исполняться установленные подключаемые модули Dr.Web для munin-node. В качестве параметров среды используется значение *community string*, используемый SNMP-агентом порт и так далее. Эти параметры необходимо

определить в файле `/etc/munin/plugin-conf.d/drweb` (создайте его при необходимости). В качестве примера данного файла используйте поставляемый файл `drweb.cfg`.

- В файле конфигурации `munin-node` (`munin-node.conf`) укажите регулярное выражение, которому должны соответствовать IP-адреса узлов сети, с которых серверам (мастерам) munin разрешено подключаться к `munin-node` на данном узле для получения значений контролируемых параметров, например:

  ```
  allow ^10\.20\.30\.40$
  ```

  В данном случае регулярное выражение разрешает получение параметров этого узла только узлу с IP-адресом `10.20.30.40`.

- Перезапустите `munin-node`, например, командой:

  ```
  # service munin-node restart
  ```

2. Настройка на сервере (мастере) Munin

   В конфигурационный файл мастера Munin (`munin.conf`), который по умолчанию хранится в каталоге `/etc` (в системах Debian и Ubuntu — `/etc/munin/munin.conf`), добавьте запись с адресом и идентификатором наблюдаемого узла:

   ```
   [<ID>;<hostname>.<domain>]
   address <host IP address>
   use_node_name yes
   ```

   где *<ID>* — отображаемый идентификатор узла; *<hostname>* — имя узла; *<domain>* — имя домена; *<host IP address>* — IP-адрес узла.

С официальной документацией по настройке системы мониторинга Munin вы можете ознакомиться по ссылке.

Интеграция с системой мониторинга Zabbix

Для подключения Dr.Web SNMPD к системе мониторинга Zabbix в каталоге `/opt/drweb.com/share/drweb-snmpd/connectors/zabbix` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/zabbix` для FreeBSD поставляются следующие файлы шаблонов:

Файл	Описание
`zbx_drweb.xml`	Шаблон описания наблюдаемого узла с установленным Dr.Web Server Security Suite.
`snmptt.drweb.zabbix.conf`	Настройки утилиты `snmptt` — приемника уведомлений *SNMP trap*.

Шаблон описания наблюдаемого узла содержит:

- Набор описаний счетчиков («*items*», в терминологии Zabbix). По умолчанию шаблон настроен на использование протокола SNMP v2.

- Набор настроенных графиков: количество проверенных файлов и распределение обнаруженных угроз по типам.

Подключение узла к Zabbix

В данной инструкции предполагается, что система мониторинга Zabbix уже корректно развернута на сервере мониторинга, а на наблюдаемом установлен и корректно функционирует Dr.Web SNMPD (возможно, в режиме прокси совместно с `snmpd`). Кроме того, если планируется получать с наблюдаемого узла оповещения *SNMP trap* (в частности, об обнаружении Dr.Web Server Security Suite угроз на защищаемом сервере), на сервере мониторинга также должен быть установлен пакет `net-snmp` (используются стандартные утилиты `snmptt` и `snmptrapd`).

1. В веб-интерфейсе Zabbix на вкладке **Configuration** → **Templates** импортируйте шаблон наблюдаемого узла из файла `/opt/drweb.com/share/drweb-snmpd/connectors/zabbix/zbx_drweb.xml` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/zabbix/zbx_drweb.xml` для FreeBSD.
2. Добавьте наблюдаемый узел в список узлов (используйте ссылку **Hosts** → **Create host**). Укажите параметры узла и корректные настройки SNMP-интерфейса (должны соответствовать настройкам `drweb-snmpd` и snmpd на узле):
   - Вкладка **Host**:

     Host name: *drweb-host*

     Visible name: *DRWEB_HOST*

     Groups: выберите *Linux servers*

     Snmp interfaces: нажмите **Add** и укажите IP-адрес и порт, используемый Dr.Web SNMPD (по умолчанию предполагается, что Dr.Web SNMPD работает на локальном узле, поэтому здесь указан адрес *127.0.0.1*, а в качестве порта указан стандартный порт *161*).
   - Вкладка **Templates**:

     Нажмите **Add**, отметьте *DRWEB*, нажмите **Select**.
   - Вкладка **Macros**:

     Macro: *{$SNMP_COMMUNITY}*

     Value: укажите *read community* для SNMP V2c (по умолчанию *public*).

     Нажмите **Save**.



Макрос *{$SNMP_COMMUNITY}* можно указать непосредственно в шаблоне узла.

По умолчанию импортированный шаблон *DRWEB* настроен на использование версии SNMP v2. Если требуется использовать другую версию SNMP, его необходимо отредактировать на соответствующей странице редактирования шаблона.

3. После привязки шаблона к наблюдаемому узлу, если настройки SNMP корректны, система мониторинга Zabbix начнет сбор данных для счетчиков (*items*), содержащихся в шаблоне. На вкладках веб-интерфейса **Monitoring** → **Latest Data** и **Monitoring** → **Graphs** будут отображаться собранные данные счетчиков.
4. Специальный элемент (*item*) *drweb-traps* служит для сбора уведомлений *SNMP trap* от Dr.Web SNMPD. Журнал полученных оповещений *SNMP trap* доступен на странице **Monitoring** → **Latest Data** → **drweb-traps** → **history**. Для сбора оповещений Zabbix использует стандартные утилиты `snmptt` и `snmptrapd` из пакета `net-snmp`. Об их настройке для получения уведомлений *SNMP trap* от Dr.Web SNMPD см. ниже.
5. В случае необходимости, вы можете настроить для добавленного наблюдаемого узла триггер, изменяющий свое состояние при получении уведомлений *SNMP trap* от Dr.Web SNMPD. Изменение состояния этого триггера можно использовать как источник событий для формирования соответствующих уведомлений. Триггер для наблюдаемого узла добавляется стандартным способом. Ниже показан пример выражения, указываемого в поле **trigger expression** для описанного триггера.
   - Для Zabbix версии *2.x*:

     ```
     ({TRIGGER.VALUE}=0 & {DRWEB:snmptrap[.*\.1\.3\.6\.1\.4\.1\.29690\..*].nodata(60)}
     =1 )|({TRIGGER.VALUE}=1 &
     {DRWEB:snmptrap[.*\.1\.3\.6\.1\.4\.1\.29690\..*].nodata(60)}=0)
     ```

   - Для Zabbix версии *3.x*:

     ```
     ({TRIGGER.VALUE}=0 and {drweb-host:snmptrap[".29690."].nodata(60)}=1 ) or
     ({TRIGGER.VALUE}=1 and {drweb-host:snmptrap[".29690."].nodata(60)}=0 )
     ```

   Данный триггер срабатывает (устанавливается в значение 1), если журнал уведомлений *SNMP trap*, поступающих от Dr.Web SNMPD, был обновлен в течение минуты. Если же журнал в течение минуты не обновлялся, то триггер выключается (меняет состояние на 0).

   В поле **Severity** для этого триггера рекомендуется устанавливать вид уведомления, отличный от *Not classified*, например, *Warning*.

Настройка приема уведомлений SNMP trap для Zabbix

1. На наблюдаемом узле в настройках Dr.Web SNMPD (параметр `TrapReceiver`) указывается адрес, который прослушивается `snmptrapd` на узле с Zabbix, например:

   ```
   SNMPD.TrapReceiver = 10.20.30.40:162
   ```

2. В конфигурационном файле `snmptrapd` (`snmptrapd.conf`) указывается тот же адрес, а также приложение, которое будет обрабатывать полученные уведомления *SNMP trap* (в данном случае, `snmptthandler`, компонент `snmptt`):

   ```
   snmpTrapdAddr 10.20.30.40:162
   traphandle default /usr/sbin/snmptthandler
   ```

   Чтобы `snmptt` не отклонял уведомления *SNMP trap*, отправленные Dr.Web SNMPD, как неизвестные, добавьте также в этот файл строку:

   ```
   outputOption n
   ```

3. Компонент `snmptthandler` сохраняет принимаемые уведомления *SNMP trap* в файл на диске в соответствии с указанным форматом, который должен соответствовать регулярному выражению, заданному в шаблоне узла для Zabbix (элемент (*item*) *drweb-traps*). Формат сохраняемого сообщения о поступлении уведомления *SNMP trap* поставляется в файле `/opt/drweb.com/share/drweb-snmpd/connectors/zabbix/snmptt.drweb.zabbix.conf` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/zabbix/snmptt.drweb.zabbix.conf` для FreeBSD, который необходимо скопировать в каталог `/etc/snmp`.
4. Кроме этого, путь к файлам формата необходимо указать в конфигурационном файле `snmptt.ini`:

   ```
   [TrapFiles]
   # A list of snmptt.conf files (this is NOT the snmptrapd.conf file).
   # The COMPLETE path and filename. Ex: '/etc/snmp/snmptt.conf'
   snmptt_conf_files = <<END
   /etc/snmp/snmptt.conf
   /etc/snmp/snmptt.drweb.zabbix.conf
   END
   ```

   После этого, если `snmptt` запущен в режиме демона, то его надо перезапустить.
5. В конфигурационном файле сервера Zabbix (`zabbix-server.conf`) необходимо задать (или проверить наличие) следующих настроек:

   ```
   SNMPTrapperFile=/var/log/snmptt/snmptt.log
   StartSNMPTrapper=1
   ```

   где `/var/log/snmptt/snmptt.log` — файл журнала, в который `snmptt` записывает информацию о поступивших уведомлениях SNMP trap.

Подробнее с официальной документацией по Zabbix вы можете ознакомиться по ссылке.

Интеграция с системой мониторинга Nagios

Для подключения Dr.Web SNMPD к системе мониторинга Nagios в каталоге `/opt/drweb.com/share/drweb-snmpd/connectors/nagios` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/nagios` для FreeBSD поставляются следующие файлы примеров конфигурации Nagios:

Файл	Описание
`nagiosgraph/rrdopts.conf-sample`	Пример конфигурационного файла RRD
`objects/drweb.cfg`	Конфигурационный файл, описывающий объекты *drweb*
`objects/nagiosgraph.cfg`	Конфигурационный файл компонента построения графиков Nagiosgraph, используемого Nagios

Файл	Описание
`plugins/check_drweb`	Скрипт для сбора данных от узла с Dr.Web Server Security Suite
`plugins/eventhandlers/submit_check_result`	Скрипт для обработки уведомлений *SNMP trap*
`snmp/snmptt.drweb.nagios.conf`	Настройки утилиты `snmptt` — приемника уведомлений *SNMP trap*

Подключение узла к Nagios

В данной инструкции предполагается, что система мониторинга Nagios уже корректно развернута на сервере мониторинга, включая настройку веб-сервера и графического средства Nagiosgraph, а на наблюдаемом узле установлен и корректно функционирует Dr.Web SNMPD (возможно, в режиме прокси совместно с snmpd). Кроме того, если планируется получать с наблюдаемого узла уведомления *SNMP trap* (в частности, об обнаружении Dr.Web Server Security Suite угроз на защищаемом сервере), на сервере мониторинга также должен быть установлен пакет `net-snmp` (используются стандартные утилиты `snmptt` и `snmptrapd`).

В данном руководстве по подключению используются следующие соглашения о путях (реальные пути зависят от ОС и установки Nagios):

- <*NAGIOS_PLUGINS_DIR*> — каталог плагинов Nagios, например, `/usr/lib64/nagios/plugins`.
- <*NAGIOS_ETC_DIR*> — каталог настроек Nagios, например, `/etc/nagios`.
- <*NAGIOS_OBJECTS_DIR*> — каталог объектов Nagios, например, `/etc/nagios/objects`.
- <*NAGIOSGRAPH_DIR*> — каталог Nagiosgraph, например, `/usr/local/nagiosgraph`.
- <*NAGIOS_PERFDATA_LOG*> — файл, в который Nagios записывает результаты выполнения команд проверки сервисов (должен совпадать с файлом `perflog` из <*NAGIOSGRAPH_DIR*>`/etc/nagiosgraph.conf`). Записи из этого файла считываются скриптом <*NAGIOSGRAPH_DIR*>`/bin/insert.pl` и записываются в соответствующие RRA-архивы RRDtool.

Настройка Nagios

1. Скопируйте файл `check_drweb` в каталог <*NAGIOS_PLUGINS_DIR*>, а файл `drweb.cfg` — в каталог <*NAGIOS_OBJECTS_DIR*>.
2. Добавьте в группу *drweb* узлы с установленным Dr.Web Server Security Suite, подлежащие наблюдению (на них должен быть запущен Dr.Web SNMPD), по умолчанию в данную группу включен только локальный узел *localhost*.

3. Отредактируйте (при необходимости) команду `check_drweb`, в которой указывается обращение к Dr.Web SNMPD на узлах *drweb* через утилиту `snmplwalk`:

   ```
   snmpwalk -c public -v 2c $HOSTADDRESS$:161
   ```

   Укажите правильную версию протокола SNMP и параметры, такие как *community string*, или параметры аутентификации, а также порт. Переменную `$HOSTADDRESS$` необходимо оставить в команде (она автоматически заменяется Nagios на правильный адрес узла при вызове команды). OID в команде указывать не требуется. Рекомендуется также указать команду вместе с полным путем к исполняемому файлу (обычно — `/usr/local/bin/snmpwalk`).

4. Подключите объекты *DrWeb* в конфигурационном файле *<NAGIOS_ETC_DIR>*`/nagios.cfg`, добавив в него строку:

   ```
   cfg_file=<NAGIOS_OBJECTS_DIR>/drweb.cfg
   ```

5. Добавьте настройки RRDtool для графиков *DrWeb* из файла `rrdopts.conf-sample` в файл *<NAGIOSGRAPH_DIR>*`/etc/rrdopts.conf`.

6. Если компонент Nagiosgraph еще не настроен, то выполните его настройку:

   - Скопируйте файл `nagiosgraph.cfg` в каталог *<NAGIOS_OBJECTS_DIR>* и исправьте путь к файлу скрипта `insert.pl` в команде `process-service-perfdata-for-nagiosgraph`, например, так:

     ```
     $ awk '$1 == "command_line" { $2 = "<NAGIOSGRAPH_DIR>/bin/insert.pl" }{ print }'
     ./objects/nagiosgraph.cfg > <NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
     ```

   - Подключите этот файл в конфигурационном файле *<NAGIOS_ETC_DIR>*`/nagios.cfg`, добавив в него строку:

     ```
     cfg_file=<NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
     ```

7. Проверьте значения параметров Nagios в конфигурационном файле *<NAGIOS_ETC_DIR>*`/nagios.cfg`:

   ```
   check_external_commands=1
   execute_host_checks=1
   accept_passive_host_checks=1
   enable_notifications=1
   enable_event_handlers=1

   process_performance_data=1
   service_perfdata_file=/usr/nagiosgraph/var/rrd/perfdata.log
   service_perfdata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDESC$||$SERVIC
   EOUTPUT$||$SERVICEPERFDATA$
   service_perfdata_file_mode=a
   service_perfdata_file_processing_interval=30
   service_perfdata_file_processing_command=process-service-perfdata-for-nagiosgraph

   check_service_freshness=1
   enable_flap_detection=1
   enable_embedded_perl=1
   enable_environment_macros=1
   ```

Настройка приема уведомлений SNMP trap для Nagios

1. На наблюдаемом узле в настройках Dr.Web SNMPD (параметр `TrapReceiver`) укажите адрес, который прослушивается `snmptrapd` на узле с Nagios, например:

   ```
   SNMPD.TrapReceiver = 10.20.30.40:162
   ```

2. Проверьте наличие файла скрипта *<NAGIOS_PLUGINS_DIR>*`/eventhandlers/submit_check_result`, который будет вызываться при получении уведомлений *SNMP trap*. Если этого файла нет, то следует скопировать в это место файл `submit_check_result` из каталога `/opt/drweb.com/share/drweb-snmpd/connectors/nagios/plugins/eventhandlers/` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/nagios/plugins/eventhandlers/` для FreeBSD. Необходимо в этом файле исправить путь, указанный в параметре `CommandFile`. Он должен иметь то же значение, что и параметр `command_file` в файле *<NAGIOS_ETC_DIR>*`/nagios.cfg`.

3. Скопируйте файл `snmptt.drweb.nagios.conf` в каталог `/etc/snmp/snmp/`. В этом файле измените путь к файлу скрипта `submit_check_result`, например, выполнив команду:

   ```
   $ awk '$1 == "EXEC" { $2 = <NAGIOS_PLUGINS_DIR>/eventhandlers/submit_check_result }
   { print}' ./snmp/snmptt.drweb.nagios.conf > /etc/snmp/snmp/snmptt.drweb.nagios.conf
   ```

4. Добавьте в файл `/etc/snmp/snmptt.ini` строку «`/etc/snmp/snmptt.drweb.nagios.conf`». После этого, если `snmptt` запущен в режиме демона, то его надо перезапустить.

После того как все требуемые файлы конфигурации Nagios были добавлены и отредактированы, необходимо запустить Nagios в режиме отладки командой:

```
# nagios -v <NAGIOS_ETC_DIR>/nagios.cfg
```

В этом случае Nagios проверит наличие ошибок конфигурации. Если ошибки не были найдены при проверке, перезапустите Nagios стандартным способом, например, командой:

```
# service nagios restart
```

Подробнее с официальной документацией по Nagios вы можете ознакомиться по ссылке.

9.14.5. Dr.Web SNMP MIB

Перечень параметров работы Dr.Web Server Security Suite, которые могут быть получены внешними системами мониторинга по протоколу SNMP, представлен в таблице ниже.

Имя параметра	OID параметра	Тип и описание параметра
Общий префикс имен: `.iso.org.dod.internet.private.enterprises.drweb.drwebSnmpd` Общий префикс OID: `.1.3.6.1.4.1.29690.2`		
alert	**Асинхронные уведомления о событиях (SNMP traps)**	
threatAlert	`.1.1`	Уведомление об обнаруженной угрозе
`threatAlertFile`	`.1.1.1`	Имя инфицированного файла (строка)
`threatAlertType`	`.1.1.2`	Тип угрозы (целое число*)
`threatAlertName`	`.1.1.3`	Название угрозы (строка)
`threatAlertOrigin`	`.1.1.4`	Идентификатор компонента, обнаружившего угрозу (целое число***)
`threatAlertRemoteIp`	`.1.1.5`	IP-адрес удаленного узла, с которого производился доступ к файлу (строка)
`threatAlertRemoteUser`	`.1.1.6`	Имя удаленного пользователя, обращавшегося к файлу (строка)
`threatAlertRemoteDomain`	`.1.1.7`	Имя удаленного узла (FQDN), с которого производился доступ к файлу (строка)
threatActionErrorAlert	`.1.2`	Уведомление об ошибке при попытке нейтрализации угрозы
`threatActionErrorAlertFile`	`.1.2.1`	Имя инфицированного файла (строка)
`threatActionErrorAlertType`	`.1.2.2`	Тип угрозы (целое число*)
`threatActionErrorAlertName`	`.1.2.3`	Название угрозы (строка)
`threatActionErrorAlertOrigin`	`.1.2.4`	Идентификатор компонента, обнаружившего угрозу (целое число***)
`threatActionErrorAlertError`	`.1.2.5`	Описание ошибки (строка)
`threatActionErrorAlertErrorCode`	`.1.2.6`	Код ошибки (целое число, соответствует кодам из

Имя параметра	OID параметра	Тип и описание параметра
		таблицы каталога ошибок)
threatActionErrorAlertAction	.1.2.7	Действие, попытка совершить которое привела к ошибке (целое число: 1 — лечить; 2 — переместить в карантин; 3 — удалить; 4 — информировать; 5 — игнорировать)
componentFailureAlert	.1.3	Уведомление о сбое в работе компонента
componentFailureAlertName	.1.3.1	Идентификатор компонента (целое число***)
componentFailureAlertExitCodeDescription	.1.3.2	Описание кода завершения компонента (строка)
componentFailureAlertExitCode	.1.3.3	Код завершения компонента (целое число, соответствует кодам из таблицы каталога ошибок)
infectedUrlAlert	.1.4	Уведомление о блокировании доступа к веб-ресурсу, содержащему угрозу (для соединений HTTP/HTTPS)
infectedUrlAlertUrl	.1.4.1	Заблокированный URL (строка)
infectedUrlAlertDirection	.1.4.2	Направление HTTP-сообщения (целое число: 1 — запрос, 2 — ответ)
infectedUrlAlertType	.1.4.3	Тип угрозы (целое число*)
infectedUrlAlertName	.1.4.4	Название угрозы (строка)
infectedUrlAlertOrigin	.1.4.5	Идентификатор компонента, обнаружившего угрозу (целое число***)
infectedUrlAlertSrcIp	.1.4.6	IP-адрес источника соединения (строка)
infectedUrlAlertSrcPort	.1.4.7	Порт источника соединения (целое число)
infectedUrlAlertDstIp	.1.4.8	IP-адрес точки назначения соединения (строка)

Имя параметра	OID параметра	Тип и описание параметра
infectedUrlAlertDstPort	.1.4.9	Порт точки назначения соединения (целое число)
infectedUrlAlertSniHost	.1.4.10	SNI точки назначения соединения (для SSL-соединений) (строка)
infectedUrlAlertExePath	.1.4.11	Исполняемый путь программы-инициатора соединения (строка)
infectedUrlAlertUserName	.1.4.12	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
categoryUrlAlert	.1.6	Уведомление о блокировании доступа к веб-ресурсу, входящему в нежелательную категорию
categoryUrlAlertUrl	.1.6.1	Заблокированный URL (строка)
categoryUrlAlertCategory	.1.6.2	Категория веб-ресурсов, к которой относится URL (целое число**)
categoryUrlAlertOrigin	.1.6.3	Идентификатор компонента, обнаружившего угрозу (целое число***)
categoryUrlAlertSrcIp	.1.6.4	IP-адрес источника соединения (строка)
categoryUrlAlertSrcPort	.1.6.5	Порт источника соединения (целое число)
categoryUrlAlertDstIp	.1.6.6	IP-адрес точки назначения соединения (строка)
categoryUrlAlertDstPort	.1.6.7	Порт точки назначения соединения (целое число)
categoryUrlAlertSniHost	.1.6.8	SNI точки назначения соединения (для SSL-соединений) (строка)
categoryUrlAlertExePath	.1.6.9	Исполняемый путь программы-инициатора соединения (строка)

Имя параметра	OID параметра	Тип и описание параметра
categoryUrlAlertUserName	.1.6.10	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
expiringLicenseAlert	.1.10	Дней до истечения лицензии (целое число)
outdatedBasesAlert	.1.11	Время последней успешной попытки обновления баз (*Unix time*)
stat	**Статистические показатели работы Dr.Web Server Security Suite**	
threatCounters	.2.1	Счетчики обнаруженных угроз
knownVirus	.2.1.1	Число обнаруженных известных угроз (счетчик; целое число)
suspicious	.2.1.2	Число обнаруженных подозрительных объектов (счетчик; целое число)
adware	.2.1.3	Число обнаруженных рекламных программ (счетчик; целое число)
dialers	.2.1.4	Число обнаруженных программ дозвона (счетчик; целое число)
joke	.2.1.5	Число обнаруженных шуточных программ (счетчик; целое число)
riskware	.2.1.6	Число обнаруженных потенциально опасных программ (счетчик; целое число)
hacktool	.2.1.7	Число обнаруженных программ взлома (счетчик; целое число)
scanErrors	.2.2	Счетчики произошедших ошибок проверки файлов
sePathNotAbsolute	.2.2.1	Количество возникновений ошибки «Не абсолютный

Имя параметра	OID параметра	Тип и описание параметра
		путь» (счетчик; целое число)
seFileNotFound	.2.2.2	Количество возникновений ошибки «Файл не найден» (счетчик; целое число)
seFileNotRegular	.2.2.3	Количество возникновений ошибки «Специальный (не регулярный) файл» (счетчик; целое число)
seFileNotBlockDevice	.2.2.4	Количество возникновений ошибки «Файл — не блочное устройство» (счетчик; целое число)
seNameTooLong	.2.2.5	Количество возникновений ошибки «Слишком длинный путь или имя файла» (счетчик; целое число)
seNoAccess	.2.2.6	Количество возникновений ошибки «Доступ запрещен» (счетчик; целое число)
seReadError	.2.2.7	Количество возникновений ошибки «Ошибка чтения» (счетчик; целое число)
seWriteError	.2.2.8	Количество возникновений ошибки «Ошибка записи» (счетчик; целое число)
seFileTooLarge	.2.2.9	Количество возникновений ошибки «Файл слишком большой» (счетчик; целое число)
seFileBusy	.2.2.10	Количество возникновений ошибки «Файл занят» (счетчик; целое число)
seUnpackingError	.2.2.20	Количество возникновений ошибки «Ошибка распаковки» (счетчик; целое число)
sePasswordProtecetd	.2.2.21	Количество возникновений ошибки «Защищено паролем» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
seArchCrcError	.2.2.22	Количество возникновений ошибки «Ошибка контрольной суммы архива» (счетчик; целое число)
seArchInvalidHeader	.2.2.23	Количество возникновений ошибки «Недопустимый заголовок архива» (счетчик; целое число)
seArchNoMemory	.2.2.24	Количество возникновений ошибки «Недостаточно памяти для обработки архива» (счетчик; целое число)
seArchIncomplete	.2.2.25	Количество возникновений ошибки «Неожиданный конец архива» (счетчик; целое число)
seCanNotBeCured	.2.2.26	Количество возникновений ошибки «Объект не может быть вылечен» (счетчик; целое число)
sePackerLevelLimit	.2.2.30	Количество возникновений ошибки «Превышение допустимого уровня вложенности для запакованных объектов» (счетчик; целое число)
seArchiveLevelLimit	.2.2.31	Количество возникновений ошибки «Превышение допустимого уровня вложенности для архивов» (счетчик; целое число)
seMailLevelLimit	.2.2.32	Количество возникновений ошибки «Превышение допустимого уровня вложенности для почтовых файлов» (счетчик; целое число)
seContainerLevelLimit	.2.2.33	Количество возникновений ошибки «Превышение допустимого уровня вложенности для

Имя параметра	OID параметра	Тип и описание параметра
		контейнеров» (счетчик; целое число)
seCompressionLimit	.2.2.34	Количество возникновений ошибки «Превышение допустимой величины коэффициента сжатия» (счетчик; целое число)
seReportSizeLimit	.2.2.35	Количество возникновений ошибки «Превышение допустимого размера отчета о проверке» (счетчик; целое число)
seScanTimeout	.2.2.40	Количество возникновений ошибки «Истекло время на проверку файла» (счетчик; целое число)
seEngineCrash	.2.2.41	Количество возникновений ошибки «Обнаружен сбой сканирующего ядра» (счетчик; целое число)
seEngineHangup	.2.2.42	Количество возникновений ошибки «Перестало отвечать сканирующее ядро» (счетчик; целое число)
seEngineError	.2.2.44	Количество возникновений ошибки «Внутренняя ошибка сканирующего ядра» (счетчик; целое число)
seNoLicense	.2.2.45	Количество возникновений ошибки «Не найдена действующая лицензия» (счетчик; целое число)
seCuringLimitReached	.2.2.47	Количество возникновений ошибки «Достигнут предел попыток лечения» (счетчик; целое число)
seNonSupportedDisk	.2.2.50	Количество возникновений ошибки «Не поддерживаемый диск» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
seUnexpectedError	.2.2.100	Количество возникновений ошибки «Неожиданная ошибка» (счетчик; целое число)
scanLoadAverage	.2.3	Показатели нагрузки проверки файлов
filesScannedTable	.2.3.1	Скорость проверки файлов по запросам от компонентов
filesScannedEntry	.2.3.1.1	Компонент (строка таблицы; запись)
filesScannedIndex	.2.3.1.1.1	Индекс компонента (идентификатор; целое число***)
filesScannedOrigin	.2.3.1.1.2	Имя компонента
filesScanned1min	.2.3.1.1.3	Среднее (за минуту) количество файлов, проверенных в секунду (строка)
filesScanned5min	.2.3.1.1.4	Среднее (за 5 минут) количество файлов, проверенных в секунду (строка)
filesScanned15min	.2.3.1.1.5	Среднее (за 15 минут) количество файлов, проверенных в секунду (строка)
bytesScannedTable	.2.3.2	Скорость проверки (в байтах) по запросам от компонентов
bytesScannedEntry	.2.3.2.1	Компонент (строка таблицы; запись)
bytesScannedIndex	.2.3.2.1.1	Индекс компонента (идентификатор; целое число***)
bytesScannedOrigin	.2.3.2.1.2	Имя компонента
bytesScanned1min	.2.3.2.1.3	Среднее (за минуту) количество байт, проверенных в секунду (строка)

Имя параметра	OID параметра	Тип и описание параметра
bytesScanned5min	.2.3.2.1.4	Среднее (за 5 минут) количество байт, проверенных в секунду (строка)
bytesScanned15min	.2.3.2.1.5	Среднее (за 15 минут) количество байт, проверенных в секунду (строка)
cacheHitFilesTable	.2.3.3	Использование кеша проверенных файлов по запросам от компонентов
cacheHitFilesEntry	.2.3.3.1	Компонент (строка таблицы; запись)
cacheHitFilesIndex	.2.3.3.1.1	Индекс компонента (идентификатор; целое число***)
cacheHitFilesOrigin	.2.3.3.1.2	Имя компонента
cacheHitFiles1min	.2.3.3.1.3	Среднее (за минуту) количество отчетов о проверке, извлеченных из кеша в секунду (строка)
cacheHitFiles5min	.2.3.3.1.4	Среднее (за 5 минут) количество отчетов о проверке, извлеченных из кеша в секунду (строка)
cacheHitFiles15min	.2.3.3.1.5	Среднее (за 15 минут) количество отчетов о проверке, извлеченных из кеша в секунду (строка)
errorsTable	.2.3.4	Число ошибок проверки по запросам от компонентов
errorsEntry	.2.3.4.1	Компонент (строка таблицы; запись)
errorsIndex	.2.3.4.1.1	Индекс компонента (идентификатор; целое число***)
errorsOrigin	.2.3.4.1.2	Имя компонента
errors1min	.2.3.4.1.3	Среднее (за минуту) количество ошибок в секунду (строка)

Имя параметра	OID параметра	Тип и описание параметра
errors5min	.2.3.4.1.4	Среднее (за 5 минут) количество ошибок в секунду (строка)
errors15min	.2.3.4.1.5	Среднее (за 15 минут) количество ошибок в секунду (строка)
net	.2.4	Показатели сетевой активности
info	**Информация о состоянии Dr.Web Server Security Suite**	
components	.3.1	Состояние компонентов Dr.Web Server Security Suite
configd	.3.1.1	Данные о компоненте drweb-configd
configdState	.3.1.1.1	Состояние компонента (целое число****)
configdExitCode	.3.1.1.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
configdExitTime	.3.1.1.3	Время завершения работы (*Unix time*)
configdInstalledApps	.3.1.1.101	Перечень установленных компонентов
configdAppEntry	.3.1.1.101.1	Информация об установленном компоненте (строка таблицы; запись)
configdAppIndex	.3.1.1.101.1.1	Индекс (номер) установленного компонента (целое число)
configdAppName	.3.1.1.101.1.2	Имя установленного компонента (строка)
configdAppExePath	.3.1.1.101.1.3	Путь к исполняемому файлу компонента (строка)
configdAppInstallTime	.3.1.1.101.1.4	Время установки компонента (*Unix time*)

Имя параметра	OID параметра	Тип и описание параметра
configdAppIniSection	.3.1.1.101.1.5	Имя секции с параметрами компонента в конфигурационном файле (строка)
scanEngine	.3.1.2	Данные о компоненте drweb-se
scanEngineState	.3.1.2.1	Состояние компонента (целое число****)
scanEngineExitCode	.3.1.2.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
scanEngineExitTime	.3.1.2.3	Время завершения работы (*Unix time*)
scanEngineStatus	.3.1.2.101	Состояние Dr.Web Virus-Finding Engine (целое число)
scanEngineVersion	.3.1.2.102	Версия Dr.Web Virus-Finding Engine (строка)
scanEngineVirusRecords	.3.1.2.103	Число записей об угрозах (целое число)
scanEngineMaxForks	.3.1.2.104	Максимальное число дочерних сканирующих процессов (целое число)
scanEngineQueues	.3.1.2.105	Очереди задач на проверку
scanEngineQueuesLow	.3.1.2.105.1	Очередь низкоприоритетных задач
scanEngineQueueLowOut	.3.1.2.105.1.1	Число низкоприоритетных задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueLowSize	.3.1.2.105.1.2	Число низкоприоритетных задач, ожидающих обработки в очереди (счетчик; целое число)
scanEngineQueuesMedium	.3.1.2.105.2	Очередь задач обычного приоритета

Имя параметра	OID параметра	Тип и описание параметра
scanEngineQueueMediumOut	.3.1.2.105.2.1	Число задач обычного приоритета, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueMediumSize	.3.1.2.105.2.2	Число задач обычного приоритета, ожидающих обработки в очереди (счетчик; целое число)
scanEngineQueuesHigh	.3.1.2.105.3	Очередь высокоприоритетных задач
scanEngineQueueHighOut	.3.1.2.105.3.1	Число высокоприоритетных задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueHighSize	.3.1.2.105.3.2	Число высокоприоритетных задач, ожидающих обработки в очереди (счетчик; целое число)
scanEngineVirusBasesTable	.3.1.2.106	Перечень вирусных баз
scanEngineVirusBasesEntry	.3.1.2.106.1	Информация о вирусной базе (строка таблицы; запись)
scanEngineVirusBaseIndex	.3.1.2.106.1.1	Индекс вирусной базы (целое число)
scanEngineVirusBasePath	.3.1.2.106.1.2	Путь к файлу вирусной базы (строка)
scanEngineVirusBaseRecords	.3.1.2.106.1.3	Число записей в вирусной базе (целое число)
scanEngineVirusBaseVersion	.3.1.2.106.1.4	Версия вирусной базы (целое число)
scanEngineVirusBaseTimestamp	.3.1.2.106.1.5	Метка времени для вирусной базы (*Unix time*)
scanEngineVirusBaseMD5	.3.1.2.106.1.6	Контрольная сумма MD5 (строка)
scanEngineVirusBaseLoadResult	.3.1.2.106.1.7	Результат загрузки вирусной базы (строка)

Имя параметра	OID параметра	Тип и описание параметра
scanEngineQueuesTab	.3.1.2.107	Перечень очередей задач на проверку
scanEngineQueueEntry	.3.1.2.107.1	Информация об очереди (строка таблицы; запись)
scanEngineQueueIndex	.3.1.2.107.1.1	Индекс (номер) очереди (целое число)
scanEngineQueueName	.3.1.2.107.1.2	Имя очереди (строка)
scanEngineQueueOut	.3.1.2.107.1.3	Число задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueSize	.3.1.2.107.1.4	Число задач, ожидающих обработки в очереди (счетчик; целое число)
fileCheck	.3.1.3	Данные о компоненте drweb-filecheck
fileCheckState	.3.1.3.1	Состояние компонента (целое число****)
fileCheckExitCode	.3.1.3.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
fileCheckExitTime	.3.1.3.3	Время завершения работы (*Unix time*)
fileCheckScannedFiles	.3.1.3.101	Число проверенных файлов (счетчик; целое число)
fileCheckScannedBytes	.3.1.3.102	Число проверенных байт (счетчик; целое число)
fileCheckCacheHitFiles	.3.1.3.103	Число отчетов о проверке, извлеченных из кеша проверенных файлов (счетчик; целое число)
fileCheckScanErrors	.3.1.3.104	Число ошибок сканирующего ядра (счетчик; целое число)
fileCheckScanStat	.3.1.3.105	Перечень клиентов

Имя параметра	OID параметра	Тип и описание параметра
fileCheckClientEntry	.3.1.3.105.1	Информация о клиенте (строка таблицы; запись)
fileCheckClientIndex	.3.1.3.105.1.1	Индекс (номер) клиента (целое число)
fileCheckClientName	.3.1.3.105.1.2	Имя компонента-клиента (строка)
fileCheckClientScannedFiles	.3.1.3.105.1.3	Число файлов, проверенных для данного клиента (счетчик; целое число)
fileCheckClientScannedBytes	.3.1.3.105.1.4	Число байт, проверенных для данного клиента (счетчик; целое число)
fileCheckClientCacheHitFiles	.3.1.3.105.1.5	Число отчетов о проверке для данного клиента, извлеченных из кеша проверенных файлов (счетчик; целое число)
fileCheckClientScanErrors	.3.1.3.105.1.6	Число ошибок сканирующего ядра для данного клиента (счетчик; целое число)
update	.3.1.4	Данные о компоненте drweb-update
updateState	.3.1.4.1	Состояние компонента (целое число****)
updateExitCode	.3.1.4.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
updateExitTime	.3.1.4.3	Время завершения работы (*Unix time*)
updateBytesSent	.3.1.4.101	Число отправленных байт (счетчик; целое число)
updateBytesReceived	.3.1.4.102	Число принятых байт (счетчик; целое число)
esagent	.3.1.5	Данные о компоненте drweb-esagent
esagentState	.3.1.5.1	Состояние компонента (целое число****)

Имя параметра	OID параметра	Тип и описание параметра
esagentExitCode	.3.1.5.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
esagentExitTime	.3.1.5.3	Время завершения работы (*Unix time*)
esagentWorkStatus	.3.1.5.101	Режим работы компонента (целое число: 1 — автономный, 2 — подключается, 3 — ожидает подключения, 4 — подключение одобрено)
esagentIsConnected	.3.1.5.102	Подключен ли к серверу (целое число: 0 — нет, 1 — да)
esagentServer	.3.1.5.103	Адрес используемого сервера централизованной защиты (строка)
netcheck	.3.1.6	Данные о компоненте drweb-netcheck
netcheckState	.3.1.6.1	Состояние компонента (целое число****)
netcheckExitCode	.3.1.6.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
netcheckExitTime	.3.1.6.3	Время завершения работы (*Unix time*)
netcheckLocalSeForks	.3.1.6.101	Число ядер сканирования, доступных локально (целое число)
netcheckRemoteSeForks	.3.1.6.102	Число доступных удаленных ядер сканирования (целое число)
netcheckLocalFilesScanned	.3.1.6.103	Число файлов, проверенных локально (счетчик; целое число)
netcheckNetworkFilesScanned	.3.1.6.104	Число файлов, проверенных удаленно (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
netcheckLocalBytesScanned	.3.1.6.105	Число байт, проверенных локально (счетчик; целое число)
netcheckNetworkBytesScanned	.3.1.6.106	Число байт, проверенных удаленно (счетчик; целое число)
netcheckLocalBytesIn	.3.1.6.107	Число байт, полученных от локальных клиентов (счетчик; целое число)
netcheckLocalBytesOut	.3.1.6.108	Число байт, отправленных локальным клиентам (счетчик; целое число)
netcheckNetworkBytesIn	.3.1.6.109	Число байт, полученных от удаленных узлов (счетчик; целое число)
netcheckNetworkBytesOut	.3.1.6.110	Число байт, отправленных на удаленные узлы (счетчик; целое число)
netcheckLocalScanErrors	.3.1.6.111	Число ошибок локальных ядер сканирования (счетчик; целое число)
netcheckNetworkScanErrors	.3.1.6.112	Число ошибок удаленных ядер сканирования (счетчик; целое число)
httpd	.3.1.7	Данные о компоненте drweb-httpd
httpdState	.3.1.7.1	Состояние компонента (целое число****)
httpdExitCode	.3.1.7.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
httpdExitTime	.3.1.7.3	Время завершения работы (*Unix time*)
snmpd	.3.1.8	Данные о компоненте drweb-snmpd
snmpdState	.3.1.8.1	Состояние компонента (целое число****)

Имя параметра	OID параметра	Тип и описание параметра
snmpdExitCode	.3.1.8.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
snmpdExitTime	.3.1.8.3	Время завершения работы (*Unix time*)
statd	.3.1.9	Данные о компоненте drweb-statd
statdState	.3.1.9.1	Состояние компонента (целое число****)
statdExitCode	.3.1.9.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
statdExitTime	.3.1.9.3	Время завершения работы (*Unix time*)
statdConnectionsIn	.3.1.9.101	Число принятых соединений (счетчик; целое число)
statdConnectionsCount	.3.1.9.102	Текущее число открытых соединений (счетчик; целое число)
clamd	.3.1.20	Данные о компоненте drweb-clamd
clamdState	.3.1.20.1	Состояние компонента (целое число****)
clamdExitCode	.3.1.20.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
clamdExitTime	.3.1.20.3	Время завершения работы (*Unix time*)
smbspider	.3.1.40	Данные о компоненте drweb-smbspider-daemon
smbspiderState	.3.1.40.1	Состояние компонента (целое число****)
smbspiderExitCode	.3.1.40.2	Последний код завершения (целое число, соответствует

Имя параметра	OID параметра	Тип и описание параметра
		кодам из таблицы каталога ошибок)
smbspiderExitTime	.3.1.40.3	Время завершения работы (*Unix time*)
smbspiderConnectionsIn	.3.1.40.101	Общее число открытых соединений (счетчик; целое число)
smbspiderConnectionsCount	.3.1.40.102	Текущее число открытых соединений (счетчик; целое число)
smbspiderShareTable	.3.1.40.103	Статистика по защищаемым ресурсам Samba
smbspiderShareEntry	.3.1.40.103.1	Информация о защищаемом ресурсе Samba (строка таблицы; запись)
smbspiderShareIndex	.3.1.40.103.1.1	Индекс (номер) защищаемого ресурса Samba (целое число)
smbspiderSharePath	.3.1.40.103.1.2	Путь к защищаемому ресурсу Samba (строка)
smbspiderShareConnectionsIn	.3.1.40.103.1.3	Общее число открытых соединений (счетчик; целое число)
smbspiderShareConnectionsCount	.3.1.40.103.1.4	Число соединений, открытых в данный момент (счетчик; целое число)
cloudd	.3.1.50	Данные о компоненте drweb-cloudd
clouddState	.3.1.50.1	Состояние компонента (целое число****)
clouddExitCode	.3.1.50.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
clouddExitTime	.3.1.50.3	Время завершения работы (*Unix time*)
meshd	.3.1.52	Данные о компоненте drweb-meshd

Имя параметра	OID параметра	Тип и описание параметра
meshdState	.3.1.52.1	Состояние компонента (целое число****)
meshdExitCode	.3.1.52.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
meshdExitTime	.3.1.52.3	Время завершения работы (*Unix time*)
linuxspider	.3.1.201	Данные о компоненте drweb-spider (для GNU/Linux)
linuxspiderState	.3.1.201.1	Состояние компонента (целое число****)
linuxspiderExitCode	.3.1.201.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxspiderExitTime	.3.1.201.3	Время завершения работы (*Unix time*)
linuxspiderWorkStatus	.3.1.201.101	Режим работы компонента (целое число: 0 — не задан, 1 — загружается, 2 — через fanotify, 3 — LKM)
linuxnss	.3.1.202	Данные о компоненте drweb-nss (для GNU/Linux)
linuxnssState	.3.1.202.1	Состояние компонента (целое число****)
linuxnssExitCode	.3.1.202.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxnssExitTime	.3.1.202.3	Время завершения работы (*Unix time*)
linuxnssScannedFiles	.3.1.202.101	Число проверенных файлов (счетчик; целое число)
linuxnssScannedBytes	.3.1.202.102	Число проверенных байт (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
linuxnssScanErrors	.3.1.202.103	Число ошибок сканирования (счетчик; целое число)
ctl	.3.1.300	Данные о компоненте drweb-ctl
ctlState	.3.1.300.1	Состояние компонента (целое число****)
ctlExitCode	.3.1.300.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
ctlExitTime	.3.1.300.3	Время завершения работы (*Unix time*)
license	.3.2	Состояние лицензии
licenseEsMode	.3.2.1	Лицензия выдана сервером централизованной защиты (целое число: 0 — нет, 1 — да)
licenseNumber	.3.2.2	Номер лицензии (целое число)
licenseOwner	.3.2.3	Владелец лицензии (строка)
licenseActivated	.3.2.4	Дата активации лицензии (*Unix time*)
licenseExpires	.3.2.5	Дата прекращения действия лицензии (*Unix time*)

*) Типы угроз:

Код	Тип угрозы
1	Известная угроза (*known virus*)
2	Подозрительный объект (*suspicious*)
3	Рекламная программа (*adware*)
4	Программа дозвона (*dialer*)
5	Программа-шутка (*joke program*)
6	Потенциально опасная программа (*riskware*)
7	Программа взлома (*hacktool*)

**) Категории URL:

Код	Тип угрозы
1	Источник распространения угроз (*infectionSource*)
2	Не рекомендуемый (*notRecommended*)
3	Сайты для взрослых (*adultContent*)
4	Насилие (*violence*)
5	Оружие (*weapons*)
6	Азартные игры (*gambling*)
7	Наркотики (*drugs*)
8	Нецензурная лексика (*obsceneLanguage*)
9	Чаты (*chats*)
10	Терроризм (*terrorism*)
11	Бесплатная электронная почта (*freeEmail*)
12	Социальные сети (*socialNetworks*)
13	Добавленные по обращению правообладателя (*ownerNotice*)
14	Онлайн-игры (*onlineGames*)
15	Анонимайзеры (*anonymizers*)
16	Пулы добычи криптовалют (*cryptocurrencyMiningPools*)
17	Вакансии (*Jobs*)
20	Черный список (*blackList*)

***) Коды компонентов Dr.Web:

Код	Компонент
1	Dr.Web ConfigD (`drweb-configd`)
2	Dr.Web Scanning Engine (`drweb-se`)
3	Dr.Web File Checker (`drweb-filecheck`)
4	Dr.Web Updater (`drweb-update`)

Код	Компонент
5	Dr.Web ES Agent (`drweb-esagent`)
6	Dr.Web Network Checker (`drweb-netcheck`)
7	Dr.Web HTTPD (`drweb-httpd`)
8	Dr.Web SNMPD (`drweb-snmpd`)
20	Dr.Web ClamD (`drweb-clamd`)
40	SpIDer Guard для SMB (`drweb-smbspider-daemon`)
50	Dr.Web CloudD (`drweb-cloudd`)
52	Dr.Web MeshD (`drweb-meshd`)
201	SpIDer Guard (`drweb-spider`)
202	SpIDer Guard для NSS (`drweb-nss`)
300	Dr.Web Ctl (`drweb-ctl`)
400	Сканирование по заданию сервера централизованной защиты (не является компонентом Dr.Web Server Security Suite)

****) Состояния компонентов:

Код	Состояние
0	Не установлен
1	Установлен, но не запущен
2	Запускается
3	Работает
4	Завершает работу

Для непосредственного получения значений переменных используйте утилиту `snmpwalk`:

```
$ snmpwalk -Os -c <community> -v <версия SNMP> <адрес узла> <OID>
```

Например, для получения статистики по обнаруженным угрозам на локальном узле (при настройках Dr.Web SNMPD по умолчанию) выполните команду:

```
$ snmpwalk -Os -c public -v 2c 127.0.0.1 .1.3.6.1.4.1.29690.2.2.1
```

9.15. Dr.Web MeshD

Компонент Dr.Web MeshD представляет собой агент, включающий узел с установленным Dr.Web Server Security Suite в «локальное облако», объединяющее узлы, на которых установлены продукты Dr.Web для Unix. Данное облако позволяет одним узлам облака получить доступ к сканирующему ядру других, другими словами, воспользоваться услугой по проверке файлов.

Для объединения узлов с установленными продуктами Dr.Web для Unix в составе каждого узла должен присутствовать компонент Dr.Web MeshD, обеспечивающий включение этого узла в облако. Полномочия узла в рамках облака и возможности облака, используемые узлом, гибко регулируются настройками компонента Dr.Web MeshD.

Обмен данными с другими узлами облака производится по защищенному каналу SSH.

9.15.1. Принципы работы

В этом разделе

- Типы подключений
- Режимы работы
- Услуги
  - Удаленное сканирование файлов (Engine)
  - Передача файлов на проверку (File)
  - Проверка URL (Url)

Dr.Web MeshD играет роль посредника, обеспечивающего взаимодействие между узлом, на котором установлен Dr.Web Server Security Suite, и другими узлами облака.

Типы подключений

При работе Dr.Web MeshD использует подключения следующих типов:

- *Клиентские (сервисные)* используются Dr.Web MeshD для подключения к нему других узлов облака, которые являются клиентами услуг, предоставляемых данным узлом.

  Компоненты Dr.Web Server Security Suite, работающие на узле и использующие услуги, предоставленные облаком, подключаются к Dr.Web MeshD, работающий на этом же узле, через локальный Unix-сокет. Клиентское подключение при этом не используется.

- *Партнерские (одноранговые)* используются Dr.Web MeshD для взаимодействия с равноправными (в рамках некоторой услуги) узлами-партнерами облака. Обычно подобные горизонтальные связи используются для масштабирования и

распределения нагрузки при взаимодействии с облаком, а также синхронизации состояния узлов облака.

- *Восходящие* используются Dr.Web MeshD для подключения данного узла в роли клиента к узлам облака, предоставляющим услуги (например, передача файлов на проверку и т. д.).

Использование подключений всех трех типов настраивается для разных услуг облака независимо друг от друга. При этом один и тот же узел может быть настроен как сервер для обслуживания клиентских запросов в рамках одной услуги (например, проверки URL) и как клиент — в рамках другой услуги (например, удаленного сканирования файлов).

В рамках облака узлы осуществляют взаимодействие по защищенному протоколу SSH, т. е. все стороны в рамках каждого межузлового взаимодействия всегда взаимно аутентифицированы. Для аутентификации используются узловые ключи (*host keys*) согласно RFC 4251. Клиентское подключение от локального компонента всегда считается доверенным.

Режимы работы

Dr.Web MeshD может работать как в режиме демона, так и запускаться по запросам от других компонентов Dr.Web Server Security Suite, расположенных на локальном узле. Если Dr.Web MeshD настроен на обслуживание клиентских подключений (параметр `ListenAddress` не пуст) и активирована возможность оказания хотя бы одной из услуг, Dr.Web MeshD запускается как демон и ждет подключения со стороны клиентов.

Если Dr.Web MeshD не настроен на обслуживание клиентских подключений (параметр `ListenAddress` пуст) и запросы к нему отсутствуют в течение периода времени, указанного в параметре `IdleTimeLimit`, работа компонента автоматически завершается.

Услуги

Удаленное сканирование файлов (Engine)

Данная услуга позволяет использовать Dr.Web Scanning Engine для проверки удаленных файлов: узлы, работающие в роли клиентов, отправляют файлы на проверку на серверный узел, а серверные узлы предоставляют услугу по проверке файлов, отправленных клиентскими узлами. Типовые настройки клиента следующие:

```
…
[MeshD]
EngineChannel = On
EngineUplink = <адрес сервера>
ListenAddress =
…
```

На узле, выполняющем роль локального сервера сканирования, заданы следующие настройки:

```
EngineChannel = On
EngineUplink =
ListenAddress = <адрес>:<порт>
```

Здесь *<адрес сервера>* в восходящем соединении клиента должен указывать на те *<адрес>* и *<порт>*, которые используются серверным узлом для организации клиентских подключений.

Передача файлов на проверку (File)

Данная функциональность не используется (функция удаленного сканирования оказывается в рамках услуги *Engine*).

Проверка URL (Url)

Данная услуга предназначена для проверки URL на принадлежность к потенциально опасным и нежелательным категориям: узлы, выступающие в роли клиентов, отправляют URL для проверки на серверный узел. Типовые настройки клиента следующие:

```
…
[MeshD]
UrlChannel = On
UrlUplink = <адрес сервера>
ListenAddress =
…
```

На узле, выступающем в качестве сервера для проверки URL, заданы следующие настройки:

```
UrlChannel = On
UrlUplink =
ListenAddress = <адрес>:<порт>
```

Здесь *<адрес сервера>* в восходящем соединении клиента должен указывать на те *<адрес>* и *<порт>*, которые используются серверным узлом для организации клиентских подключений.

9.15.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web MeshD из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-meshd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-meshd [<параметры>]
```

Dr.Web MeshD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-meshd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web MeshD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-meshd`.

9.15.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[MeshD]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента.

Параметр	Описание
	Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-meshd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-meshd`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`DebugSsh` *{логический}*	Сохранять или не сохранять в журнале сообщения протокола SSH (используется для передачи сообщений и данных), полученных и отправленных компонентом Dr.Web MeshD, работающим на данном узле, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`ListenAddress` *<IP-адрес>:<порт>*	Сетевой сокет (адрес и порт) клиентского подключения, на котором компонент ожидает поступления соединений от узлов облака, являющихся клиентами услуг, предоставляемых данным узлом облака. Чтобы компонент мог прослушивать интерфейс IPv6 и определять клиентские узлы облака по IPv6, параметр должен быть обязательно установлен. Если значение не задано, то компонент не принимает запросы от клиентов. Значение по умолчанию: `0.0.0.0:7090`, если установлен пакет `drweb-scanning-server`, в противном случае значение не задано
`DnsResolverConfPath` *{путь к файлу}*	Путь к файлу настроек DNS. Значение по умолчанию: `/etc/resolv.conf`

Параметр	Описание
`DiscoveryResponderPort` *{номер порта}*	Порт, на котором вышестоящий узел MeshD отвечает по протоколу UDP на запросы клиентов. Механизм *discovery* работает только если задан параметр `ListenAddress`. Значение по умолчанию: `18008`
`FileChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге обмена файлами. Если этот параметр установлен в значение `On`, то компонент Dr.Web MeshD будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD. Значение по умолчанию: `On`
`FileUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, принимающего на проверку файлы с этого узла. Возможные значения: • *значение не указано* — сервер для этой услуги не задан, и Dr.Web MeshD не будет ни к кому подключаться. • *<IP-адрес>:<порт>* — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`*<имя сервиса>*`[:`*<домен>*`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена *<домен>*. Если *<домен>* не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним. • `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`FileDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги обмена файлами, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`EngineChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге предоставления сканирующего ядра. Если этот параметр установлен в значение `On`, то компонент Dr.Web MeshD будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD. Значение по умолчанию: `On`

Параметр	Описание
`EngineUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, предоставляющего услуги сканирующего ядра для данного узла. Возможные значения: • *значение не указано* — сервер для этой услуги не задан, и Dr.Web MeshD не будет ни к кому подключаться. • *<IP-адрес>:<порт>* — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`*<имя сервиса>*`[:`*<домен>*`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена *<домен>*. Если *<домен>* не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним. • `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`EngineDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги сканирования, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`UrlChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге проверки URL. Значение по умолчанию: `On`
`UrlUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, проверяющего URL для данного узла. Возможные значения: • *значение не указано* — сервер проверки URL не задан. • *<IP-адрес>:<порт>* — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`*<имя сервиса>*`[:`*<домен>*`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена *<домен>*. Если *<домен>* не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним. • `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`UrlDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги проверки URL, если установлен уровень подробности

Параметр	Описание
	журнала `LogLevel = Debug`. Значение по умолчанию: `No`



В текущей версии Dr.Web Server Security Suite услуга передачи файлов на проверку *File* не используется. Вместо нее следует использовать услугу сканирующего ядра *Engine*.

9.16. Dr.Web CloudD

В этом разделе

- Принципы работы
- Работа с сервисом Dr.Web Cloud
- Аргументы командной строки
- Параметры конфигурации

Принципы работы

Компонент Dr.Web CloudD предназначен для обращения к облачному сервису Dr.Web Cloud компании «Доктор Веб». Сервис Dr.Web Cloud собирает от всех антивирусных продуктов Dr.Web свежую информацию об обнаруженных угрозах, что позволяет:

- нейтрализовать новейшие угрозы, описание которых еще не внесено в вирусные базы;
- снизить вероятность ложных срабатываний сканирующего ядра Dr.Web Scanning Engine.

Если компонент включен, то он будет периодически отправлять облачному сервису Dr.Web Cloud статистику обнаружения инфицированных файлов.



Все данные, отправляемые компонентом на серверы компании «Доктор Веб», являются обезличенными и не позволяют идентифицировать пользователя.

Dr.Web Server Security Suite по умолчанию не подключен к облачному сервису Dr.Web Cloud.

Облачный сервис Dr.Web Cloud используется как дополнительный эшелон защиты при проверке файловых систем. Если компонент Dr.Web CloudD включен, то он задействуется при всех операциях проверки файловых систем.

Работа с сервисом Dr.Web Cloud

Подключение Dr.Web Server Security Suite к сервису Dr.Web Cloud происходит автоматически при включении компонента Dr.Web CloudD.

Вы можете включить или отключить компонент Dr.Web CloudD с помощью:

- утилиты Dr.Web Ctl;
- веб-интерфейса управления;
- редактирования конфигурационного файла вручную.

Включение или отключение с помощью утилиты Dr.Web Ctl

Чтобы включить Dr.Web CloudD, выполните команду:

```
# drweb-ctl cfset Root.UseCloud Yes
```

Чтобы отключить этот компонент, выполните команду:

```
# drweb-ctl cfset Root.UseCloud No
```

Включение или отключение с помощью веб-интерфейса управления (на примере локального компьютера)

1. Откройте веб-браузер и введите адрес `https://127.0.0.1:4443/`.
2. Укажите имя и пароль пользователя, обладающего привилегиями администратора.
3. Выберите **Настройки**, затем — **Общие настройки**.
4. Установите флажок напротив текста **UseCloud**, чтобы включить компонент, в противном случае снимите этот флажок.

Подробнее про настройку Dr.Web Server Security Suite с помощью веб-интерфейса управления.

Включение или отключение путем редактирования конфигурационного файла вручную



Вы должны быть уверены в корректности изменений, вносимых в конфигурационный файл.

1. Откройте конфигурационный файл `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD в предпочитаемом вами текстовом редакторе с правами администратора. Чтобы получить права администратора, используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.
2. Если в конфигурационном файле отсутствует секция `[Root]`, то перейдите в конец файла и добавьте с новой строки:
   - Для включения компонента и подключения к сервису:

     ```
     [Root]
     UseCloud = Yes
     ```

   - Для выключения компонента и отключения от сервиса:

     ```
     [Root]
     UseCloud = No
     ```

   Если конфигурационный файл уже включает секцию `[Root]`:

   - Если параметр `UseCloud` отсутствует, добавьте его, указав `UseCloud = Yes` для подключения к сервису или `UseCloud = No` для отключения от него.

- Если параметр `UseCloud` уже указан в секции `[Root]`, то измените его значение на `Yes` для подключения к сервису или на `No` для отключения от него.

3. Перезагрузите конфигурацию Dr.Web Server Security Suite, выполнив команду:

```
# drweb-ctl reload
```

для применения внесенных изменений.

Компонент Dr.Web CloudD запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-cloudd`.

Аргументы командной строки

Чтобы показать справочную информацию о компоненте Dr.Web CloudD, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-cloudd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-cloudd [<параметры>]
```

`drweb-cloudd` принимает следующие параметры:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-cloudd --help
```

Эта команда выведет на экран краткую справку о компоненте Dr.Web CloudD.

Параметры конфигурации

Компонент Dr.Web CloudD использует параметры конфигурации, заданные в секции `[CloudD]` объединенного конфигурационного файла Dr.Web Server Security Suite.

Чтобы изменить значение какого-либо параметра Dr.Web CloudD, выполните команду:

```
# drweb-ctl cfset CloudD.<параметр> <значение>
```

В секции `[CloudD]` представлены следующие параметры:

Параметр	Допустимые значения	Описание
`LogLevel`	*Debug, Info, Notice, Warning или Error*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log`	*Auto, Syslog[:<Daemon, User, Mail или Local0..7>] или <путь к файлу>*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath`	*путь к файлу*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-cloudd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-cloudd`
`RunAsUser`	*<UID> или <имя пользователя>*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit`	*интервал времени*	Максимальное время простоя компонента, при превышении которого он завершает свою работу.

Параметр	Допустимые значения	Описание
		Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `1h`

`FixedSocketPath`	*путь к файлу*	Путь к файлу Unix-сокета фиксированного экземпляра компонента.
		
		При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр компонента, доступный клиентам через этот сокет.
		
		
		Убедитесь, что каталогу с файлом сокета назначены следующие права доступа:
		`drwxr-xr-x`
		Чтобы просмотреть права доступа, выполните команду:
		`$ ls -ld <путь к каталогу>`
		
		Значение по умолчанию: *(не задано)*

`PersistentCache`	*On, Yes, True, Off, No или False*	Включать или нет сохранение на диск кеша ответов, получаемых от Dr.Web Cloud. Значение по умолчанию: `Off`
`DebugSdk`	*On, Yes, True, Off, No или False*	Включать или нет в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения от Dr.Web Cloud. Значение по умолчанию: `No`

9.17. Dr.Web StatD

Компонент Dr.Web StatD предназначен для накопления статистики событий, возникающих в процессе работы компонентов Dr.Web Server Security Suite. Полученные события регистрируются в постоянном хранилище и могут быть получены по запросу.

9.17.1. Принципы работы

Компонент Dr.Web StatD обеспечивает накопление и постоянное хранение событий, поступающих от компонентов Dr.Web Server Security Suite в процессе работы. Регистрируются события неожиданного завершения работы компонента.

Просмотр событий и управление ими обеспечивается командой `events` утилиты Dr.Web Ctl.

9.17.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web StatD из командной строки, выполните команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-statd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-statd [<параметры>]
```

Dr.Web StatD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-statd --help
```

Эта команда выведет на экран краткую справку компонента Dr.Web StatD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Server Security Suite из командной строки.



Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки выполните команду `man 1 drweb-statd`.

9.17.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[StatD]` объединенного конфигурационного файла Dr.Web Server Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-statd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-statd`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`

Параметр	Описание
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`MaxEventStoreSize` *{размер}*	Максимальный разрешенный размер базы событий. Задается в `mb`, например: `MaxEventStoreSize = 100mb`. Минимальное значение: `50mb`. Значение по умолчанию: `1GB`

10. Приложения

10.1. Приложение А. Виды компьютерных угроз

В этом разделе

- Компьютерные вирусы
- Компьютерные черви
- Троянские программы
- Программы взлома
- Рекламные программы
- Программы-шутки
- Программы дозвона
- Потенциально опасные программы
- Подозрительные объекты

Под термином *«угроза»* в этой классификации понимается любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они также могут нанести вред пользователю.

Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется *инфицированием*. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Значительное число вирусов создается для повреждения или уничтожения данных.

В компании «Доктор Веб» вирусы классифицируются по типам файлов, которые они инфицируют:

- *Файловые вирусы* инфицируют файлы операционной системы (обычно исполняемые файлы и динамические библиотеки) и активизируются при обращении к инфицированному файлу.
- *Макро-вирусы* инфицируют документы, которые используют программы из пакета Microsoft® Office (и другие программы, которые используют макросы, написанные, например, на языке Visual Basic). *Макросы* — это встроенные программы, написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в Microsoft® Word макросы могут запускаться при открытии, закрытии или сохранении документа).
- *Скрипт-вирусы* пишутся на языках скриптов и в большинстве случаев инфицируют другие файлы скриптов (например, служебные файлы операционной системы). Они также могут инфицировать файлы других типов, которые поддерживают исполнение скриптов, и могут распространяться, например, посредством уязвимых веб-приложений.
- *Загрузочные вирусы* инфицируют загрузочные секторы дисков и разделов, а также главные загрузочные секторы жестких дисков. Они занимают очень мало памяти и остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными механизмами защиты от обнаружения, которые постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- *Шифрованные вирусы* шифруют свой код при каждом новом инфицировании, что затрудняет его обнаружение в файле, памяти или загрузочном секторе. Каждый экземпляр таких вирусов содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры.
- *Полиморфные вирусы* используют помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур.
- *Стелс-вирусы* (вирусы-невидимки) предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (например, низкоуровневый типа языка ассемблера или высокоуровневый типа языка Go) и по инфицируемым ими операционным системам.

Компьютерные черви

Как и вирусы, программы типа *«компьютерный червь»* способны создавать свои копии, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего во вложениях сообщений электронной почты или через интернет) и рассылает свои функциональные копии на другие компьютеры. Черви используют действия пользователя, либо распространяются автоматически.

Черви не обязательно целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в оперативную память компьютера и «догружает» по сети непосредственно само тело червя в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс оперативной памяти). Если же в системе оказывается тело червя, то справиться с ним может только антивирус.

За счет интенсивного распространения черви способны вывести из строя целые сети, даже если они не несут никакой полезной нагрузки (не наносят прямой вред системе).

В компании «Доктор Веб» червей классифицируют по способу (среде) распространения:

- *Сетевые черви* распространяются посредством различных сетевых протоколов и протоколов обмена файлами.
- *Почтовые черви* распространяются посредством почтовых протоколов (POP3, SMTP и т. д.).
- *Чат-черви* распространяются, используя популярные системы мгновенного обмена сообщениями (ICQ, IM, IRC и т. д.).

Троянские программы

Вредоносные программы этого типа не способны к саморепликации. Троянские программы выдают себя за одну из популярных программ и выполняют ее функции (или имитируют исполнение этих функций), одновременно производя какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т. д.), либо делая возможным несанкционированное использование компьютера злоумышленником, например, для нанесения вреда третьим лицам.

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловых сервера, записываются на носители информации или пересылаются в виде вложений в сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.

Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполняться другими типами угроз, принято приписывать только троянским программам. Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- *Бэкдоры* — это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы.
- *Руткиты* предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, каталоги, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в составе другой вредоносной программы. По принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (*User Mode Rootkits — UMR*), и руткиты, работающие в режиме ядра (перехват функций на уровне ядра системы, что значительно усложняет обнаружение и обезвреживание) (*Kernel Mode Rootkits — KMR*).
- *Клавиатурные перехватчики* (*кейлоггеры*) используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действий является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т. д.).
- *Кликеры* переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь перенаправляется с целью увеличения рекламного трафика сайтов или для организации распределенных атак отказа в обслуживании (DDoS-атак).
- *Прокси-трояны* предоставляют злоумышленнику анонимный выход в интернет через компьютер жертвы.

Кроме перечисленных выше, троянские программы могут выполнять и другие вредоносные действия, например, изменять стартовую страницу в веб-браузере или удалять определенные файлы. Однако такие действия могут выполняться и угрозами других типов (например, вирусами и червями).

Программы взлома

Программы взлома созданы с целью помочь взломщику. Наиболее распространенным видом подобных программ являются сканеры портов, которые позволяют обнаруживать уязвимости в межсетевых экранах (файерволах, брандмауэрах) и других компонентах, обеспечивающих безопасность компьютера. Кроме хакеров, такими инструментами могут пользоваться администраторы для проверки надежности своих сетей. Иногда к программам взлома относят программы, использующие методы социальной инженерии (элементы социотехники).

Рекламные программы

Чаще всего под этим термином понимают программный код, встроенный в различное бесплатное программное обеспечение, при использовании которого пользователю принудительно показывается реклама. Но иногда такой код может скрытно распространяться посредством других вредоносных программ и демонстрировать рекламу, например, в веб-браузерах. Зачастую рекламные программы работают на основании данных, собранных шпионскими программами.

Программы-шутки

Это тип вредоносных программ, которые, как и рекламные программы, не наносят прямого вреда системе. Чаще всего они генерируют сообщения о несуществующих ошибках и угрожают действиями, которые могут привести к повреждению данных. Их основной функцией является запугивание пользователя, либо навязчивое его раздражение.

Программы дозвона

Это специальные компьютерные программы, разработанные для сканирования некоего диапазона телефонных номеров для нахождения такого, на который ответит модем. В дальнейшем злоумышленники используют найденные номера для накручивания оплаты за телефон или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам.

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться злоумышленниками или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-серверы и т. д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут относиться к любому типу компьютерных угроз (возможно, даже неизвестному для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать

в карантин, а также отправлять на анализ специалистам антивирусной лаборатории «Доктор Веб».

10.2. Приложение Б. Устранение компьютерных угроз

В этом разделе

- Методы обнаружения угроз
  - Сигнатурный анализ
  - Origins Tracing™
  - Эмуляция исполнения
  - Эвристический анализ
  - Облачные технологии обнаружения угроз
- Действия с угрозами

Все антивирусные продукты, разработанные компанией «Доктор Веб», применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.

Методы обнаружения угроз

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных угроз. Сигнатурой называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в вирусных базах Dr.Web составлены таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Origins Tracing™

Это уникальная технология Dr.Web, которая позволяет определять новые и модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы инфицирования и нанесения ущерба. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения Dr.Web от таких угроз, как троянская программа-вымогатель Trojan.Encoder.18 (также известная под названием gpcode). Кроме того, использование технологии Origins Tracing™ позволяет значительно снизить количество ложных

срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing™, добавляется постфикс `.Origin`.

Эмуляция исполнения

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и шифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи *эмулятора* — программной модели процессора и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (*буфером эмуляции*). При этом инструкции не передаются на центральный процессор для реального исполнения. Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.

Эвристический анализ

Работа эвристического анализатора основывается на наборе *эвристик* — предположений о характерных признаках как вредоносного, так и безопасного исполняемого кода, статистическая значимость которых подтверждена опытным путем. Каждый признак кода имеет определенный *вес* (т. е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.

Эвристический анализатор также использует технологию FLY-CODE™ — универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке запакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, запакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому

объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Во время любой из проверок все компоненты антивирусных продуктов Dr.Web используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты антивирусной лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.

Облачные технологии обнаружения угроз

Облачные методы обнаружения позволяют проверить любой объект (файл, приложение, расширение для браузера и т. п.) по *хеш-сумме*. Она представляет собой уникальную последовательность цифр и букв заданной длины. При анализе по хеш-сумме объекты проверяются по существующей базе и затем классифицируются на категории: чистые, подозрительные, вредоносные и т. д.

Подобная технология оптимизирует время проверки файлов и экономит ресурсы устройства. Благодаря тому, что анализируется не сам объект, а его уникальная хеш-сумма, решение выносится практически моментально. При отсутствии подключения к серверам Dr.Web Cloud, файлы проверяются локально, а облачная проверка возобновляется при восстановлении связи.

Таким образом, облачный сервис Dr.Web Cloud собирает информацию от многочисленных пользователей и оперативно обновляет данные о ранее неизвестных угрозах, тем самым повышая эффективность защиты устройств.

Действия с угрозами

В продуктах Dr.Web реализована возможность применять определенные действия к обнаруженным объектам для обезвреживания компьютерных угроз. Пользователь может оставить автоматически применяемые к определенным типам угроз действия, заданные по умолчанию, изменить их или выбирать нужное действие для каждого обнаруженного объекта отдельно. Ниже приведен список доступных действий. В скобках указан параметр, обозначающий соответствующее действие и используемый в объединенном конфигурационном файле и командах утилиты Dr.Web Ctl.

- **Сообщать** (`REPORT`) — уведомить о наличии угрозы, но ничего не делать с инфицированным объектом.
- **Игнорировать** (`PASS`) — пропустить обнаруженную угрозу, не предпринимая никаких действий.

- **Блокировать** (BLOCK) — заблокировать все виды доступа к инфицированному файлу (действие может быть доступно не для всех компонентов).
- **Лечить** (CURE) — попытаться вылечить инфицированный объект, удалив из него вредоносное содержимое, и оставив в целости полезное содержимое.



Это действие применимо не ко всем видам угроз.

- **В карантин** (QUARANTINE) — переместить инфицированный объект (если он допускает эту операцию) в специальный каталог карантина с целью его изоляции.
- **Удалить** (DELETE) — безвозвратно удалить инфицированный объект.



Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т. п.), вместо удаления выполняется перемещение контейнера в карантин.

10.3. Приложение B. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

1. Ознакомьтесь с последними версиями описаний и руководств.
2. Прочитайте раздел часто задаваемых вопросов.
3. Посетите форумы компании «Доктор Веб».

Если после этого не удалось решить проблему, заполните веб-форму в соответствующей секции раздела официального сайта, чтобы связаться со службой технической поддержки компании «Доктор Веб».

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте.

Для упрощения работы службы технической поддержки по анализу возникшей у вас проблемы рекомендуется предварительно сформировать пакет информации об установленном у вас продукте, его настройках и системном окружении. Для этого предназначена специализированная утилита, входящая в состав Dr.Web Server Security Suite.

Для сбора информации для службы технической поддержки введите команду:

- для GNU/Linux:

```
# /opt/drweb.com/bin/support-report.sh <путь к файлу>
```

- для FreeBSD:

```
# /usr/local/libexec/drweb.com/bin/support-report.sh <путь к файлу>
```

где <*путь к файлу*> — путь к архиву в формате `.tgz`, в котором будет сохранена отладочная информация о продукте и системном окружении, например, `/tmp/report.tgz`. Уже имеющиеся файлы не перезаписываются. Если путь не указан, то архив будет сохранен в каталоге суперпользователя, запустившего утилиту (например, `/root`), и будет называться следующим образом:

```
drweb.report.<timestamp>.tgz
```

где <*timestamp*> — полная метка времени создания отчета, включая миллисекунды, например: 20190618151718.23625.



Утилиту для сбора информации для службы технической поддержки необходимо запускать с правами суперпользователя (*root*). Для получения прав суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

В процессе работы утилита собирает и упаковывает в архив следующую информацию:

- информация об ОС (название, архитектура, вывод команды `uname -a`);
- список установленных в системе пакетов, в том числе пакетов «Доктор Веб»;
- содержимое журналов:
  - журналы Dr.Web Server Security Suite (если настроены для отдельных компонентов);
  - журнал, ведущийся демоном журналирования `syslog` (`/var/log/syslog`, `/var/log/messages`);
  - журнал системного пакетного менеджера (`apt`, `yum` и т. п.);
  - журнал `dmesg`;
- результаты запуска команд `df`, `ip a` (`ifconfig -a`), `ldconfig -p`, `iptables-save`, `nft export xml`.
- информация о настройках и конфигурации Dr.Web Server Security Suite:
  - перечень загруженных вирусных баз (`drweb-ctl baseinfo -l`);
  - перечень файлов из каталогов Dr.Web Server Security Suite и их MD5-хеши;
  - версия и MD5-хеш файла антивирусного ядра Dr.Web Virus-Finding Engine;
  - информация о пользователе и разрешениях, извлеченная из ключевого файла, если Dr.Web Server Security Suite работает не в режиме централизованной защиты.

10.4. Приложение Г. Конфигурационный файл Dr.Web Server Security Suite

Параметрами конфигурации всех компонентов Dr.Web Server Security Suite управляет координирующий демон управления конфигурацией Dr.Web ConfigD. Измененные параметры конфигурации всех компонентов хранятся в едином файле `drweb.ini`, который по умолчанию располагается в каталоге `/etc/opt/drweb.com/` для GNU/Linux или `/usr/local/etc/drweb.com/` для FreeBSD.



В текстовом файле конфигурации хранятся значения только тех параметров, установленные значения которых не совпадают со значением по умолчанию. Если параметр отсутствует в файле конфигурации, то это означает, что он имеет значение по умолчанию.

Чтобы просмотреть перечень всех параметров, доступных для изменения, включая те, которые отсутствуют в конфигурационном файле, так как имеют значения по умолчанию, выполните команду:

```
$ drweb-ctl cfshow
```

Изменить значение любого параметра можно двумя способами:

- Выполнив команду:

  ```
  # drweb-ctl cfset <секция>.<параметр> <новое значение>
  ```

  Для выполнения этой команды утилита управления Dr.Web Ctl должна запускаться от имени суперпользователя (пользователя *root*). Для получения прав суперпользователя используйте команду `su` или `sudo`.

  Синтаксис команд `cfshow` и `cfset` утилиты Dr.Web Ctl (модуль `drweb-ctl`) подробнее описан в разделе Dr.Web Ctl.

- Задав этот параметр в конфигурационном файле (отредактировав файл в любом текстовом редакторе) и перезапустив конфигурацию Dr.Web Server Security Suite для применения внесенных в файл изменений с помощью команды:

  ```
  # drweb-ctl reload
  ```

10.4.1. Структура файла

Конфигурационный файл сформирован в соответствии с правилами, приведенными ниже.

- Содержимое файла разбито на последовательность именованных секций. Возможные имена секций жестко заданы и не могут быть произвольными. Имя секции указывается в квадратных скобках и совпадает с именем компонента Dr.Web Server Security Suite, использующего параметры из этой секции (за исключением секции

`[Root]`, в которой хранятся параметры демона управления конфигурацией Dr.Web ConfigD).

- Символы `;` или `#` в начале строк конфигурационного файла обозначают комментарий. Такие строки пропускаются компонентами Dr.Web Server Security Suite при чтении параметров из конфигурационного файла.
- В одной строке файла содержится только один параметр:

```
<имя параметра> = <значение>
```

- Возможные имена параметров жестко заданы и не могут быть произвольными.
- Все имена секций и параметров регистронезависимы. Значения параметров, за исключением имен каталогов и файлов в путях (для Unix-подобных ОС), также регистронезависимы.
- Значения параметров в конфигурационном файле должны быть заключены в кавычки в том случае, если они содержат пробелы.
- Некоторые параметры могут иметь несколько значений, в этом случае значения параметра разделяются запятой или значение параметра задается несколько раз в разных строках конфигурационного файла. При перечислении значений параметра через запятую пробелы между значением и запятой, если встречаются, игнорируются. Если пробел является частью значения параметра, все значение заключается в кавычки.

  Параметру можно присвоить несколько значений:

  - перечислив их через запятую:

    ```
    Parameter = "Value1", "Value2","Value 3"
    ```

  - в виде последовательности строк:

    ```
    Parameter = Value2
    Parameter = Value1
    Parameter = "Value 3"
    ```

  Порядок значений параметра также несущественен.



Пути к файлам всегда заключаются в кавычки, если они перечисляются через запятую, например:

```
ExcludedPaths = "/etc/file1", "/etc/file2"
```

Описание секций конфигурационного файла приведено в описании использующих его компонентов Dr.Web Server Security Suite.

10.4.2. Типы параметров

Параметры конфигурации могут принадлежать к следующим типам:

1. *Адрес* — адрес сетевого соединения в виде пары *<IPv4-адрес>:<порт>* или *<IPv6-адрес>:<порт>*. Значение IPv6-адреса указывается в квадратных скобках. В некоторых случаях порт может быть опущен (в каждом случае это указывается в описании параметра).

2. *Логический* — параметр-флаг, принимающий значения `On`, `Yes`, `True` (параметр включен) и `Off`, `No`, `False` (параметр выключен).
3. *Целое число* — неотрицательное целое число.
4. *Дробное число* — в качестве значения параметра может быть указано неотрицательное число, содержащее дробную часть.
5. *Интервал времени* — в качестве значения параметра указывается длина временного интервала, состоящего из целого неотрицательного числа и буквы-суффикса, указывающего заданную единицу измерения. Могут быть использованы суффиксы, задающие единицы измерения:
   - `w` — недели (`1w` = `7d`);
   - `d` — сутки (`1d` = `24h`);
   - `h` — часы (`1h` = `60m`);
   - `m` — минуты (`1m` = `60s`);
   - `s` или без суффикса — секунды.

   Для временного интервала, заданного в секундах, можно указать миллисекунды после точки (не более трех знаков, например, `0.5s` — 500 миллисекунд). В записи одного временного интервала можно использовать совокупность интервалов, измеренных в различных единицах, в этом случае он будет образовываться их суммой (в реальности в параметрах конфигурации всегда сохраняется количество миллисекунд, образующих указанный временной интервал).

   В общем виде любой интервал времени может быть представлен выражением N_1wN_2dN_3hN_4mN_5[.N_6]s, где N_1, ..., N_6 — число соответствующих единиц времени, включенных в данный интервал. Например, год (как 365 суток) можно представить следующим образом (все записи эквивалентны): `365d`, `52w1d`, `52w24h`, `51w7d24h`, `51w7d23h60m`, `8760h`, `525600m`, `31536000s`.

   Примеры задания интервала длиной в 30 минут, 2 секунды, 500 миллисекунд:

   - в файле конфигурации:

   ```
   UpdateInterval = 30m2.5s
   ```

   - с помощью команды `drweb-ctl cfset`:

   ```
   # drweb-ctl cfset Update.UpdateInterval 1802.5s
   ```

   - задание через параметр командной строки (например, для сканирующего ядра):
     - для GNU/Linux:

     ```
     # /opt/drweb.com/bin/drweb-se <сокет> --WatchdogInterval 1802.5
     ```

     - для FreeBSD:

     ```
     # /usr/local/libexec/drweb.com/bin/drweb-se <сокет> --WatchdogInterval 1802.5
     ```

6. *Размер* — в качестве значения параметра указывается размер какого-либо объекта (файла, буфера, кеша и т. п.), состоящий из целого неотрицательного числа и суффикса, указывающего заданную единицу измерения. Могут быть использованы суффиксы, задающие единицы размера:
   - `GB` — гигабайты (`1GB` = `1024MB`);
   - `MB` — мегабайты (`1MB` = `1024KB`);
   - `KB` — килобайты (`1KB` = `1024B`);
   - `B` — байты.

   Если суффикс опущен, считается, что размер задан в байтах. В записи одного размера можно использовать совокупность размеров, измеренных в различных единицах, в этом случае он будет образовываться их суммой (фактически, в параметрах конфигурации размер всегда сохраняется в байтах).
7. *Путь к каталогу (файлу)* — в качестве значения параметра выступает строка, представляющая собой допустимый путь к каталогу (файлу).

   Путь к файлу должен заканчиваться именем файла.

   В Unix-подобных операционных системах имена каталогов и файлов регистрозависимы. Если это не оговорено непосредственно в описании параметра, в качестве пути нельзя использовать маски, содержащие специальные символы (`?`, `*`).

8. *Уровень подробности* — параметр задает уровень подробности записи в журнал для компонента Dr.Web Server Security Suite. Возможные значения:
   - `Debug` — самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация.
   - `Info` — выводятся все сообщения.
   - `Notice` — выводятся сообщения об ошибках, предупреждения, уведомления.
   - `Warning` — выводятся сообщения об ошибках и предупреждения.
   - `Error` — выводятся только сообщения об ошибках.
9. *Тип журнала* — параметр определяет способ ведения журнала компонентом Dr.Web Server Security Suite. Возможные значения:
   - `Stderr[:ShowTimestamp]` — сообщения будут выводиться в стандартный поток ошибок *stderr*. Данное значение может быть использовано *только* в настройках демона управления конфигурацией. При этом, если он работает в фоновом режиме («*daemonized*»), т. е. запущен с указанием параметра `-d`, это значение *не может* быть использовано, поскольку компоненты, работающие в фоновом режиме, не имеют доступа к потокам ввода/вывода терминала). Дополнительный параметр `ShowTimestamp` предписывает добавлять к каждому сообщению метку времени.
   - `Auto` — сообщения для сохранения в журнал передаются демону управления конфигурацией Dr.Web ConfigD, который сохраняет их в единое место в

соответствии с собственными настройками (параметр `Log` в секции `[Root]`). Данное значение определено для всех компонентов, *кроме демона управления конфигурацией*, и используется как значение по умолчанию.

- `Syslog[:<facility>]` — сообщения будут передаваться компонентом системной службе журналирования `syslog`.
- Дополнительная метка *<facility>* используется для указания типа журнала, в котором `syslog` будет сохранять сообщения. Возможные значения:
  - `Daemon` — сообщения демонов,
  - `User` — сообщения пользовательских процессов,
  - `Mail` — сообщения почтовых программ,
  - `Local0` — сообщения локальных процессов 0,
  - ...
  - `Local7` — сообщения локальных процессов 7.
- *<путь к файлу>* — сообщения будут сохраняться компонентом непосредственно в указанный файл журнала.

Примеры задания параметра:

- в файле конфигурации:

```
Log = Stderr:ShowTimestamp
```

- с помощью команды `drweb-ctl cfset`:

```
# drweb-ctl cfset Root.Log /tmp/log
```

- задание через параметр командной строки (например, для сканирующего ядра):
  - для ОС семейства GNU/Linux:

    ```
    # /opt/drweb.com/bin/drweb-se <сокет> --Log Syslog:DAEMON
    ```

  - для ОС FreeBSD:

    ```
    # /usr/local/libexec/drweb.com/bin/drweb-se <сокет> --Log Syslog:DAEMON
    ```

10. *Действие* — действие компонента Dr.Web Server Security Suite при обнаружении угроз определенного типа или при возникновении какого-либо другого события. Возможные значения:
    - **Сообщать** (`REPORT`) — только сформировать уведомление об угрозе, не предпринимая никаких других действий;
    - **Блокировать** (`BLOCK`) — оставить файл неизменным, но заблокировать все виды доступа к нему (действие может быть доступно не для всех компонентов);
    - **Лечить** (`CURE`) — попытаться выполнить лечение (удалить из тела файла только вредоносное содержимое);
    - **В карантин** (`QUARANTINE`) — переместить инфицированный файл в карантин;
    - **Удалить** (`DELETE`) — удалить инфицированный файл.



Некоторые из действий могут быть неприменимы в некоторых случаях (например, для события «Ошибка сканирования» неприменимо действие `CURE`). Перечень разрешенных действий всегда указывается в описании каждого параметра, имеющего тип *действие*.

Прочие типы параметров и их возможные значения указаны непосредственно в описании параметров конфигурации.

10.5. Приложение Д. Генерация сертификатов SSL

Для компонентов Dr.Web Server Security Suite, использующих для обмена данными защищенный канал передачи данных SSL/TLS и основанные на нем прикладные протоколы, такие как HTTPS, LDAPS, SMTPS и т. п., необходимо обеспечить наличие закрытых ключей SSL и соответствующих им сертификатов. Для некоторых компонентов ключи и сертификаты генерируются автоматически, а для других они должны быть предоставлены пользователем Dr.Web Server Security Suite. Все компоненты используют сертификаты, представленные в формате PEM.

Для генерации закрытых ключей и сертификатов, используемых для соединений через SSL/TLS, в том числе для удостоверяющих сертификатов центра сертификации (ЦС) и для подписанных сертификатов, можно использовать утилиту командной строки `openssl` (входит в состав криптографического пакета OpenSSL).

Рассмотрим последовательность действий, необходимых для создания закрытого ключа и соответствующего ему сертификата SSL, а также сертификата SSL, подписанного удостоверяющим сертификатом ЦС.

Чтобы сгенерировать закрытый ключ SSL и сертификат

1. Для генерации закрытого ключа (алгоритм RSA, длина ключа — 2048 бит) выполните команду:

   ```
   $ openssl genrsa -out keyfile.key 2048
   ```

   Если требуется защитить ключ паролем, дополнительно используйте опцию `-des3`. Сгенерированный ключ находится в файле `keyfile.key` в текущем каталоге.

   Для просмотра сгенерированного ключа выполните команду:

   ```
   $ openssl rsa -noout -text -in keyfile.key
   ```

2. Для генерации сертификата на указанный срок на основании имеющегося закрытого ключа (в данном примере — на 365 суток) выполните команду:

   ```
   $ openssl req -new -x509 -days 365 -key keyfile.key -out certificate.crt
   ```

   Эта команда запросит данные, идентифицирующие сертифицируемый объект (такие как имя, организация и т. п.). Сгенерированный сертификат будет помещен в файл `certificate.crt`.

   Для проверки содержимого сгенерированного сертификата выполните команду:

   ```
   $ openssl x509 -noout -text -in certificate.crt
   ```

Чтобы зарегистрировать сертификат в качестве доверенного сертификата ЦС

1. Переместите или скопируйте файл сертификата в системный каталог доверенных сертификатов (в Debian или Ubuntu — `/etc/ssl/certs`).

2. Создайте в каталоге доверенных сертификатов символическую ссылку на сертификат, именем которой будет являться хеш сертификата.
3. Переиндексируйте содержимое системного каталога сертификатов.

Приведенный ниже пример выполняет все эти три действия. Предполагается, что текущим каталогом является системный каталог доверенных сертификатов `/etc/ssl/certs`, а сертификат, который регистрируется в качестве доверенного, располагается в файле `/home/user/ca.crt`:

```
# cp /home/user/ca.crt .
# ln -s ca.crt `openssl x509 -hash -noout -in ca.crt`.0
# c_rehash /etc/ssl/certs
```

Чтобы создать подписанный сертификат

1. Сгенерируйте файл-запрос на подписание сертификата *(Certificate Signing Request — CSR)* на основании имеющегося закрытого ключа. Если ключа нет, сгенерируйте его.

   Запрос на подписание создается командой:

   ```
   $ openssl req -new -key keyfile.key -out request.csr
   ```

   Эта команда, так же как и команда создания сертификата, запрашивает данные, идентифицирующие сертифицируемый объект. Здесь `keyfile.key` — имеющийся файл закрытого ключа. Полученный запрос будет сохранен в файл `request.csr`.

   Для проверки результата создания запроса выполните команду:

   ```
   $ openssl req -noout -text -in request.csr
   ```

2. Для создания подписанного сертификата на основании запроса и имеющегося сертификата ЦС выполните команду:

   ```
   $ openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -set_serial 01 -in request.csr
   -out sigcert.crt
   ```

   Для создания подписанного сертификата нужно иметь три файла: файл корневого сертификата `ca.crt` и его закрытый ключ `ca.key` (в качестве `ca.crt` и `ca.key` можно использовать сертификат `certificate.crt` и ключ `keyfile.key`, тогда полученный сертификат будет самоподписанными), а также файл запроса на подписание сертификата `request.csr`. Созданный подписанный сертификат будет сохранен в файл `sigcert.crt`.

   Для проверки результата выполните команду:

   ```
   $ openssl x509 -noout -text -in sigcert.crt
   ```

Повторите процедуру создания ключа и сертификата (или подписанного сертификата, в зависимости от необходимости) столько раз, сколько уникальных сертификатов вам требуется. Например, с точки зрения соображений безопасности, каждый агент распределенной проверки файлов Dr.Web Network Checker, входящий в сканирующий кластер, должен иметь собственную пару ключ/сертификат.

Преобразование подписанного сертификата

Некоторые браузеры или почтовые клиенты могут потребовать преобразования подписанного сертификата, используемого для удостоверения личности, в формат PKCS12.

Указанное преобразование выполняется командой:

```
# openssl pkcs12 -export -in sigcert.crt -out sigcert.pfx -inkey keyfile.key
```

Здесь sigcert.crt — имеющийся файл подписанного сертификата, а keyfile.key — файл соответствующего ему закрытого ключа. Полученный преобразованный сертификат будет сохранен в файл sigcert.pfx.

10.6. Приложение E. Описание известных ошибок

В этом разделе

- Рекомендации по идентификации ошибок
- Коды ошибок
- Ошибки без кода

Если у вас возникла ошибка, описание которой отсутствует в данном разделе, обратитесь в техническую поддержку. Будьте готовы сообщить код ошибки и описать обстоятельства ее возникновения.

Рекомендации по идентификации ошибок

- Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.
- Для облегчения идентификации ошибки рекомендуется настроить вывод журнала в отдельный файл и разрешить вывод расширенной отладочной информации. Для этого выполните команды:

```
# drweb-ctl cfset Root.Log <путь к файлу журнала>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- Для возврата настроек ведения журнала по умолчанию выполните команды:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

Коды ошибок

Сообщение об ошибке: *Error on monitor channel (Ошибка связи с монитором)*

Код ошибки: `x1`

Внутреннее обозначение ошибки: `EC_MONITOR_IPC_ERROR`

Описание: Ошибка связи одного или нескольких компонентов с демоном управления конфигурацией Dr.Web ConfigD.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Перезапустите демон управления конфигурацией:

   ```
   # service drweb-configd restart
   ```

2. Убедитесь, что в системе установлен, настроен и корректно функционирует механизм аутентификации PAM. При необходимости установите и настройте его (за подробностями обратитесь к руководствам по администрированию вашего дистрибутива ОС).

3. Если перезапуск демона управления конфигурацией при корректно настроенном PAM не помогает, попробуйте сбросить настройки Dr.Web Server Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

4. Если демон управления конфигурацией запустить не удается, попробуйте переустановить пакет `drweb-configd`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Operation is already in progress (Операция уже выполняется)*

Код ошибки: `x2`

Внутреннее обозначение ошибки: `EC_ALREADY_IN_PROGRESS`

Описание: Запрошенная операция уже выполняется.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Подождите завершения операции и при необходимости повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Operation is in pending state (Операция ожидает выполнения)*

Код ошибки: `x3`

Внутреннее обозначение ошибки: `EC_IN_PENDING_STATE`

Описание: Запрошенная операция ожидает выполнения (возможно, в текущий момент устанавливается сетевое соединение или происходит загрузка и инициализация какого-либо компонента, требующая продолжительного времени).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Подождите начала выполнения операции и при необходимости повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Interrupted by user (Прервано пользователем)*

Код ошибки: `x4`

Внутреннее обозначение ошибки: `EC_INTERRUPTED_BY_USER`

Описание: Действие было прервано пользователем (возможно, оно выполнялось слишком долго).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Operation canceled (Операция отменена)*

Код ошибки: `x5`

Внутреннее обозначение ошибки: `EC_CANCELED`

Описание: Действие было отменено.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *IPC connection terminated (Соединение IPC разорвано)*

Код ошибки: `x6`

Внутреннее обозначение ошибки: `EC_LINK_DISCONNECTED`

Описание: IPC-соединение с одним из компонентов Dr.Web Server Security Suite разорвано (возможно, компонент завершил свою работу из-за простоя или по команде пользователя).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Если операция не была завершена, повторите ее позже. В противном случае разрыв соединения не является ошибкой.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid IPC message size (Недопустимый размер сообщения IPC)*

Код ошибки: `x7`

Внутреннее обозначение ошибки: `EC_BAD_MESSAGE_SIZE`

Описание: В процессе обмена данными между компонентами получено сообщение недопустимого размера.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Server Security Suite:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid IPC message format (Недопустимый формат сообщения IPC)*

Код ошибки: `x8`

Внутреннее обозначение ошибки: `EC_BAD_MESSAGE_FORMAT`

Описание: В процессе обмена данными между компонентами получено сообщение недопустимого формата.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Server Security Suite:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not ready (Не готов)*

Код ошибки: `x9`

Внутреннее обозначение ошибки: `EC_NOT_READY`

Описание: Требуемое действие не может быть выполнено, потому что запрошенный компонент или устройство еще не инициализированы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Component is not installed (Компонент не установлен)*

Код ошибки: `x10`

Внутреннее обозначение ошибки: `EC_NOT_INSTALLED`

Описание: Компонент, необходимый для выполнения требуемой функции, не установлен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Установите или переустановите требуемый компонент. Если неизвестно, какой именно компонент необходим, попробуйте это выяснить, ознакомившись с содержимым журнала.
2. Если установка или переустановка требуемого компонента не помогла, попробуйте переустановить Dr.Web Server Security Suite.

Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unexpected IPC message (Неожиданное сообщение IPC)*

Код ошибки: `x11`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_MESSAGE`

Описание: В процессе обмена данными между компонентами получено недопустимое сообщение.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Server Security Suite, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *IPC protocol violation (Нарушение протокола IPC)*

Код ошибки: `x12`

Внутреннее обозначение ошибки: `EC_PROTOCOL_VIOLATION`

Описание: В процессе обмена данными между компонентами произошло нарушение протокола.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Server Security Suite, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Subsystem state is unknown (Неизвестное состояние подсистемы)*

Код ошибки: `x13`

Внутреннее обозначение ошибки: `EC_UNKNOWN_STATE`

Описание: Подсистема Dr.Web Server Security Suite, необходимая для выполнения операции, находится в неизвестном состоянии.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web Server Security Suite, выполнив команду:

   ```
   # service drweb-configd restart
   ```

   после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Path must be absolute (Путь должен быть абсолютным)*

Код ошибки: `x20`

Внутреннее обозначение ошибки: `EC_NOT_ABSOLUTE_PATH`

Описание: Указан относительный путь к файлу или каталогу вместо абсолютного.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Замените относительный путь к файлу или каталогу на абсолютный и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not enough memory (Недостаточно памяти для завершения операции)*

Код ошибки: `x21`

Внутреннее обозначение ошибки: `EC_NO_MEMORY`

Описание: Недостаточно памяти для выполнения операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Попробуйте увеличить объем памяти, доступной процессам Dr.Web Server Security Suite (например, изменив лимиты при помощи команды `ulimit`), перезапустить Dr.Web Server Security Suite и повторить операцию.

В некоторых случаях системный сервис `systemd` может игнорировать заданные изменения лимита. В этом случае отредактируйте (или создайте, при его отсутствии) файл `/etc/systemd/system/drweb-configd.service.d/limits.conf`, указав в нем измененное значение лимита, например:

```
[Service]
LimitDATA=32767
```

С перечнем доступных лимитов `systemd` можно ознакомиться, выполнив команду `man systemd.exec`.

Для перезапуска Dr.Web Server Security Suite выполните команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *IO error (Ошибка ввода-вывода)*

Код ошибки: `x22`

Внутреннее обозначение ошибки: `EC_IO_ERROR`

Описание: Произошла ошибка ввода/вывода (например, дисковое устройство еще не инициализировано или раздел файловой системы более не доступен).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обеспечьте доступность требуемого устройства ввода/вывода или раздела файловой системы и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *No such file or directory (Нет такого файла или каталога)*

Код ошибки: `x23`

Внутреннее обозначение ошибки: `EC_NO_SUCH_ENTRY`

Описание: Попытка обращения к несуществующему файлу или каталогу.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного пути. При необходимости исправьте путь и повторите

операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Permission denied (Доступ запрещен)*

Код ошибки: `x24`

Внутреннее обозначение ошибки: `EC_PERMISSION_DENIED`

Описание: Недостаточно прав для доступа к указанному файлу или каталогу.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного пути и наличие необходимых прав у компонента. Если доступ к объекту запрещен, измените права доступа к нему или повысьте права компонента и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not a directory (Не каталог)*

Код ошибки: `x25`

Внутреннее обозначение ошибки: `EC_NOT_A_DIRECTORY`

Описание: Указанный объект файловой системы не является каталогом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность пути к объекту. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Data file corrupted (Файл данных поврежден)*

Код ошибки: `x26`

Внутреннее обозначение ошибки: `EC_DATA_CORRUPTED`

Описание: Запрашиваемые данные повреждены.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно

просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web Server Security Suite:

   ```
   # service drweb-configd restart
   ```

   после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *File already exists (Файл уже существует)*

Код ошибки: `x27`

Внутреннее обозначение ошибки: `EC_FILE_EXISTS`

Описание: Файл с указанным именем уже существует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность написания имени файла. При необходимости исправьте его и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Read-only file system (Файловая система только для чтения)*

Код ошибки: `x28`

Внутреннее обозначение ошибки: `EC_READ_ONLY_FS`

Описание: Файловая система доступна только для чтения.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность пути к объекту. Исправьте путь так, чтобы он указывал на раздел файловой системы, доступный для записи, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Network error (Ошибка сети)*

Код ошибки: `x29`

Внутреннее обозначение ошибки: `EC_NETWORK_ERROR`

Описание: Ошибка сети (возможно, внезапно перестал отвечать удаленный узел или не удается установить соединение).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not a drive (Не дисковое устройство)*

Код ошибки: `x30`

Внутреннее обозначение ошибки: `EC_NOT_A_DRIVE`

Описание: Производится попытка обращения к устройству ввода/вывода, которое не является дисковым устройством.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного имени устройства. Исправьте путь так, чтобы он вел к дисковому устройству, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unexpected EOF (Неожиданный конец файла)*

Код ошибки: `x31`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_EOF`

Описание: При чтении данных неожиданно был достигнут конец файла.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного имени файла. Если нужно, исправьте путь так, чтобы он вел к правильному файлу, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *File was changed (Файл был изменен)*

Код ошибки: `x32`

Внутреннее обозначение ошибки: `EC_FILE_WAS_CHANGED`

Описание: Проверяемый файл был изменен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите операцию сканирования.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not a regular file (Объект не является файлом)*

Код ошибки: `x33`

Внутреннее обозначение ошибки: `EC_NOT_A_REGULAR_FILE`

Описание: Запрашиваемый объект файловой системы не является регулярным файлом (он может быть каталогом, сокетом или другим объектом).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного имени файла. Если нужно, исправьте путь так, чтобы он вел к регулярному файлу, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Name already in use (Имя уже используется)*

Код ошибки: `x34`

Внутреннее обозначение ошибки: `EC_NAME_ALREADY_IN_USE`

Описание: Объект с указанным именем уже существует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Host is offline (Хост отключен)*

Код ошибки: `x35`

Внутреннее обозначение ошибки: `EC_HOST_OFFLINE`

Описание: Удаленный узел недоступен по сети.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте доступность требуемого узла сети. При необходимости исправьте адрес узла сети и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Resource limit reached (Достигнут предел использования ресурса)*

Код ошибки: `x36`

Внутреннее обозначение ошибки: `EC_LIMIT_REACHED`

Описание: Достигнут предел использования ресурса.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте доступность требуемого ресурса. При необходимости увеличьте лимит на использование ресурса и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Mounting points are different (Различные точки монтирования)*

Код ошибки: `x37`

Внутреннее обозначение ошибки: `EC_CROSS_DEVICE_LINK`

Описание: Восстановление файла предполагает перемещение между двумя точками монтирования.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Выберите другой путь для восстановления файла и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unpacking error (Ошибка распаковки)*

Код ошибки: `x38`

Внутреннее обозначение ошибки: `EC_UNPACKING_ERROR`

Описание: Не удалось распаковать архив (возможно, он защищен паролем или поврежден).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Убедитесь, что файл не поврежден. Если архив защищен паролем, снимите защиту, указав правильный пароль, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Virus base corrupted (Вирусная база повреждена)*

Код ошибки: `x40`

Внутреннее обозначение ошибки: `EC_BASE_CORRUPTED`

Описание: Вирусные базы повреждены.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса

управления.

- Также вы можете воспользоваться утилитой управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Non-supported virus database version (Неподдерживаемая версия вирусных баз)*

Код ошибки: `x41`

Внутреннее обозначение ошибки: `EC_OLD_BASE_VERSION`

Описание: Вирусные базы предназначены для старой версии программы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Также вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir -r
   ```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;

- или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Empty virus database (Вирусная база пуста)*

Код ошибки: `x42`

Внутреннее обозначение ошибки: `EC_EMPTY_BASE`

Описание: Вирусная база пуста.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Также вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir -r
   ```
2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

   ```
   $ drweb-ctl update
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Object cannot be cured (Объект не может быть вылечен)*

Код ошибки: `x43`

Внутреннее обозначение ошибки: `EC_CAN_NOT_BE_CURED`

Описание: Действие **Лечить** было применено к неизлечимому объекту.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно

просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Выберите действие, допустимое для данного объекта, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Non-supported virus database combination (Неподдерживаемая комбинация вирусных баз)*

Код ошибки: `x44`

Внутреннее обозначение ошибки: `EC_INVALID_BASE_SET`

Описание: Несовместимые вирусные базы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Также вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir -r
   ```
2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Scan limit reached (Достигнут предел проверки)*

Код ошибки: `x45`

Внутреннее обозначение ошибки: `EC_SCAN_LIMIT_REACHED`

Описание: При сканировании объекта превышены заданные ограничения (например, на величину распакованного файла, на глубину уровней вложенности и т. п.).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Измените ограничения для сканирования объектов (в настройках соответствующего компонента) любым удобным вам способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`.
2. После изменения настроек повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Authentication failed (Неверные учетные данные пользователя)*

Код ошибки: `x47`

Внутреннее обозначение ошибки: `EC_AUTH_FAILED`

Описание: Попытка пройти аутентификацию с неверными учетными данными пользователя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Authorization failed (Пользователь не имеет требуемых прав)*

Код ошибки: `x48`

Внутреннее обозначение ошибки: `EC_NOT_AUTHORIZED`

Описание: Текущий пользователь не имеет прав на выполнение требуемой операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите попытку авторизации, указав правильные учетные данные пользователя, имеющего

необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Access token is invalid (Недопустимый токен доступа)*

Код ошибки: `x49`

Внутреннее обозначение ошибки: `EC_INVALID_TOKEN`

Описание: Компонент Dr.Web Server Security Suite предъявил некорректный токен авторизации при попытке выполнения операции, требующей повышенные права.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Пройдите аутентификацию, указав правильные учетные данные пользователя, имеющего необходимые полномочия, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid argument (Недопустимый аргумент)*

Код ошибки: `x60`

Внутреннее обозначение ошибки: `EC_INVALID_ARGUMENT`

Описание: Команда не может быть выполнена, так как указан недопустимый аргумент.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность написания и формат команды.
2. Повторите требуемое действие, указав допустимый аргумент.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid operation (Недопустимая операция)*

Код ошибки: `x61`

Внутреннее обозначение ошибки: `EC_INVALID_OPERATION`

Описание: Совершена попытка выполнить недопустимую команду.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно

просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие, указав допустимую команду.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Superuser privileges required (Требуются полномочия суперпользователя)*

Код ошибки: `x62`

Внутреннее обозначение ошибки: `EC_ROOT_ONLY`

Описание: Для выполнения требуемого действия требуются полномочия суперпользователя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повысьте свои права до суперпользователя и повторите требуемое действие. Для повышения прав можно воспользоваться командой `su` или `sudo`.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not allowed in centralized protection mode (Не разрешено в режиме централизованной защиты)*

Код ошибки: `x63`

Внутреннее обозначение ошибки: `EC_STANDALONE_MODE_ONLY`

Описание: Требуемое действие можно выполнить только при работе Dr.Web Server Security Suite в автономном режиме.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Переведите Dr.Web Server Security Suite в автономный режим и повторите операцию снова.

Для перевода Dr.Web Server Security Suite в автономный режим:

- сбросьте флажок **Включить режим централизованной защиты** на странице настроек **Централизованная защита** веб-интерфейса управления;
- или выполните команду:

```
# drweb-ctl esdisconnect
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Non-supported OS (Неподдерживаемая ОС)*

Код ошибки: `x64`

Внутреннее обозначение ошибки: `EC_NON_SUPPORTED_OS`

Описание: Операционная система, установленная на узле, не поддерживается Dr.Web Server Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Установите операционную систему из списка, указанного в системных требованиях.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Feature not implemented (Функция не реализована)*

Код ошибки: `x65`

Внутреннее обозначение ошибки: `EC_UNKNOWN_OPTION`

Описание: Запрашиваемые функции компонента отсутствуют в текущей версии.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Попробуйте сбросить настройки Dr.Web Server Security Suite в значения по умолчанию.

Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

- для GNU/Linux:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

- для FreeBSD:

```
# cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
# echo "" > /usr/local/etc/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unknown option (Неизвестный параметр)*

Код ошибки: `x66`

Внутреннее обозначение ошибки: `EC_UNKNOWN_OPTION`

Описание: Файл конфигурации содержит параметры, неизвестные или не поддерживаемые в текущей версии Dr.Web Server Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Откройте файл `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD в любом текстовом редакторе, удалите строку, содержащую недопустимый параметр, сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если это не поможет, попробуйте сбросить настройки Dr.Web Server Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unknown section (Неизвестная секция)*

Код ошибки: `x67`

Внутреннее обозначение ошибки: `EC_UNKNOWN_SECTION`

Описание: Файл конфигурации содержит секции, неизвестные или не поддерживаемые в текущей версии Dr.Web Server Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Откройте файл `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD в любом текстовом редакторе и удалите неизвестную секцию, после чего сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если это не поможет, попробуйте сбросить настройки Dr.Web Server Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid option value (Недопустимое значение параметра)*

Код ошибки: `x68`

Внутреннее обозначение ошибки: `EC_INVALID_OPTION_VALUE`

Описание: Для одного или нескольких параметров в файле конфигурации указано недопустимое значение.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Измените значение параметра любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`.

   Если вы не знаете, какое значение параметра допустимо, обратитесь к справке по компоненту,

использующему данный параметр, или попытайтесь сбросить значение этого параметра в значение по умолчанию.

2. Также можно отредактировать непосредственно файл конфигурации `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD. Для этого откройте его в любом текстовом редакторе, найдите строку, содержащую недопустимое значение параметра, задайте допустимое значение, сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

   ```
   # service drweb-configd restart
   ```

3. Если предыдущие шаги не помогли, попробуйте сбросить настройки Dr.Web Server Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid state (Недопустимое состояние)*

Код ошибки: `x69`

Внутреннее обозначение ошибки: `EC_INVALID_STATE`

Описание: Недопустимое состояние компонента или Dr.Web Server Security Suite в целом для выполнения запрошенной операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие через некоторое время.
2. При повторении ошибки перезапустите Dr.Web Server Security Suite, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Only one value allowed (Разрешено только одно значение)*

Код ошибки: `x70`

Внутреннее обозначение ошибки: `EC_NOT_LIST_OPTION`

Описание: В файле конфигурации для параметра, который может иметь только одно значение, задано значение в виде списка.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Измените значение параметра любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`.

   Если вы не знаете, какое значение параметра допустимо, обратитесь к справке по компоненту, использующему данный параметр, или попытайтесь сбросить значение этого параметра в значение по умолчанию.
2. Также можно отредактировать непосредственно файл конфигурации `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD. Для этого откройте его в любом текстовом редакторе, найдите строку, содержащую недопустимое значение параметра, задайте допустимое значение, сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

   ```
   # service drweb-configd restart
   ```
3. Если предыдущие шаги не помогли, попробуйте сбросить настройки Dr.Web Server Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:
   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```
   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Record not found (Запись не найдена)*

Код ошибки: `x80`

Внутреннее обозначение ошибки: `EC_RECORD_NOT_FOUND`

Описание: Информация о найденной угрозе отсутствует (возможно, угроза уже была обработана другим компонентом).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Record is in process now (Запись обрабатывается в данный момент)*

Код ошибки: `x81`

Внутреннее обозначение ошибки: `EC_RECORD_BUSY`

Описание: Угроза уже обрабатывается другим компонентом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *File has already been quarantined (Файл уже находится в карантине)*

Код ошибки: `x82`

Внутреннее обозначение ошибки: `EC_QUARANTINED_FILE`

Описание: Файл уже находится в карантине. Возможно, угроза уже была обработана другим компонентом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Update zone is not provided by cloud (Зона обновления в облаке недоступна)*

Код ошибки: `x83`

Внутреннее обозначение ошибки: `EC_NO_ZONE_IN_CLOUD`

Описание: Попытка обновления с помощью Dr.Web Cloud завершилась неудачей.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Update zone is not provided on disk (Зона обновления на диске недоступна)*

Код ошибки: `x84`

Внутреннее обозначение ошибки: `EC_NO_ZONE_ON_DISK`

Описание: Попытка обновления вирусных баз в режиме оффлайн завершилась неудачей.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Убедитесь, что путь к устройству, с которого производится обновление, указан верно.
2. Убедитесь, что пользователь, от имени которого выполняется обновление, обладает правами на чтение каталога с обновлениями.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Cannot backup before update (Не удалось сохранить резервную копию перед обновлением)*

Код ошибки: `x89`

Внутреннее обозначение ошибки: `EC_BACKUP_FAILED`

Описание: Перед началом загрузки обновлений с сервера обновлений не удалось сохранить резервную копию подлежащих обновлению файлов.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для

FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу, хранящему резервные копии обновляемых файлов и при необходимости исправьте его (параметр `BackupDir` в секции `[Update]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу настроек **Updater** веб-интерфейса управления.
   - Вы также можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Update.BackupDir
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Update.BackupDir <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Update.BackupDir -r
   ```
2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```
3. Если ошибка повторяется, проверьте, что пользователь, от имени которого исполняется компонент, имеет права на запись в каталог, указанный в параметре `BackupDir`. Имя пользователя указано в параметре `RunAsUser`. При необходимости измените имя пользователя, изменив значение параметра `RunAsUser`, или предоставьте недостающие права в свойствах каталога.
4. Если ошибка повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid DRL file (Недопустимый DRL-файл)*

Код ошибки: `x90`

Внутреннее обозначение ошибки: `EC_BAD_DRL_FILE`

Описание: Нарушена структура одного из файлов со списками серверов обновлений.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к файлу списка серверов и при необходимости исправьте его

(параметры с именем вида `*DrlDir` в секции `[Update]` файла конфигурации).

- Для просмотра и исправления пути перейдите на страницу настроек **Updater** веб-интерфейса управления.
- Вы также можете воспользоваться утилитой управления из командной строки.

Для просмотра текущего значения параметра введите команду (<*DrlDir> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значения всех параметров в секции, опустив часть команды, заключенную в квадратные скобки):

```
$ drweb-ctl cfshow Update[.<*DrlDir>]
```

Для установки нового значения параметра введите команду (<*DrlDir> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду (<*DrlDir> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```
3. Если ошибка повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid LST file (Недопустимый LST-файл)*

Код ошибки: `x91`

Внутреннее обозначение ошибки: `EC_BAD_LST_FILE`

Описание: Нарушена структура файла с перечнем обновляемых вирусных баз.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Обновите вирусные базы повторно через некоторое время:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```
2. Если ошибка повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid compressed file (Недопустимый сжатый файл)*

Код ошибки: `x92`

Внутреннее обозначение ошибки: `EC_BAD_LZMA_FILE`

Описание: Нарушена структура загруженного файла с обновлениями.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите вирусные базы повторно через некоторое время:

- нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
- или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Proxy authentication error (Ошибка аутентификации на прокси-сервере)*

Код ошибки: `x93`

Внутреннее обозначение ошибки: `EC_PROXY_AUTH_ERROR`

Описание: Не удалось подключиться к серверам обновлений через прокси-сервер, указанный в настройках.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность параметров подключения к прокси-серверу (задаются в параметре с именем `Proxy` в секции `[Update]` файла конфигурации).
   - Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater** веб-интерфейса управления.
   - Вы также можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Update.Proxy
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Update.Proxy <новые параметры>
   ```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Update.Proxy -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *No update servers available (Нет доступных серверов обновлений)*

Код ошибки: `x94`

Внутреннее обозначение ошибки: `EC_NO_UPDATE_SERVERS`

Описание: Не удалось подключиться ни к одному из серверов обновлений.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте доступность сети и исправьте при необходимости сетевые настройки.
2. Если доступ к сети возможен только через прокси-сервер, задайте параметры подключения к прокси-серверу (задаются в параметре с именем `Proxy` в секции `[Update]` файла конфигурации).
   - Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater** веб-интерфейса управления.
   - Вы также можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Update.Proxy
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Update.Proxy <новые параметры>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Update.Proxy -r
   ```

3. Если параметры сетевого подключения, в том числе используемого прокси-сервера, правильные, а ошибка происходит, убедитесь в том, что вы используете доступный список серверов обновления. Перечень используемых серверов обновления указывается в параметрах вида `*DrlDir` в секции `[Update]` файла конфигурации.

   Если параметры вида `*CustomDrlDir` указывают на существующий корректный файл списка серверов, то указанные там серверы будут использоваться вместо серверов стандартной зоны обновления (значение, указанное в соответствующем параметре `*DrlDir`, игнорируется).

- Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater** веб-интерфейса управления.
- Вы также можете воспользоваться утилитой управления из командной строки.

Для просмотра текущего значения параметра введите команду (<*DrlDir> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значение всех параметров в секции, опустив часть команды, заключенную в квадратные скобки):

```
$ drweb-ctl cfshow Update[.<*DrlDir>]
```

Для установки нового значения параметра введите команду (<*DrlDir> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду (<*DrlDir> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

4. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid key file format (Недопустимый формат ключевого файла)*

Код ошибки: `x95`

Внутреннее обозначение ошибки: `EC_BAD_KEY_FORMAT`

Описание: Нарушен формат ключевого файла.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте наличие ключевого файла и правильности пути к нему. Путь к ключевому файлу задается в параметре `KeyPath` в секции `[Root]` файла конфигурации.
   - Для просмотра и задания пути к ключевому файлу перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Вы также можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.KeyPath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.KeyPath <путь к файлу>
   ```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.KeyPath -r
```

2. Если у вас отсутствует ключевой файл, или используемый ключевой файл поврежден, приобретите и установите его. Описание ключевого файла, способы приобретения и установки описаны в разделе Лицензирование.
3. Для установки имеющегося у вас ключевого файла вы можете воспользоваться также формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
4. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *License is already expired (Срок действия лицензии истек)*

Код ошибки: `x96`

Внутреннее обозначение ошибки: `EC_EXPIRED_KEY`

Описание: Срок действия лицензии истек.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла вы также можете воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
3. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Network operation timed out (Истек тайм-аут сетевой операции)*

Код ошибки: `x97`

Внутреннее обозначение ошибки: `EC_NETWORK_TIMEDOUT`

Описание: Истекло время ожидания сетевого соединения (возможно, внезапно перестал отвечать удаленный узел или не удается установить требуемое соединение).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid checksum (Недопустимая контрольная сумма)*

Код ошибки: `x98`

Внутреннее обозначение ошибки: `EC_BAD_CHECKSUM`

Описание: Неверная контрольная сумма загруженного файла с обновлениями.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Обновите вирусные базы повторно через некоторое время:

- нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
- или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid trial license (Недопустимый демонстрационный ключевой файл)*

Код ошибки: `x99`

Внутреннее обозначение ошибки: `EC_BAD_TRIAL_KEY`

Описание: Демонстрационный ключевой файл недействителен (например, он был получен для другого компьютера).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Запросите новый демонстрационный период для данного компьютера, или приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла вы также можете воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
3. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Blocked license key (Лицензионный ключевой файл заблокирован)*

Код ошибки: `x100`

Внутреннее обозначение ошибки: `EC_BLOCKED_LICENSE`

Описание: Текущая лицензия заблокирована (возможно, нарушены условия лицензионного соглашения на использование Dr.Web Server Security Suite).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла можно воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
3. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid license (Недопустимая лицензия)*

Код ошибки: `x101`

Внутреннее обозначение ошибки: `EC_BAD_LICENSE`

Описание: Используемая лицензия предназначена для другого программного продукта или не содержит необходимых разрешений для работы компонентов Dr.Web Server Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла можно воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
3. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web**.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid configuration (Недопустимая конфигурация)*

Код ошибки: `x102`

Внутреннее обозначение ошибки: `EC_BAD_CONFIG`

Описание: Компонент Dr.Web Server Security Suite не может функционировать из-за неправильных настроек конфигурации.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Если имя компонента, вызвавшего ошибку, неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.
2. Если ошибка вызвана компонентом SpIDer Guard, то, вероятнее всего, задан способ работы компонента, который не поддерживается операционной системой. Проверьте установленный режим работы компонента и при необходимости исправьте его, указав значение *Auto* (параметр `Mode` в секции `[LinuxSpider]` файла конфигурации).
   - Для просмотра и исправления режима перейдите на страницу настроек **SpIDer Guard** веб-интерфейса управления.
   - Вы также можете воспользоваться утилитой управления из командной строки.

   Для установки значения *Auto* введите команду:

   ```
   # drweb-ctl cfset LinuxSpider.Mode Auto
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset LinuxSpider.Mode -r
   ```

   Если ошибка повторится, выполните ручную сборку и установку загружаемого модуля ядра для компонента SpIDer Guard.

   Работа компонента SpIDer Guard и загружаемого модуля ядра гарантируется только в том случае, если используемая вами ОС входит в список поддерживаемых (см. раздел Системные требования и совместимость).

3. Если ошибка вызвана другим компонентом, то сбросьте его настройки в значения по умолчанию любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`;
   - отредактировав вручную файл конфигурации (удалив все параметры из секции компонента).
4. Если предыдущие шаги не помогли, сбросьте настройки Dr.Web Server Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

- для FreeBSD:

```
# cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
# echo "" > /usr/local/etc/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid executable file (Недопустимый исполняемый файл)*

Код ошибки: `x104`

Внутреннее обозначение ошибки: `EC_BAD_EXECUTABLE`

Описание: Невозможно запустить компонент. Исполняемый файл поврежден или путь к нему указан неверно.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Если имя компонента, вызвавшего ошибку, неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.
2. Проверьте значение пути к исполняемому файлу компонента в конфигурации Dr.Web Server Security Suite (параметр `ExePath` в секции компонента), выполнив команду (замените *<секция компонента>* на название соответствующей секции файла конфигурации):

   ```
   $ drweb-ctl cfshow <секция компонента>.ExePath
   ```

3. Сбросьте путь в значение по умолчанию, выполнив команду (замените *<секция компонента>* на название соответствующей секции файла конфигурации):

   ```
   # drweb-ctl cfset <секция компонента>.ExePath -r
   ```

4. Если предыдущие шаги не помогли, переустановите пакет соответствующего компонента.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Core engine is not available (Ядро Virus-Finding Engine недоступно)*

Код ошибки: `x105`

Внутреннее обозначение ошибки: `EC_NO_CORE_ENGINE`

Описание: Файл антивирусного ядра Dr.Web Virus-Finding Engine отсутствует или недоступен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с

содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к файлу антивирусного ядра `drweb32.dll` и при необходимости исправьте его (параметр `CoreEnginePath` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Вы также можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.CoreEnginePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.CoreEnginePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Root.CoreEnginePath -r
   ```
2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```
3. Если путь правильный и ошибка повторяется после обновления вирусных баз, переустановите пакет `drweb-bases`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *No virus databases (Вирусные базы отсутствуют)*

Код ошибки: `x106`

Внутреннее обозначение ошибки: `EC_NO_VIRUS_BASES`

Описание: Вирусные базы отсутствуют.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.

- Также вы можете воспользоваться утилитой управления из командной строки.

  Для просмотра текущего значения параметра введите команду:

  ```
  $ drweb-ctl cfshow Root.VirusBaseDir
  ```

  Для установки нового значения параметра введите команду:

  ```
  # drweb-ctl cfset Root.VirusBaseDir <новый путь>
  ```

  Для сброса значения параметра в значение по умолчанию введите команду:

  ```
  # drweb-ctl cfset Root.VirusBaseDir -r
  ```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Process terminated by signal (Процесс завершен по сигналу)*

Код ошибки: `x107`

Внутреннее обозначение ошибки: `EC_APP_TERMINATED`

Описание: Компонент завершил работу (возможно, из-за простоя или вследствие команды пользователя).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Если выполнявшаяся операция не была завершена, то повторите ее запуск снова. В противном случае завершение работы не является ошибкой.
2. Если компонент постоянно завершает свою работу, попробуйте сбросить настройки компонента в значения по умолчанию любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`;
   - отредактировав вручную файл конфигурации (удалив все параметры из секции компонента).
3. Если это не помогло, попробуйте сбросить настройки Dr.Web Server Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

```
# cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
# echo "" > /usr/local/etc/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unexpected process termination (Непредвиденное завершение процесса)*

Код ошибки: `x108`

Внутреннее обозначение ошибки: `EC_APP_CRASHED`

Описание: Компонент неожиданно завершил работу по причине сбоя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Повторите выполнявшуюся операцию.
2. Если компонент постоянно аварийно завершает свою работу, сбросьте настройки компонента в значения по умолчанию любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`;
   - отредактировав вручную файл конфигурации (удалив все параметры из секции компонента).
3. Если это не помогло, сбросьте настройки Dr.Web Server Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

4. Если ошибка повторяется после сброса настроек Dr.Web Server Security Suite, переустановите пакет компонента.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Incompatible software detected (Обнаружено несовместимое ПО)*

Код ошибки: `x109`

Внутреннее обозначение ошибки: `EC_INCOMPATIBLE`

Описание: Один или несколько компонентов Dr.Web Server Security Suite не могут функционировать корректно. В системе обнаружено программное обеспечение, препятствующее их работе.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Отключите или перенастройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *NSS is not available (Компонент NSS недоступен)*

Код ошибки: `x111`

Внутреннее обозначение ошибки: `EC_NO_LINUX_NSS`

Описание: Компонент SplDer Guard для NSS, необходимый для проверки томов NSS, отсутствует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-nss` и при необходимости исправьте его (параметр `ExePath` в секции `[NSS]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow NSS.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset NSS.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset NSS.ExePath -r
   ```

2. При отсутствии настроек компонента SplDer Guard для NSS в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет

`drweb-nss`.

Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Kernel module is not available (Недоступен модуль ядра Linux для SplDer Guard)*

Код ошибки: `x113`

Внутреннее обозначение ошибки: `EC_NO_KERNEL_MODULE`

Описание: Модуль ядра Linux, необходимый для работы SplDer Guard, отсутствует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте установленный режим работы компонента и при необходимости исправьте его, указав значение *Auto* (параметр `Mode` в секции `[LinuxSpider]` файла конфигурации).
   - Для просмотра и исправления режима перейдите на страницу настроек **SplDer Guard** веб-интерфейса управления.
   - Вы также можете воспользоваться утилитой управления из командной строки.

   Для установки значения *Auto* введите команду:

   ```
   # drweb-ctl cfset LinuxSpider.Mode Auto
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset LinuxSpider.Mode -r
   ```
2. Если ошибка повторится, выполните ручную сборку и установку загружаемого модуля ядра для компонента SplDer Guard.

   Работа компонента SplDer Guard и загружаемого модуля ядра гарантируется только в том случае, если используемая вами ОС входит в список поддерживаемых (см. раздел Системные требования и совместимость).

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *MeshD is not available (Компонент MeshD недоступен)*

Код ошибки: `x114`

Внутреннее обозначение ошибки: `EC_NO_MESHD`

Описание: Отсутствует компонент Dr.Web MeshD (требуется для распределения нагрузки при проверке файлов).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-meshd` и при необходимости исправьте его (параметр `ExePath` в секции `[MeshD]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow MeshD.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset MeshD.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset MeshD.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web MeshD в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-meshd`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *ScanEngine is not available (Scanning Engine недоступен)*

Код ошибки: `x119`

Внутреннее обозначение ошибки: `EC_NO_SCAN_ENGINE`

Описание: Компонент Dr.Web Scanning Engine отсутствует или не может быть запущен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-se` и при необходимости исправьте его (параметр `ExePath` в секции `[ScanEngine]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow ScanEngine.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset ScanEngine.ExePath <новый путь>
   ```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset ScanEngine.ExePath -r
```

2. В случае возникновения ошибки при указании правильного пути:
   - Выполните команду:

     ```
     $ drweb-ctl rawscan /
     ```

     Если в выводе на экран присутствует строка «`Error: No valid license provided`», то это означает, что отсутствует действующий ключевой файл. Зарегистрируйте Dr.Web Server Security Suite и получите лицензию. Если лицензия вами получена, то проверьте наличие ключевого файла и установите его при необходимости.
   - Если ваша ОС использует подсистему безопасности SELinux, настройте политику безопасности для модуля `drweb-se` (см. раздел Настройка политик безопасности SELinux).
3. При отсутствии настроек компонента Dr.Web Scanning Engine в конфигурации, или если предыдущие шаги не помогли, установите или переустановите пакет `drweb-se`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *FileCheck is not available (File Checker недоступен)*

Код ошибки: `x120`

Внутреннее обозначение ошибки: `EC_NO_FILE_CHECK`

Описание: Компонент Dr.Web File Checker отсутствует или не может быть запущен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-filecheck` и при необходимости исправьте его (параметр `ExePath` в секции `[FileCheck]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow FileCheck.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset FileCheck.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset FileCheck.ExePath -r
   ```
2. В случае возникновения ошибки при указании правильного пути:
   - Если ваша ОС использует подсистему безопасности SELinux, настройте политику безопасности для модуля `drweb-filecheck` (см. раздел Настройка политик безопасности SELinux).
3. При отсутствии настроек компонента Dr.Web File Checker в конфигурации, или если предыдущие

шаги не помогли, установите или переустановите пакет `drweb-filecheck`.

Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *ESAgent is not available (ES Agent недоступен)*

Код ошибки: `x121`

Внутреннее обозначение ошибки: `EC_NO_ESAGENT`

Описание: Отсутствует компонент Dr.Web ES Agent, необходимый для подключения к серверу централизованной защиты.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-esagent` и при необходимости исправьте его (параметр `ExePath` в секции `[ESAgent]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow ESAgent.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset ESAgent.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset ESAgent.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web ES Agent в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-esagent`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *NetCheck is not available (Network Checker недоступен)*

Код ошибки: `x123`

Внутреннее обозначение ошибки: `EC_NO_NETCHECK`

Описание: Отсутствует компонент Dr.Web Network Checker, необходимый для проверки файлов по сети.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с

содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-netcheck` и при необходимости исправьте его (параметр `ExePath` в секции `[Netcheck]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Netcheck.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Netcheck.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Netcheck.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web Network Checker в конфигурации или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-netcheck`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *CloudD is not available (Компонент CloudD недоступен)*

Код ошибки: `x124`

Внутреннее обозначение ошибки: `EC_NO_CLOUDD`

Описание: Отсутствует компонент Dr.Web CloudD, необходимый для обращения к облаку Dr.Web Cloud.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-cloudd` и при необходимости исправьте его (параметр `ExePath` в секции `[CloudD]` файла конфигурации).

   Вы можете воспользоваться утилитой управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow CloudD.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset CloudD.ExePath <новый путь>
   ```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset CloudD.ExePath -r
```

2. При отсутствии настроек компонента Dr.Web CloudD в конфигурации или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-cloudd`.

   Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unexpected error (Непредвиденная ошибка)*

Код ошибки: `x125`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_ERROR`

Описание: Возникла непредвиденная ошибка в работе одного или нескольких компонентов.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Server Security Suite (при настройках по умолчанию его можно просмотреть командой `# journalctl` для GNU/Linux или `# less /var/log/messages` для FreeBSD). Вы также можете выполнить команду `# drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Server Security Suite, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Ошибки без кода

Симптомы: В FreeBSD 13, 14 или 15 возникает одна из следующих ошибок:

- Не удается запустить компонент Dr.Web ConfigD.
- Пути к сокетам, указанные в параметрах `Root.AdminSocketPath` и `Root.AdminSocketPath` (по умолчанию `/var/run/.com.drweb.public` и `/var/run/.com.drweb.admin` соответственно), не существуют или эти сокеты недоступны.

Описание: Работа Dr.Web Server Security Suite невозможна из-за отсутствия пакета совместимости `compat12x`.

Устранение ошибки

Установите пакет совместимости `compat12x`. Пример необходимых для этого действий приведен ниже.

1. Откройте консоль или эмулятор терминала и выполните команды:

   ```
   # pkg update
   # pkg search compat12x
   ```

   В выводе последней команды будет указано полное название пакета в репозитории вашей ОС.

2. Укажите название пакета и установите его, например:

```
# pkg install compat12x-amd64-12.2.1202000.20210406_2
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы: После установки модуля ядра SplDer Guard работа операционной системы аварийно завершается с ошибкой ядра «*Kernel panic*».

Описание: Работа модуля ядра SplDer Guard невозможна в среде исполнения ядра ОС (например, ОС работает в среде гипервизора Xen).

Устранение ошибки

1. Отмените загрузку модуля ядра SplDer Guard (модуль ядра имеет имя `drweb`), добавив в загрузчике GNU GRUB строку:

```
drweb.blacklist=yes
```

   в строку параметров загрузки ядра ОС.
2. После загрузки ОС удалите модуль `drweb.ko` из каталога дополнительных модулей `/lib/modules/`uname -r`/extra`.
3. Установите для SplDer Guard режим работы *Auto*, выполнив команды:

```
# drweb-ctl cfset LinuxSpider.Mode Auto
# drweb-ctl reload
```

4. Если используемая вами ОС не поддерживает механизм *fanotify*, или использование этого режима не позволяет использовать SplDer Guard для полноценного контроля файловой системы и режим *LKM* становится обязательным, то откажитесь от использования гипервизора Xen.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы: Такие компоненты, как Dr.Web ClamD, не проверяют сообщения; в журнале Dr.Web Server Security Suite наблюдаются сообщения `Too many open files`.

Описание: В связи большой загрузкой по проверке данных компонент Dr.Web Network Checker исчерпал лимит на число доступных файловых дескрипторов.

Устранение ошибки

1. Увеличьте лимит на число открытых файловых дескрипторов, доступных приложению, используя команду `ulimit -n` (по умолчанию лимит на число дескрипторов для Dr.Web Server Security Suite составляет 16384).



В некоторых случаях системный сервис `systemd` может игнорировать заданные изменения лимита.

В этом случае отредактируйте (или создайте, при его отсутствии) файл `/etc/systemd/system/drweb-configd.service.d/limits.conf`, указав в нем измененное значение лимита:

```
[Service]
LimitNOFILE=16384
```

С перечнем доступных лимитов `systemd` можно ознакомиться, выполнив команду `man systemd.exec`.

2. После изменения лимита перезапустите Dr.Web Server Security Suite, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы: Не удается установить соединение с веб-интерфейсом управления Dr.Web в браузере, компоненты Dr.Web отсутствуют в перечне запущенных процессов (`ps ax | grep drweb`), выполнение любой команды `drweb-ctl <команда>`, за исключением команды `drweb-ctl rawscan`, выводит сообщение об ошибке:

`Error: connect: No such file or directory: "<путь>/.com.drweb.public"`

или

`Error: connect: Connection refused: "<путь>/.com.drweb.public".`

Описание: Dr.Web Server Security Suite не может запуститься, поскольку демон управления конфигурацией Dr.Web ConfigD недоступен.

Устранение ошибки

1. Выполните команду:

```
# service drweb-configd restart
```

для перезапуска Dr.Web ConfigD и Dr.Web Server Security Suite в целом.

2. Если эта команда вернет ошибку или не даст никакого эффекта, выполните отдельную установку пакета `drweb-configd`.



Это также может означать, что в системе для аутентификации пользователей не используется PAM. Если это так, то установите и настройте его, поскольку без PAM корректная работа Dr.Web Server Security Suite невозможна.

3. Если и после этого ошибка повторится, удалите Dr.Web Server Security Suite целиком, после чего установите его повторно.

Инструкции по установке и удалению Dr.Web Server Security Suite и его компонентов см. в разделах Установка Dr.Web Server Security Suite и Удаление Dr.Web Server Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

10.7. Приложение Ж. Список сокращений

В данном руководстве следующие сокращения использованы без расшифровки:

Обозначение	Расшифровка
AD	Microsoft Active Directory
FQDN	Fully Qualified Domain Name
GID	Group ID (системный идентификатор группы пользователей)
GNU	Проект GNU (GNU is Not Unix)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure (через SSL/TLS)
ID	Идентификатор
IMA/EVM	Integrity Measurement Architecture and Extended Verification Module (подсистема ядра Linux, позволяющая осуществлять контроль целостности файловой системы)
IP	Internet Protocol
LKM	Loadable Kernel Module (загружаемый модуль ядра)
MBR	Master Boot Record
NSS	Novell Storage Services
OID	(SNMP) Object ID
PID	Process ID (системный идентификатор процесса)
PAM	Pluggable Authentication Modules
RPM	Red Hat Package Manager (формат пакетов)
RRA	Round-Robin Archive
RRD	Round-Robin Database
SMB	Server Message Block (протокол доступа к файлам)
SNMP	Simple Network Management Protocol
SP	Service Pack

Обозначение	Расшифровка
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	User ID (системный идентификатор пользователя)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VBR	Volume Boot Record
ОС	Операционная система

© «Доктор Веб», 2026