Dr.WEB

для файловых серверов UNIX

Руководство администратора

Dr.Web для файловых серверов UNIX
Версия 11.1
Руководство администратора
01.09.2023

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 2, корп. 12-а

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах вы можете найти на официальном сайте компании.

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

Введение

Благодарим вас за приобретение решения Dr.Web для файловых серверов UNIX. Оно 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, в установке и использовании Dr.Web для файловых серверов UNIX версии 11.1.

Соглашение о путях к файлам

Пути, используемые для размещения компонентов и служебных файлов, зависят от операционной системы. В документе используются следующие условные обозначения для каталогов:

- <*opt_dir*> — каталог, используемый для размещения основных файлов, включая исполняемые файлы и библиотеки;
- <*etc_dir*> — каталог, используемый для размещения конфигурационного и ключевого файлов;
- <*var_dir*> — каталог, используемый для размещения вспомогательных и временных файлов.

Реальные пути, соответствующие введенным обозначениям в разных операционных системах, приведены в таблице ниже.

Тип ОС	Условное обозначение	Реальный путь
GNU/Linux	<*opt_dir*>	`/opt/drweb.com`
	<*etc_dir*>	`/etc/opt/drweb.com`
	<*var_dir*>	`/var/opt/drweb.com`
FreeBSD	<*opt_dir*>	`/usr/local/libexec/drweb.com`
	<*etc_dir*>	`/usr/local/etc/drweb.com`
	<*var_dir*>	`/var/drweb.com`

Для экономии места в примерах условные обозначения будут раскрываться в пути, характерные для ОС GNU/Linux. В тех местах документа, где это возможно, будут приводиться примеры реальных путей для всех типов ОС.

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 ко вводу `$` или `#`, определяющим, какие полномочия пользователя необходимы для исполнения указанной команды. Стандартным для UNIX-систем образом подразумевается, что:

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

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

Перечень сокращений приведен в разделе Приложение Ж. Список сокращений.

О продукте

В этом разделе

Назначение

Dr.Web для файловых серверов UNIX создан для защиты файловых серверов, работающих под управлением ОС семейства UNIX (GNU/Linux и FreeBSD) от вирусов и всех прочих видов вредоносного программного обеспечения, а также для предотвращения распространения через них угроз, разработанных для различных платформ.

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 и мобильных устройств, работающих под управлением распространенных операционных систем, от угроз, предназначенных для различных платформ. В настоящее время, наряду с Dr.Web для файловых серверов UNIX, в компании «Доктор Веб» разработаны также и другие антивирусные решения как для операционных систем семейства UNIX (GNU/Linux и FreeBSD), так и для ОС IBM OS/2, Novell NetWare, macOS и Windows. Кроме того, разработаны антивирусные решения, обеспечивающие защиту мобильных устройств, работающих под управлением ОС Android, Symbian, BlackBerry.

Компоненты Dr.Web для файловых серверов UNIX постоянно обновляются, а вирусные базы, базы категорий веб-ресурсов и базы правил спам-фильтрации сообщений электронной почты регулярно дополняются новыми сигнатурами угроз, что обеспечивает актуальный уровень защищенности серверов, рабочих станций и мобильных устройств пользователей, а также используемых ими программ и данных. 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 (данная функция доступна не во всех продуктах Dr.Web).

Основные функции Dr.Web для файловых серверов UNIX

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 файлами с набором различных уровней доступа, сканирование файлов, недоступных на текущем уровне доступа, может производиться в специальном режиме автономной копии.

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

   Утилита управления из командной строки Dr.Web Ctl, входящая в состав Dr.Web для файловых серверов UNIX, 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 необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, на роутерах и прочих «умных» устройствах вы можете воспользоваться механизмом 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 вирусных инцидентов; ведение журнала обнаруженных угроз. Отправка уведомлений об обнаруженных угрозах по SNMP внешним системам мониторинга и серверу централизованной защиты, если Dr.Web для файловых серверов UNIX работает в режиме централизованной защиты, а также облачному сервису Dr.Web Cloud.
6. **Обеспечение работы под управлением сервера централизованной защиты** (такого как Dr.Web Enterprise Server или в рамках сервиса Dr.Web AV-Desk) для применения на сервере единых политик безопасности, принятых в некоторой сети, 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 к интернету.

Структура Dr.Web для файловых серверов UNIX

Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX. 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 для файловых серверов UNIX — 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 для файловых серверов UNIX и т. д.);
- интерфейсные компоненты, предоставляющие (пользователю или сторонним приложениям) интерфейс для управления работой Dr.Web для файловых серверов UNIX.

Перечень компонентов, входящих в состав Dr.Web для файловых серверов UNIX, перечислен в таблицах ниже.

1. Базовые антивирусные компоненты

Компонент	Описание
Dr.Web Virus-Finding Engine	Антивирусное ядро. Реализует алгоритмы поиска и распознавания вирусов и 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 для файловых серверов UNIX) 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 для файловых серверов UNIX 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 для файловых серверов UNIX 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`

2. Компоненты поиска угроз

Компонент	Описание
SplDer Guard	Монитор файловой системы 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 механизм *fanotify* (API, предоставляемый ОС) 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 режиме, блокируя доступ к файлам (всех типов или только к исполняемым файлам), которые еще не проверены, до момента окончания их проверки. По умолчанию усиленный режим мониторинга отключен. Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Исполняемый файл компонента: `drweb-spider`. Внутреннее наименование, выводимое в журнал: `LinuxSpider`
Модуль ядра GNU/Linux для SplDer Guard	Модуль ядра GNU/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 исходных кодов, позволяющих осуществить сборку и установку модуля ядра ОС вручную (инструкция по сборке приведена в разделе Сборка модуля ядра для SplDer Guard). Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Для архитектур ARM64 и E2K 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. 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 для файловых серверов UNIX. • 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 для файловых серверов UNIX 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 для файловых серверов UNIX и накопленную статистику вирусных инцидентов Исполняемый файл компонента: `drweb-esagent`. Внутреннее наименование, выводимое в журнал: `ESAgent`
Dr.Web StatD	Компонент для хранения статистики событий компонентов Dr.Web для файловых серверов UNIX. Получает и организует хранение событий, поступающих от компонентов программного комплекса (таких, как аварийное завершение работы, обнаружение угрозы и т. п.) 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`

4. Интерфейсные компоненты

Компонент	Описание
Dr.Web HTTPD	Веб-сервер управления компонентами Dr.Web для файловых серверов UNIX. Предоставляет специализированный HTTP API для управления компонентами Dr.Web для файловых серверов UNIX. Указанный API используется веб-интерфейсом управления (должен быть установлен дополнительно). 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 для файловых серверов UNIX из командной строки операционной системы. Позволяет осуществлять запуск проверки файлов, просматривать содержимое карантина и управлять им, запускать обновление вирусных баз, подключать Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX с внешними системами мониторинга посредством протокола SNMP. Такая интеграция позволяет отслеживать состояние работы

Компонент	Описание
	компонентов комплекса, а также собирать статистику обнаружения и нейтрализации угроз. 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 для файловых серверов UNIX 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 для файловых серверов UNIX и его взаимодействия с внешними приложениями.

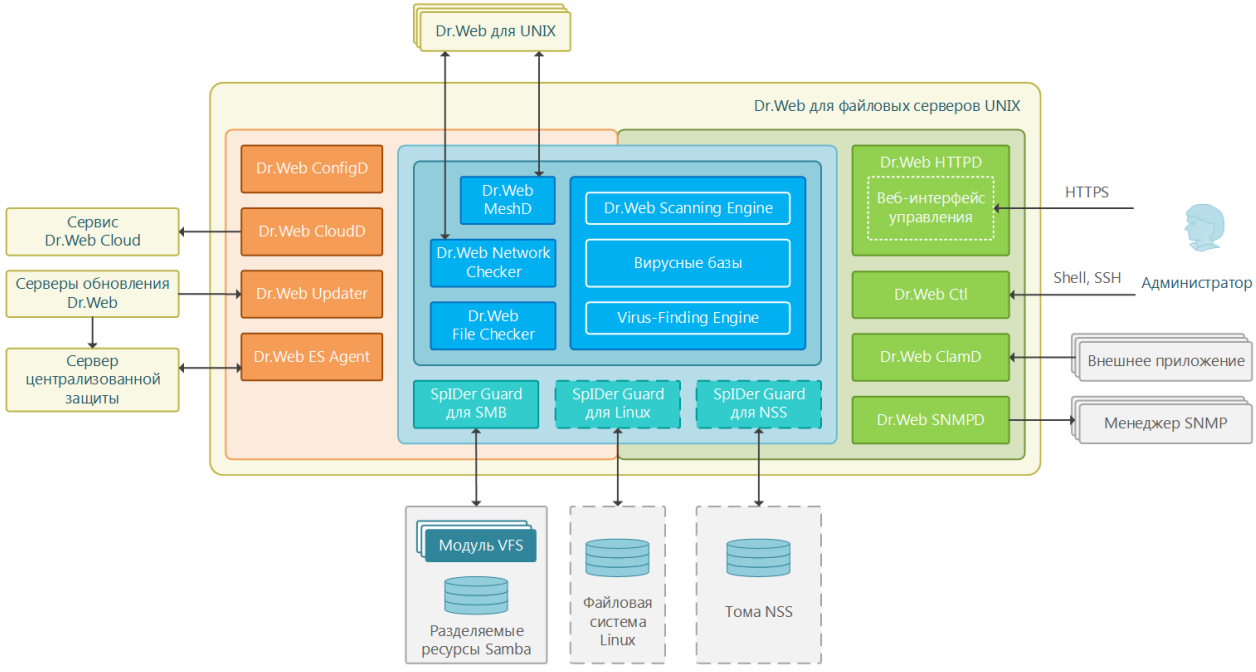

Рисунок 1. Структура Dr.Web для файловых серверов UNIX

На приведенном рисунке использованы следующие обозначения:

	— Dr.Web для файловых серверов UNIX в целом и внешние по отношению к нему программные продукты Dr.Web, не входящие непосредственно в его состав

	— внешние по отношению к Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX
	— компоненты, используемые для антивирусной проверки
	— базовые антивирусные компоненты, образующие ядро Dr.Web для файловых серверов UNIX. Используются компонентами, осуществляющими проверку файлов и данных

Компоненты, обозначенные пунктирной границей, могут отсутствовать, в зависимости от поставки или сценария использования Dr.Web для файловых серверов UNIX.

Более подробно компоненты Dr.Web для файловых серверов UNIX описаны в разделе Компоненты Dr.Web для файловых серверов UNIX.

Размещение карантина

Карантин Dr.Web для файловых серверов UNIX версии 11.1 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 для файловых серверов UNIX (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 для файловых серверов UNIX. Кроме того, при перемещении файла в карантин, у него всегда сбрасывается бит исполнения для предотвращения его 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 файловую систему операционной системы.

Каталоги карантина Dr.Web всегда имеют имя `.com.drweb.quarantine` и создаются по мере необходимости, в тот момент, когда к какой-либо угрозе применяется действие **В карантин**, т. е. 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 файловую систему операционной системы периодически и в различные точки.

Пользователь может управлять содержимым карантина из командной строки, используя утилиту Dr.Web Ctl, или через веб-интерфейс управления (если он установлен). При этом всегда обрабатывается консолидированный карантин, объединяющий в себе все каталоги с изолированными объектами, доступные в данный момент.

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 для файловых серверов UNIX используют карантин для изоляции угроз. Например, его не использует компонент Dr.Web ClamD, а также компоненты Dr.Web ICAPD (не входит в состав используемого вами продукта) и Dr.Web MailD (не входит в состав используемого вами продукта).

Полномочия для работы с файлами

При сканировании объектов файловой системы и нейтрализации угроз Dr.Web для файловых серверов UNIX (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 архива (Отображение только элементов, которые содержат ошибку или угрозу)	Без ограничений. Специальных полномочий не требуется

Действие	Требуемые полномочия
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 (*root*) вы можете воспользоваться командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

Сканирующее ядро Dr.Web Scanning Engine не может работать с файлами, размер которых больше 4 ГБ (при попытке проверки таких файлов будет выдаваться ошибка *«Файл слишком большой»*).

Режимы работы

Антивирусное решение Dr.Web для файловых серверов UNIX может работать как в одиночном 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 для файловых серверов UNIX.

- *В одиночном режиме (standalone mode)* 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 для файловых серверов UNIX полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов обновлений компании «Доктор Веб».

- *В режиме централизованной защиты (enterprise mode)* защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки Dr.Web для файловых серверов UNIX 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 с выбранного сервера централизованной защиты, к которому подключен Dr.Web для файловых серверов UNIX. Лицензионный или демонстрационный ключевой файл пользователя, если он имеется на локальном компьютере, не используется. На сервер централизованной защиты отсылается статистика работы Dr.Web для файловых серверов UNIX, включая статистику вирусных инцидентов. Обновление вирусных баз также выполняется с сервера централизованной защиты.
- *В мобильном режиме (mobile mode)* Dr.Web для файловых серверов UNIX 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 использования данного режима зависит от разрешений, заданных на сервере централизованной защиты.

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 компонентами Dr.Web для файловых серверов UNIX), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

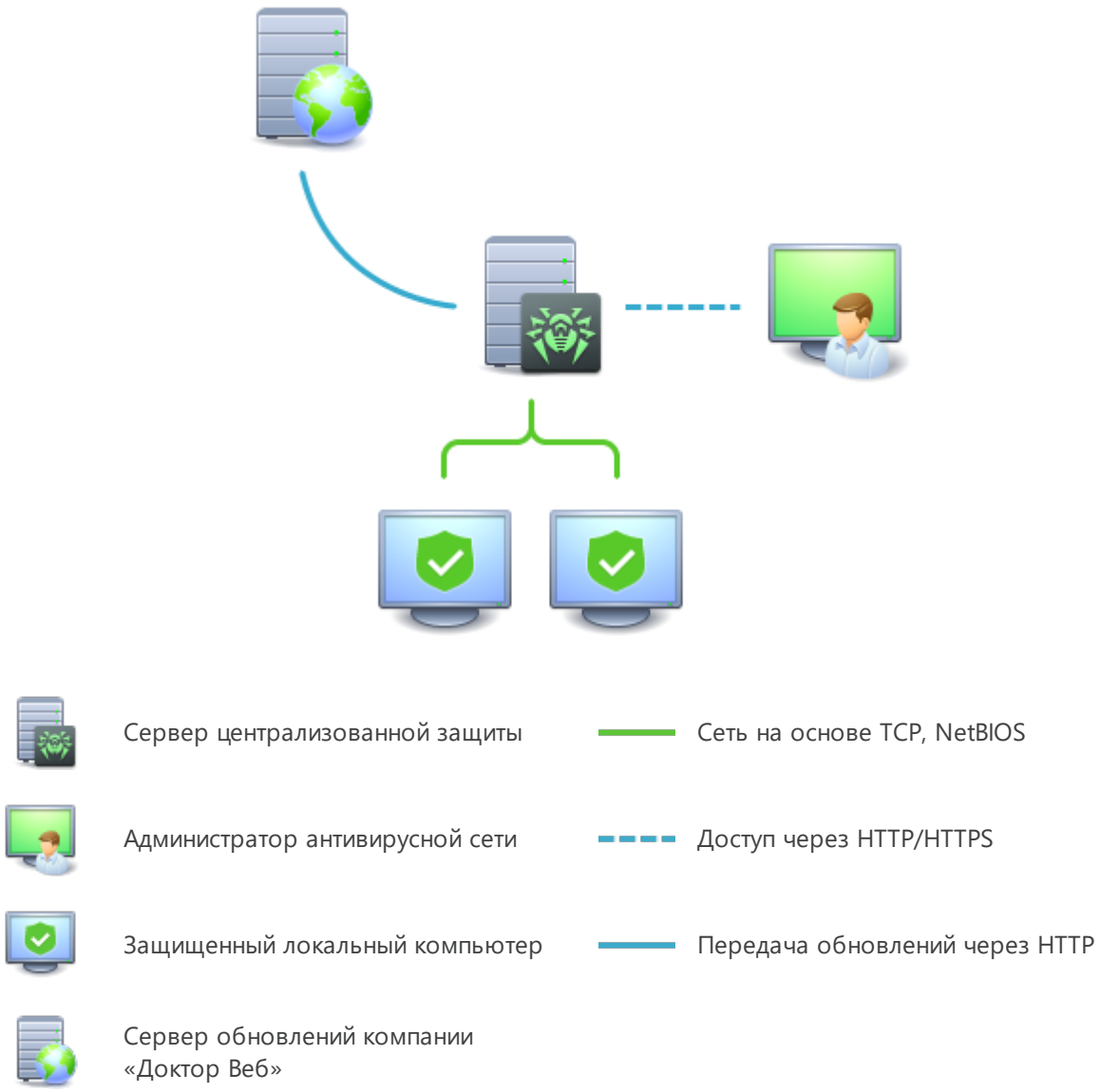

Рисунок 2. Логическая структура антивирусной сети

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 и потере важных данных.

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

Подключение к серверу централизованной защиты

Dr.Web для файловых серверов UNIX может быть подключен к серверу централизованной защиты антивирусной сети при помощи команды `esconnect` утилиты управления из командной строки Dr.Web 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 для файловых серверов UNIX.

Если Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX в мобильный режим работы зависит от разрешений, заданных на используемом сервере централизованной защиты.

Отключение от сервера централизованной защиты

Dr.Web для файловых серверов UNIX может быть отключен от сервера централизованной защиты антивирусной сети при помощи команды `esdisconnect` утилиты управления из командной строки Dr.Web Ctl.

Системные требования и совместимость

В этом разделе

Системные требования

Использование Dr.Web для файловых серверов UNIX возможно на компьютере, удовлетворяющем следующим требованиям:

Компонент	Требование
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 POWER (*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; • 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 для файловых серверов UNIX 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 Special Edition 1.5 (с кумулятивным патчем 20201201SE15), 1.6 (с кумулятивным патчем 20200722SE16), 1.7; • Astra Linux Common Edition (Орел) 2.12; • Debian 9, 10; • Fedora 31, 32; • CentOS 7, 8; • Ubuntu 18.04, 20.04, 22.04; • Альт Рабочая станция 9, 10; • Альт Сервер 9, 10; • Альт 8 СП; • РЕД ОС 7.2 МУРОМ, РЕД ОС 7.3 МУРОМ; • Гослинукс IC6; • SUSE Linux Enterprise Server 12 SP3; • Red Hat Enterprise Linux 7, 8
x86	• CentOS 7; • Debian 10; • Альт Рабочая станция 9, 10; • Альт 8 СП
ARM64	• Ubuntu 18.04; • CentOS 7, 8; • Альт Рабочая станция 9, 10; • Альт Сервер 9, 10; • Альт 8 СП;

Платформа	Поддерживаемые версии GNU/Linux
	• Astra Linux Special Edition (Новороссийск) 4.7
E2K	• Astra Linux Special Edition (Ленинград) 8.1 (с кумулятивным патчем 20200429SE81); • Альт 8 СП; • Эльбрус-Д МЦСТ 1.4; • ОПО ВК Эльбрус-8.32 ТВГИ.00311-28
ppc64el	• CentOS 8; • Ubuntu 20.04

В ОС Альт 8 СП, Astra Linux Special Edition (Новороссийск) 4.11, 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 для файловых серверов UNIX не гарантируется. При возникновении проблем с совместимостью с вашим дистрибутивом обратитесь в техническую поддержку.

- **FreeBSD**

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

Для ОС FreeBSD установка Dr.Web для файловых серверов UNIX возможна только из универсального пакета.

Дополнительные пакеты и компоненты

Dr.Web для файловых серверов UNIX не требует установки дополнительных пакетов и компонентов ОС (кроме программного обеспечения защищаемого серверного решения, см. ниже).

Для удобной работы с Dr.Web для файловых серверов UNIX 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 и E2K.
- 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

1. Файловая служба Samba

Для интеграции с файловой службой Samba требуется установленный и настроенный сервер Samba одной из следующих версий: 3.6–4.16.

Монитор SpIDer Guard для SMB, входящий в состав Dr.Web для файловых серверов UNIX, 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 для файловых серверов UNIX 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 исходных кодов описана в разделе Сборка модуля VFS SMB.

2. 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 для файловых серверов UNIX не совместим с подсистемой улучшения безопасности SELinux. Кроме того, по умолчанию Dr.Web для

файловых серверов UNIX 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 для файловых серверов UNIX 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 для файловых серверов UNIX. Подробнее см. в разделе Настройка подсистем безопасности.

Лицензирование

Права пользователя на использование копии Dr.Web для файловых серверов UNIX подтверждаются и регулируются *лицензией*, приобретенной пользователем у компании «Доктор Веб» или ее партнеров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением (см. https://license.drweb.com/agreement/), условия которого принимаются пользователем при установке Dr.Web для файловых серверов UNIX на свой компьютер. В лицензии фиксируется информация о пользователе и продавце, а также параметры использования приобретенной копии, в частности:

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

Имеется также возможность активировать для приобретенной копии Dr.Web для файловых серверов UNIX *демонстрационный период*. В этом случае, если не нарушены условия активации демонстрационного периода, пользователь получает право на полноценное использование Dr.Web для файловых серверов UNIX в течение демонстрационного периода.

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а на локальном компьютере пользователя с лицензией связывается специальный файл, регулирующий работу компонентов в соответствии с параметрами лицензии. Он называется *лицензионным* ключевым файлом. При активации демонстрационного периода также автоматически формируется специальный ключевой файл, называемый *демонстрационным*.

В случае отсутствия у пользователя действующей лицензии или активированного демонстрационного периода, антивирусные функции компонентов Dr.Web для файловых серверов UNIX блокируются, кроме того, недоступен сервис регулярных обновлений вирусных баз с серверов обновлений компании «Доктор Веб». Однако имеется возможность активировать Dr.Web для файловых серверов UNIX, подключив его к серверу централизованной защиты антивирусной сети предприятия или сети, организованной интернет-провайдером. В этом случае управление антивирусными функциями и обновлениями копии Dr.Web для файловых серверов UNIX, установленной на компьютере, включенном в состав антивирусной сети, возлагается на сервер централизованной защиты.

Установка и удаление

В этом разделе

В этом разделе описываются процедуры установки и удаления Dr.Web для файловых серверов UNIX версии 11.1, а также процедура получения текущих обновлений и процедура перехода на новую версию, если на вашем компьютере уже установлен Dr.Web для файловых серверов UNIX предыдущей версии.

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

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

Не гарантируется совместимость Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX 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 для Linux, и вы хотите в дополнение к нему установить Dr.Web для файловых серверов UNIX), необходимо предварительно убедиться, что версия уже установленного продукта совпадает с версией Dr.Web для файловых серверов UNIX, 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 следует обновить уже установленный продукт до версии Dr.Web для файловых серверов UNIX, которую вы хотите установить дополнительно.

Для ОС FreeBSD установка Dr.Web для файловых серверов UNIX возможна только из универсального пакета.

Установка Dr.Web для файловых серверов UNIX

Вы можете установить Dr.Web для файловых серверов UNIX одним из двух способов:

1. Загрузив с веб-сайта компании «Доктор Веб» установочный файл, содержащий универсальный пакет для UNIX-систем, снабженный программой установки (так как программа установки разработана для режима командной строки, для ее работы в режиме графического рабочего стола необходимо наличие эмулятора терминала).
2. Выполнив установку Dr.Web для файловых серверов UNIX в виде набора нативных пакетов (для этого потребуется подключиться к соответствующему репозиторию пакетов компании «Доктор Веб»).

Для ОС FreeBSD установка Dr.Web для файловых серверов UNIX возможна только из универсального пакета.

В Альт 8 СП и других ОС, использующих устаревшие версии пакетного менеджера, рекомендуется устанавливать Dr.Web для файловых серверов UNIX из универсального пакета.

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 для файловых серверов UNIX.

Dr.Web для файловых серверов UNIX, 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 для файловых серверов UNIX. При необходимости выполните также настройку подсистем безопасности GNU/Linux для корректной работы Dr.Web для файловых серверов UNIX. При возникновении проблем с функционированием отдельных компонентов вы можете выполнить их выборочную установку и удаление, не удаляя Dr.Web для файловых серверов UNIX целиком.

После установки Dr.Web для файловых серверов UNIX любым из указанных в данном руководстве способов, в начале работы вам потребуется активировать лицензию и установить полученный ключевой файл. Кроме того, вы можете подключить Dr.Web для файловых серверов UNIX к серверу централизованной защиты. Подробнее см. в разделе 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 для файловых серверов UNIX, как это описано в разделе Начало работы.

Установка универсального пакета

Универсальный пакет Dr.Web для файловых серверов UNIX распространяется в виде установочного файла с именем `drweb-<версия>-av-srv-<ОС>-<платформа>.run`, где <*ОС*> — тип операционной системы семейства UNIX, а <*платформа*> — строка, указывающая тип платформы, для которой предназначен Dr.Web для файловых серверов UNIX (для 32-битных платформ — `x86`, для 64-битных платформ — `amd64`, `arm64` и `e2s`). Например:

```
drweb-11.1.0-av-srv-linux-x86.run
```

Далее в данном разделе руководства имя установочного файла, соответствующее формату, указанному выше, обозначается как <*имя_файла*>`.run`.

Чтобы установить компоненты Dr.Web для файловых серверов UNIX

1. Если у вас отсутствует установочный файл, содержащий универсальный пакет, загрузите его с официального веб-сайта компании «Доктор Веб»: https://download.drweb.com/.
2. Сохраните установочный файл на жесткий диск компьютера.
3. Разрешите исполнение файла, например, командой:

```
# chmod +x <имя_файла>.run
```

4. Запустите его на исполнение командой:

```
# ./<имя_файла>.run
```

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

В случае установки Dr.Web для файловых серверов UNIX в среде ОС Astra Linux SE версий 1.6 и 1.7, работающей в режиме *замкнутой программной среды*, 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 *замкнутой программной среды* (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 `sudo`). Если попытка повышения прав окончится неудачей, установка будет завершена.

Если в части файловой системы, содержащей временный каталог, не имеется достаточного количества свободного места для распаковки дистрибутива, процесс установки будет завершен после выдачи соответствующего сообщения. В этом случае следует повторить распаковку, изменив значение системной переменной окружения `TMPDIR` таким образом, чтобы она указывала на каталог, имеющий достаточное количество свободного места. Также вы можете воспользоваться ключом распаковки в указанный каталог `--target`.

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

5. Следуйте инструкциям программы установки.
6. Имеется возможность запустить программу установки в полностью автоматическом режиме, выполнив команду:

```
# ./<имя_файла>.run -- --non-interactive
```

В этом случае программа установки будет запущена в полностью автоматическом режиме, без показа интерфейса пользователя (включая диалоги 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 для файловых серверов UNIX вы можете, прочитав файл `/opt/drweb.com/share/doc/LICENSE`. 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 для файловых серверов UNIX после установки.

Запуск программы установки в полностью автоматическом режиме требует наличия прав суперпользователя. Для повышения прав вы можете использовать команды `su` и `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 для того, чтобы в дальнейшем антивирусные компоненты работали корректно.

Об условных обозначениях путей <*opt_dir*>, <*etc_dir*> и <*var_dir*> см. Введение.

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

Рекомендуется сохранить файл <*имя_файла*>`.run`, из которого производилась установка, для возможной переустановки Dr.Web для файловых серверов UNIX или его компонентов в последующем, без обновления его версии.

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 «Do you want to continue?». 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 Dr.Web, 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 выбранных компонентов Dr.Web. При этом на экран будет выводиться информация о ходе 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 для файловых серверов UNIX.

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, следует устранить проблемы, вызвавшие ошибку установки, и повторить процесс установки заново.

Установка из репозитория

Нативные пакеты Dr.Web для файловых серверов UNIX находятся в официальном репозитории Dr.Web https://repo.drweb.com/. 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.

Все нижеприведенные команды для подключения репозиториев, импортирования ключей, установки и удаления пакетов должны быть выполнены с правами суперпользователя. Для этого используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Для ОС FreeBSD установка Dr.Web для файловых серверов UNIX возможна только из универсального пакета.

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

- Debian, Mint, Ubuntu (apt),
- ALT Linux, PCLinuxOS (apt-rpm),
- Mageia, OpenMandriva Lx (urpmi),
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf),

- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

Чтобы установить Dr.Web для файловых серверов UNIX из репозитория

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:

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
8C42FC58D8752769
```

2. Чтобы подключить репозиторий, добавьте следующую строку в файл `/etc/apt/sources.list`:

```
deb http://repo.drweb.com/drweb/debian 11.1 non-free
```

Вы можете выполнить пункты 1 и 2, загрузив из репозитория и установив специальный DEB-пакет https://repo.drweb.com/drweb/drweb-repo11.1.deb.

3. Для установки Dr.Web для файловых серверов UNIX 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.

ALT Linux, PCLinuxOS (apt-rpm)

Чтобы установить Dr.Web для файловых серверов UNIX из репозитория

1. Чтобы подключить репозиторий, добавьте следующую строку в файл `/etc/apt/sources.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`.

2. Для установки Dr.Web для файловых серверов UNIX 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)

Чтобы установить Dr.Web для файловых серверов UNIX из репозитория

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 для файловых серверов UNIX 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)

Чтобы установить Dr.Web для файловых серверов UNIX из репозитория

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 из репозитория и установив специальный RPM-пакет https://repo.drweb.com/drweb/drweb-repo11.1.rpm.

2. Для установки Dr.Web для файловых серверов UNIX 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)

Чтобы установить Dr.Web для файловых серверов UNIX из репозитория

1. Чтобы подключить репозиторий, запустите следующую команду:

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

2. Для установки Dr.Web для файловых серверов UNIX из репозитория выполните команды:

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

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

Обновление Dr.Web для файловых серверов UNIX

Предусмотрено два режима обновления Dr.Web для файловых серверов UNIX.

1. Получение обновлений пакетов и компонентов, выпущенных в рамках эксплуатации текущей версии Dr.Web для файловых серверов UNIX (как правило, такие обновления содержат исправления ошибок и мелкие улучшения в функционировании компонентов).

2. Переход на новую версию Dr.Web для файловых серверов UNIX. Этот способ обновления используется, если компания «Доктор Веб» выпустила новую версию Dr.Web для файловых серверов UNIX, отличающуюся новыми возможностями.

Dr.Web для файловых серверов UNIX предоставляет возможность обновления вирусных баз и антивирусного ядра даже при отсутствии доступа в интернет на защищаемом сервере.

Обновление пакетов и компонентов

После установки Dr.Web для файловых серверов UNIX 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 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 для файловых серверов UNIX на ваш компьютер.

  Чтобы получить и установить обновленные пакеты Dr.Web этим менеджером, перейдите в каталог <*opt_dir*>`/bin` (для GNU/Linux — `/opt/drweb.com/bin`), 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 поддержки `compat10x-amd64` и повторите попытку обновления.

Для установки пакета используйте 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, OpenMandriva Lx используйте команду `urpmi`,
  - в Alt Linux, PCLinuxOS, Debian, Mint, Ubuntu используйте команду `apt-get`.

Также вы можете использовать и 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 для файловых серверов UNIX, 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. Переход на новую версию).

Переход на новую версию продукта

В этом разделе

Предварительные замечания

Перед тем, как выполнить переход на новую версию, убедитесь, что ваш сервер отвечает системным требованиям новой версии, в том числе, что на нем установлены необходимые дополнительные программы.

Переход на новую версию Dr.Web для файловых серверов UNIX следует выполнять тем же способом, каким была установлена версия Dr.Web для файловых серверов UNIX, подлежащая обновлению.

- Если версия Dr.Web для файловых серверов UNIX, подлежащая обновлению, была установлена из репозитория, то переход на новую версию следует выполнять обновлением из репозитория.
- Если версия Dr.Web для файловых серверов UNIX, подлежащая обновлению, была установлена из универсального пакета, то переход на новую версию следует производить установкой из универсального пакета, содержащего новую версию Dr.Web для файловых серверов UNIX.

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

Для ОС FreeBSD установка Dr.Web для файловых серверов UNIX возможна только из универсального пакета.

Если вы не имеете возможности обновить Dr.Web для файловых серверов UNIX тем же способом, каким он был установлен изначально, вам следует предварительно удалить текущую версию, а потом выполнить установку новой версии Dr.Web для файловых серверов UNIX доступным для вас способом. Способы установки и удаления предыдущих версий Dr.Web для файловых серверов UNIX аналогичны способам установки и удаления, рассмотренным в данном руководстве для версии 11.1. Для дополнительной информации обратитесь к Руководству пользователя установленной у вас версии Dr.Web для файловых серверов UNIX.

Если версия Dr.Web для файловых серверов UNIX, подлежащая обновлению, работает под управлением сервера централизованной защиты, то перед началом обновления рекомендуется сохранить адрес сервера централизованной защиты, к которому подключен Dr.Web для файловых серверов UNIX. Например, для получения адреса сервера централизованной защиты, к которому подключен Dr.Web для файловых серверов UNIX с версией новее 6.0.2, вы можете воспользоваться командой:

```
$ 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 для файловых серверов UNIX, а также к администратору вашей антивирусной сети.

Обновление через установку универсального пакета

Выполните установку Dr.Web для файловых серверов UNIX версии 11.1 из универсального пакета. Если автоматическое обновление невозможно, то в процессе

установки новой версии программа установки предложит вам автоматически удалить имеющиеся компоненты старой версии Dr.Web для файловых серверов UNIX.

Если в процессе обновления вам необходимо выполнить удаление имеющейся версии Dr.Web для файловых серверов UNIX и на вашем сервере одновременно установлено несколько серверных продуктов Dr.Web (например, для файловых серверов, для почтовых серверов и интернет-шлюзов), то для сохранения работоспособности продуктов, не подлежащих обновлению (для почтовых серверов и интернет-шлюзов) 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 версии 11.1 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 для файловых серверов UNIX на отдельную машину.

Чтобы обновить текущую версию Dr.Web для файловых серверов UNIX, установленную из репозитория компании «Доктор Веб»

В зависимости от типа используемых пакетов, вам необходимо выполнить следующие действия:

- **Пакеты RPM (yum, dnf)**

1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 11.1).

   

   Имя репозитория, хранящего пакеты версии 11.1, 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 для файловых серверов UNIX 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 установку Dr.Web для файловых серверов UNIX. При необходимости см. разделы Удаление Dr.Web для файловых серверов UNIX, установленного из репозитория и Установка из репозитория (пункты, соответствующие используемой вами ОС и менеджеру пакетов).

- **Пакеты DEB (apt-get)**

1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов версии 11.1).
2. Обновите пакеты Dr.Web для файловых серверов UNIX, выполнив команды:

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

В ОС Ubuntu 14.04 (64-битная версия) применение команды `apt-get dist-upgrade` для обновления дистрибутива может завершиться неудачей. В этом случае используйте менеджер пакетов aptitude (для обновления дистрибутива используйте команду aptitude `dist-upgrade`).

Перенос ключевого файла

При любом способе обновления Dr.Web для файловых серверов UNIX уже имеющийся у вас ключевой файл будет автоматически установлен в надлежащее место для использования новой версией.

В случае возникновения проблем с автоматической установкой лицензионного ключевого файла, вы можете выполнить его установку вручную.

В случае утраты действующего лицензионного ключевого файла обратитесь в службу технической поддержки.

Повторное подключение к серверу централизованной защиты

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

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

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

Обновление баз 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, куда будут загружены обновления>
   ```

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
   ```

Удаление Dr.Web для файловых серверов UNIX

В зависимости от способа установки, вы можете удалить Dr.Web для файловых серверов UNIX одним из двух способов.

1. Запустите программу удаления универсального пакета.
2. Удалите пакеты, установленные из репозитория компании «Доктор Веб», используя системный менеджер пакетов.

> После удаления Dr.Web для файловых серверов UNIX, 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).

Удаление универсального пакета

Удаление Dr.Web для файловых серверов UNIX, установленного из универсального пакета, можно выполнить при помощи командной строки (в графическом режиме необходимо наличие эмулятора терминала).

Программа удаления удалит не только Dr.Web для файловых серверов UNIX, но и все другие продукты Dr.Web, установленные на вашем компьютере.

Если на вашем компьютере, кроме Dr.Web для файловых серверов UNIX, установлены и другие продукты Dr.Web, для удаления только Dr.Web для файловых серверов UNIX вместо запуска программы автоматического удаления воспользуйтесь процедурой выборочной установки/удаления компонентов.

Удаление Dr.Web для файловых серверов UNIX из командной строки

Для запуска программы удаления запустите файл скрипта `uninst.sh`, который расположен в каталоге <*opt_dir*>`/bin` (в ОС GNU/Linux — `/opt/drweb.com/bin`). Процедура удаления Dr.Web для файловых серверов UNIX рассмотрена в разделе Удаление в режиме командной строки.

Имеется возможность запустить программу удаления в полностью автоматическом режиме, запустив скрипт с помощью команды:

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

В этом случае программа удаления будет запущена в полностью автоматическом режиме, без показа интерфейса пользователя (включая диалоги программы удаления для режима командной строки).

Запуск программы удаления в полностью автоматическом режиме требует наличия прав суперпользователя. Для повышения прав вы можете использовать команды `su` и `sudo`.

В Альт 8 СП и других ОС, использующих устаревшие версии пакетного менеджера, во время удаления универсального пакета 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.

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 «Do you want to continue?». 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.

Удаление Dr.Web для файловых серверов UNIX, установленного из репозитория

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

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

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

Debian, Mint, Ubuntu (apt)

Для удаления корневого метапакета Dr.Web для файловых серверов UNIX выполните команду:

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

Для удаления метапакета Dr.Web для файловых серверов UNIX вместе со всеми зависимостями воспользуйтесь опцией `--autoremove`:

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

Для автоматического удаления из системы всех более не используемых пакетов можно дополнительно воспользоваться командой:

```
# apt-get autoremove
```

Особенности удаления

1. Первый вариант команды удалит только пакет `drweb-file-servers`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Второй вариант команды удалит из системы все пакеты, название которых начинается на "`drweb`" (стандартное наименование для пакетов программных продуктов Dr.Web).
   Эта команда удалит из системы все пакеты с таким именем, а не только пакеты Dr.Web для файловых серверов UNIX.
3. Третий вариант команды удалит из системы все пакеты, которые были автоматически установлены для удовлетворения зависимостей других пакетов, но более не требуемые (например, ввиду удаления исходного пакета).
   Эта команда удалит из системы все более не требуемые пакеты, а не только пакеты Dr.Web для файловых серверов UNIX.

Удаление пакетов Dr.Web для файловых серверов UNIX также может осуществляться с помощью альтернативных менеджеров (например, Synaptic или aptitude).

ALT Linux, PCLinuxOS (apt-rpm)

Удаление Dr.Web для файловых серверов UNIX в данном случае выполняется так же, как и в Debian, Ubuntu (см. выше).

Удаление пакетов Dr.Web для файловых серверов UNIX также может осуществляться 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)

Для удаления Dr.Web для файловых серверов UNIX выполните команду:

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

Для автоматического удаления из системы всех более не используемых пакетов можно воспользоваться командой:

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

Особенности удаления

1. Первый вариант команды удалит только пакет `drweb-file-servers`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Второй вариант команды удалит из системы пакет `drweb-file-servers`, а также все пакеты, которые были автоматически установлены для удовлетворения зависимостей других пакетов, но более не требуемые (например, ввиду удаления исходного пакета).
   Эта команда удалит из системы все более не требуемые пакеты, а не только пакеты Dr.Web для файловых серверов UNIX.

Удаление пакетов Dr.Web для файловых серверов UNIX также может осуществляться с помощью альтернативных менеджеров (например, `rpmdrake`).

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

Для удаления всех установленных пакетов Dr.Web выполните команду (в некоторых системах символ '`*`' требуется экранировать: '`\*`'):

```
# yum remove drweb*
```

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

```
# dnf remove drweb*
```

Особенности удаления

Эти варианты команд удалят из системы все пакеты, название которых начинается на "`drweb`" (стандартное наименование для пакетов программных продуктов Dr.Web).
Эти команды удалят из системы все пакеты с таким именем, а не только пакеты Dr.Web для файловых серверов UNIX.

Удаление пакетов Dr.Web для файловых серверов UNIX также может осуществляться с помощью альтернативных менеджеров (например, PackageKit или Yumex).

SUSE Linux (zypper)

Для удаления Dr.Web для файловых серверов UNIX выполните команду:

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

Для удаления всех установленных пакетов Dr.Web выполните команду (в некоторых системах символ '*' требуется экранировать: '*'):

```
# zypper remove drweb*
```

Особенности удаления

1. Первый вариант команды удалит только пакет `drweb-file-servers`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Второй вариант команды удалит из системы все пакеты, название которых начинается на "`drweb`" (стандартное наименование для пакетов программных продуктов Dr.Web).
   Эта команда удалит из системы все пакеты с таким именем, а не только пакеты Dr.Web для файловых серверов UNIX.

Удаление пакетов Dr.Web для файловых серверов UNIX также может осуществляться с помощью альтернативных менеджеров (например, YaST).

Дополнительно

Пакеты и файлы Dr.Web для файловых серверов UNIX

Пакеты

Dr.Web для файловых серверов UNIX 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 для

Пакет	Содержимое
	файловых серверов UNIX, 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 для файловых серверов UNIX
`drweb-ctl`	Файлы компонента Dr.Web Ctl
`drweb-documentation`	Файлы HTML-документации по продуктам Dr.Web для UNIX
`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 для файловых серверов UNIX
`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 SpIDer 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 SpIDer Guard для SMB (демон мониторинга SMB)
`drweb-smbspider`	Файлы компонента SpIDer Guard для SMB
`drweb-smbspider-modules`	Файлы компонента SpIDer Guard для SMB (модули VFS SMB)

Пакет	Содержимое
drweb-smbspider-modules-src	Файлы компонента SpIDer Guard для SMB (исходные коды модуля VFS SMB)
drweb-snmpd	Файлы компонента Dr.Web SNMPD
drweb-spider	Файлы компонента SpIDer Guard
drweb-spider-kmod	Файлы модуля ядра GNU/Linux для работы SpIDer 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 для файловых серверов UNIX.

Файлы

Файлы Dr.Web для файловых серверов UNIX 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
`<etc_dir>/`	Общий конфигурационный файл `drweb.ini` и ключевой файл `drweb32.key`. Кроме этого, содержит:
`certs/`	– файлы используемых сертификатов.
<opt_dir>`/`	Основной каталог Dr.Web для файловых серверов UNIX. 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:

Каталог	Содержимое
doc/	▫ документация Dr.Web для файловых серверов UNIX (файлы readme, текст Лицензионного соглашения и руководства администратора, если пакеты с документацией установлены),
drweb-bases/	▫ файлы вирусных баз Dr.Web (исходные образы, поставляемые при установке),
drweb-spider-kmod/	▫ файлы модуля ядра для работы компонента SplDer Guard (исходные коды для ручной сборки),
scripts/	▫ файлы вспомогательных скриптов.
<*var_dir*>/	Вспомогательные и временные файлы, в том числе:
bases/	– файлы вирусных баз Dr.Web (актуальная обновленная версия);
cache/	– кеш обновлений;
drl/	– списки используемых серверов обновлений;
dws/	– файлы базы категорий веб-ресурсов;
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.

Дополнительную информацию о принятой системе обозначений каталогов см. в разделе Введение.

Выборочные установка и удаление компонентов

В этом разделе

- Типовые комплекты компонентов для выборочной установки
- Установка и удаление компонентов Dr.Web для файловых серверов UNIX:
  - установленного из репозитория
  - установленного из универсального пакета

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

Для переустановки некоторого компонента вы можете сначала удалить его, а потом установить заново.

Типовые комплекты компонентов для выборочной установки

Если требуется установить Dr.Web для файловых серверов UNIX 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 наборы компонентов, предназначенные для решения типовых задач Dr.Web для файловых серверов UNIX. В столбце **Пакет для установки** перечислены пакеты, которые необходимо установить для получения указанного набора 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 для файловых серверов UNIX, установленного из репозитория

Если Dr.Web для файловых серверов UNIX был установлен из репозитория, для установки и удаления отдельного компонента воспользуйтесь соответствующей командой менеджера пакетов, используемого в вашей ОС. Например:

1. Чтобы удалить компонент Dr.Web ClamD (пакет `drweb-clamd`) из состава Dr.Web для файловых серверов UNIX, установленного в ОС CentOS, используйте команду:

   ```
   # yum remove drweb-clamd
   ```

2. Чтобы добавить компонент Dr.Web ClamD (пакет `drweb-clamd`) в состав Dr.Web для файловых серверов UNIX, установленного в ОС Ubuntu, используйте команду:

   ```
   # apt-get install drweb-clamd
   ```

При необходимости воспользуйтесь справкой по менеджеру пакетов, используемому в вашей ОС.

Установка и удаление компонентов Dr.Web для файловых серверов UNIX, установленного из универсального пакета

Если Dr.Web для файловых серверов UNIX был установлен из универсального пакета, и вы желаете дополнительно установить или переустановить пакет некоторого компонента, вам понадобится установочный файл (с расширением `.run`), из которого был установлен Dr.Web для файловых серверов UNIX. Если вы не сохранили этот файл, загрузите его с веб-сайта компании «Доктор Веб».

Распаковка установочного файла

При запуске run-файла вы можете воспользоваться следующими параметрами командной строки:

`--noexec` — вместо запуска процесса установки просто распаковать установочные файлы Dr.Web для файловых серверов UNIX. Файлы будут распакованы в каталог, указанный в системной переменной `TMPDIR` (обычно это каталог `/tmp`);

`--keep` — не удалять установочные файлы Dr.Web для файловых серверов UNIX и журнал установки по окончании установки;

`--target` <*каталог*> — распаковать установочные файлы Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX следует обратиться к каталогу, содержащему распакованные установочные файлы. Если этот каталог отсутствует, выполните команду:

```
$ ./<имя_файла>.run --noexec --target <каталог>
```

В результате в каталоге <*каталог*> появится вложенный каталог <*имя_файла*>, содержащий распакованные установочные файлы.

Выборочная установка компонентов

Установочный run-файл содержит пакеты всех компонентов, из которых состоит Dr.Web для файловых серверов UNIX (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 для файловых серверов UNIX. Имена всех пакетов, содержащих компоненты Dr.Web для файловых серверов UNIX, начинаются с префикса «drweb».

Для установки пакетов в состав установочного комплекта включен менеджер пакетов. Для выборочной установки следует использовать служебный скрипт `installpkg.sh`. Для этого необходимо предварительно распаковать содержимое установочного пакета в некоторый каталог.

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

Чтобы выполнить установку пакета компонента, необходимо перейти в каталог, содержащий распакованный установочный комплект, и выполнить в консоли (или в эмуляторе консоли — терминале для графического режима) команду:

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

Например:

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

Если требуется запустить программу установки Dr.Web для файловых серверов UNIX целиком, следует запустить скрипт автоматической установки, выполнив команду:

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

Кроме этого, вы можете установить все пакеты Dr.Web для файловых серверов UNIX (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

Для выборочного удаления пакета некоторого компонента используйте соответствующую команду удаления менеджера пакетов вашей операционной системы, если в вашей ОС используется формат пакетов RPM:

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

Например, для Red Hat Enterprise Linux:

```
# yum remove drweb-clamd
```

Если ваша ОС использует пакеты формата DEB (в т. ч. ОС МСВС 3.0), либо если в составе системы не имеется менеджера пакетов (FreeBSD), для выборочного удаления следует воспользоваться менеджером пакетов `zypper`, автоматически установленным в рамках установки Dr.Web для файловых серверов UNIX. Для этого перейдите в каталог *<opt_dir>*`/bin` (для GNU/Linux — `/opt/drweb.com/bin`), и выполните команду:

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

Например:

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

Если вы хотите удалить Dr.Web для файловых серверов UNIX целиком, запустите скрипт автоматического удаления, выполнив команду:

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

Для переустановки некоторого компонента вы можете сначала удалить его, а потом установить, запустив выборочную или полную установку из комплекта.

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 для файловых серверов UNIX при настройках по умолчанию. Для обеспечения корректной работы Dr.Web для файловых серверов UNIX в этом случае необходимо внести дополнительные изменения в настройки подсистемы безопасности и/или Dr.Web для файловых серверов UNIX.

В этом разделе рассматриваются следующие настройки, обеспечивающие корректную работу Dr.Web для файловых серверов UNIX:

- настройка политик безопасности SELinux;
- настройка запуска в режиме замкнутой программной среды (ОС Astra Linux SE, версии 1.6 и 1.7).

Настройка разрешений системы мандатного доступа PARSEC для Dr.Web для файловых серверов UNIX позволит обходить его компонентам 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 для файловых серверов UNIX, 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`. При этом будет возможна проверка файлов, для доступа к которым необходим уровень привилегий не выше уровня, с которым работает пользователь, запустивший сеанс проверки.

Данный режим имеет особенности:

- для запуска автономной копии 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 для файловых серверов UNIX подключен к серверу централизованной защиты, автономная копия не сообщает серверу централизованной защиты об угрозах, обнаруженных при запуске в режиме автономной копии;
- все вспомогательные компоненты, обслуживающие работу запущенной автономной копии, 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, созданным запущенной автономной копии в каталоге временных файлов (указанном в системной переменной окружения `TMPDIR`);
- пути к файлам вирусных баз, антивирусного ядра и исполняемым файлам используемых при сканировании компонентов заданы по умолчанию, либо берутся из специальных переменных окружения;
- число одновременно работающих автономных копий не ограничено;
- при завершении работы автономно запущенной копии также завершает работу и комплект обслуживающих ее работу компонентов.

Настройка политик безопасности SELinux

Если используемый вами дистрибутив GNU/Linux оснащен подсистемой безопасности SELinux (*Security-Enhanced Linux — Linux с улучшенной безопасностью*), то для того, чтобы служебные компоненты Dr.Web для файловых серверов UNIX (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 для файловых серверов UNIX 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 для файловых серверов UNIX.

Если попытка установки Dr.Web для файловых серверов UNIX из установочного файла 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:

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

Если SELinux работает в режиме *Enforced*, следует временно (на период установки Dr.Web для файловых серверов UNIX) перевести 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 для файловых серверов UNIX из установочного файла, но до его запуска и активации верните режим *Enforced*, для чего выполните команду:

```
# setenforce 1
```

Проблемы функционирования Dr.Web для файловых серверов UNIX

В некоторых случаях при работающем SELinux отдельные компоненты Dr.Web для файловых серверов UNIX (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 располагается 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, необходимо скомпилировать 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 для файловых серверов UNIX. Если это не так, следует или дождаться таких инцидентов в процессе работы Dr.Web для файловых серверов UNIX, или создать 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 для файловых серверов UNIX.

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 Linux.

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 котором запускаются только приложения, исполняемые файлы которых подписаны цифровой подписью разработчика, чей открытый ключ добавлен в перечень ключей, которым доверяет ОС.

По умолчанию компоненты Dr.Web для файловых серверов UNIX, поставляемые для исполнения в среде Astra Linux SE, подписаны цифровой подписью компании «Доктор Веб», а открытый ключ для этой цифровой подписи автоматически добавляется в перечень доверенных при установке программы, в связи с чем Dr.Web для файловых серверов UNIX должен корректно запускаться при активизации режима ЗПС в ОС Astra Linux SE версии 1.5 и более старой.

Начиная с версии 1.6, в ОС Astra Linux SE механизм подписи был изменен. Для обеспечения запуска Dr.Web для файловых серверов UNIX в режиме ЗПС в ОС версий 1.6 и 1.7 необходимо выполнить предварительные настройки системы.

Чтобы настроить Astra Linux SE версий 1.6 и 1.7 для запуска Dr.Web для файловых серверов UNIX в режиме ЗПС

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

Начало работы

1. Для начала работы с установленным Dr.Web для файловых серверов UNIX выполните его активацию, получив и установив ключевой файл.
2. Далее рекомендуется выполнить проверку работоспособности Dr.Web для файловых серверов UNIX.
3. Интегрируйте Dr.Web для файловых серверов UNIX 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, в зависимости от поставки).

   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, вы можете воспользоваться:

   - Утилитой управления из командной строки Dr.Web Ctl (используйте команды `drweb-ctl appinfo`, `drweb-ctl cfshow` и `drweb-ctl cfset`).
   - Веб-интерфейсом управления Dr.Web для файловых серверов UNIX (по умолчанию доступ через браузер по адресу `https://127.0.0.1:4443/`).

Регистрация и активация

В этом разделе

Приобретение и регистрация лицензий

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» https://license.drweb.ru/license_manager.

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем Dr.Web для файловых серверов UNIX, и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки. Приобретенная лицензия может быть активирована непосредственно на веб-сайте компании «Доктор Веб» по адресу https://products.drweb.ru/register/v4.

При активации приобретенной лицензии необходимо указать ее серийный номер. Этот номер может поставляться вместе с Dr.Web для файловых серверов UNIX или по электронной почте, при покупке или продлении лицензии онлайн.

Запрос демонстрационного периода

Для получения демонстрационного периода на использование Dr.Web для файловых серверов UNIX следует обратиться к мастеру запроса демо на веб-сайте компании «Доктор Веб» по адресу https://download.drweb.ru/demoreq/biz/v2/. 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 для файловых серверов UNIX может быть выдан повторно для того же компьютера только по истечении определенного периода времени.

Вы можете воспользоваться командой `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.

Установка ключевого файла

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

При работе Dr.Web для файловых серверов UNIX ключевой файл по умолчанию должен находиться в каталоге <*etc_dir*> (для GNU/Linux — `/etc/opt/drweb.com`) и называться `drweb32.key`.

Компоненты Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX 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 zip-архивы. Архив, содержащий ключевой файл для активации Dr.Web для файловых серверов UNIX, обычно имеет имя `agent.zip`. Если в сообщении 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).

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 для файловых серверов UNIX переносится на другой сервер), имеется возможность активировать Dr.Web для файловых серверов UNIX, просто указав путь к имеющемуся ключевому файлу. Это можно сделать следующим образом:

1. Распакуйте ключевой файл, если он был вами получен в архиве.
2. Далее выполните любое из указанных ниже действий.
   - Скопируйте его в каталог <*etc_dir*> и, при необходимости, переименуйте в `drweb32.key`.
   - В файле конфигурации Dr.Web для файловых серверов UNIX установите значение параметра `KeyPath` таким образом, чтобы он указывал на ключевой файл.
3. Перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

   ```
   # drweb-ctl reload
   ```

   для применения внесенных изменений.

Вы можете также воспользоваться командой:

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

В последнем случае перезапускать Dr.Web для файловых серверов UNIX не требуется. Ключевой файл не будет скопирован в каталог *<etc_dir>*, а останется в исходном каталоге.

Об условных обозначениях путей *<opt_dir>*, *<etc_dir>* и *<var_dir>* см. Введение.

Если ключевой файл не скопирован в каталог *<etc_dir>*, 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 необходимо указать 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 https://products.drweb.com/register/. 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.

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 вируса.

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 COM-файла для ОС MS DOS/MS Windows, в результате исполнения которого на консоль 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 файл, содержащий приведенную выше строку, то в результате получится программа, которая и будет описанным «вирусом».

В случае корректной работы Dr.Web для файловых серверов UNIX, 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 для файловых серверов UNIX при помощи тестовой программы EICAR из командной строки:

```
$ tail <opt_dir>/share/doc/drweb-se/readme.eicar | grep X5O > testfile &&
drweb-ctl rawscan testfile && rm testfile
```

Данная команда выделяет из файла <*opt_dir*>`/share/doc/drweb-se/readme.eicar` (поставляется вместе с Dr.Web для файловых серверов UNIX) строку, представляющую собой тело тестовой программы EICAR, записывает ее 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).

Об условных обозначениях путей <*opt_dir*>, <*etc_dir*> и <*var_dir*> см. Введение.

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 (см. Приложение Е. Описание известных ошибок).

Если в системе работает монитор файловой системы SpIDer 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.

Настройка мониторинга файловой системы

В этом разделе

Для настройки мониторинга файловой системы GNU/Linux монитором SpIDer 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 воспользуйтесь командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

- Для переключения SplDer Guard в режим работы `FANOTIFY` используйте команду:

```
$ sudo drweb-ctl cfset LinuxSpider.Mode FANOTIFY
```

- Для изменения режима мониторинга используйте команду:

```
$ sudo 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.

- Для изменения срока актуальности результатов проверки файлов, хранимых Dr.Web File Checker в кеше, используйте команду:

```
$ sudo drweb-ctl cfset FileCheck.RescanInterval <период>
```

где *<период>* определяет период актуальности предыдущих результатов проверки, находящихся в кэше. Допустимо значение от `0s` до `1m` (включительно). Если указан период менее 1 секунды, то файл будет проверяться при любом запросе.

После внесения изменений в настройки перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

```
# drweb-ctl reload
```

Также вы можете выполнить перезапуск демона управления конфигурацией Dr.Web ConfigD с помощью команды:

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

Интеграция с файловым сервером Samba

В этом разделе

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 для файловых серверов UNIX 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 исходных кодов см. в разделе 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/vfs`) создать символическую ссылку `smb_spider.so`, указывающую на модуль VFS SMB Dr.Web, соответствующий используемой версии сервера Samba.

   Модули VFS SMB, поставляемые Dr.Web, расположены в каталоге с библиотеками <*opt_dir*>`/lib/<`*архитектура*`>-linux-gnu/samba/vfs` (в Debian, Ubuntu, Mint) или <*opt_dir*>`/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 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` (см. ниже).

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 персональные 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, достаточно использовать команду `drweb-ctl cfset SmbSpider.Share.<имя ресурса>.<параметр> <значение>`, например:

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

   Данная команда добавит в файл конфигурации секцию `[SMBSpider.Share.UserFiles]`. 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 работу SpIDer Guard для SMB, задав для параметра `Start` значение `Yes`.

После внесения изменений в настройки перезапустите как сервер Samba, так и Dr.Web для файловых серверов UNIX, выполнив команду:

```
# drweb-ctl reload
```

Также вы можете выполнить перезапуск демона 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, используйте 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
```

Интеграция с томами NSS

Для интеграции Dr.Web для файловых серверов UNIX 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 должен быть исключены из проверки и наоборот, проверяться монитором SpIDer Guard для NSS. Допускается указание путей как к каталогам, так и к конкретным файлам. Если указан каталог, то будет пропускаться или проверяться все содержимое этого каталога.

  

  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 работу SpIDer Guard для NSS, задав для параметра `Start` значение `Yes`.

После внесения изменений в настройки перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

```
# drweb-ctl reload
```

Также вы можете выполнить перезапуск демона управления конфигурацией Dr.Web ConfigD с помощью команды:

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

Краткие инструкции

В этом разделе

Как подключить Dr.Web для файловых серверов UNIX к серверу Samba

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

Как подключить Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX

Для перезапуска уже работающего Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX.

Скрипт для управления Dr.Web ConfigD располагается в стандартном для ОС каталоге (для GNU/Linux — `/etc/init.d/`; для FreeBSD — `/usr/local/etc/rc.d/`) 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 для файловых серверов UNIX.
`stop`	Завершить работу Dr.Web ConfigD, если он запущен. При завершении работы Dr.Web ConfigD завершит работу всех компонентов Dr.Web для файловых серверов UNIX.
`restart`	Перезапустить (завершить и запустить) Dr.Web ConfigD. Dr.Web ConfigD, соответственно, завершит и запустит все компоненты Dr.Web для файловых серверов UNIX. 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 для файловых серверов UNIX. Используется для инициации процесса перечитывания конфигурации всеми компонентами Dr.Web для файловых серверов UNIX.
`status`	Вывести на консоль текущее состояние Dr.Web ConfigD.

Например, для перезапуска (или запуска, если он не был запущен) Dr.Web для файловых серверов UNIX в GNU/Linux используйте 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, возможно, дополнительные параметры, такие, как идентификатор рабочей станции и пароль, или идентификаторы основной и тарифной группы.
2. Воспользуйтесь командой `esconnect` утилиты управления Dr.Web для файловых серверов UNIX из командной строки Dr.Web Ctl.

Для подключения обязательно нужно использовать опцию `--Certificate`, указав путь к файлу сертификата сервера. Дополнительно вы можете указать идентификатор узла («рабочей 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 опцию `--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 для файловых серверов UNIX к серверу централизованной защиты:

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

После успешного подключения к серверу централизованной защиты Dr.Web для файловых серверов UNIX 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 того, чтобы потребовать безусловного использования мобильного режима, необходимо установить значение этого параметра в значение `On`. Для работы в режиме централизованной защиты параметр следует установить в значение `Off`.

Типовой пример команды перевода Dr.Web для файловых серверов UNIX, 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 для файловых серверов UNIX в мобильный режим.

Как отключиться от сервера централизованной защиты

Для отключения Dr.Web для файловых серверов UNIX от сервера централизованной защиты и перевода его в одиночный (standalone) режим воспользуйтесь командой `esdisconnect` управления Dr.Web для файловых серверов UNIX из командной строки Dr.Web Ctl:

```
# drweb-ctl esdisconnect
```

Для успешной работы Dr.Web для файловых серверов UNIX в одиночном режиме необходимо иметь действующий лицензионный ключевой файл. В противном случае антивирусные функции Dr.Web для файловых серверов UNIX после перехода в одиночный режим *будут заблокированы*.

Как активировать Dr.Web для файловых серверов UNIX

1. Пройдите регистрацию на веб-сайте компании «Доктор Веб» по адресу https://products.drweb.ru/register/v4.
2. Получите на указанный при регистрации адрес электронной почты (или загрузите непосредственно с веб-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*> — произвольная строка-комментарий (не обязательно).
2. Если требуется задать для добавленного разделяемого каталога настройки проверки, отличающиеся от заданных для SplDer 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 для файловых серверов UNIX.

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 для файловых серверов UNIX.

Как обновить версию Dr.Web для файловых серверов UNIX

Обновите версии компонентов или выполните переход на новую версию.

Вам может быть предложено удалить текущую версию Dr.Web для файловых серверов UNIX.

Как добавить или удалить компонент Dr.Web для файловых серверов UNIX

Воспользуйтесь процедурой выборочной установки и удаления.

При установке или удалении компонента для удовлетворения зависимостей могут быть дополнительно установлены или удалены другие компоненты Dr.Web для файловых серверов UNIX.

Как управлять работой компонентов

Для просмотра состояния компонентов Dr.Web для файловых серверов UNIX и управления их работой вы можете воспользоваться:

- Утилитой управления из командной строки Dr.Web Ctl (используйте команды `drweb-ctl appinfo`, `drweb-ctl cfshow` и `drweb-ctl cfset`. Для просмотра перечня доступных команд управления используйте команду `drweb-ctl --help`).
- Веб-интерфейсом управления Dr.Web для файловых серверов UNIX (по умолчанию доступ через браузер по адресу `https://127.0.0.1:4443/`).

Как просмотреть журнал Dr.Web для файловых серверов UNIX

При настройках по умолчанию общий журнал всех компонентов Dr.Web для файловых серверов UNIX выводится в `syslog` (файл, в который записывает сообщения системный компонент `syslog`, зависит от системы, и располагается 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 воспользоваться командой `drweb-ctl log`.

Для изменения настроек ведения журнала используйте утилиту управления из командной строки Dr.Web Ctl или веб-интерфейс управления Dr.Web для файловых серверов UNIX (если он установлен).

- Для облегчения идентификации ошибок рекомендуется настроить вывод общего журнала всех компонентов в отдельный файл и разрешить вывод расширенной отладочной информации. Для этого выполните следующие команды:

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

- Для возврата настроек ведения общего журнала всех компонентов по умолчанию выполните следующие команды:

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

Компоненты Dr.Web для файловых серверов UNIX

В разделе перечислены компоненты, входящие в состав Dr.Web для файловых серверов UNIX. Для каждого компонента указано его назначение, принципы функционирования, а также параметры, которые он хранит в файле конфигурации.

Dr.Web ConfigD

Демон управления конфигурацией Dr.Web ConfigD — это центральный управляющий компонент Dr.Web для файловых серверов UNIX. Он обеспечивает централизованное хранение конфигураций для всех компонентов Dr.Web для файловых серверов UNIX, управляет активностью всех компонентов и организует доверительный обмен данными между ними.

Демон управления конфигурацией Dr.Web ConfigD выполняет следующие функции:

- запуск и остановка компонентов Dr.Web для файловых серверов UNIX 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 лицензионных данных от компонентов;
- получение новой лицензионной инфорации от специализированных компонентов;
- оповещение запущенных компонентов об изменении лицензионных данных.

Принципы работы

Демон управления конфигурацией Dr.Web ConfigD всегда запускается с правами суперпользователя *root*. Он запускает остальные компоненты Dr.Web для файловых серверов UNIX и связывается с ними через предварительно открытый сокет. Демон управления конфигурацией принимает подключения от прочих компонентов Dr.Web для файловых серверов UNIX через информационный сокет (публично доступный) и управляющий сокет (доступный только компонентам, запущенным с правами суперпользователя). Он 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 для файловых серверов UNIX.

При получении сигнала `SIGHUP`, Dr.Web ConfigD перечитывает параметры конфигурации и данные из лицензионного ключевого файла. В случае необходимости он 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 для файловых серверов UNIX 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 для файловых серверов UNIX.
   - 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 им «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, он отправляет соответствующее сообщение в *stderr* и завершает работу к 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`. Через 30 секунд после завершения сигнала компонент должен завершить работу.
   - Если компонент не завершает работу в течение положенных 30 секунд, Dr.Web ConfigD отправляет ему сигнал `SIGKILL` для принудительного завершения работы.

Аргументы командной строки

Для запуска демона управления конфигурацией Dr.Web ConfigD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-configd [<параметры>]
```

Демон управления конфигурацией 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 для файловых серверов UNIX 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 стандартном для ОС каталоге (для

GNU/Linux — `/etc/init.d/`; для FreeBSD — `/usr/local/etc/rc.d/`). Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

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

Параметры конфигурации

Демон управления конфигурацией Dr.Web ConfigD использует параметры, указанные в секции `[Root]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

В секции представлены следующие параметры:

Параметр	Описание
`DefaultLogLevel` *{уровень подробности}*	Определяет уровень подробности ведения журнала *для всех* компонентов Dr.Web для файловых серверов UNIX по умолчанию. Используется, если в конфигурации какого-либо из компонентов не указан свой уровень подробности ведения журнала. Значение по умолчанию: `Notice`
`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. Обратите внимание, что 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 для файловых серверов UNIX.

Параметр	Описание
	Значение по умолчанию: `/var/run/.com.drweb.public`
`AdminSocketPath` *{путь к файлу}*	Путь к сокету, используемому для взаимодействия компонентов Dr.Web для файловых серверов UNIX, обладающих повышенными (административными) полномочиями. Значение по умолчанию: `/var/run/.com.drweb.admin`
`CoreEnginePath` *{путь к файлу}*	Путь к динамической библиотеке антивирусного ядра Dr.Web Virus-Finding Engine. Значение по умолчанию: <*var_dir*>`/lib/drweb32.dll` • 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: <*var_dir*>`/bases` • Для GNU/Linux: `/var/opt/drweb.com/bases` • Для FreeBSD: `/var/drweb.com/bases`
`KeyPath` *{путь к файлу}*	Путь к ключевому файлу (лицензионному или демонстрационному). Значение по умолчанию: <*etc_dir*>`/drweb32.key` • Для GNU/Linux: `/etc/opt/drweb.com/drweb32.key` • Для FreeBSD: `/usr/local/etc/drweb.com/drweb32.key`
`CacheDir` *{путь к каталогу}*	Путь к каталогу кеша (используется как для кеша обновлений, так и для кеша проверенных файлов). Значение по умолчанию: <*var_dir*>`/cache` • 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 `/tmp`.
`RunDir` *{путь к каталогу}*	Путь к каталогу, в котором находятся PID-файлы запущенных компонентов и сокеты, используемые для взаимодействия компонентов Dr.Web для файловых серверов UNIX. Значение по умолчанию: `/var/run`
`VarLibDir` *{путь к каталогу}*	Путь к каталогу библиотек, используемых компонентами Dr.Web для файловых серверов UNIX. Значение по умолчанию: <*var_dir*>`/lib` • Для GNU/Linux: `/var/opt/drweb.com/lib`

Параметр	Описание
	• Для FreeBSD: `/var/drweb.com/lib`
`VersionDir` *{путь к каталогу}*	Путь к каталогу, в котором хранится информация о текущих версиях используемых компонентов Dr.Web для файловых серверов UNIX. Значение по умолчанию: <*var_dir*>`/version` • Для GNU/Linux: `/var/opt/drweb.com/version` • Для FreeBSD: `/var/drweb.com/version`
`DwsDir` *{путь к каталогу}*	Параметр не используется. Значение по умолчанию: <*var_dir*>`/dws` • Для GNU/Linux: `/var/opt/drweb.com/dws` • Для FreeBSD: `/var/drweb.com/dws`
`AdminGroup` *{имя группы | GID}*	Группа пользователей, обладающих административными правами в рамках Dr.Web для файловых серверов UNIX. Данные пользователи наряду с суперпользователем *root* могут повышать полномочия компонентов Dr.Web для файловых серверов UNIX до полномочий суперпользователя. Значение по умолчанию: *Определяется автоматически* в момент установки Dr.Web для файловых серверов UNIX
`TrustedGroup` *{имя группы | GID}*	Параметр не используется. Значение по умолчанию: `drweb`
`DebugIpc` *{логический}*	Включать или нет 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 обращение к сервису Dr.Web Cloud для получения сведений о вредоносности файлов и URL. Значение по умолчанию: `No`
`AntispamCorePath` *{путь к файлу}*	Параметр не используется. Значение по умолчанию: <*var_dir*>`/lib/vaderetro.so` • Для GNU/Linux: `/var/opt/drweb.com/lib/vaderetro.so` • Для FreeBSD: `/var/drweb.com/lib/vaderetro.so`
`VersionNotification` *{логический}*	Уведомлять пользователя о наличии обновлений для текущей установленной версии Dr.Web для файловых серверов UNIX. Значение по умолчанию: `Yes`
`UseVxcube` *{логический}*	Использовать Dr.Web vxCube при проверке почтовых вложений в режиме внешнего фильтра, подключенного к MTA. Значение по умолчанию: `No`

Параметр	Описание
`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)*

Dr.Web Ctl

В этом разделе

Общие сведения

Имеется возможность управлять работой Dr.Web для файловых серверов UNIX из командной строки операционной системы. 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 ниже).
- Запуск обновления антивирусных компонентов (вирусных баз, антивирусного ядра, и прочих, в зависимости от поставки).
- Просмотр и изменение параметров конфигурации Dr.Web для файловых серверов UNIX.
- Просмотр состояния компонентов Dr.Web для файловых серверов UNIX и статистики обнаруженных угроз.

- Просмотр карантина и управление его содержимым.
- Просмотр карантина и управление его содержимым (через компонент Dr.Web File Checker).
- Подключение к серверу централизованной защиты и 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).

Обратите внимание, что 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 для файловых серверов UNIX, 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.

Обратите внимание, что 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 для файловых серверов UNIX 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`).

Формат вызова из командной строки

1. Формат вызова утилиты управления из командной строки

Утилита управления работой Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX (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. Зависит от команды. У некоторых команд опции отсутствуют.

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`

3. Команды

Команды управления Dr.Web для файловых серверов UNIX разделены на следующие группы:

- команды антивирусной проверки;
- команды управления обновлением и работой в режиме централизованной защиты;
- команды управления конфигурацией;
- команды управления угрозами и карантином;
- информационные команды.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-ctl`.

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.

Команда	Описание
	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 отдельную копию Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если Dr.Web для файловых серверов UNIX работает под его управлением. `--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). `--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. `--Report` <*тип*> — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*число*> — установить тайм-аут на проверку одного файла в мс. Значение `0` указывает, что время проверки не ограничено.

Команда	Описание
	Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — установить 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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т. п.), в которые вложены другие архивы, в которые, в свою очередь, могут быть вложены еще архивы, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке файлов почтовых программ (pst, tbb и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (HTML-страницы, jar-файлы и т. п.). 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*> — установить максимальную допустимую степень сжатия проверяемых объектов. Значение должно быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <size> — установить 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: нет.

Команда	Описание
	`--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--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`). `--FollowSymlinks` — автоматически разрешать символические ссылки
`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 отдельную копию Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если Dr.Web для файловых серверов UNIX работает под его управлением. `--Report` *<тип>* — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` *<число>* — установить тайм-аут на проверку одного файла в мс. 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.

Команда	Описание
	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. **Опции** `-a [--Autonomous]` — запустить отдельную копию Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если Dr.Web для файловых серверов UNIX работает под его управлением. `--Report` <*тип*> — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*число*> — установить тайм-аут на проверку одного файла в мс. 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`. `--PackerMaxLevel` <*число*> — установить 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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, и т. п. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться.

Команда	Описание
	Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--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`.  При обнаружении угроз в исполняемом файле все запущенные из него процессы принудительно завершаются Dr.Web для файловых серверов UNIX.

Команда	Описание
`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*> — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*число*> — установить тайм-аут на проверку одного файла в мс. 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`. `--PackerMaxLevel` <*число*> — установить 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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т. п.), в которые вложены другие архивы, в которые, в свою очередь, могут быть вложены еще архивы, и т. п. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться.

Команда	Описание
	Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — установить максимальный уровень вложенности объектов при проверке файлов почтовых программ (pst, tbb и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (HTML-страницы, jar-файлы и т. п.). 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*> — установить максимальную допустимую степень сжатия проверяемых объектов. Значение должно быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <size> — установить 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: нет. `--Cure` <*Yes*|*No*> — требуется ли делать попытки лечения обнаруженных угроз. Если указано `No`, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: `No`
`flowscan` <*путь*>	**Назначение**: инициировать проверку компонентом проверки файлов Dr.Web File Checker указанного файла или каталога с использованием метода проверки «flow» (штатно этот метод проверки используется монитором SplDer Guard). ⚠ Для проверки файлов и каталогов рекомендуется использовать команду `scan`. **Аргументы** <*путь*> — путь к файлу или каталогу, который нужно проверить.

Команда	Описание
	Опции `--ScanTimeout` <*число*> — установить тайм-аут на проверку одного файла в мс. 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`. `--PackerMaxLevel` <*число*> — установить 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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т. п.), в которые вложены другие архивы, в которые, в свою очередь, могут быть вложены еще архивы, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке файлов почтовых программ (pst, tbb и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (HTML-страницы, jar-файлы и т. п.). 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*> — установить максимальную допустимую степень сжатия проверяемых объектов.

Команда	Описание
	Должна быть не менее `2`. Значение по умолчанию: `3000`. `--OnKnownVirus` <*действие*> — действие, которое следует 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`).
`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. Обратите внимание, что угрозы, обнаруженные при «сыром» сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). 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 запущена автономная копия сканирующего ядра (будет завершена после завершения проверки). `--Report <тип>` — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout <число>` — установить тайм-аут на проверку одного файла в мс. Значение `0` указывает, что время проверки не ограничено.

Команда	Описание
	Значение по умолчанию: `0`. `--PackerMaxLevel <число>` — установить 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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, и т. п. 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>` — установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т. п.), в которые вложены другие архивы, в которые, в свою очередь, могут быть вложены еще архивы, и т. п. 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>` — установить максимальный уровень вложенности объектов при проверке файлов почтовых программ (pst, tbb и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. п. 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>` — установить максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (HTML-страницы, jar-файлы и т. п.). 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>` — установить максимальную допустимую степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <size> — установить 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: нет.

Команда	Описание
	`--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`. `--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*. Обратите внимание, что угрозы, обнаруженные при удаленном сканировании, не будут нейтрализованы, а также они не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). 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 `-m [--Method]` <*SSH*|*Telnet*> — метод (протокол) подключения к удаленному узлу. Если метод не указан, будет использован SSH. `-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. `-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). `--ForceInteractive` — использовать интерактивную сессию SSH (только для метода подключения SSH). *Необязательная опция.* `--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. `--Password` <*пароль*> — пароль для аутентификации указанного пользователя через выбранный протокол. Обратите внимание, что пароль передается в открытом виде. `--Exclude` <*путь*> — путь, который необходимо исключить 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.

Команда	Описание
	`--Report` <*mun*> — установить тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*число*> — установить тайм-аут на проверку одного файла в мс. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — установить 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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т. п.), в которые вложены другие архивы, в которые, в свою очередь, могут быть вложены еще архивы, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке файлов почтовых программ (pst, tbb и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. п. 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*> — установить максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (HTML-страницы, jar-файлы и т. п.). 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`.

Команда	Описание
	`--MaxCompressionRatio` <*степень*> — установить максимальную допустимую степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <size> — установить 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: нет. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`

3.2. 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 и антивирусного ядра, и прочих, в зависимости от поставки) с серверов обновлений компании «Доктор Веб» или из локального облака, через Dr.Web MeshD, прервать уже запущенный процесс обновления или откатить результаты последнего обновления, восстановив предыдущие версии обновленных файлов.  Команда не имеет эффекта, если Dr.Web для файловых серверов UNIX работает под управлением сервера централизованной защиты. **Аргументы**: нет. **Опции** `-l [--local-cloud]` — использовать для загрузки обновлений локальное облако, к которому подключен Dr.Web для файловых серверов UNIX. Если опция не указана, обновления загружаются с серверов обновлений компании «Доктор Веб» (поведение по умолчанию). `--From` <*путь*> — выполнить обновление из указанного каталога без подключения к интернету.

Команда	Описание
	`--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. `--Rollback` — откатить последнее обновление и восстановить последние сохраненные копии обновленных файлов. `--Stop` — прервать уже идущий процесс обновления
`esconnect` <*сервер*>`[:`<*порт*>`]`	**Назначение**: подключить Dr.Web для файловых серверов UNIX к указанному серверу централизованной защиты (например, Dr.Web Enterprise Server). 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. `--Login` <*ID*> — логин (идентификатор рабочей станции) для подключения к серверу централизованной защиты. `--Password` <*пароль*> — пароль для подключения к серверу централизованной защиты. `--Group` <*ID*> — идентификатор группы на сервере, в которую следует поместить рабочую станцию при подключении. `--Rate` <*ID*> — идентификатор тарифной группы, которую следует применить к рабочей станции при ее включении в группу на сервере централизованной защиты (может быть указана только совместно с опцией `--Group`). `--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).

Команда	Описание
	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 для файловых серверов UNIX от сервера централизованной защиты и перевести его в одиночный режим работы. Команда не имеет эффекта, если Dr.Web для файловых серверов UNIX уже работает в одиночном режиме (standalone mode). **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`.

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 для файловых серверов UNIX. **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 для файловых серверов UNIX, 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 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*>, используйте команду:

Команда	Описание
	`cfset ClamD.Endpoint.<point> -a`, например: `cfset ClamD.Endpoint.point1 -a` `cfset SmbSpider.Share.<tag> -a`, например: `cfset SmbSpider.Share.BuhFiles -a` Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя. При необходимости используйте команды `su` или `sudo`.
`cfshow [<секция>[.<параметр>]]`	**Назначение**: вывести на экран параметры текущей конфигурации Dr.Web для файловых серверов UNIX. 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. **Опции** `--Uncut` — вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. В противном случае 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 INI-файла: 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**: послать сигнал `SIGHUP` демону управления конфигурацией Dr.Web ConfigD. Получив этот сигнал, Dr.Web ConfigD перечитывает конфигурацию и рассылает ее изменения всем компонентам Dr.Web для файловых серверов UNIX; переоткрывает журнал Dr.Web для файловых серверов UNIX; перезагружает компоненты, использующие вирусные

Команда	Описание
	базы (включая антивирусное ядро), а также пытается перезапустить компоненты, работа которых была нештатно завершена. **Аргументы**: нет. **Опции**: нет

3.4. 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); • 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]` — выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (CTRL+C прерывает ожидание). Если эта опция указана совместно с любой из опций-действий, она игнорируется. `--Directory <список каталогов>` — выводить только те угрозы, которые были обнаружены в файлах в каталогах из *<списка каталогов>*.

Команда	Описание
	Если эта опция указана совместно с любой из опций, приведенных ниже, 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
`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** `-a [--Autonomous]` — запустить отдельную копию компонента проверки файлов Dr.Web File Checker для выполнения заданного действия с карантином, завершив ее работу после окончания действия. Эта опция может быть применена совместно с любой из опций, указанных ниже. `--Format "`<*строка формата*>`"` — выводить информацию об объектах, находящихся в карантине, в указанном формате. Описание строки формата приведено ниже.

Команда	Описание
	Если эта опция указана совместно с любой из опций-действий, она игнорируется. `-f [--Follow]` — выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (CTRL+C прерывает ожидание). Если эта опция указана совместно с любой из опций-действий, она игнорируется. `--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). 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 автономной копии, т. е. с опцией `-a` (`--Autonomous`), но без опции `--Discovery`, то это равносильно вызову: `quarantine --Autonomous --Discovery` `--Delete <`*объект*`>` — удалить указанный объект из карантина. Обратите внимание: удаление из карантина — необратимая операция. `--Cure <`*объект*`>` — попытаться вылечить указанный объект в карантине. Обратите внимание: даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина воспользуйтесь опцией восстановления `--Restore`. `--Restore <`*объект*`>` — восстановить указанный объект из карантина в исходное место. Обратите внимание: для выполнения этого действия может потребоваться, чтобы `drweb-ctl` была запущена от имени суперпользователя. Восстановить файл из карантина можно, даже если он инфицирован. `--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, так и относительный (относительно текущего каталога) путь. Обратите внимание: опция применяется только совместно с опцией восстановления `--Restore`.

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

Если в настройках SplDer 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 (вируса) по классификации компании «Доктор Веб»
`%{threat_type}`	Тип угрозы («known virus» и т. д.) по классификации компании «Доктор Веб»

Маркер	Описание
`%{size}`	Размер исходного файла
`%{origin}`	Полное имя исходного файла с путем
`%{path}`	Синоним для `%{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 для файловых серверов UNIX, 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 повторно 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

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

3.5. Информационные команды

Доступны следующие информационные команды:

Команда	Описание
`appinfo`	**Назначение**: вывести на экран информацию о работающих компонентах Dr.Web для файловых серверов UNIX. 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.

Команда	Описание
	Опции `-f [--Follow]` — выполнять ожидание поступления новых сообщений об изменении состояния модулей и выводить их на экран сразу, как только они будут поступать (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 вирусных записей; • 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 вирусных записей в каждом файле
`certificate`	**Назначение**: вывести на экран содержимое доверенного сертификата Dr.Web, который используется Dr.Web для файловых серверов UNIX. Для сохранения сертификата в файл <*cert_name*>`.pem` вы можете использовать команду: `$ drweb-ctl certificate > <cert_name>.pem` **Аргументы**: нет. **Опции**: нет
`events`	**Назначение**: просмотреть события Dr.Web для файловых серверов UNIX. Кроме этого команда позволяет выполнить управление событиями (отметка как «прочитанные», удаление). **Аргументы**: нет. **Опции** `--Report` <*mun*> — установить тип отчета о событиях. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON.

Команда	Описание
	`-f [--Follow]` — выполнять ожидание поступления новых событий и выводить их на экран сразу, как только они будут поступать (нажатие CTRL+C прерывает ожидание). `-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). Доступны следующие типы событий: • `Mail` — обнаружена угроза в сообщении электронной почты; • `UnexpectedAppTermination` — аварийное завершение работы некоторого компонента. Для вывода событий всех типов используйте `All`. `--ShowSeen` — показать также и уже прочитанные события. `--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). 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 для файловых серверов UNIX в виде HTML-страницы (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` выше. Обязательный аргумент. **Опции** `-o [--Output]` <*путь к файлу*> — сохранить отчет в указанный файл. Обязательная опция.

Команда	Описание
	`-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. Например, команда: `$ drweb-ctl report Mail -o report.html` сформирует отчет по всем имеющимся событиям обнаружения угроз в сообщениях электронной почты на основе шаблона по умолчанию и сохранит результат в файл `report.html` в текущем каталоге
`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 одиночного 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. **Опции** `--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). Если серийный номер не является серийным номером демонстрационного периода, то он должен быть предварительно зарегистрирован на сайте компании. `--Proxy http://`<*имя пользователя*>`:`<*пароль*>`@`<*адрес сервера*>`:`<*номер порта*> — получить лицензионный ключ через прокси-сервер (используется только совместно с опцией `--GetRegistered`). Подробнее о лицензировании продуктов Dr.Web см. раздел Лицензирование.

Команда	Описание
	 Для регистрации серийного номера требуется наличие подключения к интернету.
`log`	**Назначение**: вывести на экран консоли (в поток *stdout*) последние записи журнала Dr.Web для файловых серверов UNIX (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 запятую. Если параметр не указан, выводятся 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` (см. выше). `-f [--Follow]` — выполнять ожидание поступления новых записей в журнал и выводить их на экран консоли сразу же, как только они будут поступать (нажатие CTRL+C прерывает ожидание)
`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:

Команда	Описание
	• среднее за секунду количество проверенных файлов; • среднее за секунду количество переданных и полученных байт; • среднее за секунду количество ошибок. **Аргументы**: нет. **Опции** `-n [--netcheck]` — вывести на экран статистику работы агента сетевой проверки данных

Примеры использования

В этом разделе приведены примеры использования утилиты Dr.Web Ctl (`drweb-ctl`):

- Проверка объектов:
  - Простые команды проверки
  - Проверка файлов, отобранных по критериям
  - Проверка дополнительных объектов
- Управление конфигурацией
- Управление угрозами
- Пример работы в режиме автономной копии

1. Проверка объектов

1.1. Простые команды проверки

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

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

2. Выполнить проверку списка путей, перечисленных 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
```

1.2. 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 01 мая 2017 года:

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

1.3. Проверка дополнительных объектов

1. Проверка объектов, расположенном в каталоге `/tmp` на удаленном узле *192.168.0.1*, подключившись к нему через SSH как пользователь *user* с паролем *passw*:

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

2. Управление конфигурацией

1. Вывести на экран информацию о текущем составе Dr.Web для файловых серверов UNIX, включая информацию о запущенных компонентах:

```
$ drweb-ctl appinfo
```

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

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

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

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

Обратите внимание, что 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 для файловых серверов UNIX:

```
$ drweb-ctl update
```

5. Выполнить перезагрузку конфигурации для компонентов Dr.Web для файловых серверов UNIX:

```
# drweb-ctl reload
```

Обратите внимание, что 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 для файловых серверов UNIX 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 для файловых серверов UNIX к серверу централизованной защиты, используя файл настроек подключения settings.cfg:

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

8. Отключить Dr.Web для файловых серверов UNIX от сервера централизованной защиты:

```
# drweb-ctl esdisconnect
```

Обратите внимание, что 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 для файловых серверов UNIX:

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

3. 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
```

4. Пример работы в режиме автономной копии

1. Проверить файлы и обработать карантин в режиме автономной копии:

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

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

Параметры конфигурации

Утилита управления из командной строки Dr.Web Ctl не имеет собственной секции параметров в объединенном конфигурационном файле Dr.Web для файловых серверов UNIX. Она использует параметры, указанные в секции `[Root]`.

Веб-интерфейс управления Dr.Web

В этом разделе:

Назначение

Веб-интерфейс управления Dr.Web для файловых серверов UNIX позволяет выполнять следующие действия:

1. Просматривать состояние компонентов Dr.Web для файловых серверов UNIX, запускать и останавливать работу некоторых из них.
2. Просматривать состояние обновлений и запускать обновление вручную при необходимости.
3. Просматривать состояние лицензии и загружать лицензионный ключ при необходимости.
4. Просматривать перечень обнаруженных угроз и управлять содержимым карантина (отображаются только угрозы, обнаруженные в файлах локальной файловой системы при помощи компонента Dr.Web File Checker).
5. Выполнять редактирование настроек компонентов Dr.Web для файловых серверов UNIX.
6. Подключать Dr.Web для файловых серверов UNIX к серверу централизованной защиты или переводить его в автономный режим работы.
7. 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 — версия 11 и новее.
- Mozilla Firefox — версия 25 и новее.
- Google Chrome — версия 30 и новее.

Доступ к управлению через веб-интерфейс

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

```
https://<host_with_drweb>:<port>/
```

где *<host_with_drweb>* — IP-адрес или имя узла, на котором работает Dr.Web для файловых серверов UNIX, в составе которого функционирует сервер веб-интерфейса Dr.Web HTTPD, а *<port>* — порт на этом узле, прослушиваемый Dr.Web HTTPD. Для доступа к компонентам Dr.Web для файловых серверов UNIX, работающего на локальном узле, достаточно использовать IP-адрес `127.0.0.1` или имя `localhost`. 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 для файловых серверов UNIX.

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 для файловых серверов UNIX 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 и удаление вредоносных объектов.
- **Настройки** — открывает страницу управления настройками компонентов Dr.Web для файловых серверов UNIX, 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 ее закрытия.
- **Выйти** — завершает сеанс работы текущего пользователя с веб-интерфейсом управления (недоступно, если используется авторизация по личному сертификату пользователя).

Управление компонентами

Просмотр перечня компонентов, включенных в состав Dr.Web для файловых серверов UNIX, и управление их работой осуществляются на странице **Главная**.

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

1. **Название**. Щелчок мышью по названию позволяет перейти к странице настроек этого 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, достаточно щелкнуть мышью по переключателю. 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. Щелчок мышью по значку  выводит на экран 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 с компонентом в течение последней минуты, 5 минут, 15 минут (три числа, разделенных косой чертой).

При наведении курсора мыши на значок  можно получить всплывающую подсказку.

Под таблицей основных компонентов в виде набора плиток перечисляются вспомогательные компоненты Dr.Web для файловых серверов UNIX (такие, как сканирующее ядро, компонент проверки файлов и т. д.). Для них также указываются состояние и статистика их работы. Щелчок мышью по названию компонента открывает 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 вспомогательного компонента доступен выключатель для управления его запуском.

В нижней части страницы указывается информация о состоянии обновлений вирусных баз и о состоянии 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 для файловых серверов UNIX.

Управление угрозами

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

На этой странице показывается полный перечень угроз, обнаруженных в процессе работы компонентами Dr.Web для файловых серверов UNIX, 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. Активная категория, угрозы из которой в данный момент отображаются в списке, отмечается в меню жирным шрифтом. Для отображения в списке угроз требуемой категории угроз достаточно щелкнуть мышью по названию требуемой категории 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 Dr.Web для файловых серверов UNIX, обнаружившего угрозу в данном файле.
- **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 щелчке по 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 изолирован в карантин.
- Полный путь к файлу в исходном месте (там, где в нем была обнаружена угроза).

Чтобы выделить объект в списке, достаточно щелкнуть левой кнопкой мыши в строке списка. Чтобы выделить в списке более одного объекта, необходимо отметить флажки в строках выделяемых объектов. Чтобы за один раз выделить все объекты, или снять выделение со всех объектов в списке, необходимо отметить или снять отметку у флажка, расположенного 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 (обратите внимание, что некоторые из них могут быть недоступны в зависимости от типа выделенных угроз):

	– Удалить отмеченные файлы.
	– Восстановить отмеченные файлы из карантина в исходное место.
	– Применить некоторое 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.

Обратите внимание, что 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 `Quarantine`, то при восстановлении угрозы этого типа из карантина на том NSS, она будет снова незамедлительно перемещена в карантин. Например, настройки монитора по умолчанию помещают все неизлечимые объекты в карантин. Поэтому, при восстановлении неизлечимого объекта из карантина на том NSS, он будет снова незамедлительно перемещен в карантин.

На странице списка угроз доступна также панель фильтрации списка угроз на основании поискового запроса. Чтобы отфильтровать список угроз, оставив в нем только те объекты, в описании которых присутствует заданная строка, необходимо воспользоваться 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 (регистр букв не имеет значения для поиска). Для очистки результатов поиска и возвращения к исходному списку необходимо щелкнуть левой кнопкой мыши по значку в строке поиска или очистить поисковое слово.

Управление настройками

Просмотр и изменение текущих параметров конфигурации компонентов, входящих в состав Dr.Web для файловых серверов UNIX и перечисленных на главной странице, производятся на странице **Настройки**. Кроме того, на этой странице вы можете переключить Dr.Web для файловых серверов UNIX в режим *централизованной защиты* или в *одиночный* режим работы (подробнее о режимах работы см. в разделе Режимы работы).

В левой части страницы располагается меню, в котором перечисляются все компоненты Dr.Web для файловых серверов UNIX, настройки которых доступны для просмотра и редактирования. Для просмотра и возможного изменения настроек компонента необходимо выбрать его в меню, для чего необходимо щелкнуть по его имени. 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 для файловых серверов UNIX.

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 значок сворачивания имеет вид ▸, то дополнительные секции скрыты и не видны. Если значок сворачивания имеет вид ▾, то дополнительные секции также отображаются в меню, по одной строке на дополнительную секцию. Чтобы развернуть или свернуть список подчиненных секций компонента, необходимо щелкнуть по значку сворачивания/разворачивания сбоку от имени интересующего компонента в меню.

- Дополнительные секции настроек компонента отображаются с отступом вправо. Чтобы просмотреть или отредактировать параметры дополнительной секции, щелкните по ее названию.
- Чтобы добавить для компонента новую подчиненную секцию параметров, если он допускает такую возможность, щелкните по значку +, расположенному справа от имени компонента (появляется при наведении курсора 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, щелкните по значку ×, расположенному справа от имени (тега) секции (появляется при наведении курсора 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 редакторе (в табличной форме) все параметры конфигурации компонента, доступные для просмотра и изменения.
- **Измененные** — отобразить в редакторе (в табличной форме) 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 текстовом редакторе в формате 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  . Для фильтрации списка параметров следует ввести произвольное слово в строку поиска, при этом из списка параметров будут скрыты все параметры, не содержащие в своем описании указанного слова (регистр букв не имеет значения для поиска). Для очистки результатов поиска и возвращения к исходному списку параметров, необходимо щелкнуть левой кнопкой мыши по значку  в строке поиска или очистить 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**), они отображаются в виде таблицы, каждая строка которой 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, выводятся в списке жирным шрифтом.

Общий список параметров разбит на разделы (такие как **Основные**, **Дополнительные** и т. д.). Для сворачивания и разворачивания раздела таблицы достаточно щелкнуть левой кнопкой мыши по заголовку раздела. Если раздел свернут, и параметры, входящие в него, не отображаются в таблице, то слева от имени раздела отображается значок ›.

Если раздел развернут и входящие в него параметры отображаются в таблице, слева от имени раздела отображается значок .

Для изменения параметра необходимо щелкнуть левой кнопкой мыши по текущему значению параметра в таблице (для параметра логического типа — включить или выключить флажок). Если параметр имеет строго ограниченный набор значений, то при щелчке по значению откроется выпадающее меню, в котором необходимо выбрать требуемое значение. Если значение параметра — число, то при щелчке оно будет доступно в поле редактирования прямо в таблице. В этом случае следует указать новое требуемое значение и нажать клавишу ENTER. Во всех этих случаях измененное значение параметра сразу же фиксируется в конфигурации компонента.

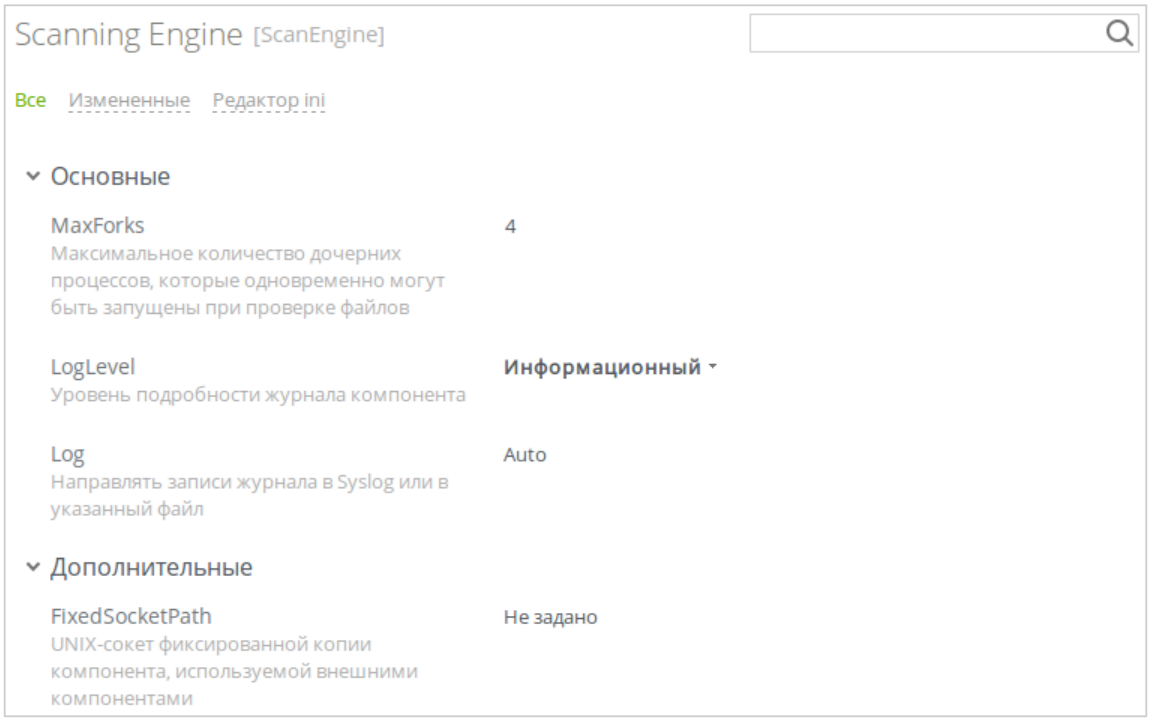

Рисунок 3. Представление настроек компонента в табличной форме

Если параметр имеет строковое значение или список произвольных значений, то при щелчке по текущему значению параметра на экране появляется всплывающее окно, в котором выводится текущее значение параметра. Если параметр имеет список значений, то элементы списка выводятся в многострочном поле редактирования, по одному в строке, как показано на рисунке ниже. Для редактирования элементов списка необходимо изменить, удалить или добавить требуемые строки в поле редактирования.

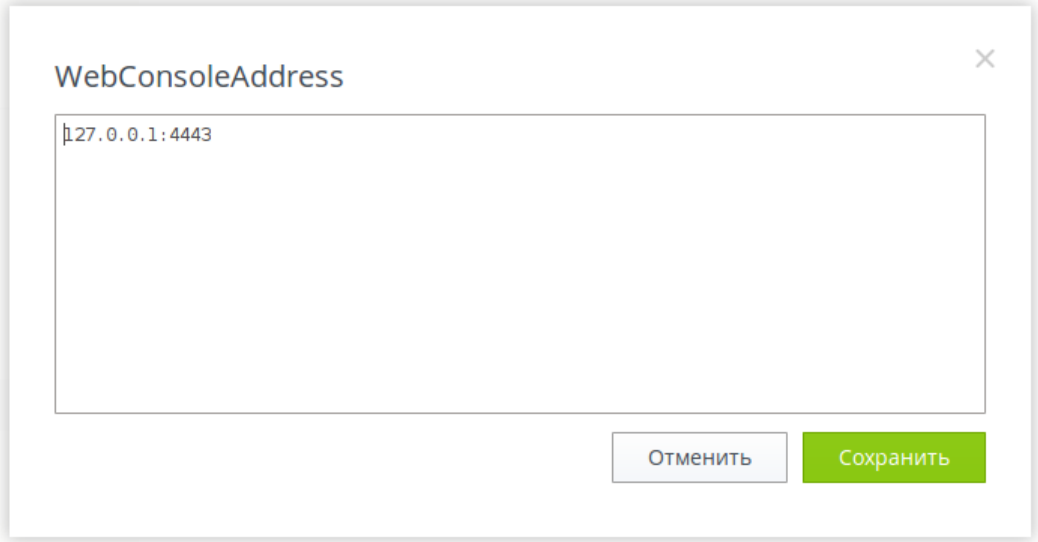

Рисунок 4. Редактирование списка значений

После редактирования значения параметра, для сохранения внесенных изменений и закрытия окна, нажмите **Сохранить**. Для закрытия окна без сохранения внесенных изменений нажмите **Отменить** или нажать значок ✕ в верхнем правом углу всплывающего окна.

Просмотр и изменение настроек компонента в текстовом редакторе

При просмотре параметров в режиме **Редактор ini**, они отображаются в простом текстовом редакторе в формате 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 редакторе простого вида показан на рисунке ниже.

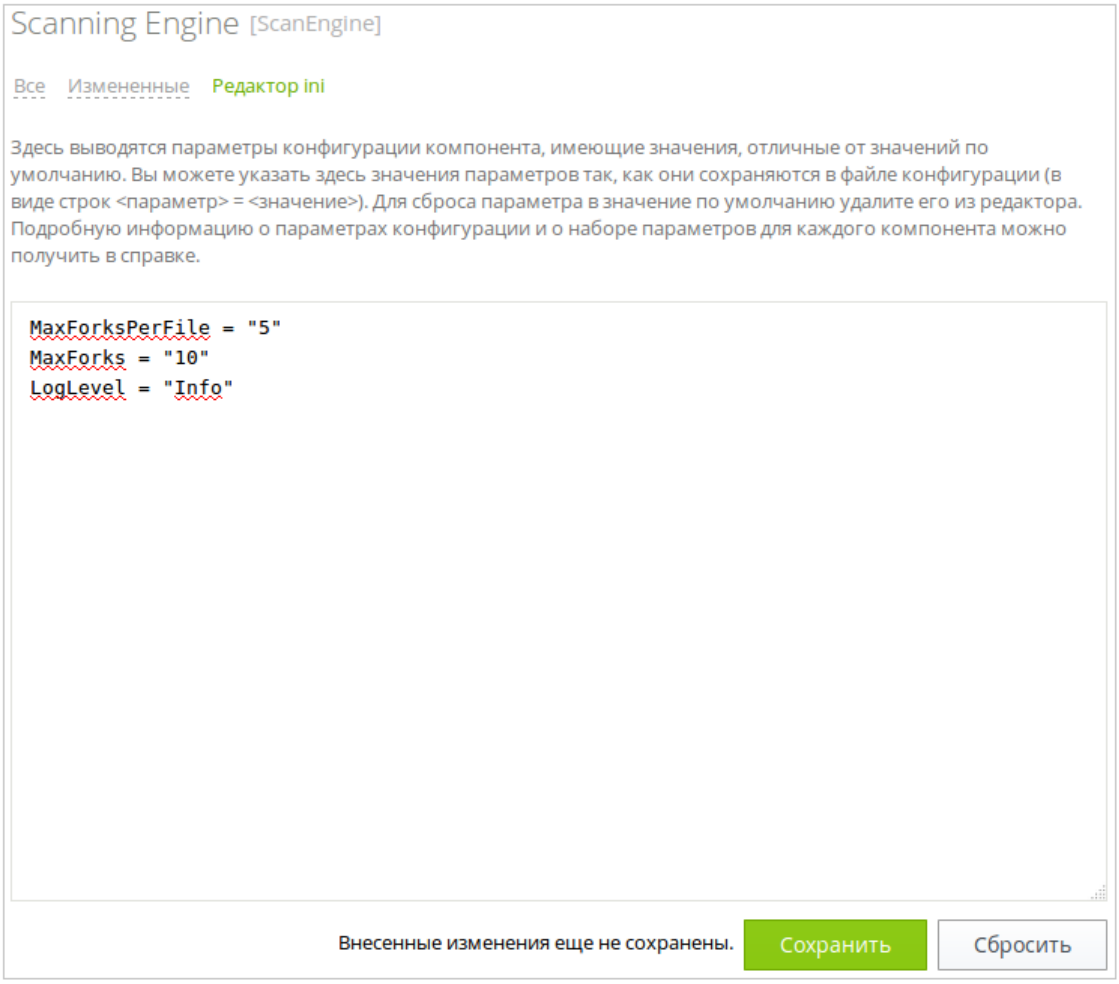

Рисунок 5. Редактор настроек для простого вида

Для внесения изменений необходимо отредактировать текст в текстовом редакторе, 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.

После редактирования, для сохранения внесенных изменений, нажмите **Сохранить**. Для отмены внесенных изменений нажмите **Отменить**.

При нажатии кнопки **Сохранить** выполняется проверка корректности текста, введенного в редактор: 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 для файловых серверов UNIX.

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.

Управление централизованной защитой

Вы можете подключить Dr.Web для файловых серверов UNIX к серверу централизованной защиты или отключить его от сервера централизованной защиты, переведя его 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 для файловых серверов UNIX 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.

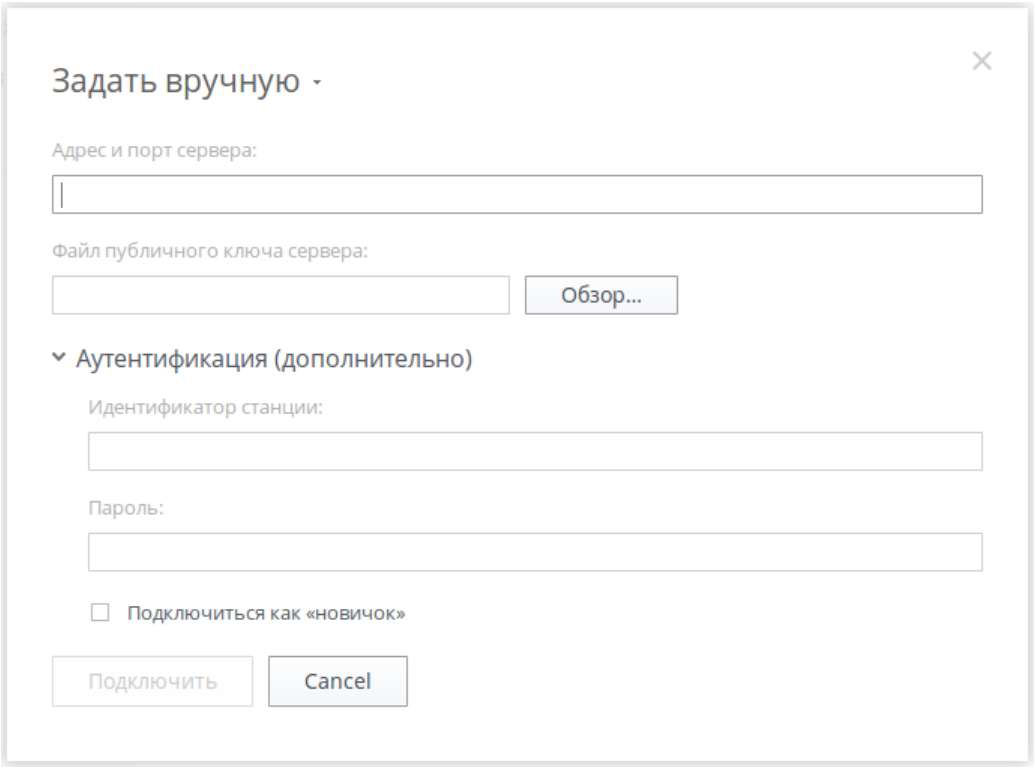

Рисунок 6. Окно подключения к серверу централизованной защиты

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

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

В случае выбора варианта *Загрузить из файла* достаточно указать 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. Обратите внимание, что 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 для файловых серверов UNIX 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 для файловых серверов UNIX.

Проверка локальных файлов

Веб-интерфейс предоставляет возможность оперативной проверки на наличие угроз файлов, находящихся на локальном компьютере, с которого осуществляется доступ к веб-интерфейсу управления, используя сканирующее ядро, входящее в состав Dr.Web для файловых серверов UNIX. Проверяемые файлы будут загружены на сервер по протоколу HTTP, но после проверки, даже в случае обнаружения угроз, они не будут сохранены на сервере, в том числе не будут добавлены в карантин. Пользователь, отправивший файлы на проверку, будет только проинформирован о ее результате.

Данная функция доступна только в том случае, если в состав Dr.Web для файловых серверов UNIX включен компонент Dr.Web Network Checker.

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.

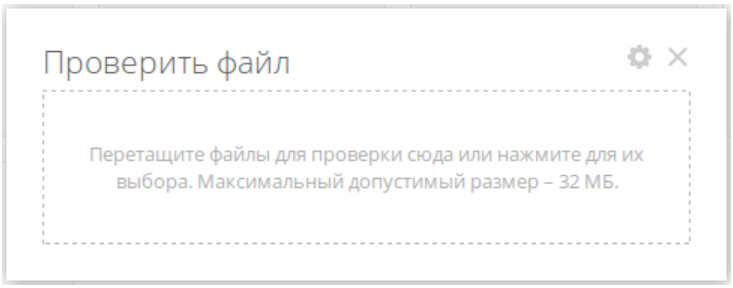

Рисунок 7. Панель проверки локальных файлов

Для закрытия панели нажмите ✕ в верхнем правом углу панели. Нажатие значка ⚙ позволяет перейти к настройкам проверки локальных файлов. В режиме настройки имеется возможность указать следующие параметры проверки локальных файлов: максимальное время отведенное на проверку файла (не считая времени его загрузки на север с локального компьютера), использование эвристического анализа при проверке, а также максимальную степень сжатия для сжатых объектов и глубину вложенности для объектов, упакованных в контейнеры (такие как архивы).

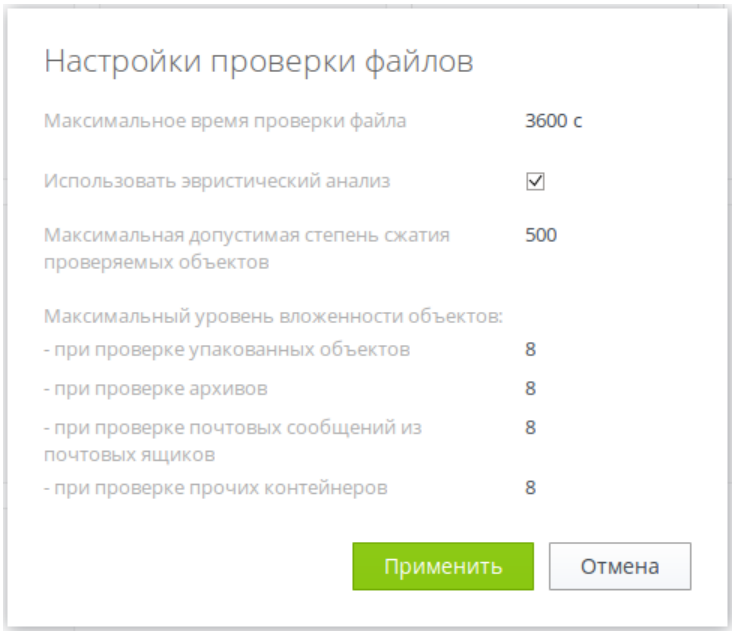

Рисунок 8. Настройка параметров проверки локальных файлов

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 щелкните левой клавишей мыши по надписи-мишени **Перетащите файлы для проверки сюда или нажмите для их выбора**. При щелчке по

надписи откроется стандартное окно выбора файлов файлового менеджера операционной системы. Вы можете выбрать одновременно несколько файлов для проверки. Обратите внимание, что выбор каталогов для проверки не допускается. Также вы 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 для файловых серверов UNIX и проверка по мере загрузки. В процессе загрузки и проверки файлов панель проверки отображает общий прогресс процесса проверки.

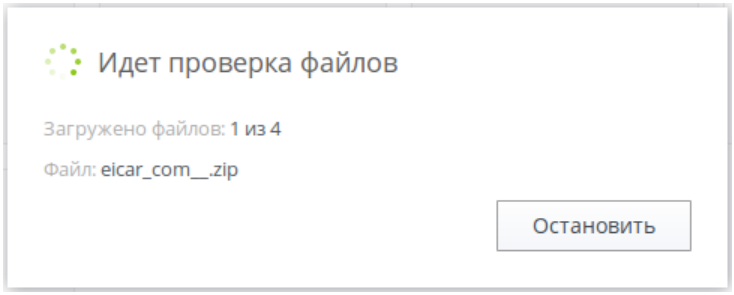

Рисунок 9. Прогресс проверки локальных файлов

В случае необходимости вы можете прервать процесс загрузки и проверки файлов. Для этого нажмите **Остановить**. По окончанию проверки на панели отображается отчет о проверке загруженных файлов.

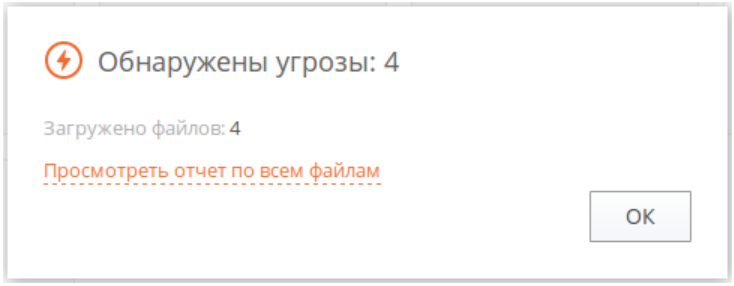

Рисунок 10. Результат проверки локальных файлов

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

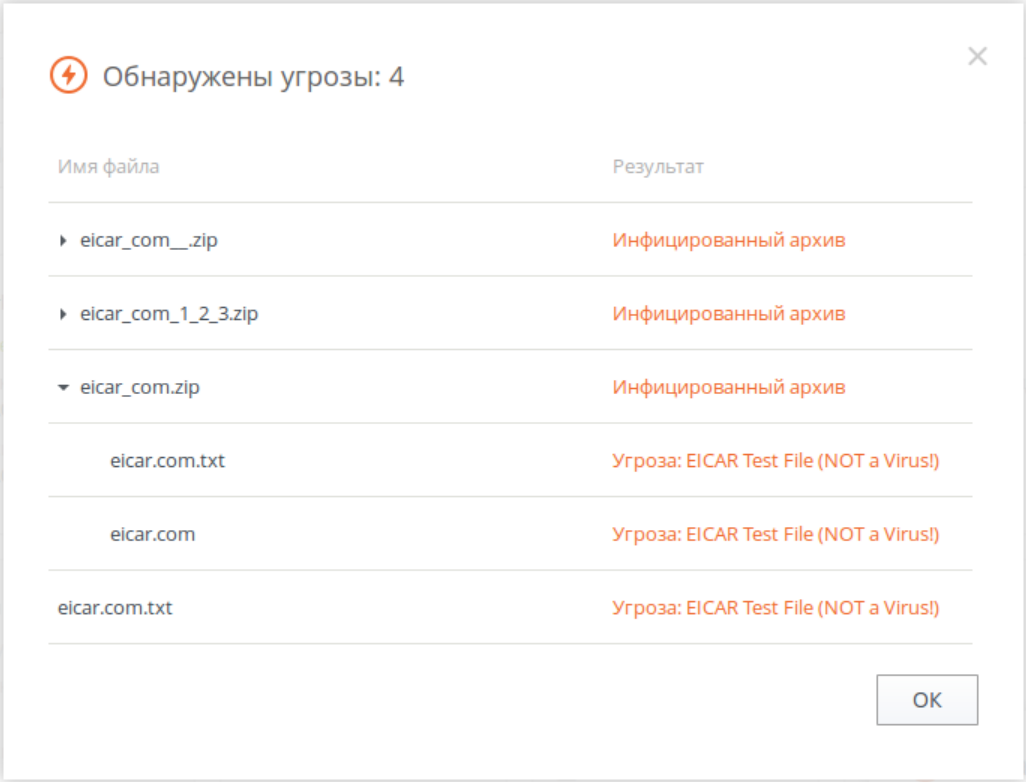

Рисунок 11. Расширенный отчет о проверке локальных файлов

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

Запуск проверки локальных файлов (с текущими настройками проверки) возможен даже тогда, когда панель проверки локальных 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.

SpIDer Guard

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

Монитор файловой системы Linux 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 если да, то он 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 программ из исполняемых файлов. Если программа, содержащаяся в исполняемом файле, по результатам проверки будет признана вредоносной, все процессы, запущенные из этого файла, будут принудительно завершены.

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 либо механизм fanotify, предоставляемый ОС, либо специальный *модуль ядра* Linux (*LKM — Linux 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 сначала попытается использовать 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 SplDer Guard уже в скомпилированном виде. Если для ОС, в которой используется SplDer Guard, модуль ядра не поставляется в скомпилированном виде, используйте исходные коды модуля, предоставляемые компанией «Доктор Веб» для сборки и установки модуля ядра вручную (инструкция по сборке приведена в разделе Сборка модуля ядра для SplDer 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).

SplDer 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 SplDer 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 SplDer 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. Обратите внимание, что 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

SplDer Guard может использовать три режима мониторинга:

- *Обычный* (установлен по умолчанию) — отслеживаются операции по доступу 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. Для файлов, считающихся исполняемыми, при попытке доступа SplDer Guard блокирует запрошенную операцию доступа до тех пор, пока не станут известны результаты проверки файла на наличие угроз.

  

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

- *«Параноидальный» режим* — при попытке доступа к любому файлу SplDer Guard блокирует запрошенную операцию доступа до тех пор, пока не станут известны результаты проверки этого файла 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 SpIDer Guard и режимах мониторинга файлов см. в разделе Настройка мониторинга файловой системы.

Аргументы командной строки

Для запуска компонента SpIDer Guard из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-spider [<параметры>]
```

SpIDer 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 SpIDer Guard.

Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически, при старте операционной системы, демоном управления конфигурацией Dr.Web ConfigD. Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

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

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[LinuxSpider]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

- Параметры компонента.
- Настройка индивидуальных параметров мониторинга защищаемых пространств.

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_dir>*`/bin/drweb-spider`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-spider`
`Start` *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно попытаться 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.
`Mode` *{LKM | FANOTIFY | AUTO}*	Определяет режим работы SplDer Guard. Возможные значения: • `LKM` — работа через LKM-модуль Dr.Web, установленный в ядро операционной системы (*LKM — Linux kernel module*); • `FANOTIFY` — работа через системный механизм *fanotify*;

Параметр	Описание
	• `AUTO` — автоматическое определение оптимального режима работы. Изменять значения этого параметра следует производить с крайней осторожностью, поскольку ядра различных ОС GNU/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 исходных кодов и установить его в систему, следуя инструкции в разделе Сборка модуля ядра для SplDer Guard. Значение по умолчанию: `AUTO`
`DebugAccess` *{логический}*	Включать/не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о доступе к файлам. Значение по умолчанию: `No`
`ExcludedProc` *{путь к файлу}*	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). Пример: Добавить в список процессы `wget` и `curl`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке: `[LinuxSpider]` `ExcludedProc = "/usr/bin/wget", "/usr/bin/curl"`

Параметр	Описание
	• Две строки (по одному значению в строке): `[LinuxSpider]` `ExcludedProc = /usr/bin/wget` `ExcludedProc = /usr/bin/curl` 2. Добавление значений через команду `drweb-ctl cfset`: `# drweb-ctl cfset LinuxSpider.ExcludedProc -a /usr/bin/wget` `# drweb-ctl cfset LinuxSpider.ExcludedProc -a /usr/bin/curl` Значение по умолчанию: *(не задано)*
`ExcludedFilesystem` *{имя файловой системы}*	Не контролировать доступ к файлам указанной файловой системе. 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`. 1. 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` 2. Добавление значений через команду `drweb-ctl cfset`: `# drweb-ctl cfset LinuxSpider.ExcludedFilesystem -a cifs` `# drweb-ctl cfset LinuxSpider.ExcludedFilesystem -a nfs` Значение по умолчанию: `cifs`
`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;

Параметр	Описание
	• `Executables` — блокировать доступ к исполняемым файлам (формата PE, ELF и скриптов, содержащих преамбулу `#!`), не проверенным монитором; • `All` — блокировать доступ к любым файлам, не проверенным монитором. Файлы блокируются только в режиме `FANOTIFY`. Значение по умолчанию: `Off`
`[*] ExcludedPath` *{путь к файлу или каталогу}*	Путь к объекту, который должен быть пропущен при мониторинге файловых операций. Допускается указание пути как к каталогу, так и к конкретному файлу. Если указан каталог, то будут исключены из наблюдения все файлы этого каталога. Допускается использовать файловые маски (содержащие символы '?' и '*', а также символьные классы '`[ ]`', '`[! ]`', '`[^ ]`'). 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 файлы `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации. • Два значения в одной строке: `[LinuxSpider]` `ExcludedPath = "/etc/file1", "/usr/bin"` • Две строки (по одному значению в строке): `[LinuxSpider]` `ExcludedPath = /etc/file1` `ExcludedPath = /usr/bin` 2. Добавление значений через команду `drweb-ctl cfset`: `# drweb-ctl cfset LinuxSpider.ExcludedPath -a /etc/file1` `# drweb-ctl cfset LinuxSpider.ExcludedPath -a /usr/bin` Обратите внимание, что не имеет смысла указывать здесь пути к символическим ссылкам, поскольку при проверке файла всегда анализируется прямой путь к нему, поэтому указанные здесь символические ссылки не будут иметь никакого эффекта. Значение по умолчанию: `/proc, /sys`

Параметр	Описание
`[*] 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. 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`

Параметр	Описание
`[*] ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`) включительно. Значение по умолчанию: `30s`
`[*] HeuristicAnalysis` *{On | Off}*	Использовать/не использовать эвристический анализ для поиска возможных неизвестных угроз. Эвристический анализ повышает надежность проверки, но увеличивает ее длительность. Реакция на срабатывание эвристического анализа задается в параметре `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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, 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`
`[*] ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (zip, rar и т. п.), в которые вложены другие архивы, в которые, в свою очередь, могут быть вложены еще архивы, и т. п. 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 вложены объекты, и т. п. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться.

Параметр	Описание
	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, HTML-страницы, jar-файлы 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`

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
`Enable` *{логический}*	Содержимое защищаемого пространства, расположенное внутри пути `Path` (см. ниже), 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`

`Path` *{путь к каталогу}*	Определяет путь к каталогу файловой системы, хранящем 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)*

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 символом "`[*]`" в таблице выше, и переопределяющих данный параметр для этого защищаемого пространства (например, реакцию на обнаружение угроз, максимальную глубину проверки архивов и т. п.). Если для защищаемого пространства не указан некоторый из параметров, то к наблюдению над файлами в этом пространстве применяются значения соответствующих параметров, взятых 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`), достаточно использовать 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]`.

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 SpIDer 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 SpIDer Guard поставляется скомпилированный модуль ядра для всех ОС, указанных в разделе Системные требования и совместимость. Кроме этого совместно с компонентом SpIDer Guard поставляется архив в формате `tar.bz2`, содержащий исходные файлы загружаемого модуля ядра, чтобы его можно было собрать вручную.

Загружаемый модуль ядра, используемый SpIDer Guard, предназначен для работы с ядрами GNU/Linux версий 2.6.* и новее.

В Dr.Web для файловых серверов UNIX для архитектур ARM64 и E2K работа с загружаемым модулем ядра не поддерживается.

Архив с исходными кодами загружаемого модуля ядра располагается в каталоге основных файлов Dr.Web для файловых серверов UNIX <*opt_dir*> (для GNU/Linux — `/opt/drweb.com`), в подкаталоге `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 для файловых серверов UNIX. 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 для файловых серверов UNIX).

Для выполнения ручной сборки загружаемого модуля ядра из исходных кодов необходимо обладать правами суперпользователя (*root*). Для получения прав суперпользователя при сборке воспользуйтесь командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

Инструкция по сборке модуля ядра

1. Распакуйте архив с исходными кодами 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 исходными кодами и выполните команду:

   ```
   # make
   ```

   В случае возникновения ошибок на этапе `make` следует их устранить (см. ниже) и выполнить компиляцию повторно.

3. После успешного окончания этапа `make` выполните следующие команды:

   ```
   # make install
   # depmod
   ```

4. После успешной сборки модуля ядра и его регистрации в системе, выполните дополнительно настройку SplDer 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 SplDer Guard будет пробовать использовать не только модуль ядра, но и системный механизм fanotify. Для получения дополнительной информации используйте 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 исходных кодов ядра. В этом случае используйте команду `make` с параметром `KDIR=`*<путь к исходным кодам ядра>*. Обычно они размещаются в каталоге `/usr/src/kernels/`*<версия ядра>*.

Версия ядра, выдаваемая командой `uname -r`, может не совпадать с именем каталога *<версия ядра>*.

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 исходных кодов описана в разделе Сборка модуля VFS SMB.

Принципы работы

В этом разделе:

- Общие сведения.

- Определение 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, возможно, инфицирован какой-либо вредоносной программой. Получив такую информацию, пользователь может выполнить антивирусную проверку своего компьютера, обнаружить и обезвредить свои 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.

Определение областей файловой системы, подлежащих наблюдению

Имеется возможность запретить компоненту наблюдать за указанными каталогами и файлами, находящимися внутри контролируемых разделяемых каталогов сервера Samba. Это может быть необходимо, если некоторые файлы изменяются слишком часто, что заставляет монитор столь же часто их проверять. Частая проверка файлов в хранилище 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` — содержит список путей, подлежащих мониторингу («область наблюдения»).
- `ExcludedPath` — содержит список путей, которые требуется исключить 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 принадлежат исключения, определяемой списком `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, параметр `IncludedPath` имеет смысл использовать для включения в область наблюдения отдельных каталогов и файлов, находящихся внутри области исключения.

Имеется возможность задать различные параметры защиты для различных разделяемых каталогов Samba, находящихся под защитой монитора SpIDer Guard для SMB, включая различные 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 для файловых серверов UNIX с файловой службой см. в разделе Интеграция с файловым сервером Samba.

Аргументы командной строки

Для запуска компонента SpIDer Guard для SMB из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически, при старте операционной системы, демоном управления конфигурацией Dr.Web ConfigD. Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

> Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-smbspider-daemon`.

Параметры конфигурации

В этом разделе

- Параметры компонента
- Настройка индивидуальных параметров мониторинга

Компонент использует параметры конфигурации, заданные в секции `[SMBSpider]` объединенного Приложение Г. Конфигурационный файл Dr.Web для файловых серверов UNIX Dr.Web для файловых серверов UNIX.

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`

Параметр	Описание
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: <*opt_dir*>`/bin/drweb-smbspider-daemon`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-smbspider-daemon`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-smbspider-daemon`
`Start` *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: `No`
`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)*
`SmbSocketPath` *{путь к файлу}*	Путь к файлу сокета для взаимодействия SplDer Guard для SMB с модулям VFS SMB. Этот путь всегда является относительным и дополняет путь, указанный в значении параметра `SambaChrootDir` (если параметр `SambaChrootDir` пуст, то дополняется путь к корню файловой системы `/`). Значение по умолчанию: `var/run/.com.drweb.smb_spider_vfs`
`ActionDelay` *{интервал времени}*	Определяет величину задержки, которую SplDer 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: `24h`

Параметр	Описание
`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`
`[*] ExcludedPath` *{путь к файлу или каталогу}*	Путь к объекту внутри разделяемого каталога, который должен быть пропущен при проверке. Допускается указание пути как к каталогу, так и к конкретному файлу. 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 файлы `/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` 2. Добавление значений через команду `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 как к каталогу, так и к конкретному файлу. Допускается использовать файловые маски (содержащие символы '`?`' и '`*`', а также символьные классы '`[ ]`', '`[! ]`', '`[^ ]`').

Параметр	Описание
	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 `/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 через команду `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. Обратите внимание, что этот параметр имеет приоритет над параметром `ExcludedPath` (см. выше), т. е. если один и тот же объект (файл или каталог) включен в оба параметра, то он будет проверен. Значение по умолчанию: *(не задано)*
`[*] AlertFiles` *{логический}*	Создавать/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. Значение по умолчанию: `Yes`
`[*] OnKnownVirus` *{действие}*	Действие при обнаружении известной угрозы. Допустимые значения: `Block`, `Cure`, `Quarantine`, `Delete`. Значение по умолчанию: `Cure`

Параметр	Описание
`[*] 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`, `Block`, `Quarantine`, `Delete`. Значение по умолчанию: `Quarantine`
`[*] OnAdware` *{действие}*	Действие при обнаружении рекламной программы. Допустимые значения: `Pass`, `Block`, `Quarantine`, `Delete`. Значение по умолчанию: `Pass`
`[*] OnDialers` *{действие}*	Действие при обнаружении программы автоматического дозвона. Допустимые значения: `Pass`, `Block`, `Quarantine`, `Delete`. Значение по умолчанию: `Pass`
`[*] OnJokes` *{действие}*	Действие при обнаружении программы-шутки. Допустимые значения: `Pass`, `Block`, `Quarantine`, `Delete`. Значение по умолчанию: `Pass`
`[*] OnRiskware` *{действие}*	Действие при обнаружении потенциально опасной программы. Допустимые значения: `Pass`, `Block`, `Quarantine`, `Delete`. Значение по умолчанию: `Pass`
`[*] OnHacktools` *{действие}*	Действие при обнаружении хакерской программ. Допустимые значения: `Pass`, `Block`, `Quarantine`, `Delete`. Значение по умолчанию: `Pass`
`[*] BlockOnError` *{логический}*	Блокировать/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. При отсутствии действующей лицензии, если этот параметр установлен в значение `Yes`, SplDer Guard для SMB будет блокировать все файлы, помещаемые в защищаемый им разделяемый каталог.

Параметр	Описание
	Допустимые значения: • `Yes` — блокировать доступ к файлу; • `No` — не блокировать. 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/не использовать эвристический анализ для поиска возможных неизвестных угроз. Эвристический анализ повышает надежность проверки, но увеличивает ее длительность. Реакция на срабатывание эвристического анализа задается в параметре `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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, 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`
`[*] ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (zip, rar и т. п.), в которые вложены другие архивы, в которые, в свою очередь, могут быть вложены еще архивы, и т. п. 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 т. п.), в которые могут быть вложены объекты, в которые также могут вложены объекты, 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`
`[*] ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов с вложениями (например, HTML-страницы, jar-файлы 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, то он будет пропущен при проверке, инициированной по запросу SplDer Guard для SMB. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`

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 некоторого модуля VFS SMB определен уникальный тег *<имя>*, то имеется возможность добавить в конфигурационный файл Dr.Web для файловых серверов UNIX, наряду с секцией `[SMBSpider]`, хранящей все параметры работы с SMB, отдельную секцию, регулирующую только параметры проверки конкретного хранилища,

защищаемого модулем VFS SMB, имеющим присвоенный тег. Эта 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.

Для всех параметров, которые не указаны в индивидуальной секции `[SMBSpider.Share.<имя>]`, использующий ее модуль VFS SMB будет брать соответствующих параметров 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 некоторый 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 для файловых серверов UNIX из командной строки Dr.Web Ctl (запускается командой `drweb-ctl`), достаточно использовать команду:

```
# drweb-ctl cfset SmbSpider.Share -a <имя>
```

Пример:

```
# drweb-ctl cfset SmbSpider.Share -a BuhFiles
# drweb-ctl cfset SmbSpider.Share.BuhFiles.OnAdware Quarantine
```

Первая команда добавит в файл конфигурации секцию `[SMBSpider.Share.BuhFiles]`, 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]`.

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.

Исходные коды вспомогательного модуля VFS SMB, используемого SpIDer Guard для SMB, поставляются в отдельном пакете `drweb-smbspider-modules-src` и запакованы в архив формата `tar.gz`. При установке пакета `drweb-smbspider-modules-src` архив с исходными кодами 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 для файловых серверов UNIX).

Кроме исходных кодов модуля VFS SMB, используемого SpIDer Guard для SMB, вам потребуются также исходные коды используемой вами версии сервера Samba. В случае их отсутствия загрузите их, например, воспользовавшись источником https://www.samba.org/samba/download/. Для определения, какая версия Samba у вас используется, введите команду:

```
$ smbd -V
```

Вспомогательный модуль VFS SMB, используемый SpIDer Guard для SMB, должен быть собран с использованием исходных кодов той версии Samba, которая работает на вашем файловом сервере, в противном случае работоспособность SpIDer Guard для SMB не гарантируется.

Для выполнения сборки из исходных кодов необходимо обладать правами суперпользователя. Для получения прав суперпользователя при сборке воспользуйтесь командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

Инструкция по сборке модуля VFS SMB

1. Распакуйте архив с исходными кодами 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 исходные коды, 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 исходными кодами 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 исходных кодов Samba, обратитесь к документации разработчика, например, перейдя по ссылке https://www.samba.org/samba/docs/.

   

   Сборка Samba из исходных кодов нужна только для последующей правильной сборки модуля VFS SMB, используемого SplDer Guard для SMB. Замены установленного у вас сервера Samba на собранный из исходных кодов не потребуется.

5. После успешного окончания сборки Samba перейдите в каталог с исходными кодами модуля VFS SMB и выполните команду:

   ```
   # ./configure --with-samba-source=<путь к каталогу исходных кодов Samba> && make
   ```

   где *<путь к каталогу исходных кодов 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/samba/vfs`) с переименованием файла в `smb_spider.so`, выполнив, например, команду:

   ```
   # cp ./.libs/libsmb_spider.so /usr/lib/samba/vfs/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 для файловых серверов UNIX с сервером Samba, как это описано в соответствующем разделе Руководства администратора (обратите внимание, что на первом шаге интеграции в данном случае не требуется создавать символической ссылки `smb_spider.so` в каталоге VFS-модулей сервера Samba).

SpIDer Guard для NSS

Компонент 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 и более поздних.

Монитор томов NSS 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 монитор формирует задание компоненту проверки файлов Dr.Web File Checker на проверку содержимого измененного файла.

Принципы работы

В этом разделе

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 некоторого типа 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.

Задание путей к проверяемым объектам

Монитор томов NSS SplDer Guard для NSS будет проверять только те объекты файловой системы, которые находятся на защищаемых томах (параметр `ProtectedVolumes`) и пути к которым на этих томах не соответствуют путям, указанным в параметре `ExcludedPath`, или 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 некотором каталоге 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 вирусной активности, а следствием работы некоторой доверенной программы, то можно добавить путь к этому каталогу или файлам в список исключений. В этом случае монитор томов NSS SplDer Guard для NSS не будет реагировать на изменения этих файлов. Параметр `IncludedPath` разумно использовать, если нужно обеспечить проверку некоторых 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` не будут

проверяться только файлы в каталоге `/path2`, но при этом будут проверяться файлы во всех прочих каталогах этого тома, не находящихся в каталоге `/path2`, а также содержимое каталога `/path2/incl`. Обратите внимание, что 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 этот каталог не находится в зоне исключений, заданной для тома `vol2` (она содержит только каталог `/sys`).

Параметры `IncludedPath` и `ExcludedPath` допускают использование файловых масок (*wildcards*). Например, следующая 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 для файловых серверов UNIX с файловой службой см. в разделе Интеграция с томами NSS.

Аргументы командной строки

Для запуска компонента SpIDer Guard для NSS из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически, при старте операционной системы, демоном управления конфигурацией Dr.Web ConfigD. Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-nss`

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[NSS]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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`
`LogProtocol` *{логический}*	Определяет, следует ли сохранять в журнал монитора томов NSS SplDer Guard для NSS также и сообщения протокола. Возможные значения: • `Yes` — сохранять; • `No` — не сохранять. Значение по умолчанию: `No`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: <*opt_dir*>`/bin/drweb-nss`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-nss`
`Start` *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. 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.

Параметр	Описание
	• Два значения в одной строке: `[NSS]` ` ProtectedVolumes = "vol1", "vol2"` • Две строки (по одному значению в строке): `[NSS]` ` ProtectedVolumes = vol1` ` ProtectedVolumes = vol2` 2. Добавление значений через команду `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 (каталогу или файлу), который должен быть пропущен при проверке. Если указан каталог, то будет пропущено все содержимое этого каталога, включая подкаталоги, 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 файлы `/etc/file1` и каталог `/usr/bin`. 1. Добавление значений в файл конфигурации. • 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 через команду `drweb-ctl cfset`: `# drweb-ctl cfset NSS.ExcludedPath -` `a /etc/file1` `# drweb-ctl cfset NSS.ExcludedPath -a /usr/bin`

Параметр	Описание
	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 `ExcludedPath` 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 файлы `/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 через команду `drweb-ctl cfset`: `# drweb-ctl cfset NSS.IncludedPath -a /etc/file1` `# drweb-ctl cfset NSS.IncludedPath -a /usr/bin` Параметр допускает использование файловых масок (*wildcards*). 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)*

Параметр	Описание
`OnKnownVirus` *{действие}*	Действие при обнаружении известной угрозы. Допустимые значения: `Cure`, `Quarantine`, `Delete`. Значение по умолчанию: `Cure`
`OnIncurable` *{действие}*	Действие в случае неудачной попытки обнаружения 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`
`OnError` *{действие}*	Действие в случае ошибки во время проверки файла. Допустимые значения: `Report`, `Quarantine`, `Delete`. Значение по умолчанию: `Report`

Параметр	Описание
`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/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. Реакция на срабатывание эвристического анализа задается в параметре `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 других). Такие объекты могут включать другие запакованные объекты, в состав которых тоже могут входить другие запакованные объекты, 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`
`ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (zip, rar и т. п.), в которые вложены другие архивы, в которые, в свою очередь, могут быть вложены еще архивы, и т. п. 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 вложены объекты, и т. п. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться.

Параметр	Описание
	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, HTML-страницы, jar-файлы 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, 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.

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®, использовать для антивирусной проверки файлов Dr.Web для файловых серверов UNIX.

Принципы работы

Компонент позволяет выполнять по запросу от внешних приложений проверку на наличие угроз как содержимого файлов, расположенных в локальной файловой системе, так и непосредственно потоки данных, передаваемые внешним приложением через сокет. Кроме того, компонент может проверять содержимое файлов, для которых внешнее приложение передало через сокет отрытый дескриптор.

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 для файловых серверов UNIX, чтобы обеспечить его запуск, 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 `clamd`. Подробнее см. в разделе Интеграция с внешними приложениями.

Обнаруженные угрозы *не нейтрализуются* средствами Dr.Web для файловых серверов UNIX, внешнему приложению только возвращается результат проверки. Таким образом, внешнее приложение само несет ответственность за нейтрализацию обнаруженной угрозы.

Аргументы командной строки

Для запуска компонента Dr.Web ClamD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD по мере необходимости (обычно при старте операционной системы). Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

> Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-clamd`.

Параметры конфигурации

В этом разделе

- Параметры компонента

- Особенность настроек компонента

Компонент использует параметры конфигурации, заданные в секции `[ClamD]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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_dir*>`/bin/drweb-clamd`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-clamd`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-clamd`
`Start` *{логический}*	Компонент должен быть запущен демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно попытаться запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: `No`
`Endpoint.`<*тег*>`.ClamdSocket` *{IP-адрес | UNIX-сокет}*	Определяет точку подключения с именем <*тег*> и сокет (адрес IPv4 или адрес сокета UNIX) для клиентов, желающих проверять файлы на наличие угроз. Для одной точки <*тег*> может быть задан только один сокет.

Параметр	Описание
	Значение по умолчанию: не задано
`[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. 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.

Параметр	Описание
	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>.]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), поступившего 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

Параметр	Описание
	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 других). Они могут включать другие запакованные объекты, а те в свою очередь могут включать еще запакованные объекты, и т. п. 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 свою очередь могут содержать еще архивы, и т. п. 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 т. п.), в которые

Параметр	Описание
	могут быть вложены объекты, в которые также могут быть вложены объекты, и т. п. 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`
`[Endpoint.<тег>.]ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов, содержащих вложенные объекты (например, HTML-страницы или jar-файлы). Эти объекты могут содержать другие вложенные объекты, которые в свою очередь могут содержать еще вложенные объекты, и т. п. 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}*	Максимальная допустимая степень сжатия запакованных 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`

Особенность настроек компонента

Параметры, отмеченные необязательным префиксом `Endpoint.<имя>`, могут быть сгруппированы. Каждая такая группа определяет *точку подключения* (*endpoint*) с задаваемым уникальным идентификатором *<имя>*, 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.<имя>`, 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.<имя>`).

Параметр `ClamdSocket` должен обязательно задаваться с префиксом `Endpoint.<имя>`, 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, по умолчанию эвристический анализ должен быть выключен, 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 в случае непосредственной правки файла конфигурации необходимо применить измененные настройки, отправив сигнал `SIGHUP` модулю `drweb-configd` (для этого вы можете выполнить команду `drweb-ctl reload`).

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: http://www.proftpd.org/docs/. Описание и исходные коды модуля `mod_clamav`: https://github.com/jbenden/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
```

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 для файловых серверов UNIX 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.

Принципы работы

Компонент используется для доступа к любым объектам файловой системы (файлы, каталоги, загрузочные записи). Запускается с правами суперпользователя *root*.

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 компонентов Dr.Web для файловых серверов UNIX 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, 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 для файловых серверов UNIX (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 данный метод, один раз инициализирует параметры проверки и обезвреживания угроз, и далее эти параметры будут применяться ко всему потоку заявок на проверку файлов, поступающих от 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.

Имеется возможность проверить файлы с использованием метода *«flow»*, используя команду `flowscan` утилиты Dr.Web Ctl (запускается командой `drweb-ctl`), однако для обычной проверки файлов по требованию рекомендуется использовать только команду `scan`.

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.

Аргументы командной строки

Для запуска компонента Dr.Web File Checker из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при поступлении от других компонентов

Dr.Web для файловых серверов UNIX заявок на проверку объектов файловой системы. Для управления параметрами работы компонента, а также для проверки файлов по требованию пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для проверки сканирования произвольного файла или каталога компонентом Dr.Web File Checker вы можете воспользоваться командой `scan` утилиты Dr.Web Ctl:

```
$ drweb-ctl scan <путь к каталогу или файлу>
```

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-filecheck`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[FileCheck]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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: <*opt_dir*>`/bin/drweb-filecheck`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-filecheck`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-filecheck`
`DebugClientIpc` *{логический}*	Сохранять/не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC. Значение по умолчанию: `No`
`DebugScan` *{логический}*	Сохранять/не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения, поступающие в процессе проверки файлов. Значение по умолчанию: `No`

Параметр	Описание
`DebugFlowScan` *{логический}*	Сохранять/не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о проверке файлов методом *«flow»*. (Обычно метод *«flow»* используется монитором SpIDer Guard). Значение по умолчанию: `No`
`DebugProxyScan` *{логический}*	Сохранять/не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о проверке файлов методом *«proxy»*. (Обычно метод *«proxy»* используется монитором SpIDer Guard для SMB и компонентом Dr.Web ClamD). Значение по умолчанию: `No`
`DebugCache` *{логический}*	Сохранять/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`) включительно. Если указан интервал менее `1s`, то задержка отсутствует, файл будет проверяться при любом запросе. Значение по умолчанию: `1s`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`) включительно. Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `30s`

Dr.Web Network Checker

Агент 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 для файловых серверов UNIX с целью приема и передачи данных (например, содержимого файлов) между узлами сети для их проверки. 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.

Обратите внимание, что этот компонент всегда используется для проверки данных, полученных через сетевые соединения. Поэтому, если данный компонент 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 величину лимита на число файловых дескрипторов, доступных Dr.Web для файловых серверов UNIX.

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.

Принципы работы

Компонент позволяет передать на сканирование в сканирующее ядро Dr.Web Scanning Engine (расположенное на локальном или удаленном узле) данные, не представленные в виде файлов в локальной файловой системе. С такими данными работают компоненты, отправляющие данные на проверку через сетевое соединение (SpIDer Gate, Dr.Web ClamD). Следует иметь в виду, что данные компоненты всегда используют Dr.Web Network Checker для передачи файлов на проверку сканирующему ядру Dr.Web Scanning

Engine, даже тому, который расположен на локальном узле. Поэтому, если Dr.Web Network Checker недоступен, *эти компоненты не смогут корректно функционировать*.

Кроме этого, Dr.Web Network Checker позволяет организовать соединение Dr.Web для файловых серверов UNIX с заданным набором узлов в сети с установленным на них Dr.Web для файловых серверов UNIX (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 этом узле). 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 он для включения Dr.Web для файловых серверов UNIX в сканирующий кластер, или только для обеспечения внутренних нужд компонентов, работающих локально в составе Dr.Web для файловых серверов UNIX.

Имеется возможность 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.

Аргументы командной строки

Для запуска компонента Dr.Web Network Checker из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD по мере необходимости (обычно при старте операционной системы). При этом, если в конфигурации компонента задано значение параметра `FixedSocket`, а параметр `InternalOnly` установлен в значение `No`, то агент всегда будет запущен демоном управления конфигурацией и доступен клиентам через этот UNIX-сокет. Для управления параметрами работы компонента, а также для запуска сетевого сканирования (при наличии настроенного соединения с другими узлами сети) пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`). Если соединение с другими узлами сети не настроено, вместо сетевого сканирования будет запущено обычное сканирование силами локального сканирующего ядра.

Для проверки обработки произвольного файла или каталога компонентом Dr.Web Network Checker вы можете воспользоваться командой `netscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl netscan <путь к файлу или каталогу>
```

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-netcheck`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[NetCheck]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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_dir*>`/bin/drweb-netcheck`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-netcheck`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-netcheck`
`FixedSocket` *{путь к файлу | адрес}*	Сокет фиксированной копии агента Dr.Web Network Checker. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелась запущенная копия агента распределенной проверки файлов, доступная клиентам через этот сокет. Возможные значения: • <*путь к файлу*> — путь к файлу локального UNIX-сокета; • <*адрес*> — сетевой сокет в виде пары <*IP-адрес*>:<*порт*>. Значение по умолчанию: *(не задано)*
`InternalOnly`	Управление режимом работы компонента.

Параметр	Описание
{логический}	Если задано значение `Yes`, то компонент используется только для внутренних нужд компонентов Dr.Web для файловых серверов UNIX: он не используется для вхождения в сканирующий кластер и для обслуживания внешних (по отношению к Dr.Web для файловых серверов UNIX) клиентских приложений, вне зависимости от настроек `LoadBalance*` и заданного значения параметра `FixedSocket`. Значение по умолчанию: `No`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Можно указать как числовой UID пользователя, так и 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 не указано, то 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. 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`) включительно. Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `30s`
`LoadBalanceUseSsl` *{логический}*	Использовать/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`

Параметр	Описание
`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. Обратите внимание, что файл сертификата и файл закрытого ключа (определяется следующим параметром) должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`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. Обратите внимание, что файл сертификата и файл закрытого ключа (определяется предыдущим параметром) 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)*
`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)*
`LoadBalanceServerSocket` *{адрес}*	Сетевой сокет (IP-адрес и порт), прослушиваемый Dr.Web Network Checker на данном узле для получения файлов на проверку от удаленных узлов (если она может работать как сервер сетевого сканирования). Значение по умолчанию: *(не задано)*

Параметр	Описание
`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. • 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 через команду `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).

Параметр	Описание
	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"` • Две строки (по одному значению в строке): `[NetCheck]` ` LoadBalanceTo = 192.168.0.1:1234` ` LoadBalanceTo = 10.20.30.45:5678` 2. Добавление значений через команду `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/netcheck`
`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 весов всех доступных узлов-серверов сканирования, то файл будет оставлен агентом для локальной проверки.

Параметр	Описание
	Минимальное значение: `1`. Значение по умолчанию: `1`

Организация сканирующего кластера

В этом разделе

Вводные замечания

Для организации сканирующего кластера, позволяющего выполнять распределенную проверку данных (при сканировании файлов или иных объектов), необходимо иметь набор узлов сети с установленных на каждом из них компонентом Dr.Web Network Checker. Чтобы узел кластера не только мог принимать и передавать данные, подлежащие проверке, необходимо также иметь на узле установленным сканирующее ядро Dr.Web Scanning Engine. Таким образом, для организации узла сканирующего кластера необходимо, чтобы на сервер были установлены (минимально) следующие компоненты (прочие компоненты Dr.Web для файловых серверов UNIX, 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, подлежащие проверке, 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.

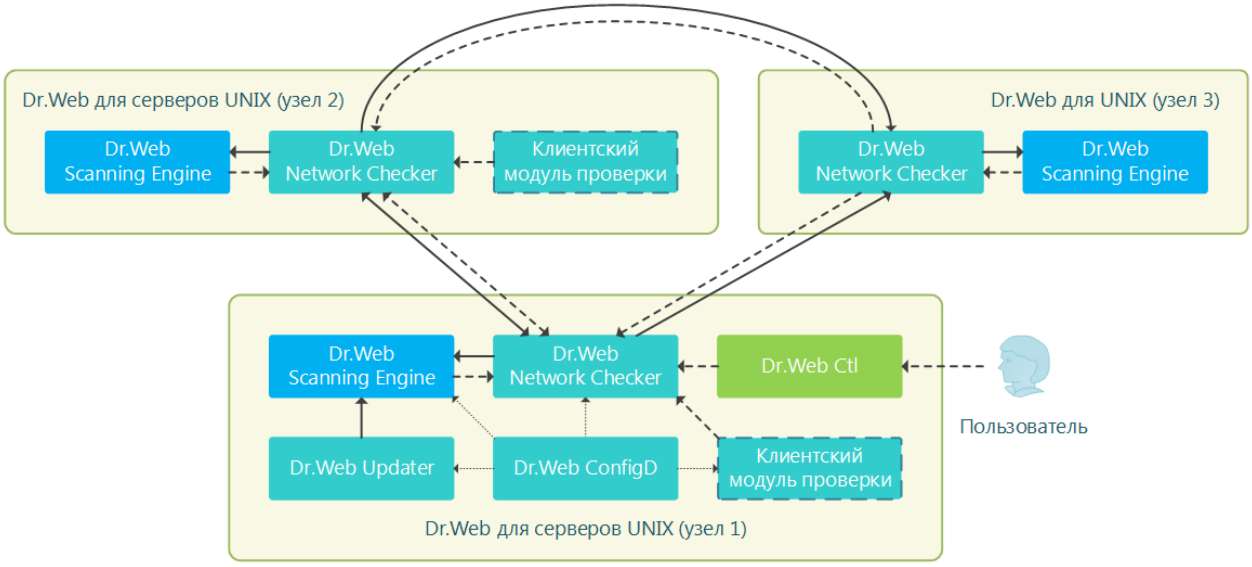

Рисунок 12. Структура сканирующего кластера

В данном случае предполагается, что кластер состоит из трех узлов (обозначенных на рисунке как *узел 1, узел 2* и *узел 3*). При этом узел 1 и узел 2 представляют собой серверы с установленным полноценным продуктом Dr.Web для серверов UNIX (например, Dr.Web для почтовых серверов UNIX или Dr.Web для интернет-шлюзов UNIX, 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 работать как в качестве серверов, так и клиентов 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.

Через «Клиентский модуль проверки» на схеме обозначены компоненты серверов, формирующие компоненту Dr.Web Network Checker на узле задания на проверку, которые будут (в зависимости от соотношения нагрузки) распределены между локально установленным сканирующим ядром Dr.Web Scanning Engine и узлами-партнерами кластера, исполняющими роль серверов сканирования.

Важно отметить, что 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 мониторами 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 будут даны в формате файла `.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. Если необходимо использовать SSL, то необходимо задать значение `Yes` для параметра `LoadBalanceUseSsl`, а также задать актуальные значения параметров `LoadBalanceSslCertificate`, `LoadBalanceSslKey` и `LoadBalanceSslCa`.

Проверка работы кластера

Для проверки работы кластера в режиме разделения данных при сканировании воспользуйтесь на узлах 1 и 2 командой:

```
$ drweb-ctl netscan <путь к файлу или каталогу>
```

При выполнении указанной команды файлы из указанного каталога должны провериться через компонент Dr.Web Network Checker, который должен распределить проверку по настроенным узлам кластера. Для просмотра статистики сетевой проверки на каждом из узлов перед началом проверки запустите вывод статистики Dr.Web Network Checker командой (для прерывания вывода статистики нажмите CTRL+C):

```
$ drweb-ctl stat -n
```

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 для файловых серверов UNIX 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 никакая антивирусная проверка на данном узле не производится (за исключением случаев, когда в составе Dr.Web для файловых серверов UNIX присутствует компонент Dr.Web MeshD, в настройках которого задано соединение с узлами локального облака, предоставляющими услугу сканирующего ядра).

Принципы работы

Компонент работает в качестве сервиса, принимающего от других компонентов Dr.Web для файловых серверов UNIX запросы на проверку объектов файловой системы (файлов, загрузочных записей на дисках) на наличие внедренных угроз. Формирует очереди задач на проверку объектов, 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 для файловых серверов UNIX, 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 для файловых серверов UNIX функционирует в режиме централизованной защиты, то функции обновления вирусных баз и антивирусного ядра берет на себя агент централизованной защиты Dr.Web ES Agent. Этот компонент 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 для файловых серверов UNIX, выполняющие запросы к сканирующему ядру на предмет проверки файлов, используют тот же программный интерфейс, что и внешние приложения.

Имеется возможность 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» (https://partners.drweb.com/).

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 сканирующим ядром 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.

Следует помнить, что эвристический анализ не гарантирует достоверного распознавания угроз и может допускать ошибки первого и второго рода.

- *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 анализом, 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 и лечение как простых файлов, так и запакованных объектов и объектов, содержащихся в различных контейнерах (таких, как архивы, сообщения электронной почты и т. п.).

Аргументы командной строки

Для запуска сканирующего ядра Dr.Web Scanning Engine из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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: Указать 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: Указать путь к каталогу, содержащему файлы вирусных баз. Краткий вариант: Нет. Аргументы: *<путь к каталогу>* — полный путь к каталогу вирусных баз.
`--TempDir`	Назначение: Указать путь к каталогу временных файлов. Краткий вариант: Нет.

	Аргументы: <*путь к каталогу*> — полный путь к каталогу временных файлов.
`--Key`	Назначение: Указать путь к используемому ключевому файлу. Краткий вариант: Нет. Аргументы: <*путь к файлу*> — полный путь к ключевому файлу.
`--MaxForks`	Назначение: Определить 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: Установить 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.
`--Shelltrace`	Назначение: Включить отслеживание оболочки (вывод в журнал расширенной информации о проверке файлов ядром Dr.Web Virus-Finding Engine). Краткий вариант: Нет. Аргументы: Нет.
`--LogLevel`	Назначение: Задать 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: Задать способ ведения журнала сообщений компонента. Краткий вариант: Нет. Аргументы: <*тип журнала*>. Возможные значения: • `Stderr[:ShowTimestamp]` — сообщения будут выводиться в стандартный поток ошибок *stderr*. Дополнительная 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`

Пример:

```
$ /opt/drweb.com/bin/drweb-se /tmp/drweb.ipc/.se --MaxForks=5
```

Данная команда запустит копию сканирующего ядра Dr.Web Scanning Engine, заставив его создать для взаимодействия с клиентскими компонентами UNIX-сокет `/tmp/drweb.ipc/.se` и порождать не более 5 сканирующих дочерних процессов при проверке файлов.

Замечания о запуске

При необходимости может быть запущено произвольное количество копий сканирующего ядра Dr.Web Scanning Engine, предоставляющих клиентским приложениям (не обязательно только компонентам Dr.Web для файловых серверов UNIX) сервис по проверке файлов на наличие угроз. При этом, если в конфигурации компонента задано значение параметра `FixedSocketPath`, то одна копия сканирующего ядра всегда будет автоматически запущена демоном управления конфигурацией Dr.Web ConfigD и доступна клиентам через этот 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 пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для проверки сканирования произвольного файла или каталога компонентом Dr.Web Scanning Engine вы можете воспользоваться командой `rawscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl rawscan <путь к каталогу или файлу>
```

Для получения справки о компоненте из командной строки используйте. команду `man 1 drweb-se`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ScanEngine]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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: <*opt_dir*>`/bin/drweb-se`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-se`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-se`
`FixedSocketPath` *{путь к файлу}*	Путь к файлу UNIX-сокета фиксированной копии сканирующего ядра Dr.Web Scanning Engine. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелась запущенная копия сканирующего ядра, доступная клиентам через этот сокет. Значение по умолчанию: *(не задано)*
`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).

Параметр	Описание
	Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`) включительно. Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `1h`
`MaxForks` *{целое число}*	Определяет максимальное разрешенное количество копий дочерних сканирующих процессов, порождаемых сканирующим ядром Dr.Web Scanning Engine, которые одновременно могут быть запущены. Значение по умолчанию: *Автоматически определяется при старте*, как удвоенное число доступных процессорных ядер, или `4`, если полученное число меньше 4.
`BufferedIo` *{On | Off}*	Использовать буферизованный ввод-вывод при проверке файлов. Использование буферизованного ввода-вывода в ОС FreeBSD и GNU/Linux может увеличить скорость проверки файлов, расположенных на медленных дисковых устройствах. Значение по умолчанию: `Off`
`WatchdogInterval` *{интервал времени}*	Определяет периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность порожденных им дочерних сканирующих процессов для обнаружения зависаний при проверке («сторожевой таймер»). Значение по умолчанию: `1.5s`

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» а также синхронизировать обновления с локальным облаком продуктов Dr.Web для UNIX (через компонент Dr.Web MeshD, если он присутствует в составе продукта).

Если Dr.Web для файловых серверов UNIX работает в режиме централизованной защиты, то в качестве источника обновлений используется сервер централизованной защиты (например, Dr.Web Enterprise Server), причем все обновления получаются с сервера через Dr.Web ES Agent, а Dr.Web Updater для загрузки обновлений не используется (синхронизация обновлений с локальным облаком продуктов Dr.Web для UNIX также не производится).

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 (этот файл подписан с целью невозможности его модификации). При подключении к серверам обновлений через прокси-сервер поддерживается только базовая и дайджест-аутентификация.

Если Dr.Web для файловых серверов UNIX 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. Запуск производится с периодичностью, указанной в настройках. Также компонент может быть запущен демоном управления конфигурацией в ответ на поступившую команду пользователя (внеочередное обновление).

При наличии на серверах обновлений доступных обновлений, они загружаются в каталог <*var_dir*>`/cache` (для GNU/Linux — `/var/opt/drweb.com/cache/`), после чего размещаются в рабочих каталогах Dr.Web для файловых серверов UNIX.

По умолчанию все обновления производятся 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 который указывается в отдельном файле (по умолчанию, с именем `custom.drl`), располагающемся в каталоге, указанном в соответствующем параметре `*CustomDrlDir`. В этом случае компонент обновлений будет получать 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 для файловых серверов UNIX из командной строки Dr.Web Ctl (запускается командой `drweb-ctl`).

Если Dr.Web для файловых серверов UNIX подключен к локальному облаку продуктов Dr.Web для UNIX, и не работает под управлением сервера централизованной защиты, компонент Dr.Web Updater используется также для синхронизации обновлений, получаемых узлами облака, т. е. передает свежие обновления, полученные с серверов обновления, в облако, и получает свежие обновления из облака, что позволяет уменьшить суммарную нагрузку на сервера обновлений Dr.Web. Данная возможность включается и отключается в настройках компонента.

Аргументы командной строки

Для запуска компонента Dr.Web Updater из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. 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 для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте. команду `man 1 drweb-update`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[Update]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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: <*opt_dir*>`/bin/drweb-update`. • 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. Можно указать как числовой UID пользователя, так и 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 не указано, то работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`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`
`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`) включительно. 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 выполнить обновление с серверов обновления окончилась 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`

Параметр	Описание
`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; • <*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`». 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 использованием 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`

Параметр	Описание
	Значение по умолчанию: *(не задано)*
`ExcludedFiles` *{имя файла}*	Определяет 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`. 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 через команду `drweb-ctl cfset`: `# drweb-ctl cfset Update.ExcludedFiles -a 123.vdb` `# drweb-ctl cfset Update.ExcludedFiles -a 456.dws` Значение по умолчанию: `drweb32.lst`
`NetworkTimeout` *{интервал времени}*	Тайм-аут на сетевые операции компонента обновления при выполнении обновлений с серверов обновления 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. Минимально значение: `5s`. Значение по умолчанию: `60s`
`BaseDrlDir` *{путь к каталогу}*	Определяет путь к каталогу, хранящему файлы для подключения к серверам из стандартной зоны обновления, используемым для обновления вирусных баз и антивирусного ядра. Значение по умолчанию: <*var_dir*>`/drl/bases`. • Для GNU/Linux: `/var/opt/drweb.com/drl/bases`. • Для FreeBSD: `/var/drweb.com/drl/bases`

Параметр	Описание
`BaseCustomDrlDir` *{путь к каталогу}*	Определяет 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 не пустой подписанный файл списка серверов (файл `.drl`), то обновление ведется только с этих серверов, а сервера основной зоны (см. выше) не используются для обновления вирусных баз и антивирусного ядра. Значение по умолчанию: <*var_dir*>`/custom-drl/bases`. • Для GNU/Linux: `/var/opt/drweb.com/custom-drl/bases`. • Для FreeBSD: `/var/drweb.com/custom-drl/bases`
`BaseUpdateEnabled` *{логический}*	Флаг, указывающий, разрешено или запрещено 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`
`VersionDrlDir` *{путь к каталогу}*	Определяет путь к каталогу, хранящему файлы для подключения к серверам, используемым для обновления версий компонентов Dr.Web для файловых серверов UNIX. Значение по умолчанию: <*var_dir*>`/drl/version`. • Для GNU/Linux: `/var/opt/drweb.com/drl/version`. • Для FreeBSD: `/var/drweb.com/drl/version`
`VersionUpdateEnabled` *{логический}*	Флаг, указывающий, разрешено или запрещено обновление версий компонентов Dr.Web для файловых серверов UNIX. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`
`DwsCustomDrlPath` *{путь к файлу}*	Параметр не используется. Значение по умолчанию: <*var_dir*>`/drl/dws/custom.drl`. • Для GNU/Linux: `/var/opt/drweb.com/drl/dws/custom.drl`. • Для FreeBSD: `/var/drweb.com/drl/dws/custom.drl`
`DwsDrlDir` *{путь к каталогу}*	Параметр не используется. Значение по умолчанию: <*var_dir*>`/drl/dws`. • Для GNU/Linux: `/var/opt/drweb.com/drl/dws`. • Для FreeBSD: `/var/drweb.com/drl/dws`

Параметр	Описание
`DwsCustomDrlDir` *{путь к каталогу}*	Параметр не используется. Значение по умолчанию: <*var_dir*>`/custom-drl/dws`. • Для GNU/Linux: `/var/opt/drweb.com/custom-drl/dws`. • Для FreeBSD: `/var/drweb.com/custom-drl/dws`
`DwsUpdateEnabled` *{логический}*	Параметр не используется. Значение по умолчанию: `Yes`
`AntispamDrlDir` *{путь к каталогу}*	Параметр не используется. Значение по умолчанию: <*var_dir*>`/drl/antispam`. • Для GNU/Linux: `/var/opt/drweb.com/drl/antispam`. • Для FreeBSD: `/var/drweb.com/drl/antispam`
`AntispamCustomDrlDir` *{путь к каталогу}*	Параметр не используется. Значение по умолчанию: <*var_dir*>`/custom-drl/antispam`. • Для GNU/Linux: `/var/opt/drweb.com/custom-drl/antispam`. • Для FreeBSD: `/var/drweb.com/custom-drl/antispam`
`AntispamUpdateEnabled` *{логический}*	Параметр не используется. Значение по умолчанию: `No`
`BackupDir` *{путь к каталогу}*	Определяет 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: `/tmp/update-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`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Компонент запускается при очередном обновлении по расписанию или по явной команде `drweb-ctl update [--local-cloud]`. По окончанию обновления ждет указанный интервал времени, и, если новых запросов не поступает (в том числе по взаимодействию с облаком, если `UseLocalCloud = Yes`), то завершает свою работу до следующей попытки обновления.

Параметр	Описание
	Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`) включительно. Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `30s`
`UseLocalCloud` *{логический}*	Взаимодействовать с локальным облаком продуктов Dr.Web для UNIX через компонент Dr.Web MeshD для синхронизации обновлений (передавать свежие обновления в облако, получать свежие обновления из облака) в дополнении к серверам обновлений Dr.Web. Допустимые значения: • `No` — обновление только с серверов обновлений Dr.Web. Синхронизация обновлений с облаком не производится, но может быть выполнено явно, командой `drweb-ctl update --local-cloud`; • `Yes` — синхронизация обновлений на узле с локальным облаком (получение обновлений из облака, если в облаке есть более свежие обновления, передача обновлений в облако, если обновления на узле свежее тех, что имеются на узлах в облаке). Значение по умолчанию: `Yes`

Dr.Web ES Agent

Агент централизованной защиты Dr.Web ES Agent предназначен для подключения Dr.Web для файловых серверов UNIX к серверу централизованной защиты (например, к Dr.Web Enterprise Server).

Когда Dr.Web для файловых серверов UNIX подключен к серверу централизованной защиты, Dr.Web ES Agent синхронизирует лицензионный ключевой файл в соответствии с ключами, хранящимися на сервере централизованной защиты. Кроме того, Dr.Web ES Agent передает на сервер централизованной защиты, к которому он подключен, статистику вирусных инцидентов, перечень запущенных компонентов и их состояние.

Также Dr.Web ES Agent выполняет обновление вирусных баз Dr.Web для файловых серверов UNIX непосредственно с подключенного сервера централизованной защиты, минуя компонент обновления Dr.Web Updater.

Принципы работы

Компонент Dr.Web ES Agent осуществляет подключение к серверу централизованной защиты (например, к Dr.Web Enterprise Server), 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, обеспечивающего управление антивирусной защитой сети через сервер централизованной защиты.

Кроме того, если данная возможность разрешена на сервере централизованной защиты, имеется возможность подключить к нему узел с защищаемым сервером («рабочую станцию») в режиме «новичок». В этом случае, после подтверждения заявки на подключение станции администратором, сервер централизованной защиты автоматически сгенерирует для узла новые идентификатор и пароль, которые отправит агенту для использования при последующих подключениях.

Аргументы командной строки

Для запуска компонента Dr.Web ES Agent из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически, при старте операционной системы, демоном управления конфигурацией Dr.Web ConfigD. Для управления параметрами работы компонента, а также для подключения Dr.Web для файловых серверов UNIX к серверу централизованной защиты пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-esagent`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ESAgent]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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_dir*>`/bin/drweb-esagent`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-esagent`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-esagent`
`DebugIpc` *{логический}*	Включать или нет 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`
`MobileMode` *{On | Off | Auto}*	Dr.Web для файловых серверов UNIX возможность работать в мобильном режиме при подключении к серверу централизованной защиты. Допустимые значения: • `On` — использовать мобильный режим, если он разрешен сервером централизованной защиты (выполнять обновления с серверов обновлений компании «Доктор Веб» через Dr.Web Updater); • `Off` — не использовать мобильный режим, оставаться в режиме централизованной защиты (обновления всегда получаются только с сервера централизованной защиты); • `Auto` — использовать мобильный режим, если он разрешен сервером централизованной защиты, а обновления выполнять как с серверов обновлений компании «Доктор Веб» через Dr.Web Updater, так и с

Параметр	Описание
	сервера централизованной защиты, в зависимости от того, какое соединение доступно и качество какого соединения лучше. Обратите внимание, что поведение данного параметра зависит от разрешений на сервере: если мобильный режим на используемом сервере не разрешен, то этот 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` — не разрешать агенту принимать и обрабатывать *discovery*-запросы. Обратите внимание, что параметр имеет приоритет выше, чем настройки 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}*	Указывает агенту получать с сервера централизованной защиты обновления для антивирусного ядра, разработанного для указанной платформы, где *название платформы* — строка, содержащая название платформы. Допустимые значения: • для GNU/Linux: `unix-linux-32`, `unix-linux-64`, `unix-linux-mips`; • для FreeBSD: `unix-freebsd-32`, `unix-freebsd-64`; • для Darwin: `unix-darwin-32`, `unix-darwin-64`. ⚠ Настоятельно не рекомендуется изменять значение параметра, если вы не уверены, что это действительно необходимо. Значение по умолчанию: *Зависит от используемой платформы*
`SrvMsgAutoremove` *{целое число}*	Указывает 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`.

Параметр	Описание
	Значение по умолчанию: `1w`

Dr.Web HTTPD

Компонент Dr.Web HTTPD обеспечивает инфраструктуру для локального или удаленного взаимодействия с Dr.Web для файловых серверов UNIX посредством протокола HTTP (например — через веб-браузер). Компонент интерфейс для управления Dr.Web для файловых серверов UNIX.

Помимо управления Dr.Web для файловых серверов UNIX через веб-интерфейс от Dr.Web, имеется возможность использовать непосредственно командный интерфейс (HTTP API) Dr.Web HTTPD для взаимодействия с компонентами Dr.Web для файловых серверов UNIX по протоколу HTTPS. Данная возможность позволяет разработать для Dr.Web для файловых серверов UNIX 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`. Пример использования утилиты `openssl` для генерации сертификатов и закрытых ключей приведен в разделе Приложение Д. Генерация сертификатов SSL.

Принципы работы

Dr.Web HTTPD представляет собой веб-сервер, специально разработанный для управления работой Dr.Web для файловых серверов UNIX, позволяя тем самым не использовать для этих целей как сторонние веб-серверы (такие как Apache HTTP Server или 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. Безопасный протокол HTTPS используется для управления Dr.Web для файловых серверов UNIX.

Веб-интерфейс управления Dr.Web не является обязательным для функционирования Dr.Web для файловых серверов UNIX, и может отсутствовать, поэтому соответствующий блок на схеме обведены пунктирной границей.

Компонент Dr.Web HTTPD формирует управляющие команды к демону управления конфигурацией Dr.Web ConfigD Dr.Web для файловых серверов UNIX, компоненту проверки файлов Dr.Web File Checker и другим компонентам, на основании команд, полученных через HTTP API.

Если веб-интерфейс управления Dr.Web для файловых серверов UNIX, использующий Dr.Web HTTPD, входит в состав Dr.Web для файловых серверов UNIX, то его описание приведено в соответствующем разделе.

Если в состав Dr.Web для файловых серверов UNIX не включен веб-интерфейс управления Dr.Web, имеется возможность подключить к нему любой внешний интерфейс управления, использующий для взаимодействия HTTP API Dr.Web HTTPD (описан в разделе Описание HTTP API).

Аргументы командной строки

Для запуска компонента Dr.Web HTTPD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD по мере необходимости (обычно при старте

операционной системы). Если компонент запущен, а также если установлен веб-интерфейс управления, то для управления работой компонентов Dr.Web для файловых серверов UNIX достаточно выполнить HTTPS-подключение к одному из адресов, обслуживающих функционирование веб-интерфейса, при помощи любого стандартного браузера. Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-httpd`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[HTTPD]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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_dir*>`/bin/drweb-httpd`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-httpd`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-httpd`
`Start` *{логический}*	Запустить/остановить компонент с помощью демона конфигурации Dr.Web ConfigD (`Yes` — запустить, `No` — остановить). Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно попытаться 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
`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, если он установлен, 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 через команду `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 (если он установлен) невозможно. Значение по умолчанию: `127.0.0.1:4443`
`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 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 через команду `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 (если он установлен), используя данные адреса, невозможно. Значение по умолчанию: *(не задано)*
`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. Обратите внимание, что файл сертификата и файл закрытого ключа (определяется следующим параметром) должны соответствовать друг другу. Значение по умолчанию: <*etc_dir*>`/certs/serv.crt`. • 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. Обратите внимание, что файл сертификата (определяется предыдущим параметром) и файл закрытого ключа должны соответствовать друг другу. Значение по умолчанию: <*etc_dir*>`/certs/serv.key`. • Для GNU/Linux: `/etc/opt/drweb.com/certs/serv.key`.

Параметр	Описание
	• Для FreeBSD: `/usr/local/etc/drweb.com/certs/serv.key`
`AdminSslCA` *{путь к файлу}*	Путь к файлу сертификата доверенного ЦС (центра сертификации) для сертификатов, используемых клиентами, при подключении к административному сокету по протоколу HTTPS. Если сертификат клиента подписан указанным здесь сертификатом, то для клиента не производится аутентификация через указание 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)*
`WebconsoleRoot` *{путь к каталогу}*	Путь к каталогу с файлами веб-интерфейса управления, если он установлен (аналог каталога `htdocs` для Apache HTTP Server). Значение по умолчанию: <*opt_dir*>`/share/drweb-httpd/webconsole`. • Для GNU/Linux: `/opt/drweb.com/share/drweb-httpd/webconsole`. • Для FreeBSD: `/usr/local/libexec/drweb.com/share/drweb-httpd/webconsole`
`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)*

Описание HTTP API

В этом разделе

1. Общие положения

HTTP API представляет собой инструмент для интеграции Dr.Web для файловых серверов UNIX 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`.

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.

2. 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.

2.1. 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 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

Команда API	Описание
	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": string, //Имя пользователя
 "password": string //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": string //Имя пользователя
 }
}
```

3) `Error` — объект, содержащий информацию о произошедшей ошибке:

```
{
 "error" :
```

```
 {
 "code" : string, //Строковый код ошибки вида EC_XXX
 *"what": string  //Описание ошибки
 }
}
```

Символом «*» помечен факультативный 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 для файловых серверов UNIX. Этот код представляет собой строку вида `EC_XXX`. Для уточнения числового кода и получения описания ошибки обратитесь к разделу «Описание известных ошибок» (Приложение Е Руководства администратора).

2.2. 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 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 используйте при установлении соединения подписанный сертификат.

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

3. Управление Dr.Web для файловых серверов UNIX

Команды API для просмотра и изменения текущих 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`

Команда API	Описание
	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 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)
`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)

Команда API	Описание
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: Отключить режима 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 для файловых серверов UNIX, 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": string, //Имя опции (параметра конфигурации или секции)
 *"value": LexValue, //Если данная опция является параметром
 *"map": LexMap //Если данная опция является секцией
}
```

Символом «*» помечены факультативные параметры.

Объект LexOption представляет собой секцию или параметр конфигурации Dr.Web для файловых серверов UNIX. 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": string[] //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 результаты изменения значения каждого из параметров, указанных в команде.

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 для каждого из указанных в команде параметров.

6) `SetOptionResultItem` — объект, содержащий информацию об изменении значения параметра:

```
{
 "option": string, //Имя параметра
 "result": string, //Результат изменения значения (код ошибки)
 *"lower_limit": string, //Нижняя допустимая граница значений
 *"upper_limit": string //Верхняя допустимая граница значений
}
```

Символом «*» помечены факультативные 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" : number //Идентификатор запущенного процесса обновления
  }
}
```

8) `ESConnection` — объект, содержащий информацию о подключении к серверу централизованной защиты:

```
{
 *"server": string,    //<Адрес узла>:<порт> (без префикса http/https)
 "certificate": string, //Ключ сервера в base64
 *"newbie": boolean,   //По умолчанию false
 *"login": string,     //Имя пользователя
 *"password": string   //Пароль
}
```

Символом «*» помечены факультативные 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" : number //Временная метка базы
 "vdb_bases" : VirusBaseInfo[] //Детальная информация о базе
}
```

10) `VirusBaseInfo` — объект, содержащий подробную информацию о вирусной базе:

```
{
  "path" : string //Путь до файла базы
  "virus_records" : number //Количество записей в базе
  "version" : number //Версия базы
  "timestamp" : number //Временная метка базы
  "md5" : string //MD5-хеш базы
  "load_result" : string //Результат загрузки базы (в случае успешной
загрузки - EC_OK)
  *"sha1" : string - SHA1-хеш базы
}
```

Символом «*» помечен факультативный параметр.

4. 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, колонки которой соответствуют полям объекта ScanStat.

Описание используемых объектов JSON

1) `ScanOptions` — объект, содержащий параметры, используемые при создании *endpoint* для проверки файлов:

```
{
 "scan_timeout_ms": number, //Тайм-аут на проверку файла в мс
 "cure": boolean, //Применять лечение к инфицированному файлу
 "heuristic_analysis": boolean, //Использовать эвристический анализ
 "packer_max_level": number, //Максимальный уровень вложенности для
запакованных объектов
 "archive_max_level": number, //Максимальный уровень вложенности для
архивов
 "mail_max_level": number, //Максимальный уровень вложенности для почтовых
```

```
объектов
 "container_max_level": number, //Максимальный уровень вложенности для
прочих сложных объектов (контейнеров)
 "max_compression_ratio": number //Максимальная величина коэффициента
сжатия архивов
 "min_size_to_scan" : number, //Минимальный размер объекта для
сканирования
 "max_size_to_scan" : number,  //Максимальный размер объекта для
сканирования
 "threat_hash" : boolean   //Получать хеши обнаруженных угроз
}
```

2) `ScanPathOptions` — объект, содержащий параметры сканирования файла или каталога по указанному пути:

```
{
 "path" : string //Абсолютный путь до файла или каталога, который надо
сканировать
    *"exclude_path" : string[] //Список путей, исключенных из сканирования
(можно использовать маски)
    *"scan_timeout_ms" : number //Тайм-аут сканирования одного объекта
    *"archive_max_level" : number//Максимальный уровень вложенности для
архивных объектов
    *"packer_max_level" : number//Максимальный уровень вложенности для
запакованных объектов
    *"mail_max_level" : number//Максимальный уровень вложенности для
почтовых сообщений
    *"container_max_level" : number//Максимальный уровень вложенности для
прочих сложных объектов (контейнеров)
    *"max_compression_ratio" : number //Максимальная величина коэффициента
сжатия архивов
    *"heuristic_analysis" : boolean //Использовать эвристический анализ
(по умолчанию true)
    *"follow_symlinks" : boolean - //Переходить по символическим ссылкам
    *"min_size_to_scan" : number //Минимальный размер объекта для
сканирования
    *"max_size_to_scan" : number //Максимальный размер объекта для
сканирования
    *"timeout_ms" : number //Тайм-аут на сканирование всех объектов
    *"threat_hash" : boolean //Возвращать SHA1- и SHA256-хеши угроз
}
```

Символом «*» помечены факультативные параметры.

3) `ScanPathResult` — объект, содержащий результаты сканирования файла или каталога по указанному пути:

```
{
 ScanPathResult:
    "results": ScanResult[]  //Результаты сканирования
    *"error": string  //Ошибка, если весь процесс завершился (например, по
тайм-ауту)
}
```

Символом «*» помечен факультативный 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" : string   //Хеш SHA1 угрозы
    *"sha256" : string  //Хеш SHA256 угрозы
}
```

Символом «*» помечены факультативные параметры.

5) `ScanReport` — объект, содержащий информацию о файле с обнаруженной угрозой:

```
{
 ScanReport:
"object" : string  //Строка, имя отсканированного объекта.
    Для файла  //Абсолютный путь, для вложенного объекта - имя файла.
    Для вызова scan_endpoint будет всегда указывать на временный файл.
*"size" : number //Размер объекта
*"compressed_size" : number //Размер объекта в сжатом состоянии.
*"core_fingerprint" : string //Отпечаток движка
*"packer" : string[]  //Список упаковщиков, которыми был запакован объект
*"compression_ratio" : number //Коэффициент сжатия архива
*"archive" : Archive //Сведения о типе архива(контейнера), если объект
распознан как таковой
*"virus" : Virus[] //Вирусы, обнаруженные в объекте (если были найдены)
*"item" : ScanReport[] //Отчеты о сканировании вложенных объектов (если
они были)
*"error" : string  //Ошибка сканирования, если возникла в процессе
*"heuristic_analysis" : boolean //Флаг использования эвристического
анализа
*"cured" : boolean //Указывает, был ли объект вылечен (true - вылечен,
false - нет).
*"cured_by_deletion" : boolean //Указывает, был ли объект удален в ходе
лечения (true - удален, false - нет).
*"new_path" : string //Новый путь к объекту, переименованному в ходе
лечения
*"user_time" : number //Время, проведенное в системных вызовах во время
сканирования
*"system_time" : number //Время, проведенное в пространстве пользователя
}
```

Символом «*» помечены факультативные 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": string //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": string, //Тип выявленной угрозы
 "name": string  //Название угрозы
}
```

Поле `type` (тип угрозы) — строка вида `SE_XXX`:

- `SE_KNOWN_VIRUS` — известный вирус;
- `SE_VIRUS_MODIFICATION` — модификация известного вируса;
- `SE_UNKNOWN_VIRUS` — неизвестный вирус (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" : string //Тип архива, может принимать одно из значений:
        "SE_ARCHIVE" //Архив
        "SE_MAIL" //Письмо
        "SE_CONTAINER" //Другой тип контейнера
 "name" : string  //Формат архива
}
```

9) `ScanStat` — объект, содержащий статистику проверок:

```
{
 "origin": string //Приложение, по запросу которого было выполнено
сканирование
    #Счетчики зараженных объектов:
    "known_virus": number //Количество зараженных известными вирусами
объектов
    "virus_modification": number //Количество объектов, зараженных
модификацией известного вируса
    "unknown_virus": number //Количество зараженных неизвестными вирусами
объектов
    "adware": number //Количество объектов с SE_ADWARE
```

```
    "dialer": number //Количество объектов с SE_DIALER
    "joke": number  //Количество объектов с SE_JOKE
    "riskware": number //Количество объектов с SE_RISKWARE
    "hacktool" : number //Количество объектов с SE_HACKTOOL
    "cured": number  //Количество вылеченных угроз
    "quarantined": number //Количество угроз, помещенных в карантин
    "deleted": number //Количество удаленных угроз
}
```

5. Управление списком угроз

Для управления списком угроз, обнаруженных при сканировании или монитором файловой системы SpIDer Guard, 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 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*>

Команда API	Описание
	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 возвращает команда `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": number, //Идентификатор угрозы
 "detection_time": UNIXTime, //Время обнаружения угрозы
 "report": ScanReport, //Отчет о проверке файла
 "stat": FileStat, //Информация о файле
 "origin": string, //Имя компонента, обнаружившего угрозу
 "origin_pid": number, //PID компонента, обнаружившего угрозу
 "task_id": number, //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": string, //Объект файловой системы с угрозой
 "size": number, //Размер файла с угрозой в байтах
 "virus": VirusInfo[], //Перечень сведений об обнаруженных
 //угрозах
 *"error": string, //Сообщение об ошибке
 "heuristic_analysis": boolean //Флаг использования эвристического
 //анализа
}
```

Символом «*» помечен факультативный 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": number, //Устройство
 "ino": number, //Индексный дескриптор (inode)
 *"size": number, //Размер файла
 *"uid": User, //Идентификатор пользователя-владельца
 *"gid": Group, //Идентификатор группы владельцев
 *"mode": number, //Режим доступа к файлу
 *"mtime": UNIXTime, //Время модификации файла
 *"ctime": UNIXTime //Время создания файла
 *"rsrc_size": number, //
 *"finder_info": string, //
 *"ext_finder_info": string, //
 *"uchg": string, //
 *"volume_name": string, //Имя тома
 *"volume_root": string, //Корень (точка монтирования) тома
 *"xattr": Xattr[] //Расширенная информация о файле
}
```

Символом «*» помечены факультативные параметры.

Поле `xattr` представляет собой массив объектов `Xattr`. Этот объект содержит два строковых (*string*) 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": string, //Применяемое действие
 "action_time": UNIXTime, //Время применения
 "result": string, //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.

6. 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
`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

Команда API	Описание
	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": string,
 "entry_id": string
}
```

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": string, //Части идентификатора
 *"chunk_id": string, //изолированного объекта
 *"quarantine_dir": string, //Каталог карантина
 "restore_path": string, //Путь, куда будет восстановлен
 //объект
 "creation_time": number, //Момент помещения в карантин
 //(UNIX time)
 "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": number, //Момент обнаружения угрозы
 *"origin": string //Компонент, обнаруживший угрозу
}
```

Символом «*» помечены факультативные 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": string, //Действие, применявшееся к объекту
 //(см. обозначения ниже)
 "action_time": number, //Время применения действия (UNIX Time)
 "result": string, //Ошибка применения действия (код вида
 //EC_XXX)
 *"restore_path": string, //Путь восстановления объекта из карантина
 //(если action = "QENTRY_ACTION_RESTORE")
 *"rescan_report": ScanReport //Отчет о повторной проверке (если
 //action = "QENTRY_ACTION_RESCAN")
}
```

Символом «*» помечены факультативные 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": string, //IP-адрес пользователя
 *"user": string, //Имя пользователя
 *"domain": string //Домен пользователя
}
```

Символом «*» помечены факультативные 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.

7. 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":"0D2DD5A869DAB7AE354153A4D5F7
0F45",
"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":"2F686F6D652F757365722F2E636F6D2E64727765622E71756172616E
74696E65",
"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":"467CD4C6D423C55448B71CD5B815
2776",
"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"}]}
   ```

Dr.Web SNMPD

Dr.Web SNMPD — это SNMP-агент, предназначенный для интеграции Dr.Web для файловых серверов UNIX с системами мониторинга, использующими протокол SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов Dr.Web для файловых серверов UNIX, а также собирать статистику обнаружения и нейтрализации угроз. Агент поддерживает предоставление системам мониторинга или любым SNMP-менеджерам следующей информации:

- Состояние любого компонента Dr.Web для файловых серверов UNIX.
- 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 для файловых серверов UNIX.
2. Статистика работы Dr.Web для файловых серверов UNIX.
3. Состояние компонентов Dr.Web для файловых серверов UNIX.

Подробнее о данных, которые можно получить, используя протокол SNMP, см. в соответствующем разделе.

Принципы работы

В этом разделе

Общие сведения

По умолчанию компонент запускается автоматически при старте Dr.Web для файловых серверов UNIX. После запуска компонент формирует структуры данных в соответствии со структурой, описанной в MIB Dr.Web, и начинает ожидать поступление запросов на получение информации от внешних менеджеров SNMP. Компонент получает информацию о статусе компонентов Dr.Web для файловых серверов UNIX, 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 для файловых серверов UNIX. 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 для файловых серверов UNIX) 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 для GNU/Linux — `/etc/snmp/snmpd.conf`), 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
```

Обратите внимание, что, 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).

Аргументы командной строки

Для запуска компонента Dr.Web SNMPD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD по мере необходимости (обычно при старте операционной системы). Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-snmpd`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[SNMPD]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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: <*opt_dir*>`/bin/drweb-snmpd`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-snmpd`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-snmpd`
`Start` *{логический}*	Запускать/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. Можно указать как числовой UID пользователя, так и 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 не указано, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`ListenAddress` *{адрес}*	Адрес (IP-адрес и порт), прослушиваемый агентом Dr.Web SNMPD в ожидании подключений от клиентов (менеджеров SNMP). Обратите внимание, что для совместной работы с snmpd необходимо указать порт, отличный от стандартного (`161`), а кроме того, у snmpd необходимо настроить проксирование.

Параметр	Описание
	Значение по умолчанию: `127.0.0.1:161`
`SnmpVersion` *{V2c | V3}*	Используемая версия протокола SNMP (*SNMPv2c* или *SNMPv3*). Значение по умолчанию: `V2c`
`V3EngineId` *{строка}*	Строка-идентификатор *Engine ID* для *SNMPv3* (согласно RFC 3411). Значение по умолчанию: `800073FA044452574542`
`TrapReceiver` *{список адресов}*	Список адресов (IP-адрес и порт), на которые Dr.Web SNMPD отправляет уведомления *SNMP trap* при обнаружении угроз компонентами Dr.Web для файловых серверов UNIX. 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 через команду `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 задан)*
`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`
`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 использованием 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*). Возможные значения: • `DES(<secret>)` — используется алгоритм шифрования DES;

Параметр	Описание
	• `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 использованием команды `drweb-ctl cfset`: `drweb-ctl cfset SNMPD.V3Privacy AES128\(supersecret\)` Параметр используется, если задано `SnmpVersion = V3`. Значение по умолчанию: `None`

Интеграция с системами мониторинга

SNMP-агент Dr.Web может выступать поставщиком данных для любой системы мониторинга, использующей протокол SNMP версии *2c* или *3*. Перечень данных, доступных для контроля и их структура описаны в файле описания MIB Dr.Web `DRWEB-SNMPD-MIB.txt`, поставляемом совместно с Dr.Web для файловых серверов UNIX. Этот файл находится в каталоге *<opt_dir>*`/share/drweb-snmpd/mibs`.

Для удобства настройки, совместно с компонентом поставляются необходимые шаблоны настроек для популярных систем мониторинга:

- Munin
- Nagios
- Zabbix

Шаблоны настроек для систем мониторинга находятся в каталоге *<opt_dir>*`/share/drweb-snmpd/connectors`.

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_dir*>`/share/drweb-snmpd/connectors/munin/plugins` 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.
- Статистика проверки почтовых сообщений (получить статистику проверки почтовых сообщений можно только с помощью компонента Dr.Web MailD. Этот компонент не входит в состав Dr.Web для файловых серверов UNIX).

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 для файловых серверов UNIX через Dr.Web SNMPD.

В каталоге <*opt_dir*>`/share/drweb-snmpd/connectors/munin` 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 для файловых серверов UNIX на узле.
`plugins/snmp__drweb_filecheck`	Подключаемый модуль munin-node для опроса Dr.Web SNMPD через SNMP с целью получения статистики проверки файлов Dr.Web для файловых серверов UNIX 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/Ubuntu это путь `/usr/share/munin/plugins`).
   - Сконфигурируйте 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. Обратите внимание, что 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/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 http://guide.munin-monitoring.org/en/latest.

Интеграция с системой мониторинга Zabbix

Для подключения Dr.Web SNMPD к системе мониторинга Zabbix в каталоге <*opt_dir*>`/share/drweb-snmpd/connectors/zabbix` поставляются следующие файлы шаблонов.

Файл	Описание
`zbx_drweb.xml`	Шаблон описания наблюдаемого узла с установленным Dr.Web для файловых серверов UNIX
`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 для файловых серверов UNIX 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_dir>*`/share/drweb-snmpd/connectors/zabbix/zbx_drweb.xml`.
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**.

     Примечание: 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`. О 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 формировать соответствующих нотификаций. 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, как неизвестные, уведомления *SNMP trap*, отправленные Dr.Web SNMPD, добавьте в этот файл также 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_dir*>`/share/drweb-snmpd/connectors/zabbix/snmptt.drweb.zabbix.conf`, 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` — это файл журнала, в который `snmptt` записывает информацию о поступивших уведомлениях SNMP trap.

Подробнее с официальной документацией по Zabbix вы можете ознакомиться по ссылке https://www.zabbix.com/documentation/current/en.

Интеграция с системой мониторинга Nagios

Для подключения Dr.Web SNMPD к системе мониторинга Nagios в каталоге <*opt_dir*>`/share/drweb-snmpd/connectors/nagios` 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
`plugins/check_drweb`	Скрипт для сбора данных от узла с Dr.Web для файловых серверов UNIX

Файл	Описание
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 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 для файловых серверов UNIX 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 RRD Tool.

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 для файловых серверов UNIX, 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 RRD Tool 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 переменных конфигурации 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=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDES
C$||$SERVICEOUTPUT$||$SERVICEPERFDATA$
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_dir>*`/share/drweb-snmpd/connectors/nagios/plugins/eventhandlers/`. Необходимо в этом файле исправить путь, указанный в параметре `CommandFile`. Он должен иметь такое 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, используя следующую 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 при проверке ошибки не найдены, перезапустите Nagios стандартным способом (например, командой ОС `service nagios restart`).

Подробнее с официальной документацией по Nagios вы можете ознакомиться по ссылке https://www.nagios.org/documentation.

Dr.Web SNMP MIB

Перечень параметров работы Dr.Web для файловых серверов UNIX, 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 trap)**	
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 таблицы каталога ошибок)

Имя параметра	OID параметра	Тип и описание параметра
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)
infectedUrlAlertDstPort	.1.4.9	Порт точки назначения соединения (целое число)

Имя параметра	OID параметра	Тип и описание параметра
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)
infectedEmailAttachmentAlert	.1.5	Уведомление об обнаружении вредоносного вложения в сообщении электронной почты
infectedEmailAttachmentAlertType	.1.5.1	Тип угрозы (целое число *)
infectedEmailAttachmentAlertName	.1.5.2	Название угрозы (строка)
infectedEmailAttachmentAlertOrigin	.1.5.3	Идентификатор компонента, обнаружившего угрозу (целое число***)
infectedEmailAttachmentAlertSocket	.1.5.4	IP-адрес, с которого было получено сообщение электронной почты (строка)
infectedEmailAttachmentAlertMailFrom	.1.5.5	Отправитель сообщения электронной почты (строка)
infectedEmailAttachmentAlertRcptTo	.1.5.6	Список получателей сообщения электронной почты (строка)
infectedEmailAttachmentAlertMessageId	.1.5.7	Значение заголовка `Message-ID` сообщения электронной почты (строка)
infectedEmailAttachmentAlertAction	.1.5.8	Действие, примененное к сообщению электронной почты в целом или инфицированному вложению (целое число: 1 — перепаковано; 2 — отклонено; 3 — отброшено; 4 — вылечено; 5 — перемещено в карантин, 6 — удалено)
infectedEmailAttachmentAlertDivert	.1.5.9	Направление движения сообщения электронной почты

Имя параметра	OID параметра	Тип и описание параметра
		(целое число: 1 — входящее; 2 — исходящее)
infectedEmailAttachmentAlertSrcIp	.1.5.10	IP-адрес источника соединения (строка)
infectedEmailAttachmentAlertSrcPort	.1.5.11	Порт источника соединения (целое число)
infectedEmailAttachmentAlertDstIp	.1.5.12	IP-адрес точки назначения соединения (строка)
infectedEmailAttachmentAlertDstPort	.1.5.13	Порт точки назначения соединения (целое число)
infectedEmailAttachmentAlertSniHost	.1.5.14	SNI точки назначения соединения (для SSL-соединений) (строка)
infectedEmailAttachmentAlertProtocol	.1.5.15	Тип протокола (целое число: 1 — SMTP; 2 — POP3; 3 — IMAP; 4 — HTTP)
infectedEmailAttachmentAlertExePath	.1.5.16	Исполняемый путь программы-инициатора соединения (строка)
infectedEmailAttachmentAlertUserName	.1.5.17	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)

Имя параметра	OID параметра	Тип и описание параметра
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)
categoryUrlAlertUserName	.1.6.10	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
categoryUrlEmailAttachmentAlert	.1.7	Уведомление об обнаружении нежелательного URL в сообщении электронной почты
categoryUrlEmailAttachmentAlertType	.1.7.1	Категория веб-ресурсов, к которой относится URL (целое число**)
categoryUrlEmailAttachmentAlertOrigin	.1.7.2	Идентификатор компонента, обнаружившего угрозу (целое число***)
categoryUrlEmailAttachmentAlertSocket	.1.7.3	IP-адрес, с которого было получено сообщение электронной почты (строка)
categoryUrlEmailAttachmentAlertMailFrom	.1.7.4	Отправитель сообщения электронной почты (строка)
categoryUrlEmailAttachmentAlertRcptTo	.1.7.5	Список получателей сообщения электронной почты (строка)
categoryUrlEmailAttachmentAlertMessageId	.1.7.6	Значение заголовка `Message-ID` сообщения электронной почты (строка)
categoryUrlEmailAttachmentAlertAction	.1.7.7	Действие, примененное к сообщению электронной почты в целом или к вложению (целое число: 1 — перепаковано; 2 — отклонено; 3 — отброшено; 4 —

Имя параметра	OID параметра	Тип и описание параметра
		вылечено; 5 — перемещено в карантин, 6 — удалено)
categoryUrlEmailAttachmentAlertDivert	.1.7.8	Направление движения сообщения электронной почты (целое число: 1 — входящее; 2 — исходящее)
categoryUrlEmailAttachmentAlertSrcIp	.1.7.9	IP-адрес источника соединения (строка)
categoryUrlEmailAttachmentAlertSrcPort	.1.7.10	Порт источника соединения (целое число)
categoryUrlEmailAttachmentAlertDstIp	.1.7.11	IP-адрес точки назначения соединения (строка)
categoryUrlEmailAttachmentAlertDstPort	.1.7.12	Порт точки назначения соединения (целое число)
categoryUrlEmailAttachmentAlertSniHost	.1.7.13	SNI точки назначения соединения (для SSL-соединений) (строка)
categoryUrlEmailAttachmentAlertProtocol	.1.7.14	Тип протокола (целое число: 1 — SMTP; 2 — POP3; 3 — IMAP; 4 — HTTP)
categoryUrlEmailAttachmentAlertExePath	.1.7.15	Исполняемый путь программы-инициатора соединения (строка)
categoryUrlEmailAttachmentAlertUserName	.1.7.16	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
spamEmailAlert	.1.8	Уведомление о признании сообщения электронной почты спамом
spamEmailAlertOrigin	.1.8.1	Идентификатор компонента, обнаружившего угрозу (целое число***)
spamEmailAlertSocket	.1.8.2	IP-адрес, с которого было получено сообщение электронной почты (строка)
spamEmailAlertMailFrom	.1.8.3	Отправитель сообщения электронной почты (строка)

Имя параметра	OID параметра	Тип и описание параметра
spamEmailAlertRcptTo	.1.8.4	Список получателей сообщения электронной почты (строка)
spamEmailAlertMessageId	.1.8.5	Значение заголовка `Message-ID` сообщения электронной почты (строка)
spamEmailAlertAction	.1.8.6	Действие, примененное к сообщению электронной почты в целом или к вложению (целое число: 1 — перепаковано; 2 — отклонено; 3 — отброшено; 4 — вылечено; 5 — перемещено в карантин, 6 — удалено)
spamEmailAlertDivert	.1.8.7	Направление движения сообщения электронной почты (целое число: 1 — входящее; 2 — исходящее)
spamEmailAlertSrcIp	.1.8.8	IP-адрес источника соединения (строка)
spamEmailAlertSrcPort	.1.8.9	Порт источника соединения (целое число)
spamEmailAlertDstIp	.1.8.10	IP-адрес точки назначения соединения (строка)
spamEmailAlertDstPort	.1.8.11	Порт точки назначения соединения (целое число)
spamEmailAlertSniHost	.1.8.12	SNI точки назначения соединения (для SSL-соединений) (строка)
spamEmailAlertProtocol	.1.8.13	Тип протокола (целое число: 1 — SMTP; 2 — POP3; 3 — IMAP; 4 — HTTP)
spamEmailAlertExePath	.1.8.14	Исполняемый путь программы-инициатора соединения (строка)
spamEmailAlertUserName	.1.8.15	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
blockedConnectionAlert	.1.9	Уведомление о блокировке сетевого соединения

Имя параметра	OID параметра	Тип и описание параметра
blockedConnectionAlertOrigin	.1.9.1	Идентификатор компонента, обнаружившего угрозу (целое число***)
blockedConnectionAlertDivert	.1.9.2	Направление соединения (целое число: 1 — входящее; 2 — исходящее)
blockedConnectionAlertSrcIp	.1.9.3	IP-адрес источника соединения (строка)
blockedConnectionAlertSrcPort	.1.9.4	Порт источника соединения (целое число)
blockedConnectionAlertDstIp	.1.9.5	IP-адрес точки назначения соединения (строка)
blockedConnectionAlertDstPort	.1.9.6	Порт точки назначения соединения (целое число)
blockedConnectionAlertSniHost	.1.9.7	SNI точки назначения соединения (для SSL-соединений) (строка)
blockedConnectionAlertProtocol	.1.9.8	Тип протокола (целое число: 1 — SMTP; 2 — POP3; 3 — IMAP; 4 — HTTP)
blockedConnectionAlertExePath	.1.9.9	Исполняемый путь программы-инициатора соединения (строка)
blockedConnectionAlertUserName	.1.9.10	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
stat	**Статистические показатели работы Dr.Web для файловых серверов UNIX**	
threatCounters	.2.1	Счетчики обнаруженных угроз
knownVirus	.2.1.1	Число обнаруженных известных вирусов (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)

Имя параметра	OID параметра	Тип и описание параметра
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 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)

Имя параметра	OID параметра	Тип и описание параметра
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)
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)

Имя параметра	OID параметра	Тип и описание параметра
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 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)

Имя параметра	OID параметра	Тип и описание параметра
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)
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)

Имя параметра	OID параметра	Тип и описание параметра
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)
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)

Имя параметра	OID параметра	Тип и описание параметра
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)
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
markedAsSpam	.2.4.1	Число сообщений электронной почты, отмеченных, как спам (счетчик; целое число)
blockedInfectionSource	.2.4.101	Число заблокированных URL из категории «Источники распространения вирусов» (счетчик; целое число)
blockedNotRecommended	.2.4.102	Число заблокированных URL из категории «Нерекомендуемые» (счетчик; целое число)
blockedAdultContent	.2.4.103	Число заблокированных URL из категории «Сайты для взрослых» (счетчик; целое число)
blockedViolence	.2.4.104	Число заблокированных URL из категории «Насилие» (счетчик; целое число)
blockedWeapons	.2.4.105	Число заблокированных URL из категории «Оружие» (счетчик; целое число)
blockedGambling	.2.4.106	Число заблокированных URL из категории «Азартные игры» (счетчик; целое число)
blockedDrugs	.2.4.107	Число заблокированных URL из категории «Наркотики» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
blockedObsceneLanguage	.2.4.108	Число заблокированных URL из категории «Нецензурная лексика» (счетчик; целое число)
blockedChats	.2.4.109	Число заблокированных URL из категории «Чаты» (счетчик; целое число)
blockedTerrorism	.2.4.110	Число заблокированных URL из категории «Терроризм» (счетчик; целое число)
blockedFreeEmail	.2.4.111	Число заблокированных URL из категории «Бесплатная электронная почта» (счетчик; целое число)
blockedSocialNetworks	.2.4.112	Число заблокированных URL из категории «Социальные сети» (счетчик; целое число)
blockedOwnersNotice	.2.4.113	Число заблокированных URL из категории «По обращению правообладателя» (счетчик; целое число)
blockedOnlineGames	.2.4.114	Число заблокированных URL из категории «Онлайн-игры» (счетчик; целое число)
blockedAnonymizers	.2.4.115	Число заблокированных URL из категории «Анонимайзеры» (счетчик; целое число)
blockedCryptocurrencyMiningPools	.2.4.116	Число заблокированных URL из категории «Пулы добычи криптовалют» (счетчик; целое число)
blockedJobs	.2.4.117	Число заблокированных URL из категории "Вакансии" (счетчик: целое число)
blockedBlackList	.2.4.120	Число заблокированных URL из пользовательского черного списка (счетчик; целое число)
info	**Информация о состоянии Dr.Web для файловых серверов UNIX**	

Имя параметра	OID параметра	Тип и описание параметра
components	.3.1	Состояние компонентов Dr.Web для файловых серверов UNIX
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*)
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)

Имя параметра	OID параметра	Тип и описание параметра
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 вирусных записей (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
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)

Имя параметра	OID параметра	Тип и описание параметра
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)
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)

Имя параметра	OID параметра	Тип и описание параметра
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
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)

Имя параметра	OID параметра	Тип и описание параметра
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****)
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 — одиночный, 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)

Имя параметра	OID параметра	Тип и описание параметра
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)
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)

Имя параметра	OID параметра	Тип и описание параметра
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****)
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*)
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*)

Имя параметра	OID параметра	Тип и описание параметра
icapd	.3.1.21	Данные о компоненте drweb-icapd
icapdState	.3.1.21.1	Состояние компонента (целое число****)
icapdExitCode	.3.1.21.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
icapdExitTime	.3.1.21.3	Время завершения работы (*UNIX time*)
icapdConnectionsIn	.3.1.21.101	Число принятых соединений (счетчик; целое число)
icapdConnectionsCount	.3.1.21.102	Текущее число открытых соединений (счетчик; целое число)
icapdOptions	.3.1.21.103	Число запросов *OPTIONS* (счетчик; целое число)
icapdReqmod	.3.1.21.104	Число запросов *REQMOD* (счетчик; целое число)
icapdRespmod	.3.1.21.105	Число запросов *RESPMOD* (счетчик; целое число)
icapdBad	.3.1.21.106	Число некорректных запросов (счетчик; целое число)
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 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)

Имя параметра	OID параметра	Тип и описание параметра
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)
gated	.3.1.41	Данные о компоненте `drweb-gated`
gatedState	.3.1.41.1	Состояние компонента (целое число****)
gatedExitCode	.3.1.41.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
gatedExitTime	.3.1.41.3	Время завершения работы (*UNIX time*)
gatedInterceptedIn	.3.1.41.101	Число перехваченных соединений (счетчик; целое число)
gatedInterceptedCount	.3.1.41.102	Число соединений, которые находятся под наблюдением в данный момент (счетчик; целое число)
maild	.3.1.42	Данные о компоненте `drweb-maild`

Имя параметра	OID параметра	Тип и описание параметра
maildState	.3.1.42.1	Состояние компонента (целое число****)
maildExitCode	.3.1.42.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
maildExitTime	.3.1.42.3	Время завершения работы (*UNIX time*)
maildStat	.3.1.42.4	Статистика работы компонента `drweb-maild`
maildStatNative	.3.1.42.4.1	Статистика проверки сообщений электронной почты через внутренний интерфейс компонента `drweb-maild` (сообщения, полученные от SplDer Gate в рамках проверки перехваченных соединений SMTP, POP3, IMAP)
maildStatNativePassed	.3.1.42.4.1.1	Число пропущенных сообщений (счетчик; целое число)
maildStatNativeRepacked	.3.1.42.4.1.2	Число перепакованных сообщений (счетчик; целое число)
maildStatNativeRejected	.3.1.42.4.1.3	Число отвергнутых сообщений (счетчик; целое число)
maildStatNativeFailed	.3.1.42.4.1.4	Число ошибок проверки сообщений (счетчик; целое число)
maildStatNativeQueueSize	.3.1.42.4.1.5	Длина очереди, т. е. число сообщений, ожидающих проверки через данный интерфейс (целое число)
maildStatMilter	.3.1.42.4.2	Статистика проверки сообщений электронной почты через интерфейс *Milter* компонента `drweb-maild`
maildStatMilterPassed	.3.1.42.4.2.1	Число пропущенных сообщений (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
maildStatMilterRepacked	.3.1.42.4.2.2	Число перепакованных сообщений (счетчик; целое число)
maildStatMilterRejected	.3.1.42.4.2.3	Число отвергнутых сообщений (счетчик; целое число)
maildStatMilterFailed	.3.1.42.4.2.4	Число ошибок проверки сообщений (счетчик; целое число)
maildStatMilterQueueSize	.3.1.42.4.2.5	Длина очереди, т. е. число сообщений, ожидающих проверки через данный интерфейс (целое число)
maildStatSpamc	.3.1.42.4.3	Статистика проверки сообщений электронной почты через интерфейс *Spamd* компонента `drweb-maild`
maildStatSpamcPassed	.3.1.42.4.3.1	Число пропущенных сообщений (счетчик; целое число)
maildStatSpamcRepacked	.3.1.42.4.3.2	Число перепакованных сообщений (счетчик; целое число)
maildStatSpamcRejected	.3.1.42.4.3.3	Число отвергнутых сообщений (счетчик; целое число)
maildStatSpamcFailed	.3.1.42.4.3.4	Число ошибок проверки сообщений (счетчик; целое число)
maildStatSpamcQueueSize	.3.1.42.4.3.5	Длина очереди, т. е. число сообщений, ожидающих проверки через данный интерфейс (целое число)
maildStatRspamc	.3.1.42.4.4	Статистика проверки сообщений электронной почты через интерфейс *Rspamd* компонента `drweb-maild`
maildStatRspamcPassed	.3.1.42.4.4.1	Число пропущенных сообщений (счетчик; целое число)
maildStatRspamcRepacked	.3.1.42.4.4.2	Число перепакованных сообщений (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
maildStatRspamcRejected	.3.1.42.4.4.3	Число отвергнутых сообщений (счетчик; целое число)
maildStatRspamcFailed	.3.1.42.4.4.4	Число ошибок проверки сообщений (счетчик; целое число)
maildStatRspamcQueueSize	.3.1.42.4.4.5	Длина очереди, т. е. число сообщений, ожидающих проверки через данный интерфейс (целое число)
lookupd	.3.1.43	Данные о компоненте drweb-lookupd
lookupdState	.3.1.43.1	Состояние компонента (целое число****)
lookupdExitCode	.3.1.43.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
lookupdExitTime	.3.1.43.3	Время завершения работы (*UNIX time*)
antispam	.3.1.44	Данные о компоненте drweb-ase
antispamState	.3.1.44.1	Состояние компонента (целое число****)
antispamExitCode	.3.1.44.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
antispamExitTime	.3.1.44.3	Время завершения работы (*UNIX time*)
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)

Имя параметра	OID параметра	Тип и описание параметра
clouddExitTime	.3.1.50.3	Время завершения работы (*UNIX time*)
meshd	.3.1.52	Данные о компоненте drweb-meshd
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*)
lotus	.3.1.60	Данные о компоненте drweb-lotus
lotusState	.3.1.60.1	Состояние компонента (целое число****)
lotusExitCode	.3.1.60.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
lotusExitTime	.3.1.60.3	Время завершения работы (*UNIX time*)
macgui	.3.1.100	Данные о компоненте drweb-gui (для macOS)
macguiState	.3.1.100.1	Состояние компонента (целое число****)
macguiExitCode	.3.1.100.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
macguiExitTime	.3.1.100.3	Время завершения работы (*UNIX time*)
macspider	.3.1.102	Данные о компоненте drweb-spider (для macOS)
macspiderState	.3.1.102.1	Состояние компонента (целое число****)

Имя параметра	OID параметра	Тип и описание параметра
macspiderExitCode	.3.1.102.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
macspiderExitTime	.3.1.102.3	Время завершения работы (*UNIX time*)
macspiderWorkStatus	.3.1.102.101	Режим работы компонента (целое число: 0 — не задан, 1 — загружается, 2 — запущен)
macfirewall	.3.1.103	Данные о компоненте `drweb-firewall` (для macOS)
macfirewallState	.3.1.103.1	Состояние компонента (целое число****)
macfirewallExitCode	.3.1.103.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
macfirewallExitTime	.3.1.103.3	Время завершения работы (*UNIX time*)
linuxgui	.3.1.200	Данные о компоненте `drweb-gui` (для GNU/Linux)
linuxguiState	.3.1.200.1	Состояние компонента (целое число****)
linuxguiExitCode	.3.1.200.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxguiExitTime	.3.1.200.3	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)

Имя параметра	OID параметра	Тип и описание параметра
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)
linuxnssScanErrors	.3.1.202.103	Число ошибок сканирования (счетчик; целое число)
linuxfirewall	.3.1.203	Данные о компоненте `drweb-firewall` (для GNU/Linux)
linuxfirewallState	.3.1.203.1	Состояние компонента (целое число****)
linuxfirewallExitCode	.3.1.203.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxfirewallExitTime	.3.1.203.3	Время завершения работы (*UNIX time*)
ctl	.3.1.300	Данные о компоненте `drweb-ctl`
ctlState	.3.1.300.1	Состояние компонента (целое число****)

Имя параметра	OID параметра	Тип и описание параметра
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	Известный вирус (*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 вирусов (*infectionSource*)
2	Не рекомендуемый (*notRecommended*)

Код	Тип угрозы
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`)
5	Dr.Web ES Agent (`drweb-esagent`)
6	Dr.Web Network Checker (`drweb-netcheck`)
7	Dr.Web HTTPD (`drweb-httpd`)

Код	Компонент
8	Dr.Web SNMPD (`drweb-snmpd`)
20	Dr.Web ClamD (`drweb-clamd`)
21	Dr.Web ICAPD (`drweb-icapd`)
40	SpIDer Guard для SMB (`drweb-smbspider-daemon`)
41	SpIDer Gate (`drweb-gated`)
42	Dr.Web MailD (`drweb-maild`)
43	Dr.Web LookupD (`drweb-lookupd`)
50	Dr.Web CloudD (`drweb-cloudd`)
52	Dr.Web MeshD (`drweb-meshd`)
60	Dr.Web для Lotus
100	`drweb-gui` для macOS
102	SpIDer Guard для macOS для macOC
103	Dr.Web Firewall для macOS для macOS
200	`drweb-gui` для GNU/Linux
201	SpIDer Guard (`drweb-spider`)
202	SpIDer Guard для NSS (`drweb-nss`)
203	Dr.Web Firewall для Linux (`drweb-firewall`) для GNU/Linux
300	Dr.Web Ctl (`drweb-ctl`)
400	Сканирование по заданию сервера централизованной защиты (не является компонентом Dr.Web для файловых серверов UNIX)

****) Состояния компонентов:

Код	Состояние
0	Не установлен
1	Установлен, но не запущен
2	Запускается
3	Работает

Код	Состояние
4	Завершает работу

Для непосредственного получения значений переменных вы можете воспользоваться утилитой `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) используйте следующую команду:

```
$ snmpwalk -Os -c public -v 2c 127.0.0.1 .1.3.6.1.4.1.29690.2.2.1
```

Dr.Web MeshD

Компонент Dr.Web MeshD представляет собой агент, включающий узел с установленным Dr.Web для файловых серверов UNIX в «локальное облако», объединяющее узлы с установленными продуктами Dr.Web для UNIX. Данное облако позволяет решать следующие задачи:

- предоставление одними узлами облака другим услуг по сканированию файлов (услуга по предоставлению сканирующего ядра);
- распространение между узлами облака обновлений вирусных баз.

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.

Принципы работы

В этом разделе

Dr.Web MeshD играет роль посредника, обеспечивающего взаимодействие между узлом с установленным Dr.Web для файловых серверов UNIX 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, являющимися клиентами услуг, предоставляемых данным узлом.

  Компоненты Dr.Web для файловых серверов UNIX, работающие на узле, и обращающиеся к услугам, представляемым облаком, через работающий на этом же узле Dr.Web MeshD, подключаются к нему 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, являющимися провайдерами услуг (например, распространение обновлений вирусных баз, передача файлов на проверку и т. п.).

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, для раздачи свежих обновлений), 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 для файловых серверов UNIX, 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 стартует в роли демона и ждет подключения со стороны клиентов. Кроме того, Dr.Web MeshD может включиться по запросу на локальном узле, например при выполнении команды:

```
$ drweb-ctl update --local-cloud
```

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

Обмен обновлениями (Update)

Данная услуга позволяет узлу подписываться на обновления вирусных и иных баз, рассылать уведомления о наличии свежего обновления, загружать и раздавать файлы обновлений между узлами облака. Настройки использования данной услуги задаются параметрами `Update*`.

Стандартный сценарий использования услуги предполагает, что в локальной сети предприятия на некотором числе машин (исполняющих роль клиентов услуги) установлен Dr.Web MeshD со включенной функцией получения обновлений. Типовые настройки клиента следующие:

```
…
[MeshD]
UpdateChannel = On
UpdateUplink = <адрес сервера>
ListenAddress =
…
[Update]
UseLocalCloud = Yes
…
```

На узле, выполняющем роль локального сервера распространения обновлений, заданы следующие настройки:

```
UpdateChannel = On
UpdateUplink =
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.

Как только на каком-либо из узлов происходит обновление с серверов обновления (внешних по отношению к локальному облаку — серверов обновления ВСО Dr.Web или с сервера централизованной защиты), узел рассылает уведомление всем заинтересованным клиентам (если он настроен на работу в роли сервера услуги обмена обновлениями), а также сообщает серверному узлу новый список файлов, доступных для раздачи с этого узла. Получив это уведомление, клиентские узлы могут запросить загрузку обновленных файлов с сервера, который, в свою очередь, может запросить файлы у клиента, чтобы сохранить их у себя локально, либо отдать другому клиенту, который запросил эти файлы у сервера.

При использовании такой схемы обновление происходит с меньшей задержкой, поскольку клиенты опрашивают ВСО Dr.Web в различное время, и при этом первый обновившийся клиент сразу же раздает свежие файлы обновлений всем заинтересованным узлам облака. При этом также снижается количество передаваемого трафика и нагрузка на серверы ВСО Dr.Web.

Обратите внимание, что при использовании локального облака для распространения обновлений, на узлах помимо компонента Dr.Web MeshD должен присутствовать компонент обновления Dr.Web Updater.

Удаленное сканирование файлов (Engine)

Данная услуга предназначена для предоставления возможности использования 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 нерекомендованным 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, 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.

Аргументы командной строки

Для запуска компонента Dr.Web MeshD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически, по мере необходимости, демоном управления конфигурацией Dr.Web ConfigD. Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-meshd`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[MeshD]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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_dir>*`/bin/drweb-meshd`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-meshd`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-meshd`
`DebugSsh` *{логический}*	Сохранять/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`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`) включительно. Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `30s`
`DnsResolverConfPath` *{путь к файлу}*	Путь к файлу настроек DNS. Значение по умолчанию: `/etc/resolv.conf`
`ListenAddress` *<IP-адрес>:<порт>*	Сетевой сокет (адрес и порт) клиентского подключения, на котором компонент ожидает поступление соединений от узлов облака, являющихся клиентами услуг, предоставляемых данным узлом облака.

Параметр	Описание
	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: *(не задано)*
`UpdateChannel` *{On | Off}*	Включение или выключение для компонента Dr.Web MeshD, работающего на данном узле, возможности принимать участие в услуге по обмену обновлениями вирусных баз между узлами облака (в частности получать обновления вирусных баз от других узлов облака и отправлять свежие обновления в облако). 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`
`UpdateUplink` *{адрес}*	Адрес вышестоящего узла, раздающего обновления 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, то 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 в сети с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`UpdateDebugIpc` *{логический}*	Выполнять вывод отладочной информации в журнал для услуги обмена обновлениями, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`UpdateTraceContent` *{логический}*	Выполнять вывод передаваемых данных в журнал для услуги обмена обновлениями, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`FileChannel` *{On | Off}*	Включение или выключение для компонента Dr.Web MeshD, работающего на данном узле, возможности принимать участие в услуге обмена файлами.

Параметр	Описание
	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 отладочную информацию в журнал для услуги обмена файлами, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`EngineChannel` *{On | Off}*	Включение или выключение для компонента Dr.Web MeshD, работающего на данном узле, возможности 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`
`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

Параметр	Описание
	(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}*	Выполнять вывод отладочной информации в журнал для услуги сканирования, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`UrlChannel` *{On | Off}*	Включение или выключение для компонента Dr.Web MeshD, работающего на данном узле, возможности 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)*
`DiscoveryResponderPort` *{номер порта}*	Порт, на котором вышестоящий узел MeshD отвечает по протоколу UDP на запросы клиентов. Механизм *discovery* работает, если установлена настройка `ListenAddress`. Значение по умолчанию: `18008`
`UrlDebugIpc` *{логический}*	Выводить отладочную информацию в журнал для услуги проверки URL, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`

В текущей версии Dr.Web для файловых серверов UNIX услуга передачи файлов на проверку *File* не используется. Вместо нее следует использовать услугу сканирующего ядра *Engine*.

Dr.Web CloudD

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 с целью ограждения пользователей от посещения нежелательных веб-сайтов и защиты операционных систем серверов и рабочих станций от инфицированных файлов, содержащих новейшие угрозы, описание которых еще не внесено в вирусные базы Dr.Web. Кроме этого, использование облачного сервиса Dr.Web Cloud снижает вероятность ложных срабатываний сканирующего ядра Dr.Web Scanning Engine.

Принципы работы

Компонент предназначен для обращения к облачному сервису Dr.Web Cloud компании «Доктор Веб» с целью проверки содержимого указанного файла на наличие угроз, неизвестных локальному сканирующему ядру Dr.Web Scanning Engine, а также с целью проверки, к каким из предопределенных компанией «Доктор Веб» категорий интернет-ресурсов относится указанный URL. Кроме того, компонент периодически отправляет облачному сервису Dr.Web Cloud статистику обнаружения инфицированных файлов и информацию об операционной системе, на которой установлен Dr.Web для файловых серверов UNIX.

Dr.Web CloudD автоматически запускается демоном управления конфигурацией. Запуск производится в ответ на поступившую команду от пользователя или некоторого компонента Dr.Web для файловых серверов UNIX.

Запросы к облачному сервису Dr.Web (на проверку URL или файлов) через данный компонент могут отправлять различные компоненты Dr.Web для файловых серверов UNIX (в зависимости от состава продукта).

Кроме того, компонент используется при проверке файлов по команде от утилиты управления Dr.Web для файловых серверов UNIX из командной строки Dr.Web Ctl (запускается командой `drweb-ctl`): при обнаружении угроз сканирующее ядро Dr.Web Scanning Engine отправляет отчет о файле в облачный сервис Dr.Web Cloud.

Аргументы командной строки

Для запуска компонента Dr.Web CloudD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/bin/drweb-cloudd [<параметры>]
```

Dr.Web CloudD 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-cloudd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web CloudD.

Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD по мере необходимости. Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-cloudd`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[CloudD]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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_dir*>`/bin/drweb-cloudd`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-cloudd`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-cloudd`
`RunAsUser` *{UID | имя пользователя}*	Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой UID пользователя, так и 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 не указано, то 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. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`) включительно. Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `1h`
`PersistentCache` *{On | Off}*	Включать или нет сохранение на диск кеша ответов, получаемых от Dr.Web Cloud. Значение по умолчанию: `Off`
`DebugSdk` *{логический}*	Включать или нет в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения от Dr.Web Cloud. Значение по умолчанию: `No`

Dr.Web StatD

Компонент Dr.Web StatD предназначен для накопления статистики событий, возникающих в процессе работы компонентов Dr.Web для файловых серверов UNIX. Полученные события сохраняются в постоянное хранилище и могут быть получены по запросу.

Принципы работы

Компонент обеспечивает накопление и постоянное хранение событий, поступающих от компонентов Dr.Web для файловых серверов UNIX в процессе работы. Регистрируются события следующих типов:

- аварийное завершение работы компонента;
- обнаружение угрозы (в частности в сообщении электронной почты).

Dr.Web StatD работает в режиме демона и автоматически запускается демоном управления конфигурацией. Просмотр событий и управление ими обеспечивается командой `events` утилиты Dr.Web Ctl.

Аргументы командной строки

Для запуска компонента Dr.Web StatD из командной строки операционной системы используется следующая команда:

```
$ <opt_dir>/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
```

Данная команда выведет на экран краткую справку компонента Dr.Web StatD.

Замечания о запуске

Не предусмотрен запуск компонента непосредственно из командной строки операционной системы в автономном режиме. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD по мере необходимости. Для управления параметрами работы компонента пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web для файловых серверов UNIX из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-statd`.

Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[StatD]` объединенного конфигурационного файла Dr.Web для файловых серверов UNIX.

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_dir*>`/bin/drweb-statd`. • Для GNU/Linux: `/opt/drweb.com/bin/drweb-statd`. • Для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-statd`
`RunAsUser` *{UID | имя пользователя}*	Параметр указывает компоненту, от имени какого пользователя ему следует запускаться при работе. Можно указать как числовой UID пользователя, так и 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 не указано, то работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`

Параметр	Описание
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`) включительно. Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `30s`
`MaxEventStoreSize` *{размер}*	Максимальный разрешенный размер базы событий. Задается в `mb`, например: `MaxEventStoreSize = 100mb`. Минимальное значение: `50mb`. Значение по умолчанию: `1GB`

Приложения

Приложение А. Виды компьютерных угроз

Под термином *«угроза»* в данной классификации следует понимать 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. Большая часть вирусов создается для повреждения или уничтожения данных.

В компании «Доктор Веб» вирусы делят по типу 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 могут инфицировать также другие типы файлов, которые поддерживают исполнение скриптов, пользуясь уязвимыми скриптами в веб-приложениях;
- *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 защитными механизмами против обнаружения. Методы защиты от обнаружения 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 такого вируса 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 (большинство пишутся на языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках скриптов и т. д.) и по инфицируемым ими операционным системам.

Компьютерные черви

В последнее время вредоносные программы типа «компьютерный червь» стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны создавать свои копии, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через интернет) и рассылает свои функциональные копии на другие компьютеры. Для начала распространения черви могут использовать как действия пользователя, так и автоматический режим выбора и атаки компьютера.

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 делят 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 программы для пересылки мгновенных сообщений (ICQ, IM, IRC и т. д.).

Троянские программы

Этот тип вредоносных программ не способен к саморепликации. Троянские программы подменяют какую-либо из часто запускаемых 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 выполнять другие типы 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; они прописывают себя в реестре, модифицируя ключи;
- *руткиты* предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, 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 системного ядра, 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) веб-сайты. Обычно пользователь перенаправляется с целью увеличения рекламного трафика веб-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 хакерами 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 являться любым типов компьютерных угроз (возможно, даже неизвестным для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать в карантин, а также их следует отправлять на анализ специалистам антивирусной лаборатории «Доктор Веб».

Приложение Б. Устранение компьютерных угроз

В этом приложении

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 определить новые или 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, статистическая значимость которых подтверждена опытным путем) о характерных признаках вредоносного и, наоборот, безопасного исполняемого кода. 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 действия для каждого обнаруженного объекта отдельно. Ниже приведен список доступных действий:

- **Ignore** *(Игнорировать)* — пропустить обнаруженную угрозу, не предпринимая никаких действий.
- **Report** *(Сообщать)* — уведомить о наличии угрозы, но ничего не делать с инфицированным объектом.
- **Block** *(Блокировать)* — заблокировать все виды доступа к инфицированному файлу (действие может быть доступно не для всех компонентов).
- **Cure** *(Лечить)* — попытаться вылечить инфицированный объект, удалив из него вредоносное содержимое, и оставив в целости полезное содержимое. Обратите внимание, что это действие применимо не ко всем видам угроз.
- **Quarantine** *(В карантин)* — переместить инфицированный объект (если он допускает эту операцию) в специальный каталог карантина с целью его изоляции.
- **Delete** *(Удалить)* — 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.

Приложение В. 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:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела https://support.drweb.com/;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.

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 для файловых серверов UNIX.

Для сбора информации для службы технической поддержки введите команду:

```
# <opt_dir>/bin/support-report.sh
```

где <*opt_dir*> — каталог, используемый для размещения основных файлов Dr.Web для файловых серверов UNIX, включая исполняемые файлы и библиотеки (по умолчанию для GNU/Linux — `/opt/drweb.com`). Дополнительную информацию о принятой системе обозначений каталогов см. в разделе Введение.

Для сбора информации для службы технической поддержки рекомендуется запустить утилиту с правами суперпользователя (пользователя *root*). Для получения прав суперпользователя воспользуйтесь командой смены пользователя `su` или командой 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 для файловых серверов UNIX (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 для файловых серверов UNIX:
  - перечень загруженных вирусных баз (`drweb-ctl baseinfo -l`);
  - перечень файлов из каталогов Dr.Web для файловых серверов UNIX и их MD5-хеши;
  - версия и MD5-хеш файла антивирусного ядра Dr.Web Virus-Finding Engine;
  - параметры конфигурации Dr.Web для файловых серверов UNIX (в том числе: содержимое файла `drweb.ini`, правила и файлы значений, используемые в правилах, Lua-процедуры и т. д.);
  - информация о пользователе и разрешениях, извлеченная из ключевого файла, если Dr.Web для файловых серверов UNIX работает не в режиме централизованной защиты.

Сформированный архив с информацией о продукте и системном окружении будет сохранен в домашний каталог пользователя, запустившего утилиту, и будет называться:

```
drweb.report.<timestamp>.tgz
```

где <*timestamp*> — полная метка времени создания отчета, включая миллисекунды, например: `20190618151718.23625`.

Приложение Г. Конфигурационный файл Dr.Web для файловых серверов UNIX

Параметрами конфигурации всех компонентов Dr.Web для файловых серверов UNIX управляет координирующий демон управления конфигурацией Dr.Web ConfigD. Параметры конфигурации всех компонентов хранятся в едином файле `drweb.ini`, который по умолчанию располагается в каталоге <*etc_dir*> (`/etc/opt/drweb.com` для GNU/Linux).

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.

Об условных обозначениях путей <*opt_dir*>, <*etc_dir*> и <*var_dir*> см. Введение.

Просмотреть перечень всех параметров, доступных для изменения, включая те, которые отсутствуют в конфигурационном файле, так как имеют значения по умолчанию, можно при помощи команды:

```
$ drweb-ctl cfshow
```

Изменить значение любого параметра можно двумя способами:

1. Задать его в конфигурационном файле (отредактировав файл в любом текстовом редакторе) и отправить сигнал SIGHUP демону управления конфигурацией (модуль `drweb-configd`) для применения внесенных в файл изменений. Для этого вы можете выполнить команду:

   ```
   # drweb-ctl reload
   ```

2. Выполнить в командной строке команду:

   ```
   # drweb-ctl cfset <секция>.<параметр> <новое значение>
   ```

   

   Для выполнения этой команды утилита управления Dr.Web Ctl должна запускаться от имени суперпользователя. Для получения прав суперпользователя используйте команду `su` или `sudo`.

Подробнее о синтаксисе команд `cfshow` и `cfset` консольной утилиты управления Dr.Web Ctl (модуль `drweb-ctl`) см. в разделе Dr.Web Ctl.

Структура файла

Конфигурационный файл сформирован в соответствии со следующими правилами.

- 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 для файловых серверов UNIX, использующего параметры из этой секции (за исключением секции `[Root]`, в которой хранятся параметры демона управления конфигурацией Dr.Web ConfigD).
- Символы '`;`' или '`#`' в строках конфигурационного файла обозначают начало комментария — весь текст, идущий в строке после этих символов, пропускается компонентами Dr.Web для файловых серверов UNIX при чтении параметров из конфигурационного файла.
- В одной строке файла содержится значение только одного параметра:

  ```
  <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.
- Секции в файле, равно как и параметры внутри каждой секции
- Значения параметров в конфигурационном файле могут быть заключены в кавычки, и должны быть заключены в кавычки в том случае, если они содержат пробелы.
- Некоторые параметры могут иметь несколько значений 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:

  1) перечислив их через запятую:

     ```
     Parameter = Value1, Value2,"Value 3"
     ```

  2) 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"
```

При перечислении путей в виде последовательности строк кавычки не используются:

```
ExcludedPaths = /etc/file1
ExcludedPaths = /etc/file2
```

- Если параметр может принимать несколько значений, это указано в комментариях в конфигурационного файле или в тексте настоящего Руководства.

Описание секций конфигурационного файла приведено в описании использующих его компонентов Dr.Web для файловых серверов UNIX.

Типы параметров

Параметры конфигурации могут принадлежать к следующим типам:

- *адрес* — адрес сетевого соединения в виде пары *<IP-адрес>:<порт>*. В некоторых случаях порт может быть опущен (в каждом случае это указывается в описании параметра);
- *логический* — параметр-флаг. В качестве значений параметра могут быть использованы только значения `Yes` и `No`;
- *целое число* — неотрицательное целое число;
- *дробное число* — в качестве значения параметра может быть указано неотрицательное число, содержащее дробную часть;
- *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:
  1) `w` — недели (`1w` = `7d`);
  2) `d` — сутки (`1d` = `24h`);
  3) `h` — часы (`1h` = `60m`);
  4) `m` — минуты (`1m` = `60s`);
  5) `s` или без суффикса — секунды.

  Для интервала, заданного в секундах, можно после точки указать миллисекунды (не более трех знаков после запятой, 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:

1) в файле конфигурации:

```
UpdateInterval = 30m2.5s
```

2) с использованием команды `drweb-ctl cfset`:

```
# drweb-ctl cfset Update.UpdateInterval 1802.5s
```

3) задание через параметр командной строки (например, для сканирующего ядра Аргументы командной строки):

```
$ drweb-se --WatchdogInterval 1802.5
```

- *размер* — в качестве значения параметра указывается размер некоторого 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:
  - `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 (в реальности в параметрах конфигурации размер всегда сохраняется в байтах);
- *путь к каталогу (файлу)* — в качестве значения параметра выступает строка, содержащая допустимый путь к каталогу (файлу).

Путь к файлу должен заканчиваться именем файла.

В UNIX-подобных операционным системах имена каталогов и файлов регистрозависимы. Если это не оговорено непосредственно в описании параметра, в качестве пути нельзя использовать маски, содержащие специальные символы (`?`, `*`).

- *уровень подробности* — параметр задает уровень подробности записи в журнал для компонента Dr.Web для файловых серверов UNIX. 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;

- *тип журнала* — параметр определяет способ ведения журнала компонентом Dr.Web для файловых серверов UNIX. 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*> — сообщения будут сохраняться компонентом непосредственно в указанный файл журнала.

  Примеры задания параметра:

  1) в файле конфигурации:

```
Log = Stderr:ShowTimestamp
```

  2) с использованием команды `drweb-ctl cfset`:

```
# drweb-ctl cfset Root.Log /var/opt/drweb.com/log/general.log
```

3) задание через параметр командной строки (например, для сканирующего ядра Аргументы командной строки):

```
$ drweb-se --Log Syslog:DAEMON
```

- *действие* — действие компонента Dr.Web для файловых серверов UNIX при обнаружении угроз некоторого типа или при возникновении некоторого другого события. Возможные значения:
  - `Report` — только сформировать уведомление об угрозе, не предпринимать более никаких действий;
  - `Block` — оставить файл неизменным, но заблокировать все виды доступа к нему (действие может быть доступно не для всех компонентов);
  - `Cure` — попытаться выполнить лечение (удалить из тела файла только вредоносное содержимое);
  - `Quarantine` — переместить инфицированный файл в карантин;
  - `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.

Приложение Д. Генерация сертификатов SSL

Для компонентов Dr.Web для файловых серверов UNIX, 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 для файловых серверов UNIX. 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 можно использовать 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
   ```

   

   Данная 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 можно воспользоваться командой:

   ```
   $ 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/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 не имеется, 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 можно воспользоваться командой:

   ```
   $ openssl req -noout -text -in request.csr
   ```

2. На основании запроса и имеющегося сертификата ЦС создать подписанный сертификат. Создание подписанного сертификата производится командой:

   ```
   $ 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 можно воспользоваться командой:

```
$ 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 может быть выполнено 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`.

Приложение Е. Описание известных ошибок

В этом разделе

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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой:

```
# 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки конфигурационного файла перезапустите демон управления конфигурацией.
4. Если демон управления конфигурацией запустить не удается, попробуйте переустановить пакет `drweb-configd`.

   Инструкции по установке и удалению Dr.Web для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Operation is already in progress (Операция уже выполняется)*

Код ошибки: `x2`

Внутреннее обозначение ошибки: `EC_IN_PENDING_STATE`

Описание: Запрошенная операция уже выполняется.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Подождите завершения операции и при необходимости повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Подождите начала выполнения операции и при необходимости повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие снова.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Link disconnected (Соединение IPC разорвано)*

Код ошибки: `x6`

Внутреннее обозначение ошибки: `EC_LINK_DISCONNECTED`

Описание: IPC-соединение с одним из компонентов Dr.Web для файловых серверов UNIX 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. 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, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Перезапустите Dr.Web для файловых серверов UNIX:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Invalid IPC message size (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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Перезапустите Dr.Web для файловых серверов UNIX:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 для файловых серверов UNIX.

   Инструкции по установке и удалению Dr.Web для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX, необходимая для выполнения операции, находится в неизвестном состоянии.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

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

   после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Замените относительный путь к файлу или каталогу на абсолютный и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Попробуйте увеличить объем памяти, доступной процессам Dr.Web для файловых серверов UNIX (например, изменив лимиты при помощи команды `ulimit`), перезапустить Dr.Web для файловых серверов UNIX 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` вы можете ознакомиться в документации `man systemd.exec`.

   Для перезапуска Dr.Web для файловых серверов UNIX выполните команду:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 недоступен).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте доступность требуемого устройства ввода/вывода или раздела файловой системы. При необходимости примонтируйте его и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность указанного пути. При необходимости исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность указанного пути и наличие необходимых прав у компонента. При необходимости доступа к объекту, измените права доступа к нему или повысьте права компонента и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Not a directory (Не каталог)*

Код ошибки: `x25`

Внутреннее обозначение ошибки: `EC_BAD_MESSAGE_SIZE`

Описание: Указанный объект файловой системы не является каталогом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к объекту. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web для файловых серверов UNIX:

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

   после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность написания имени файла и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к объекту. Исправьте путь так, чтобы он вел на раздел файловой системы, доступный для записи, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. 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, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. 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, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите операцию сканирования.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. 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, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте доступность требуемого узла сети. При необходимости исправьте адрес узла сети и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте доступность требуемого ресурса. При необходимости увеличьте лимит на использование ресурса и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Выберите другой путь для восстановления файла и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Unpacking error (Ошибка распаковки)*

Код ошибки: `x38`

Внутреннее обозначение ошибки: `EC_BAD_MESSAGE_SIZE`

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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. 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, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - или выполните команду:

   ```
   $ drweb-ctl update
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Non-supported virus database version (Не поддерживаемая 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - или выполните команду:

   ```
   $ drweb-ctl update
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Empty virus database (Вирусная база пуста)*

Код ошибки: `x42`

Внутреннее обозначение ошибки: `EC_EMPTY_BASE`

Описание: Вирусные базы пусты.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).

- Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Object can 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Выберите действие, допустимое для данного объекта, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Non-supported virus database combination (Не поддерживаемая комбинация вирусных баз)*

Код ошибки: `x44`

Внутреннее обозначение ошибки: `EC_INVALID_BASE_SET`

Описание: Набор вирусных баз несовместим.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в

файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - или выполните команду:

   ```
   $ drweb-ctl update
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - 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, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Пройдите аутентификацию, указав правильные учетные данные пользователя, имеющего необходимые полномочия, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность написания и формат команды.
2. Повторите требуемое действие снова, указав допустимый аргумент.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие снова, указав допустимую команду.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повысьте свои права до суперпользователя и повторите требуемое действие снова. Для повышения прав вы можете воспользоваться командами `su` и `sudo`.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Not allowed in cental 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 для файловых серверов UNIX в одиночном (standalone) режиме.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Переведите Dr.Web для файловых серверов UNIX в одиночный режим и повторите операцию снова.
2. Для перевода Dr.Web для файловых серверов UNIX в одиночный режим:
   - сбросьте флажок **Включить режим централизованной защиты** на странице настроек **Централизованная защита** веб-интерфейса управления, если он установлен;
   - или выполните команду:

```
# drweb-ctl esdisconnect
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Non-supported OS (Не поддерживаемая ОС)*

Код ошибки: `x64`

Внутреннее обозначение ошибки: `EC_NON_SUPPORTED_OS`

Описание: Операционная система, установленная на узле, не поддерживается Dr.Web для файловых серверов UNIX.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Установите операционную систему из списка, указанного в системных требованиях.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Попробуйте сбросить настройки Dr.Web для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также

вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Откройте файл <*etc_dir*>`/drweb.ini` 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 для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Откройте файл <*etc_dir*>`/drweb.ini` 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 для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Измените значение параметра любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления (если он установлен);
   - 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 вы можете отредактировать непосредственно файл конфигурации <*etc_dir*>`/drweb.ini`. 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 для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX в целом для выполнения запрошенной операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие через некоторое время.
2. При повторении ошибки перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Измените значение параметра любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления (если он установлен);
   - 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 вы можете отредактировать непосредственно файл конфигурации <*etc_dir*>`/drweb.ini`. 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 для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - 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, попробуйте переустановить пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления, если он установлен;
   - или выполните команду:

```
$ drweb-ctl update
```

3. Если ошибка повторяется, попробуйте переустановить пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Обновите вирусные базы повторно через некоторое время:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления, если он установлен;
   - или выполните команду:

```
$ drweb-ctl update
```

2. Если ошибка повторяется, попробуйте переустановить пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web для файловых серверов UNIX и его компонентов

см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Обновите вирусные базы повторно через некоторое время:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления, если он установлен;
   - или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - или выполните команду:

   ```
   $ drweb-ctl update
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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 (если он установлен).
4. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 можете воспользоваться также формой

активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления (если он установлен).

3. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Invalid checksum (Недопустимая контрольная сумма)*

Код ошибки: `x98`

Внутреннее обозначение ошибки: `EC_BAD_CHECKSUM`

Описание: Нарушена контрольная сумма загруженного файла с обновлениями.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Обновите вирусные базы повторно через некоторое время:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления, если он установлен;
   - или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 можете воспользоваться также формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления (если он установлен).
3. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 можете воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления (если он установлен).
3. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 можете воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления (если он установлен).
3. Параметры текущей лицензии вы можете просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Сообщение об ошибке: *Invalid configuration (Недопустимая конфигурация)*

Код ошибки: `x102`

Внутреннее обозначение ошибки: `EC_BAD_CONFIG`

Описание: Компонент Dr.Web для файловых серверов UNIX не может функционировать из-за неправильных настроек конфигурации.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 скорее 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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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 SplDer Guard.

> ⚠ Работа компонента SplDer Guard и загружаемого модуля ядра гарантируется только в том случае, если используемая вами ОС входит в список поддерживаемых дистрибутивов UNIX (см. раздел Системные требования и совместимость).

3. Если ошибка вызвана другим компонентом, то попробуйте сбросить настройки компонента в значения по умолчанию любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления (если он установлен);
   - 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, попробуйте сбросить настройки Dr.Web для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   После очистки файла конфигурации перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также

вы можете воспользоваться командой `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 для файловых серверов UNIX (параметр `ExePath` в секции компонента), выполнив команду (замените <*секция компонента*> на название соответствующей секции файла конфигурации):

   ```
   $ drweb-ctl cfshow <секция компонента>.ExePath
   ```

3. Попробуйте сбросить 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, попробуйте переустановить пакет соответствующего компонента.

   Инструкции по установке и удалению Dr.Web для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - 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 для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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, если он установлен;
   - или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен);
   - 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 для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   После очистки файла конфигурации перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Попробуйте повторить выполнявшуюся операцию.
2. Если компонент постоянно аварийно 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 (если он установлен);
   - 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 для файловых серверов UNIX в значения по умолчанию.

   Для этого очистите содержимое файла <*etc_dir*>`/drweb.ini` (при этом рекомендуется выполнить сохранение резервной копии файла конфигурации), например, выполнив команды:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   После очистки файла конфигурации перезапустите Dr.Web для файловых серверов UNIX, выполнив команду:

   ```
   # service drweb-configd restart
   ```
4. Если ошибка повторяется после сброса настроек Dr.Web для файловых серверов UNIX, попробуйте переустановить пакет компонента.

   Инструкции по установке и удалению Dr.Web для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Отключите или перенастройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 командами утилиты 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 для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 (если он установлен).
   - Также вы можете воспользоваться командами утилиты 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 дистрибутивов UNIX (см. раздел Системные требования и совместимость).

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 командами утилиты 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 для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 командами утилиты 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 для файловых серверов UNIX 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 для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 командами утилиты 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 для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 командами утилиты 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 для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 командами утилиты 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 для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `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 командами утилиты 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 для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив 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 для файловых серверов UNIX (по умолчанию он находится в

файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Также вы можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Попробуйте перезапустить Dr.Web для файловых серверов UNIX:

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

Если устранить ошибку не удастся, обратитесь в техническую поддержку, сообщив код ошибки.

Ошибки без кода

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 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 для файловых серверов UNIX наблюдаются сообщения `Too many open files`.

Описание: В связи большой загрузкой по проверке данных компонент Dr.Web Network Checker исчерпал доступный 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 для файловых серверов UNIX 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` вы можете ознакомиться в документации `man systemd.exec`.

2. После изменения лимита перезапустите Dr.Web для файловых серверов UNIX, 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 для файловых серверов UNIX 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 для файловых серверов UNIX 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 для файловых серверов UNIX невозможна.

3. Если и после этого ошибка повторится, удалите Dr.Web для файловых серверов UNIX целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web для файловых серверов UNIX и его компонентов см. в разделах Установка Dr.Web для файловых серверов UNIX и Удаление Dr.Web для файловых серверов UNIX.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Приложение Ж. Список сокращений

В данном руководстве следующие сокращения использованы без расшифровки:

Обозначение	Расшифровка
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
IP	Internet Protocol
LKM	Linux Kernel Module
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
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol

Обозначение	Расшифровка
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

Предметный указатель

Предметный указатель

Предметный указатель

Т

У

Ф

Ц