



Dr.WEB®

Антивирус
для Novell Storage Services

Защити созданное

Руководство администратора

© 2012 "Доктор Веб". Все права защищены.

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

ТОРГОВЫЕ ЗНАКИ

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

Linux® – зарегистрированный товарный знак Линуса Торвальдса на территории Соединенных Штатов Америки и других стран.

UNIX® – зарегистрированный товарный знак The Open Group.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

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

Антивирус Dr.Web® для Novell Storage Services

Версия 6.0.2

Руководство администратора

08.02.2012

Доктор Веб, Центральный офис в России

125124

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: www.drweb.com

Телефон: +7 (495) 789-45-87

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

«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	8
Используемые обозначения и сокращения	10
Системные требования	11
Совместимость с дистрибутивами Linux	12
Расположение файлов пакета	12
Конфигурационные файлы	13
Установка и удаление Dr.Web для Novell Storage Services	17
Установка универсального пакета для UNIX систем	18
Пользовательский интерфейс графического инсталлятора	21
Использование консольного инсталлятора	28
Удаление универсального пакета для UNIX систем	30
Пользовательский интерфейс графического деинсталлятора	31
Использование консольного деинсталлятора	34
Обновление универсального пакета для UNIX систем	36
Запуск Dr.Web для Novell Storage Services	37
Операционная система с SELinux	38
Регистрация продукта	40
Dr.Web для Novell Storage Services	44
Параметры командной строки	47
Обрабатываемые сигналы	49



Внутренняя статистика работы	49
Статистика проверки файлов	51
Карантин	52
Управление через drweb-nss-qcontrol	53
Файл отчета	57
Проверка конфигурации	58
Конфигурационный файл	59
Секция [General]	59
Секция [Logging]	60
Секция [NSS]	61
Секция [DaemonCommunication]	64
Секция [Actions]	66
Секция [Stat]	68
Секция [Quarantine]	69
Секция [Notifications]	69
Модуль обновления Dr.Web Updater	74
Обновление антивируса и вирусных баз	74
Настройка cron	77
Параметры командной строки	77
Блокирование обновлений для компонентов	79
Восстановление компонентов	80
Настройки	81
Процедура обновления	87
Dr.Web Control Agent	88
Режимы работы	88
Параметры командной строки	91



Конфигурационный файл	93
Секция [Logging]	93
Секция [Agent]	94
Секция [Server]	96
Секция [EnterpriseMode]	97
Секция [StandaloneMode]	99
Секция [Update]	100
Запуск	101
Взаимодействие с компонентами программного комплекса	103
Интеграция с Dr.Web Enterprise Security Suite	104
Настройка компонентов для работы в режиме Enterprise	105
Автоматическое создание учетной записи	106
Создание учетной записи на сервере вручную	106
Задание конфигурации компонентов через веб-интерфейс сервера	107
Экспорт существующей конфигурации на сервер	107
Запуск комплекса	108
Работа с вирусной статистикой	108
Dr.Web Monitor	114
Режимы работы	114
Параметры командной строки	117
Конфигурационный файл	117
Секция [Logging]	117
Секция [Monitor]	119
Запуск	123



Взаимодействие с компонентами программного комплекса	124
Консольный сканер Dr.Web Scanner	126
Параметры командной строки	126
Настройки	134
Запуск	148
Антивирусный модуль Dr.Web Daemon	151
Параметры командной строки	151
Запуск	152
Проверка работоспособности Dr.Web Daemon	154
Режимы проверки	158
Обрабатываемые сигналы	159
Файл отчета	160
Настройки	162
Контакты	181



Введение

Руководство адресовано лицу, отвечающему за антивирусную безопасность и настройку сетей, называемому в данном руководстве "администратором".

Антивирус Dr.Web® для Novell Storage Services служит для обнаружения и обезвреживания вирусов в файловой системе Novell Storage Services™ (NSS) на базе платформы Novell Open Enterprise Server™ под управлением операционной системы SUSE Linux Enterprise Server™. Несмотря на то, что большинство вирусов разрабатывается не для UNIX систем, через файловые серверы могут распространяться вирусы для всех операционных систем, в том числе и макровирусы для приложений.

Данный продукт позволяет обезвреживать все известные вирусы и работает в асинхронном режиме: файлы не блокируются при обработке. Проверка файлов на вирусы может запускаться автоматически при проведении любых файловых операций: создание, изменение, копирование, удаление и т.п.

В программном комплексе **Dr.Web для Novell Storage Services:**

- консольный сканер **Dr.Web Scanner (Сканер)** служит для обнаружения и лечения вирусов на локальной машине, в том числе и в директориях общего доступа;
- резидентный компонент **Dr.Web Daemon (Демон)** используется в качестве подключаемого внешнего антивирусного фильтра;
- резидентный модуль **Dr.Web Monitor (Монитор)** используется для запуска и перезапуска прочих модулей **Dr.Web** в нужном порядке;
- резидентный модуль **Dr.Web Control Agent (Агент)** используется для управления конфигурацией модулей **Dr. Web**, сбора статистической информации и интеграции с **Dr.Web Enterprise Security Suite;**



- Perl-скрипт **Dr.Web Updater** используется для автоматического обновления вирусных баз данных;
- Резидентный модуль **Dr.Web NSS** - основной модуль системы, обеспечивающий взаимодействие с файловой системой NSS.

В настоящем руководстве будет рассмотрен процесс настройки и использования программного комплекса **Dr.Web для Novell Storage Services**, а именно:

- общая характеристика продукта;
- установка программного комплекса **Dr.Web для Novell Storage Services**;
- запуск программного комплекса **Dr.Web для Novell Storage Services**;
- использование модуля обновления **Dr.Web Updater**;
- использование модуля **Dr.Web Agent**;
- использование консольного сканера **Dr.Web Scanner**;
- использование антивирусного модуля **Dr.Web Daemon**;
- использование модуля **Dr.Web Monitor**;
- общее описание работы программного комплекса и модуля **Dr.Web для Novell Storage Services**

В заключении руководства приведена информация для контактов со службой технической поддержки.

Необходимо отметить, что продукты "**Доктор Веб**" находятся в постоянном развитии. Обновления баз данных известных вирусов выходят ежедневно (как правило, несколько раз в день). Периодически появляются новые версии отдельных компонентов. Изменения в продуктах касаются как совершенствования приемов диагностики и борьбы с вирусами, так и средств интеграции с другими приложениями UNIX систем. Кроме того, постоянно расширяется круг приложений, способных работать совместно с продуктами "**Доктор Веб**". Поэтому не исключено, что некоторые детали настройки и использования текущей версии будут отличаться от описанных в настоящем руководстве.



Используемые обозначения и сокращения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в руководстве.
Зеленое и полужирное начертание	Наименования продуктов Доктор Веб или их компонентов.
<u>Зеленое и подчеркнутое начертание</u>	Ссылки на страницы руководства и веб-сайты.
Моноширинный шрифт	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением.
<i>Курсив</i>	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Знак плюса (+)	Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
Восклицательный знак	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

Также для указания директорий, в которые устанавливаются компоненты программного комплекса, используются условные обозначения `%bin_dir`, `%etc_dir` и `%var_dir`:



```
%bin_dir = /opt/drweb/  
%etc_dir = /etc/drweb/  
%var_dir = /var/drweb/
```

Системные требования

Для работы программного комплекса **Dr.Web для Novell Storage Services** требуется:

- Novell Open Enterprise Server SP2 на базе операционной системы SUSE Linux Enterprise Server 10 SP3;
- установленная служба Novell Storage Services (NSS);
- файловая система NSS, смонтированная в определенную директорию системы.

С точки зрения аппаратного обеспечения требования программного комплекса **Dr.Web для Novell Storage Services** совпадают с требованиями операционной системы SUSE Linux Enterprise Server 10 SP3.

Для установки требуется не менее 300 мегабайт свободного места на диске.

Для работы графического инсталлятора требуется X Window System. Для работы установочного скрипта в графическом режиме необходимо, чтобы в системе был установлен эмулятор терминала xterm или xvt.

В зависимости от задач, решаемых программным комплексом **Dr. Web для Novell Storage Services**, рабочей нагрузки, к аппаратному обеспечению компьютера могут предъявляться дополнительные требования.



Совместимость с дистрибутивами Linux

Программный комплекс **Dr.Web для Novell Storage Services** совместим с дистрибутивом Linux SUSE Linux Enterprise Server 10 SP3.

Расположение файлов пакета

По умолчанию **Dr.Web для Novell Storage Services** устанавливается в директории `%bin_dir`, `%etc_dir` и `%var_dir`. В этих директориях создается структура поддиректорий, не зависящая от ОС:

- `%bin_dir` — исполняемые модули программного комплекса и модуль обновления компонентов **Dr.Web Updater** (perl-скрипт `update.pl`);
- `%bin_dir/lib/` — антивирусное ядро в виде подгружаемой библиотеки (`drweb32.dll`). В той же поддиректории могут располагаться различные служебные библиотеки, необходимые для работы компонентов программного комплекса;
- `%etc_dir/agent/` — дополнительные конфигурационные файлы модуля **Dr.Web Agent**;
- `%etc_dir/monitor/` — дополнительные конфигурационные файлы модуля **Dr.Web Monitor**;
- `%var_dir/bases/*.vdb` — базы данных известных вирусов;
- `%etc_dir` — конфигурационные файлы программного комплекса: `drweb32.ini`, `agent.conf`, `monitor.conf`, `drwebd.enable` и `drweb-monitor.enable` (последние два - для настройки работы демонов);
- `%bin_dir/lib/ru_scanner.dwl` — файл языковых ресурсов модуля **Dr.Web Scanner**;
- `%bin_dir/scripts/` — дополнительные скрипты, скрипт автоконфигурации **Dr.Web для Novell Storage**



Services, скрипт миграции для переноса конфигурационных параметров со старых версий продуктов **Dr.Web**;

- `%etc_dir/templates/` — шаблоны уведомлений, которые генерируются и высылаются различным типам получателей при обнаружении в письме вредоносных объектов, а также при возникновении ошибок в работе **Демона** или подключаемых модулей.
- `%bin_dir/doc/` — документация. Вся документация представлена в виде текстовых файлов и присутствует в двух вариантах — англоязычном и русскоязычном (в кодировках KOI8-R и UTF-8);
- `%var_dir/infected/` — карантин для перемещения в него зараженных файлов, если такая реакция компонентов программного комплекса на обнаружение зараженных или подозрительных файлов задана в настройках.

Конфигурационные файлы

Настройка большинства компонентов программного комплекса **Dr.Web для Novell Storage Services** производится с помощью конфигурационных файлов. Конфигурационные файлы являются текстовыми файлами (что позволяет редактировать их любым текстовым редактором), построенными по следующему принципу:

```
--- начало файла ---  
[ Имя секции 1]  
Параметр1 = значение1, ..., значениеК  
...  
ПараметрМ = значение1, ..., значениеК  
...  
[ Имя секции X]  
Параметр1 = значение1, ..., значениеК  
...
```



```
ПараметрУ = значение1, ..., значениеК  
--- конец файла ---
```

Символы ";" или "#" в строках конфигурационного файла обозначают начало комментария - весь текст, идущий в строке за этими символами, пропускается модулями **Dr.Web для Novell Storage Services** при чтении параметров из конфигурационного файла.

Если какой-либо параметр не задан, это не означает, что у данного параметра нет значения. В таких случаях берется заданное в коде программы значение по умолчанию. Лишь некоторые параметры являются необязательными или не имеют значений по умолчанию, о чем, как правило, упоминается отдельно.

Если значение какого-либо параметра задано некорректно, **Dr. Web для Novell Storage Services** выводит сообщение об ошибке и завершает свою работу.

Если при загрузке какого-либо конфигурационного файла в нем обнаруживаются неизвестные параметры, работа программы продолжается в нормальном режиме, но в файл отчета выводится соответствующее предупреждение.

Значения параметров в конфигурационном файле могут быть заключены в кавычки (и должны быть заключены в кавычки в том случае, если содержат пробелы).

Некоторые параметры могут иметь несколько значений, в этом случае значения параметра разделяются запятой (","), или значение параметра задается несколько раз в разных строках конфигурационного файла. При описании параметра возможность существования нескольких значений указывается явно.

Примеры:

Перечисление нескольких значений через запятую:

```
Names = XXXXXX, YYYY
```

Задание тех же значений параметра в разных строках



конфигурационного файла:

Names = XXXXX

Names = YYYYY

В данном руководстве параметры описываются следующим образом:

ИмяПараметра = {Тип параметра | возможные значения параметра}

Описание параметра.

{Может ли иметь несколько значений}.

Значение по умолчанию:

ИмяПараметра = {значение | отсутствует}

Описание параметров дано в порядке их следования в файле конфигурации, создаваемом при установке программного комплекса **Dr.Web для Novell Storage Services**.

Поле Тип параметра может принимать следующие значения:

- численное значение (numerical value) — значение параметра является целым положительным числом.
- время (time) — значение параметра задается в единицах измерения времени. Значение состоит из целого числа, после которого может идти буква, определяющая вид единиц измерения времени (s — секунды, m — минуты, h — часы, регистр букв не учитывается). Если в значении параметра буквы нет, то считается, что время задано в секундах.

Примеры: 30s, 15m

- размер (size) — значение параметра задается в единицах измерения объема памяти (дисковой или оперативной). Значение состоит из целого числа, после которого может идти буква, определяющая вид единиц



измерения объема памяти (b – байты, k – килобайты, m – мегабайты, g – гигабайты, регистр букв не учитывается). Если в значении параметра буквы нет, то считается, что размер задан в байтах.

Примеры: 20b, 15k

- права (permissions) — значение параметра задается числом, обозначающим права доступа к файлам. Право чтения (r) обозначается числом 4, право записи (w) обозначается числом 2, право исполнения (x) обозначается числом 1 - при задании прав эти числа суммируются для каждой категории пользователей (владельца файла, группы владельцев файла и всех остальных, не являющихся ни владельцами, ни членами соответствующей группы).

Примеры: 755 (-rwxr-xr-x), 644 (-rw-r--r--)

- путь к файлу/директории (path to file/directory) — параметр задает расположение файла или директории в файловой системе.
- действия (actions) — действия, совершаемые над объектами, вызвавшими какую-либо реакцию компонентов программного комплекса **Dr.Web для Novell Storage Services**. Для разных параметров набор допустимых действий может различаться, и в этом случае он указывается отдельно для каждого параметра.



Установка и удаление Dr.Web для Novell Storage Services

Ниже описывается процедура установки, обновления и удаления программного комплекса **Dr.Web для Novell Storage Services** из универсального пакета для UNIX систем. Для осуществления этих операций необходимы права администратора (root).

Универсальный пакет для UNIX систем поставляется в формате RPM для использования с менеджером пакетов RPM (RPM Package Manager). Отдельные сценарии для установки и удаления компонентов, а также стандартные графические инсталляторы и деинсталляторы, входящие в состав пакетов такого типа, относятся исключительно к самому RPM-пакету, а не к упакованному в него программному комплексу в целом, и не к отдельным его модулям.

Соответственно, установка, обновление и удаление **Dr.Web для Novell Storage Services** могут быть осуществлены с помощью:

- графических инсталлятора и деинсталлятора;
- консольных инсталляторов и деинсталляторов.

При установке поддерживается работа с зависимостями, т.е. если для установки какого-либо из компонентов программного комплекса должен быть предварительно установлен другой компонент (например, для установки компонента `drweb-daemon` предварительно должны быть установлены компоненты `drweb-common` и `drweb-bases`), то он будет установлен автоматически.

Необходимо отметить, что если вы устанавливаете программный комплекс **Dr.Web для Novell Storage Services** на компьютер, куда ранее из аналогичного универсального RPM-пакета был установлен какой-либо другой продукт **Доктор Веб**, то при каждом использовании графического деинсталлятора вам будет предложено удалить абсолютно все



модули **Доктор Веб**, включая установленные ранее в составе других продуктов.



Крайне внимательно подходите к удалению компонентов, чтобы по ошибке не удалить те из них, которые вы планируете использовать в дальнейшем.

Установка универсального пакета для UNIX систем

Дистрибутив программного комплекса **Dr.Web для Novell Storage Services** распространяется в виде самораспаковывающегося архива `drweb-nss_[номер версии]~linux_[тип архитектуры процессора].run`. В общем случае в архиве содержатся следующие пакеты:

- `drweb-common`: пакет содержит основной конфигурационный файл `drweb32.ini`, библиотеки, документацию и структуру директорий. В процессе установки данного компонента будут созданы пользователь `drweb` и группа `drweb`;
- `drweb-bases`: пакет содержит антивирусное ядро и вирусные базы. Для установки требует пакет `drweb-common`;
- `drweb-libs`: пакет содержит библиотеки, общие для всех компонентов продукта;
- `drweb-epm6.0.2-libs`: пакет содержит библиотеки для графических [инсталлятора](#) и [деинсталлятора](#). Для установки требует пакет `drweb-libs`;
- `drweb-epm6.0.2-uninst`: пакет содержит файлы [графического деинсталлятора](#). Для установки требует пакет `drweb-epm6.0.2-libs`;
- `drweb-boost147`: пакет содержит библиотеки, используемые **Dr.Web Agent** и **Dr.Web Monitor** совместно. Для установки требует пакет `drweb-libs`;
- `drweb-updater`: пакет содержит модуль обновления



антивирусного ядра и вирусных баз. Для установки требуются пакеты `drweb-common` и `drweb-libs`;

- `drweb-agent`: пакет содержит исполняемые файлы **Dr. Web Agent** и документацию к нему. Для установки требуются пакеты `drweb-boost147` и `drweb-common`;
- `drweb-agent-es`: пакет содержит файлы для работы **Dr. Web Agent** в режиме центральной защиты. Для установки требуются пакеты `drweb-agent`, `drweb-updater` и `drweb-scanner`;
- `drweb-monitor`: пакет содержит исполняемые файлы **Dr. Web Monitor** и документацию к нему. Для установки требуются пакеты `drweb-boost147`, `drweb-agent` и `drweb-common`;
- `drweb-daemon`: пакет содержит исполняемые файлы **Dr. Web Daemon** и документацию к нему. Для установки требуются пакеты `drweb-bases` и `drweb-libs`;
- `drweb-scanner`: пакет содержит исполняемые файлы консольного сканера **Dr. Web Scanner** и документацию к нему. Для установки требуются пакеты `drweb-bases` и `drweb-libs`;
- `drweb-perftools0`: пакет содержит библиотеку Google Performance Tools, используемую **Dr. Web NSS**. Для установки требует пакет `drweb-libs`;
- `drweb-nss-doc`: пакет содержит документацию программного комплекса **Dr. Web для Novell Storage Services**;
- `drweb-nss`: пакет содержит исполняемые файлы **Dr. Web NSS** и документацию к нему. Для установки требуются пакеты `drweb-common`, `drweb-perftools0`, `drweb-agent` и `drweb-monitor`.

В версии для 64-битных систем в архив включены два пакета: `drweb-libs` и `drweb-libs32` - в которых содержатся библиотеки для 64-битных и 32-битных компонентов соответственно.

Для автоматической установки компонентов программного комплекса **Dr. Web для Novell Storage Services** разрешите



исполнение архива, например, командой:

```
# chmod +x drweb-nss_[номер версии]
~linux_[тип архитектуры процессора].run
```

и затем запустите его на исполнение командой:

```
# ./drweb-nss_[номер версии] ~linux_[тип
архитектуры процессора].run
```

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

При этом будет создана директория `drweb-nss_[номер версии]~linux_[тип архитектуры процессора]` с набором файлов внутри, и автоматически запустится [графический инсталлятор](#). Если запуск был осуществлен не с правами администратора, то инсталлятор сам попытается получить нужные права.

Если запустить графический инсталлятор не удалось, то автоматически запустится [интерактивный консольный инсталлятор](#).

Если необходимо только распаковать архив, не запуская при этом графический инсталлятор, следует воспользоваться параметром командной строки `--noexec`:

```
# ./drweb-nss_[номер версии] ~linux_[тип
архитектуры процессора].run --noexec
```

Для продолжения установки с помощью графического инсталлятора запустите его командой:

```
# drweb-nss_[номер версии] ~linux_[тип
архитектуры процессора]/install.sh
```

Для установки с использованием консольного инсталлятора потребуется выполнить команду:



```
# drweb-nss_[ номер версии] ~linux_[ тип архитектуры процессора]/setup.sh
```

При установке любым из описанных ниже способов происходит следующее:

- в директорию `%etc_dir/software/conf/` записываются оригиналы дистрибутивных конфигурационных файлов с названиями в формате `[имя_конфигурационного_файла].N`;
- конфигурационные файлы устанавливаются в соответствующие директории системы;
- устанавливаются остальные файлы, причем если файл с таким именем уже имеется (например, остался после неаккуратного удаления пакетов других типов), то на его место записывается новый файл, а копия старого сохраняется как `[имя_файла].O`. Если в директории уже имеется файл с таким именем (`[имя_файла].O`), то он будет удален, а новый файл будет записан на его место;

Пользовательский интерфейс графического инсталлятора

1. При запуске графического инсталлятора командой:

```
# drweb-nss_[ номер версии] ~linux_[ тип архитектуры процессора]/install.sh
```

открывается окно программы установки.

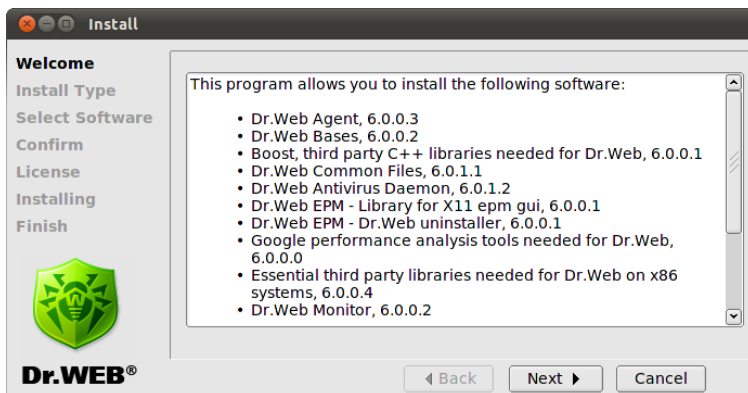


Рис. 1. Окно начала установки программы

Навигация осуществляется с помощью кнопок **Back** и **Next**. Установку можно прервать в любой момент, нажав кнопку **Cancel**.

2. В следующем окне **Install Type** вы можете выбрать тип установки. В **Dr.Web для Novell Storage Services** поддерживается только один тип установки - **Dr.Web for Novell Storage Services**. Нажмите **Next** для продолжения установки.

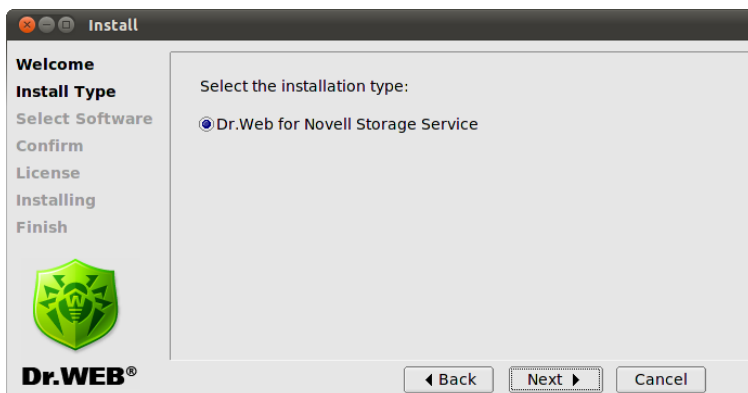


Рис. 2. Тип установки



Следующим откроется окно **Select Software**, в котором вы сможете указать необходимые вам компоненты.

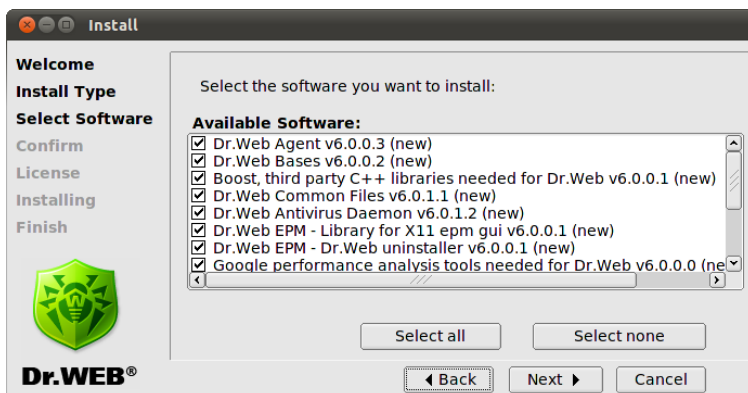


Рис. 3. Окно выбора компонентов для установки



Если для установки выбранного вами компонента должен быть предварительно установлен другой компонент, то соответствующая зависимость будет отмечена автоматически. Таким образом, если вы установите флаг напротив **Dr.Web Antivirus Daemon**, то флаги автоматически появятся напротив пунктов **Dr.Web Bases** и **Dr.Web Common Files**.

Нажатие на кнопку **Select all** выберет все компоненты, нажатие на кнопку **Select none** снимет все установленные флажки.

3. В окне **Confirm** вы увидите все выбранные вами компоненты и сможете принять окончательное решение.

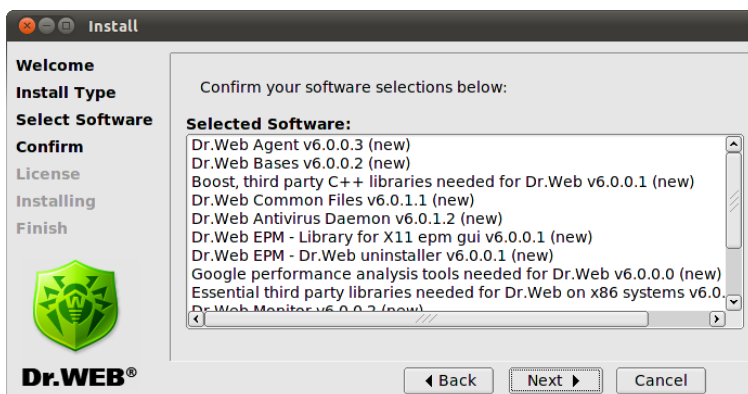


Рис. 4. Окно подтверждения установки компонентов

4. Ознакомьтесь с текстом **Лицензионного Договора** и подтвердите свое согласие с ним, чтобы продолжить установку. С помощью меню **Select language** вы можете выбрать язык (русский или английский), на котором будет изложен текст **Лицензионного Договора**.

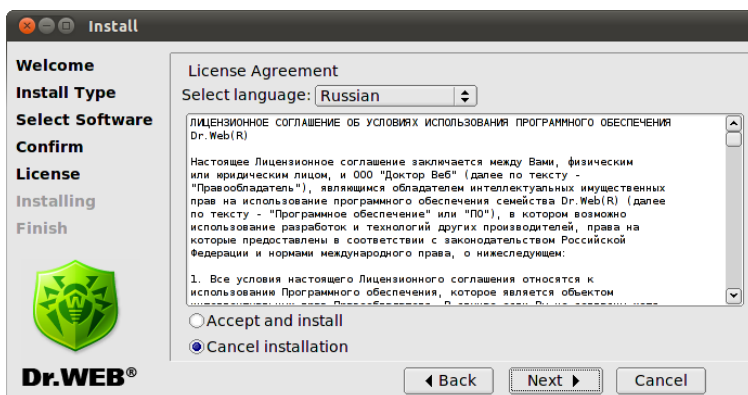


Рис. 5. Окно ознакомления с лицензионным соглашением

5. В следующем окне **Installing** выводится отчет о процессе установки в режиме реального времени.

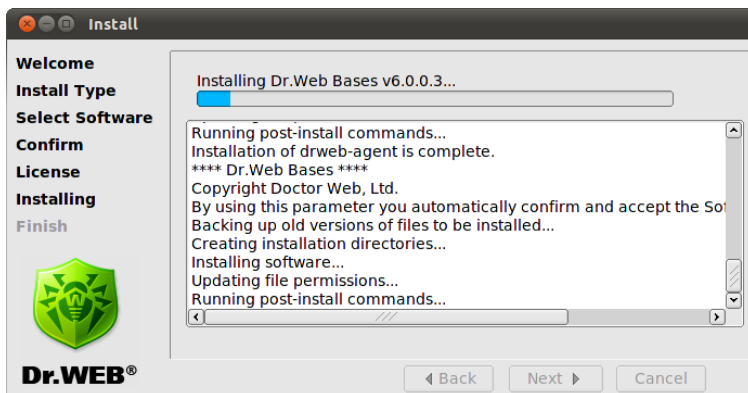


Рис. 6. Окно установки компонентов программы

Одновременно данный отчет копируется в файл `install.log`, расположенный в директории `drweb-nss_[номер версии]~linux_[тип архитектуры процессора]`. Если установлен флаг **Run interactive postinstall script**, то после установки компонентов будет запущен инсталляционный скрипт для настройки базовой функциональности **Dr.Web для Novell Storage Services**.



```
DrWeb
This installation script will help you to configure Dr.Web for Novell Storage Services

Do you want to continue? (YES/no) y
yes
Do you want to install Dr.Web license key file? (YES/no)
yes
Enter path to the Dr.Web license key file or '0' to skip: /home/hully/drweb32.key

Setting 'User' to 'root' in [Monitor] of /etc/drweb/monitor.conf .
Adding 'NSS' to 'RunApplList' in [Monitor] of /etc/drweb/monitor.conf .
/etc/drweb/monitor.conf is up-to-date, it is not necessary to modify it.

Setting 'User' to 'root' in [Daemon] of /etc/drweb/drweb32.ini .
/etc/drweb/drweb32.ini is up-to-date, it is not necessary to modify it.

Enter the path to your NSS share [/media]:

Setting 'NSSVolumesMountDir' to '/media' in [NSS] of /etc/drweb/drweb-nss.conf .
Setting up 'ProtectedVolumes' in [NSS] of /etc/drweb/drweb-nss.conf .

Do you want to select volumes to protect?
(answer "no" to protect all of them) (yes/NO)
no

Enter the drwebd address [pid:/var/drweb/run/drwebd.pid]:

Setting 'address' to 'pid:/var/drweb/run/drwebd.pid' in [DaemonCommunication] of /etc/drweb/drweb-nss.conf .
Info: /etc/drweb/drweb-nss.conf.drwebsave exists. Saving /etc/drweb/drweb-nss.conf as /etc/drweb/drweb-nss.conf.20101027-11_06_25
Your /etc/drweb/drweb-nss.conf has been altered by this script.
The original has been backed up.

Configuration of drweb-nss is completed successfully.

Do you want to configure services? (YES/no) █
```

Рис. 7. Интерактивный установочный скрипт

Скрипт предложит указать путь к лицензионному ключевому файлу, установить порядок работы подключаемых модулей, и автоматически подключить необходимые для работы сервисы (**Dr.Web Daemon**, **Dr. Web Agent**, **Dr.Web Monitor**).

При запуске скрипта вам будет предложено:

- установить лицензионный ключевой файл, полученный после регистрации продукта;
- указать путь к директории, где смонтированы разделы NSS (NSS share);
- указать, если требуется, какие разделы NSS будут защищены от вирусов (по умолчанию защищаются все разделы);



- указать адрес сокета для связи с **Dr.Web Daemon** (drwebd address). По умолчанию предлагается использовать реальный адрес процесса **Демона**, запущенного на локальной машине pid: /var/drweb/run/drwebd.pid;
- если был установлен лицензионный ключевой ключ, запустить модули **Dr.Web Daemon** и **Dr.Web Monitor** (configure services).

Если конфигурационные файлы уже существуют, перед внесением изменений будут сохранены их резервные копии с расширением .drwebsave .

```
DrWeb
Loading /var/drweb/bases/dwn50009.vdb - Ok, virus records: 1445
Loading /var/drweb/bases/dwn50008.vdb - Ok, virus records: 1896
Loading /var/drweb/bases/dwn50007.vdb - Ok, virus records: 2312
Loading /var/drweb/bases/dwn50006.vdb - Ok, virus records: 3006
Loading /var/drweb/bases/dwn50005.vdb - Ok, virus records: 2146
Loading /var/drweb/bases/dwn50004.vdb - Ok, virus records: 1714
Loading /var/drweb/bases/dwn50003.vdb - Ok, virus records: 2096
Loading /var/drweb/bases/dwn50002.vdb - Ok, virus records: 2715
Loading /var/drweb/bases/dwn50001.vdb - Ok, virus records: 2545
Loading /var/drweb/bases/dwn50000.vdb - Ok, virus records: 2801
Loading /var/drweb/bases/dwnrisk9.vdb - Ok, virus records: 6197
Loading /var/drweb/bases/dwnrisk8.vdb - Ok, virus records: 28348
Total virus records: 1711302
Key file: /opt/drweb/drweb32.key - loaded.
License key number: 0010041374
License key activates: 2010-07-05
License key expires: 2011-01-05
License for Internet gateways: Unlimited
License for file-servers: Unlimited
License for mail-servers: Unlimited
Daemon is installed, active interfaces: /var/drweb/run/.daemon 127.0.0.1:3000
Done.
Configuring startup of drweb-monitor...
Starting Dr.Web Monitor...
Done.
Configuration completed successfully.
Press Enter to finish.
```

Рис. 8. Автоматический запуск сервисов

6. В последнем окне **Finish** Нажав на кнопку **Close**, вы закроете окно программы установки компонентов.

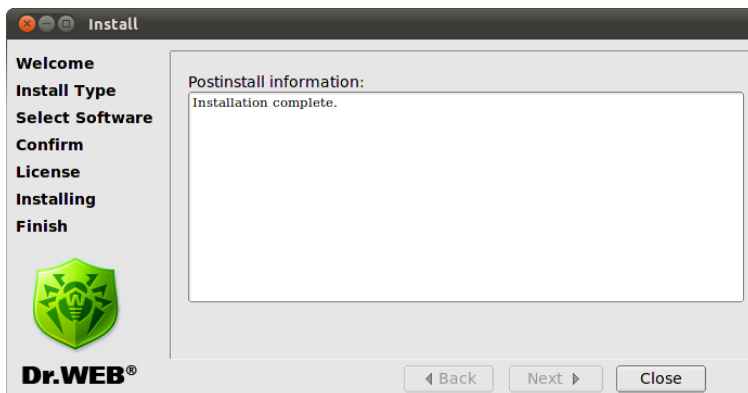


Рис. 9. Окно завершения установки программы

Использование консольного инсталлятора

Консольный инсталлятор запускается автоматически в том случае, если не удалось запустить графический инсталлятор. Если консольный инсталлятор не был запущен автоматически (как правило, это происходит при невозможности повысить права), то можно попробовать запустить его с привилегиями пользователя `root`, выполнив команду:

```
# drweb-nss_[номер версии]~linux_[тип архитектуры процессора]/setup.sh
```

Откроется диалоговое окно консольного инсталлятора.



```
user@hostname: ~
Файл Правка Вид Поиск Терминал Справка

This installation script will help you install Dr.Web for Novell Storage Services

Do you want to continue? (YES/no)
```

Если вы хотите установить **Dr.Web для Novell Storage Services**, укажите **Y** или **Yes** в строке ввода (значения регистронезависимы) и нажмите клавишу ENTER. В противном случае введите **N** или **No**.

На следующем этапе вам будет предложено ознакомиться с текстом **Лицензионного Договора**. Для пролистывания текста договора нажимайте клавишу ПРОБЕЛ.

```
user@hostname: ~
Файл Правка Вид Поиск Терминал Справка

Dr.Web(R) SOFTWARE USAGE LICENSE AGREEMENT

The present License agreement is concluded between you (either a legal
entity or home user) and Doctor Web ("the right holder"), that
possesses intellectual property rights with regard to usage of Dr.Web(R)
software ("software") including usage of technologies and software
from other vendors where corresponding rights are acquired under law of
the Russian Federation and International Law, as follows:

1. All terms and conditions provided herein regulate usage of the
software which is an object of the intellectual property rights of the
right holder. If you do not agree with at least one term or condition
stipulated herein, do not use the software. Violation of the terms of
the present license agreement is considered an unauthorized use of the
software and entails civil, administrative and criminal responsibility.

2. If you are a legal owner of the Software's copy, you receive the
--More-- (24%)
```

Для продолжения установки вы должны будете принять **Лицензионный Договор**, указав **Y** или **Yes** в строке ввода и нажав ENTER. В противном случае установка будет прекращена.



После того, как вы примете **Лицензионный Договор**, будет запущен процесс установки. Отчет о результатах прохождения каждого из этапов процесса будет выводиться на консоль в режиме реального времени.

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
Creating installation directories...
Installing software...
Updating file permissions...
Running post-install commands...
Installation of drweb-libs is complete.
Backing up old versions of files to be installed...
Creating installation directories...
Installing software...
Updating file permissions...
Installation of drweb-boost144 is complete.
Backing up old versions of files to be installed...
Creating installation directories...
Installing software...
Checking configuration files...
Updating file permissions...
Running post-install commands...
Installation of drweb-agent is complete.
Copyright Doctor Web, Ltd.
```

После установки компонентов будет запущен инсталляционный скрипт для настройки базовой функциональности **Dr.Web для Novell Storage Services**. Скрипт предложит указать путь к лицензионному ключевому файлу, установить порядок работы подключаемых модулей, указать список защищаемых сетей и доменов и автоматически подключить необходимые для работы сервисы (**Dr.Web Daemon**, **Dr.Web Agent**, **Dr.Web Monitor**).

Удаление универсального пакета для UNIX систем

Для удаления с помощью [графического деинсталлятора](#), запустите его командой:

```
# %bin_dir/remove.sh
```

Если запуск был осуществлен не с правами администратора, то деинсталлятор сам попытается получить нужные права.



Если запустить графический деинсталлятор не удалось, то автоматически запустится [интерактивный консольный деинсталлятор](#).

После деинсталляции продукта можно удалить средствами ОС пользователя `drweb` и группу `drweb`.

При удалении любым из вышеописанных способов происходит следующее:

- из директории `%etc_dir/software/conf/` удаляются все дистрибутивные конфигурационные файлы;
- если рабочие конфигурационные файлы не были изменены пользователем, то они тоже удаляются. Если пользователь вносил в них изменения, они остаются в неприкосновенности;
- удаляются остальные файлы, причем если при установке была создана копия какого-либо старого файла в виде `[имя_файла].O`, то этот файл восстанавливается в прежнем виде;
- лицензионные ключевые файлы и файлы отчетов различных компонентов программного комплекса в соответствующих директориях сохраняются.

Пользовательский интерфейс графического деинсталлятора

1. При запуске графического деинсталлятора командой:

```
# %bin_dir/remove.sh
```

открывается окно программы удаления компонентов.

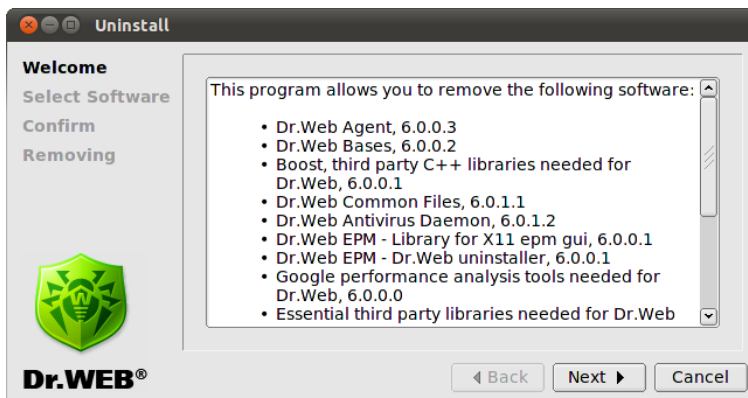


Рис. 10. Окно начала удаления программы

Навигация осуществляется с помощью кнопок **Back** и **Next**. Выйти из программы можно в любой момент, нажав кнопку **Cancel**.

2. В следующем окне **Select Software** вы можете выбрать компоненты, которые хотите удалить. Флаги для соответствующих зависимостей будут проставлены автоматически.

В случае, если ранее на этом компьютере из EPM-пакета был установлен какой-либо другой продукт **Dr.Web**, то в список компонентов для удаления войдут и его модули тоже. Поэтому необходимо быть крайне внимательным при выборе, чтобы случайно не удалить те компоненты, которые планируется использовать в дальнейшем.

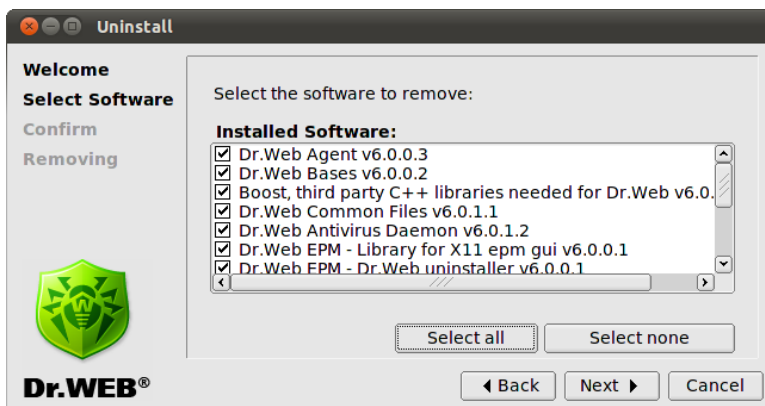


Рис. 11. Окно выбора компонентов для удаления

Нажав на кнопку **Select all**, вы сможете отметить сразу все компоненты. Нажатие на кнопку **Select none** удалит все проставленные флаги.

3. В следующем окне **Confirm** вы увидите все выбранные вами компоненты и сможете принять окончательное решение об их удалении.

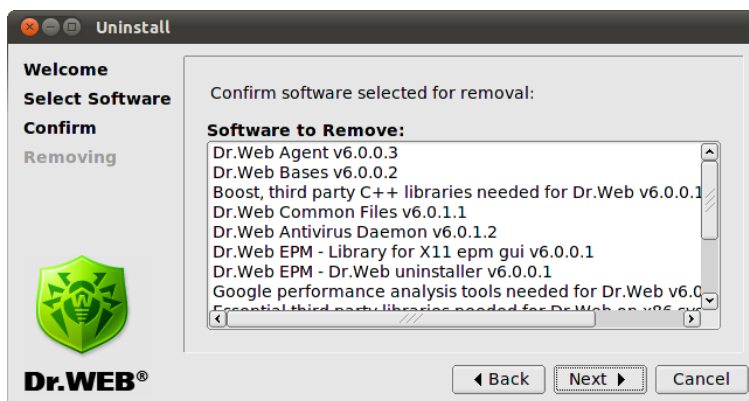


Рис. 12. Окно подтверждения удаления компонентов

4. В последнем окне **Removing** выводится отчет о процессе



удаления компонентов программного комплекса в режиме реального времени.

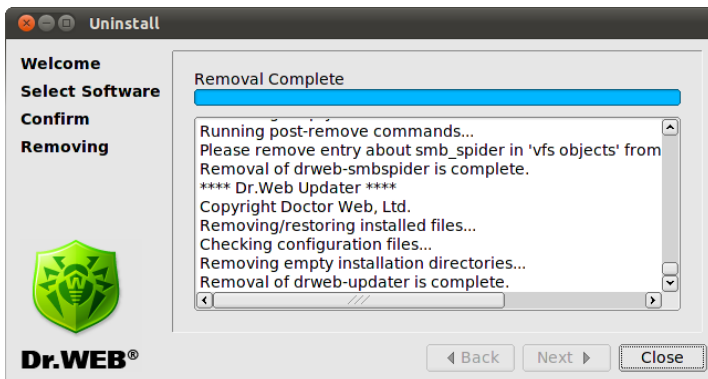


Рис. 13. Окно удаления компонентов программы

5. Нажав на кнопку **Close**, вы закроете окно программы удаления компонентов.

Использование консольного деинсталлятора

Консольный деинсталлятор запускается автоматически в том случае, если не удалось запустить графический деинсталлятор.

Открывается диалоговое окно консольного деинсталлятора.



```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка

This script will help you remove Dr.Web packages

Do you wish to continue? (YES/no)
```

Вам будет предложено выбрать из списка компонентов те, которые вы желаете удалить (следуйте инструкциям на экране).

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка

[ ] 4 Dr.Web Common Files (6.0.1.1)
[ ] 5 Dr.Web Antivirus Daemon (6.0.1.2)
[ ] 6 Dr.Web EPM - Library for X11 epm gui (6.0.0.1)
[ ] 7 Dr.Web EPM - Dr.Web uninstaller (6.0.0.1)
[ ] 8 Google performance analysis tools needed for Dr.Web (6.0.0.0)
[ ] 9 Essential third party libraries needed for Dr.Web on x86 systems (6.0.0.4)
)
[ ] 10 Dr.Web Monitor (6.0.0.2)
[ ] 11 Documentation for Dr.Web Anti-virus for Novell Storage Services (6.0.0.0)
)
[ ] 12 DrWeb for Novell Storage Services (6.0.0.0)
[ ] 13 Dr.Web Antivirus Scanner (6.0.1.2)
[ ] 14 Dr.Web Updater (6.0.0.3)

To select a package you want to remove or deselect some previously
selected package - enter the corresponding package number and press Enter.

You may enter A or All to select all the packages, and N or None to deselect all of the
m.
Enter R or Remove to remove selected packages.
Enter 0, Q or Quit to quit the dialog.
All values are case insensitive.
Select:
```

Для запуска процедуры удаления компонентов вы должны будете подтвердить сделанный выбор, указав **Y** или **Yes** в строке ввода (значения регистронезависимы) и нажав клавишу ENTER.



```
user@hostname: ~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
A list of packages marked for removal:  
drweb-agent  
drweb-bases  
drweb-boost144  
drweb-common  
drweb-daemon  
drweb-epm6.0.0-libs  
drweb-epm6.0.0-uninst  
drweb-gperftools0  
drweb-libs  
drweb-monitor  
drweb-nss-doc  
drweb-nss  
drweb-scanner  
drweb-updater  
Are you sure you want to remove the selected packages? (YES/no) █
```

Отчет о результатах прохождения каждого из этапов процесса удаления компонентов выводится на консоль в режиме реального времени.

Обновление универсального пакета для UNIX систем

Обновление сочетает в себе процессы установки и удаления. Для обновления программного комплекса **Dr.Web для Novell Storage Services** необходимо получить свежую версию продукта, удалить предыдущую версию и установить новую.

При обновлении измененные пользователем конфигурационные файлы, лицензионные ключевые файлы и файлы отчетов различных компонентов программного комплекса сохраняются в соответствующих директориях.



Запуск Dr.Web для Novell Storage Services

Все необходимые процедуры для запуска комплекса можно осуществить с помощью интерактивного конфигурационного скрипта.

Если вы хотите запустить **Dr.Web для Novell Storage Services** вручную:

1. Зарегистрируйте продукт.
2. Скопируйте или переместите полученный после регистрации лицензионный ключевой файл с расширением `.key` в директорию с исполняемыми файлами **Dr.Web для Novell Storage Services** (по умолчанию `/opt/drweb/`). Имя ключевого файла может варьироваться в зависимости от комплекта поставки (подробнее см. в главе [Регистрация продукта](#)). Если вы хотите использовать ключевой файл, расположенный в какой-либо другой директории, путь к нему должен быть задан в параметре `Key` конфигурационного файла `drweb32.ini`. Поскольку **Dr.Web для Novell Storage Services** может работать только в `Standalone` режиме (без интеграции с **Dr.Web Enterprise Security Suite**), путь к ключевому файлу также должен быть указан в параметре `LicenseFile` конфигурационного файла модуля **Dr.Web Control Agent** `agent.conf`.
3. Внесите все необходимые изменения в конфигурационные файлы для настройки **Dr.Web для Novell Storage Services**. Чтобы получить описание конфигурационных параметров различных модулей **Dr.Web для Novell Storage Services** обратитесь к соответствующим разделам Руководства.



4. Откройте файл `/etc/drweb/drwebd.enable`, и установите параметр `ENABLE = 1`. Это позволит запустить **Dr.Web Daemon**.
Если запускать **Dr.Web Daemon** на локальной машине не нужно (используется **Демон**, запущенный на другом компьютере в локальной сети), то для переменной `ENABLE` нужно оставить присвоенное по умолчанию значение `0`.
5. Откройте файл `/etc/drweb/drweb-monitor.enable` и установите параметр `ENABLE = 1`. Это позволит запустить **Dr.Web Monitor**.
6. Запустите **Демон** и **Монитор** через командный интерфейс или файловый менеджер. Все остальные модули **Dr.Web для Novell Storage Services** будут запущены **Монитором**. Каждый из модулей может быть запущен и отдельно, при этом модуль **Dr.Web Control Agent** должен быть запущен самым первым, поскольку все прочие модули получают настройки через него.

Операционная система с SELinux

Чтобы при работающем SELinux компоненты **Dr.Web Scanner** и **Dr.Web Daemon** могли успешно функционировать, необходимо скомпилировать политики для работы с соответствующими модулями `drweb-scanner` и `drweb-daemon`.

Пожалуйста, обратите внимание, что во время компиляции модули политик используют шаблоны, большинство из которых разные в зависимости от дистрибутива Linux, его версии, набора политик SELinux и пользовательских настроек. Соответственно, для получения более подробной информации о компиляции модулей политик вы можете обратиться к документации вашего дистрибутива Linux.

Чтобы создать необходимые политики, воспользуйтесь командой `policygentool`, указав в качестве параметров имя модуля, работу с которым вы хотите настроить, и полный путь к его исполняемому файлу.



Пример:

```
# policygentool drweb-scanner %bin_dir/drweb.  
real - для Сканера.
```

```
# policygentool drweb-daemon %bin_dir/drwebd.  
real - для Демона.
```

Вам будет предложено указать несколько общих характеристик домена, после чего для каждого модуля будут созданы три файла: [module_name].te, [module_name].fc и [module_name].if.

Чтобы скомпилировать файл [module_name].te выполните следующую команду:

```
checkmodule -M -m -o module-name [module_name].  
te
```

Пожалуйста, обратите внимание, что для успешной работы этой команды в системе должен быть установлен пакет checkpolicy.

Для компиляции нужной политики выполните команду:

```
semodule_package -o [module_name].pp -m module-  
name
```

Для установки скомпилированного модуля политики к остальным модулям выполните команду:

```
semodule -i [module_name].pp
```



Регистрация продукта

Права на использование программного комплекса **Dr.Web для Novell Storage Services** регулируются при помощи специального файла, называемого ключевым файлом. В ключевом файле содержится, в частности, следующая информация:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование продукта;
- другие ограничения (например, по числу защищаемых рабочих станций).

Ключевой файл имеет расширение `key` и при работе комплекса по умолчанию должен находиться в одной директории с исполняемыми файлами продукта.

Ключевой файл защищен от редактирования при помощи механизма электронной подписи. Редактирование файла делает его недействительным. Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

Коммерческие пользователи, приобретающие **Dr.Web для Novell Storage Services** у авторизованных поставщиков продукта, получают лицензионный ключевой файл. Параметры этого ключевого файла, регулирующие права пользователя, установлены в соответствии с лицензионным договором. В такой файл также заносится информация о пользователе и продавце продукта.

Для целей ознакомления с программным комплексом **Dr.Web для Novell Storage Services** может быть получен демонстрационный ключевой файл. Такие ключевые файлы обеспечивают полную функциональность основных компонентов комплекса, но имеют ограниченный срок действия и не предполагают оказания поддержки пользователю.



Ключевые файлы поставляются пользователю:

- в виде ключевого файла для рабочей станции `drweb32.key` или в виде ZIP-архива, содержащего этот файл, в случае приобретения **Dr.Web для Novell Storage Services** в качестве отдельного продукта.
- в виде zip-архива, содержащего ключевой файл для Сервера (`enterprise.key`) и ключевой файл для рабочей станции (`agent.key`) в случае приобретения **Dr.Web для Novell Storage Services** в составе программного комплекса **Dr.Web Enterprise Security Suite**.

Ключевой файл может быть получен пользователем:

- по электронной почте в виде ZIP-архива, содержащего файл с расширением `key` (обычно после регистрации на веб-сайте, см. ниже). Необходимо извлечь файл при помощи архиватора данного формата и скопировать/переместить его в директорию с исполняемыми файлами программного комплекса **Dr.Web для Novell Storage Services** (по умолчанию `%bin_dir` для UNIX систем);
- в составе дистрибутива продукта;
- на отдельном носителе в виде файла с расширением `key`. В этом случае его необходимо скопировать в вышеуказанную директорию.

Лицензионный ключевой файл высылается пользователям по электронной почте, как правило, после регистрации на специальном веб-сайте (адрес сайта регистрации указан в регистрационной карточке, прилагаемой к продукту). Для получения лицензионного ключевого файла необходимо зайти на указанный сайт, заполнить форму со сведениями о покупателе и ввести в соответствующее поле регистрационный серийный номер (находится на регистрационной карточке). Это процедура активации лицензии, в результате которой для данного серийного номера создается лицензионный ключевой файл. Затем этот файл высылается на указанный при регистрации адрес электронной почты.

Рекомендуется сохранять лицензионный ключевой файл до истечения срока его действия и использовать его при



переустановке или восстановлении программы. В случае утраты лицензионного ключевого файла можно использовать ту же процедуру, что и при активации лицензии: повторно ввести регистрационный серийный номер и адрес электронной почты — и робот вышлет соответствующий указанному серийному номеру ключевой файл.

Регистрация с одним и тем же регистрационным серийным номером допускается не более 25 раз. При необходимости восстановить утерянный лицензионный ключевой файл после 25 регистраций следует разместить запрос на восстановление ключевого файла по адресу в Интернете <http://support.drweb.com/request/>, указать данные, введенные при регистрации, адрес электронной почты и подробно описать ситуацию. Запрос будет рассмотрен специалистами службы технической поддержки. В случае положительного решения ключевой файл будет либо выдан через автоматизированную систему поддержки пользователей, либо выслан по электронной почте.

Путь к ключу для соответствующего компонента должен быть задан в настройках конфигурационного файла `drweb32.ini` значением параметра **Key**.

Пример:

```
Key = %bin_dir/drweb32.key
```

Если ключевой файл, указанный в параметре **Key**, не удастся прочитать (неверный путь, нет прав), истек срок действия, файл заблокирован или недействителен, то соответствующий компонент завершит свою работу.

Если до истечения срока действия ключевого файла осталось менее двух недель, **Сканер** предупредит об этом при запуске. **Демон** в такой ситуации может извещать пользователя по электронной почте. Сообщения отправляются для каждого установленного ключевого файла при каждом запуске, перезапуске или перезагрузке **Демона**, если до истечения срока действия лицензионного ключевого файла осталось менее двух недель. Чтобы воспользоваться этой возможностью, следует настроить параметр **MailCommand** в секции `[Daemon]` файла `drweb32.ini`.



Если требуется расположить ключевой файл в директории, отличной от стандартной, то следует также указать его новое расположение в параметре **LicenseFile** секции [StandaloneMode] конфигурационного файла компонента **Dr.Web Agent** (см. раздел [Секция \[StandaloneMode\]](#)).



Dr.Web для Novell Storage Services

Программный комплекс **Dr.Web для Novell Storage Services** обеспечивает антивирусную защиту разделов файловой системы NSS с помощью следующих совместно работающих модулей:

- резидентный модуль **Dr.Web NSS** - основной модуль системы, обеспечивающий взаимодействие с файловой системой NSS;
- **Dr.Web Daemon (Демон)** - резидентный модуль, осуществляющий проверку на вирусы по запросу;
- **Dr.Web Monitor (Монитор)** - вспомогательный модуль, запускающий и останавливающий модули системы в заданном порядке, а также контролирующий их работу;
- **Dr.Web Control Agent (Агент)** используется для интеграции с **Dr.Web Enterprise Security Suite** и собирает статистическую информацию о работе модулей системы;

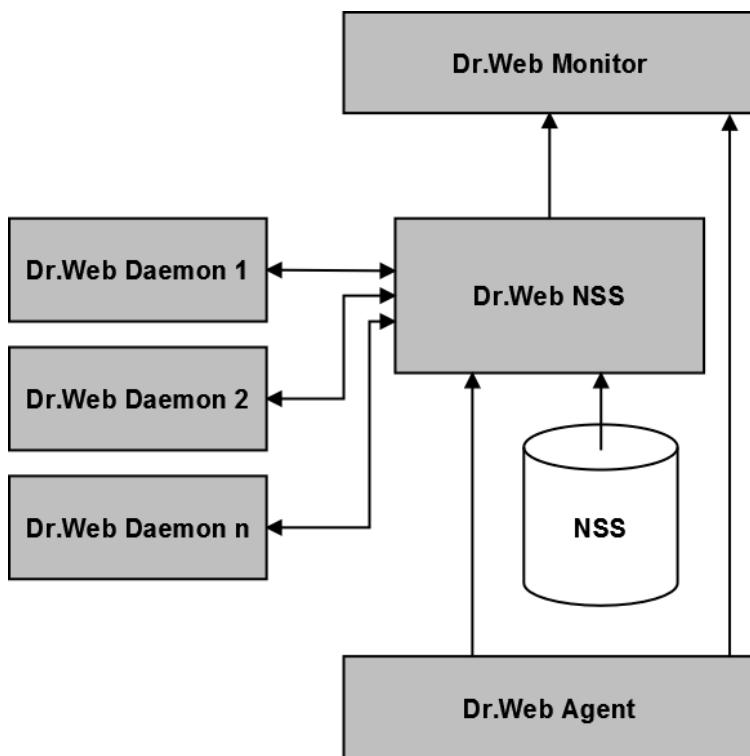


Рис. 14. Схема работы программного комплекса Dr.Web для Novell Storage Services

Dr.Web NSS осуществляет мониторинг избранных томов файловой системы NSS, получает список измененных файлов и обрабатывает их в зависимости от своих настроек. Проверяемые разделы указываются в параметрах секции [NSS] [конфигурационного файла](#) (/etc/drweb/drweb-nss.conf):

- Если задано значение параметра `ProtectedVolumes`, мониторинг осуществляется в разделах, указанных в этом параметре.



- Если значения параметра `ProtectedVolumes` не задано, мониторинг осуществляется во всех разделах, смонтированных в директории, указанной в параметре `NSSVolumesMountDir`.

Перед отправкой на проверку, каждый из файлов проходит первичную фильтрацию:

- не проверяются файлы, размер которых равен нулю;
- не проверяются файлы, размер которых превышает значение, установленное в параметре `MaxFileSizeToScan` секции `[NSS]` конфигурационного файла (если это значение не равно нулю);
- не проверяются файлы, пути к которым указаны в значении параметра `ExcludedPaths` секции `[NSS]` конфигурационного файла и одновременно НЕ указаны в параметре `IncludedPaths`;

Если файл не был отфильтрован, он добавляется во внутреннюю очередь на проверку. Список заданий в очереди выводится в файл отчета на уровне `INFO` каждый раз при получении сигнала `SIGHUP`. Все задания на проверку обрабатываются через пул потоков, который можно настроить в параметре `CheckPoolOptions` секции `[NSS]` конфигурационного файла.

Файлы на проверку передаются **Dr.Web Daemon** для проверки на вирусы. Параметры настройки взаимодействия с **Демоном** находятся в секции `[DaemonCommunication]` конфигурационного файла. **Dr.Web NSS** способен работать одновременно как с **Демоном**, запущенным на локальной машине, так и с **Демонами** на удаленных серверах. В параметре `Address` секции `[DaemonCommunication]` конфигурационного файла вы можете указать список адресов сокетов для связи с **Демонами** и веса этих адресов. При работе с несколькими **Демонами**, **Dr.Web NSS** распределяет нагрузку на них в зависимости от указанных весов: адрес с большим весом будет получать большее количество запросов на сканирование.

Если при проверке **Демоном** были обнаружены вирусы, файл



обрабатывается в соответствии с параметрами секции [Actions] конфигурационного файла, в зависимости от типа обнаруженной угрозы. Не прошедший проверку файл может быть удален, перемещен в карантин (параметры настройки карантин находятся в секции [Quarantine] конфигурационного файла). Об обнаруженной угрозе высылаются уведомления (настройки секции [Notifications]), информация об обработке каждого файла фиксируется в файлах отчета (настройки секции [Logging]).

Кроме того по результатам проверки каждого файла собирается статистика, которая передается модулю **Dr.Web Agent**. Статистика по инфицированным объектам передается сразу, общая статистика передается в **Dr.Web Control Agent** периодически (период указывается в параметре `SendPeriod`). Настройки статистики указаны в секции [Stat] .

Если в процессе обработки файла происходит ошибка, к файлу будет применено действие, указанное в значении параметра `ProcessingError` секции [Actions] .

Параметры командной строки

Как и для любых UNIX программ, в **Dr.Web для Novell Storage Services** предусмотрены параметры командной строки. Команда запуска имеет следующий формат:

```
drweb-nss [ параметры] сокет_агента
```

где:

- параметры – необязательные параметры командной строки;
- сокет_агента – сокет, через который **Dr.Web NSS** получает от **Dr.Web Agent** конфигурационную информацию.

Полный список параметров можно получить, запустив компонент с параметром `-h` либо `--help`. В текущей версии



Dr.Web для Novell Storage Services модули поддерживают следующие параметры командной строки:

- `-v, --version` - информация о текущей версии **Dr. Web для Novell Storage Services**;
- `-l <уровень>, --level <уровень>` - уровень детализации файла отчета (значение по умолчанию: `info`);
- `-t <значение в секундах>, --timeout <значение в секундах>` - максимальное время ожидания получения конфигурационных данных;
- `--component <имя>` - имя модуля, под которым данный модуль будет обращаться к **Dr.Web Agent** для получения конфигурации;
- `--log-name <имя>` - имя, под которым модуль будет выводить сообщения в файл отчета;
- `--check-only` - компонент запускается в режиме проверки конфигурации. Для успешной проверки должен быть запущен **Dr.Web Agent**. Если при проверке не было найдено ошибок, выводится сообщение:

```
Options OK
```

Если были найдены ошибки, выводится их описание и сообщение:

```
Options ERROR
```

Пример:

```
$ drweb-nss -t 30 local:/var/drweb/ipc/.  
agent
```

Эта команда запускает **Dr.Web NSS** со временем ожидания конфигурационных данных 30 секунд и сокетом **Агента**, располагающимся по адресу `local:/var/drweb/ipc/.agent`.



Обрабатываемые сигналы

Все резидентные модули программного комплекса **Dr.Web для Novell Storage Services** поддерживают обработку следующих сигналов:

- **SIGHUP** – при получении этого сигнала модули перечитывают свои конфигурационные файлы. Если этот сигнал получает модуль **Dr.Web Monitor**, конфигурационные файлы перечитываются всеми управляемые им модулями.
- **SIGINT** и **SIGTERM** – при получении любого из этих сигналов модули завершают свою работу.

Модуль **Dr.Web NSS** поддерживает обработку дополнительных сигналов:

- **SIGUSR1** - при получении данного сигнала **Dr.Web NSS** сохраняет в директорию, указанную в значении параметра `BaseDir` секции `[General]` конфигурационного файла, файлы со статистикой по работе динамических потоков и постоянных соединений (подробнее см. внутренняя статистика работы).
- **SIGALRM** – при получении данного сигнала **Dr.Web NSS** отправляет всю собранную статистику модулю **Dr.Web Agent**.

Внутренняя статистика работы

Статистика по работе пулов потоков и постоянных соединений, связанных с данным пулом, накапливается только, если ее явно включить в настройках пула потока (параметр `CheckPoolOptions` секции `[NSS]` конфигурационного файла), установив дополнительный параметр `stat = yes`.



Пример:

`CheckPoolOptions = 2-20, stat = yes`

Имена файлов, формирующиеся по сигналу SIGUSR1, имеют шаблон:

- `name_(cli|srv)[.unique-id].txt` - для статистики по соединениям;
- `name_(thr[N])[.unique-id].txt` - для статистики по потокам.

где:

- `name` - имя модуля без части "drweb-".
- `cli` - для соединений клиентской части.
- `srv` - для соединений серверной части.
- `unique-id` - указывается для модулей, запущенных с уникальным идентификатором.
- `thr` - указывается для пула потоков.

Если такой файл уже существует, то статистика будет добавлена в конец файла.

Каждая запись начинается со строк:

```
=====
start: Tue Oct 9 14:44:15 2008
curr: Tue Oct 9 14:44:29 2008
period: 0d 0h 0m 14s
```

в которых указывается время старта сбора статистики, время сброса статистики в файл и временной период отчета.

Затем указывается число созданных по запросу соединений, число соединений, закрытых из-за истечения времени ожидания, среднее число соединений и их текущее количество:

```
closed: 0 (0 num/sec)
```



```
total created = 0 (0 num/sec)
max rea = 0 est = 0 don = 0 act = 0
```

Для `nss_thr.txt` вывод имеет вид:

```
min = 2 max = 2147483647 type = 0 freetime =
120
busy max = 0 avg = 0
requests for new threads = 0 (0 num/sec)
creating fails = 0
max processing time = 0 ms; avg = 0 ms
curr = 2 busy = 0
```

Здесь указывается:

- в первой строке - минимальное/максимальное число потоков в пуле, тип пула, время в секундах, в течение которого дополнительный поток будет в бездействии перед тем, как завершится;
- во второй строке - максимальное и среднее число занятых одновременно потоков;
- в третьей строке - число запросов на создание дополнительных потоков и частота таких запросов;
- в четвертой строке - число неудавшихся попыток создания потоков (скорее всего из-за нехватки ресурсов);
- в пятой строке - максимальное и среднее время обработки одного запроса в миллисекундах;
- в шестой и последней строке - текущее число потоков в пуле и какое их количество сейчас занято обработкой.

Статистика проверки файлов

В процессе работы комплекса может собираться статистика двух видов: общая статистика и статистика по обнаруженным угрозам. Общая статистика представляет из себя общую информацию о работе комплекса **Dr.Web для Novell Storage Services** за определенный период: число проверенных файлов,



их размер, число зараженных файлов, и т.д. Статистика по обнаруженным угрозам представляет из себя информацию о конкретных файлах, в которых было обнаружено что-либо нежелательное, например, вирус.

Общая статистика накапливается во внутреннем кэше и периодически (по умолчанию, раз в 5 минут) отправляется модулю **Dr.Web Agent**. Период времени для отправления статистики устанавливается в параметре `SendPeriod` секции `[Stat]` конфигурационного файла. Если **Dr.Web NSS** некорректно завершил свою работу, часть общей статистики за этот период будет потеряна.

Статистика по инфицированным файлам передается в **Dr.Web Agent** сразу при обнаружении файла.

Подключить или отключить сбор статистики можно в параметре `SendToAgent` секции `[Stat]` конфигурационного файла.

Карантин

Директория карантина используется для изоляции зараженных и подозрительных файлов. В карантин перемещаются все файлы, для которых определено действие `quarantine`. Директория карантина задается в параметре `Path` секции `[Quarantine]`.

При перемещении файла в карантин к концу его имени добавляются 6 случайных символов. Вместе основным файлом сохраняется дополнительный файл, в котором хранится служебная информация: оригинальный путь к основному файлу, права и т.п. Имя дополнительного файла формируется из нового имени основного файла с постфиксом `"-info"`. Для обоих файлов устанавливаются права доступа, указанные в значении параметра `FilesMode` секции `[Quarantine]`.

Пример:

`eicar.com` - исходное имя файла;



`eicar.comf8JRCG` - имя файла в карантине;

`eicar.comf8JRCG-info` - имя дополнительного файла в карантине.

Вместе с файлом в карантине можно сохранять и дополнительные свойства, которые поддерживает NSS, такие как квоты и NSS-атрибуты. Данные свойства будут автоматически устанавливаться заново при восстановлении файла из карантина

Чтобы было возможно сохранение этих свойств, необходимо включить поддержку расширенных атрибутов Linux (Linux extended attributes) в NSS. Для этого можно добавить в файл `/etc/opt/novell/nss/nssstart.cfg` следующие строки:

```
/ListXattrNWMetadata  
/CtimeIsMetadataModTime
```

Следует учесть, что поддержка расширенных атрибутов Linux в NFS реализована только начиная в Open Enterprise Server 2. Подробнее про использование расширенных атрибутов Linux можно прочитать в [документации Open Enterprise Server](#).

Управление через `drweb-nss-qcontrol`

Для управления карантинном и осуществления поиска файлов в нем предназначена специальная утилита `drweb-nss-qcontrol`. При запуске она подключается к **Dr.Web Agent** (если не был указан пустой параметр командной строки `--agent`, см. ниже) и получает от него конфигурационные параметры.

Утилита `drweb-nss-qcontrol` поддерживает следующие параметры командной строки:

- `-h [--help]` - вывод справки;
- `-v [--version]` - вывод версии программы;



- `-l [--level] <уровень>` - уровень подробности ведения файла отчета (все настройки файла отчета берутся из секции [Logging] конфигурационного файла, так же, как и для **Dr.Web NSS**);
- `-i [--ipc-level] <уровень>` - уровень подробности файла отчета библиотеки IPC;
- `--log-filename <имя файла>` - имя файла отчета;
- `--agent <адрес>` - адрес Агента, от которого будет получены конфигурационные параметры. Если значение параметра не задано, то запрос конфигурации от Агента не происходит, и используются параметры командной строки и значения по умолчанию;
- `--timeout <время>` - максимальное время ожидания получения конфигурационных параметров от **Агента** и ответа от **Демона**;
- `-show <выражение>` - показывает общую информацию по файлам, которые хранятся в карантине. В качестве значения указывается регулярное выражение, описывающее имена файлов, информацию по которым требуется получить. Информация выводится в следующем формате

```
ИМЯ:      original=[ ПУТЬ]      size=РАЗМЕР
put_time=ВРЕМЯ      viruses=[ ВИРУСЫ]
code=КОД mode=АТРИБУТЫ
```

где:

- ИМЯ - имя файла в карантине;
- ПУТЬ - абсолютный путь к оригинальному расположению файла;
- РАЗМЕР - размер файла в байтах;
- ВРЕМЯ - локальное время помещения файла в карантин;
- ВИРУСЫ - список всех обнаруженных в файле вирусов, вирусы перечисляются через запятую;
- КОД - шестнадцатеричный код возврата **Демона**;



- АТТРИБУТЫ - восьмеричные оригинальные атрибуты файла (будут установлены заново при восстановлении файла).

Сохраненные свойства NSS в данном выводе не показываются.

Пример вывода:

```
eicar.comf8JRCG: original=[ /media/nss/
VOLENC/eicar.com] size=105
\put_time=2010-Aug-26 14:08:10
viruses=[infected with EICAR Test
File\NOT a Virus!)] code=0x20
mode=0100666
```

- `--remove <выражение>` - удалить из директории карантина все файлы, имена которых соответствуют регулярному выражению, переданному в качестве параметра.

Пример:

```
drweb-nss-qcontrol --remove .
```

В результате карантин будет полностью очищен.



- `--restore <выражение>` - попытаться восстановить файлы, имена которых соответствуют регулярному выражению, переданному в качестве параметра. Файлы восстанавливаются в оригинальное местоположение, со всеми свойствами и атрибутами. Если указан параметр `--restore-dir` файл восстанавливается в директорию, указанную в этом параметре, свойства файла поддерживаемые только NSS будут восстановлены только если новая директория находится в NSS разделе. Если восстанавливаемый файл является зараженным, перед восстановлением необходимо указать его оригинальное местоположение в параметре конфигурационного файла `ExcludedPaths` (и убедиться, что оно не указано в параметре `IncludedPaths`), так как в противном случае **Dr.Web NSS** сразу же обнаружит его и может вернуть обратно в карантин. Если после обновления антивирусных баз файл, помещенный в карантин как подозрительный, перестал считаться инфицированным, для его восстановления необходимо использовать параметр командной строки `--rescan`. Если при восстановлении файла окажется, что по оригинальному пути уже находится некий файл, будет задан вопрос о необходимости заменить этот файл на файл из карантина.

Пример:

```
drweb-nss-qcontrol --restore eicar
```

Будет предпринята попытка восстановить все файлы, в имени которых содержится `eicar`, в исходное местоположение.

- `--restore-dir <директория>` - при выполнении действия `--restore` восстанавливать файлы в указанную директорию, а не в исходное местоположение. Если указанная директория находится не в NSS-разделе, свойства файла поддерживаемые только файловой системой NSS восстановлены не будут.

Пример:

```
drweb-nss-qcontrol --restore-dir  
sample/directory --restore eicar
```



Будет предпринята попытка восстановить все файлы в имени которых содержится `eicar`, в директорию `"sample/directory"`.

- `--answer <ответ>` - указывает автоматический ответ на вопрос о замене файла при выполнении действия `--restore`.

Пример:

```
drweb-nss-qcontrol --restore eicar.  
comf8JRCG --answer yes
```

Если в оригинальном местоположении восстанавливаемого файла уже имеется другой файл, он будет автоматически перезаписан.

- `--rescan <выражение>` - отправить файлы, имена которых соответствуют регулярному выражению, заново **Демону** на сканирование. Если при повторной проверке в файле не будет обнаружено вредоносных программ, для него автоматически выполняется действие `--restore` (восстановление файла).

С помощью этого параметра командной строки можно организовать автоматическое периодическое восстановление чистых файлов из карантина, добавив в `crontab` подобную строку(повторно сканировать файлы в карантине каждые 30 минут, не перезаписывать файлы при восстановлении):

```
*/30 * * * * sh -c "/opt/drweb/drweb-  
nss-qcontrol --rescan . --answer no"
```

Файл отчета

Dr.Web для Novell Storage Services может осуществлять протоколирование своей работы с помощью демона `syslog` или в отдельный файл отчета. В случае использования `syslog`, в системный файл отчета записываются строки следующего формата:

```
'['tid']' name[.sub] level text
```

где:



- `tid` - идентификатор потока, осуществляющего запись в отчет;
- `name` - название модуля, осуществляющего запись в отчет;
- `sub` - название службы модуля, осуществляющего запись в отчет.
К самым важным службам относятся следующие:
 - `ipc` - служба межпроцессного взаимодействия;
 - `thrN` - служба поддержки пула потоков с номером N.
- `level` - уровень подробности. Возможны следующие значения: `FATAL`, `ERROR`, `WARN`, `INFO`, `DEBUG`;
- `text` - текст сообщения, записываемого в отчет.

По умолчанию при запуске модуля устанавливается уровень подробности протоколирования `INFO`. После получения конфигурационной информации от **Агента**, будет установлен уровень, определенный в конфигурации.

Если необходимо сразу установить уровень `DEBUG` (например, чтобы в файл отчета были выведена информация о загруженных через агента параметрах), воспользуйтесь параметром командной строки `--level`. Обратите внимание, что после загрузки конфигурационной информации от **Агента**, уровень подробности будет установлен в соответствии с конфигурацией **Агента**.

Проверка конфигурации

Вы можете проверить корректность изменений, произведенных в конфигурационных файлах, или параметров, получаемых модулями от **Агента**. Для этого каждый модуль поддерживает параметр командной строки `--check-only`. Этот параметр может использоваться только при запущенном **Агенте**, который используется для получения конфигурационных параметров.

Если проверка прошла успешно, на консоль выводится сообщение:



Options OK

Если обнаружены ошибки, выводится их описание и сообщение:

Options ERROR

Dr.Web Monitor также поддерживает параметр `--check-all` для проверки конфигурации **Монитора** и всех управляемых им модулей.

Конфигурационный файл

Настройки **Dr.Web NSS** задаются отдельным конфигурационным файлом `/etc/drweb/drweb-nss.conf`. Формат конфигурационного файла и краткое описание возможных значений параметров даны разделе [Конфигурационные файлы](#).

Секция [General]

В секции [General] собраны общие настройки работы **Dr. Web NSS**:

Параметр	Описание	Значение по умолчанию
Секция [General]		
BaseDir = { путь к директории }	Основная рабочая директория, в которой содержатся сокет, база данных и другие файлы. В текущей версии этот параметр не может быть изменен при перезапуске по сигналу SIGHUP.	BaseDir = / var/drweb



Параметр	Описание	Значение по умолчанию
<code>MaxTimeoutForThreadActivity = { время}</code>	Максимальное время закрытия одного потока. Параметр используется при перезапуске, а также при завершении работы. Общее максимальное время завершения работы рассчитывается следующим образом: количество пулов умножается на значение параметра MaxTimeoutForThreadActivity и к результату прибавляется некоторая временная константа.	<code>MaxTimeoutForThreadActivity = 2m</code>
<code>IpcTimeout = { время}</code>	Максимальное время установки соединения между компонентами.	<code>IpcTimeout = 2m</code>

Секция [Logging]

В секции [Logging] собраны параметры, управляющие ведением протоколов работы основных модулей программного комплекса **Dr.Web для Novell Storage Services**:

Параметр	Описание	Значение по умолчанию
Секция [Logging]		
<code>Level = { Quiet Error Alert Info Debug}</code>	Определяет уровень подробности работы.	<code>Level = Info</code>
<code>IpcLevel = { Quiet Error Alert Info Debug}</code>	Уровень подробности протокола работы библиотеки IPC.	<code>IpcLevel = Alert</code>



Параметр	Описание	Значение по умолчанию
<code>SyslogFacility = {Daemon Mail Local0.. Local7}</code>	Тип подсистемы, через которую системный сервис <code>syslogd</code> , ведущий протоколирование работы Dr.Web для Novell Storage Services и его подсистем, выдает сообщения о событиях (более подробную информацию вы можете получить в документации по <code>syslogd</code>).	<code>SyslogFacility = Daemon</code>
<code>FileName = {syslog путь к файлу}</code>	Путь к файлу отчета или " <code>syslog</code> ", если отчет о работе ведется с помощью системной службы <code>syslogd</code> .	<code>FileName = syslog</code>

Секция [NSS]

В секции [NSS] содержатся общие настройки проверки файлов и взаимодействия с файловой системой NSS.

Параметр	Описание	Значение по умолчанию
Секция [NSS]		
<code>NSSVolumesMountDir = {директория}</code>	Путь к директории, в которой смонтированы все разделы NSS. Список защищаемых разделов указывается в значении параметра <code>ProtectedVolumes</code> .	<code>NSSVolumesMountDir = /media/nss</code>
<code>ProtectedVolumes = {список разделов}</code>	Список защищаемых разделов. Значения разделены запятыми.	<code>ProtectedVolumes =</code>



Параметр	Описание	Значение по умолчанию
	Если список пустой, то будут защищаться все каталоги в директории, указанной в параметре NSSVolumesMountDir . Если в этой директории не все каталоги являются разделами NSS, произойдет ошибка при инициализации.	
CheckPoolOptions = {настройки пула}	Настройки пула потоков для обработки заданий на проверку.	CheckPoolOptions = {2-20}
HeuristicAnalysis = {yes no}	Включение/выключение эвристического анализатора. Эвристический анализатор позволяет Демону Dr.Web обнаруживать неизвестные вирусы, не включенные в вирусные базы данных. Поскольку эвристический анализ носит вероятностный характер, а работа некоторых программ может быть похожа на вирусную активность, обнаруженные таким образом файлы считаются подозрительными. Рекомендуется помещать такие файлы в карантин, до выхода новых версий баз, позволяющих однозначно определить, являются ли они угрозами. Вы можете прислать такие файлы в компанию "Доктор Веб" на анализ через сайт http://vms.drweb.com/sendvirus .	HeuristicAnalysis = yes



Параметр	Описание	Значение по умолчанию
	Использование эвристического анализатора может привести к увеличению времени сканирования.	
<code>MaxFileSizeToScan = {Size}</code>	Максимальный размер файла для проверки. Если размер файла превышает указанный, файл не будет отправляться Демону Dr.Web на сканирование. Если установлено значение <code>0</code> , размер файла не проверяется.	<code>MaxFileSizeToScan = 0b</code>
<code>IncludedPaths = {список путей}</code>	<p>Список относительных путей, которые всегда требуется проверять. Все пути, которые начинаются со значений, указанных в данном параметре, будут проверяться на вирусы, вне зависимости от параметра ExcludedPaths.</p> <p>Пути указываются относительно директории, указанной в параметре NSSVolumesMountDir: сначала указывается раздел, а затем его поддиректории и файлы.</p> <p>Пути должны указываться в нормализованном виде (т.е. без использования символов текущей и вышестоящей директории: "." и "..").</p>	<code>IncludedPaths =</code>



Параметр	Описание	Значение по умолчанию
<code>ExcludedPaths</code> = { список путей}	<p>Список относительных путей, которые не требуется проверять. Все пути, которые начинаются со значений, указанных в данном параметре, не будут проверяться на вирусы, если они не указаны в параметре ExcludedPaths.</p> <p>Пути указываются относительно директории, указанной в параметре NSSVolumesMountDir: сначала указывается раздел а затем его поддиректории и файлы.</p> <p>Пути должны указываться в нормализованном виде (т.е. без использования символов текущей и вышестоящей директории: "." и "..").</p>	<code>ExcludedPaths =</code>

Секция [DaemonCommunication]

В секции [DaemonCommunication] находятся параметры, управляющие взаимодействием **Dr.Web NSS** с **Демоном Dr.Web**:

Параметр	Описание	Значение по умолчанию
Секция [DaemonCommunication]		
<code>Address</code> = { АДРЕС1 [ВЕС1], АДРЕС2 [ВЕС2] ..}	Сокет, через который Dr.Web NSS взаимодействует с Демоном Dr.Web .	<code>Address =</code> <code>pid: /var/</code> <code>drweb/run/</code> <code>drwebd.pid</code> <code>1</code>



Параметр	Описание	Значение по умолчанию
	<p>Адреса задаются в виде ADDRESS [WEIGHT], где ADDRESS - адрес в стандартном формате (UNIX или TCP сокет), а WEIGHT - необязательный вес этого адреса.</p> <p>Вес определяет относительную нагрузку на данный узел сети и может принимать значения от 0 до 100 включительно. В первую очередь файлы для проверки будут передаваться на адреса с большим весом.</p> <p>Если для адресов указан одинаковый вес, они считаются полностью равноправными и получают одинаковый объем запросов. Если указан вес, равный 0, адреса с этим весом считаются резервными адресами и файлы для проверки передаются на них только если не удалось передать их ни на один адрес с весом, большим 1.</p> <p>Выбор веса следует осуществлять на основе имеющихся ресурсов на каждом из узлов.</p> <p>Среди указанных адресов должен присутствовать хотя бы один корректный адрес сервера.</p> <p>Примеры:</p> <p>Указывается путь к PID файлу:</p> <pre>Address = pid: /var/drweb/run/drwebd.pid</pre>	



Параметр	Описание	Значение по умолчанию
	Указываем несколько адресов с весами: <code>Address = pid: /var/ drweb/run/drwebd.pid 10, \inet: 3000@srv2. example.com 5</code>	
Timeout = { время}	Максимальное время ожидания исполнения команды Демоном Dr.Web . Если значение параметра равно 0, время ожидания не ограничено.	Timeout = 2m

Секция [Actions]

В секции [Actions] вы можете задать действия, применяемые к файлам, в которых были обнаружены угрозы.

Возможные действия:

- pass - пропустить файл;
- cure - попытаться вылечить зараженный файл, если лечение невозможно выполняется действие, указанное в параметре Incurable;
- report - только отправить сообщение (см. [секцию \[Notifications\]](#));
- quarantine - поместить файл в директорию карантина;
- remove - удалить файл.

Информация о всех действиях выводится в файл отчета. Для всех действий, кроме pass, отправляются сообщения, заданные в [секции \[Notifications\]](#).

Параметр	Описание	Значение по умолчанию
Секция [Actions]		



Параметр	Описание	Значение по умолчанию
<code>Infected = {remove quarantine cure}</code>	Файл заражен известным вирусом.	<code>Infected = cure</code>
<code>Suspicious = {remove quarantine pass report}</code>	Возможно, файл заражен неизвестным вирусом.	<code>Suspicious = quarantine</code>
<code>Incurable = {remove quarantine}</code>	Файл заражен и не может быть вылечен (имеет смысл, только если InfectedFiles = Cure).	<code>Incurable = quarantine</code>
<code>Adware = {remove quarantine pass report}</code>	Файл содержит программу для показа рекламы (adware).	<code>Adware = quarantine</code>
<code>Dialers = {remove quarantine pass report}</code>	Файл содержит программу автоматического дозвона.	<code>Dialers = quarantine</code>
<code>Jokes = {remove quarantine pass report}</code>	Файл содержит программу-шутку, которая может пугать или раздражать пользователя.	<code>Jokes = report</code>
<code>Riskware = {remove quarantine pass report}</code>	Файл содержит потенциально опасную программу, которая может быть использована не только ее владельцем, но и злоумышленниками.	<code>Riskware = report</code>
<code>ArchiveRestriction = {remove quarantine pass report}</code>	Действие, совершаемое с архивами, которые не были проверены Демоном Dr.Web из-за ограничений, заданных для архивов в главном конфигурационном файле drweb32.ini .	<code>ArchiveRestriction = quarantine</code>



Параметр	Описание	Значение по умолчанию
<code>Hacktools = {remove quarantine pass report}</code>	Файл содержит программу, предназначенную для получения несанкционированного доступа к компьютерным системам.	<code>Hacktools = report</code>
<code>SkipObject = {remove quarantine pass report}</code>	Действие, совершаемое с файлами, которые не могут быть проверены Демоном Dr.Web .	<code>SkipObject = report</code>
<code>DaemonError = {remove quarantine pass report}</code>	Действие, применяемое к файлам, при сканировании которых у Демона Dr.Web возникли ошибки.	<code>DaemonError = quarantine</code>
<code>LicenseError = {remove quarantine pass report}</code>	Действие, применяемое к файлам, которые не были проверены Демоном Dr.Web по причине лицензионных ограничений.	<code>LicenseError = report</code>
<code>ProcessingError = {remove quarantine pass report}</code>	Действия применяемые к файлам, при обработке которых у Dr.Web NSS возникли ошибки.	<code>ProcessingError = report</code>

Секция [Stat]

В секции [Stat] собраны параметры сбора статистики работы **Dr.Web для Novell Storage Services**:

Параметр	Описание	Значение по умолчанию
	Секция [Stat]	



Параметр	Описание	Значение по умолчанию
SendToAgent = {yes no}	Включение/выключение отправления Агенту Dr.Web статистической информации о работе Dr.Web NSS . Если установлено значение no , сбор статистики не производится.	SendToAgent = yes
SendPeriod = { время }	Промежуток времени, через который общая статистика посылается Агенту Dr.Web .	SendPeriod = 5m

Секция [Quarantine]

В секции [Quarantine] собраны настройки работы **Карантина**.

Параметр	Описание	Значение по умолчанию
Секция [Quarantine]		
Path = { путь к директории }	Путь к директории карантина. У Dr.Web NSS должны быть права на создание, изменение, удаление и чтение файлов в этом каталоге.	Path = /var/drweb/infected/nss
FilesMode = { числовое значение }	Права доступа, устанавливаемые для файлов, которые перемещаются в карантин.	FilesMode = 0660

Секция [Notifications]

В секции [Notifications] собраны содержатся настройки уведомлений, отправляемых при различных событиях.



Параметр	Описание	Значение по умолчанию
Секция [Notifications]		
ExternalProgram = {String}	<p>Команда для запуска внешней программы, после выполнения действия над файлом (remove, quarantine, cure, report). После выполнения команды событие записывается в файл отчета.</p> <p>Поток, выполняющий команду, ждет ее завершения, и, если код возврата отличен от 0, вносит соответствующую запись в файл отчета.</p> <p>В команде для запуска программы можно указывать дополнительные макросы:</p> <ul style="list-style-type: none">• \$HOSTMASTER\$ - значение параметра Hostmaster;• \$REASON\$ - название события, приведшего к выполнению команды;• \$ACTION\$ - название действия, которое было применено в результате возникновения события;• \$VERSION\$ - текущая версия продукта;• \$FILES\$ - полный путь к файлу, при обработке которого возникло событие;• \$SIZE\$ - размер (в байтах) файла, приведшего к возникновению события;	ExternalProgram =



Параметр	Описание	Значение по умолчанию
	<ul style="list-style-type: none">• \$TIMES\$ - локальное время на сервере в момент, когда была выполнена эта команда;• \$DAEMON_REPORT\$ - отчет Демона Dr.Web, полученный в результате обработки файла, вызвавшего событие. Может быть пустым. Строки отчета разделены символом перевода строки;• \$VIRUSES\$ - список вирусов, найденных в результате обработки файла, вызвавшего событие. Может быть пустым. Вирусы в списке перечислены через запятую. <p>Пример (ввод должен быть осуществлен в одну строку):</p> <pre>"kdialog -- passivepopup \"<html>< font color=\"red\" size=\"5\">Attention, \$REASON\$ event is occured! </ font>
File \$FILE\$ (size=\$SIZE\$) </ font>
 action=\$ACTION\$
</ html>\" 10"</pre>	



Параметр	Описание	Значение по умолчанию
	<p>В системе KDE при каждом событии (обнаружение угрозы, ошибка сканирования и т.п.) будет выводиться всплывающее окно с описанием события.</p>	
<code>SendMail = {yes no}</code>	<p>Включение/выключение отправки почтовых уведомлений после выполнения действий <code>remove</code>, <code>quarantine</code>, <code>cure</code> и <code>report</code>. Команда отправки уведомления выполняется после выполнения действия над файлом, но до записи этого события в файл отчета.</p> <p>Письмо с уведомлением отправляется по адресу, указанному в значении параметра Hostmaster данной секции. Шаблоны для писем берутся из директории, указанной в значении параметра Templates.</p>	<code>SendMail = no</code>
<code>Templates = {путь_к_директории}</code>	<p>Путь к директории, содержащей шаблоны уведомлений.</p> <p>В данный момент там должен содержаться только шаблон email.templ. В этом шаблоне могут быть использованы макросы, список которых перечислен в описании параметра ExternalProgram.</p>	<code>Templates = /etc/drweb/templates/nss</code>
<code>Hostmaster = {EmailAddress}</code>	<p>Электронный адрес, на который отправляются уведомления.</p>	<code>Hostmaster = root@localhost</code>



Параметр	Описание	Значение по умолчанию
MailCommand = { строка}	Команда, выполняемая для отправления администратору уведомлений о происходящих событиях.	MailCommand = "/usr/ sbin/ sendmail -i -bm -f drweb-nss -- %s"



Модуль обновления Dr.Web Updater

Для автоматизации получения и установки обновлений вирусных баз "**Доктор Веб**" используется модуль обновления **Dr.Web Updater**. Модуль обновления представляет собой написанный на Perl скрипт `update.pl` и находится в директории, содержащей исполняемые файлы программного комплекса **Dr.Web для Novell Storage Services**.

Настройки модуля обновления хранятся в секции `[Updater]` главного конфигурационного файла (`drweb32.ini` по умолчанию), который находится в директории `%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске скрипта обновления.

Для запуска скрипта обновления используйте команду:

```
$ %bin_dir/update.pl [параметры]
```

Обновление антивируса и вирусных баз

Компоненты программного комплекса **Dr.Web для Novell Storage Services** нуждаются в регулярном обновлении баз данных вирусов.

Вирусные базы **Dr.Web для Novell Storage Services** состоят из нескольких файлов с расширением `vdb`. На серверах обновлений эти файлы могут храниться также в `lzma`-архивах. При появлении новых вирусов выпускаются небольшие, размером в один или несколько килобайт, файлы (дополнения), которые содержат фрагменты баз, описывающие эти вирусы.

Дополнения являются едиными для всех поддерживаемых



платформ и делятся на два вида:

- ежедневные "горячие" обновления (`drwtoday.vdb`);
- еженедельные регулярные обновления (`drwXXXXYY.vdb`), где `XXX` – номер версии антивируса, а `YY` – порядковый номер обновления, начиная с номера `00` (например, файл первого регулярного обновления для версии `6.0.1` именуется `drw60100.vdb`).

"Горячие" обновления выпускаются ежедневно или несколько раз в день для оперативной реакции на новые вирусные угрозы. Особенность установки "горячих" дополнений связана с тем, что в промежутке между выходом регулярных (нумерованных) дополнений файл `drwtoday.vdb` пополняется новыми записями, т.е. его необходимо устанавливать вместо имевшегося ранее. В момент выхода очередного регулярного дополнения все записи из этого файла переписываются в регулярное дополнение, а сам он очищается (выпускается файл `drwtoday.vdb`, не содержащий ни одной записи базы данных).

Следовательно, при обновлении баз вручную необходимо устанавливать все отсутствующие у пользователя регулярные дополнения, после чего переписывать файл "горячего" дополнения вместо имевшегося ранее.

Чтобы подключить дополнение к основным вирусным базам, соответствующий файл должен быть помещен в директорию программного комплекса **Dr.Web для Novell Storage Services** (по умолчанию в `%var_dir/bases/`) или иную директорию, определенную в конфигурационном файле.

Сигнатуры, позволяющие обнаруживать и предотвращать распространение вирусоподобных вредоносных программ (рекламных, программ дозвона, программ взлома и т.п.), поставляются в виде двух отдельных вирусных баз с аналогичной структурой - `drwrisky.vdb` и `drwnasty.vdb`. К этим базам также поставляются регулярные обновления `dwrXXXXY.vdb` и `dwnXXXXY.vdb`, а также "горячие" обновления `dwrtday.vdb` и `dwnoday.vdb`.



Периодически (в частности, в связи с появлением радикально новых вирусных и антивирусных технологий) выпускаются новые версии пакета с обновленными алгоритмами, заложенными в антивирусное ядро. Одновременно с этим сводятся воедино все ранее выпущенные дополнения баз, и новая версия пакета комплектуется новейшими вирусными базами, содержащими описание всех известных на момент ее выхода вирусов. Как правило, при переходе на новую версию пакета сохраняется преемственность формата баз, т.е. новые вирусные базы могут быть подключены к старому антивирусному ядру. Однако при этом не гарантируется обнаружение или излечение новых вирусов, для борьбы с которыми потребовались обновленные алгоритмы антивирусного ядра.

При регулярном получении дополнений вирусные базы пакета приобретает следующую структуру:

- `drwebase.vdb` – основная база, получаемая вместе с новой версией пакета;
- `drwXXXXYY.vdb` – еженедельные регулярные дополнения вирусных баз;
- `drwtoday.vdb` – "горячие" дополнения;
- `drwnasty.vdb` – основная база вредоносных программ, получаемая вместе с новой версией пакета;
- `dwnXXXXYY.vdb` – еженедельные регулярные дополнения базы вредоносных программ;
- `dwntoday.vdb` – "горячие" дополнения базы вредоносных программ;
- `drwrisky.vdb` – основная база потенциально опасных программ, получаемая вместе с новой версией пакета;
- `dwrXXXXYY.vdb` – еженедельные регулярные дополнения базы потенциально опасных программ;
- `dwrtoday.vdb` – "горячие" дополнения базы потенциально опасных программ.

Вирусные базы могут быть автоматически обновлены, используя модуль обновления компонентов **Dr.Web Updater** (`/opt/drweb/update.pl`). После установки создаётся файл `/etc/cron.d/drweb-update` для запуска **Dr.Web Updater**



каждые 30 минут. Это обеспечивает регулярное обновление и наилучшую защиту. Вы можете исправить файл для изменения периода обновления.

Настройка cron

При установке компонентов программного комплекса в `/etc/cron.d/` будет создан пользовательский файл для настройки взаимодействия cron с **Dr.Web Updater**.



В создаваемом задании для `crond` используется наиболее распространённый синтаксис `viXie` cron. Если в вашей системе используется другой демон cron, например `dcron`, необходимо вручную создать задание для автоматического запуска модуля обновления **Dr.Web Updater**.

При значениях по умолчанию демон `cron` запускает модуль **Dr. Web Updater** в 0 и 30 минут каждого часа. Это может вызывать повышенную нагрузку на сервера обновления компании **"Доктор Веб"** и приводить к задержке обновления. Чтобы избежать подобной ситуации, рекомендуется изменять значения по умолчанию на произвольные.

Параметры командной строки

Параметр `--help` используется для вывода краткой справки о ключах программы.

Для использования другого конфигурационного файла, полный путь к нему необходимо указать параметром командной строки `--ini`. Если имя конфигурационного файла не задано, используется `%etc_dir/drweb32.ini`.

**Пример:**

```
$ /opt/drweb/update.pl --ini=/path/to/conf_file
```

Параметр командной строки `--what` позволяет временно переопределить значение параметра **Section** при запуске модуля обновления. Значение параметра будет действовать до следующего запуска скрипта. Возможные значения: `scanner` или `daemon`.

Пример:

```
$ /opt/drweb/update.pl --what=Scanner
```

Чтобы просмотреть список всех компонентов продукта, доступных для обновления, нужно указать параметр `--components`.

Пример:

```
$ /opt/drweb/update.pl --components
```

В качестве параметра командной строки также может быть указан `--not-need-reload`. Возможны три варианта его использования:

- Если данный параметр не задан, то по завершении работы модуля обновления `update.pl` будут перезагружаться все демоны (**Dr.Web Daemon** для программного комплекса **Dr.Web для Novell Storage Services**), для которых в процессе обновления был изменен/удален/добавлен хотя бы один компонент;
- Если указать параметр `--not-need-reload`, не задав значения, то по завершении работы модуля обновления `update.pl` ни один из демонов перезагружаться не будет;
- Если при задании параметра `--not-need-reload` в качестве его значения были указаны названия демонов (через запятую, без пробелов, регистр не важен), то соответствующие демоны перезагружаться не будут, а все остальные — будут при наличии обновлений.

Пример:



```
$ /opt/drweb/update.pl --not-need-reload=drwebd
```

Блокирование обновлений для компонентов

Вы можете заблокировать обновления для определенных компонентов **Dr.Web для Novell Storage Services**.

Чтобы получить список доступных компонентов запустите **Dr. Web Updater** с параметром командной строки `--components`.

Пример:

```
# ./update.pl --components
```

```
Available Components:
```

```
agent
drweb          (frozen)
icapd          (frozen)
vaderetro_lib
```

Если обновления для компонента заблокированы, такой компонент будет отмечен как замороженный (frozen). Замороженные компоненты не будут обновляться при запуске **Dr.Web Updater**.

Блокирование обновлений

Чтобы заблокировать обновления для определенных компонентов, запустите **Dr.Web Updater** с параметром командной строки `--freeze=<components>`, где `<components>` - это список имен компонентов, разделенных запятыми.

Пример:

```
# ./update.pl --freeze=drweb
Updates for component 'drweb' are frozen.
Run command './updater --unfreeze=drweb' to
```



start updates again.

Разблокирование обновлений

Чтобы вновь разрешить обновления для замороженных компонентов, запустите **Dr.Web Updater** с параметром командной строки `--unfreeze=<components>`, где `<components>` - это список имен компонентов, разделенных запятыми.

Пример:

```
# ./update.pl --unfreeze=drweb
Updates for component 'drweb' are no longer
frozen.
```



Размораживание компонента само по себе не приведет к его обновлению.

Восстановление компонентов

При обновлении компонентов **Dr.Web для Novell Storage Services, Dr.Web Updater** сохраняет в рабочей директории их резервные копии. Это позволяет вам вернуть компонент к предыдущему состоянию в случае каких-либо проблем с обновлением.

Чтобы восстановить компонент к предыдущему состоянию, запустите **Updater** с параметром командной строки `--restore=<components>`, где `<components>` - это список имен компонентов, разделенных запятыми.

Пример:

```
# ./update.pl --restore=drweb
Restoring backup for component 'drweb'...
Updates for component 'drweb' are frozen.
Run command './updater --unfreeze=drweb' to
```



```
start updates again.
```

```
Backup for component 'drweb' has been restored!  
Dr.Web (R) restore details:
```

```
Following files has been restored:
```

```
    /var/drweb/bases/drwtoday.vdb  
    /var/drweb/bases/dwntoday.vdb  
    /var/drweb/bases/dwrtoday.vdb  
    /var/drweb/bases/timestamp  
    /var/drweb/updates/timestamp
```



При восстановлении компонент будет автоматически заморожен. Чтобы возобновить обновления для восстановленного компонента, его необходимо разморозить.

Настройки

Настройки модуля обновления компонентов **Dr.Web Updater** хранятся в секции Updater конфигурационного файла программы (по умолчанию drweb32.ini), который размещается в директории %etc_dir. Устройство конфигурационного файла и краткое описание его параметров приведены в разделе [Конфигурационные файлы](#).

Секция [Updater]

```
UpdatePluginsOnly =  
{ Yes | No }
```

Значение Yes предписывает модулю не производить обновление **Демона** и **Сканера**, а ограничиться только обновлением плагинов.

Значение по умолчанию:

```
UpdatePluginsOnly = No
```



<pre>Section = { Daemon Scanner}</pre>	<p>Указывает, из какой секции конфигурационного файла Dr.Web Updater берёт настройки, такие как путь к ключевому файлу, путь к вирусным базам и т.п. Возможные значения параметра: <code>Scanner</code> или <code>Daemon</code>.</p> <p>Значение параметра возможно временно переопределить при запуске модуля обновления с помощью параметра командной строки <code>--what</code>. Измененное таким образом значение параметра будет действовать до следующего запуска скрипта.</p> <p><u>Значение по умолчанию:</u></p> <pre>Section = Daemon</pre>
<pre>ProgramPath = { путь к файлу}</pre>	<p>Путь к исполняемому файлу компонента, который будет обновляться. Требуется модулю обновления для получения информации о версии компонента.</p> <p><u>Значение по умолчанию:</u></p> <pre>ProgramPath = %bin_dir/drwebd</pre>
<pre>SignedReader = { путь к файлу}</pre>	<p>Путь к файлу программы чтения подписанных файлов.</p> <p><u>Значение по умолчанию:</u></p> <pre>SignedReader = %bin_dir/ read_signed</pre>
<pre>LzmaDecoderPath = { путь к файлу}</pre>	<p>Путь к файлу программы для распаковывания <code>Lzma</code>-архивов.</p> <p><u>Значение по умолчанию:</u></p> <pre>LzmaDecoderPath = %bin_dir/</pre>



LockFile = { путь к файлу}	<p>Путь к файлу, предназначенному для предотвращения совместного использования некоторых файлов на время их обработки модулем обновления.</p> <p><u>Значение по умолчанию:</u></p> LockFile = %var_dir/run/update.lock
CronSummary = { Yes No}	<p>Значение Yes предписывает модулю обновления выдавать отчет сессии обновления на стандартный вывод (stdout). Данный режим используется для отправки уведомлений администратору по электронной почте при запуске модуля обновления демоном cron.</p> <p><u>Значение по умолчанию:</u></p> CronSummary = Yes
DrlFile = { путь к файлу}	<p>Путь к специальному файлу, содержащему список серверов обновления. Модуль обновления выбирает сервера обновления из этого списка случайным образом. Данный файл подписан Доктор Веб, не подлежит редактированию пользователем и обновляется автоматически.</p> <p><u>Значение по умолчанию:</u></p> DrlFile = %var_dir/bases/update.drl
CustomDrlFile = { путь к файлу}	<p>Путь к альтернативному файлу, содержащему список серверов обновления. Модуль обновления выбирает сервера обновления из этого списка случайным образом.</p>



	<p>Данный файл подписан компанией Доктор Веб, не подлежит редактированию пользователем и обновляется автоматически.</p> <p><u>Значение по умолчанию:</u></p> <pre>CustomDrlFile = %var_dir/ bases/custom.drl</pre>
<pre>FallbackToDrl = { Yes No}</pre>	<p>Определяет поведение модуля обновления в случае, когда заданы значения обоих параметров DrlFile и CustomDrlFile одновременно. При указании значения Yes модуль обновления сперва попытается использовать путь из значения параметра CustomDrlFile, а в случае неудачи использует путь из значения DrlFile.</p> <p><u>Значение по умолчанию:</u></p> <pre>FallbackToDrl = Yes</pre>
<pre>DrlDir = { путь к директории}</pre>	<p>Путь к директории, содержащей подписанные Доктор Веб drl-файлы со списками серверов обновления для каждого из плагинов.</p> <p><u>Значение по умолчанию:</u></p> <pre>DrlDir = %var_dir/drl/</pre>
<pre>Timeout = { время в секундах}</pre>	<p>Максимальное время ожидания для загрузки обновлений.</p> <p><u>Значение по умолчанию:</u></p> <pre>Timeout = 90</pre>
<pre>Tries = { числовое значение}</pre>	<p>Количество попыток установки соединения модулем обновления.</p> <p><u>Значение по умолчанию:</u></p> <pre>Tries = 3</pre>



ProxyServer = { имя или IP-адрес прокси-сервера}	Имя или IP-адрес используемого прокси-сервера. <u>Значение по умолчанию:</u> ProxyServer =
ProxyLogin = { имя пользователя прокси-сервера}	Имя пользователя прокси-сервера. <u>Значение по умолчанию:</u> ProxyLogin =
ProxyPassword = { пароль пользователя прокси-сервера}	Пароль пользователя прокси-сервера. <u>Значение по умолчанию:</u> ProxyPassword =
LogFileName = { имя файла}	Имя файла отчета. В качестве имени можно указать значение <code>syslog</code> , тогда отчет будет вестись средствами системного сервиса <code>syslogd</code> . При использовании <code>syslog</code> нужно обратить внимание на параметры SyslogFacility и SyslogPriority (см. ниже). Поскольку <code>syslogd</code> имеет несколько файлов для протоколирования разных событий и разных степеней их важности, то, основываясь на этих двух параметрах и содержимом конфигурационного файла <code>syslogd</code> (обычно <code>/etc/syslogd.conf</code>), можно определить, куда будет записываться отчет программы. <u>Значение по умолчанию:</u> LogFileName = <code>syslog</code>
SyslogFacility = { Daemon Local0 .. Local7 Kern User Mail}	Тип записи при использовании системного сервиса <code>syslogd</code> . <u>Значение по умолчанию:</u> SyslogFacility = <code>Daemon</code>



<code>LogLevel = { Debug Verbose Info Warning Error Quiet}</code>	Уровень подробности ведения файла отчета <u>Значение по умолчанию:</u> <code>LogLevel = Info</code>
<code>LotusdPidFile = { путь к файлу}</code>	Путь к PID-файлу для демона Lotus . <u>Значение по умолчанию:</u> <code>LotusdPidFile = %var_dir/run/ drweblotusd.pid</code>
<code>MaildPidFile = { путь к файлу}</code>	Путь к PID-файлу для drweb-maild. <u>Значение по умолчанию:</u> <code>MaildPidFile = %var_dir/run/ drweb-maild.pid</code>
<code>IcapdPidFile = { путь к файлу}</code>	Путь к PID-файлу для drweb-icapd. <u>Значение по умолчанию:</u> <code>IcapdPidFile = %var_dir/run/ drweb_icapd.pid</code>
<code>BlacklistPath = { путь к директории}</code>	Путь к директории с dws файлами. <u>Значение по умолчанию:</u> <code>BlacklistPath = %var_dir/dws</code>
<code>AgentConfPath = { путь к файлу}</code>	Путь к конфигурационному файлу Агента . <u>Значение по умолчанию:</u> <code>AgentConfPath = %var_dir/ agent.conf</code>
<code>PathToVadeRetro = { путь к файлу}</code>	Путь к библиотеке libvaderetro.so. <u>Значение по умолчанию:</u> <code>PathToVadeRetro = %var_dir/ lib/libvaderetro.so</code>



<code>ExpiredTimeLimit = { number }</code>	<p>Количество дней до истечения срока действия лицензии, в течение которых Dr.Web Updater будет пытаться обновить лицензионный ключевой файл.</p> <p><u>Значение по умолчанию:</u></p> <code>ExpiredTimeLimit = 14</code>
<code>ESLockfile = { путь к файлу }</code>	<p>Путь к блокирующему файлу. Если данный файл существует, Dr.Web Updater перестает использовать расписания <code>crontab</code> для обновления.</p> <p><u>Значение по умолчанию:</u></p> <code>ESLockfile = %var_dir/run/es_updater.lock</code>

Процедура обновления

Обновление происходит следующим образом:

1. Модуль обновления читает конфигурационный файл.
2. Из конфигурационного файла используются параметры, находящиеся в секции [Updater] (описание параметров см. выше), а также параметры **EnginePath**, **VirusBase**, **UpdatePath** и **PidFile**.
3. Модуль запрашивает с сервера список обновлений, затем lzma-архивы соответствующих баз. В случае отсутствия последних базы скачиваются в виде vdb-файлов. Для распаковывания lzma-архивов используется утилита lzma, путь к которой задается значением параметра **LzmaDecoderPath** в секции [Updater] .
4. Обновления раскладываются по директориям, как описано в разделе [Обновление антивируса и вирусных баз](#).



Dr.Web Control Agent

Компонент **Dr.Web Control Agent** (далее **Агент**) представлен модулем `drweb-agent`. Это постоянно загруженный модуль, который управляет настройками модулей программного комплекса **Dr.Web для Novell Storage Services**, определяет политику работы комплекса в зависимости от установленной лицензии и собирает антивирусную статистику.

В ходе работы **Агент** может взаимодействовать с другими модулями программного комплекса, обмениваясь с ними различными управляющими сигналами.

Поскольку все компоненты **Dr.Web для Novell Storage Services** (кроме **Монитора**) получают свои конфигурационные данные через модуль `drweb-agent`, он должен запускаться перед другими компонентами, непосредственно после Монитора.

Пожалуйста, обратите внимание, что если в конфигурационном файле компонента указано несколько параметров с одним именем, то **Агент** их объединяет через запятую.



При задании значений параметров и правил в конфигурационных файлах можно использовать обратный слэш "\". В этом случае **Агент** объединит в одну строку все строки, разделённые с помощью обратного слэша. Использование пробела после слэша не допускается.

Режимы работы

При необходимости продукты компании "**Доктор Веб**" могут быть подключены к корпоративной или частной антивирусной сети, управляемой комплексом **Dr.Web Enterprise Security Suite** (далее **Dr.Web ESS**). Работа в таком режиме центральной защиты не требует установки дополнительного



программного обеспечения или удаления **Dr.Web для Novell Storage Services**.

Для обеспечения этой возможности, **Агент** может работать в одном из двух режимов:

- Одиночном (standalone mode) режиме, когда защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационные и ключевые файлы находятся на локальных дисках, а **Агент** полностью управляется с защищаемого компьютера.
- Режиме центральной защиты (enterprise mode), когда защитой компьютера управляет сервер центральной защиты. В этом режиме некоторые функции и настройки **Dr.Web для Novell Storage Services** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты. В этом режиме используется лицензионный ключевой файл с центрального сервера защиты. Персональный лицензионный ключевой файл на локальном компьютере не используется.

Чтобы использовать режим центральной защиты

1. Свяжитесь с системным администратором вашей сети чтобы получить файл с открытым ключом и параметры соединения с центральным сервером защиты.
2. В конфигурационном файле **Агента** (по умолчанию, `%etc_dir/agent.conf`) установите значения следующих параметров в секции [EnterpriseMode] :

- Укажите путь к файлу с открытым ключом, полученному от администратора сети, в параметре `PublicKeyFile` (обычно, `%var_dir/drwcsd.pub`). Этот файл содержит открытый ключ, используемый для зашифрованного соединения с сервером **Dr.Web Enterprise Server** (далее - **Enterprise Сервер**). Если вы - администратор сети, вы можете найти этот файл в соответствующей директории на **Enterprise Сервере**.



- Укажите IP-адрес или имя узла сервера **Enterprise Сервера** в параметре `ServerHost`.
 - Укажите номер порта для связи с **Enterprise Сервером** параметре `ServerPort`.
3. Чтобы включить режим центральной защиты, установите **Yes** в качестве значения параметра `UseEnterpriseMode`.

В режиме центральной защиты некоторые функции и настройки **Dr.Web для Novell Storage Services** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты. В этом режиме используется лицензионный ключевой файл с центрального сервера защиты. Персональный лицензионный ключевой файл на локальном компьютере не используется.

Для работы **Агента** в режиме центральной защиты должен быть установлен пакет `drweb-agent-es`.



Чтобы **Dr.Web для Novell Storage Services** полностью поддерживал режим центральной защиты, **Монитор** также должен работать в режиме центральной защиты. Для подробностей обратитесь к разделу [Режимы работы Монитора](#).

Чтобы использовать одиночный (standalone) режим

1. Убедитесь, что все параметры в секции `[StandaloneMode]` конфигурационного файла **Агента** (по умолчанию, `%etc_dir/agent.conf`) установлены корректно.
2. Установите **No** в качестве значения параметра `UseEnterpriseMode` секции `[EnterpriseMode]` конфигурационного файла **Агента**.

При включении этого режима все настройки **Dr.Web для Novell Storage Services** будут разблокированы и вы вновь получите доступ ко всем функциям и настройкам **Dr.Web для Novell Storage Services**.



Для работы в одиночном режиме **Dr.Web для Novell Storage Services** необходим действующий лицензионный ключ. Ключевые файлы, полученные с сервера центральной защиты, не могут быть использованы в этом режиме.

Совместное использование Dr.Web для Novell Storage Services и Антивируса Dr.Web для Linux в режиме центральной защиты

Ввиду особенностей реализации, одновременное использование в режиме централизованной защиты **Dr.Web для Novell Storage Services** и **Антивируса Dr.Web для Linux**, установленных на одном компьютере, невозможно. Для включения режима централизованной защиты **Dr.Web для Novell Storage Services** необходимо перевести **Антивирус Dr.Web для Linux** в режим автономной работы, после чего удалить или переместить в другую директорию файлы

```
%etc_dir/agent/drweb-cc.amc и %etc_dir/agent/  
drweb-spider.amc.
```

Рекомендуется сохранить эти файлы в качестве резервной копии в директории, отличной от `%etc_dir/agent`, если в дальнейшем вы планируете перевести перевести **Антивирус Dr.Web для Linux** в режим централизованной защиты. В таком случае, отключите режим централизованной защиты **Dr.Web для Novell Storage Services**, копируйте резервные копии файлов `drweb-cc.amc` и `drweb-spider.amc` в директорию `%etc_dir/agent/` и следуйте инструкциям, представленным в руководстве пользователя **Антивируса Dr.Web для Linux**.

Параметры командной строки

Dr.Web Control Agent, в дополнение к параметрам командной строки, поддерживаемым всеми модулями программного комплекса, допускает использование следующих параметров:



- `-h, --help` - краткая справка по параметрам командной строки;
- `-v, --version` - вывод информации о текущей версии **Агента**;
- `-u, --update-all` - запуск процесса обновления для всех компонентов;
- `-f, --update-failed` - запуск процесса обновления для компонентов, которые не удалось обновить в штатном режиме;
- `-C, --check-only` - проверка конфигурации **Агента**. Данный параметр командной строки не может быть использован при запущенном **Агенте**.
- `-c <путь к файлу>, --conf <путь к файлу>` - использование альтернативного файла конфигурации;
- `-d, --droppwd` - сбросить регистрационную информацию (имя пользователя и пароль) **Enterprise Сервера**. При следующей попытке соединения с **Enterprise Сервером**, будет запущен процесс регистрации новой станции;
- `-p, --newpwd` - смена пользовательского имени и пароля на сервере центральной защиты;
- `-s <путь к файлу>, --socket <путь к файлу>` - использование альтернативного сокета;
- `-P <путь к файлу>, --pid-file <путь к файлу>` - PID-файл **Агента**;
- `-e <название приложения>, --export-config <название приложения>` - экспорт конфигурации приложения, указанного в аргументе, на **Enterprise Сервер**. В качестве аргумента используется имя приложения, указанное в заголовке секции Application "имя приложения" соответствующего атс-файла. Данный параметр командной строки не может быть использован при запущенном **Агенте**. Также данный не может быть использован для экспорта конфигурации **Антивируса Dr.Web для Linux**.



Конфигурационный файл

Настройки компонента **Dr.Web Agent** задаются отдельным конфигурационным файлом `%etc_dir/agent.conf`. Устройство конфигурационного файла и краткое описание его параметров даны в разделе [Конфигурационные файлы](#).

Секция [Logging]

В секции [Logging] собраны параметры, управляющие ведением протоколов работы компонента **Dr.Web Agent** программного комплекса **Dr.Web для Novell Storage Services**:

Секция [Logging]

<pre>Level = { Quiet Error Alert Info Debug}</pre>	<p>Устанавливает уровень подробности ведения протокола работы компонента.</p> <p><u>Значение по умолчанию:</u></p> <pre>Level = Info</pre>
<pre>IPCLevel = { Quiet Error Alert Info Debug}</pre>	<p>Устанавливает уровень подробности протокола работы библиотеки IPC.</p> <p><u>Значение по умолчанию:</u></p> <pre>IPCLevel = Error</pre>
<pre>SyslogFacility = { Daemon Local0 .. Local7 Kern User Mail}</pre>	<p>Тип подсистемы, через которую системный сервис <code>syslogd</code>, ведущий протоколирование, выдает сообщения о событиях (более подробную информацию вы можете получить в документации по <code>syslog</code>).</p> <p><u>Значение по умолчанию:</u></p> <pre>SyslogFacility = Daemon</pre>



<code>FileName = { строка }</code>	Имя файла отчета. В качестве имени можно указать <code>syslog</code> , тогда отчет будет вестись средствами системного сервиса <code>syslogd</code> . При использовании <code>syslogd</code> нужно обратить внимание на параметры <code>SyslogFacility</code> , <code>IPCLevel</code> , и <code>Level</code> . Поскольку <code>syslogd</code> имеет несколько файлов для протоколирования разных событий и разных степеней их важности, то, основываясь на этих трех параметрах и содержанием конфигурационного файла <code>syslogd</code> (обычно <code>/etc/syslogd.conf</code>), можно определить, куда будет писаться отчет программы.
	<u>Значение по умолчанию:</u>
	<code>FileName = syslog</code>

Секция [Agent]

В секции [Agent] собраны основные настройки компонента **Dr.Web Agent**:

Секция [Agent]



MetaConfigDir = { путь к директории}	<p>Расположение файлов мета-конфигурации drweb-agent. В файлах мета-конфигурации описываются особенности взаимодействия Агента с другими модулями программного комплекса. Содержание файлов мета-конфигурации задается разработчиками "Доктор Веб" и не требует редактирования.</p> <p><u>Значение по умолчанию:</u></p> <pre>MetaConfigDir = %etc_dir/ agent/</pre>
UseMonitor = { Yes No}	<p>Значение Yes данного параметра, указывает модулю drweb-agent, что в составе программного комплекса используется Монитор.</p> <p><u>Значение по умолчанию:</u></p> <pre>UseMonitor = Yes</pre>
MonitorAddress = { адрес}	<p>Сокет, через который Агент взаимодействует с Монитором (значение параметра должно совпадать со значением параметра Address конфигурационного файла Монитора).</p> <p><u>Значение по умолчанию:</u></p> <pre>MonitorAddress = local:% var_dir/ipc/.monitor</pre>
MonitorResponseTime = { время в секундах}	<p>Максимальное время отклика модуля drweb-monitor. Если в течение этого времени от него не поступает реакции, то предполагается, что он не запущен, и Агент больше не предпринимает попыток взаимодействия с Монитором.</p> <p><u>Значение по умолчанию:</u></p> <pre>MonitorResponseTime = 5</pre>



PidFile = { путь к файлу}	Путь к файлу, в который записывается PID модуля drweb-agent при запуске. <u>Значение по умолчанию:</u> PidFile = %var_dir/run/drweb-agent.pid
----------------------------------	--

Секция [Server]

В этой секции располагаются параметры, управляющие взаимодействием **Dr.Web Agent** с другими модулями программного комплекса **Dr.Web для Novell Storage Services**:

Секция [Server]

Address = { адрес}	Сокет, через который модуль drweb-agent взаимодействует с другими модулями программного комплекса. Допускается несколько сокетов, перечисленных через запятую. <u>Значение по умолчанию:</u> Address = local:%var_dir/ipc/.agent, inet:4040@127.0.0.1
---------------------------	--

Threads = { численное значение}	Количество одновременных потоков drweb-agent. Параметр управляет максимальным количеством одновременных подключений к модулям, передающим Агенту вирусную статистику. Этот параметр не может быть изменен при перезапуске по сигналу SIGHUP. Если указано значение 0, количество одновременных потоков не ограничивается (не рекомендуется). <u>Значение по умолчанию:</u> Threads = 2
--	---



Timeout = { время в секундах}	Максимальное время установления соединения между Агентом и другими компонентами программного комплекса. Если указано значение 0, время установления соединения не ограничивается.
	<u>Значение по умолчанию:</u> Timeout = 15

Секция [EnterpriseMode]

В этой секции расположены параметры, управляющие работой **Dr.Web Agent** в режиме Enterprise:

Секция [EnterpriseMode]

UseEnterpriseMode = { Yes No}	При значении Yes данного параметра drweb-agent работает в режиме Enterprise, при значении No – в режиме Standalone.
	<u>Значение по умолчанию:</u> UseEnterpriseMode = No
ComputerName = { имя компьютера}	Название компьютера в антивирусной сети.
	<u>Значение по умолчанию:</u> ComputerName =
VirusbaseDir = { путь к директории}	Путь к вирусным базам.
	<u>Значение по умолчанию:</u> VirusbaseDir = %var_dir/bases
PublicKeyFile = { путь к файлу}	Путь к файлу открытого ключа для доступа к Enterprise Серверу .
	<u>Значение по умолчанию:</u>



	PublicKeyFile = %bin_dir/ drwcsd.pub
ServerHost = { IP- адрес}	IP-адрес Enterprise Сервера . <u>Значение по умолчанию:</u> ServerHost = 127.0.0.1
ServerPort = { номер порта}	Порт доступа к Enterprise Серверу . <u>Значение по умолчанию:</u> ServerPort = 2193
CryptTraffic = { Yes Possible No}	Шифрование трафика между сервером Enterprise Сервером и модулем drweb-agent. <u>Значение по умолчанию:</u> CryptTraffic = possible
CompressTraffic = { Yes Possible No}	Сжатие трафика между Enterprise Сервером и модулем drweb-agent. <u>Значение по умолчанию:</u> CompressTraffic = possible
CacheDir = { путь к директории}	Путь к директории, в которой хранятся служебные файлы: конфигурационные файлы компонентов и файлы, содержащие информацию о правах каждого из приложений, на случай, если Enterprise Сервер по какой-либо причине окажется недоступен, файлы с регистрационной информацией на Enterprise Сервере и т.п. <u>Значение по умолчанию:</u> CacheDir = %var_dir/agent



Секция [StandaloneMode]

Настройки drweb-agent для одиночного режима работы.

Секция [StandaloneMode]

StatisticsServer = { адрес сервера }	URL сервера вирусной статистики. Если URL сервера не указан, то статистика не будет отправляться. <u>Значение по умолчанию:</u> StatisticsServer = stat.drweb.com:80/update
StatisticsUpdatePeriod = { время в минутах }	Период обновления статистической информации. Не может быть меньше 5 минут <u>Значение по умолчанию:</u> StatisticsUpdatePeriod = 10
StatisticsProxy = { адрес прокси-сервера }	IP-адрес или имя хоста прокси-сервера для вирусной статистики. Обратите внимание, что если значение параметра не задано, используется значение переменной окружения http_proxy. <u>Пример:</u> StatisticsProxy = localhost:3128 <u>Значение по умолчанию:</u> StatisticsProxy =
StatisticsProxyAuth = { параметры аутентификации }	Имя пользователя и пароль для доступа к прокси-серверу. <u>Пример:</u> StatisticsProxyAuth = test:



	<code>testpwd</code> <u>Значение по умолчанию:</u> StatisticsProxyAuth =
UUID = {идентификатор}	Личный идентификатор пользователя на сервере статистики http://stat.drweb.com . Данный параметр является обязательным для передачи статистики — соответственно, если вы желаете подключить эту возможность, вы должны указать в его значении персональный UUID (в качестве которого обычно используется md5 сумма лицензионного ключевого файла). <u>Значение по умолчанию:</u> UUID =
LicenseFile = {список путей к файлам}	Расположение ключевых файлов программного комплекса Dr.Web для Novell Storage Services (лицензионных или демонстрационных). <u>Значение по умолчанию:</u> LicenseFile = %bin_dir/ drweb32.key
ProtectedEmails = {lookups}	Список защищаемых почтовых адресов. Их можно задать непосредственно, либо указать путь к файлу, в котором они перечислены. <u>Значение по умолчанию:</u> ProtectedEmails = file:%etc_dir/ email.ini

Секция [Update]

В этой секции собраны параметры, относящиеся к процессу



обновления компонентов программного комплекса **Dr.Web для Novell Storage Services** через **Enterprise Сервер** (подробнее см. в руководстве администратора **Dr.Web ESS**):

Секция [Update]

CacheDir = { путь к директории}	Директория, в которой Агент временно сохраняет загруженные файлы обновлений.
	<u>Значение по умолчанию:</u> CacheDir = %var_dir/updates/cache
Timeout = { время в секундах}	Максимальное время обработки Агентом полученных обновлений. Если указано значение 0, время обработки не ограничивается.
	<u>Значение по умолчанию:</u> Timeout = 120
RootDir = { путь к директории}	Путь к корневой директории.
	<u>Значение по умолчанию:</u> RootDir = /

Запуск



Обратите внимание, что в процессе работы установочного скрипта при выборе соответствующей возможности в диалоге все сервисы, включая **Агента**, будут запущены автоматически.

В процессе запуска **Агента** при установках по умолчанию осуществляются следующие действия:

- производится поиск и загрузка конфигурационного файла; если файл не найден, то загрузка прекращается;



- если в файле конфигурации заданы параметры секции [EnterpriseMode] (и программный комплекс **Dr.Web для Novell Storage Services** работает в составе антивирусной сети), **Агент** запускается в режиме Enterprise. В противном случае, если в файле настроек заданы параметры секции [Standalone], **Агент** запускается в одиночном режиме. Если параметры секции [Standalone] также не заданы, то загрузка **Агента** прекращается;
- создается сокет для взаимодействия с другими модулями программного комплекса. В случае TCP-соединения подключений может быть несколько (загрузка продолжается, если удалось создать хотя бы одно из них). Если используется UNIX сокет, он может быть создан только когда директория, его содержащая, доступна на запись и чтение пользователю, с чьими правами работает модуль drweb-agent. Если ни один сокет не может быть создан, загрузка **Агента** прекращается.

Дальнейший процесс загрузки **Агента** зависит от того, в каком режиме он работает.

Если **Агент** работает в режиме Enterprise:

- производится соединение с сервером централизованной защиты **Dr.Web**. Если при первом подключении сервер недоступен, либо **Агенту** не удалось авторизоваться, **Агент** завершает свою работу. Если ранее **Агент** уже работал с данным сервером, но в данный момент он недоступен (например, в случае проблем с соединением), **Агент** использует резервные копии конфигурационных файлов, полученных от сервера во время предыдущего подключения. Данные файлы зашифрованы и не предназначены для правки пользователем. Попытка изменить их вручную приведёт к их неработоспособности;
- если соединение успешно установлено, происходит получение лицензионных ключей и настроек компонентов программного комплекса с сервера централизованной защиты. После завершения этой операции **Агент** готов к работе.



Если **Агент** работает в режиме Standalone:

- загружаются файлы мета-конфигурации компонентов программного комплекса. В файлах мета-конфигурации описываются особенности взаимодействия **Агента** с компонентами. Расположение файлов мета-конфигурации берется из параметра **MetaConfigDir** секции настроек [Agent] файла конфигурации **Агента**. После завершения этой операции **Агент** готов к работе.

Взаимодействие с компонентами программного комплекса

Взаимодействие с компонентами программного комплекса осуществляется с помощью атс-файлов. В этих файлах описывается конфигурация компонентов и параметры, значения которых **Агент** выдает компонентам.

Описание каждого компонента содержится в секции `Application "имя_компонента"`. В конце секции обязательно должно быть поставлено `EndApplication`. В описании компонента должны присутствовать следующие параметры:

- **id**: идентификатор компонента на **Enterprise Сервере**;
- **ConfFile**: путь к конфигурационному файлу компонента;
- **Components**: описание компонентов. В конце описания ставится `EndComponents`. Для каждого из компонентов указываются: его название и через пробел — список секций конфигурационного файла и параметров в них, которые требуются компоненту для нормальной работы. Секции и параметры перечисляются через запятую. Для описания параметров необходимо указывать полный путь к ним (например, `/Quarantine/DBISettings`), а для описания секций достаточно указания имени секции (например, `General`).

Пример атс-файла для Dr.Web NSS:



```
Application "NSS"
  id 108
  ConfFile "/etc/drweb/drweb-nss.conf"
  Components
    drweb-nss General, Logging,
  DaemonCommunication, NSS, Actions, \
    Quarantine, Stat,
  Notifications
  EndComponents
EndApplication
```

Интеграция с Dr.Web Enterprise Security Suite

Возможны следующие ситуации, в которых требуется интегрировать программный комплекс **Dr.Web для Novell Storage Services** с **Dr.Web Enterprise Security Suite**:

- первоначальная установка и настройка почтового сервера UNIX в уже работающей системе **Dr.Web ESS**;
- встраивание работающего почтового сервера UNIX с установленным и настроенным программным комплексом **Dr.Web для Novell Storage Services** в систему **Dr.Web ESS**.

Для того, чтобы программный комплекс **Dr.Web для Novell Storage Services** мог работать в составе **Dr.Web Enterprise Security Suite**, необходимо настроить компоненты **Агент** и **Монитор** для работы в режиме **Enterprise** и зарегистрировать комплекс на сервере **Dr.Web Enterprise Server** (далее - **Enterprise Сервер**).

В соответствии с политикой подключения новых станций (подробнее см. руководство администратора **Dr.Web Enterprise Security Suite**), подключить **Dr.Web для Novell Storage Services** к **Enterprise Серверу** можно двумя способами:



- создав учетную запись на сервере автоматически;
- создав учетную запись на сервере вручную.

Настройка компонентов для работы в режиме Enterprise

После установки для запуска в режиме Enterprise необходимо вручную внести изменения в локальные конфигурационные файлы **Агента** и **Монитора**.

Для Агента

В секции [EnterpriseMode] конфигурационного файла **Агента** `%etc_dir/agent.conf` установите следующие значения параметров:

- **UseEnterpriseMode** = Yes;
- **PublicKeyFile** = `%var_dir/drwcsd.pub` (открытый ключ шифрования для доступа к **Enterprise Серверу**. Администратор должен самостоятельно взять данный файл из соответствующей директории **Enterprise Сервера** и положить его по указанному пути);
- **ServerHost** = IP-адрес или имя хоста **Enterprise Сервера**;
- **ServerPort** = порт **Enterprise Сервера** (2193 по умолчанию).

Для Монитора

В секции [Monitor] конфигурационного файла **Монитора** `%etc_dir/monitor.conf` установите следующие значения параметров:

- **UseEnterpriseMode** = Yes.



Автоматическое создание учетной записи

При автоматическом создании учетной записи:

- при первом запуске в режиме **Enterprise Агент** запрашивает регистрационные данные (идентификатор станции и пароль) у **Enterprise Сервера**;
- если на **Enterprise Сервере** установлен режим "**Ручное подтверждение доступа**" (режим по умолчанию, см. руководство администратора **Dr.Web Enterprise Security Suite**), то администратору в течение одной минуты с момента запроса необходимо подтвердить регистрацию новой станции через веб-интерфейс **Центра управления Dr.Web**;
- после первого подключения **Агент** записывает хэш идентификатора станции и пароля пользователя в файл `agent.pwd`. Данный файл создается в директории, заданной значением параметра `CacheDir` секции `[EnterpriseMode]` (по умолчанию `%var_dir/agent/`);
- в дальнейшем данные из этого файла используются для подключения программного комплекса **Dr.Web для Novell Storage Services** к **Enterprise Серверу**;
- удаление файла с паролем приведет к повторному запросу регистрационных данных у ESS-сервера при следующем запуске **Агента**.

Создание учетной записи на сервере вручную

Для создания учетной записи на сервере вручную:

- Создайте учетную запись на сервере с указанием идентификатора станции и пароля (см. руководство администратора **Dr.Web Enterprise Security Suite**);
- Запустите **Агент** с параметром командной строки `--newpwd` (или `-p`) и введите идентификатор и пароль. Хэш идентификатора станции и пароля пользователя в файл



agent.pwd. Данный файл создаётся в директории, путь к которой задается значением параметра `CacheDir` секции `[EnterpriseMode]` (по умолчанию `%var_dir/agent/`);

- В дальнейшем данные из этого файла используются для подключения **Dr.Web для Novell Storage Services** к **Enterprise Serverу**;
- Удаление файла с паролем приведет к необходимости повторить процедуру регистрации при следующем запуске **Агента**.

Задание конфигурации компонентов через веб-интерфейс сервера

Через веб-интерфейс **Центра Управления Dr.Web** можно управлять настройкой конфигурации компонентов **Dr.Web для Novell Storage Services** и **Dr.Web Daemon** (антивирусного модуля, входящего в базовый пакет **Dr.Web**).

В поставку **Dr.Web Enterprise Security Suite** включены стандартные конфигурационные файлы компонентов **Dr.Web для Novell Storage Services** и **Dr.Web Daemon** для основных UNIX-платформ: Linux, FreeBSD и Solaris. Соответственно, при настройке компонентов задание значений параметров происходит в этих файлах через веб-интерфейс **Центра Управления Dr.Web**. Затем каждый раз при запуске какого-либо из компонентов **Агент** запрашивает и получает конфигурацию от сервера централизованной защиты.

Экспорт существующей конфигурации на сервер

При помощи работающего в режиме **Enterprise Агента** возможно автоматически экспортировать конфигурацию компонентов на ESS-сервер. Для этого необходимо экспортировать конфигурацию параметром командной строки `--export-config` (или `-e`) с обязательным указанием названия компонента (`DAEMON, NSS`).

**Пример:**

```
# %bin_dir/drweb-agent --export-config  
NSS
```

Запуск комплекса

Чтобы запустить комплекс:

- Через веб-интерфейс **Центра Управления Dr.Web** в настройках **Монитора** установите флаги Daemon и NSS для запуска соответствующих компонентов комплекса;
- Запустите **Монитор** на локальной станции:

```
# /etc/init.d/drweb-monitor start
```

Работа с вирусной статистикой

При работе программного комплекса **Dr.Web для Novell Storage Services** с подключенным антивирусным модулем может производиться сбор сведений о вирусных событиях. Собранная информация передается на сервер статистики "**Доктор Веб**" (<http://stat.drweb.com/>), либо на сервер централизованной защиты **Dr.Web**, если **Агент** работает в режиме Enterprise. Для соединения **Агента** с сервером статистики "**Доктор Веб**" необходим идентификатор пользователя – UUID. По умолчанию в качестве UUID используется md5 ключевого файла. Также вы можете получить персональный UUID, обратившись в службу поддержки. Такой UUID прописывается в файле конфигурации **Агента**.

По адресу <http://stat.drweb.com/> можно ознакомиться как с результатами обработки статистических данных по вашему серверу, так и с обобщенной статистической информацией по всем серверам, обслуживаемым антивирусом **Dr.Web для UNIX** либо программным комплексом **Dr.Web для Novell Storage Services** с подключенным антивирусным модулем.



Результаты обработки содержат сведения о наиболее часто обнаруживаемых вирусах (количество обнаружений и процент от общей суммы) за определенный период.

Сведения могут представляться как в формате HTML, так и в виде файла с XML-разметкой. Последний вариант особенно удобен, если предполагается публикация полученных данных на веб-сайте, поскольку позволяет предварительно преобразовать данные в соответствии с дизайном сайта и концепцией представления информации на нем.

Для получения обобщенной статистики по всем обслуживаемым серверам откройте в веб-браузере страницу <http://stat.drweb.com/>. На странице представлен список обнаруженных вирусов на обслуживаемых серверах (в порядке убывания частоты встречаемости) с указанием для каждого из них количества обнаружений в абсолютной и процентной форме. Внешний вид страницы может различаться в зависимости от используемого веб-браузера.

Дата начала: 9 Jun 2009 00:00 Почта
Дата окончания: 9 Jun 2009 14:00 Файлы
Топ: 10 Запросить График

09.06.2009 00:00 - 09.06.2009 14:00		
1	Win32_HLLM.Netsky_35328	96597 (30.91%)
2	Win32_HLLM.MyDoom_33808	38672 (12.37%)
3	Trojan.Fatnetlog_9	24103 (7.71%)
4	Win32_HLLM.Beagle	23878 (7.64%)
5	Win32_HLLM.MyDoom_based	17834 (5.71%)
6	Trojan.DownLoad_36339	16496 (5.28%)
7	Win32_HLLM.MyDoom_44	12463 (3.99%)
8	Trojan.MulDrop_19648	9236 (2.95%)
9	Win32_HLLM.Beagle_32768	8961 (2.87%)
10	Trojan.MulDrop_13408	8033 (2.57%)

Всего проверено: 2,300,493,581
Инфицировано: 312,558 (0.01%)

Рис. 15. Вирусная статистика

Вы можете изменить параметры запроса и повторить его:

- Установите переключатель в положение **Почта** или **Файлы** для получения статистики по вирусам, найденным



в почтовых сообщениях или файлах.

- В раскрывающихся списках **Дата начала** и **Дата окончания** установите время и дату начала и окончания периода, за который требуется статистика.
- Введите в поле **Топ** количество строк в таблице (будут представлены только наиболее часто встречающиеся вирусы).
- Нажмите на кнопку **Запросить**.
- Установите флажок **График**, если вы хотите получить статистическую информацию в графическом виде.

Файл с обобщенной статистикой в формате XML находится по адресу <http://info.drweb.com/export/xml/top/>.

Пример такого файла приведен ниже:

```
<drwebvirustop          period="24"          top="5"
vdbaseurl="http://info.drweb.com/
virus_description/"      updatedutc="2009-06-09
09:32:02">
<item>
<vname>Win32.HLLM.Netsky</vname>
<dwvlid>62083</dwvlid>
<place>1</place>
<percents>34.201062139103</percents>
</item>
<item>
<vname>Win32.HLLM.MyDoom</vname>
<dwvlid>9353</dwvlid>
<place>2</place>
<percents>25.1303270912579</percents>
</item>
<item>
<vname>Win32.HLLM.Beagle</vname>
<dwvlid>26997</dwvlid>
```



```
<place>3</place>
<percents>13.4593034783378</percents>
</item>
<item>
<vname>Trojan.Botnetlog.9</vname>
<dwvlid>438003</dwvlid>
<place>4</place>
<percents>7.86446592583328</percents>
</item>
<item>
<vname>Trojan.DownLoad.36339</vname>
<dwvlid>435637</dwvlid>
<place>5</place>
<percents>7.31494163115527</percents>
</item>
</drwebvirustop>
```

В данном файле используются следующие атрибуты:

- `period` - продолжительность времени сбора статистики (в часах);
- `top` - количество представленных в таблице наиболее часто встречающихся вирусов;
- `updatedutc` - время последнего обновления статистики;
- `vname` - наименование вируса;
- `place` - место в статистике;
- `percents` - процент от общего числа обнаружений.



Пользователь не может задать продолжительность периода сбора статистики и размер выборки.

Для получения персональной статистики откройте страницу <http://stat.drweb.com/view/<UID>>, где <UID> - это md5 ключевого файла пользователя. Страница персональной статистики имеет формат, полностью аналогичный формату страницы обобщенной статистики.

Файл с персональной статистикой в формате XML находится по адресу <http://stat.drweb.com/xml/<UID>>, где <UID> - это md5 ключевого файла пользователя.

Ниже приводится сокращенный пример такого файла:

```
<drwebvirustop period="24" top="2" user="<UID>"
lastdata="2005-04-12 07:00:00+04">
<item>
<caught>69</caught>
<percents>24.1258741258741</percents>
<place>1</place>
<vname>Win32.HLLM.Netsky.35328</vname>
</item>
<item>
<caught>57</caught>
<percents>19.9300699300699</percents>
<place>2</place>
<vname>Win32.HLLM.MyDoom.54464</vname>
</item>
</drwebvirustop>
```

В данном файле используются следующие атрибуты:

- `period` - продолжительность времени сбора статистики (в часах);



- `top` - количество представленных в таблице наиболее часто встречающихся вирусов;
- `user` - идентификатор пользователя;
- `lastdata` - время последнего получения данных от пользователя;
- `vname` - наименование вируса;
- `place` - место в статистике;
- `caught` - количество обнаружений данного вируса;
- `percents` - процент от общего числа обнаружений.



Как и в случае запроса обобщенной статистики, пользователь не может задать продолжительность периода сбора статистики и размер выборки.



Dr.Web Monitor

Компонент **Dr.Web Monitor** (далее **Монитор**) представлен модулем `drweb-monitor` и предназначен для повышения отказоустойчивости всего программного комплекса **Dr.Web для Novell Storage Services**. Он осуществляет запуск всех модулей, подгружая при необходимости их дополнительные компоненты. Если запустить какой-либо модуль не удалось, **Монитор** повторяет попытку. Количество попыток и время между ними определяются настройками компонента.

После того, как все модули были загружены, **Монитор** осуществляет постоянный контроль их работы. **Монитор** может обмениваться с этими модулями различными управляющими сигналами. В случае сбоя какого-либо модуля или одного из его компонентов **Монитор** перезапускает его. Максимальное количество попыток перезапуска и время между ними также определяются настройками **Монитора**. При возникновении неполадок в работе какого-либо модуля **Монитор** одним из доступных ему способов оповещает об этом администратора.

Режимы работы

При необходимости продукты компании "**Доктор Веб**" могут быть подключены к корпоративной или частной антивирусной сети, управляемой комплексом **Dr.Web Enterprise Security Suite**. Работа в таком режиме центральной защиты не требует установки дополнительного программного обеспечения или удаления **Dr.Web для Novell Storage Services**.

Для обеспечения этой возможности, **Монитор** может работать в одном из двух режимов:



- Одиночном (standalone mode) режиме, когда защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационные и ключевые файлы находятся на локальных дисках, **Монитор** полностью управляется с защищаемого компьютера, а все необходимые модули **Dr.Web** запускаются в соответствии с локальными настройками **Монитора**.
- Режиме центральной защиты (enterprise mode), когда защитой компьютера управляет сервер центральной защиты. В этом режиме некоторые функции и настройки **Dr.Web для Novell Storage Services** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты. В этом режиме используется лицензионный ключевой файл с центрального сервера защиты. Персональный лицензионный ключевой файл на локальном компьютере не используется.

Чтобы использовать режим центральной защиты

1. Свяжитесь с системным администратором вашей сети чтобы получить файл с открытым ключом и параметры соединения с центральным сервером защиты.
2. В конфигурационном файле **Монитора** (по умолчанию, %etc_dir/monitor.conf) установите Yes в качестве значения параметра UseEnterpriseMode.



В режиме центральной защиты некоторые функции и настройки **Dr.Web для Novell Storage Services** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты. В этом режиме используется лицензионный ключевой файл с центрального сервера защиты. Персональный лицензионный ключевой файл на локальном компьютере не используется.



Чтобы **Dr.Web для Novell Storage Services** полностью поддерживал режим центральной защиты, **Агент** также должен работать в режиме центральной защиты. Для подробностей обратитесь к разделу [Режимы работы Агента](#).

Чтобы использовать одиночный (standalone) режим

1. Убедитесь, что все необходимые модули, указанные в параметре `RunAppList` в секции `[Monitor]` конфигурационного файла **Монитора** (по умолчанию, `%etc_dir/monitor.conf`), установлены корректно.
2. Установите `No` в качестве значения параметра `UseEnterpriseMode` секции `[Monitor]` конфигурационного файла **Монитора**.

При включении этого режима все настройки **Dr.Web для Novell Storage Services** будут разблокированы, и вы вновь получите доступ ко всем функциям и настройкам **Dr.Web для Novell Storage Services**.



Для работы в одиночном режиме **Dr.Web для Novell Storage Services** необходим действующий лицензионный ключ. Ключевые файлы, полученные с сервера центральной защиты, не могут быть использованы в этом режиме.



Параметры командной строки

Dr.Web Monitor допускает использование следующих параметров:

- `-h, --help` - вывод краткой справки по параметрам командной строки **Монитора**;
- `-v, --version` - вывод информации о текущей версии **Монитора**;
- `-u, --update` - запуск процесса обновления;
- `-C, --check-only` - проверка конфигурации **Монитора**;
- `-A, --check-all` - проверка конфигурации всех компонентов;
- `-c <путь к файлу>, --conf <путь к файлу>` - использование альтернативного конфигурационного файла;
- `-r, --run приложение1 [, приложение2]` - запуск приложений.

Пример:

```
-r AGENT, NSS
```

Конфигурационный файл

Настройки компонента **Dr.Web Monitor** задаются отдельным конфигурационным файлом `%etc_dir/monitor.conf`. Устройство конфигурационного файла и краткое описание его параметров даны в разделе [Конфигурационные файлы](#).

Секция [Logging]

В секции [Logging] собраны параметры, управляющие ведением протоколов работы компонента **Dr.Web Monitor**

программного комплекса **Dr.Web для Novell Storage Services:**

Секция [Logging]

Level = { Quiet Error Alert Info Debug}	Устанавливает уровень подробности ведения протокола работы компонента. <u>Значение по умолчанию:</u> Level = Info
IPCLevel = { Quiet Error Alert Info Debug}	Устанавливает уровень подробности протокола работы библиотеки IPC. <u>Значение по умолчанию:</u> IPCLevel = Error
SyslogFacility = { Daemon Local0 .. Local7 Kern User Mail}	Тип подсистемы, через которую системный сервис syslogd, ведущий протоколирование, выдает сообщения о событиях (более подробную информацию вы можете получить в документации по syslog). <u>Значение по умолчанию:</u> SyslogFacility = Daemon
FileName = { строка}	Имя файла отчета. В качестве имени можно указать syslog, тогда отчет будет вестись средствами системного сервиса syslogd. При использовании syslogd нужно обратить внимание на параметры SyslogFacility , IPCLevel , и Level . Поскольку syslogd имеет несколько файлов для протоколирования разных событий и разных степеней их важности, то, основываясь на этих трех параметрах и содержанием конфигурационного файла syslogd (обычно /etc/syslogd.conf), можно определить, куда будет писаться отчет программы. <u>Значение по умолчанию:</u>



```
FileName = syslog
```

Секция [Monitor]

В секции [Monitor] собраны основные настройки компонента **Dr.Web Monitor**:

Секция [Monitor]

```
RunForeground =  
{ Yes | No }
```

Значение **Yes** запрещает **Монитору** переходить в режим демона, т.е. становиться фоновым процессом без управляющего терминала. Эта возможность может быть использована некоторыми средствами мониторинга (например, daemontools).

Значение по умолчанию:

```
RunForeground = No
```

```
User = { имя  
пользователя }
```

Имя пользователя, с правами которого запускается **Монитор**.

Значение по умолчанию:

```
User = drweb
```

```
Group = { название  
группы }
```

Имя пользовательской группы, с правами которой запускается **Монитор**.

Значение по умолчанию:

```
Group = drweb
```

```
PidFileDir = { путь  
к директории }
```

Имя директории, где содержится файл, в который при запуске **Монитора** записывается информация об идентификаторе его процесса (PID).

Значение по умолчанию:

```
PidFileDir = %var_dir/run/
```



ChDir = { путь к директории}	<p>Смена активной директории при запуске Монитора. Если значение параметра задано, то при запуске Монитор делает активной директорию, указанную в значении этого параметра. Если значение параметра не задано, то смена активной директории не происходит.</p> <p><u>Значение по умолчанию:</u></p> <p>ChDir = /</p>
MetaConfigDir = { путь к директории}	<p>Путь к директории с файлами мета-конфигурации. В этих файлах задаются параметры работы Монитора с модулями программного комплекса. Содержание файлов мета-конфигурации задается разработчиками программного продукта и не требует редактирования.</p> <p><u>Значение по умолчанию:</u></p> <p>MetaConfigDir = %etc_dir/monitor/</p>
Address = { адрес}	<p>Сокет, через который Монитор взаимодействует с другими модулями антивируса.</p> <p><u>Значение по умолчанию:</u></p> <p>Address = local:%var_dir/ipc/.monitor</p>
Timeout = { время в секундах}	<p>Максимальное время установления соединения между Монитором и другими компонентами программного комплекса.</p> <p><u>Значение по умолчанию:</u></p> <p>Timeout = 5</p>



<pre>TmpFileFmt = { текст}</pre>	<p>Шаблон имени временных файлов Монитора. Формат шаблона: путь_к_файлу.XXXXXX, где X - произвольные буквы и цифры в именах создаваемых временных файлов.</p> <p><u>Значение по умолчанию:</u></p> <pre>TmpFileFmt = %var_dir/msgs/ tmp/monitor.XXXXXX</pre>
<pre>RunAppList = { текст}</pre>	<p>Список модулей, запускаемых Монитором. Названия модулей отделяются друг от друга запятыми.</p> <p>Обратите внимание, что при удалении какого-либо модуля из системы его название не удаляется из списка RunAppList автоматически и должно быть удалено вручную. В противном случае Монитор не сможет запуститься сам и запустить остальные компоненты.</p> <p><u>Значение по умолчанию:</u></p> <pre>RunAppList = AGENT</pre>
<pre>UseEnterpriseMode = { Yes No}</pre>	<p>При значении Yes данного параметра список модулей, запускаемых Монитором, берется не из параметра RunAppList, а от модуля drweb-agent.</p> <p><u>Значение по умолчанию:</u></p> <pre>UseEnterpriseMode = No</pre>
<pre>RecoveryTimeList = { время в секундах}</pre>	<p>Временные промежутки между попытками перезапуска "зависших" приложений. Для параметра можно задать несколько значений, перечислив их через запятую. Первая попытка перезагрузки приложения производится через время, указанное первым значением параметра, вторая – через время, указанное вторым и т.д.</p>



	<p><u>Значение по умолчанию:</u></p> <pre>RecoveryTimeList = 0,30,60</pre>
<pre>InjectCmd = { строка }</pre>	<p>Команда для отсылки отчетов. Обратите внимание, что для отправки сообщений на адрес, отличный от root@localhost, надо в команде указать действительный адрес.</p> <p><u>Значение по умолчанию:</u></p> <pre>InjectCmd = "/usr/sbin/ sendmail -t"</pre>
<pre>AgentAddress = { lookups }</pre>	<p>Сокет, через который Монитор взаимодействует с Агентом (значение параметра должно совпадать со значением параметра Address конфигурационного файла Агента).</p> <p><u>Значение по умолчанию:</u></p> <pre>AgentAddress = local:%var_dir/ ipc/.agent</pre>
<pre>AgentResponseTime = { время в секундах }</pre>	<p>Максимальное время отклика модуля drweb-agent. Если в течение этого времени от модуля не поступает ответа, то Монитор перезапускает его. Если указано значение 0, время отклика не ограничивается.</p> <p><u>Значение по умолчанию:</u></p> <pre>AgentResponseTime = 5</pre>



Запуск



Обратите внимание, что в процессе работы установочного скрипта при выборе соответствующей возможности в диалоге все сервисы, включая **Монитор**, будут запущены автоматически.

В процессе запуска **Монитора** (при установках по умолчанию) осуществляются следующие действия:

- производится поиск и загрузка конфигурационного файла; если файл не найден, то загрузка прекращается;
- **Монитор** переходит в режим демона, поэтому сообщения о дальнейших проблемах не могут быть выведены на терминал и выводятся только в файл отчета;
- создается сокет для взаимодействия с другими модулями программного комплекса **Dr.Web для Novell Storage Services**. В случае использования TCP-соединений, подключений может быть несколько (загрузка продолжится, если удалось создать хотя бы одно из них). Если используется UNIX сокет, то он может быть создан только когда директория, его содержащая, доступна на запись и чтение пользователю, с чьими привилегиями работает модуль `drweb-monitor`. Если ни один сокет не может быть создан, загрузка прекращается;
- создается PID-файл, в котором хранится информация об идентификаторе процесса **Монитора**. Если создать PID-файл не удалось, то загрузка прекращается;



- модуль `drweb-monitor` запускает остальные модули программного комплекса **Dr.Web для Novell Storage Services**. Если какой-либо из модулей не загружается, **Монитор** пытается запустить его повторно. Если все попытки **Монитора** загрузить модуль окончились неудачей, **Монитор** выгружает все уже загруженные модули и завершает свою работу. Обо всех проблемах с запуском модулей программного комплекса **Монитор** сообщает одним из доступных ему способов (записью в файл протокола, сообщением электронной почты, запуском произвольной программы). Способы оповещения, используемые для разных модулей, задаются в файле мета-конфигурации **Монитора**.

Для успешного запуска Монитора в автоматическом режиме:

- либо в файле `%etc_dir/drweb-monitor.enable` переменной `ENABLE` должно быть присвоено значение `1`.

Взаимодействие с компонентами программного комплекса

Взаимодействие с компонентами программного комплекса осуществляется с помощью `mtc`-файлов. В этих файлах описывается состав компонентов, расположение бинарных файлов, порядок их запуска и параметры запуска.

Описание каждого компонента содержится в секции `Application "имя_компонента"`. В конце секции обязательно должно быть поставлено `EndApplication`.

В описании компонента должны присутствовать следующие параметры:

- **FullName**: полное имя приложения;
- **Path**: путь к бинарным файлам;
- **Depends**: имена компонентов, которые должны



запускаться до запуска описываемого компонента. Например, компонент AGENT должен запускаться до компонента DAEMON, поэтому в mmc-файле для **Dr.Web Daemon** параметр **Depends** имеет значение "AGENT". Если подобные зависимости отсутствуют, то параметр может быть пропущен;

- **Components**: список бинарных файлов компонентов, запускаемых при старте приложения. Компоненты запускаются в том порядке, в котором перечислены. Для каждого из компонентов через пробел указываются: аргументы командной строки (могут быть заключены в кавычки), максимальное время, отводимое на запуск компонента, максимальное время для остановки, тип оповещения и права для запуска. Тип оповещения - указывает, куда высылать сообщения о сбоях компонента. Он может принимать значения MAIL (осуществляется отсылка оповещений по почте) и LOG (информация о сбоях только записывается в лог). Права для запуска - указывают группу и пользователя, с чьими правами будет запускаться компонент.

Пример mmc-файла Dr.Web Daemon для Linux:

```
Application "DAEMON"  
    FullName      "Dr. Web (R) Daemon"  
    Path          "/opt/drweb/"  
    Depends       "AGENT"  
    Components  
        # name      args      MaxStartTime  
    MaxStopTime   NotifyType User:Group  
        drwebd    "-a=local:/var/drweb/ipc/.agent  
--foreground=yes" 30 10 MAIL drweb:drweb  
    EndComponents  
EndApplication
```



Консольный сканер Dr.Web Scanner

Консольный сканер **Dr.Web Scanner** служит для обнаружения и лечения вирусов на локальной машине.

Параметры командной строки

Общий формат запуска программы следующий:

```
$ %bin_dir/drweb <путь> [параметры  
командной строки]
```

где <путь> - путь или пути к проверяемым каталогам или маска проверяемых файлов. Если путь задан с префиксом: `disk://<путь к файлу устройства>`, то будет проверен загрузочный сектор соответствующего устройства и при необходимости произведено его лечение. Запущенный без параметров, только с указанием пути в качестве аргумента, консольный сканер **Dr.Web Scanner** (далее **Сканер**) осуществляет проверку указанной директории, используя набор параметров по умолчанию. В следующем примере проверяется домашняя директория пользователя:

```
$ %bin_dir/drweb ~
```

По окончании проверки, в случае обнаружения зараженных или подозрительных файлов, **Сканер** выводит информацию обо всех таких файлах в следующем виде:

```
    /path/file      инфицирован      [вирусом]  
ИМЯ_ВИРУСА
```

После вывода информации о зараженных и подозрительных файлах, если таковые были обнаружены, **Сканер** выдает отчет примерно следующего вида:



```
Отчет для "/opt/drweb/tmp":
Проверено      : 34/32   Исцелено      : 0
Инфицировано : 5/5     Удалено       : 0
Модификаций   : 0/0     Переименовано: 0
Подозрительных: 0/0     Перемещено    : 0
Время проверки: 00:00:02  Скорость      :
5233 KB/s
```

Числа, разделенные символом "/", означают: первое - общее количество файлов, второе - количество файлов в архивах.

Для того, чтобы пользователь имел возможность проверить работоспособность антивируса, в состав дистрибутива продукта входит специальный тестовый файл `readme.eicar.rus`. С помощью текстового редактора из него легко изготовить программу `ecar.com` (см. указания внутри самого файла), которая ведет себя подобно вирусу, вызывая сообщение вида:

```
%bin_dir/doc/ecar.com инфицирован Eicar
Test File (Not a Virus!)
```

Этот файл не является вирусом и используется исключительно для тестирования. С этой целью все современные антивирусные программы включают информацию о нем в свои вирусные базы.

Сканер "Доктор Веб" может быть настроен с помощью многочисленных параметров командной строки. Они отделяются от указания пути пробелом и начинаются с символа "-" (дефис). Полный список параметров командной строки можно получить, запустив программу `drweb` с параметрами `-?`, `-h` или `-help`.

Основные параметры программы могут быть сгруппированы следующим образом:

- параметры области проверки;
- параметры диагностики;
- параметры действий;



- параметры интерфейса.

Параметры области проверки указывают, где следует проводить проверку:

- `path` – необязательный параметр для задания пути для сканирования. В одном параметре может быть задано несколько путей;
- `@[+] <файл>` – проверка объектов, перечисленных в указанном файле. Символ "+" (плюс) предписывает не удалять файл со списком объектов по окончании проверки. Этот файл может содержать пути к периодически проверяемым директориям или просто список подлежащих регулярной проверке файлов;
- `sd` – рекурсивный поиск и проверка файлов в поддиректориях, начиная с текущего;
- `fl` – указание следовать символическим ссылкам, как для файлов, так и для директорий. Ссылки, приводящие к "зацикливанию", игнорируются;
- `mask` – указание игнорировать маски имен файлов.

Параметры диагностики, определяющие, какие типы объектов должны проверяться на вирусы:

- `al` – диагностика всех файлов на заданном устройстве или в указанной в качестве аргумента директории;
- `ar[d] m[r] [n]` – проверка файлов в архивах (ARJ, CAB, GZIP, RAR, TAR, ZIP и др.). `d` – удаление, `m` – перемещение, `r` – переименование архивов, содержащих зараженные объекты, `n` – отключение вывода имен архиваторов. Под архивом в данном случае понимаются не только собственно архивы (например, вида `*.tar`), но и их сжатые формы (в частности, сжатые tar-архивы вида `*.tar.bz2` и `*.tbz`);
- `cn[d] m[r] [n]` – проверка файлов в контейнерах (HTML, RTF, PowerPoint и др.). `d` – удаление, `m` – перемещение, `r` – переименование контейнеров, содержащих зараженные объекты, `n` – отключение вывода типа контейнера;
- `ml[d] m[r] [n]` – проверка файлов почтовых программ.



d - удаление, m - перемещение, r - переименование файлов почтовых программ, содержащих зараженные объекты, n - отключение вывода типа файлов почтовых программ;

- upn - проверка исполняемых файлов, упакованных LZEXE, DIET, PKLITE, EXEPACK, с отключенным выводом имен утилит упаковки;
- ex - диагностика файлов, имена которых соответствуют заданным маскам (см. параметр конфигурационного файла **FilesTypes**);
- ha - эвристический анализ файлов, поиск неизвестных вирусов.

Параметры действия определяют, какие манипуляции должны быть выполнены в отношении зараженных (или подозрительных) файлов:

- cu[d| m| r] - лечение зараженных файлов. Дополнительные параметры: d - удаление, m - перемещение, r - переименование зараженных файлов;
- ic[d| m| r] - действия для неизлечимых файлов: d - удаление, m - перемещение, r - переименование неизлечимых файлов;
- sp[d| m| r] - действия для подозрительных файлов: d - удаление, m - перемещение, r - переименование подозрительных файлов;
- adw[d| m| r| i] - действия для файлов, содержащих рекламные программы: d - удаление, m - перемещение, r - переименование, i - игнорирование;
- dls[d| m| r| i] - действия для файлов, содержащих программы дозвона: d - удаление, m - перемещение, r - переименование, i - игнорирование;
- jok[d| m| r| i] - действия для файлов, содержащих программы-шутки: d - удаление, m - перемещение, r - переименование, i - игнорирование;
- rsk[d| m| r| i] - действия для файлов, содержащих потенциально опасные программы: d - удаление, m -



перемещение, r – переименование, i – игнорирование;

- hck[d|m|r|i] – действия для файлов, содержащих программы, используемые для взлома: d – удаление, m – перемещение, r – переименование, i – игнорирование.

Параметры интерфейса определяют условия вывода результатов работы программы:

- v, version – вывод информации о версии продукта и версии антивирусного ядра;
- ki – вывод информации о ключе и его владельце (только в кодировке UTF8);
- foreground[yes|no] – запуск **Сканера** в приоритетном или в фоновом режиме;
- ot – вывод информации на stdout, т.е стандартный вывод;
- oq – отключение вывода информации;
- ok – вывод сообщения Ok для не зараженных вирусами файлов;
- log=<путь к файлу> – запись отчета о работе в указанный файл;
- ini=<путь к файлу> – использование альтернативного конфигурационного файла;
- lng=<путь к файлу> – использование альтернативного языкового файла. Если во время установки был выбран английский язык интерфейса, то для вывода сообщений на русском языке в качестве такого файла следует указать ru_scanner.dwl;
- -a=<адрес Агента> – запуск **Сканера** в режиме центральной защиты;
- --only-key – при запуске **Сканер** получает от **Агента** только лицензионный ключевой файл.

Некоторые из параметров отменяют соответствующее им действие, если оканчиваются символом "-" (дефис). К ним принадлежат параметры:



```
-ar -cu -ha -ic -fl -ml -ok -sd -sp
```

Например, при запуске **Сканера** командой вида:

```
$ drweb <путь> -ha-
```

проверка будет производиться без эвристического анализа файлов, который обычно по умолчанию включен.

Если не производились действия по перенастройке программы, то по умолчанию (т.е. без отдельного указания параметров), **Сканер** запускается с параметрами:

```
-ar -ha -fl- -ml -sd
```

Этот набор параметров по умолчанию (включающий проверку архивов и упакованных файлов, файлов почтовых программ, рекурсивный поиск, эвристический анализ и т.д.) достаточно целесообразен для целей диагностики и может использоваться в большинстве типичных случаев. Если какой-либо из параметров по умолчанию не нужен в конкретной ситуации, его можно отключить, указав после него символ "-" (дефис), как это было показано выше на примере параметра `-ha` (эвристический анализ).

Следует добавить, что отключение проверки архивированных и упакованных файлов резко снижает уровень антивирусной защиты, т.к. именно в виде архивов (часто самораспаковывающихся) распространяются файловые вирусы в виде почтовых вложений. Документы прикладных программ, потенциально подверженные заражению макровирусами (Word, Excel и др.), также обычно пересылаются по электронной почте в архивированном и упакованном виде.

При запуске **Сканера** с параметрами по умолчанию не осуществляется лечение зараженных файлов. Не предусмотрены также действия в отношении неизлечимых файлов и подозрительных файлов. Все эти действия требуют указания дополнительных параметров командной строки - параметров действия.

Наборы параметров действия могут различаться в каждом конкретном случае, однако обычно представляются



целесообразными следующие:

- `cu` – лечение зараженных файлов и системных областей, без удаления, перемещения или переименования зараженных файлов;
- `icd` – удаление неизлечимых файлов;
- `spm` – перемещение подозрительных файлов;
- `spr` – переименование подозрительных файлов.

Запуск **Сканера** с параметром лечения означает, что программа предпримет попытку восстановить состояние зараженного объекта. Это возможно только тогда, когда обнаружен известный вирус, причем необходимые инструкции по излечению имеются в вирусных базах, однако и в этих случаях попытка излечения может не быть успешной, например, если зараженный файл уже серьезно поврежден.

Если при проверке архивов в их составе были обнаружены зараженные файлы, лечение последних, как и удаление, перемещение или переименование, не производится. Для уничтожения вирусов в таких объектах архивы должны быть вручную распакованы соответствующими программными средствами, желательно, в отдельную директорию, которая и будет указана как аргумент при повторном запуске **Сканера**.

При запуске с параметром удаления программа уничтожит зараженный файл на диске. Этот параметр целесообразен для неизлечимых (необратимо поврежденных вирусом) файлов.

Параметр переименования вызывает замену расширения имени файла на некое установленное (по умолчанию `*.###`, т.е. первый символ расширения заменяется символом "#"). Этот параметр целесообразно применять для файлов других ОС, выявленных при эвристическом анализе как подозрительные. Переименование сделает невозможным случайный запуск исполняемых модулей в этих системах или загрузку зараженных документов приложений без дальнейшей проверки и таким образом предотвратит заражение возможным вирусом и дальнейшее его распространение.

Параметр перемещения переместит зараженный (или



подозрительный) файл в предназначенную для этого директорию карантина (по умолчанию `%var_dir/infected/`). Пока он имеет чисто теоретическое значение: для файлов других ОС перемещение не имеет смысла, т.к. они не могут нанести вреда UNIX системе, перемещение же подозрительных файлов самой UNIX системы может вызвать ошибки в работе системы, вплоть до полного ее отказа.

В результате форма запуска **Сканера** для повседневного использования представляется следующей:

```
$ drweb <путь> -cu -icd -spm -ar -ha -fl-  
-ml -sd
```

Такая команда может быть сохранена в виде текстового файла, который затем с помощью команды:

```
# chmod a+x [имя файла]
```

может быть оформлен как сценарий командной оболочки или серия сценариев для различных ситуаций. Однако набор параметров по умолчанию может быть изменен и при настройке **Сканера**, о чем говорится в следующем разделе.



Настройки

Разумеется, можно использовать **Сканер** с настройками по умолчанию, но значительно удобнее настроить его для соответствия конкретным требованиям и условиям эксплуатации. Настройки **Сканера** хранятся в конфигурационном файле программы (по умолчанию `drweb32.ini`), который размещается в директории

`%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске **Сканера**, например:

```
$ %bin_dir/drweb -ini=%bin_dir/etc/drweb.ini
```

Устройство конфигурационного файла и краткое описание его параметров приведены в разделе [Конфигурационные файлы](#).

Секция [Scanner]

EnginePath = { путь к файлу, обычное расширение dll}	Расположение модуля <code>drweb32.dll</code> (антивирусное ядро). Этот параметр также используется модулем обновления. <u>Значение по умолчанию:</u> EnginePath = <code>%bin_dir/lib/drweb32.dll</code>
VirusBase = { список путей (масок) к файлам, обычное расширение vdb}	Маски для подключаемых вирусных баз. Этот параметр также используется модулем обновления. Допустимо перечисление нескольких масок. <u>Значение по умолчанию:</u> VirusBase = <code>%var_dir/bases/*.vdb,%var_dir/bases/*.VDB</code>
UpdatePath = { путь к директории}	Этот параметр используется модулем обновления (<code>update.pl</code>) и должен быть задан обязательно.



	<p><u>Значение по умолчанию:</u></p> <p>UpdatePath = %var_dir/updates/</p>
<p>TempPath = { путь к директории}</p>	<p>Эта директория используется антивирусным ядром для создания временных файлов. При нормальной работе директория практически не используется, она нужна для распаковки некоторых видов архивов, или когда в системе не хватает памяти.</p> <p><u>Значение по умолчанию:</u></p> <p>TempPath = /tmp/</p>
<p>LngFileName = { путь к файлу языковых ресурсов, обычное расширение dwl}</p>	<p>Расположение файла языковых ресурсов.</p> <p><u>Значение по умолчанию:</u></p> <p>LngFileName = %bin_dir/lib/ru_scanner.dwl</p>
<p>Key = { путь к ключевому файлу, обычное расширение key}</p>	<p>Расположение ключевого файла (лицензионного или демонстрационного).</p> <p><u>Значение по умолчанию:</u></p> <p>Key = %bin_dir/drweb32.key</p>
<p>OutputMode = {Terminal Quiet}</p>	<p>Режим вывода информации при запуске: Terminal - вывод на консоль, Quiet — отменяет вывод.</p> <p><u>Значение по умолчанию:</u></p> <p>OutputMode = Terminal</p>



<p>HeuristicAnalysis = { Yes No }</p>	<p>Включение использования эвристического анализатора. Эвристический анализ делает возможным обнаружение неизвестных вирусов по априорным соображениям об устройстве вирусного кода. Особенностью этого типа поиска вирусов является вероятностный характер обнаружения заражения, что позволяет говорить не о зараженных, а о подозрительных объектах. При отключении этого режима осуществляется только поиск известных вирусов по вирусным базам "Доктор Веб". Целый класс программ ввиду использования сходного с вирусами кода может вызывать ложные срабатывания эвристического анализатора. Кроме того, данный режим может незначительно увеличить время проверки. Данные обстоятельства могут быть доводами в пользу отключения эвристического анализа. Вместе с тем, включение этого типа анализа увеличивает надежность антивирусной защиты. Все файлы, обнаруженные эвристическим анализатором, лучше всего отправить разработчикам через сайт http://vms.drweb.com/sendvirus/. Отправку подозрительных файлов рекомендуется производить следующим образом: запаковать файл в архив с паролем, пароль сообщить в теле письма, при этом желательно приложить отчет Сканера.</p> <p><u>Значение по умолчанию:</u></p> <p>HeuristicAnalysis = Yes</p>
<p>ScanPriority = { значение }</p>	<p>Приоритет работы Сканера. Значение параметра должно быть в диапазоне от высшего значения (-20) до низшего (19 для Linux, 20 для остальных ОС).</p> <p><u>Значение по умолчанию:</u></p>



	<code>ScanPriority = 0</code>
<code>FileTypes =</code> { список расширений}	<p>Типы файлов, которые будут проверяться при сканировании по типу, т.е. когда параметр <code>ScanFiles</code> (см. ниже) имеет значение <code>ByType</code>. Допускаются символы "*" и "?". Допускается несколько строк с этим параметром; в этом случае задаваемые списки суммируются.</p> <p><u>Значение по умолчанию:</u></p> <pre>FileTypes = EXE, COM, SYS, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, VXD, 386, DLL, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, AR?, ZIP, R??, PP?, OBJ, LIB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SHS, SHB, PIF, SO, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, BMP, MPP, OCX, DVB, CPY, MSG, EML</pre>
<code>FileTypesWarnings</code> = { Yes No}	<p>Предупреждение о файлах неизвестных типов.</p> <p><u>Значение по умолчанию:</u></p> <p><code>FileTypesWarnings = Yes</code></p>
<code>ScanFiles = { All </code> <code>ByType}</code>	<p>Дополнительное ограничение на файлы, подлежащие проверке. При задании значения <code>ByType</code> учитываются расширения файлов, значения которых заданы или по умолчанию, или в параметре (параметрах) <code>FileTypes</code>.</p> <p>Внутри почтовых файлов всегда действует режим <code>All</code>. Значение <code>ByType</code> может быть использовано только в режимах локального сканирования.</p> <p><u>Значение по умолчанию:</u></p>



	ScanFiles = All
ScanSubDirectories = { Yes No }	Проверка содержимого поддиректорий. <u>Значение по умолчанию:</u> ScanSubDirectories = Yes
CheckArchives = { Yes No }	Распаковка архивов форматов ZIP (WinZip, InfoZIP и др.), RAR, ARJ, TAR, GZIP, CAB и др. <u>Значение по умолчанию:</u> CheckArchives = Yes
CheckEMailFiles = { Yes No }	Проверка файлов в почтовых (e-mail) форматах. <u>Значение по умолчанию:</u> CheckEMailFiles = Yes
ExcludePaths = { список путей (масок) для исключения из проверки }	Маски для тех файлов, которые не должны проверяться. <u>Значение по умолчанию:</u> ExcludePaths = /proc, /sys, /dev
FollowLinks = { Yes No }	Следование символическим ссылкам при сканировании. <u>Значение по умолчанию:</u> FollowLinks = No



<pre>RenameFilesTo = { маска}</pre>	<p>Маска для переименования файлов, если для данной ситуации (зараженный или подозрительный файл) задано действие Rename. К примеру, если задана маска #??, то первая буква расширения файла будет заменена на символ #, а остальные буквы будут сохранены. Если файл не имел расширения, оно будет состоять из одного символа #.</p> <p><u>Значение по умолчанию:</u></p> <pre>RenameFilesTo = #??</pre>
<pre>MoveFilesTo = { путь к директории}</pre>	<p>Путь к директории карантина.</p> <p><u>Значение по умолчанию:</u></p> <pre>MoveFilesTo = %var_dir/ infected/</pre>
<pre>EnableDeleteArchive Action = { Yes No}</pre>	<p>Применение действия Delete (Удалить) для составных объектов (архивов, почтовых ящиков, html-страниц), если они содержат зараженные объекты. Важно понимать, что будет удален весь составной объект, т.е. весь архив или весь почтовый ящик, а не только зараженное письмо или элемент архива.</p> <p><u>Значение по умолчанию:</u></p> <pre>EnableDeleteArchiveAction = No</pre>
<pre>InfectedFiles = { Report Cure Delete Move Rename Ignore}</pre>	<p>Задаёт реакцию на обнаружение файла, зараженного известным вирусом. Допустимые значения параметра:</p> <ul style="list-style-type: none">• Report - только вывести информацию в отчет;• Cure - попытаться вылечить объект (только для параметра InfectedFiles);• Delete - удалить зараженный файл;



	<ul style="list-style-type: none">• Move - переместить файл в директорию, заданную параметром MoveFilesTo;• Rename - переименовать файл, используя маску, заданную параметром RenameFilesTo;• Ignore – пропустить файл. <p>Удаление и перемещение, заданное в связи с обнаружением зараженных объектов в архивах, контейнерах и почтовых ящиках, применяется к соответствующему архиву, контейнеру или почтовому ящику целиком.</p> <p><u>Значение по умолчанию:</u></p> <p>InfectedFiles = Report</p>
--	---

Далее указаны параметры, аналогичные параметру **InfectedFiles** и задающие реакцию программы на обнаружение тех или иных объектов. Для них предусмотрены те же возможные значения, что и для параметра **InfectedFiles**, кроме значения Cure:

SuspiciousFiles = { Report Delete Move Rename Ignore}	Возможно, файл заражен неизвестным вирусом <u>Значение по умолчанию:</u> SuspiciousFiles = Report
---	--

IncurableFiles = { Report Delete Move Rename Ignore}	Файл заражен и не может быть вылечен (имеет смысл, только если InfectedFiles = Cure) <u>Значение по умолчанию:</u> IncurableFiles = Report
--	--

ActionAdware = { Report Delete Move Rename Ignore}	Файл содержит программу для показа рекламы (adware). <u>Значение по умолчанию:</u> ActionAdware = Report
--	---



<pre>ActionDialers = { Report Delete Move Rename Ignore}</pre>	<p>Файл содержит программу автоматического дозвона.</p> <p><u>Значение по умолчанию:</u></p> <pre>ActionDialers = Report</pre>
<pre>ActionJokes = { Report Delete Move Rename Ignore}</pre>	<p>Файл содержит программу-шутку, которая может пугать или раздражать пользователя</p> <p><u>Значение по умолчанию:</u></p> <pre>ActionJokes = Report</pre>
<pre>ActionRiskware = { Report Delete Move Rename Ignore}</pre>	<p>Файл содержит потенциально опасную программу, которая может быть использована не только ее владельцем, но и злоумышленниками.</p> <p><u>Значение по умолчанию:</u></p> <pre>ActionRiskware = Report</pre>
<pre>ActionHacktools = { Report Delete Move Rename Ignore}</pre>	<p>Файл содержит программу, которая используется для взлома компьютеров.</p> <p><u>Значение по умолчанию:</u></p> <pre>ActionHacktools = Report</pre>
<pre>ActionInfectedMail = { Report Delete Move Rename Ignore}</pre>	<p>Сообщение или почтовый ящик содержат зараженный объект.</p> <p><u>Значение по умолчанию:</u></p> <pre>ActionInfectedMail = Report</pre>
<pre>ActionInfectedArchive = { Report Delete Move Rename Ignore}</pre>	<p>Архив (ZIP, TAR, RAR и др.) содержит зараженный файл.</p> <p><u>Значение по умолчанию:</u></p> <pre>ActionInfectedArchive = Report</pre>
<pre>ActionInfectedContainer</pre>	<p>Контейнер (OLE, HTML, PowerPoint и др.) содержит зараженный объект.</p>



```
iner = { Report |  
Delete | Move |  
Rename | Ignore}
```

Значение по умолчанию:

```
ActionInfectedContainer =  
Report
```

Параметры регистрации событий:

```
LogFileName = { имя  
файла}
```

Имя файла отчета. В качестве имени можно указать `syslog`, тогда отчет будет вестись средствами системного сервиса `syslogd`. При использовании `syslogd` нужно обратить внимание на параметры **SyslogFacility** и **SyslogPriority** (см. ниже). Поскольку `syslogd` имеет несколько файлов для протоколирования разных событий и разных степеней их важности, то, основываясь на этих двух параметрах и содержанием конфигурационного файла `syslogd` (обычно `/etc/syslogd.conf`), можно определить, куда будет писаться отчет программы.

Значение по умолчанию:

```
LogFileName = syslog
```

```
SyslogFacility =  
{ Daemon | Local0 ..  
Local7 | Kern |  
User | Mail}
```

Тип записи при использовании системного сервиса `syslogd`.

Значение по умолчанию:

```
SyslogFacility = Daemon
```

```
SyslogPriority =  
{ Alert | Warning |  
Notice | Info |  
Error}
```

Приоритет записи при использовании системного сервиса `syslogd`.

Значение по умолчанию:

```
SyslogPriority = Info
```



LimitLog = { Yes No}	<p>Ограничение размера файла отчета. Параметр не влияет на работу программы при значении LogFile = syslog. Ограничение размера файла отчета реализуется следующим образом: при запуске Сканер проверяет размер файла отчета, и если он превышает значение, заданное в параметре MaxLogSize, файл отчета стирается и ведение отчета начинается с нуля.</p> <p><u>Значение по умолчанию:</u></p> LimitLog = No
MaxLogSize = { значение в КБайтах}	<p>Максимальный размер файла отчета. Имеет смысл только если LimitLog = Yes. Если указано значение 0, размер файла отчета проверяться не будет.</p> <p><u>Значение по умолчанию:</u></p> MaxLogSize = 512
LogScanned = { Yes No}	<p>Вывод в файл отчета информации обо всех проверяемых объектах, независимо от того, обнаружены вирусы или нет.</p> <p><u>Значение по умолчанию:</u></p> LogScanned = Yes
LogPacked = { Yes No}	<p>Вывод в файл отчета дополнительной информации о файлах, упакованных утилитами DIET, PKLITE и др.</p> <p><u>Значение по умолчанию:</u></p> LogPacked = Yes
LogArchived = { Yes No}	<p>Вывод в файл отчета дополнительной информации об архиваторах.</p> <p><u>Значение по умолчанию:</u></p>



	LogArchived = Yes
LogTime = { Yes No }	Вывод в файл отчета времени каждой записи. Параметр не имеет смысла, если LogFileName = syslog. <u>Значение по умолчанию:</u> LogTime = Yes
LogStatistics = { Yes No }	Запись в отчет суммарной статистики задания для сканирования. <u>Значение по умолчанию:</u> LogStatistics = Yes
RecodeNonprintable = { Yes No }	Перекодировка при выводе в файл отчета символов, не являющихся отображаемыми для данного терминала (см. следующие два параметра). <u>Значение по умолчанию:</u> RecodeNonprintable = Yes
RecodeMode = { Replace QuotedPrintable }	При RecodeNonprintable = Yes задает метод перекодировки неотображаемых символов. При RecodeMode = Replace все такие символы заменяются на значение параметра RecodeChar (см. ниже). При RecodeMode = QuotedPrintable производится перекодировка неотображаемых символов в формат Quoted Printable. <u>Значение по умолчанию:</u> RecodeMode = QuotedPrintable
RecodeChar = { "?" "_" ... }	При RecodeMode = Replace задает символ, на который будут заменены все неотображаемые символы.



Значение по умолчанию:

RecodeChar = "?"

Следующие параметры могут быть использованы для уменьшения времени проверки архивов за счет отказа от проверки некоторых объектов в архиве.

MaxCompressionRatio
= { значение }

Максимальный коэффициент сжатия, т. е. отношение длины файла в распакованном виде к длине файла в упакованном виде (внутри архива). Если коэффициент превышает данное значение, файл не будет извлечен и, соответственно, не будет проверен. Письмо с таким файлом воспринимается программой как "почтовая бомба".

Параметр может принимать только натуральные значения. Если указано значение 0, проверка коэффициента сжатия проводиться не будет.

Значение по умолчанию:

MaxCompressionRatio = 5000

CompressionCheckThreshold = { значение в КБайтах }

Минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия (если это предписано параметром **MaxCompressionRatio**).

Значение по умолчанию:

CompressionCheckThreshold = 1024

MaxFileSizeToExtract
= { значение в КБайтах }

Максимальный размер файла, извлекаемого из архива. Если размер файла внутри архива превышает это значение, он будет пропущен. Письмо с таким файлом воспринимается программой как "почтовая бомба".



	<p><u>Значение по умолчанию:</u></p> <p>MaxFileSizeToExtract = 500000</p>
<p>MaxArchiveLevel = { значение }</p>	<p>Максимальный уровень вложенности архивов (когда архив вложен в архив, который тоже вложен в архив и т.д.). При превышении этого уровня архив будет пропущен (не будет проверен). Письмо с таким файлом воспринимается программой как "почтовая бомба".</p> <p>Если указано значение 0, уровень вложенности проверяемых архивов проверяться не будет.</p> <p><u>Значение по умолчанию:</u></p> <p>MaxArchiveLevel = 8</p>
<p>MaximumMemoryAllocationSize = { значение в МБайтах }</p>	<p>Максимальный размер памяти, выделяемой Сканером при сканировании одного файла (в мегабайтах). Если установлено значение 0, размер выделяемой памяти не ограничен.</p> <p><u>Значение по умолчанию:</u></p> <p>MaximumMemoryAllocationSize = 0</p>
<p>ScannerScanTimeout = { время в секундах }</p>	<p>Максимальное время сканирования одного файла (в секундах). Если установлено значение 0, время сканирования одного файла не ограничено.</p> <p><u>Значение по умолчанию:</u></p> <p>ScannerScanTimeout = 0</p>



```
MaxBasesObsolescencePeriod = { время в часах}
```

Максимальный период времени (в часах) с момента последнего обновления, в течение которого вирусные базы считаются "свежими". По истечении этого времени в консоли выводится уведомление о том, что базы устарели. Если установлено значение 0, "свежесть" вирусных баз не проверяется.

Значение по умолчанию:

```
MaxBasesObsolescencePeriod = 24
```

```
ControlAgent = { адрес сокета Агента}
```

Адрес сокета **Агента** в формате ТИП: АДРЕС, где ТИП может принимать значения inet (для TCP-сокетов), local и unix (для UNIX сокетов).

Пример:

```
ControlAgent = inet:4040@127.0.0.1,local:/var/drweb/ipc/.agent
```

Сканер получает от **Агента** ключ и конфигурационный файл (если в качестве значения параметра **OnlyKey** задано No).

Значение по умолчанию:

```
ControlAgent = local:%var_dir/ipc/.agent
```

```
OnlyKey = { Yes | No}
```

Подключение возможности запросить только ключевой файл от **Агента**, не запрашивая конфигурацию. При этом будет использоваться локальный конфигурационный файл.



Если указан адрес сокета Агента и значение параметра OnlyKey установлено в No, Агенту будет отправляться статистика работы Сканера (после сканирования каждого файла Сканер будет отправлять информацию Агенту).
<u>Значение по умолчанию:</u>
OnlyKey = No

Запуск

Запуск **Dr.Web Scanner** осуществляется командой:

```
$ %bin_dir/drweb
```

В том случае, если директория `%bin_dir` внесена в переменную окружения командной оболочки PATH, запуск осуществляется из произвольной директории. Следует учесть, что последний вариант не рекомендуется из соображений безопасности, равно как и создание символической ссылки на исполняемый файл `drweb` в какой-либо из директорий типа `/bin/`, `/usr/bin/` и т.д.

Сканер может быть запущен как с правами администратора, так и с правами обычного пользователя. Разумеется, в последнем случае проверка будет выполняться только в тех директориях, к которым пользователь имеет доступ на чтение, а лечение зараженных файлов будет производиться только в директориях, в которых он имеет право на запись (обычно это домашняя директория пользователя, `$HOME`). Существуют и другие ограничения при запуске **Сканера** в пользовательском режиме, например, на перемещение и переименование зараженных файлов.

После запуска **Сканера** на экран выводится заставка с названием программы и ее целевой платформы, номером



версии и датой ее выпуска, контактными координатами. Далее выводится сообщение о регистрационных данных пользователя и загрузке вирусных баз "Доктор Веб", включая их обновления, если они были установлены:

```
Dr. Web (R) Сканер для Linux v6.0.1 (19 февраля 2010)
```

```
Copyright (c) Игорь Данилов, 1992-2010
```

```
"Доктор Веб", Москва, Российская Федерация.
```

```
Техподдержка: http://support.drweb.com/
```

```
Отдел продаж: http://buy.drweb.com/
```

```
Версия оболочки: 6.0.1.10060 <API:2.2>
```

```
Антивирусное ядро: 6.0.1.9170 <API:2.2>
```

```
Загрузка /var/drweb/bases/drwtoday.vdb - Ok,  
вирусных записей: 1533
```

```
Загрузка /var/drweb/bases/drw60012.vdb - Ok,  
вирусных записей: 3511
```

```
-----  
Загрузка /var/drweb/bases/drw60000.vdb - Ok,  
вирусных записей: 1194
```

```
Загрузка /var/drweb/bases/dwn60001.vdb - Ok,  
вирусных записей: 840
```

```
Загрузка /var/drweb/bases/drwebase.vdb - Ok,  
вирусных записей: 78674
```

```
Загрузка /var/drweb/bases/drwrisky.vdb - Ok,  
вирусных записей: 1271
```

```
Загрузка /var/drweb/bases/drwnasty.vdb - Ok,  
вирусных записей: 4867
```

```
Вирусных записей: 538681
```

```
Ключевой файл: /opt/drweb/drweb32.key
```

```
Номер лицензионного ключа: XXXXXXXXXXXX
```



Дата активации лицензионного ключа: XXXX-XX-XX

Дата истечения действия лицензионного ключа:
XXXX-XX-XX

После этого возвращается приглашение командной оболочки.

Все иные действия по обнаружению и обезвреживанию вирусов требуют применения параметров командной строки.



Антивирусный модуль Dr.Web Daemon

Dr.Web Daemon - постоянно загруженный антивирусный модуль, который позволяет по запросу от других компонентов комплекса проверять файлы на диске или данные, переданные по сокету. Запросы осуществляются по специальному протоколу через UNIX сокеты или TCP-сокеты. **Dr.Web Daemon** использует то же ядро и вирусные базы, что и **Dr.Web Scanner**, и способен обнаруживать и лечить все известные вирусы.

Dr.Web Daemon всегда готов к выполнению своих функций и имеет понятный и доступный протокол для запросов сканирования, что делает его подходящим компонентом для создания антивирусного фильтра для файловых серверов. Программный комплекс **Dr.Web для Novell Storage Services** является готовым решением по интеграции **Dr.Web Daemon** с файловой системой NSS.

Параметры командной строки

Как и для любой UNIX программы, для **Демона Dr.Web** предусматриваются параметры командной строки. Они отделяются от указания пути пробелом и предваряются символом "-" (дефис). Полный список можно получить, запустив программу `drwebd` с параметрами `-?`, `-h` или `-help`.

Параметры командной строки **Демона Dr.Web**:

- `-ini=<путь к файлу>` — использование альтернативного конфигурационного файла;
- `--foreground=<yes|no>` — задание режима работы **Демона** при запуске. Если выбрано значение `Yes`, то



Демон будет работать как приоритетная задача; при значении No **Демон** будет работать в фоновом режиме;

- `--check-only` <параметры командной строки для проверки> — проверка правильности конфигурации **Демона** при запуске. Если указаны какие-либо параметры командной строки, то правильность задаваемых с их помощью значений также будет проверена;
- `-a=<адрес Агента>` — запуск **Демона** в режиме центральной защиты;
- `--only-key` — при запуске **Демон** получает от **Агента** только лицензионный ключевой файл.

Запуск

В процессе загрузки **Демона** осуществляются следующие действия:

- поиск и загрузка конфигурационного файла. Если конфигурационный файл не найден, загрузка **Демона** прекращается. Путь к конфигурационному файлу может быть задан при запуске параметром командной строки `-ini: {путь/к/drweb32.ini}`, иначе будет использовано значение по умолчанию (`%etc_dir/drweb32.ini`). При загрузке проверяется допустимость некоторых параметров и, если значение параметра недопустимо, берется значение по умолчанию;
- создается файл отчета. Директория с файлом отчета должна быть доступна на запись пользователю, с чьими правами работает **Демон**. Директория по умолчанию `/var/log/` недоступна пользователям на запись. Поэтому, если задано значение параметра `User`, необходимо также указать путь к альтернативной директории для хранения отчётов в значении параметра `LogFile` `LogFileName`;
- производится загрузка ключевого файла по пути, указанному в конфигурационном файле. Если ключевой файл не найден, загрузка **Демона** прекращается;



- если задан параметр **User**, **Демон** пытается изменить свои права;
- производится загрузка антивирусного ядра (drweb32.dll). Если антивирусное ядро не найдено (ошибки в конфигурационном файле) или повреждено, загрузка **Демона** прекращается;
- загружаются вирусные базы. Поиск вирусных баз осуществляется по заданным в конфигурационном файле путям, порядок загрузки вирусных баз не регламентирован. Если вирусные базы повреждены или отсутствуют, загрузка **Демона** продолжается;
- **Демон** отключается от терминала, поэтому сообщения о дальнейших проблемах не могут быть выведены на терминал и выводятся только в файл отчета;
- создается сокет, в случае использования TCP-сокетов, возможно, не один. Если какой-либо TCP-сокет создать не удалось, загрузка **Демона** продолжается. В случае использования UNIX сокета следует убедиться, что директория, его содержащая, доступна на запись и чтение пользователю, с чьими правами работает **Демон**. Для пользователей, с правами которых будут работать интеграционные модули, директория должна быть доступна на выполнение, а сам файл сокета — на запись и чтение. Директория по умолчанию /var/run/ недоступна пользователям на запись и выполнение. Поэтому, если задано значение параметра **User**, необходимо также указать путь к альтернативной директории для сокетов в значении параметра **Socket**. Если UNIX сокет создать не удалось, загрузка **Демона** прекращается;



- после этого создается PID-файл, в котором хранится информация об идентификаторе процесса **Демона** и о транспортных адресах, по которым доступен **Демон**. Директория с PID-файлом должна быть доступна на запись пользователю, с чьими правами работает **Демон**. Директория по умолчанию `/var/run/` недоступна пользователям на запись и выполнение. Поэтому, если задано значение параметра `User`, необходимо также указать путь к альтернативной директории для PID-файла в значении параметра `PidFile`. Если создать PID-файл не удалось, загрузка **Демона** прекращается.

Проверка работоспособности Dr.Web Daemon

Если в ходе загрузки не возникло проблем, **Демон** готов к работе. Для проверки корректности загрузки **Демона** можно узнать, созданы ли необходимые для его работы сокеты. Для этого используется команда:

```
$ netstat -a
```

В случае TCP-сокетов:

```
--- cut ---
```

```
Active Internet connections (servers and established)
```

```
Proto Recv-Q Send-Q Local Address Foreign Address State
```

```
tcp 0 0 localhost:3000 *:* LISTEN
```

```
raw 0 0 *:icmp *:* 7
```

```
raw 0 0 *:tcp *:* 7
```

```
Active UNIX domain sockets (servers and established)
```

```
Proto RefCnt Flags Type State I-Node Path
unix 0 [ ACC ] STREAM LISTENING 384 /dev/gpmctl
```



```
unix 0 [ ] STREAM CONNECTED 190 @0000001b
unix 1 [ ] STREAM CONNECTED 1091
@00000031
unix 0 [ ACC ] STREAM LISTENING 403 /tmp/.
font-unix/fs7100
unix 4 [ ] DGRAM 293 /dev/log
unix 1 [ ] STREAM CONNECTED 1092 /dev/
gpmctl
unix 0 [ ] DGRAM 450
unix 0 [ ] DGRAM 433
unix 0 [ ] DGRAM 416
unix 0 [ ] DGRAM 308
--- cut ---
```

В случае UNIX сокетов:

```
--- cut ---
Active Internet connections (servers and
established)
Proto Recv-Q Send-Q Local Address Foreign
Address State
raw 0 0 *:icmp *:* 7
raw 0 0 *:tcp *:* 7
Active UNIX domain sockets (servers and
established)
Proto RefCnt Flags Type State I-Node Path
unix 0 [ ACC ] STREAM LISTENING 384 /dev/
gpmctl
unix 0 [ ] STREAM CONNECTED 190 @0000001b
unix 1 [ ] STREAM CONNECTED 1091 @00000031
unix 0 [ ACC ] STREAM LISTENING 1127 %
var_dir/.daemon
```



```
unix 0 [ ACC ] STREAM LISTENING 403 /tmp/.  
font-unix/fs7100  
unix 4 [ ] DGRAM 293 /dev/log  
unix 1 [ ] STREAM CONNECTED 1092 /dev/  
gpmctl  
unix 0 [ ] DGRAM 450  
unix 0 [ ] DGRAM 433  
unix 0 [ ] DGRAM 416  
unix 0 [ ] DGRAM 308  
--- cut ---
```

Если созданные сокеты не появились в списке, значит, имеются проблемы загрузки.

Для проверки работоспособности **Демона** можно использовать консольный клиент **Демона** (`drwebdc`), запустив его для получения служебной информации о **Демоне**. Если запустить `drwebdc`, он выдаст список всех поддерживаемых параметров.

В случае TCP-сокета:

```
$ drwebdc -nHOSTNAME -pPORTNUM -sv -sb
```

В случае UNIX сокета:

```
$ drwebdc -uSOCKETFILE -sv -sb
```

На консоли появится информация, подобная следующей:

```
--- cut ---  
- Version: DrWeb Daemon 6.00  
- Loaded bases:  
Base /var/drweb/bases/drwtoday.vdb  
contains 5 records.  
Base /var/drweb/bases/drw60003.vdb  
contains 409 records.  
Base /var/drweb/bases/drw60002.vdb
```



```
contains 543 records.  
Base /var/drweb/bases/drwebase.vdb  
contains 51982 records.  
Base /var/drweb/bases/drw60001.vdb  
contains 364 records.  
Total 53303 virus-finding records.  
--- cut ---
```

Если этого не произошло, следует провести расширенную диагностику:

В случае TCP-сокета:

```
$ drwebdc -nHOSTNAME -pPORTNUM -sv -sb -v
```

В случае UNIX сокета:

```
$ drwebdc -uSOCKETFILE -sv -sb -v
```

Более подробный вывод может прояснить ситуацию:

```
dwlib: fd: connect() failed - Connection  
refused  
dwlib: tcp: connecting to 127.0.0.1:3300 -  
failed  
dwlib: cannot create connection with a DrWeb  
daemon  
ERROR: cannot retrieve daemon version  
Error -12
```

Проверить работоспособность **Демона** можно с помощью программы `eicar.com`, получаемой из входящего в дистрибутив файла `readme.eicar.rus` с помощью любого текстового редактора (см. указания об этом внутри самого файла).



В случае лицензии для файловых серверов:

Для TCP-сокета:

```
$ drwebdc -ИМЯ_УЗЛА -ПНОМЕР_ПОРТА  
eicar.com
```

Для UNIX сокета:

```
$ drwebdc -uФАЙЛ_СОКЕТА eicar.com
```

Результатом команды должно быть сообщение:

```
--- cut ---
```

```
Results: daemon return code 0x20
```

```
(known virus is found)
```

```
--- cut ---
```

Если его не появилось, проверьте в файле отчета **Демона** наличие записи о проверке этого файла. Если файл так и не был проверен, проведите расширенную диагностику (см. выше).

Если проверка файла прошла успешно, **Демон** находится в рабочем состоянии.

Обратите внимание, что **Демон** не может сканировать файлы размером больше 2 гигабайт. Такие файлы не будут отправляться на сканирование клиентами **Демона**.



При сканировании архивов больших размеров могут возникать ошибки, связанные с истечением времени ожидания. При возникновении таких ошибок увеличьте значения, указанные в параметрах `FileTimeout` и `SocketTimeout`.

Режимы проверки

Демон Dr.Web имеет два основных режима проверки:

- проверка фрагмента памяти, полученного из сокета;



- проверка файла на диске (локальное сканирование).

При использовании первого режима **Демон** получает данные для проверки из сокета — фактически, это некоторый фрагмент данных. Данный фрагмент может быть поименованным или нет, что отразится исключительно на форме записи в файле отчета **Демона**. Пример работы **Демона** в этом режиме приведен в предыдущем пункте: клиент читает файл и отправляет его **Демону** для проверки. **Демон** может проверять любой фрагмент данных, не обязательно файл.

Более эффективен режим, в котором **Демон** проверяет указанный файл на диске — локальное сканирование. Клиент (консольный клиент или фильтр для почты) сообщает **Демону** лишь путь к файлу, а не передает весь файл. Путь к проверяемому файлу задается относительно **Демона** (т.к. клиенты могут находиться на других машинах и т.д.). Этот режим обеспечивает большую производительность и упрощает создание рабочих схем с лечением (например, на файловых серверах).

Режим локального сканирования требует более тщательной настройки прав, т.к. **Демону** проверяемый файл должен быть доступен на чтение, а в случае почтовых файлов и использования действий Cure и Delete - необходимы и права на запись.

В корректно настроенной системе **Демону** в большинстве случаев не требуется прав администратора.

Обрабатываемые сигналы

Демон Dr.Web может принимать и обрабатывать следующие сигналы:

- SIGHUP — перезагрузка конфигурационного файла;
- SIGTERM — корректное завершение работы **Демона**;
- SIGKILL — принудительное завершение работы **Демона** (в случае проблем).



Файл отчета

Поскольку **Демон Dr.Web** является резидентной программой, информация о его работе может быть получена только из файла отчета. Файл отчета содержит подробности обработки каждого запроса на сканирование, полученного **Демоном**. Имя файла отчета указывается в значении параметра конфигурационного файла `LogFile`.

Демон может выводить данные об обработке запросов на сканирование в разные файлы, в зависимости от клиента, который выслал запрос. В параметре `ClientsLogs` конфигурационного файла можно указать отдельные файлы отчета (или назначить службу протоколирования `syslog`) для каждого из клиентских приложений **Dr.Web** (например, **Dr.Web для Novell Storage Services**).

Вне зависимости от параметра `ClientsLogs`, если клиентское приложение было распознано **Демоном**, результаты сканирования будут отмечены специальным префиксом при выводе в файл отчета. Возможны следующие префиксы:

- `<web>` - **Dr.Web ICAPD**;
- `<smb_spider>` - **Dr.Web Samba SpIDer**;
- `<mail>` - **Dr.Web MailD**;
- `<drwebdc>` - консольный клиент **Демона Dr.Web**;
- `<kerio>` - **Dr.Web для интернет-шлюзов Kerio**;
- `<lotus>` - **Dr.Web для IBM Lotus Domino**.



В операционной системе FreeBSD вывод на консоль **Демона** может быть перехвачен системной службой `syslog` и выведен в файл отчета посимвольно. Эта проблема проявляется если в конфигурационном файле `syslog.conf` установлен уровень протоколирования `*.info`.



Статистика пула процессов

Статистика пула процессов, который используется для обработки запросов на сканирование может быть выведена в файл отчета по сигналу SIGUSR1 (сигнал должен посылаться только родительскому процессу, для дочерних процессов SIGUSR1 приведет к завершению процесса) и при завершении работы **Демона**.

Пример вывода статистики пула процессов:

```
Fri Oct 15 19:47:51 2010 processes pool
statistics: min = 1 max = 1024 (auto) freetime
= 121 busy max = 1024 avg = 50.756950 requests
for new process = 94 (0.084305 num/sec)
creating fails = 0 max processing time = 40000
ms; avg = 118646 ms curr = 0 busy = 0
```

где:

`min` - минимальное количество процессов в пуле;
`max` - минимальное количество процессов в пуле;
`(auto)` - выводится, если ограничения пула процессов определяются автоматически;
`freetime` - максимальное время бездействия процесса в пуле;
`busy max` - максимальное количество одновременно занятых процессов, `avg` - среднее количество одновременно занятых процессов;
`requests for new process` - количество запросов на создание дополнительных процессов (в скобках приводится частота запросов в секунду);
`creating fails` - количество неудачных попыток создания процесса (обычно, по причине нехватки системных ресурсов);
`max processing time` - максимальное время обработки одного запроса в миллисекундах, `avg` - среднее время обработки одного запроса в миллисекундах;
`curr` - текущее общее количество процессов в пуле;



`busy` - текущее количество занятых процессов.

Настройки

Можно запустить **Демон** с настройками по умолчанию, но предпочтительнее настроить его в соответствии с требованиями и условиям эксплуатации. Конфигурационный файл `drweb32.ini` читается **ДЕМОНОМ** из директории `%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске **Демона**.

Устройство конфигурационного файла и краткое описание его параметров приведены в разделе [Конфигурационные файлы](#).

Секция [Daemon]

EnginePath = { путь к файлу, обычное расширение dll}	Расположение модуля <code>drweb32.dll</code> (антивирусное ядро). Этот параметр также используется модулем обновления. <u>Значение по умолчанию:</u> EnginePath = <code>%bin_dir/lib/drweb32.dll</code>
VirusBase = { список путей (масок) к файлам, обычное расширение vdb}	Маски для подключаемых вирусных баз. Этот параметр также используется модулем обновления. Допустимо перечисление нескольких масок. <u>Значение по умолчанию:</u> VirusBase = <code>%var_dir/bases/*.vdb,%var_dir/bases/*.VDB</code>
UpdatePath = { путь к директории}	Этот параметр используется модулем обновления (<code>update.pl</code>) и должен быть задан обязательно.



	<p><u>Значение по умолчанию:</u></p> <p>UpdatePath = %var_dir/updates/</p>
<p>TempPath = { путь к директории}</p>	<p>Эта директория используется антивирусным ядром для создания временных файлов. При нормальной работе директория практически не используется, она нужна для распаковки некоторых видов архивов или когда в системе не хватает памяти.</p> <p><u>Значение по умолчанию:</u></p> <p>TempPath = /tmp/</p>
<p>Key = { путь к ключевому файлу, обычное расширение key}</p>	<p>Расположение ключевого файла (лицензионного или демонстрационного). Ключевой файл может быть различным для Демона и для Сканера. Соответственно, при необходимости нужно изменить настройки данного параметра. Параметр может задаваться несколько раз, указывая несколько лицензионных ключевых файлов. В таком случае Демон пытается объединить права, предоставляемые различными лицензиями.</p> <p><u>Значение по умолчанию:</u></p> <p>Key = %bin_dir/drweb32.key</p>
<p>MailAddressesList = { путь к файлу}</p>	<p>Параметр используется только в случае адресной лицензии на 15 или 30 адресов. В задаваемом параметром файле должен быть задан список адресов (но не более количества, заданного в лицензии), которые будут проверяться (входящая и исходящая корреспонденция). Формат файла - один адрес на строке. Алиасы любого вида считаются отдельными адресами.</p> <p><u>Значение по умолчанию:</u></p>



	<code>MailAddressesList = %etc_dir/ email.ini</code>
<code>OutputMode = {Terminal Quiet}</code>	<p>Режим вывода информации при запуске: Terminal - вывод на консоль, Quiet - отменяет вывод.</p> <p><u>Значение по умолчанию:</u></p> <code>OutputMode = Terminal</code>
<code>RunForeground = {Yes No}</code>	<p>Значение Yes запрещает Демону переходить в режим демона, т.е. становиться фоновым процессом без управляющего терминала. Эта возможность может быть использована некоторыми средствами мониторинга (например, Монитором).</p> <p><u>Значение по умолчанию:</u></p> <code>RunForeground = No</code>
<code>User = {имя пользователя}</code>	<p>Пользователь, с правами которого работает Демон. Рекомендуется завести в системе специального пользователя drweb, который будет использоваться Демоном и некоторыми фильтрами. Использовать Демон с правами root нежелательно, хотя такое решение значительно проще настраивается. Значение этого параметра не изменяется во время процедуры перечитывания конфигурации "на лету" (обработки сигнала SIGHUP).</p> <p><u>Значение по умолчанию:</u></p> <code>User = drweb</code>



PidFile = { путь к файлу }

Имя файла, в который при запуске **Демона** записывается информация об идентификаторе его процесса (`pid`), а также сокет (если параметр **Socket** задает использование UNIX сокета) или номер порта (если параметр **Socket** задает использование TCP-сокета). Если задано более одного параметра **Socket**, в данном файле будет присутствовать информация обо всех заданных сокетах (по одному в строке).

Значение по умолчанию:

```
PidFile = %var_dir/run/drwebd.  
pid
```

BusyFile = { путь к файлу }

Данный файл сигнализирует о занятости **Демона**: он создается сканирующей "копией" **Демона** при получении команды и уничтожается после передачи результата ее выполнения. Имя файла, создаваемого каждой "копией" **Демона**, дополняется точкой и ASCII-представлением `pid` (например, `/var/run/drwebd.bsy.123456`).

Значение по умолчанию:

```
BusyFile = %var_dir/run/  
drwebd.bsy
```

ProcessesPool =
{ настройки пула процессов }

Настройки динамического пула процессов.

Первым определяется количество процессов в пуле:

- `auto` - количество процессов определяется автоматически в зависимости от загрузки системы;
- `N` - целое неотрицательное число. Как минимум `N` процессов в пуле будут активны, а новые процессы будут создаваться по мере надобности;



	<ul style="list-style-type: none">• N-M - целые положительные значения, и $M \geq N$. Как минимум N процессов в пуле будут активны, а новые процессы будут создаваться по мере надобности, пока число процессов не достигнет значения M. <p>Далее определяются дополнительные параметры:</p> <ul style="list-style-type: none">• timeout = { время в секундах} - если процесс не становится активным в течение заданного периода времени, процесс закрывается. Этот параметр не влияет на первые N процессов (ожидающих запросов бесконечно).• stat = {yes no} - статистика по процессам в пуле. Статистика сохраняется при получении системного сигнала SIGUSR1 в директории, определенной значением параметра BaseDir секции General.• stop_timeout = { время в секундах} - время ожидания остановки работающего процесса. <p><u>Значение по умолчанию:</u></p> <pre>ProcessesPool = auto, timeout = 120, stat = no, stop_timeout = 1</pre>
<p>OnlyKey = { Yes No }</p>	<p>Подключение возможности запросить только ключевой файл от Агента, не запрашивая конфигурацию. При этом будет использоваться локальный конфигурационный файл.</p>



	<p>Если указан адрес сокета Агента и значение параметра OnlyKey установлено в No, то Агенту будет отправляться статистика работы Демона (после сканирования каждого файла Демон будет отправлять информацию Агенту).</p> <p><u>Значение по умолчанию:</u></p> <p>OnlyKey = No</p>
<pre>ControlAgent = { адрес сокета Агента}</pre>	<p>Адрес сокета Агента в формате ТИП: АДРЕС, где ТИП может принимать значения inet (для TCP-сокетов), local и unix (для UNIX сокетов).</p> <p>Пример:</p> <pre>ControlAgent = inet: 4040@127.0.0.1, local: / var/drweb/ipc/.agent</pre> <p>Демон получает от Агента лицензионный ключ и конфигурационный файл (если в качестве значения параметра OnlyKey задано No).</p> <p><u>Значение по умолчанию:</u></p> <pre>ControlAgent = local: %var_dir/ ipc/.agent</pre>



<p>MailCommand = { команда}</p>	<p>Команда, используемая Демоном и модулем обновления для отсылки уведомлений пользователю (администратору) по электронной почте. Демон использует этот механизм при каждом запуске (перезапуске, перезагрузке), если до истечения срока действия ключевого файла (одного из ключевых файлов) осталось менее 14 дней. Модуль обновления использует этот механизм для рассылки пользователям информационных материалов, подготовленных компанией Доктор Веб, в том числе по вопросам, связанным с обновлениями файлов программы.</p> <p><u>Значение по умолчанию:</u></p> <pre>MailCommand = "/usr/sbin/ sendmail -i -bm -f drweb -- root"</pre>
<p>NotifyPeriod = { значение}</p>	<p>Значение данного параметра определяет, за сколько дней до окончания срока действия ключевого файла рассылаются уведомления о необходимости продления лицензии. Если указано значение 0, уведомления рассылаются сразу после окончания действия ключа.</p> <p><u>Значение по умолчанию:</u></p> <pre>NotifyPeriod = 14</pre>
<p>NotifyFile = { путь к файлу}</p>	<p>Путь к файлу с меткой времени последнего уведомления о продлении лицензии. Этот файл отсылается администратору по истечении срока действия лицензионного ключа.</p> <p><u>Значение по умолчанию:</u></p> <pre>NotifyFile = %var_dir/.notify</pre>



<code>NotifyType = { Ever Everyday Once}</code>	<p>Регулярность отправления уведомления о продлении лицензии. <code>Once</code> - уведомление посылается единожды. <code>Everyday</code> - уведомление посылается каждый день. <code>Ever</code> - уведомление посылается при каждой перезагрузке Демона или обновлении баз</p> <p><u>Значение по умолчанию:</u></p> <code>NotifyType = Ever</code>
<code>FileTimeout = { значение в секундах}</code>	<p>Максимальное время проверки одного файла. Если указано значение 0, время проверки файла не ограничивается.</p> <p><u>Значение по умолчанию:</u></p> <code>FileTimeout = 30</code>
<code>StopOnFirstInfected = { Yes No}</code>	<p>Прекращение проверки письма после первого обнаруженного вируса. Установка значения <code>Yes</code> может резко сократить нагрузку на почтовый сервер и время проверки писем.</p> <p><u>Значение по умолчанию:</u></p> <code>StopOnFirstInfected = No</code>
<code>ScanPriority = { значение}</code>	<p>Приоритет сканирующих процессов Демона. Значение параметра должно быть в диапазоне от высшего значения (-20) до низшего (19 для Linux, 20 для остальных ОС).</p> <p><u>Значение по умолчанию:</u></p> <code>ScanPriority = 0</code>



FileTypes = { список расширений}	<p>Типы файлов, которые будут проверяться при сканировании по типу, т.е. когда параметр ScanFiles (см. ниже) имеет значение ByType. Допускаются символы "*" и "?". Допускается несколько строк с этим параметром, в этом случае задаваемые списки суммируются.</p> <p><u>Значение по умолчанию:</u></p> <p>FileTypes = EXE, COM, SYS, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, VXD, 386, DLL, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, AR?, ZIP, R??, PP?, OBJ, LIB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SHS, SHB, PIF, SO, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, BMP, MPP, OCX, DVB, CPY, MSG, EML</p>
FileTypesWarnings = { Yes No }	<p>Предупреждение о файлах неизвестных типов.</p> <p><u>Значение по умолчанию:</u></p> <p>FileTypesWarnings = Yes</p>
ScanFiles = { All ByType }	<p>Дополнительное ограничение на файлы, подлежащие проверке. При задании значения ByType учитываются расширения файлов, значения которых заданы или по умолчанию, или в параметре (параметрах) FileTypes.</p> <p>Внутри почтовых файлов всегда действует режим All. Значение ByType может быть использовано только в режимах локального сканирования.</p> <p><u>Значение по умолчанию:</u></p> <p>ScanFiles = All</p>



CheckArchives = { Yes No}	Распаковка архивов форматов ZIP (WinZip, InfoZIP и др.), RAR, ARJ, TAR, GZIP, CAB и др. <u>Значение по умолчанию:</u> CheckArchives = Yes
CheckEMailFiles = { Yes No}	Проверка файлов в почтовых (e-mail) форматах. <u>Значение по умолчанию:</u> CheckEMailFiles = Yes
ExcludePaths = { список путей (масок) для исключения из проверки}	Маски для тех файлов, которые не должны проверяться. <u>Значение по умолчанию:</u> ExcludePaths = /proc, /sys, /dev
FollowLinks = { Yes No}	Следование символическим ссылкам при сканировании. <u>Значение по умолчанию:</u> FollowLinks = No
RenameFilesTo = { маска}	Маска для переименования файлов, если для данной ситуации (зараженный или подозрительный файл) задано действие Rename. К примеру, если задана маска #??, то первая буква расширения файла будет заменена на символ #, а остальные буквы будут сохранены. Если файл не имел расширения, оно будет состоять из одного символа #. <u>Значение по умолчанию:</u> RenameFilesTo = #??
MoveFilesTo = { путь к директории}	Путь к директории карантина. <u>Значение по умолчанию:</u>



	MoveFilesTo = %var_dir/ infected/
BackupFilesTo = { путь к директории}	Директория для сохранения зараженных файлов, которые были вылечены. <u>Значение по умолчанию:</u> BackupFilesTo = %var_dir/ infected/

Параметры регистрации событий:

LogFileName = { имя файла}	Имя файла отчета. В качестве имени можно указать syslog, тогда отчет будет вестись средствами системного сервиса syslogd. При использовании syslogd нужно обратить внимание на параметры SyslogFacility и SyslogPriority (см. ниже). Поскольку syslogd имеет несколько файлов для протоколирования разных событий и разных степеней их важности, то, основываясь на этих двух параметрах и содержанием конфигурационного файла syslogd (обычно /etc/syslogd.conf), можно определить, куда будет писаться отчет программы. <u>Значение по умолчанию:</u> LogFileName = syslog
SyslogFacility = { Daemon Local0 .. Local7 Kern User Mail}	Тип записи при использовании системного сервиса syslogd. <u>Значение по умолчанию:</u> SyslogFacility = Daemon
SyslogPriority = { Alert Warning Notice Info	Приоритет записи при использовании системного сервиса syslogd. <u>Значение по умолчанию:</u>



<code>Error}</code>	<code>SyslogPriority = Info</code>
<code>LimitLog = { Yes No }</code>	<p>Ограничение размера файла отчета. Параметр не влияет на работу программы при значении <code>LogFileName = syslog</code>. Ограничение размера файла отчета реализуется следующим образом: при запуске или получении сигнала HUP Демон проверяет размер файла отчета, и если он превышает значение, заданное в параметре <code>MaxLogSize</code>, файл отчета стирается и ведение отчета начинается с нуля.</p> <p><u>Значение по умолчанию:</u></p> <code>LimitLog = No</code>
<code>MaxLogSize = { значение в КБайтах }</code>	<p>Максимальный размер файла отчета. Имеет смысл только если <code>LimitLog = Yes</code>. Если указано значение 0, размер файла отчета проверяться не будет.</p> <p><u>Значение по умолчанию:</u></p> <code>MaxLogSize = 512</code>
<code>LogScanned = { Yes No }</code>	<p>Вывод в файл отчета информации обо всех проверяемых объектах, независимо от того, обнаружены вирусы или нет.</p> <p><u>Значение по умолчанию:</u></p> <code>LogScanned = Yes</code>
<code>LogPacked = { Yes No }</code>	<p>Вывод в файл отчета дополнительной информации о файлах, упакованных утилитами DIET, PKLITE и др.</p> <p><u>Значение по умолчанию:</u></p> <code>LogPacked = Yes</code>
<code>LogArchived = { Yes No }</code>	<p>Вывод в файл отчета дополнительной информации об архиваторах.</p>



	<p><u>Значение по умолчанию:</u></p> <p>LogArchived = Yes</p>
LogTime = { Yes No }	<p>Вывод в файл отчета времени каждой записи. Параметр не имеет смысла, если LogFileName = syslog.</p> <p><u>Значение по умолчанию:</u></p> <p>LogTime = Yes</p>
LogProcessInfo = { Yes No }	<p>Вывод в файл отчета перед каждой записью данных о pid сканирующего процесса и адресе фильтра (имени хоста или IP-адресе), с которого инициирована проверка.</p> <p><u>Значение по умолчанию:</u></p> <p>LogProcessInfo = Yes</p>
RecodeNonprintable = { Yes No }	<p>Перекодировка при выводе в файл отчета символов, не являющихся отображаемыми для данного терминала (см. следующие два параметра).</p> <p><u>Значение по умолчанию:</u></p> <p>RecodeNonprintable = Yes</p>
RecodeMode = { Replace QuotedPrintable }	<p>При RecodeNonprintable = Yes задает метод перекодировки неотображаемых символов. При RecodeMode = Replace все такие символы заменяются на значение параметра RecodeChar (см. ниже). При RecodeMode = QuotedPrintable производится перекодировка неотображаемых символов в формат Quoted Printable.</p> <p><u>Значение по умолчанию:</u></p> <p>RecodeMode = QuotedPrintable</p>



<pre>RecodeChar = {"?" "_" ...}</pre>	<p>При RecodeMode = Replace задает символ, на который будут заменены все неотображаемые символы.</p> <p><u>Значение по умолчанию:</u></p> <pre>RecodeChar = "?"</pre>
<pre>Socket = { адрес сокета}</pre>	<p>Описание сокета, который будет использован для связи с Демоном.</p> <p>Существует несколько вариантов задания сокетов для связи с Демоном.</p> <p>Если необходимо указать несколько сокетов в одной строке, то можно использовать формат записи ТИП: АДРЕС, где ТИП может принимать значения inet (для TCP-сокетов), local и unix (для UNIX сокетов).</p> <p>Пример:</p> <pre>Socket = inet:3000@127.0.0.1, local:%var_dir/.daemon</pre> <p>Также можно адрес каждого из сокетов указывать в отдельном параметре в формате ПОРТ [интерфейсы] ФАЙЛ [доступ]. Соответственно, для TCP-сокета: ПОРТ - десятичный номер порта, интерфейсы - список имен интерфейсов или IP-адресов, на которых Демон будет принимать запросы.</p> <p>Пример:</p> <pre>Socket = 3000 127.0.0.1, 192.168.0.100</pre> <p>Для UNIX сокета: ФАЙЛ - имя сокета, доступ - восьмеричное значение прав доступа к нему.</p> <p>Пример:</p> <pre>Socket = %var_dir/.daemon 0660</pre>



	<p>Количество параметров Socket не ограничено, Демон будет работать со всеми из описанных сокетов. Чтобы Демон принимал запросы через все доступные интерфейсы, для параметра следует задать значение 3000 0.0.0.0.</p>
	<p><u>Значение по умолчанию:</u></p> <p>Socket = %var_dir/run/.daemon</p>

<p>SocketTimeout = { значение в секундах }</p>	<p>Время, отведенное для приема/передачи всех данных через сокет (время сканирования файла не учитывается). Если указано значение 0, время не будет ограничено.</p>
	<p><u>Значение по умолчанию:</u></p> <p>SocketTimeout = 10</p>

Следующие параметры могут быть использованы для уменьшения времени проверки архивов (за счет отказа от проверки некоторых объектов в архиве). Если объект подпадает под ограничения, созданные этими параметрами, то к нему применяется действие **ArchiveRestriction**, которое задано в файлах конфигурации различных фильтров.

<p>MaxCompressionRatio = { значение }</p>	<p>Максимальный коэффициент сжатия, т. е. отношение длины файла в распакованном виде к длине файла в запакованном виде (внутри архива). Если коэффициент превышает данное значение, файл не будет извлечен и, соответственно, не будет проверен.</p> <p>Параметр может принимать только натуральные значения. Если указано значение 0, проверка коэффициента сжатия проводиться не будет.</p>
	<p><u>Значение по умолчанию:</u></p> <p>MaxCompressionRatio = 5000</p>



CompressionCheckThreshold = { значение в КБайтах}	<p>Минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия (если это предписано параметром MaxCompressionRatio).</p> <p><u>Значение по умолчанию:</u></p> CompressionCheckThreshold = 1024
MaxFileSizeToExtract = { значение в КБайтах}	<p>Максимальный размер файла, извлекаемого из архива. Если размер файла внутри архива превышает это значение, он будет пропущен.</p> <p><u>Значение по умолчанию:</u></p> MaxFileSizeToExtract = 40960
MaxArchiveLevel = { значение}	<p>Максимальный уровень вложенности архивов (когда архив вложен в архив, который тоже вложен в архив и т.д.). При превышении этого уровня архив будет пропущен (не будет проверен).</p> <p>Если указано значение 0, уровень вложенности архивов не будет ограничиваться.</p> <p><u>Значение по умолчанию:</u></p> MaxArchiveLevel = 8



```
ClientsLogs =  
{ список }
```

Параметр разделения файлов отчета. Если при обращении к **Демону** клиент передает в расширенных опциях свой идентификатор, файл отчета клиента заменяется на тот, который указан в параметре `ClientsLogs`. Описания логов разделяются запятыми или пробелами. В случае задания в параметре больше шести файлов отчета строка конфигурационного файла считается неверной. Файлы отчета клиентов задаются в виде:
`ClientsLogs=<имя клиента1>:
<путь к файлу>,<имя клиента2>:
<путь к файлу>`.

Имя клиента может быть одним из следующих:

- `web` — **Dr.Web ICAPD**;
- `smb_spider` — **Dr.Web Samba SpIDer**;
- `mail` — **Dr.Web MailD**;
- `drwebdc` — консольный клиент **Демона Dr.Web**;
- `kerio` — **Dr.Web для интернет-шлюзов Kerio**;
- `lotus` — **Dr.Web для IBM Lotus Domino**.

Пример:

```
drwebdc: /var/drweb/log/  
drwebdc.log,  
smb: syslog,  
mail: /var/drweb/log/drwebmail.  
log
```

Значение по умолчанию:

```
ClientsLogs =
```



<p>MaxBasesObsolescencePeriod = {значение в часах}</p>	<p>Максимальный период времени (в часах) с момента последнего обновления, в течение которого вирусные базы считаются "свежими". По истечении этого времени, в консоли выводится уведомление о том, что базы устарели.</p> <p>Если установлено значение 0, то актуальность вирусных баз не проверяется.</p> <p><u>Значение по умолчанию:</u></p> <p>MaxBasesObsolescencePeriod = 24</p>
<p>MessagePatternFileName = {путь к файлу}</p>	<p>Путь к файлу шаблона сообщения об истечении срока действия лицензии. Позволяет пользователю определить сообщение об истечении срока действия лицензии в удобном для него виде. В шаблоне сообщения могут быть использованы следующие переменные, вместо которых будут автоматически подставлены следующие значения:</p> <ul style="list-style-type: none">• \$EXPIRATIONDAYS — количество дней до истечения срока лицензии;• \$KEYFILENAME — путь к лицензионному ключевому файлу;• \$KEYNUMBER — номер лицензии;• \$KEYACTIVATES — дата активации лицензии;• \$KEYEXPIRES — дата завершения срока действия лицензии. <p>Если пользовательский шаблон отсутствует, используется сообщение по умолчанию на английском языке.</p> <p><u>Значение по умолчанию:</u></p>



	<code>MessagePatternFileName = % etc_dir/templates/drwebd/msg. tpl</code>
<code>MailTo = {адрес электронной почты}</code>	Почтовый адрес администратора для отправки сообщений об истечении срока действия лицензии, устаревании вирусных баз и пр.
	<u>Значение по умолчанию:</u> <code>MailTo =</code>



Контакты

Программный комплекс **Dr.Web для Novell Storage Services** находится в постоянном развитии. Наиболее свежую информацию о его обновлениях, а также новости можно получить на сайте:

<http://www.drweb.com/>

Отдел продаж:

<http://buy.drweb.com/>

Техническая поддержка:

<http://support.drweb.com/>

В письме необходимо предоставить следующую дополнительную информацию, которая поможет лучше разобраться в ситуации:

- полное название и версию дистрибутива UNIX системы;
- версии компонентов программного комплекса **Dr.Web для Novell Storage Services**;
- конфигурационные файлы компонентов;
- файлы отчета компонентов.

