



Dr.WEB®

Антивирус

для Novell Storage Services

Защити созданное

Руководство администратора

© 2013 "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

15.01.2013

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	11
Системные требования	14
Совместимость с дистрибутивами Linux	15
Расположение файлов пакета	15
Конфигурационные файлы	17
Ведение журналов (логов)	24
Действия с зараженными и подозрительными объектами	27
Установка и удаление Dr.Web для Novell Storage Services	29
Установка универсального пакета для UNIX систем	30
Пользовательский интерфейс графического инсталлятора	33
Использование консольного инсталлятора	40
Удаление универсального пакета для UNIX систем	42
Пользовательский интерфейс графического деинсталлятора	43
Использование консольного деинсталлятора	46
Обновление универсального пакета для UNIX систем	48
Запуск Dr.Web для Novell Storage Services	49



Операционные системы с SELinux	51
Регистрация продукта	55
Dr.Web для Novell Storage Services	59
Параметры командной строки	61
Обрабатываемые сигналы	63
Внутренняя статистика работы	63
Статистика проверки файлов	65
Карантин	66
Управление через drweb-nss-qcontrol	67
Файл журнала Dr.Web NSS	71
Проверка конфигурации	72
Конфигурационный файл	73
Секция [General]	73
Секция [Logging]	74
Секция [NSS]	75
Секция [DaemonCommunication]	78
Секция [Actions]	80
Секция [Stat]	84
Секция [Quarantine]	84
Секция [Notifications]	85
Модуль обновления Dr.Web Updater	89
Обновление антивируса и вирусных баз	89
Настройка cron	92
Параметры командной строки	93
Блокирование обновлений для компонентов	94
Восстановление компонентов	95



Настройки	96
Процедура обновления	102
Dr.Web Agent	104
Режимы работы	104
Параметры командной строки	108
Конфигурационный файл	109
Секция [Logging]	110
Секция [Agent]	111
Секция [Server]	113
Секция [EnterpriseMode]	114
Секция [StandaloneMode]	116
Секция [Update]	118
Запуск	118
Взаимодействие с компонентами программного комплекса	120
Интеграция с Dr.Web Enterprise Security Suite	121
Настройка компонентов для работы в режиме Enterprise	122
Автоматическое создание учетной записи	123
Создание учетной записи на сервере вручную	124
Задание конфигурации компонентов через Центр Управления Dr.Web	124
Экспорт существующей конфигурации на сервер	125
Запуск комплекса	125
Работа с вирусной статистикой	125
Dr.Web Monitor	132



Режимы работы	132
Параметры командной строки	135
Конфигурационный файл	136
Секция [Logging]	136
Секция [Monitor]	138
Запуск	142
Взаимодействие с компонентами программного комплекса	143
Консольный сканер Dr.Web Scanner	146
Запуск	146
Параметры командной строки	149
Настройки	160
Антивирусный модуль Dr.Web Daemon	175
Параметры командной строки	175
Запуск	176
Проверка работоспособности Dr.Web Daemon	178
Режимы проверки	182
Обрабатываемые сигналы	183
Журнал работы и статистика пула процессов	183
Настройки	186
Контакты	204



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.

Программный комплекс **Dr.Web для Novell Storage Services** состоит из следующих компонентов:

- **Консольный сканер Dr.Web Scanner** служит для обнаружения и лечения вирусов на локальной машине, в том числе и в каталогах общего доступа;
- **Резидентный компонент Dr.Web Daemon** используется в качестве подключаемого внешнего антивирусного фильтра;
- **Резидентный компонент Dr.Web Monitor** используется для запуска и перезапуска прочих модулей **Dr.Web** в нужном порядке;
- **Резидентный компонент Dr.Web Agent** используется для управления конфигурацией модулей **Dr.Web**, сбора статистической информации и интеграции с **Dr.Web Enterprise Security Suite**;
- **Антивирусное ядро Dr.Web Engine** и набор постоянно



обновляемых вирусных баз данных;

- **Компонент Dr.Web Updater**, выполненный в виде perl-скрипта, используется для автоматического обновления вирусных баз данных;
- **Резидентный компонент Dr.Web NSS** – основной модуль системы, обеспечивающий взаимодействие с файловой системой NSS.

Структура компонентов **Dr.Web для Novell Storage Services** изображена на рисунке ниже:

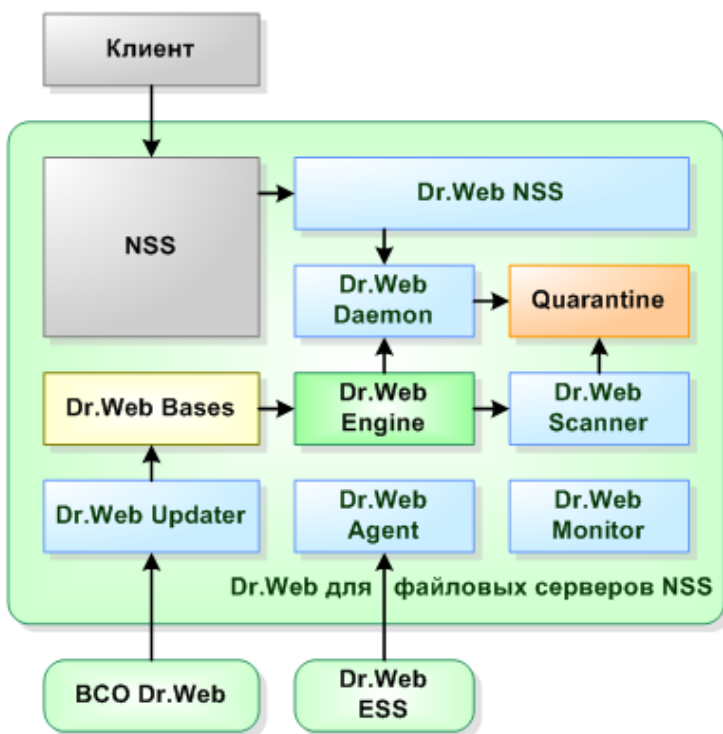


Рис. 1. Структура компонентов Dr.Web для Novell Storage Services



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 каталогов, 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/
```

В документе используются следующие термины и сокращения:

Сокращение	Расшифровка
ASCII	American Standard Code for Information Interchange — американская стандартная кодировочная таблица для печатных символов и некоторых специальных кодов
CIDR	Classless Inter-Domain Routing — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации
DEB	Расширение имён файлов «бинарных» пакетов для распространения и установки программного обеспечения в ОС проекта Debian и других, использующих систему управления пакетами dpkg
DNS	Domain Name System — компьютерная распределённая система для получения информации о доменах
HTML	HyperText Markup Language — язык разметки гипертекста, стандартный язык разметки Web-документов
IP	Internet Protocol — маршрутизируемый межсетевой протокол сетевого уровня семейства TCP/IP
IPv4	Протокол IP, версия 4
IPv6	Протокол IP, версия 6
IPC	Inter-Process Communication — набор способов обмена данными между множеством потоков в одном или более процессах, запущенных на одном или более компьютерах, связанных между собой сетью



Сокращение	Расшифровка
MD5	Message Digest 5 — 128-битный алгоритм хеширования, предназначенный для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности
PID	Process IDentifier — уникальный идентификатор, присваиваемый ОС экземпляру процесса при его запуске
POSIX	Portable Operating System Interface for Unix — набор стандартов, определяющих интерфейсы взаимодействия между операционной системой и прикладной программой, созданный для обеспечения совместимости различных UNIX-подобных операционных систем и переносимости прикладных программ на уровне исходного кода
RFC	Request for Comments — документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети
RPM	Формат пакетов распространения программного обеспечения и название менеджера управления ими
SSL	Secure Socket Layers — так же как и TLS — криптографический протокол, обеспечивающие защищённую передачу данных между узлами в сети Интернет
TCP	Transmission Control Protocol — один из основных сетевых протоколов Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP
TLS	Transport Layer Security — криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет. Использует асимметричную криптографию для обмена ключами, симметричное шифрование для конфиденциальности и коды аутентичности для сохранения целостности сообщений



Сокращение	Расшифровка
URL	Uniform Resource Locator — единообразный локатор (определитель местонахождения) ресурса. Стандартизированный способ записи адреса ресурса в сети Интернет
UUID	Unique User Identifier — уникальный идентификатор пользователя
XML	eXtensible Markup Language — расширяемый язык разметки, текстовый формат, предназначенный для хранения структурированных данных, обмена информацией между программами, а также для создания на его основе более специализированных языков разметки
ОС	Операционная система — комплекс управляющих и обрабатывающих программ, предназначенных для управления устройствами, вычислительными процессами, эффективного распределения вычислительных ресурсов между вычислительными процессами и организации надёжных вычислений

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 определенный каталог системы.
- Модуль обновления **Dr.Web Updater** требует установленный **Perl 5.8.0** и выше.

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 каталоги `%bin_dir`, `%etc_dir` и `%var_dir`. В этих каталогах создается структура подкаталогов, не зависящая от ОС:

`%bin_dir/` – Исполняемые модули программного комплекса и модуль обновления компонентов **Dr.Web Updater** (perl-скрипт `update.pl`).

`%bin_dir/doc/` – Документация по продукту. Вся документация представлена в виде текстовых файлов и присутствует в двух вариантах — англоязычном и русскоязычном (в кодировках KOI8-R и UTF-8).



%bin_dir/lib/ - Антивирусное ядро **Dr.Web Engine** в виде подгружаемой библиотеки (drweb32.dll). Здесь же могут располагаться различные служебные библиотеки, необходимые для работы компонентов программного комплекса, например:

- 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/ - Конфигурационные файлы программного комплекса:

- drweb32.ini;
- agent.conf;
- monitor.conf;
- drwebd.enable;
- drweb-monitor.enable.

Последние два файла (enable-файлы) нужны для настройки работы демонов*.

%etc_dir/agent/ - Дополнительные конфигурационные файлы модуля **Dr.Web Agent**.

%etc_dir/monitor/ - Дополнительные конфигурационные файлы модуля **Dr.Web Monitor**.

%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 **Dr.Web Daemon** или подключаемых модулей.

%var_dir/bases/ - Базы данных известных вирусов (файлы *.vdb).

%var_dir/infected/ - Каталог **Карантина** для перемещения в него зараженных файлов, если такая реакция на обнаружение зараженных или подозрительных файлов задана в настройках компонентов программного комплекса.



*) Расположение `enable`-файлов зависит от способа установки **Dr.Web для Novell Storage Services**:

- Установка при помощи универсального пакета для UNIX:

Файлы располагаются в каталоге `%etc_dir` и называются
`drwebd.enable`,
`drweb-monitor.enable`.

- Установка из нативных DEB-пакетов:

Файлы располагаются в каталоге `/etc/defaults` и называются
`drwebd`,
`drweb-monitor`.

- Установка из нативных RPM-пакетов:

Файлы располагаются в каталоге `/etc/sysconfig` и называются
`drwebd.enable`,
`drweb-monitor.enable`.

Конфигурационные файлы

Общий формат конфигурационных файлов

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).



Общий формат файла конфигурации:

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

Файлы конфигурации формируются по следующему принципу:

- 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.
- Содержимое файла разбивается на последовательность именованных секций. Возможные имена секций жестко заданы и не могут быть произвольными. Имя секции задается в квадратных скобках.
- Каждая секция содержит группу параметров конфигурации, объединенных по смыслу.
- В одной строке файла задается значение только одного параметра.
- Основной формат задания значения параметра (пробелы, окружающие символ '=', если встречаются, игнорируются):

```
<Имя параметра> = <Значение>
```

- Возможные имена параметров жестко заданы и не могут быть произвольными.
- Все имена секций и параметров в файле



регистронезависимы.

- Порядок следования секций в файле и параметров внутри секций не имеет значения.
- 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 перечислении значений параметра через запятую пробелы между значением и запятой, если встречаются, игнорируются. Если пробел является частью значения, всё значение необходимо заключить в кавычки.



Возможность присвоения параметру несколько значений в данном документе указывается явно. Если для некоторого параметра в данном документе или в комментариях в файле конфигурации явно не указано, что ему можно присвоить несколько значений, то параметр может обладать только одним значением.

Пример задания параметра, имеющего несколько значений:

1) Перечисление нескольких значений через запятую:

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

2) Задание тех же значений параметра в разных строках конфигурационного файла:

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

Обратите внимание, что порядок следования значений параметра в списке несущественен.



Если какой-либо параметр не задан (отсутствует) в конфигурационном файле, это не означает, что у данного параметра нет значения. В таких случаях значение параметра считается заданным по умолчанию. Лишь некоторые параметры являются необязательными или не имеют значений по умолчанию, о чем, как правило, упоминается отдельно.

Правила описания параметров, принятые в данном документе

В данном руководстве каждый параметр описывается следующим образом:

ИмяПараметра = { Тип параметра Возможные значения}	Описание параметра. {Может ли иметь несколько значений}. {Особые замечания} {Важные замечания}
	<u>Значение по умолчанию:</u> ИмяПараметра = { значение отсутствует}

Описание параметров и секций конфигурационных файлов 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:

- **числовое значение (numerical value)** — значение параметра является целым неотрицательным 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 трехзначным числом, обозначающим права доступа к файлам в формате, принятом в UNIX-системах. Каждое право является комбинацией (суммой) трех базовых прав:
 - Право чтения (*r*) обозначается числом 4;
 - Право записи (*w*) обозначается числом 2;
 - Право исполнения (*x*) обозначается числом 1.

При этом первая цифра числа задает права для владельца файла, вторая — для группы владельцев файла, а третья — для всех остальных, не являющихся ни владельцами, ни членами соответствующей группы.

Примеры: 755, 644

- **логический (Yes/No)** — Логический тип, значения которого представляются строками "Yes" и "No".



- **путь к файлу/каталогу** (`path to file/directory`) — строка, задающая расположение файла или каталога в файловой системе. Помните, что в ОС семейства Linux/UNIX имена файлов и каталогов регистрозависимы. Если указано, что значением параметра может быть **маска**, то в качестве значений параметра можно использовать файловые маски, содержащие следующие специальные символы:

- `?` — замещает любой один символ;
- `*` — замещает любую (в том числе пустую) последовательность символов.

Пример: `"?.e*"` — маска, под которую попадают файлы, имя которых состоит из любого одного символа, а расширение любой длины, и начинается с буквы 'e' (х. `exe`, г. `e`, ф. `enable` и т.п.).

- **действие (action)** — строка, содержащая наименование действий, совершаемых над объектами, вызвавшими какую-либо реакцию компонентов программного комплекса **Dr.Web для Novell Storage Services**. В некоторых случаях для параметра можно задать одно основное действие и до трех дополнительных. Тип параметра в этом случае называется **список действий (actions list)**. Основное действие в этом случае всегда должно быть первым в списке. Для разных параметров набор допустимых действий может различаться, и в этом случае он указывается отдельно для каждого параметра. Общий перечень действий, которые могут использоваться, см. [ниже](#).



- **адрес (address)** — строка, содержащая адрес сокета компонента **Dr.Web для Novell Storage Services** или внешнего модуля или программы.

Имеет формат ТИП: АДРЕС. Допустимы следующие типы:

- **inet** — используются TCP-сокеты, АДРЕС имеет формат ПОРТ@ИМЯ_УЗЛА. ИМЯ_УЗЛА может быть как прямым IP-адресом, так и доменным именем узла.

Пример:

```
Address = inet:3003@localhost
```

- **local** — используются локальные UNIX сокеты, в этом случае адрес является путем к файлу сокета.

Пример:

```
Address = local:%var_dir/.daemon
```

- **pid** — реальный адрес процесса должен быть прочитан из его PID файла. Такой тип адреса доступен лишь в некоторых случаях и при возможности его использования в значении параметра это указывается явно.
- **текст (text value), строка (string)** — значение параметра задается в виде текстовой строки, текст в строке может быть заключен в кавычки (если в строке есть пробелы, кавычки обязательны).
- **уровень подробности (log level)** — строка, указывающая уровень подробности вывода информации в некоторый журнал или в службу **syslog**.
- **возможные значения (value)** — параметр имеет тип, не описанный в предыдущих пунктах данного списка. В этом случае перечисляется список разрешенных для него значений.

Поведение модулей при некорректно заданных файлах конфигурации

- 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 журнала (лог) выводится соответствующее предупреждение.



Некоторые параметры могут использовать в качестве значений регулярные выражения (для каждого параметра отмечается в его описании). По умолчанию используется синтаксис регулярных выражений **Perl**. С основами регулярных выражений вы можете ознакомиться, например, в **Wikipedia** (статья "[Регулярные выражения](#)").

Ведение журналов (логов)

Все компоненты программного комплекса **Dr.Web для Novell Storage Services** ведут журналы (логи) своей работы. Для каждого компонента имеется возможность указать способ ведения журнала (самостоятельная запись событий в файл или использование системной службы журналирования **syslog**).

Уровень подробности ведения журнала работы компонента может быть как очень высоким (например, если задано значение **Debug** для отладочных целей), так и отсутствовать вовсе (например, если задано значение **Quiet**, когда файл журнала не ведется).

Для задания уровня подробности используется параметр с именем **LogLevel**. Также некоторые модули могут иметь дополнительные параметры, регулирующие уровни подробности вывода некоторых сообщений в журнал (например, вывод сообщений подсистемы IPC, там, где она используется, регулируется параметром **IPCLevel**).



Если в настройках модуля отсутствуют параметр конфигурации **LogLevel**, то это означает, для него регулирование уровня подробности в журнал невозможно. По умолчанию в этом случае используется уровень журналирования, примерно равный **Debug**.

Используемые уровни подробности ведения журнала

Значения параметров, отвечающих за уровень подробности ведения журнала работы компонентов в общем случае могут задаваться из следующего набора (упорядочен от менее к более подробным):

- **Quiet** – Уровень "Тишина". Запись событий в журнал не ведется.
- **Error** – Уровень "Ошибки". Фиксируются записи только об критических ошибках.
- **Alert** – Уровень "Тревога". Фиксируются записи об ошибках и важных предупреждениях.
- **Warning** – Уровень "Предупреждения". Фиксируются записи об ошибках, важных и обычных предупреждениях.
- **Info** – Уровень "Информационный". Ведется запись сообщений об ошибках, предупреждениях и информационных сообщений.
- **Notice** – Уровень "Уведомительный". То же, что и "Информационный", но добавляются записи уведомлений.
- **Debug** – Уровень "Отладочный", То же, что и "Уведомительный", но добавляются записи отладочной информации.
- **Verbose** – Уровень "Подробный", ведется запись в журнал всех возможных сообщений (режим не рекомендуется из-за большого объема информации, выводимой в журнал, что тормозит как работу приложения, так и службу журналирования **syslog** операционной системы, если она используется).



Для каждого модуля **Dr.Web для Novell Storage Services** набор допустимых уровней подробности может различаться, о чем указано в описании соответствующих параметров

Использование службы журналирования **syslog**

При использовании для ведения службы журналирования **syslog** кроме указания уровня подробности ведения журнала указывается также метка-источник сообщений, которая может быть использована службой **syslog** для внутренней маршрутизации сообщений по разным файлам журналов. Эти правила маршрутизации настраиваются в собственном файле конфигурации демона службы **syslog** (обычно `/etc/syslogd.conf`).

Метка, присваиваемая сообщениям для службы **syslog**, указывается в конфигурационных файлах в параметре **SyslogFacility**.

Допускается использование следующих меток:

- **Daemon** – От имени резидентного системного сервиса (демона);
- **Local0, ..., Local7** – От имени локального пользовательского приложения (зарезервировано 8 номеров 0-7);
- **Kern** – От имени ядра системы;
- **User** – От имени пользовательского процесса;
- **Mail** – От имени почтовой системы.

Пожалуйста, обратите внимание, что при использовании **syslog** в файле конфигурации может дополнительно присутствовать параметр подробности ведения журнала, используемый для системы **syslog**. Этот параметр имеет название **SyslogPriority** и может принимать те же значения, что и основной параметр уровня подробности (**LogLevel**). В случае если вывод в **syslog** не используется, этот параметр, также как и **SyslogFacility**, игнорируется.



В противном случае для вывода в **syslog** выбирается наименее подробный из двух указанных уровней.

Пример:

Пусть у некоторого модуля `LogLevel = Debug`, а `SyslogPriority = Error`. Тогда, если в качестве журнала для записей событий этого модуля выбрана служба **syslog**, фактически будет вестись запись на уровне подробности `Error` (будут фиксироваться только сообщения об ошибках, а отладочная информация **syslog** будет игнорироваться).

Действия с зараженными и подозрительными объектами

В настройках **Dr.Web для Novell Storage Services** задаются действия, которые модули, входящие в его состав, должны совершать с объектами, которые по результатам проверки признаны вредоносными, опасными или подозрительными.

Для разных параметров набор допустимых действий может различаться, поэтому для каждого параметра всегда указывается перечень действий, которые могут быть в нем использованы.

При настройке параметров предусмотрено использование следующих действий:

Доступные действия для **Dr.Web Scanner**:

- Move — переместить файл в каталог **Карантина**;
- Delete — удалить зараженный файл;
- Rename — переименовать файл;
- Ignore — пропустить файл;
- Report — только вывести информацию в отчет.
- Cure — попытаться вылечить зараженный объект.



Возможные действия для модуля **Dr.Web NSS**:

- Pass — пропустить файл;
- Cure — попытаться вылечить зараженный файл;
- Report — только отправить сообщение;
- Quarantine — переместить файл в каталог **Карантина** и запретить к нему доступ;
- Remove — удалить файл.



Имена действий для указания в параметрах не чувствительны к регистру (например, значения `Report` и `report` обозначают одно и то же действие).



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 EPM для использования с менеджером пакетов EPM (ESP 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 EPM-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 EPM-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 каталогов. В процессе установки данного компонента будут созданы пользователь `drweb` и группа `drweb`;
- `drweb-bases`: пакет содержит Антивирусное ядро **Dr. Web Engine** 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, использующиеся **Dr.Web Agent** и **Dr.Web Monitor** совместно. Для установки требует пакет `drweb-libs`;



- `drweb-updater`: пакет содержит модуль обновления Антивирусного ядра **Dr.Web Engine** и вирусных баз **Dr. Web Updater**. Для установки требует пакеты `drweb-common` и `drweb-libs`;
- `drweb-agent`: пакет содержит исполняемые файлы **Dr. Web Agent** и документацию к нему. Для установки требует пакеты `drweb-boost147` и `drweb-common`;
- `drweb-agent-es`: пакет содержит файлы для работы **Dr.Web Agent** в режиме центральной защиты. Для установки требует пакеты `drweb-agent`, `drweb-updater` и `drweb-scanner`;
- `drweb-monitor`: пакет содержит исполняемые файлы **Dr.Web Monitor** и документацию к нему. Для установки требует пакеты `drweb-boost147`, `drweb-agent` и `drweb-common`;
- `drweb-daemon`: пакет содержит исполняемые файлы **Dr. Web Daemon** и документацию к нему. Для установки требует пакеты `drweb-bases` и `drweb-libs`;
- `drweb-scanner`: пакет содержит исполняемые файлы консольного сканера **Dr.Web Scanner** и документацию к нему. Для установки требует пакеты `drweb-bases` и `drweb-libs`;
- `drweb-perftools0`: пакет содержит библиотеку **Google Performance Tools**, используемую **Dr.Web NSS**. Для установки требует пакет `drweb-libs`;
- `drwen-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 требует 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 создан каталог `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 каталог `%etc_dir/software/conf/` записываются оригиналы дистрибутивных конфигурационных файлов с названиями `[имя_конфигурационного_файла].N;` в формате
- конфигурационные файлы устанавливаются в соответствующие каталоги 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 каталоге 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.

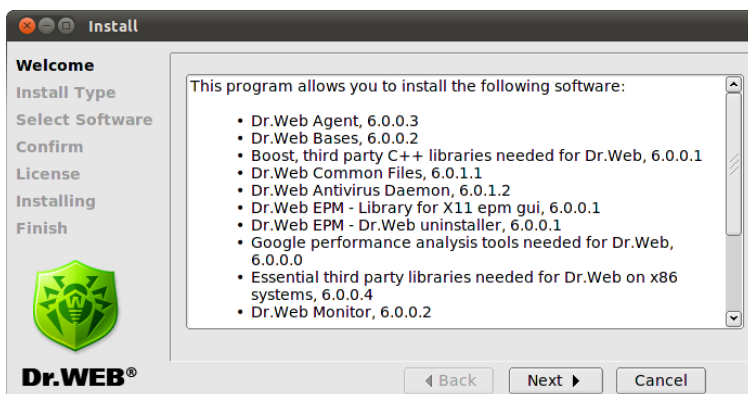


Рис. 2. Окно начала установки программы

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

- 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.

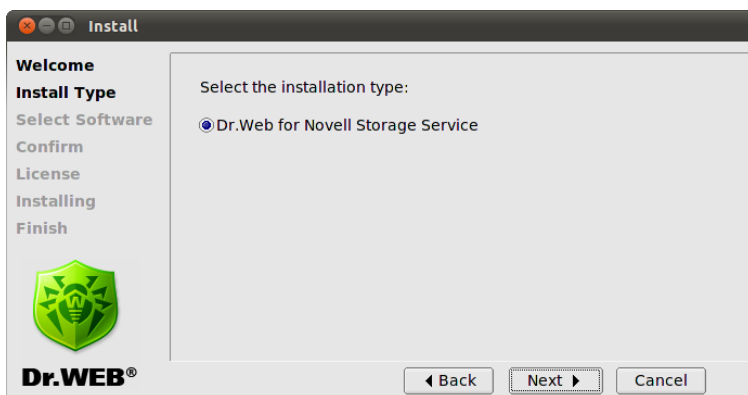


Рис. 3. Тип установки



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

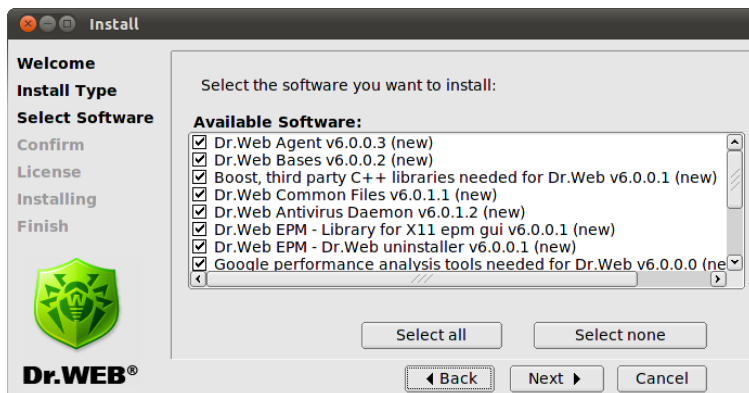


Рис. 4. Окно выбора компонентов для установки



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.

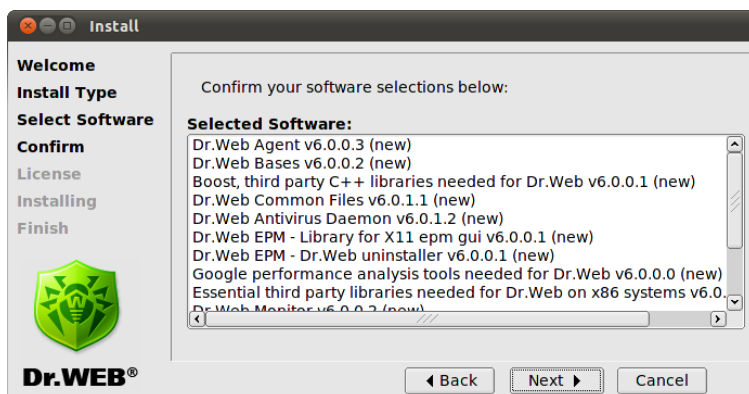


Рис. 5. Окно подтверждения установки компонентов

- 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**.

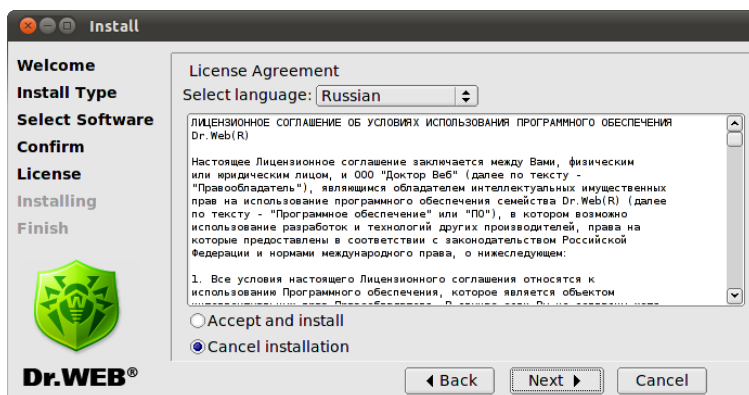


Рис. 6. Окно ознакомления с лицензионным соглашением

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

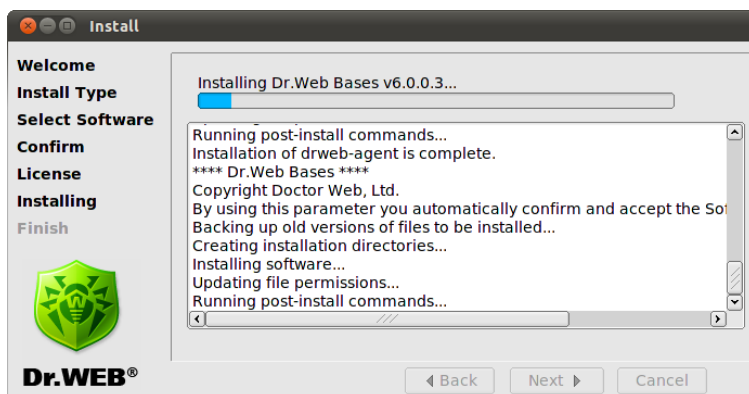


Рис. 7. Окно установки компонентов программы

Одновременно данный отчет копируется в файл `install.log`, расположенный в каталоге `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 1]:

Setting 'Address' to 'pid:/var/drweb/run/drwebd.pid 1' 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. 8. 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 каталогу, в который 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 использовать реальный адрес процесса



Dr.Web Daemon, 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: 1895
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: 2095
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/dwnrisky.vdb - Ok, virus records: 6197
Loading /var/drweb/bases/dwnasty.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. 9. Автоматический запуск сервисов

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

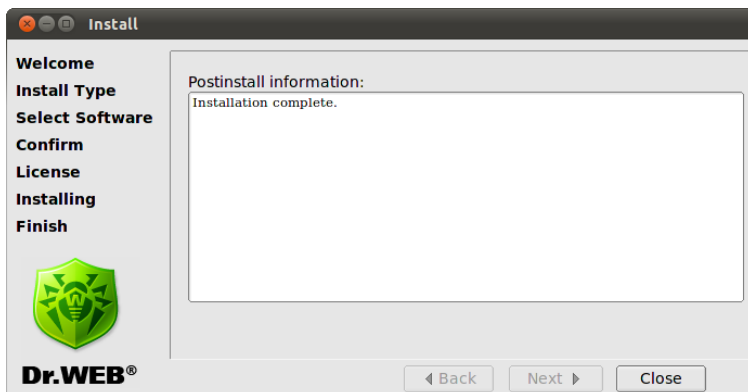


Рис. 10. Окно завершения установки программы

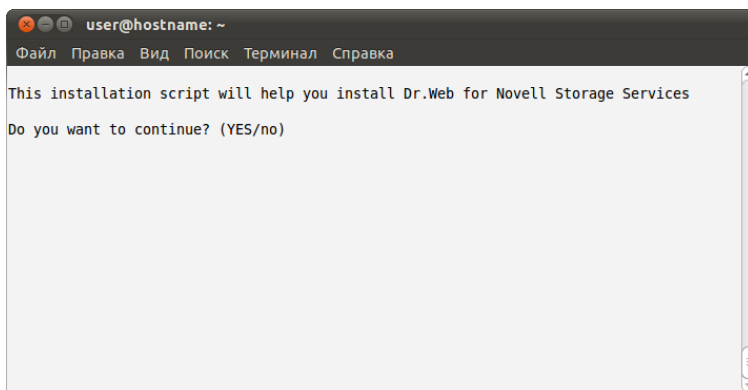
Использование консольного инсталлятора

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] /setup.sh
```



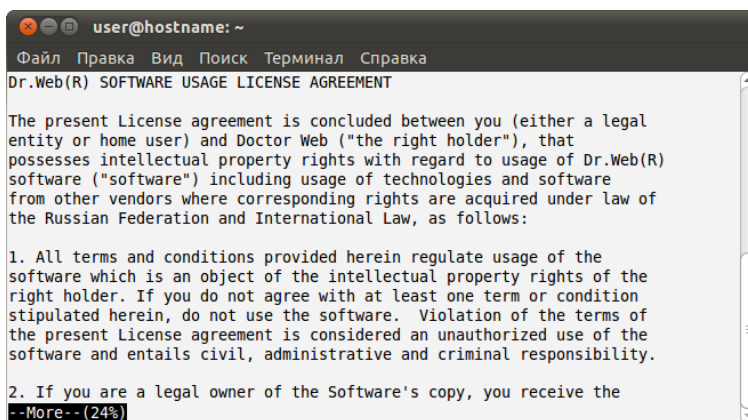

Откроется диалоговое окно консольного инсталлятора.



```
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 и автоматически подключить необходимые для работы сервисы (**Dr.Web Daemon**, **Dr.Web Agent**, **Dr.Web Monitor**). Дополнительно Вам будет предложено указать путь к каталогу, в который смонтированы разделы NSS, а также определить, какие из них будут защищены от вирусов (по умолчанию защищаются все разделы).

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 каталога `%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 каталогах сохраняются.

Пользовательский интерфейс графического деинсталлятора

1. При запуске графического деинсталлятора командой:

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

открывается окно программы удаления компонентов.

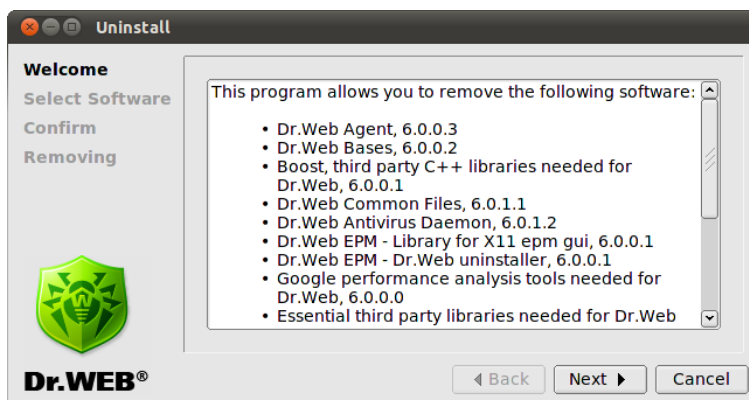


Рис. 11. Окно начала удаления программы

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 планируются использовать в дальнейшем.

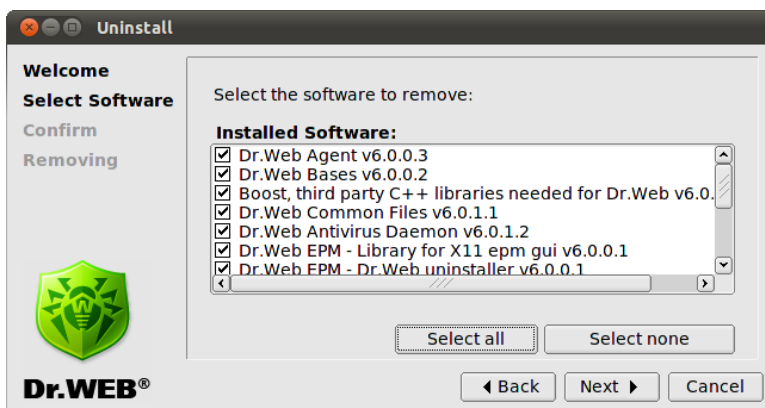


Рис. 12. Окно выбора компонентов для удаления

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

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

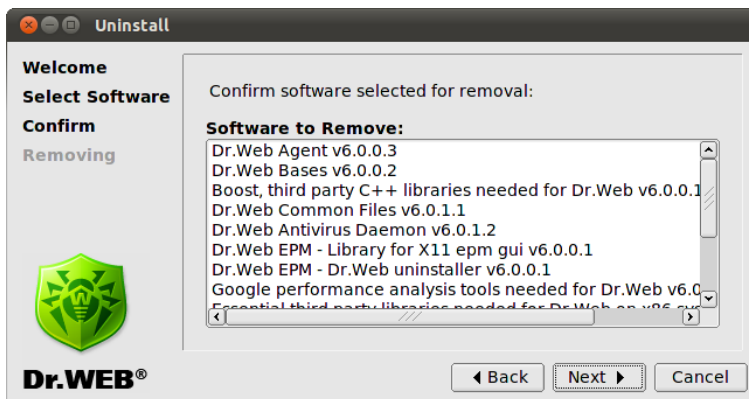


Рис. 13. Окно подтверждения удаления компонентов



4. В последнем окне **Removing** выводится отчет о процессе удаления компонентов программного комплекса в режиме реального времени.

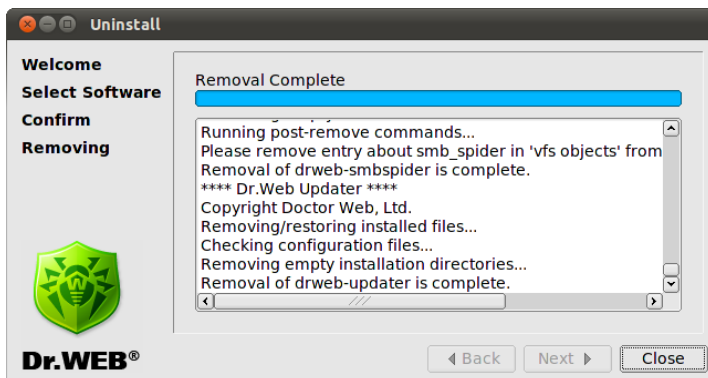


Рис. 14. Окно удаления компонентов программы

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.

Откроется 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 каталогах.



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 каталог 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 каком-либо другом каталоге, 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 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 `enable`-файл `drwebd` и установите параметр `ENABLE = 1`. Это позволит запустить **Dr.Web Daemon**. Если запускать **Dr.Web Daemon** на локальной машине не нужно (используется **Dr.Web Daemon**, запущенный на другом компьютере в локальной сети), то для переменной `ENABLE` нужно оставить присвоенное по



умолчанию значение 0

5. Откройте enable-файл **Dr.Web Monitor** и установите параметр `ENABLE = 1`. Это позволит запустить **Dr.Web Monitor**.
6. Запустите **Dr.Web Daemon** и **Dr.Web Monitor** через командный интерфейс или файловый менеджер. Все остальные модули **Dr.Web для Novell Storage Services** будут запущены **Dr.Web Monitor**. Каждый из модулей может быть запущен и отдельно, при этом модуль **Dr. Web Agent** должен быть запущен самым первым, поскольку все прочие модули получают настройки через него.

Расположение enable-файлов зависит от способа установки **Dr.Web для Novell Storage Services**:

- Установка при помощи универсального пакета для UNIX:

Файлы располагаются в каталоге `%etc_dir` и называются
`drwebd.enable`,
`drweb-monitor.enable`.

- Установка из нативных DEB-пакетов:

Файлы располагаются в каталоге `%etc_dir/defaults` и называются
`drwebd`,
`drweb-monitor`.

- Установка из нативных RPM-пакетов:

Файлы располагаются в каталоге `%etc_dir/sysconfig` и называются
`drwebd.enable`,
`drweb-monitor.enable`.



Операционные системы 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** или установить значение переменной `allow_execheap` равным 1.

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:

1. Создайте новый файл с исходным кодом политики **SELinux** (.te файл). Данный файл определяет ограничения, относящиеся к описываемому модулю. Исходный файл политики может быть создан:
 - С помощью утилиты **policygentool**. Для этого укажите в качестве параметров имя модуля, работу с которым вы хотите настроить, и полный путь к его исполняемому файлу.



Утилита **policygentool**, входящая в состав пакета **selinux-policy** в **RedHat Enterprise Linux** и **CentOS Linux**, может работать некорректно. В таком случае воспользуйтесь **audit2allow**.

Пример:

Для **Сканера**:

```
# policygentool drweb-scanner /opt/drweb/  
drweb.real
```



Для **Демона**:

```
# policygentool drweb-daemon /opt/drweb/  
drwebd.real
```

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

- С помощью утилиты **audit2allow**. Данная утилита генерирует разрешающие правила на основе сообщений об отказе в доступе в файлах системных журналов. Возможно задать автоматический поиск сообщений в файлах журналов или указать путь к файлу журнала вручную.



В общем случае при использовании в системе демона **audit**, файл журнала располагается в /var/log/audit/audit.log. В противном случае, сообщения о запрете операции записываются в файл журнала /var/log/messages.

Утилита **audit2allow** находится в пакете **polycoreutils-python** (для **RedHat Enterprise Linux, CentOS, Fedora**) или в пакете **python-sepolgen** (для **Debian, Ubuntu**).

Пример:

```
# audit2allow -M -i /var/log/audit/audit.  
log drweb
```

В данном примере **audit2allow** производит поиск сообщений об отказе в доступе в файле **audit.log**.



Пример:

```
# audit2allow -a -M drweb
```

В данном примере **audit2allow** ищет сообщения об отказе в доступе в файлах журналов автоматически.

В обоих случаях в результате работы утилиты создаются два файла: исходный файл политики **drweb.te** и готовый к установке модуль политики **drweb.pp**. Если вы хотите внести изменения в разграничения для работы компонентов **Dr.Web для Novell Storage Services**, отредактируйте файл **drweb.te** соответствующим образом и перейдите к пункту 2. Если вносить изменения в файл политики не требуется, перейдите к пункту 4 для установки модуля политики **drweb.pp**.

- Используя утилиту **checkmodule** создайте бинарное представление (.mod файл) исходного файла локальной политики. Обратите внимание, что для успешной работы этой команды в системе должен быть установлен пакет **checkpolicy**.

Пример:

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

- Создайте устанавливаемый модуль политики (.pp файл) с помощью утилиты **semodule_package**.

Пример:

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

- Для установки созданного модуля политики воспользуйтесь утилитой **semodule**.

**Пример:**

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

Также для разрешения работы компонентов **Dr.Web Scanner** и **Dr.Web Daemon** возможно, но не рекомендуется, установить значение переменной окружения `allow_execheap` равной 1. Переменная окружения `allow_execheap` позволяет или запрещает исполнение данных в куче (*memory heap*) для всех приложений, запущенных в *неограниченном* (*unconfined*) домене.

Чтобы установить значение переменной `allow_execheap`, выполните в командной строке:

```
# setsebool -P allow_execheap=1
```



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 одном каталоге 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 **Dr.Web Enterprise Server** (`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 каталог 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 вышеуказанный каталог.

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, **Dr.Web Scanner** предупредит об этом при запуске. **Dr.Web Daemon** в такой ситуации может извещать пользователя по электронной почте. Сообщения отправляются для каждого установленного ключевого файла при каждом запуске, перезапуске или перезагрузке **Dr.Web Daemon**, 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 каталоге, отличном от стандартного, 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** – резидентный модуль, осуществляющий проверку на вирусы по запросу;
- **Dr.Web Monitor** – вспомогательный модуль, запускающий и останавливающий модули системы в заданном порядке, а также контролирующий их работу;
- **Dr.Web Agent** – модуль, используемый для интеграции с сервисом **Dr.Web Enterprise Security Suite** и собирающий статистическую информацию о работе модулей системы;

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 каталоге, указанном 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, прошедшие первичную фильтрацию, передаются **Dr. Web Daemon** для проверки на вирусы. Параметры настройки взаимодействия с **Dr. Web Daemon** находятся в секции [DaemonCommunication] конфигурационного файла. **Dr. Web NSS** способен работать одновременно как с **Dr. Web Daemon**, запущенным на локальной машине, так и с **Dr. Web Daemon** на удаленных серверах. В параметре **Address** секции [DaemonCommunication] конфигурационного файла вы можете указать список адресов сокетов для связи с **Dr. Web Daemon** и веса этих адресов. При работе с несколькими **Dr. Web Daemon**, **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 **Dr. Web Daemon** 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 **Карантина** 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, а общая статистика передается 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.

В текущей версии **Dr.Web для Novell Storage Services** модуль поддерживает следующие параметры командной строки:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
Описание: Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы модуля		
-v	--version	
Описание: Вывод на экран информации о текущей версии Dr.Web NSS и завершение работы модуля		



Краткий вариант	Расширенный вариант	Аргументы
-l	--level	<уровень>
<u>Описание:</u> Установка используемого уровня детализации файла журнала (значение по умолчанию: info)		
-t	--timeout	<секунды>
<u>Описание:</u> Установка максимального времени ожидания получения конфигурационных данных от Dr.Web Agent		
	--component	<имя>
<u>Описание:</u> Установка имени, под которым данный модуль будет обращаться к Dr.Web Agent для получения конфигурации		
	--log-name	<имя>
<u>Описание:</u> Установка имени, под которым данный модуль будет выводить сообщения в файл журнала		
	--check-only	
<u>Описание:</u> Запуск компонента в режиме проверки конфигурации. Для успешной проверки должен быть запущен Dr.Web Agent . Если при проверке не было найдено ошибок, выводится сообщение Options OK, а если были найдены ошибки, то 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 обращением к **Dr.Web Agent** через сокет 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 управляемыми 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 каталог, указанный 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 `cli` выводятся число соединений, созданных по запросу и закрытых по тайм-ауту, их среднее и текущее количество:

```
created on request = 0 (0 num/sec)
closed by timeout = 0 (0 num/sec)
avg number = 0
current = 2
```

Для `thr` 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

Каталог **Карантина** используется для изоляции зараженных и подозрительных файлов. В **Карантин** перемещаются все файлы, для которых определено действие `quarantine`. Каталог **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 **NSS** реализована только начиная с **Open Enterprise Server 2**.

Подробнее про использование расширенных атрибутов **Linux** можно прочитать в [документации Open Enterprise Server](#).

Управление через `drweb-nss-qcontrol`

Для управления **Карантином** 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 **Dr.Web Agent**, от которого будет получены конфигурационные параметры. Если значение параметра не задано, то запрос конфигурации от **Dr.Web Agent** не происходит, и используются параметры командной строки и значения по умолчанию;
- `--timeout <время>` – максимальное время ожидания получения конфигурационных параметров от **Dr.Web Agent** и ответа от **Dr.Web Daemon**;
- `--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 **Dr.Web Daemon**;
- АТРИБУТЫ — 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 каталога **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 каталог, указанный в этом параметре, свойства файла поддерживаемые только **NSS** будут восстановлены только если новый каталог 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, извлеченный из **Карантина**.

Пример:

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

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

- `--restore-dir <каталог>` – при выполнении действия `--restore` восстанавливать восстановить файлы в указанный каталог, а не в исходное местоположение. Если указанный каталог 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 слово `'eicar'`, в каталог `"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 **Dr.Web Daemon** 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 журнала Dr.Web NSS

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 **Dr.Web Agent**, 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 **Dr.Web Agent**, уровень подробности будет установлен в соответствии с конфигурацией **Dr.Web Agent**.

Проверка конфигурации

Вы можете проверить корректность изменений, произведенных в конфигурационных файлах, или параметров, получаемых модулями от **Dr.Web Agent**. Для этого каждый модуль поддерживает параметр командной строки `--check-only`. Этот параметр может использоваться только при запущенном **Dr.Web Agent**, 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 **Dr.Web Monitor** 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
Секция [General]	
BaseDir = { путь к каталогу }	Основной рабочий каталог, в котором содержатся сокеты, база данных и другие файлы. В текущей версии этот параметр не может быть изменен при перезапуске по сигналу <code>SIGHUP</code> . <u>Значение по умолчанию:</u> BaseDir = <code>/var/drweb</code>
MaxTimeoutForThreadActivity = { время }	Максимальное время закрытия одного потока. Параметр используется при перезапуске, а также при завершении работы.



Параметр	Описание
	<p>Общее максимальное время завершения работы рассчитывается следующим образом: количество пулов умножается на значение этого параметра и к результату прибавляется некоторая временная константа.</p> <p><u>Значение по умолчанию:</u></p> <p>MaxTimeoutForThreadActivity = 2m</p>
IpTimeout = { время }	<p>Максимальное время установки соединения между компонентами.</p> <p><u>Значение по умолчанию:</u></p> <p>IpTimeout = 2m</p>

Секция [Logging]

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

Параметр	Описание
Секция [Logging]	
Level = { уровень подробности }	<p><u>Уровень подробности</u> сохранения в журнал работы компонента общих событий.</p> <p>Допускается использование следующих уровней:</p> <ul style="list-style-type: none">• Quiet• Error• Alert• Info• Debug <p><u>Значение по умолчанию:</u></p> <p>Level = Info</p>



Параметр	Описание
IpсLevel = { уровень подробности}	<u>Уровень подробности</u> сохранения в журнал работы компонента событий подсистемы IPC. Допускается использование следующих уровней: <ul style="list-style-type: none">• Quiet• Error• Alert• Info• Debug <u>Значение по умолчанию:</u> IpсLevel = Alert
SyslogFacility = { метка syslog}	<u>Метка записи</u> при использовании системного сервиса syslog . <u>Значение по умолчанию:</u> SyslogFacility = Daemon
FileName = { syslog путь к файлу}	Имя файла журнала или syslog, если журнал будет вестись средствами системного сервиса syslog <u>Значение по умолчанию:</u> FileName = syslog

Секция [NSS]

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

Параметр	Описание
Секция [NSS]	
NSSVolumesMountDir = { путь к каталогу}	Путь к каталогу, в котором смонтированы все разделы NSS . Список защищаемых разделов указывается в значении параметра



Параметр	Описание
	<p>ProtectedVolumes.</p> <p><u>Значение по умолчанию:</u></p> <p>NSSVolumesMountDir = /media/nss</p>
ProtectedVolumes = { список разделов }	<p>Список защищаемых разделов. Значения разделены запятыми.</p> <p>Если список пустой, то будут защищаться все каталоги в каталоге, указанном в параметре NSSVolumesMountDir. Если в этом каталоге не все каталоги являются разделами NSS, произойдет ошибка при инициализации.</p> <p><u>Значение по умолчанию:</u></p> <p>ProtectedVolumes =</p>
CheckPoolOptions = { настройки пула }	<p>Настройки пула потоков для обработки заданий на проверку.</p> <p><u>Значение по умолчанию:</u></p> <p>CheckPoolOptions = { 2-20 }</p>
HeuristicAnalysis = { логический }	<p>Включение/выключение Эвристического анализатора.</p> <p>Эвристический анализатор позволяет обнаруживать неизвестные вирусы, не включенные в вирусные базы данных.</p> <p>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.</p> <p>Вы можете прислать такие файлы в компанию "Доктор Веб" на анализ</p>



Параметр	Описание
	<p>через сайт http://vms.drweb.com/sendvirus.</p> <p>Использование Эвристического анализатора может привести к увеличению времени сканирования.</p> <p><u>Значение по умолчанию:</u></p> <p>HeuristicAnalysis = Yes</p>
MaxFileSizeToScan = { размер}	<p>Максимальный размер файла для проверки. Если размер файла превышает указанный, файл не будет отправляться Dr.Web Daemon на сканирование. Если установлено значение 0, размер файла не проверяется.</p> <p><u>Значение по умолчанию:</u></p> <p>MaxFileSizeToScan = 0b</p>
IncludedPaths = { список путей}	<p>Список относительных путей, которые всегда требуется проверять.</p> <p>Все пути, которые начинаются со значений, указанных в данном параметре, будут проверяться на вирусы, вне зависимости от параметра ExcludedPaths.</p> <p>Пути указываются относительно каталога, указанного в параметре NSSVolumesMountDir: сначала указывается раздел, а затем его подкаталоги и файлы.</p> <p>Пути должны указываться в абсолютном виде (без использования символов текущего и вышестоящего каталога: "." и "..").</p> <p><u>Значение по умолчанию:</u></p> <p>IncludedPaths =</p>
ExcludedPaths = { список путей}	<p>Список относительных путей, которые не требуется проверять.</p>



Параметр	Описание
	<p>Все пути, которые начинаются со значений, указанных в данном параметре, не будут проверяться на вирусы, если они не указаны в параметре IncludedPaths.</p> <p>Пути указываются относительно каталога, указанного в параметре NSSVolumesMountDir: сначала указывается раздел, а затем его подкаталоги и файлы.</p> <p>Пути должны указываться в абсолютном виде (т.е. без использования символов текущего и вышестоящего каталога: ". " и ". .").</p> <p><u>Значение по умолчанию:</u></p> <p>ExcludedPaths =</p>

Секция [DaemonCommunication]

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

Параметр	Описание
Секция [DaemonCommunication]	
Address = { взвешенный список адресов }	<p>Список сокетов, через которые Dr.Web NSS взаимодействует с Dr.Web Daemon.</p> <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</p>



Параметр	Описание
	<p>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> <p>Указываем несколько адресов с весами:</p> <pre>Address = pid: /var/drweb/run/drwebd.pid 10, \inet: 3000@srv2.example.com 5</pre> <p><u>Значение по умолчанию:</u></p> <pre>Address = pid: /var/drweb/run/drwebd.pid 1</pre>
Timeout = { время}	<p>Максимальное время ожидания исполнения команды Dr.Web Daemon.</p> <p>Если значение параметра равно 0, время ожидания не ограничено.</p> <p><u>Значение по умолчанию:</u></p> <pre>Timeout = 2m</pre>



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 каталог **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
Секция [Actions]	
Infected = { действие }	Действие в случае, если файл заражен известным вирусом. Доступные действия: <code>remove, quarantine, cure</code> <u>Значение по умолчанию:</u> Infected = <code>cure</code>
Suspicious = { действие }	Действие в случае, если, возможно, файл заражен неизвестным вирусом. Доступные действия: <code>remove, quarantine, pass, report</code>



Параметр	Описание
	<u>Значение по умолчанию:</u> Suspicious = quarantine
Incurable = { действие }	Действие в случае, если файл заражен и не может быть вылечен. Доступные действия: remove, quarantine <u>Значение по умолчанию:</u> Incurable = quarantine
Adware = { действие }	Действие в случае, если файл содержит программу для показа рекламы (adware). Доступные действия: remove, quarantine, pass, report <u>Значение по умолчанию:</u> Adware = quarantine
Dialers = { действие }	Действие в случае, если файл содержит программу автоматического дозвона. Доступные действия: remove, quarantine, pass, report <u>Значение по умолчанию:</u> Dialers = quarantine
Jokes = { действие }	Действие в случае, если файл содержит программу-шутку, которая может пугать или раздражать пользователя. Доступные действия: remove, quarantine, pass, report <u>Значение по умолчанию:</u> Jokes = report



Параметр	Описание
Riskware = { действие}	<p>Действие в случае, если файл содержит потенциально опасную программу, которая может быть использована не только ее владельцем, но и злоумышленниками.</p> <p>Доступные действия:</p> <p>remove, quarantine, pass, report</p> <p><u>Значение по умолчанию:</u></p> <p>Riskware = report</p>
ArchiveRestriction = { действие}	<p>Действие, совершаемое с архивами, которые не были проверены Dr.Web Daemon из-за ограничений, заданных для архивов в главном конфигурационном файле drweb32.ini.</p> <p>Доступные действия:</p> <p>remove, quarantine, pass, report</p> <p><u>Значение по умолчанию:</u></p> <p>ArchiveRestriction = quarantine</p>
Hacktools = { действие}	<p>Действие в случае, если файл содержит программу, предназначенную для получения несанкционированного доступа к компьютерным системам.</p> <p>Доступные действия:</p> <p>remove, quarantine, pass, report</p> <p><u>Значение по умолчанию:</u></p> <p>Hacktools = report</p>
SkipObject = { действие}	<p>Действие, совершаемое с файлами, которые не могут быть проверены Dr. Web Daemon.</p>



Параметр	Описание
	<p>Доступные действия:</p> <p>remove, quarantine, pass, report</p> <p><u>Значение по умолчанию:</u></p> <p>SkipObject = report</p>
DaemonError = { действие }	<p>Действие, применяемое к файлам, при сканировании которых у Dr.Web Daemon возникли ошибки.</p> <p>Доступные действия:</p> <p>remove, quarantine, pass, report</p> <p><u>Значение по умолчанию:</u></p> <p>DaemonError = quarantine</p>
LicenseError = { действие }	<p>Действие, применяемое к файлам, которые не были проверены Dr.Web Daemon по причине лицензионных ограничений.</p> <p>Доступные действия:</p> <p>remove, quarantine, pass, report</p> <p><u>Значение по умолчанию:</u></p> <p>LicenseError = report</p>
ProcessingError = { действие }	<p>Действия применяемые к файлам, при обработке которых у Dr.Web NSS возникли ошибки.</p> <p>Доступные действия:</p> <p>remove, quarantine, pass, report</p> <p><u>Значение по умолчанию:</u></p> <p>ProcessingError = report</p>



Секция [Stat]

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

Параметр	Описание
Секция [Stat]	
SendToAgent = { логический}	Включение/выключение отправления Dr.Web Agent статистической информации о работе Dr.Web NSS . Если установлено значение No , сбор статистики не производится. <u>Значение по умолчанию:</u> SendToAgent = Yes
SendPeriod = { время}	Промежуток времени, через который общая статистика посылается Dr.Web Agent . <u>Значение по умолчанию:</u> SendPeriod = 5m

Секция [Quarantine]

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

Параметр	Описание
Секция [Quarantine]	
Path = { путь к каталогу}	Путь к каталогу Карантина . У Dr.Web NSS должны быть права на создание, изменение, удаление и чтение файлов в этом каталоге.



Параметр	Описание
	<u>Значение по умолчанию:</u> Path = /var/drweb/infected/nss
FilesMode = { права }	Права доступа, устанавливаемые для файлов, которые перемещаются в Карантин . <u>Значение по умолчанию:</u> FilesMode = 0660

Секция [Notifications]

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

Параметр	Описание
Секция [Notifications]	
ExternalProgram = { строка }	<p>Команда для запуска внешней программы, после выполнения <u>действия над файлом</u> (remove, quarantine, cure, report). После выполнения команды событие записывается в журнал.</p> <p>Поток, выполняющий команду, ждет ее завершения, и, если код возврата отличен от 0, вносит соответствующую запись в журнал.</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;



Параметр	Описание
	<ul style="list-style-type: none">• \$VERSION\$ - текущая версия продукта;• \$FILE\$ - полный путь к файлу, при обработке которого возникло событие;• \$SIZE\$ - размер (в байтах) файла, приведшего к возникновению события;• \$TIME\$ - локальное время на сервере в момент, когда была выполнена эта команда;• \$DAEMON_REPORT\$ - отчет Dr.Web Daemon, 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>Attention, \$REASON\$ event is occurred!
File \$FILE\$ (size=\$SIZE\$)
 action=\$ACTION\$
</html>\" 10"</pre> <p>В системе KDE при каждом событии (обнаружение угрозы, ошибка сканирования и т.п.) будет выводиться всплывающее окно с описанием события.</p>



Параметр	Описание
	<p><u>Значение по умолчанию:</u></p> <p>ExternalProgram =</p>
SendMail = { логический }	<p>Включение/выключение отправки почтовых уведомлений после выполнения <u>действия над файлом</u> remove, quarantine, cure и report.</p> <p>Команда отправки уведомления выполняется после выполнения действия над файлом, но до записи этого события в журнал.</p> <p>Письмо с уведомлением отправляется по адресу, указанному в значении параметра Hostmaster данной секции. Шаблоны для писем берутся из каталога, указанного в значении параметра Templates.</p> <p><u>Значение по умолчанию:</u></p> <p>SendMail = No</p>
Templates = { путь к каталогу }	<p>Путь к каталогу, содержащему 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> <p><u>Значение по умолчанию:</u></p> <p>Templates = /etc/drweb/templates/nss</p>
Hostmaster = { адрес e-mail }	<p>Адрес электронной почты, на который отправляются уведомления.</p> <p><u>Значение по умолчанию:</u></p> <p>Hostmaster = root@localhost</p>
MailCommand = { строка }	<p>Команда shell, выполняемая для отправления администратору</p>



Параметр	Описание
	<p>уведомлений о происходящих событиях.</p> <p><u>Значение по умолчанию:</u></p> <pre>MailCommand = "/usr/sbin/ sendmail -i -bm -f drweb-nss -- %s"</pre>



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 каталоге, содержащем исполняемые файлы программного комплекса **Dr. Web для Novell Storage Services**.

Модуль обновления **Dr.Web Updater** требует наличия установленного **Perl 5.8.0** и выше.

Настройки модуля обновления **Dr.Web Updater** хранятся в в секции `[Updater]` главного конфигурационного файла (`drweb32.ini` по умолчанию), который находится в каталоге `%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]
```

Перечень параметров, которые можно использовать, см. в разделе [Параметры командной строки](#).

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 **Всемирной Системы Обновлений Dr.Web (BCO Dr.Web)** эти



файлы могут храниться также в lзма-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 (`drwXXXYY.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 каталог программного комплекса **Dr.Web для Novell Storage Services** (по умолчанию в `%var_dir/bases/`) или иной каталог, определенный 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 `dwrXXXXYY.vdb` и `dwnXXXXYY.vdb`, а также "горячие" обновления `dwrtoday.vdb` и `dwntoday.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 **Dr.Web Engine**. Одновременно с этим сводятся воедино все ранее выпущенные дополнения баз, и новая версия пакета комплектуется новейшими вирусными базами, содержащими описания 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;
- `dwrtoday.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;

- `dwrtday.vdb` – "горячие" дополнения базы потенциально опасных программ.

Вирусные базы могут быть автоматически обновлены, используя модуль обновления компонентов **Dr.Web Updater** (`%bin_dir/update.pl`).

После установки **Dr.Web для Novell Storage Services** автоматически создаётся файл расписания **cron** (`/etc/cron.d/drweb-update`) для запуска **Dr.Web Updater** каждые 30 минут. Это обеспечивает регулярное обновление и наилучшую защиту.

Настройка cron

При установке компонентов программного комплекса в каталоге `/etc/cron.d/` будет создан пользовательский файл расписания 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**.

Обратите внимание, что по умолчанию демон **cron** будет запускать модуль **Dr.Web Updater** с периодичностью раз в 30 минут (в 0 и 30 минут каждого часа). Это может вызывать повышенную нагрузку на сервера **BCO Dr.Web** и приводить к задержке обновления. Чтобы избежать подобной ситуации, рекомендуется изменить моменты запуска, заданные 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 скрипта 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>` – 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>` – список имен компонентов, разделенных запятыми.

Пример:

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



Обратите внимание, что 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 рабочем каталоге их резервные копии. Это позволяет вернуть компонент к предыдущему состоянию в случае каких-либо проблем с обновлением.

Чтобы восстановить компонент к предыдущему состоянию,



следует запустить **Dr.Web 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 каталоге `%etc_dir`.

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



Секция [Updater]

UpdatePluginsOnly = { логический }	<p>Значение Yes предписывает модулю не производить обновление Dr.Web Daemon и Dr.Web Scanner, а ограничиться только обновлением плагинов.</p> <p><u>Значение по умолчанию:</u></p> <p>UpdatePluginsOnly = No</p>
Section = { Daemon Scanner }	<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.</p> <p>Возможные значения параметра: Scanner или Daemon.</p> <p>Значение параметра возможно временно переопределить при запуске модуля обновления с помощью параметра командной строки --what. Измененное таким образом значение параметра будет действовать до следующего запуска скрипта.</p> <p><u>Значение по умолчанию:</u></p> <p>Section = Daemon</p>
ProgramPath = { путь к файлу }	<p>Путь к исполняемому файлу компонента, который будет обновляться.</p> <p>Требуется модулю обновления для получения информации о версии компонента.</p> <p><u>Значение по умолчанию:</u></p> <p>ProgramPath = %bin_dir/drwebd</p>
SignedReader = { путь к файлу }	<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 каталогу }</pre>	<p>Путь к каталогу, в котором располагается утилита <code>lzma</code>, используемая для распаковывания <code>lzma</code>-архивов.</p> <p><u>Значение по умолчанию:</u></p> <pre>LzmaDecoderPath = %bin_dir/</pre>
<pre>LockFile = { путь к файлу }</pre>	<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> <pre>LockFile = %var_dir/run/ update.lock</pre>
<pre>CronSummary = { логический }</pre>	<p>Значение <code>Yes</code> предписывает модулю обновления выдавать отчет сессии обновления на стандартный вывод (<code>stdout</code>).</p> <p>Данный режим используется для отправки уведомлений администратору по электронной почте при запуске модуля обновления демоном cron.</p> <p><u>Значение по умолчанию:</u></p> <pre>CronSummary = Yes</pre>
<pre>Dr1File = { путь к файлу }</pre>	<p>Путь к специальному файлу, содержащему список серверов обновления BCO Dr.Web.</p> <p>Модуль обновления выбирает сервера обновления из этого списка случайным образом.</p> <p>Подробнее об алгоритме выбора сервера</p>



	<p>для обновления см. в разделе Процедура обновления</p> <p>Данный файл подписан компанией Доктор Веб, не подлежит редактированию пользователем и обновляется автоматически.</p> <p><u>Значение по умолчанию:</u></p> <pre>DrlFile = %var_dir/bases/ update.drl</pre>
<pre>CustomDrlFile = { путь к файлу}</pre>	<p>Путь к файлу, содержащему альтернативный список серверов обновления BCO Dr.Web.</p> <p>Модуль обновления выбирает сервера обновления из этого списка случайным образом.</p> <p>Подробнее об алгоритме выбора сервера для обновления см. в разделе Процедура обновления</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 = { логический}</pre>	<p>Разрешение использовать файл DrlFile в том случае, если не удалось подключиться ни к одному из серверов, заданных в файле CustomDrlFile.</p> <p>В случае если значение параметра No, файл DrlFile не используется.</p> <p>В случае если файл CustomDrlFile не существует, обращение к файлу DrlFile производится вне зависимости от значения параметра FallbackToDrl.</p>



	<p>Подробнее об алгоритме выбора сервера для обновления см. в разделе Процедура обновления</p> <p><u>Значение по умолчанию:</u></p> <p>FallbackToDrl = Yes</p>
<p>DrlDir = { путь к каталогу }</p>	<p>Путь к каталогу, содержащему подписанные Доктор Веб drl-файлы со списками серверов обновления BCO Dr. Web для каждого из плагинов.</p> <p><u>Значение по умолчанию:</u></p> <p>DrlDir = %var_dir/drl/</p>
<p>Timeout = { числовое значение }</p>	<p>Максимальное время ожидания для загрузки обновлений с BCO Dr.Web в секундах.</p> <p><u>Значение по умолчанию:</u></p> <p>Timeout = 90</p>
<p>Tries = { числовое значение }</p>	<p>Количество попыток установки соединения модулем обновления Dr.Web Updater с серверами BCO Dr.Web</p> <p><u>Значение по умолчанию:</u></p> <p>Tries = 3</p>
<p>ProxyServer = { IP-адрес имя хоста }</p>	<p>Имя или IP-адрес используемого прокси-сервера.</p> <p><u>Значение по умолчанию:</u></p> <p>ProxyServer =</p>
<p>ProxyLogin = { текст }</p>	<p>Имя пользователя прокси-сервера.</p> <p><u>Значение по умолчанию:</u></p> <p>ProxyLogin =</p>
<p>ProxyPassword =</p>	<p>Пароль пользователя прокси-сервера.</p>



	<p><u>Значение по умолчанию:</u></p> <p>ProxyPassword =</p>
<p>LogFileName = {syslog путь к файлу}</p>	<p>Имя файла журнала или syslog, если журнал будет вестись средствами системного сервиса syslog</p> <p><u>Значение по умолчанию:</u></p> <p>LogFileName = syslog</p>
<p>SyslogFacility = {метка syslog}</p>	<p><u>Метка записи</u> при использовании системного сервиса syslog</p> <p><u>Значение по умолчанию:</u></p> <p>SyslogFacility = Daemon</p>
<p>LogLevel = {уровень подробности}</p>	<p><u>Уровень подробности</u> ведения журнала.</p> <p>Допускается использование следующих уровней:</p> <ul style="list-style-type: none">• Quiet• Error• Warning• Info• Debug• Verbose <p><u>Значение по умолчанию:</u></p> <p>LogLevel = Info</p>
<p>AgentConfPath = {путь к файлу}</p>	<p>Путь к конфигурационному файлу Dr. Web Agent.</p> <p><u>Значение по умолчанию:</u></p> <p>AgentConfPath = %var_dir/ agent.conf</p>
<p>ExpiredTimeLimit = {числовое значение}</p>	<p>Количество дней до истечения срока действия лицензии, в течение которых Dr.Web Updater будет пытаться обновить лицензионный ключевой файл.</p>



	<u>Значение по умолчанию:</u> ExpiredTimeLimit = 14
ESLockfile = { путь к файлу }	Путь к блокирующему файлу. Если данный файл существует, то Dr. Web Updater перестает использовать расписания cron для обновления. <u>Значение по умолчанию:</u> ESLockfile = %var_dir/run/es_updater.lock

Процедура обновления

Обновление происходит следующим образом:

1. Модуль обновления **Dr.Web Updater** читает конфигурационный файл (по умолчанию – drweb32.ini).
2. Из конфигурационного файла используются параметры, находящиеся в секции [Updater] (описание параметров см. [ВЫШЕ](#)), а также параметры **EnginePath**, **VirusBase**, **UpdatePath** и **PidFile**.
3. **Dr.Web Updater** выбирает сервер **BCO Dr.Web** для получения обновлений. Выбор сервера обновления происходит следующим образом:
 - Производится чтение файлов со списками серверов, указанных в параметрах **DrlFile** и **CustomDrlFile** конфигурационного файла;
 - Если оба файла отсутствуют, то обновление не происходит;
 - Если существует только один из файлов (указанный в **DrlFile** или **CustomDrlFile**), то используется существующий, вне зависимости от значения, указанного в параметре **FallbackToDrl**;
 - Если существуют оба файла, то в первую очередь проверяются сервера из файла, указанного в



`CustomDrlFile;`

- Если не получилось подключиться ни к одному из серверов, заданных в файле, указанном в `CustomDrlFile`, и значение параметра `FallbackToDrl=Yes`, то проверяются сервера из файла, указанного в `DrlFile`. В противном случае обновление не происходит.
4. Производятся попытки подключения к случайно выбираемым серверам из списка, содержащегося в файле, до тех пор, пока попытка подключения к серверу не окажется успешной (при подключении **Dr.Web Updater** ожидает ответа от выбранного сервера ответа в течение периода времени, указанного в параметре `Timeout`).
 5. Модуль запрашивает с сервера **BCO Dr.Web**, к которому удалось подключиться, список обновлений, а 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 (точнее, к каталогу, в котором она располагается) задается значением параметра `LzmaDecoderPath`.
 6. Обновления раскладываются по каталогам, как описано в разделе [Обновление антивируса и вирусных баз](#).



Dr.Web Agent

Компонент **Dr.Web Agent** 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 статистику вирусных инцидентов. Эта статистика, в зависимости от режима работы **Dr.Web Agent**, отсылается с заданной периодичностью либо на публичный сервер статистики компании **Доктор Веб**, либо на сервер централизованной защиты, под управлением которого работает **Dr.Web Agent**.

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

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

Пожалуйста, обратите внимание, что если в конфигурационном файле компонента указано несколько параметров с одним именем, то **Dr.Web Agent** их объединяет через запятую. При задании значений параметров в конфигурационных файлах можно использовать обратный слэш "\". В этом случае **Dr.Web Agent** объединит в одну строку все строки, разделённые с помощью обратного слэша. Обратите внимание, что использование пробела после символа 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, **Dr.Web Agent** 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 **Dr.Web Agent** полностью управляется с защищаемого компьютера. Статистика вирусных инцидентов отсылается на сервер статистики компании "**Доктор Веб**".
- Режим 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. Статистика вирусных инцидентов отсылается на управляющий сервер централизованной защиты.

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 **Dr.Web Agent** (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 ESS (далее – **Dr.Web Enterprise Server**). Если вы – администратор сети, то вы можете найти этот файл в соответствующем каталоге на **Dr.Web Enterprise Server**.

- Укажите IP-адрес или имя узла **Dr.Web Enterprise Server** в параметре **ServerHost**.
 - Укажите номер порта для связи с **Dr.Web Enterprise Server** 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 **Dr.Web Agent** в режиме центральной защиты должен быть установлен пакет `drweb-agent-es`.

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

Чтобы использовать одиночный (standalone) режим

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



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 другой каталог файлы

`%etc_dir/agent/drweb-cc.amc` и

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

Рекомендуется сохранить эти файлы в качестве резервной копии в каталоге, отличном от `%etc_dir/agent`, если в дальнейшем вы планируете 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 каталог `%etc_dir/agent/` и следуйте инструкциям, представленным в руководстве пользователя **Антивируса Dr.Web для Linux**.



Параметры командной строки

Для запуска **Dr.Web Agent** используется следующая команда:

```
drweb-agent [параметры]
```

Dr.Web Agent допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
<u>Описание:</u> Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы модуля		
-v	--version	
<u>Описание:</u> Вывод на экран информации о текущей версии Dr.Web Agent и завершение работы модуля		
-u	--update-all	
<u>Описание:</u> Запуск процесса обновления для всех компонентов Dr. Web для Novell Storage Services		
-f	--update-failed	
<u>Описание:</u> Запуск процесса обновления для тех компонентов Dr.Web для Novell Storage Services , которые не удалось обновить в штатном режиме		
-C	--check-only	
<u>Описание:</u> Проверка корректности конфигурации модуля Dr.Web Agent . Данный параметр командной строки не может быть использован при наличии в системе уже запущенного экземпляра Dr. Web Agent		
-c	--conf	<путь к файлу>
<u>Описание:</u> Использование при запуске указанного конфигурационного файла		



Краткий вариант	Расширенный вариант	Аргументы
-d	--droppwd	
<u>Описание:</u> Сбросить регистрационную информацию (имя пользователя и пароль), используемую Dr.Web Agent для доступа к Dr.Web Enterprise Server . При следующей попытке соединения с Dr.Web Enterprise Server будет запущен процесс регистрации новой станции		
-p	--newpwd	
<u>Описание:</u> Смена имени пользователя и пароля на используемом сервере центральной защиты Dr.Web Enterprise Server		
-s	--socket	<путь к файлу>
<u>Описание:</u> Использование компонентом для коммуникации с управляемыми модулями сокета, указанного в аргументе		
-P	--pid-file	<путь к файлу>
<u>Описание:</u> Использование в качестве PID-файла Dr.Web Agent файла, указанного в аргументе		
-e	--export-config	<имя приложения>
<u>Описание:</u> Экспорт конфигурации приложения, имя которого указано в аргументе, на Dr.Web Enterprise Server . В качестве аргумента следует использовать имя приложения, указанное в заголовке секции Application "<имя приложения>" соответствующего amc-файла (см. раздел Взаимодействие с компонентами программного комплекса). Данный параметр командной строки не может быть использован при наличии в системе уже запущенного экземпляра Dr. Web Agent . Также он 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`.



Общие принципы устройства конфигурационных файлов компонентов **Dr.Web для Novell Storage Services** и краткое описание правил задания параметров конфигурации приведены в разделе [Конфигурационные файлы](#).

Секция [Logging]

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

Секция [Logging]

Level =
{ уровень
подробности}

[Уровень_подробности](#) сохранения в журнал работы компонента общих событий.

Допускается использование следующих уровней:

- Quiet
- Error
- Alert
- Info
- Debug

Значение по умолчанию:

Level = Info

IPCLevel =
{ уровень
подробности}

[Уровень_подробности](#) сохранения в журнал работы компонента событий подсистемы IPC.

Допускается использование следующих уровней:

- Quiet
- Error
- Alert
- Info
- Debug



	<u>Значение по умолчанию:</u> IPCLevel = Error
SyslogFacility = {метка syslog}	<u>Метка записи</u> при использовании системного сервиса syslog <u>Значение по умолчанию:</u> SyslogFacility = Daemon
FileName = {syslog путь к файлу}	Имя файла журнала или syslog, если нужно использовать системный сервис syslog <u>Значение по умолчанию:</u> FileName = syslog

Секция [Agent]

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

Секция [Agent]

MetaConfigDir = {путь к каталогу}	Расположение файлов мета-конфигурации Dr.Web Agent . В файлах мета-конфигурации описываются особенности взаимодействия Dr.Web Agent с другими модулями программного комплекса. Содержание файлов мета-конфигурации задается разработчиками "Доктор Веб" и не требует редактирования. <u>Значение по умолчанию:</u> MetaConfigDir = %etc_dir/ agent/
UseMonitor = {логический}	Значение Yes данного параметра, указывает Dr.Web Agent , что в составе программного комплекса используется



	Dr.Web Monitor. <u>Значение по умолчанию:</u> UseMonitor = Yes
MonitorAddress = { адрес }	Сокет, через который Dr.Web Agent взаимодействует с Dr.Web Monitor (значение параметра должно совпадать со значением параметра Address конфигурационного файла Dr.Web Monitor). <u>Значение по умолчанию:</u> MonitorAddress = local:% var_dir/ipc/.monitor
MonitorResponseTime = { числовое значение }	Максимальное время отклика Dr.Web Monitor в секундах. Если в течение этого времени от Dr.Web Monitor не поступает реакции, то предполагается, что он не запущен, и Dr.Web Agent больше не предпринимает попыток взаимодействия с Dr.Web Monitor . <u>Значение по умолчанию:</u> MonitorResponseTime = 5
PidFile = { путь к файлу }	Путь к файлу, в который записывается PID исполняемого 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 }	<p>Сокет, через который Dr.Web Agent взаимодействует с другими модулями программного комплекса.</p> <p>Допускается несколько сокетов, перечисленных через запятую.</p> <p><u>Значение по умолчанию:</u></p> <p>Address = local:%var_dir/ ipc/.agent, inet:4040@127.0.0.1</p>
Threads = { числовое значение }	<p>Количество одновременных потоков drweb-agent.</p> <p>Параметр управляет максимальным количеством одновременных подключений к модулям, передающим Dr.Web Agent вирусную статистику. Этот параметр не может быть изменен при перезапуске по сигналу <code>SIGHUP</code>.</p> <p>Если указано значение 0, количество одновременных потоков не ограничивается (не рекомендуется).</p> <p><u>Значение по умолчанию:</u></p> <p>Threads = 2</p>
Timeout = { числовое значение }	<p>Максимальное время (в секундах) установления соединения между Dr. Web Agent и другими компонентами программного комплекса.</p> <p>Если указано значение 0, время установления соединения не ограничивается.</p>



	<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 = { логический}	При значении Yes данного параметра Dr.Web Agent работает в режиме Enterprise , при значении No – в режиме Standalone . <u>Значение по умолчанию:</u> UseEnterpriseMode = No
ComputerName = { текст}	Название этого компьютера в Антивирусной сети . <u>Значение по умолчанию:</u> ComputerName =
VirusbaseDir = { путь к каталогу}	Путь к каталогу вирусных баз. <u>Значение по умолчанию:</u> VirusbaseDir = %var_dir/bases
PublicKeyFile = { путь к файлу}	Путь к файлу открытого ключа для доступа к Dr.Web Enterprise Server . <u>Значение по умолчанию:</u> PublicKeyFile = %bin_dir/ drwcsd.pub
ServerHost = { IP-адрес}	IP-адрес Dr.Web Enterprise Server . <u>Значение по умолчанию:</u> ServerHost = 127.0.0.1



ServerPort = { числовое значение }	<p>Номер порта доступа к Dr.Web Enterprise Server.</p> <p><u>Значение по умолчанию:</u></p> <p>ServerPort = 2193</p>
CryptTraffic = { Yes Possible No }	<p>Шифрование трафика, передаваемого между Dr.Web Enterprise Server и Dr. Web Agent:</p> <ul style="list-style-type: none">• Yes – обязательно шифровать• Possible – если возможно• No – не шифровать <p><u>Значение по умолчанию:</u></p> <p>CryptTraffic = possible</p>
CompressTraffic = { Yes Possible No }	<p>Сжатие трафика, передаваемого между Dr.Web Enterprise Server и Dr.Web Agent:</p> <ul style="list-style-type: none">• Yes – обязательно шифровать• Possible – если возможно• No – не шифровать <p><u>Значение по умолчанию:</u></p> <p>CompressTraffic = possible</p>
CacheDir = { путь к каталогу }	<p>Путь к каталогу, в котором хранятся служебные файлы: конфигурационные файлы компонентов и файлы, содержащие информацию о правах каждого из приложений, на случай, если Dr.Web Enterprise Server по какой-либо причине окажется недоступен, файлы с регистрационной информацией на Dr.Web Enterprise Server и т.п.</p> <p><u>Значение по умолчанию:</u></p> <p>CacheDir = %var_dir/agent</p>



Секция [StandaloneMode]

Настройки **Dr.Web Agent** для одиночного режима работы.

Секция [StandaloneMode]

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



	<p><u>Пример:</u></p> <pre>StatisticsProxyAuth = test: testpwd</pre> <p><u>Значение по умолчанию:</u></p> <pre>StatisticsProxyAuth =</pre>
<pre>UUID = { текст }</pre>	<p>Личный идентификатор пользователя на сервере статистики http://stat.drweb.com/.</p> <p>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).</p> <p><u>Значение по умолчанию:</u></p> <pre>UUID =</pre>
<pre>LicenseFile = { список путей к файлам }</pre>	<p>Расположение ключевых файлов программного комплекса Dr.Web для Novell Storage Services (лицензионных или демонстрационных).</p> <p>Пути в списке разделяются запятой</p> <p><u>Значение по умолчанию:</u></p> <pre>LicenseFile = %bin_dir/ drweb32.key</pre>



Секция [Update]

В этой секции собраны параметры, относящиеся к процессу обновления компонентов программного комплекса **Dr.Web для Novell Storage Services** через **Dr.Web Enterprise Server** (подробнее см. в Руководстве администратора антивирусной сети **Dr.Web ESS**):

Секция [update]

CacheDir = { путь к каталогу }	<p>Каталог, в котором Dr.Web Agent временно сохраняет загруженные файлы обновлений.</p> <p><u>Значение по умолчанию:</u></p> <p>CacheDir = %var_dir/updates/cache</p>
Timeout = { числовое значение }	<p>Максимальное время обработки Dr.Web Agent полученных обновлений в секундах.</p> <p>Если указано значение 0, время обработки не ограничивается.</p> <p><u>Значение по умолчанию:</u></p> <p>Timeout = 120</p>
RootDir = { путь к каталогу }	<p>Путь к корневому каталогу.</p> <p><u>Значение по умолчанию:</u></p> <p>RootDir = /</p>

Запуск



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



В процессе запуска **Dr.Web Agent** 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**), **Dr.Web Agent** запускается в режиме **Enterprise**. В противном случае, если в файле настроек заданы параметры секции [Standalone], **Dr. Web Agent** запускается в одиночном режиме. Если параметры секции [Standalone] также не заданы, то загрузка **Dr.Web Agent** 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, то он может быть создан только тогда, когда каталог, содержащий его, доступен на запись и чтение пользователю, с чьими правами работает модуль **drweb-agent**. Если ни один сокет не может быть создан, загрузка **Dr.Web Agent** прекращается.

Дальнейший процесс загрузки **Dr.Web Agent** зависит от того, в каком режиме он работает.

Если **Dr.Web Agent** работает в режиме **Enterprise**:

- производится соединение с **Dr.Web Enterprise Server**, используемым в **Антивирусной сети**. Если при первом подключении сервер недоступен, либо **Dr.Web Agent** не удалось авторизоваться, **Dr.Web Agent** завершает свою работу. Если ранее **Dr.Web Agent** уже работал с данным сервером, но в данный момент он недоступен (например, в случае проблем с соединением), **Dr.Web Agent** 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 **Dr.Web Agent** готов к работе.

Если **Dr.Web Agent** работает в режиме **Standalone**:

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

Взаимодействие с компонентами программного комплекса

Взаимодействие с компонентами программного комплекса осуществляется с помощью **amc**-файлов. В этих файлах описывается конфигурация компонентов и параметры, значения которых **Dr.Web Agent** 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 используемом **Dr.Web Enterprise Server**;
- **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).

Символ обратного слэша "\" используется для экранирования переводов строки.

Если компоненту нужны все настройки из конфигурационного файла, достаточно указать вместо перечня секций и/или параметров путь "/*".

Пример атмс-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 **Антивирусной сетью** под управлением **Dr. Web ESS**:

- первоначальная установка и настройка **Dr.Web для Novell Storage Services** в уже работающей **Антивирусной сети** под управлением **Dr.Web ESS**;
- встраивание работающего UNIX-сервера с установленным



и настроенным программным комплексом **Dr.Web для Novell Storage Services** в **Антивирусную сеть** под управлением **Dr.Web ESS**.

Для того, чтобы **Dr.Web для Novell Storage Services** мог работать в составе **Антивирусной сети** под управлением **Dr. Web ESS**, необходимо настроить компоненты **Dr.Web Agent** и **Dr.Web Monitor** для работы в режиме **Enterprise** и зарегистрировать комплекс на сервере централизованной защиты **Dr.Web Enterprise Server**.

В соответствии с политикой подключения новых станций (подробнее см. Руководство администратора Антивирусной сети **Dr.Web ESS**), подключить **Dr.Web для Novell Storage Services** к **Dr.Web Enterprise Server** 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 **Dr.Web Agent** и **Dr.Web Monitor**.

Для Dr.Web Agent

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

- **UseEnterpriseMode** = Yes;
- **PublicKeyFile** = `%var_dir/drwcsd.pub` (открытый ключ шифрования для доступа к **Dr.Web Enterprise Server**. Администратор должен самостоятельно взять данный файл из соответствующего каталога **Dr.Web Enterprise Server** и разместить его по указанному пути);
- **ServerHost** = IP-адрес или имя хоста **Dr.Web Enterprise Server**;



- **ServerPort** = порт **Dr.Web Enterprise Server** (2193 по умолчанию).

Для Dr.Web Monitor

В секции [Monitor] конфигурационного файла **Dr.Web Monitor**

%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 Dr.Web Agent** запрашивает регистрационные данные (идентификатор станции и пароль) у **Dr.Web Enterprise Server**;
- если на **Dr.Web Enterprise Server** установлен режим "**Ручное подтверждение доступа**" (режим по умолчанию, см. Руководство администратора Антивирусной сети **Dr.Web ESS**), то администратору в течение одной минуты с момента запроса необходимо подтвердить регистрацию новой станции через веб-интерфейс **Центра управления Dr.Web**;
- после первого подключения **Dr.Web Agent** записывает хэш идентификатора станции и пароля пользователя в файл с названием `pwd`. Данный файл создается в каталоге, заданном 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 **Dr.Web Enterprise Server**;
- удаление файла с паролем приведет к повторному запросу регистрационных данных у **Dr.Web Enterprise Server** при следующем запуске **Dr.Web Agent**.



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 Антивирусной сети **Dr.Web ESS**);
- Запустите **Dr.Web Agent** с параметром командной строки `--newpwd` (или `-p`) и введите идентификатор и пароль. Хэш идентификатора станции и пароля пользователя записывается в файл с названием `pwd`. Данный файл создается в каталоге, путь к которому 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 **Dr. Web Enterprise Server**;
- Удаление файла с паролем приведет к необходимости повторить процедуру регистрации при следующем запуске **Dr.Web Agent**.

Задание конфигурации компонентов через Центр Управления Dr.Web

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 ESS** 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 **Dr.Web Agent** запрашивает и получает



конфигурацию от сервера централизованной защиты **Dr.Web Enterprise Server**.

Экспорт существующей конфигурации на сервер

При помощи **Dr.Web Agent**, работающего в режиме **Enterprise**, возможно автоматически экспортировать конфигурацию компонентов на **Dr.Web Enterprise Server**. Для этого необходимо экспортировать конфигурацию параметром командной строки `--export-config` (или `-e`) с 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 **Dr.Web Monitor** установите флаги **Daemon** и **NSS** для запуска соответствующих компонентов комплекса;
- Запустите **Dr.Web Monitor** на локальной станции:

```
# /usr/local/etc/rc.d/00.drweb-monitor.sh  
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 Enterprise Server**, если **Dr. Web Agent** работает в режиме **Enterprise**.

Для соединения **Dr.Web Agent** с сервером статистики "**Доктор Веб**" необходим идентификатор пользователя – UUID. По умолчанию в качестве UUID используется md5-хэш от ключевого файла. Также вы можете получить персональный UUID, обратившись в службу поддержки. Такой UUID указывается в файле конфигурации **Dr.Web Agent** (параметр **UUID** в секции [StandaloneMode]).



Статистика собирается только для тех модулей **Dr.Web**, которые получают настройки от **Dr.Web Agent**. Информация о том, как настроить получение настроек от **Dr.Web Agent**, приведена в описании каждого модуля.

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 антивирусными продуктами **Dr. Web** для ОС **UNIX** либо программным комплексом **Dr.Web для Novell Storage Services** с подключенным антивирусным модулем.

В случае если работа ведется в режиме централизованной защиты, со статистикой можно ознакомиться также и на специальной странице **Центра управления Dr.Web**. Однако и в этом случае вся статистика, собранная сервером централизованной защиты **Dr.Web Enterprise Server**, также передается им на сервер статистики "**Доктор Веб**" в обобщенном виде для всей **Антивирусной сети**.

Результаты обработки содержат сведения о наиболее часто обнаруживаемых вирусах (для обобщенной статистики только в виде процента от общей суммы, а для индивидуальной – и в виде количества обнаруженных вирусов) 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 процентной форме. Внешний вид страницы может различаться в зависимости от используемого веб-браузера.

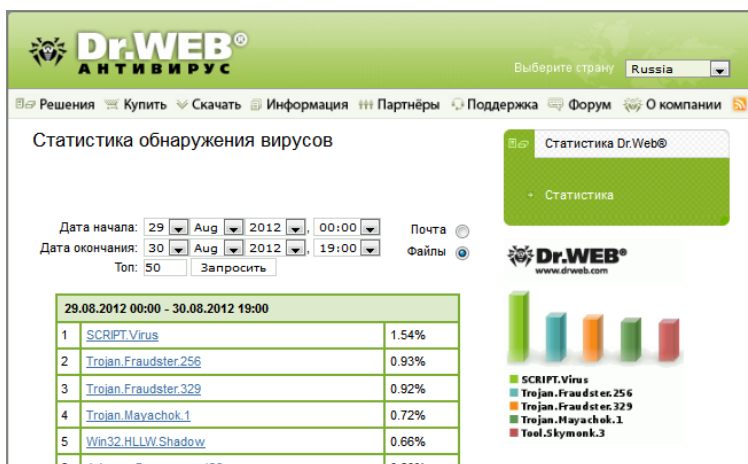


Рис. 15. Вирусная статистика

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**.

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>
    <dwvolid>62083</dwvolid>
    <place>1</place>
    <percents>34.201062139103</percents>
  </item>
  <item>
    <vname>Win32.HLLM.MyDoom</vname>
    <dwvolid>9353</dwvolid>
    <place>2</place>
    <percents>25.1303270912579</percents>
  </item>
  <item>
    <vname>Win32.HLLM.Beagle</vname>
    <dwvolid>26997</dwvolid>
    <place>3</place>
    <percents>13.4593034783378</percents>
  </item>
  <item>
    <vname>Trojan.Botnetlog.9</vname>
    <dwvolid>438003</dwvolid>
    <place>4</place>
    <percents>7.86446592583328</percents>
  </item>
  <item>
    <vname>Trojan.DownLoad.36339</vname>
    <dwvolid>435637</dwvolid>
    <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/<UUID>>, где `<UUID>` – это md5-хэш ключевого файла пользователя. Страница персональной статистики имеет формат, аналогичный формату страницы обобщенной статистики, за исключением того, что для персональной статистики указывается также количество обнаруженных вирусов, а не только процент от общего количества.

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



Ниже приводится сокращенный пример такого файла:

```
<drwebvirustop period="24" top="2"
user="<UUID>"
  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** 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, **Dr.Web Monitor** повторяет попытку. Количество попыток и время между ними определяются настройками компонента.

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

Dr.Web Monitor может взаимодействовать с компонентом **Dr. Web Agent**, обмениваясь с ним управляющими сигналами.

Режимы работы

При необходимости продукты компании "**Доктор Веб**" могут быть подключены к корпоративной или частной **Антивирусной сети**, управляемой комплексом **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, **Dr.Web Monitor** 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, **Dr.Web Monitor** полностью управляется с защищаемого компьютера, а все необходимые модули **Dr.Web** запускаются в соответствии с локальными настройками **Dr.Web Monitor**.

- Режим центральной защиты (**enterprise mode**), когда защитой компьютера управляет сервер центральной защиты **Dr.Web Enterprise Server**. 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, получаемый от сервера центральной защиты **Dr.Web Enterprise Server**. 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 **Dr.Web Monitor** (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, **Dr.Web Agent** также должен работать в режиме центральной защиты. Для подробностей обратитесь к разделу [Режимы работы Dr.Web Agent](#).

Чтобы использовать одиночный (standalone) режим

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

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 от сервера центральной защиты **Dr.Web Enterprise Server**, не могут быть использованы в этом режиме.



Параметры командной строки

Для запуска **Dr.Web Monitor** используется следующая команда:

```
drweb-monitor [параметры]
```

Dr.Web Monitor допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h	--help	
<u>Описание:</u> Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы модуля		
-v	--version	
<u>Описание:</u> Вывод на экран информации о текущей версии Dr.Web Monitor и завершение работы модуля		
-u	--update	
<u>Описание:</u> Запуск процесса обновления для всех компонентов Dr. Web для Novell Storage Services		
-C	--check-only	
<u>Описание:</u> Проверка корректности конфигурации модуля Dr.Web Monitor . Данный параметр командной строки не может быть использован при наличии в системе уже запущенного экземпляра Dr. Web Monitor		
-A	--check-all	<путь к файлу>
<u>Описание:</u> Проверка корректности конфигурации всех компонентов Dr.Web для Novell Storage Services		
-c	--conf	<путь к файлу>
<u>Описание:</u> Использование при запуске указанного конфигурационного файла		



Краткий вариант	Расширенный вариант	Аргументы
-r	--run	<имя приложения>[, <имя приложения>, ...]
<p><u>Описание:</u> Запуск указанных приложений. В качестве аргументов следует использовать имена приложений, указанных в заголовке секции Application "<имя приложения>" соответствующего mmc-файла (см. раздел Взаимодействие с компонентами программного комплекса). Данный параметр командной строки не может быть использован при наличии в системе уже запущенного экземпляра Dr. Web Monitor</p>		

Пример использования:

```
drweb-monitor -r AGENT, NSS
```

Конфигурационный файл

Настройки компонента **Dr.Web Monitor** задаются отдельным конфигурационным файлом %etc_dir/monitor.conf.

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

Секция [Logging]

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

Секция [Logging]

Level = { уровень подробности}	<u>Уровень_подробности</u> сохранения в журнал работы компонента общих событий.
---	---



	<p>Допускается использование следующих уровней:</p> <ul style="list-style-type: none">• Quiet• Error• Alert• Info• Debug <p><u>Значение по умолчанию:</u></p> <p>Level = Info</p>
<p>IPCLLevel = { уровень подробности}</p>	<p><u>Уровень_подробности</u> сохранения в журнал работы компонента событий подсистемы IPC.</p> <p>Допускается использование следующих уровней:</p> <ul style="list-style-type: none">• Quiet• Error• Alert• Info• Debug <p><u>Значение по умолчанию:</u></p> <p>IPCLLevel = Error</p>
<p>SyslogFacility = { метка syslog}</p>	<p><u>Метка_записи</u> при использовании системного сервиса syslog</p> <p><u>Значение по умолчанию:</u></p> <p>SyslogFacility = Daemon</p>
<p>FileName = { syslog путь к файлу}</p>	<p>Имя файла журнала или syslog, если нужно использовать системный сервис syslog</p> <p><u>Значение по умолчанию:</u></p> <p>FileName = syslog</p>



Секция [Monitor]

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

Секция [Monitor]

RunForeground = { логический }	<p>Значение Yes запрещает Dr.Web Monitor переходить в режим демона, т. е. становиться фоновым процессом без управляющего терминала.</p> <p>Эта возможность может быть использована некоторыми средствами мониторинга (например, daemontools).</p> <p><u>Значение по умолчанию:</u></p> <p>RunForeground = No</p>
User = { текст }	<p>Имя пользователя, с правами которого запускается Dr.Web Monitor.</p> <p><u>Значение по умолчанию:</u></p> <p>User = drweb</p>
Group = { текст }	<p>Имя пользовательской группы, с правами которой запускается Dr.Web Monitor.</p> <p><u>Значение по умолчанию:</u></p> <p>Group = drweb</p>
PidFileDir = { путь к каталогу }	<p>Имя каталога, содержащего файл, в который при запуске Dr.Web Monitor записывается информация об идентификаторе его процесса (PID).</p> <p><u>Значение по умолчанию:</u></p> <p>PidFileDir = %var_dir/run/</p>



ChDir =
{ путь к каталогу }

Смена активного каталога при запуске **Dr.Web Monitor**.

Если значение параметра задано, то при запуске **Dr.Web Monitor** делает активным каталог, указанный в значении этого параметра. Если значение параметра не задано, то смены активного каталога не происходит.

Значение по умолчанию:

ChDir = /

MetaConfigDir =
{ путь к каталогу }

Путь к каталогу с файлами мета-конфигурации.

В этих файлах задаются параметры работы **Dr.Web Monitor** с модулями программного комплекса. Содержание файлов мета-конфигурации задается разработчиками программного продукта и не требует редактирования.

Значение по умолчанию:

MetaConfigDir = %etc_dir/
monitor/

Address =
{ адрес }

Сокет, через который **Dr.Web Monitor** взаимодействует с другими модулями антивируса.

Значение по умолчанию:

Address = local:%var_dir/
ipc/.monitor

Timeout =
{ числовое значение }

Максимальное время установления соединения между **Dr.Web Monitor** и другими компонентами программного комплекса в секундах.

Значение по умолчанию:

Timeout = 5



TmpFileFmt = { текст }	<p>Шаблон имени временных файлов Dr. Web Monitor.</p> <p>Формат шаблона: путь_к_файлу. xxxxxx, где x - произвольный символ (буква или цифра) в именах создаваемых временных файлов.</p> <p><u>Значение по умолчанию:</u></p> <p>TmpFileFmt = %var_dir/msgs/ tmp/monitor.XXXXXX</p>
RunAppList = { текст }	<p>Список модулей, запускаемых Dr.Web Monitor.</p> <p>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 Dr.Web Monitor не сможет запуститься сам и запустить остальные компоненты.</p> <p><u>Значение по умолчанию:</u></p> <p>RunAppList = AGENT</p>
UseEnterpriseMode = { логический }	<p>При значении Yes данного параметра список модулей, запускаемых Dr.Web Monitor, берется не из параметра RunAppList, а от модуля Dr.Web Agent.</p> <p><u>Значение по умолчанию:</u></p> <p>UseEnterpriseMode = No</p>
RecoveryTimeList = { список числовых значений }	<p>Временные промежутки между попытками перезапуска "зависших" приложений в секундах.</p> <p>Для параметра можно задать несколько значений, перечислив их через запятую.</p>



	<p>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> <p>RecoveryTimeList = 0, 30, 60</p>
<p>InjectCmd = { текст }</p>	<p>Команда для отсылки отчетов.</p> <p>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> <p>InjectCmd = "/usr/sbin/sendmail -t"</p>
<p>AgentAddress = { адрес }</p>	<p>Сокет, через который Dr.Web Monitor взаимодействует с Dr.Web Agent (значение параметра должно совпадать со значением параметра Address конфигурационного файла Dr.Web Agent).</p> <p><u>Значение по умолчанию:</u></p> <p>AgentAddress = local:%var_dir/ipc/.agent</p>
<p>AgentResponseTime = { числовое значение }</p>	<p>Максимальное время отклика модуля Dr. Web Agent в секундах</p> <p>Если в течение этого времени от модуля не поступает ответа, то Dr.Web Monitor перезапускает его.</p> <p>Если указано значение 0, время отклика не ограничивается.</p> <p><u>Значение по умолчанию:</u></p> <p>AgentResponseTime = 5</p>



Запуск

В процессе запуска **Dr.Web Monitor** (при установках по умолчанию) осуществляются следующие действия:

- производится поиск и загрузка конфигурационного файла; если файл не найден, то загрузка прекращается;
- **Dr.Web Monitor** переходит в режим демона, поэтому сообщения о дальнейших проблемах не могут быть выведены на терминал и выводятся только в файл журнала;
- 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 тогда, когда содержащий его каталог доступен 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 **Dr.Web Monitor**. 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, **Dr.Web Monitor** пытается запустить его повторно. Если все попытки **Dr.Web Monitor** загрузить модуль окончились неудачей, **Dr.Web Monitor** выгружает все уже загруженные модули и завершает свою работу. Обо всех проблемах с запуском модулей программного комплекса **Dr.Web Monitor** сообщает одним из доступных ему способов (записью в файл журнала, сообщением электронной почты, запуском произвольной программы). Способы оповещения, используемые для разных модулей, задаются в файле мета-конфигурации **Dr.Web Monitor**.



Для успешного запуска **Dr.Web Monitor** в автоматическом режиме:

- либо в `enable`-файле **Dr.Web Monitor** переменной `ENABLE` должно быть присвоено значение 1.



В процессе работы установочного скрипта при выборе соответствующей возможности в диалоге все сервисы, включая **Dr.Web Monitor**, будут запущены автоматически.

Расположение `enable`-файлов зависит от способа установки **Dr.Web для Novell Storage Services**:

- Установка при помощи универсального пакета для UNIX:

Файлы располагаются в каталоге `%etc_dir` и называются
`drwebd.enable`,
`drweb-monitor.enable`.

- Установка из нативных DEB-пакетов:

Файлы располагаются в каталоге `/etc/defaults` и называются
`drwebd`,
`drweb-monitor`.

- Установка из нативных RPM-пакетов:

Файлы располагаются в каталоге `/etc/sysconfig` и называются
`drwebd.enable`,
`drweb-monitor.enable`.

Взаимодействие с компонентами программного комплекса

Взаимодействие с компонентами программного комплекса осуществляется с помощью `mmcs`-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. Консольный сканер представлен исполняемым модулем **drweb**.

Dr.Web Scanner проверяет указанные при запуске файлы и загрузочные записи указанных дисков. Для антивирусной проверки и лечения **Dr.Web Scanner** использует Антивирусное ядро **Dr.Web Engine** и вирусные базы, но не использует резидентный модуль **Dr.Web Daemon** (работа производится независимо от него).

Запуск

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

```
$ %bin_dir/drweb
```

В том случае, если каталог `%bin_dir` внесен в переменную окружения командной оболочки `PATH`, запуск осуществляется из произвольного каталога. Следует учесть, что последний вариант не рекомендуется из соображений безопасности, равно как и создание символической ссылки на исполняемый файл **drweb** в каком-либо из каталогов типа `/bin/`, `/usr/bin/` и т.д.

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



После запуска **Dr.Web Scanner** 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: XXXXXXXXXX
Дата активации лицензионного ключа: XXXX-XX-XX
Дата истечения действия лицензионного ключа: XXXX-
XX-XX
```

После этого возвращается приглашение командной оболочки.

При запуске **Dr.Web Scanner** 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;
- **spr** – переименование подозрительных файлов.
- **spm** – перемещение подозрительных файлов;

Запуск **Dr.Web Scanner** с параметром лечения **cu** 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 отдельный каталог, который и будет указан как аргумент при повторном запуске **Dr.Web Scanner**.

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

Параметр переименования **spr** 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 (например, DOS/Windows), выявленных при эвристическом анализе как подозрительные. Переименование делает невозможным случайный запуск исполняемых модулей в этих



системах, загрузку документов **Word** или **Excel** без дальнейшей проверки и таким образом предотвратит заражение возможным вирусом и дальнейшее его распространение.

Параметр перемещения **spm** переместит зараженный (или подозрительный) файл в предназначенный для этого каталог **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 **Dr.Web Scanner** 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.

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>` (файлы устройств размещаются в каталоге `/dev`), то будет проверен загрузочный сектор соответствующего устройства и при необходимости произведено его лечение. Путь может быть предварен необязательным ключом `path`.



Запущенный без параметров, только с указанием пути в качестве аргумента, консольный сканер **Dr.Web Scanner** осуществляет проверку указанного каталога, используя набор параметров по умолчанию (см. ниже). В следующем примере проверяется домашний каталог пользователя:

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

По окончании проверки, в случае обнаружения зараженных или подозрительных файлов, **Dr.Web Scanner** 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, **Dr.Web Scanner** 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 `eicar.com` (см. указания внутри самого файла), которая ведет себя подобно вирусу, вызывая сообщение вида:

```
%bin_dir/doc/eicar.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.

Dr.Web Scanner может быть настроен с помощью многочисленных параметров командной строки. Полный список параметров командной строки для консольного сканера **Dr.Web Scanner** можно получить, запустив программу **drweb** с параметрами `-?`, `-h` или `--help`.

Основные параметры консольного сканера **Dr.Web Scanner** можно сгруппировать следующим образом:

- [Параметры области проверки;](#)
- [Параметры диагностики;](#)
- [Параметры действий;](#)
- [Параметры интерфейса.](#)

Параметры области проверки

Эти параметры указывают, где следует проводить проверку на вирусы:

Параметр	Описание
<code>-path [=] { путь }</code>	<p>Задаёт пути для сканирования.</p> <p>В одном параметре может быть задано несколько путей. Символ '=' можно опустить, в этом случае путь для сканирования отделяется от ключа пробелом. Можно несколько раз указать ключ <code>path</code> с разными путями, в этом случае они будут объединены в один список. Кроме того, пути можно задавать, не используя ключ <code>path</code>.</p> <p>Если в параметрах запуска путь задан с префиксом:</p> <pre>disk //<путь к файлу устройства>,</pre> <p>то будет проверен загрузочный сектор (MBR) соответствующего устройства и при необходимости произведено его лечение.</p> <p>Файл устройства – это специальный файл, расположенный в каталоге файлов устройств <code>/dev</code> и имеющий имя вида <code>sdx</code></p>



Параметр	Описание
	или <code>hdx</code> , где <code>x</code> – латинская буква (<code>a</code> , <code>b</code> , <code>c</code> , ...). Например: <code>hda</code> , <code>sda</code> . Таким образом, чтобы проверить, например, загрузочную запись диска <code>sda</code> , следует указать путь: <code>disk: ///dev/sda</code>
<code>-@[+] { файл }</code>	Задаёт проверку 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 каталогам или просто список файлов, подлежащих регулярной проверке.
<code>--</code>	Указывает, что список объектов для сканирования следует считать из стандартного потока ввода <code>stdin</code> .
<code>-sd</code>	Задаёт рекурсивный поиск и проверку файлов во вложенных папках.
<code>-fl</code>	Указывает следовать символическим ссылкам как для файлов, так и для папок. Ссылки, приводящие к «зацикливанию», игнорируются.
<code>-mask</code>	Игнорировать маски имен файлов.

Параметры диагностики

Эти параметры определяют, какие типы объектов и каким образом должны проверяться на вирусы:

Параметр	Описание
<code>-al</code>	Указывает, что по заданным путям необходимо проверять все файлы вне зависимости от их расширения и внутреннего формата. Этот параметр противоположен по действию параметру <code>-ex</code> .
<code>-ex</code>	Указывает, что по заданным путям необходимо проверять только файлы заданного типа



Параметр	Описание
	<p>(разрешения). Разрешения указываются в конфигурационном файле (задается параметром -ini) в переменной FileTypes.</p> <p>По умолчанию осуществляется проверка файлов со следующими расширениями:</p> <p>EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, MPP, OCX, VS*, DVB, CPY, BMP, RPM, ISO, DEB, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, LHA, LZH, BZ2, MSG, EML, 7Z, CPIO.</p> <p>Этот параметр противоположен по действию параметру -al.</p>
-ar [d m r] [n]	<p>Задаёт проверку файлов в архивах (ARJ, CAB, GZIP, RAR, TAR, ZIP и др.). Под архивами в данном случае понимаются не только собственно архивы (например, вида *.tar), но и их сжатые формы (например, сжатые TAR-архивы вида *.tar.bz2 и *.tbz).</p> <p>Если параметр указан без дополнительных модификаторов d, m или r, то в случае обнаружения архива с вредоносными или подозрительными файлами, производится только информирование пользователя.</p> <p>Если параметр дополняется модификатором d, m или r, то применяются соответствующие действия для устранения обнаруженной угрозы.</p>
-cn [d m r] [n]	<p>Задаёт проверку файлов в контейнерах (HTML, RTF, PowerPoint).</p> <p>Если параметр указан без дополнительных модификаторов d, m или r, то в случае обнаружения контейнера с вредоносными или подозрительными объектами, производится только информирование пользователя.</p> <p>Если параметр дополняется модификатором d, m</p>



Параметр	Описание
	или <i>r</i> , то применяются соответствующие действия для устранения обнаруженной угрозы.
-ml [<i>d</i> <i>m</i> <i>r</i>] [<i>n</i>]	Задаёт проверку файлов почтовых программ. Если параметр указан без дополнительных модификаторов <i>d</i> , <i>m</i> или <i>r</i> , то в случае обнаружения файла с вредоносными или подозрительными элементами, производится только информирование пользователя. Если параметр дополняется модификатором <i>d</i> , <i>m</i> или <i>r</i> , то применяются соответствующие действия для устранения обнаруженной угрозы.
-upn	Проверка исполняемых файлов, упакованных LZEXE, DIET, PKCITE, EXEPACK без вывода имен утилит упаковки (в противном случае имя утилиты-упаковщика будет выводиться на экран).
-ha	Задаёт использование эвристического анализа для поиска неизвестных угроз.

Для некоторых параметров доступны также следующие дополнительные модификаторы:

- *d* – использовать удаление объекта для устранения угрозы;
- *m* – использовать перемещение объекта в **Карантин** для устранения угрозы;
- *r* – использовать переименование объекта для устранения угрозы (первый символ расширения заменяется на символ «#»);
- *n* – не указывать в отчете типы архиваторов, контейнеров, почтовых файлов или упаковщиков.

При обнаружении вредоносных элементов в составных объектах (архивах, контейнерах, упакованных или почтовых файлах), указанное действие применяется ко всему составному объекту целиком, а не только к вредоносному элементу.



Параметры действия

Эти параметры определяют, какие действия должны быть выполнены в отношении зараженных (или подозрительных) объектов:

Параметр	Описание
-cu [d m r]	Задаёт действие для инфицированных файлов и загрузочных секторов дисков. Если параметр указан без дополнительных модификаторов, то производится лечение излечимых объектов и удаление неизлечимых файлов (если другое не задано параметром -ic). Дополнительные модификаторы позволяют задать иное действие взамен лечения, но оно применяется только для инфицированных файлов. Действие для неизлечимых файлов в таком случае должно быть задано параметром -ic .
-ic [d m r]	Задаёт действие для неизлечимых файлов. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-sp [d m r]	Задаёт действие для подозрительных файлов. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-adw [d m r i]	Задаёт действие для файлов, содержащих рекламные программы. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-dls [d m r i]	Задаёт действие для файлов, содержащих программы дозвона. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-jok [d m r i]	Задаёт действие для файлов, содержащих программы-шутки. Если параметр указан без дополнительных



Параметр	Описание
	модификаторов, то производится только информировании об угрозе.
-rsk [d m r i]	Задаёт действие для файлов, содержащих потенциально опасные программы. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.
-hck [d m r i]	Задаёт действие для файлов, содержащих программы, используемые для взлома. Если параметр указан без дополнительных модификаторов, то производится только информировании об угрозе.

Дополнительные модификаторы задают действие, необходимое для устранения угрозы:

- d – удаление файла;
- m – перемещение файла в **Карантин**;
- r – переименование файла (первый символ расширения заменяется на символ «#»);
- i – игнорирование (доступно только для незначительных угроз, например, рекламных программ); при использовании этого модификатора объект пропускается без каких-либо действий и оповещение сообщение об угрозе не выводится.

При обнаружении вредоносных элементов в составных объектах (архивах, контейнерах, упакованных или почтовых файлах), указанное действие применяется ко всему составному объекту целиком, а не только к вредоносному элементу.

Параметры интерфейса

Эти параметры определяют условия вывода результатов работы консольного сканера **Dr.Web Scanner**:

Параметр	Описание
-v , -version , --version	Задаёт вывод информации о версии продукта и версии антивирусного ядра и завершение работы консольного сканера Dr.Web Scanner .



Параметр	Описание
<code>-ki</code>	Задаёт вывод информации о лицензии и ее владельце (только в кодировке UTF8).
<code>-go</code>	Задаёт пакетный режим работы консольного сканера Dr.Web Scanner . Все вопросы, подразумевающие ожидание ответа от пользователя, пропускаются; решения, требующие выбора, принимаются автоматически. Этот режим полезно использовать для автоматической проверки файлов, например, при ежедневной или еженедельной проверке жесткого диска.
<code>-ot</code>	Переключает вывод информации на стандартный вывод (<code>stdout</code>).
<code>-oq</code>	Отключает вывод информации на экран.
<code>-ok</code>	Задаёт вывод полного списка сканируемых объектов, сопровождая безопасные объекты пометкой Ok .
<code>-log [=+]</code> { путь к файлу }	Включает протоколирование работы консольного сканера Dr.Web Scanner в указанном файле. При отсутствии имени файла отчет записываться не будет. Символ «+» (плюс) предписывает не перезаписывать файл отчета, а добавлять новую информацию.
<code>-ini</code> = { путь к файлу }	Задаёт использование указанного конфигурационного файла. По умолчанию конфигурационный файл не входит в состав консольного сканера Dr.Web Scanner .
<code>-lng</code> = { путь к файлу }	Задаёт использование указанного альтернативного языкового файла. По умолчанию используется английский язык.



Параметр	Описание
<code>-a = {адрес Агента}</code>	Запустить консольный сканер Dr. Web Scanner в режиме централизованной защиты под управлением выбранного Dr.Web Agent .
<code>-ni</code>	Отключает использование конфигурационного файла для настройки консольного сканера Dr. Web Scanner . Настройка сканирования в данном случае будет осуществляться только с использованием параметров из командной строки.
<code>-ns</code>	Запрещает возможность прерывания проверки, в том числе при получении сигнала остановки процесса (SIGINT).
<code>--only-key</code>	При запуске от Dr.Web Agent будет получен только ключевой файл.

Некоторые из параметров отменяют соответствующее им действие, если оканчиваются символом минуса (без пробела). К ним относятся следующие параметры:

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

Например, при запуске консольного сканера **Dr.Web Scanner** командой вида:

```
$ drweb <путь> -ha-
```

проверка будет производиться без использования **Эвристического анализатора**, который обычно по умолчанию включен.

Для параметров `-cu`, `-ic` и `-sp` «отрицательная» форма отменяет выполнение любых действий, указанных в их описании. Это означает, что информация о зараженных и подозрительных объектах будет фиксироваться в отчете, но никаких действий по устранению представляемых ими угроз предприниматься не будет.



Для параметров **-al** и **-ex** «отрицательная» форма не предусмотрена, однако задание одного из них отменяет действие другого.

Если не производились действия по перенастройке программы, то по умолчанию (то есть без отдельного указания параметров) **Dr.Web Scanner** запускается с параметрами:

-ar -ha -fl- -ml -sd -al -ok

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 минус, как это было показано выше на примере параметра **-ha** (использование **Эвристического анализатора**).

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 **Dr.Web Scanner** 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.



Настройки

Можно использовать **Dr.Web Scanner** с настройками по умолчанию, но значительно удобнее настроить его для соответствия конкретным требованиям и условиям эксплуатации. Настройки **Dr.Web Scanner** хранятся в конфигурационном файле программы (по умолчанию `drweb32.ini`), который размещается в каталоге `%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске **Dr.Web Scanner**, например:

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

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

Секция [Scanner]

EnginePath = { путь к файлу }	<p>Расположение модуля drweb32.dll (Антивирусное ядро Dr.Web Engine).</p> <p>Этот параметр также используется модулем обновления Dr.Web Updater.</p> <p><u>Значение по умолчанию:</u></p> <pre>EnginePath = %bin_dir/lib/ drweb32.dll</pre>
VirusBase = { список масок файлов }	<p>Маски для подключаемых вирусных баз.</p> <p>Этот параметр также используется модулем обновления Dr.Web Updater. Допустимо перечисление нескольких масок через запятую.</p> <p>По умолчанию вирусные базы хранятся в файлах с расширением <code>.vdb</code></p> <p><u>Значение по умолчанию:</u></p> <pre>VirusBase = %var_dir/bases/*. vdb</pre>



UpdatePath = { путь к каталогу }	<p>Этот параметр используется модулем обновления Dr.Web Updater и должен быть задан обязательно.</p> <p><u>Значение по умолчанию:</u></p> <p>UpdatePath = %var_dir/ updates/</p>
TempPath = { путь к каталогу }	<p>Этот каталог используется Антивирусным ядром Dr.Web Engine для создания временных файлов.</p> <p>При нормальной работе каталог практически не используется, он нужен для распаковки некоторых видов архивов, или когда в системе не хватает памяти.</p> <p><u>Значение по умолчанию:</u></p> <p>TempPath = /tmp/</p>
LngFileName = { путь к файлу }	<p>Расположение файла языковых ресурсов. По умолчанию файлы языковых ресурсов имеют расширение .dwl</p> <p><u>Значение по умолчанию:</u></p> <p>LngFileName = %bin_dir/lib/ ru_scanner.dwl</p>
Key = { путь к ключевому файлу }	<p>Расположение ключевого файла (лицензионного или демонстрационного). По умолчанию ключевой файл имеет расширение .key</p> <p><u>Значение по умолчанию:</u></p> <p>Key = %bin_dir/drweb32.key</p>
OutputMode = { Terminal Quiet }	<p>Режим вывода информации при запуске:</p> <ul style="list-style-type: none">• Terminal – вывод на консоль,• Quiet – отменяет вывод.



	<p><u>Значение по умолчанию:</u></p> <p>OutputMode = Terminal</p>
<p>HeuristicAnalysis = { логический}</p>	<p>Включение/отключение использования Эвристического анализатора.</p> <p>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".</p> <p>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 использования Эвристического анализатора. Вместе с тем, включение этого типа анализа увеличивает надежность антивирусной защиты.</p> <p>Все файлы, обнаруженные Эвристическим анализатором, лучше всего отправить разработчикам через сайт http://vms.drweb.com/sendvirus/.</p> <p>Отправку подозрительных файлов рекомендуется производить следующим образом: запаковать файл в архив с паролем, пароль сообщить в теле письма, при этом желательно приложить отчет Dr.Web Scanner.</p>



	<p><u>Значение по умолчанию:</u></p> <p>HeuristicAnalysis = Yes</p>
<p>ScanPriority = { числовое значение }</p>	<p>Приоритет работы Dr.Web Scanner.</p> <p>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> <p>ScanPriority = 0</p>
<p>FileTypes = { список расширений файлов }</p>	<p>Список типов файлов, которые будут проверяться при сканировании по типу, т.е. когда параметр ScanFiles (см. ниже) имеет значение ByType.</p> <p>Допускаются СИМВОЛЫ МАСКИ '*' и '?'.</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>
<p>FileTypesWarnings = { логический }</p>	<p>Выводить ли предупреждение о файлах неизвестных типов.</p> <p><u>Значение по умолчанию:</u></p> <p>FileTypesWarnings = Yes</p>
<p>ScanFiles = { All ByType }</p>	<p>Дополнительное ограничение на файлы, подлежащие проверке.</p> <p>При задании значения ByType</p>



	<p>учитываются расширения файлов, значения которых заданы или по умолчанию, или в параметре (параметрах) FilesTypes. В противном случае проверяются все файлы.</p> <p>Внутри почтовых файлов всегда действует режим All. Значение buType может быть использовано только в режиме локального сканирования.</p> <p><u>Значение по умолчанию:</u></p> <p>ScanFiles = All</p>
ScanSubDirectories = { логический }	<p>Проверка содержимого вложенных подкаталогов.</p> <p><u>Значение по умолчанию:</u></p> <p>ScanSubDirectories = Yes</p>
CheckArchives = { логический }	<p>Проверка файлов, содержащихся в архивах.</p> <p>Поддерживаются архивы форматов ZIP (WinZip, InfoZIP и др.), RAR, ARJ, TAR, GZIP, CAB и др.</p> <p><u>Значение по умолчанию:</u></p> <p>CheckArchives = Yes</p>
CheckEmailFiles = { логический }	<p>Проверка файлов в почтовых (e-mail) форматах.</p> <p><u>Значение по умолчанию:</u></p> <p>CheckEmailFiles = Yes</p>
ExcludePaths = { список путей (масок) }	<p>Маски для тех файлов, которые не должны проверяться.</p> <p><u>Значение по умолчанию:</u></p> <p>ExcludePaths = /proc,/sys,/dev</p>



FollowLinks = { логический}	<p>Следование символическим ссылкам при сканировании.</p> <p><u>Значение по умолчанию:</u></p> <p>FollowLinks = No</p>
RenameFilesTo = { маска}	<p>Маска для переименования файлов, если сработало действие Rename.</p> <p><u>Значение по умолчанию:</u></p> <p>RenameFilesTo = #??</p>
MoveFilesTo = { путь к каталогу}	<p>Путь к каталогу Карантина.</p> <p><u>Значение по умолчанию:</u></p> <p>MoveFilesTo = %var_dir/ infected/</p>
EnableDeleteArchiveAction = { логический}	<p>Разрешение применения действия Delete для составных объектов (архивов, почтовых ящиков, HTML-страниц), если они содержат зараженные объекты.</p> <p>Важно понимать, что при наличии данного разрешения будет удален весь составной объект, т.е. весь архив или все письмо, а не только зараженное вложение в письмо или элемент архива.</p> <p><u>Значение по умолчанию:</u></p> <p>EnableDeleteArchiveAction = No</p>
InfectedFiles = { действие}	<p>Задаёт реакцию на обнаружение файла, зараженного известным вирусом.</p> <p><u>Допустимые значения</u> параметра:</p> <p>Report, Cure, Delete, Move, Rename, Ignore.</p> <p>Удаление и перемещение, заданное в связи с обнаружением зараженных объектов в архивах, контейнерах и</p>



	почтовых ящиках, применяется к соответствующему архиву, контейнеру или почтовому ящику целиком.
	<u>Значение по умолчанию:</u> InfectedFiles = Report

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 = { действие}	Действие, которое нужно выполнить в случае, если файл заражен неизвестным вирусом или представляет собой потенциальную угрозу. <u>Допустимые значения</u> параметра: Report, Delete, Move, Rename, Ignore. <u>Значение по умолчанию:</u> SuspiciousFiles = Report
---	--

IncurableFiles = { действие}	Действие, которое нужно выполнить в случае, если зараженный файл не может быть вылечен (параметр имеет смысл, только если InfectedFiles = Cure) <u>Допустимые значения</u> параметра: Report, Delete, Move, Rename, Ignore. <u>Значение по умолчанию:</u> IncurableFiles = Report
--	---

ActionAdware = { действие}	Действие, которое нужно выполнить в случае, если файл содержит программу для показа рекламы (adware). <u>Допустимые значения</u> параметра: Report, Delete, Move, Rename, Ignore.
--------------------------------------	---



	<p><u>Значение по умолчанию:</u></p> <p>ActionAdware = Report</p>
<p>ActionDialers = { действие}</p>	<p>Действие, которое нужно выполнить в случае, если файл содержит программу автоматического дозвона.</p> <p><u>Допустимые значения</u> параметра:</p> <p>Report, Delete, Move, Rename, Ignore.</p> <p><u>Значение по умолчанию:</u></p> <p>ActionDialers = Report</p>
<p>ActionJokes = { действие}</p>	<p>Действие, которое нужно выполнить в случае, если файл содержит программу-шутку, которая может пугать или раздражать пользователя.</p> <p><u>Допустимые значения</u> параметра:</p> <p>Report, Delete, Move, Rename, Ignore.</p> <p><u>Значение по умолчанию:</u></p> <p>ActionJokes = Report</p>
<p>ActionRiskware = { действие}</p>	<p>Действие, которое нужно выполнить в случае, если файл содержит потенциально опасную программу, которая может быть использована не только ее владельцем, но и злоумышленниками.</p> <p><u>Допустимые значения</u> параметра:</p> <p>Report, Delete, Move, Rename, Ignore.</p> <p><u>Значение по умолчанию:</u></p> <p>ActionRiskware = Report</p>
<p>ActionHacktools = { действие}</p>	<p>Действие, которое нужно выполнить в случае, если файл содержит программу, которая используется для взлома</p>



	<p>компьютеров.</p> <p><u>Допустимые значения</u> параметра:</p> <p>Report, Delete, Move, Rename, Ignore.</p> <p><u>Значение по умолчанию:</u></p> <p>ActionHacktools = Report</p>
ActionInfectedMail = { действие }	<p>Действие, которое нужно выполнить в случае, если почтовое сообщение или почтовый ящик содержат зараженный объект.</p> <p><u>Допустимые значения</u> параметра:</p> <p>Report, Delete, Move, Rename, Ignore.</p> <p><u>Значение по умолчанию:</u></p> <p>ActionInfectedMail = Report</p>
ActionInfectedArchive = { действие }	<p>Действие, которое нужно выполнить в случае, если архив (ZIP, TAR, RAR и др.) содержит зараженный файл.</p> <p><u>Допустимые значения</u> параметра:</p> <p>Report, Delete, Move, Rename, Ignore.</p> <p><u>Значение по умолчанию:</u></p> <p>ActionInfectedArchive = Report</p>
ActionInfectedContainer = { действие }	<p>Действие, которое нужно выполнить в случае, если файл контейнер (OLE, HTML, PowerPoint и др.) содержит зараженный объект.</p> <p><u>Допустимые значения</u> параметра:</p> <p>Report, Delete, Move, Rename, Ignore.</p>



	<u>Значение по умолчанию:</u> ActionInfectedContainer = Report
--	--

Параметры регистрации событий:

LogFileName = { syslog путь к файлу }	Имя файла журнала или syslog, если нужно использовать системный сервис syslog . <u>Значение по умолчанию:</u> LogFileName = syslog
---	--

SyslogFacility = { метка syslog }	<u>Метка записи</u> при использовании системного сервиса syslog . <u>Значение по умолчанию:</u> SyslogFacility = Daemon
---	---

SyslogPriority = { уровень подробности }	<u>Уровень подробности</u> ведения журнала при использовании системного сервиса syslog . Допускается использование следующих уровней: <ul style="list-style-type: none">• Error• Alert• Warning• Info• Notice <u>Значение по умолчанию:</u> SyslogPriority = Info
--	---

LimitLog = { логический }	Ограничение размера файла журнала, если не используется syslog . Ограничение размера файла отчета реализуется следующим образом: при запуске Dr.Web Scanner проверяет размер файла журнала, и если он превышает значение, заданное в
-------------------------------------	---



	<p>параметре MaxLogSize, файл журнала стирается и ведение журнала начинается с нуля.</p> <p><u>Значение по умолчанию:</u></p> <p>LimitLog = No</p>
<p>MaxLogSize = { числовое значение }</p>	<p>Максимальный размер файла журнала в килобайтах, если не используется syslog и LimitLog = Yes.</p> <p>Если указано значение 0, размер файла журнала проверяться не будет.</p> <p><u>Значение по умолчанию:</u></p> <p>MaxLogSize = 512</p>
<p>LogScanned = { логический }</p>	<p>Вывод в журнал информации обо всех проверяемых объектах, независимо от того, обнаружены вирусы или нет.</p> <p><u>Значение по умолчанию:</u></p> <p>LogScanned = Yes</p>
<p>LogPacked = { логический }</p>	<p>Вывод в журнал дополнительной информации о файлах, упакованных утилитами DIET, PKLITE и др.</p> <p><u>Значение по умолчанию:</u></p> <p>LogPacked = Yes</p>
<p>LogArchived = { логический }</p>	<p>Вывод в журнал дополнительной информации об архиваторах.</p> <p><u>Значение по умолчанию:</u></p> <p>LogArchived = Yes</p>
<p>LogTime = { логический }</p>	<p>Вывод в журнал времени каждой записи.</p> <p>Параметр игнорируется, если используется syslog</p> <p><u>Значение по умолчанию:</u></p> <p>LogTime = Yes</p>



LogStatistics = { логический}	Запись в журнал суммарной статистики задания для сканирования.
	<u>Значение по умолчанию:</u> LogStatistics = Yes
RecodeNonprintable = { логический}	Перекодировка при выводе в журнал 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.
	<u>Значение по умолчанию:</u> RecodeChar = "?"

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

MaxCompressionRatio = { числовое значение}	Максимальный коэффициент сжатия, т. е. отношение длины файла в распакованном виде к длине файла в
--	---



	<p>запакованном виде (внутри архива).</p> <p>Если коэффициент превышает данное значение, файл не будет извлечен и, соответственно, не будет проверен. Письмо с таким файлом воспринимается программой как "почтовая бомба".</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 = { числовое значение}	<p>Минимальный размер файла внутри архива (в килобайтах), начиная с которого будет производиться проверка коэффициента сжатия (если это предписано параметром MaxCompressionRatio).</p> <p><u>Значение по умолчанию:</u></p> <p>CompressionCheckThreshold = 1024</p>
MaxFileSizeToExtract = { числовое значение}	<p>Максимальный размер файла, извлекаемого из архива, в килобайтах.</p> <p>Если размер файла внутри архива превышает это значение, он будет пропущен. Письмо с таким файлом воспринимается программой как "почтовая бомба".</p> <p><u>Значение по умолчанию:</u></p> <p>MaxFileSizeToExtract = 500000</p>
MaxArchiveLevel = { числовое значение}	<p>Максимальный уровень вложенности архивов (когда архив вложен в архив, который тоже вложен в архив и т.д.).</p> <p>При превышении этого уровня архив будет пропущен (не будет проверен). Письмо с таким файлом воспринимается</p>



	<p>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 = { числовое значение}</p>	<p>Максимальный размер памяти в мегабайтах, выделяемой Dr.Web Scanner при сканировании одного файла.</p> <p>Если установлено значение 0, размер выделяемой памяти не ограничен.</p> <p><u>Значение по умолчанию:</u></p> <p>MaximumMemoryAllocationSize = 0</p>
<p>ScannerScanTimeout = { числовое значение}</p>	<p>Максимальное время сканирования одного файла (в секундах).</p> <p>Если установлено значение 0, время сканирования одного файла не ограничено.</p> <p><u>Значение по умолчанию:</u></p> <p>ScannerScanTimeout = 0</p>
<p>MaxBasesObsolescencePeriod = { числовое значение}</p>	<p>Максимальный период времени (в часах) с момента последнего обновления, в течение которого вирусные базы считаются "свежими".</p> <p>По истечении этого времени в консоли выводится уведомление о том, что базы устарели. Если установлено значение 0, "свежесть" вирусных баз не проверяется.</p> <p><u>Значение по умолчанию:</u></p> <p>MaxBasesObsolescencePeriod = 24</p>



ControlAgent =
{ адрес}

Адрес сокета **Dr.Web Agent**.

Пример:

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

Dr.Web Scanner получает от **Dr.Web Agent** ключ и конфигурационный файл (если в качестве значения параметра **OnlyKey** задано No).

Значение по умолчанию:

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

OnlyKey =
{ логический}

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

Если указан адрес сокета **Dr.Web Agent** и значение параметра **OnlyKey** установлено в No, **Dr.Web Agent** будет отправляться статистика работы **Dr. Web Scanner** (после сканирования каждого файла **Dr.Web Scanner** будет отправлять информацию **Dr.Web Agent**).

Значение по умолчанию:

```
OnlyKey = No
```



Антивирусный модуль Dr.Web Daemon

Dr.Web Daemon – основной компонент безопасности. Он представляет собой постоянно загруженный (резидентный) антивирусный модуль **drwebd**, который позволяет по запросу от других компонентов комплекса проверять файлы на диске или данные, переданные ему через сокет. Запросы на антивирусную проверку осуществляются по специальному протоколу через UNIX- или TCP-сокеты. **Dr.Web Daemon** использует то же Антивирусное ядро **Dr.Web Engine** и вирусные базы, что и **Dr.Web Scanner**, и способен обнаруживать и лечить все вирусы, известные Антивирусному ядру **Dr. Engine**.

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

Для запуска **Dr.Web Daemon** используется следующая команда:

```
drwebd [ параметры ]
```

Dr.Web Daemon допускает использование следующих параметров:

Краткий вариант	Расширенный вариант	Аргументы
-h, -?	-help, --help	
<u>Описание:</u> Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы модуля		



Краткий вариант	Расширенный вариант	Аргументы
-a		<адрес Агента>
<u>Описание:</u> Запуск Dr.Web Daemon в режиме центральной защиты под управлением указанного Dr.Web Agent		
-ini		<путь к файлу>
<u>Описание:</u> Использование указанного конфигурационного файла		
	--foreground	<yes no>
<u>Описание:</u> Задание режима работы Dr.Web Daemon при запуске. Если выбрано значение <i>yes</i> , то Dr.Web Daemon будет работать как приоритетная задача. При значении <i>no</i> Dr.Web Daemon будет работать в фоновом режиме		
	--check-only	<параметры командной строки для проверки>
<u>Описание:</u> Проверка правильности конфигурации Dr.Web Daemon при запуске. Если указаны какие-либо параметры командной строки, то правильность задаваемых с их помощью значений также будет проверена		
	--only-key	
<u>Описание:</u> При запуске Dr.Web Daemon получит от Dr.Web Agent только лицензионный ключевой файл		

Запуск

В процессе загрузки **Dr.Web Daemon** выполняются следующие действия:

1. Поиск и загрузка конфигурационного файла. Если конфигурационный файл не найден, загрузка **Dr.Web Daemon** прекращается. Путь к конфигурационному файлу может быть задан при запуске параметром командной строки `-ini: {путь/к/drweb32.ini}`, иначе будет



использовано значение `%etc_dir/drweb32.ini`, заданное по умолчанию. При загрузке проверяется допустимость некоторых параметров и, если значение параметра недопустимо, берется значение по умолчанию;

2. Создается файл отчета. Каталог с файлом отчета должен быть доступен на запись пользователю, с правами которого работает **Dr.Web Daemon**. Каталог `/var/log/`, используемый по умолчанию, недоступен пользователям на запись. Поэтому, если задано значение параметра **User**, необходимо также указать путь к альтернативному каталогу для хранения отчетов в значении параметра **LogFile**`Name`;
3. Производится загрузка ключевого файла по пути, указанному в конфигурационном файле. Если ключевой файл не найден, загрузка **Dr.Web Daemon** прекращается;
4. Если задан параметр **User**, **Dr.Web Daemon** пытается изменить свои права;
5. Производится загрузка антивирусного ядра **Dr.Web Engine** (файл `drweb32.dll`). Если Антивирусное ядро не найдено (ошибки в конфигурационном файле) или повреждено, загрузка **Dr.Web Daemon** прекращается;
6. 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 **Dr.Web Daemon** продолжается;
7. **Dr.Web Daemon** отключается от терминала, поэтому сообщения о дальнейших проблемах не могут быть выведены на терминал и выводятся только в файл отчета;
8. Создается сокет, в случае использования TCP-сокетов, возможно, не один. Если какой-либо TCP-сокет создать не удалось, загрузка **Dr.Web Daemon** продолжается. В случае использования UNIX-сокета следует убедиться, что каталог, содержащий его, доступен на запись и чтение пользователю, с чьими правами работает **Dr.Web Daemon**. Для пользователей, с правами которых будут работать интеграционные модули, каталог должен быть доступен на выполнение, а сам файл сокета — на запись и чтение. Каталог по умолчанию (`/var/run/`) недоступен



пользователям на запись и выполнение. Поэтому, если задано значение параметра **User**, необходимо также указать путь к альтернативному каталогу для сокетов в значении параметра **Socket**. Если UNIX-сокет создать не удалось, загрузка **Dr.Web Daemon** прекращается;

9. После этого создается PID-файл, в котором хранится информация об идентификаторе процесса **Dr.Web Daemon** и о транспортных адресах, по которым доступен **Dr.Web Daemon**. Каталог с PID-файлом также должен быть доступен на запись пользователю, с правами которого работает **Dr.Web Daemon**. Используемый по умолчанию каталог `/var/run/` недоступен пользователям на запись и выполнение. Поэтому, если задано значение параметра **User**, необходимо также указать путь к альтернативному каталогу для PID-файла в значении параметра **PidFile**. Если создать PID-файл не удалось, загрузка **Dr.Web Daemon** прекращается.

Проверка работоспособности Dr.Web Daemon

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

```
$ netstat -a
```

**В случае TCP-сокетов:**

```
. . .
Active Internet connections (servers and
established)
Proto  Recv-Q  Send-Q  Local Address  Foreign
Address  State
. . .
tcp    0        0          localhost:3000  *: *
        LISTEN
. . .
```

В случае UNIX-сокетов:

```
. . .
Active UNIX domain sockets (servers and established)
Proto  RefCnt  Flags  Type  State  I-Node
Path
. . .
unix    0      [ ACC ]  STREAM  LISTENING  1127
%var_dir/.daemon
. . .
```

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

Для проверки работоспособности **Dr.Web Daemon** можно использовать **Консольный клиент Dr.Web Daemon (drwebdc)**, запустив его для получения служебной информации о **Dr. Web Daemon**. 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:

```
- 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.
```

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 **Dr.Web Daemon** 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 -n<ИМЯ_УЗЛА> -p<НОМЕР_ПОРТА> eicar.com
```

Для UNIX-сокета:

```
$ drwebdc -u<ФАЙЛ_СОКЕТА> eicar.com
```

Результатом команды должно быть сообщение:

```
Results: daemon return code 0x20
(known virus is found)
```

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

Если проверка файла прошла успешно, **Dr.Web Daemon** находится в рабочем состоянии.



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

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

Dr.Web Daemon имеет два основных режима проверки:

- проверка фрагмента данных, полученного из сокета (удаленное сканирование);
- проверка файла на диске (локальное сканирование).

При использовании первого режима **Dr.Web Daemon** 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 **Dr.Web Daemon**. Пример работы **Dr.Web Daemon** в этом режиме приведен в предыдущем пункте: клиент читает файл и отправляет его **Dr.Web Daemon** для проверки. **Dr.Web Daemon** может проверять любой фрагмент данных, не обязательно файл.

Более эффективен режим, в котором **Dr.Web Daemon** проверяет указанный файл на диске — локальное сканирование. Клиент сообщает **Dr.Web Daemon** лишь путь к файлу, а не передает весь файл. Путь к проверяемому файлу задается относительно **Dr.Web Daemon** (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. **Dr.Web Daemon** 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 **Dr.Web Daemon** в большинстве случаев не требуется прав администратора.

Обрабатываемые сигналы

Dr.Web Daemon может принимать и обрабатывать следующие сигналы:

- SIGHUP — перезагрузка конфигурационного файла;
- SIGTERM — корректное завершение работы **Dr.Web Daemon**;
- SIGKILL — принудительное завершение работы **Dr.Web Daemon** (в случае проблем);
- SIGUSR1 — инициирует сохранение в журнал [статистики пула процессов](#).

Обратите внимание, что сигнал SIGUSR1 должен посылаться только родительскому процессу, поскольку для дочерних процессов SIGUSR1 приведет к завершению процесса.

Журнал работы и статистика пула процессов

Журнал работы

Поскольку **Dr.Web Daemon** является резидентной программой, информация о его работе может быть получена только из файла журнала (лога). Файл журнала содержит подробности обработки каждого запроса на сканирование, полученного **Dr. Web Daemon**. Имя файла журнала указывается в значении параметра конфигурационного файла **LogFile** **LogFileName**.



Dr.Web Daemon 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 журнала (или назначить службу журналирования **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 **Dr.Web Daemon**, результаты сканирования будут отмечены специальным префиксом при выводе в файл журнала. Возможны следующие префиксы:

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



В операционной системе **FreeBSD** вывод на консоль **Dr.Web Daemon** может быть перехвачен системной службой **syslog** и выведен в файл отчета посимвольно. Эта проблема проявляется, если в конфигурационном файле службы **syslog** `syslog.conf` установлен уровень подробности журналирования `*.info`.

Статистика пула процессов

Статистика текущего состояния пула процессов, который используется для обработки запросов на сканирование, может быть выведена в файл журнала по получению модулем **Dr.Web Daemon** сигнала **SIGUSR1** (сигнал должен посылаться только родительскому процессу, поскольку для дочерних процессов получение сигнала **SIGUSR1** приведет к завершению процесса). Накоплением статистики по пулу процессов управляет соответствующее значение **stat** (**yes** или **no**) в параметре **ProcessesPool**. Статистика не суммируется. В



каждом случае выводится состояние пула, накопленное между двумя последовательными сохранениями статистики.

Пример вывода записи со статистикой 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 **Dr.Web Daemon** с настройками по умолчанию, но предпочтительнее настроить его в соответствии с требованиями и условиям эксплуатации. Конфигурационный файл `drweb32.ini` читается **Dr.Web Daemon** из каталога `%etc_dir`. Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске **Dr.Web Daemon**.

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

Секция [Daemon]

EnginePath = { путь к файлу }	<p>Расположение модуля <code>drweb32.dll</code> (Антивирусное ядро Dr.Web Engine).</p> <p>Этот параметр также используется модулем обновления Dr.Web Updater.</p> <p><u>Значение по умолчанию:</u></p> <p>EnginePath = <code>%bin_dir/lib/drweb32.dll</code></p>
VirusBase = { список масок файлов }	<p>Маски для подключаемых вирусных баз.</p> <p>Этот параметр также используется модулем обновления Dr.Web Updater. Допустимо перечисление нескольких масок через запятую.</p> <p>По умолчанию вирусные базы хранятся в файлах с расширением <code>.vdb</code></p> <p><u>Значение по умолчанию:</u></p> <p>VirusBase = <code>%var_dir/bases/*.vdb</code></p>
UpdatePath = { путь к каталогу }	<p>Каталог хранения обновлений.</p> <p>Этот параметр используется модулем обновления Dr.Web Updater и должен</p>



	<p>быть задан обязательно.</p> <p><u>Значение по умолчанию:</u></p> <p>UpdatePath = %var_dir/ updates/</p>
<p>TempPath = { путь к каталогу }</p>	<p>Этот каталог используется Антивирусным ядром Dr.Web Engine для создания временных файлов.</p> <p>При нормальной работе каталог практически не используется, он нужен для распаковки некоторых видов архивов или когда в системе не хватает памяти.</p> <p><u>Значение по умолчанию:</u></p> <p>TempPath = %var_dir/spool/</p>
<p>Key = { список путей к файлам }</p>	<p>Расположение ключевых файлов. По умолчанию ключевой файл имеет расширение .key</p> <p>Ключевой файл может быть различным для Dr.Web Daemon и для Dr.Web Scanner. Соответственно, при необходимости нужно изменить настройки данного параметра.</p> <p>Параметр может задаваться несколько раз, указывая несколько лицензионных ключевых файлов. В таком случае Dr. Web Daemon пытается объединить права, предоставляемые различными лицензиями.</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:</p> <ul style="list-style-type: none">• Terminal – вывод на консоль,• Quiet – отменяет вывод. <p><u>Значение по умолчанию:</u></p> <p>OutputMode = Terminal</p>



RunForeground = { логический}	<p>Значение Yes запрещает Dr.Web Daemon переходить в режим демона, т. е. становиться фоновым процессом без управляющего терминала.</p> <p>Эта возможность может быть использована некоторыми средствами мониторинга (например, Dr.Web Monitor).</p> <p><u>Значение по умолчанию:</u> RunForeground = No</p>
User = { строка}	<p>Пользователь, с правами которого работает Dr.Web Daemon.</p> <p>Рекомендуется завести в системе специального пользователя drweb, который будет использоваться Dr.Web Daemon и некоторыми фильтрами. Использовать Dr.Web Daemon с правами root нежелательно, хотя такое решение значительно проще настраивается.</p> <p>Значение этого параметра не изменяется во время процедуры перечитывания конфигурации "на лету" (обработки сигнала SIGHUP).</p> <p><u>Значение по умолчанию:</u> User = drweb</p>
PidFile = { путь к файлу}	<p>Имя файла, в который при запуске Dr. Web Daemon 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).</p> <p>Если задано более одного параметра Socket, в данном файле будет присутствовать информация обо всех заданных сокетах (по одному в строке).</p>



	<p><u>Значение по умолчанию:</u></p> <pre>PidFile = %var_dir/run/ drwebd.pid</pre>
<pre>BusyFile = { путь к файлу }</pre>	<p>Данный файл сигнализирует о занятости Dr.Web Daemon: он создается сканирующей "копией" Dr.Web Daemon при получении команды и уничтожается после передачи результата ее выполнения.</p> <p>Имя файла, создаваемого каждой "копией" Dr.Web Daemon, дополняется точкой и ASCII-представлением pid (например, /var/run/drwebd.bsy.123456).</p> <p><u>Значение по умолчанию:</u></p> <pre>BusyFile = %var_dir/run/ drwebd.bsy</pre>
<pre>ProcessesPool = { настройки пула процессов }</pre>	<p>Настройки динамического пула процессов.</p> <p>Первым определяется количество процессов в пуле:</p> <ul style="list-style-type: none">• 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;• N-M — целые положительные значения, и M>=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} — собирать ли статистику по процессам в пуле. В случае если этот параметр равен yes, при получении системного сигнала SIGUSR1 Dr.Web Daemon сохранит текущую накопленную статистику в файл журнала. В противном случае учет и сохранение статистики не производится.• 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>
<pre>OnlyKey = { логический}</pre>	<p>Подключение возможности запросить только ключевой файл от Dr.Web Agent, не запрашивая конфигурацию. При этом будет использоваться локальный конфигурационный файл.</p> <p>Если указан адрес сокета Dr.Web Agent и значение параметра OnlyKey установлено в no, то Dr.Web Agent будет отправлять статистика работы Dr.Web Daemon (после сканирования каждого файла Dr.Web Daemon будет отправлять информацию Dr.Web Agent).</p>



	<p><u>Значение по умолчанию:</u></p> <p>OnlyKey = No</p>
<p>ControlAgent = { адрес}</p>	<p>Адрес сокета Dr.Web Agent.</p> <p>Пример:</p> <pre>ControlAgent = inet: 4040@127.0.0.1, local: / var/drweb/ipc/.agent</pre> <p>Dr.Web Daemon получает через этот сокет от Dr.Web Agent лицензионный ключ (и конфигурационный файл, если в качестве значения параметра OnlyKey задано No. Кроме того, в этом случае через этот сокет Dr.Web Daemon отправляет Dr.Web Agent статистику проверки файлов).</p> <p><u>Значение по умолчанию:</u></p> <pre>ControlAgent = local: % var_dir/ipc/.agent</pre>
<p>MailCommand = { строка}</p>	<p>Команда shell, вызываемая Dr.Web Daemon и модулем обновления Dr.Web Updater для отсылки уведомлений пользователю (администратору) по электронной почте.</p> <p>Dr.Web Daemon использует этот механизм при каждом запуске (перезапуске, перезагрузке), если до истечения срока действия ключевого файла (одного из ключевых файлов) осталось менее дней, чем указано в параметре NotifyPeriod.</p> <p>Модуль обновления Dr.Web Updater 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>
<pre>NotifyPeriod = { числовое значение }</pre>	<p>Значение данного параметра определяет, за сколько дней до окончания срока действия ключевого файла рассылаются уведомления о необходимости продления лицензии.</p> <p>Если указано значение 0, уведомления рассылаются сразу после окончания действия ключа.</p> <p><u>Значение по умолчанию:</u></p> <pre>NotifyPeriod = 14</pre>
<pre>NotifyFile = { путь к файлу }</pre>	<p>Путь к файлу с меткой времени последнего уведомления о продлении лицензии.</p> <p><u>Значение по умолчанию:</u></p> <pre>NotifyFile = %var_dir/.notify</pre>
<pre>NotifyType = { Ever Everyday Once }</pre>	<p>Регулярность отправления уведомления о продлении лицензии:</p> <ul style="list-style-type: none">• Once – уведомление посылается единожды.• Everyday – уведомление посылается каждый день.• Ever – уведомление посылается при каждой перезагрузке Dr.Web Daemon или обновлении баз. <p><u>Значение по умолчанию:</u></p> <pre>NotifyType = Ever</pre>
<pre>FileTimeout = { числовое значение }</pre>	<p>Максимальное разрешенное время проверки одного файла в секундах.</p> <p>Если указано значение 0, время</p>



	<p>проверки файла не ограничивается.</p> <p><u>Значение по умолчанию:</u></p> <p>FileTimeout = 30</p>
<p>StopOnFirstInfected = { логический }</p>	<p>Прекращение проверки письма после первого обнаруженного вируса.</p> <p>Установка значения Yes может резко сократить нагрузку на почтовый сервер и время проверки писем.</p> <p><u>Значение по умолчанию:</u></p> <p>StopOnFirstInfected = No</p>
<p>ScanPriority = { числовое значение }</p>	<p>Приоритет сканирующих процессов Dr. Web Daemon.</p> <p>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> <p>ScanPriority = 0</p>
<p>FileTypes = { список расширений файлов }</p>	<p>Типы файлов, которые будут проверяться при сканировании по типу, т.е. когда параметр ScanFiles (см. ниже) имеет значение byType.</p> <p>Допускаются <u>символы маски</u> '*' и '?'.</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, RTE, 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>
<p>FileTypesWarnings = { логический }</p>	<p>Предупреждение о файлах неизвестных типов.</p> <p><u>Значение по умолчанию:</u></p> <p>FileTypesWarnings = Yes</p>
<p>ScanFiles = { All ВуType }</p>	<p>Дополнительное ограничение на файлы, подлежащие проверке.</p> <p>При задании значения ВуType учитываются расширения файлов, значения которых заданы или по умолчанию, или в параметре (параметрах) FileTypes.</p> <p>Внутри почтовых файлов всегда действует режим All. Значение ВуType может быть использовано только в режиме локального сканирования.</p> <p><u>Значение по умолчанию:</u></p> <p>ScanFiles = All</p>
<p>CheckArchives = { логический }</p>	<p>Проверка файлов, содержащихся в архивах.</p> <p>Поддерживаются архивы форматов ZIP (WinZip, InfoZIP и др.), RAR, ARJ, TAR, GZIP, CAB и др.</p>



	<u>Значение по умолчанию:</u> CheckArchives = Yes
CheckEmailFiles = { логический }	Проверка файлов в почтовых (e-mail) форматах. <u>Значение по умолчанию:</u> CheckEmailFiles = Yes
ExcludePaths = { список путей (масок) }	Маски для тех файлов, которые не должны проверяться. <u>Значение по умолчанию:</u> ExcludePaths = /proc,/sys,/dev
FollowLinks = { логический }	Следование символическим ссылкам при сканировании. <u>Значение по умолчанию:</u> FollowLinks = No
RenameFilesTo = { маска }	Маска для переименования файлов, если сработало действие Rename. <u>Значение по умолчанию:</u> RenameFilesTo = #??
MoveFilesTo = { путь к каталогу }	Путь к каталогу Карантина . <u>Значение по умолчанию:</u> MoveFilesTo = %var_dir/ infected/
BackupFilesTo = { путь к каталогу }	Каталог для сохранения зараженных файлов, которые были вылечены. <u>Значение по умолчанию:</u> BackupFilesTo = %var_dir/ infected/

Параметры регистрации событий:



LogFileName = {syslog путь к файлу}	<p>Имя файла журнала или syslog, если нужно использовать системный сервис syslog.</p> <p><u>Значение по умолчанию:</u></p> <p>LogFileName = syslog</p>
SyslogFacility = {метка syslog}	<p><u>Метка_записи</u> при использовании системного сервиса syslog.</p> <p><u>Значение по умолчанию:</u></p> <p>SyslogFacility = Daemon</p>
SyslogPriority = {уровень подробности}	<p><u>Уровень подробности</u> ведения журнала при использовании системного сервиса syslog.</p> <p>Допускается использование следующих уровней:</p> <ul style="list-style-type: none">• Error• Alert• Warning• Info• Notice <p><u>Значение по умолчанию:</u></p> <p>SyslogPriority = Info</p>
LimitLog = {логический}	<p>Ограничение размера файла журнала.</p> <p>Игнорируется при использовании системного сервиса syslog.</p> <p>Ограничение размера файла журнала реализуется следующим образом: при запуске или получении сигнала HUP Dr. Web Daemon проверяет размер файла журнала, и если он превышает значение, заданное в параметре MaxLogSize, файл журнала стирается и ведение журнала начинается с нуля.</p>



	<p><u>Значение по умолчанию:</u></p> <p>LimitLog = No</p>
<p>MaxLogSize = { числовое значение }</p>	<p>Максимальный размер файла журнала в килобайтах.</p> <p>Имеет смысл только если не используется syslog и LimitLog = Yes.</p> <p>Если указано значение 0, размер файла журнала проверяться не будет.</p> <p><u>Значение по умолчанию:</u></p> <p>MaxLogSize = 512</p>
<p>LogScanned = { логический }</p>	<p>Вывод в файл журнала информации обо всех проверяемых объектах, независимо от того, обнаружены вирусы или нет.</p> <p><u>Значение по умолчанию:</u></p> <p>LogScanned = Yes</p>
<p>LogPacked = { логический }</p>	<p>Вывод в файл журнала дополнительной информации о файлах, упакованных утилитами DIET, PKLITE и др.</p> <p><u>Значение по умолчанию:</u></p> <p>LogPacked = Yes</p>
<p>LogArchived = { логический }</p>	<p>Вывод в файл журнала дополнительной информации об архиваторах.</p> <p><u>Значение по умолчанию:</u></p> <p>LogArchived = Yes</p>
<p>LogTime = { логический }</p>	<p>Вывод в файл журнала времени каждой записи.</p> <p>Параметр не имеет смысла при использовании системного сервиса syslog</p>



	<p><u>Значение по умолчанию:</u></p> <p>LogTime = Yes</p>
<p>LogProcessInfo = { логический }</p>	<p>Вывод в файл журнала 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>
<p>RecodeNonprintable = { логический }</p>	<p>Перекодировка при выводе в файл журнала символов, не являющихся отображаемыми для данного терминала (см. следующие два параметра).</p> <p><u>Значение по умолчанию:</u></p> <p>RecodeNonprintable = Yes</p>
<p>RecodeMode = { Replace QuotedPrintable }</p>	<p>При RecodeNonprintable = Yes задает метод перекодировки неотображаемых символов.</p> <p>При RecodeMode = Replace все такие символы заменяются на значение параметра RecodeChar (см. ниже).</p> <p>При RecodeMode = QuotedPrintable производится перекодировка неотображаемых символов в формат Quoted Printable.</p> <p><u>Значение по умолчанию:</u></p> <p>RecodeMode = QuotedPrintable</p>
<p>RecodeChar = { "?" "_" ... }</p>	<p>При RecodeMode = Replace задает символ, на который будут заменены все неотображаемые символы.</p> <p><u>Значение по умолчанию:</u></p> <p>RecodeChar = "?"</p>



Socket =
{ список адресов }

Описание сокета, который будет использован для связи с **Dr.Web Daemon**.

Пример:

```
Socket = inet: 3000@127.0.0.1,  
local: %var_dir/.daemon
```

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 **Dr.Web Daemon** будет принимать запросы.

Пример:

```
Socket = 3000 127.0.0.1,  
192.168.0.100
```

Для UNIX-сокета: ФАЙЛ - имя сокета, доступ - восьмеричное значение прав доступа к нему.

Пример:

```
Socket = %var_dir/.daemon  
0660
```

Количество значений в списке **Socket** не ограничено, **Dr.Web Daemon** будет работать со всеми из описанных сокетов.

Чтобы **Dr.Web Daemon** принимал запросы через все доступные интерфейсы, для параметра следует задать значение 3000 0.0.0.0.

Значение по умолчанию:

```
Socket = %var_dir/run/.daemon
```

SocketTimeout =
{ числовое значение }

Время в секундах, отведенное для приема/передачи всех данных через сокет (время сканирования файла не



	учитывается).
	Если указано значение 0, время не будет ограничено.
	<u>Значение по умолчанию:</u>
	SocketTimeout = 10

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.

MaxCompressionRatio = { числовое значение}	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. Параметр может принимать только натуральные значения. Если указано значение 0, проверка коэффициента сжатия проводиться не будет.
	<u>Значение по умолчанию:</u>
	MaxCompressionRatio = 5000

CompressionCheckThreshold = { числовое значение}	Минимальный размер файла внутри архива в килобайтах, начиная с которого будет производиться проверка коэффициента сжатия (если это предписано параметром MaxCompressionRatio). Если указано значение 0, проверка производиться не будет.
	<u>Значение по умолчанию:</u>
	CompressionCheckThreshold = 1024



MaxFileSizeToExtract =
{ числовое значение }

Максимальный размер файла в килобайтах, извлекаемого из архива.

Если размер файла внутри архива превышает это значение, он будет пропущен.

Если указано значение 0, максимальный размер не ограничен.

Значение по умолчанию:

MaxFileSizeToExtract = 40960

MaxArchiveLevel =
{ числовое значение }

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).

Если указано значение 0, уровень вложенности архивов не будет ограничиваться.

Значение по умолчанию:

MaxArchiveLevel = 8

ClientsLogs =
{ список строк }

Параметр разделения файлов журнала.

Если при обращении к **Dr.Web Daemon** клиент передает в расширенных опциях свой идентификатор, файл журнала клиента заменяется на тот, который указан в параметре ClientsLogs. Описания логов разделяются запятыми или пробелами.

В случае задания в параметре больше шести файлов журнала строка конфигурационного файла считается неверной.



	<p>Файлы отчета клиентов задаются в виде:</p> <pre>ClientsLogs=<имя клиента>: <путь к файлу>, <имя клиента2>: <путь к файлу>.</pre> <p>Имя клиента может быть одним из следующих:</p> <ul style="list-style-type: none">• 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. <p><u>Пример:</u></p> <pre>drwebdc: /var/drweb/log/ drwebdc.log, smb: syslog, mail: /var/drweb/log/ drwebmail.log</pre> <p><u>Значение по умолчанию:</u></p> <pre>ClientsLogs =</pre>
<p>MaxBasesObsolescencePeriod = { числовое значение}</p>	<p>Максимальный период времени (в часах) с момента последнего обновления, в течение которого вирусные базы считаются "свежими".</p> <p>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.</p> <p>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> <p>MessagePatternFileName = %etc_dir/templates/drwebd/msg.tpl</p>
<p>MailTo = { адрес электронной почты }</p>	<p>Почтовый адрес администратора для отправки сообщений об истечении срока действия лицензии, устаревании вирусных баз и пр.</p> <p><u>Значение по умолчанию:</u></p> <p>MailTo =</p>



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.

