Dr.WEB

Enterprise Security Suite

Приложения

© «Доктор Веб», 2021. Все права защищены

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

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

Товарные знаки

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

Ограничение ответственности

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

Dr.Web Enterprise Security Suite
Версия 12.0
Приложения
07.10.2021

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

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

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Глава 1: Введение

Назначение документа

В документации администратора антивирусной сети Dr.Web Enterprise Security Suite приведены сведения, описывающие как общие принципы, так и детали реализации комплексной антивирусной защиты компьютеров компании с помощью Dr.Web Enterprise Security Suite.

Документация администратора антивирусной сети состоит из следующих основных частей:

1. **Руководство по установке** (**drweb-12.0-esuite-install-manual-ru.pdf**)

   Будет полезно руководителю организации, принимающему решение о приобретении и установке системы комплексной антивирусной защиты.

   В руководстве по установке описан процесс создания антивирусной сети и установки ее основных компонентов.

2. **Руководство администратора** (**drweb-12.0-esuite-admin-manual-ru.pdf**)

   Адресовано *администратору антивирусной сети* — сотруднику организации, которому поручено руководство антивирусной защитой компьютеров (рабочих станций и серверов) этой сети.

   Администратор антивирусной сети должен обладать полномочиями системного администратора или сотрудничать с администратором локальной сети, быть компетентным в вопросах стратегии антивирусной защиты и детально знать антивирусные пакеты Dr.Web для всех используемых в сети операционных систем.

3. **Приложения** (**drweb-12.0-esuite-appendices-ru.pdf**)

   Содержат техническую информацию, описывающую параметры настройки компонентов Антивируса, а также синтаксис и значения инструкций, используемых при работе с ними.

Между перечисленными выше документами присутствуют перекрестные ссылки. При загрузке документов на локальный компьютер, перекрестные ссылки будут функционировать только в том случае, если документы расположены в одном каталоге и имеют изначальные названия.

Также поставляются следующие Руководства:

1. **Инструкция по развертыванию антивирусной сети**

   Содержит краткую информацию по установке и первоначальной настройке компонентов антивирусной сети. За подробной информацией обращайтесь к документации администратора.

2. **Руководства по управлению станциями**

   Содержат информацию о централизованной настройке компонентов антивирусного ПО рабочих станций, осуществляемой администратором антивирусной сети через Центр управления безопасностью Dr.Web.

3. **Руководства пользователя**

   Содержат информацию о настройке антивирусного решения Dr.Web, осуществляемой непосредственно на защищаемых станциях.

4. **Руководство по Web API**

   Содержит техническую информацию по интеграции Dr.Web Enterprise Security Suite со сторонним программным обеспечением посредством Web API.

5. **Руководство по базе данных Сервера Dr.Web**

   Содержит описание внутренней структуры базы данных Сервера Dr.Web и примеров её использования.

Все перечисленные Руководства поставляются в том числе в составе продукта Dr.Web Enterprise Security Suite и могут быть открыты через Центр управления безопасностью Dr.Web.

Перед прочтением документов убедитесь, что это последняя версия соответствующих Руководств для вашей версии продукта. Руководства постоянно обновляются, и последнюю их версию можно найти на официальном веб-сайте компании «Доктор Веб» по адресу https://download.drweb.com/doc/.

Условные обозначения и сокращения

Условные обозначения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Важное замечание или указание.
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.

Обозначение	Комментарий
`C:\Windows\`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте Руководства могут употребляться без расшифровки следующие сокращения:

- ACL — списки контроля доступа (Access Control List),
- CDN — сеть доставки контента (Content Delivery Network),
- DFS — распределенная файловая система (Distributed File System),
- DNS — система доменных имен (Domain Name System),
- FQDN — полностью определенное имя домена (Fully Qualified Domain Name),
- GUI — графический пользовательский интерфейс (Graphical User Interface), GUI-версия программы — версия, использующая средства GUI,
- MIB — база управляющей информации (Management Information Base),
- MTU — максимальный размер полезного блока данных (Maximum Transmission Unit),
- NAP — Network Access Protection,
- TTL — время жизни пакета (Time To Live),
- UDS — доменный сокет UNIX (UNIX Domain Socket),
- БД, СУБД — База Данных, Система Управления Базами Данных,
- ВСО Dr.Web — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение.

Глава 2: Приложения

Приложение А. Полный список поддерживаемых версий ОС

Для Сервера Dr.Web

ОС семейства UNIX

Linux, при наличии библиотеки `glibc` 2.13 или более поздней версии; включая ALT 8, 9 и Astra Linux Special Edition 1.6, 1.7

FreeBSD 11 или более поздней версии.

ОС Windows

- 32 bit:

Windows 7

Windows 8

Windows 8.1

Windows 10 (21H1 и более ранние)

- 64 bit:

Windows Server 2008 R2

Windows 7

Windows Server 2012

Windows Server 2012 R2

Windows 8

Windows 8.1

Windows 10 (21H1 и более ранние)

Windows 11

Windows Server 2016

Windows Server 2019

Windows Server 2022

Для Агента Dr.Web и антивирусного пакета

ОС семейства UNIX

Linux для платформ Intel x86/x86_64/arm64/e2k на основе ядра версии 2.6.37 или позднее, использующая PAM и библиотеку `glibc` 2.13 или более поздней версии.

Для корректной работы компонента SpIDer Gate ядро ОС должно быть собрано со включением следующих опций:

- `CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;`
- `CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;`
- `CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.`

В случае использования 64-битной версии операционной системы, должна быть обязательно включена поддержка исполнения 32-битных приложений.

Программный продукт поддерживается для следующих дистрибутивов **Linux**:

Платформа	Поддерживаемые дистрибутивы Linux
x86_64	• Astra Linux Special Edition (Смоленск) 1.6, 1.7 • Astra Linux 2.12 Орел • Debian 9, 10 • Fedora 31, 32 • CentOS 7, 8 • Ubuntu 18.04, 20.04 • Alt Linux Workstation 8, 9 • Alt Linux Server 8, 9 • SUSE Linux Enterprise Server 12SP3
x86	• CentOS 7 • Debian 10
ARM64	• Ubuntu 18.04 • CentOS 7, 8 • ALT Linux Workstation 9 • ALT Linux Server 9
E2K	• Astra Linux Special Edition (Ленинград) 8.1 • ALT Linux Workstation 8 СП

Платформа	Поддерживаемые дистрибутивы Linux
	• Эльбрус-Д MCST 1.4

Для прочих дистрибутивов **Linux**, соответствующих описанным требованиям, полная совместимость с Dr.Web Enterprise Security Suite не гарантируется. При возникновении проблем с совместимостью с вашим дистрибутивом обратитесь в техническую поддержку: https://support.drweb.com.

Если к Dr.Web Enterprise Security Suite подключаются компоненты версии 6, для получения информации о системных требованиях обратитесь к документации по соответствующему компоненту.

ОС Windows

- 32 bit:

Windows XP с SP2

Windows Server 2003 с SP1

Windows Vista с SP2

Windows Server 2008 с SP2

Windows 7 с SP1

Windows 8

Windows 8.1

Windows 10 (21H1 и более ранние)

- 64 bit:

Windows Vista с SP2 и более поздняя

Windows Server 2008 с SP2

Windows Server 2008 R2 с SP1

Windows 7 с SP1

Windows Server 2012

Windows Server 2012 R2

Windows 8

Windows 8.1

Windows 10 (21H1 и более ранние)

Windows 11

Windows Server 2016

Windows Server 2019

Windows Server 2022

Поскольку компания Microsoft прекратила поддержку алгоритма хеширования SHA-1, перед установкой Агента Dr.Web на Windows Vista, Windows 7, Windows Server 2008 или Windows Server 2008 R2 убедитесь, что в операционной системе поддерживается алгоритм шифрования SHA-256. Для этого установите все рекомендуемые обновления из Центра обновления Windows. Подробную информацию о необходимых пакетах обновлений вы можете найти на официальном сайте компании «Доктор Веб».

Удаленная установка Агентов Dr.Web невозможна на рабочие станции под управлением ОС семейства Windows редакций Starter и Home.

macOS

OS X 10.11 (El Capitan)

macOS 10.12 (Sierra)

macOS 10.13 (High Sierra)

macOS 10.14 (Mojave)

macOS 10.15 (Catalina)

macOS 11.5 (Big Sur)

ОС Android

Android 4.4

Android 5.0

Android 5.1

Android 6.0

Android 7.0

Android 7.1

Android 8.0

Android 8.1

Android 9.0

Android 10.0

Android 11.0

Приложение Б. Настройки для использования СУБД. Параметры драйверов СУБД

Структуру БД Сервера Dr.Web можно получить на основе sql-скрипта `init.sql`, расположенного в подкаталоге `etc` каталога установки Сервера Dr.Web.

В качестве базы данных Сервера Dr.Web может использоваться:

- встроенная СУБД;
- внешняя СУБД.

Встроенная СУБД

При настройке обращения к встроенной СУБД для хранения и обработки данных используются параметры, приведенные в таблице **Б-1**.

Таблица Б-1. Встроенная СУБД

Имя	Значение по умолчанию	Описание
`DBFILE`	`database.sqlite`	Путь к файлу базы данных
`CACHESIZE`	`2000`	Размер кеша базы данных в страницах
`SYNCHRONOUS`	`FULL`	Режим синхронной записи изменений в базе данных на диск: • FULL — полностью синхронная запись на диск, • NORMAL — синхронная запись критичных данных, • OFF — асинхронная запись

В качестве встроенной СУБД предоставляется SQLite3 — СУБД, поддерживаемая Сервером, начиная с версии 10.

Внешняя СУБД

В качестве внешней базы данных Сервера Dr.Web может использоваться:

- СУБД Oracle. Описание настройки приведено в Приложении Б2. Настройка драйвера БД для Oracle.
- СУБД PostgreSQL. Описание настроек, необходимых для СУБД PostgreSQL описано в Приложении Б3. Использование СУБД PostgreSQL.

- Microsoft SQL Server/Microsoft SQL Server Express. Для доступа к данным СУБД может использоваться ODBC-драйвер (настройка параметров ODBC-драйвера для ОС Windows приведена в Приложении Б1. Настройка ODBC-драйвера).

Поддерживается использование Microsoft SQL Server 2008 и более поздней версии. Рекомендуется использование Microsoft SQL Server 2014 и более поздней версии.

БД Microsoft SQL Server Express не рекомендуется для развертывания антивирусной сети с большим количеством станций (от 100 и больше).

При подключении Microsoft SQL Server в качестве внешней БД к Серверу, работающему под ОС семейства UNIX, корректная работа через ODBC с FreeTDS не гарантируется.

При возникновении предупреждений или ошибок в работе Сервера Dr.Web с СУБД Microsoft SQL Server через ODBC следует убедиться, что вы используете последнюю доступную версию СУБД для данной редакции.

С тем, как определить наличие обновлений, вы можете ознакомиться на следующей странице компании Microsoft: https://docs.microsoft.com/en-us/troubleshoot/sql/general/determine-version-edition-update-level.

Чтобы сократить количество блокировок при использовании СУБД Microsoft SQL Server с уровнем изоляции транзакций по умолчанию (READ COMMITTED), рекомендуется включить параметр READ_COMMITTED_SNAPSHOT, выполнив следующую SQL-команду:

```
ALTER DATABASE <название_базы_данных>
SET READ_COMMITTED_SNAPSHOT ON;
```

Команду следует выполнять в режиме неявных транзакций и при единственном существующем подключении к базе данных.

Сравнительные характеристики встроенных и внешних СУБД

Использование встроенной БД допустимо при подключении к Серверу не более 200–300 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен Сервер Dr.Web, и нагрузка по прочим задачам, выполняемым на данном компьютере, возможно подключение до 1000 станций.

В противном случае необходимо использовать внешнюю БД.

При использовании внешней БД и подключении к Серверу более 10000 станций рекомендуется выполнение следующих минимальных требований:

- процессор с частотой 3ГГц,
- оперативная память — от 4 ГБ для Сервера Dr.Web, от 8 ГБ — для сервера БД,
- ОС семейства UNIX.

При выборе между встроенной и внешней базами следует учесть некоторые параметры, присущие каждой из СУБД:

- В больших антивирусных сетях (свыше 200–300 станций) рекомендуется использовать внешнюю БД, более устойчивую к сбоям, чем встроенные БД.
- При использовании встроенной БД не требуется установка компонентов сторонних производителей. Рекомендуется при типичном использовании.
- Встроенная база данных не требует знаний администрирования СУБД и является хорошим выбором для антивирусной сети малого и среднего масштаба.
- Внешнюю базу имеет смысл использовать в том случае, если подразумевается самостоятельная работа с СУБД, требующая прямого доступа к базе. При этом могут использоваться стандартные API для доступа к базам данных, такие как: OLE DB, ADO.NET или ODBC.

Б1. Настройка ODBC-драйвера

При настройке обращения к внешней СУБД для хранения и обработки данных используются параметры, приведенные в таблице **Б-2** (конкретные значения приведены для примера).

Таблица Б-2. Параметры для ODBC-подключения

Имя	Значение	Описание
`DSN`	`drwcs`	Имя набора данных
`USER`	`drwcs`	Имя пользователя
`PASS`	`fUqRbrmlvI`	Пароль
`TRANSACTION`	`DEFAULT`	Возможные значения параметра `TRANSACTION`: • `SERIALIZABLE` • `READ_UNCOMMITTED` • `READ_COMMITTED` • `REPEATABLE_READ` • `DEFAULT` Значение по умолчанию `DEFAULT` означает "использовать умолчание SQL-сервера". Подробнее об уровнях изоляции транзакций смотрите в документации по соответствующей СУБД.

Чтобы исключить проблемы с кодировкой, необходимо отключить следующие параметры ODBC-драйвера:

- **Использовать региональные параметры при выводе валют, чисел, дат и времени** — может вызвать ошибки при форматировании числовых параметров.
- **Выполнять перевод символьных данных** — может вызывать некорректное отображение символов в Центре управления для параметров, пришедших из базы данных. Он устанавливает зависимость отображения символов от языкового параметра для программ, не использующих Unicode.

При создании новой базы данных в СУБД Microsoft SQL необходимо указывать сортировку с учетом регистра (суффикс `_CS`) и с учетом диакритических знаков (суффикс `_AS`).

Сама база данных создается предварительно на SQL-сервере с параметрами, указанными выше.

Необходимо также настроить параметры ODBC-драйвера для компьютера, на который установлен Сервер Dr.Web.

Информацию по настройке ODBC-драйвера под ОС семейства UNIX можно найти на http://www.unixodbc.org/ в разделе **Manuals**.

Настройка ODBC-драйвера для ОС Windows

Чтобы настроить параметры ODBC-драйвера

1. На **Панели управления** ОС Windows выберите пункт **Администрирование**, в открывшемся окне дважды щелкните по значку **Источники данных (ODBC)**. Откроется окно **Администратор источников данных ODBC**. Перейдите на вкладку **Системный DSN**.
2. Нажмите кнопку **Добавить**. Откроется окно выбора драйвера.
3. Выберите в списке пункт, соответствующий ODBC-драйверу для данной БД, и нажмите кнопку **Готово**. Откроется первое из окон настройки доступа к серверу баз данных.

При использовании внешней СУБД необходимо установить последнюю версию ODBC-драйвера, поставляемую с данной СУБД. Использование ODBC-драйвера, поставляемого вместе с ОС Windows, не рекомендовано. Исключением являются БД, поставляемые Microsoft без ODBC-драйвера.

4. Укажите параметры доступа к источнику данных, совпадающие с параметрами, заданными в настройках Сервера Dr.Web. Если сервер БД находится не на том же компьютере, что и Сервер Dr.Web, укажите в поле **Сервер** IP-адрес или имя сервера БД. Нажмите кнопку **Далее**.
5. Выберите опцию **проверка подлинности учетной записи SQL Server** и задайте необходимые учетные данные пользователя для доступа к БД. Нажмите кнопку **Далее**.

6. В выпадающем списке **Использовать по умолчанию базу данных** выберите базу данных, используемую Сервером Dr.Web. При этом обязательно должно быть указано имя базы данных Сервера, а не значение **Default**.

   Убедитесь, что установлены следующие флаги: **Заключенные в кавычки идентификаторы в формате ANSI**, **Значения null, Шаблоны и предупреждения в формате ANSI**. Нажмите кнопку **Далее**.

   Если при настройке ODBC-драйвера имеется возможность изменить язык системных сообщений SQL-сервера, необходимо установить английский язык.

7. По окончании настройки нажмите кнопку **Готово**. Откроется окно со сводкой заданных вами параметров.
8. Для проверки правильности настроек нажмите кнопку **Проверить источник данных**. После сообщения об успешности проверки нажмите кнопку **OK**.

Б2. Настройка драйвера БД для Oracle

Общее описание

Oracle Database (или Oracle DBMS) — объектно-реляционная СУБД. Oracle может быть использована в качестве внешней БД для Dr.Web Enterprise Security Suite.

Сервер Dr.Web может использовать СУБД Oracle в качестве внешней базы на всех платформах, кроме FreeBSD (см. п. Установка и поддерживаемые версии).

Чтобы использовать СУБД Oracle

1. Установить экземпляр БД Oracle с настройками кодировки `AL32UTF8`. Также можно использовать существующий экземпляр БД с указанной кодировкой.
2. Настроить драйвер БД на использование соответствующей внешней базы. Это можно сделать в конфигурационном файле или при помощи Центра управления: меню **Конфигурация Сервера Dr.Web**, вкладка **База данных**.

   Если вы планируете использовать в качестве внешней базы данных БД Oracle через ODBC-подключение, то при установке (обновлении) Сервера, в настройках инсталлятора отмените установку встроенного клиента для СУБД Oracle (в разделе **Поддержка баз данных → Драйвер базы данных Oracle**).

   В противном случае работа с БД Oracle через ODBC будет невозможна из-за конфликта библиотек.

   Подключение к БД Oracle от лица системных пользователей SYS и SYSTEM, а также с привилегиями SYSDBA и SYSOPER запрещено.

Установка и поддерживаемые версии

Для возможности использования БД Oracle в качестве внешней базы необходимо установить экземпляр БД Oracle и настроить для него кодировку `AL32UTF8` (`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`). Это можно сделать следующими способами:

1. При помощи инсталлятора БД Oracle (используйте расширенный режим установки и конфигурирования БД).
2. При помощи SQL команды `CREATE DATABASE`.

Более подробная информация о создании и конфигурации БД приведена в документации к БД Oracle.

В случае использования кодировки, отличной от указанной, национальные символы будут отображаться некорректно.

Клиент для доступа к БД (Oracle Instant Client) входит в состав установочного пакета Dr.Web Enterprise Security Suite.

Платформы, поддерживаемые СУБД Oracle, приведены на сайте производителя.

Платформы, поддерживаемые Oracle Client, приведены на сайте производителя.

Dr.Web Enterprise Security Suite поддерживает СУБД Oracle версии 11 и позднее.

Также обратите внимание на системные требования к Серверу Dr.Web при работе с внешней базой данных Oracle (см. **Руководство по установке**, п. Системные требования).

Параметры

При настройке обращения к СУБД Oracle используются параметры, описываемые в таблице **Б-3**.

Таблица Б-3. Параметры СУБД Oracle

Параметр	Описание
`drworacle`	Имя драйвера
`User`	Имя пользователя БД (обязательный)
`Password`	Пароль пользователя (обязательный)

Параметр	Описание
`ConnectionString`	Строка соединения с базой данных (обязательный)
`Prefetch-rows`	Количество строк для предварительной выборки при выполнении запроса к базе данных
`Prefetch-mem`	Объем памяти, выделяемой для предварительной выборки строк при выполнении запроса к базе данных

Формат строки соединения с СУБД Oracle следующий:

//<host>:<port>/<service name>

где:

- *<host>* — IP-адрес либо имя сервера Oracle;
- *<port>* — порт, который "слушает" сервер;
- *<service name>* — имя БД, к которой необходимо подключиться.

Например:

```
//myserver111:1521/bjava21
```

где:

- `myserver111` — имя сервера Oracle.
- `1521` — порт, который "слушает" сервер.
- `bjava21` — имя БД, к которой необходимо подключиться.

Конфигурация драйвера СУБД Oracle

При использовании СУБД Oracle необходимо изменить определение и настройки драйвера БД одним из следующих способов:

- В Центре управления: пункт **Администрирование** главного меню → пункт **Конфигурация Сервера Dr.Web** управляющего меню → вкладка **База данных** → выбрать в выпадающем списке **База данных** тип **Oracle**, установить настройки согласно формату, приведенному выше.
- В конфигурационном файле Сервера.

Б3. Использование СУБД PostgreSQL

Общее описание

PostgreSQL — объектно-реляционная СУБД. Является свободной альтернативой коммерческой СУБД (таким как Oracle Database, Microsoft SQL Server и др.). В больших антивирусных сетях СУБД PostgreSQL может быть использована в качестве внешней БД для Dr.Web Enterprise Security Suite.

Чтобы использовать PostgreSQL в качестве внешней БД

1. Установить сервер PostgreSQL или Postgres Pro.
2. Настроить Сервер Dr.Web на использование соответствующей внешней базы. Это можно сделать в конфигурационном файле или при помощи Центра управления: в меню **Конфигурация Сервера Dr.Web**, на вкладке **База данных**.

При подключении к БД PostgreSQL может быть использована только авторизация trust, password и MD5.

Установка и поддерживаемые версии

1. Загрузите самую последнюю версию бесплатного продукта PostgreSQL (сервер PostgreSQL и, если необходимо, соответствующий ODBC-драйвер) или, по крайней мере, не используйте версию ранее чем **8.4**. или 11.4.1 для Postgres Pro.
2. Создайте базу данных PostgreSQL одним из следующих способов:
   a) При помощи графического интерфейса `pgAdmin`.
   b) При помощи SQL-команды `CREATE DATABASE`.

База данных должна быть создана в кодировке UTF8.

Переход на внешнюю БД описан в п. Смена типа СУБД Dr.Web Enterprise Security Suite.

Также обратите внимание на системные требования к Серверу Dr.Web при работе с внешней базой данных PostgreSQL (см. **Руководство по установке**, п. Системные требования).

Параметры

При настройке обращения к БД PostgreSQL используются параметры, описываемые в таблице **Б-4**.

Таблица Б-4. PostgreSQL

Имя	Значение по умолчанию	Описание
`host`	*<Локальный UNIX-сокет>*	Хост сервера PostgreSQL
`port`		Порт сервера PostgreSQL или расширение имени файла сокета
`dbname`	`drwcs`	Название базы данных
`user`	`drwcs`	Имя пользователя
`password`	`drwcs`	Пароль
`options`		Опции отладки/трассировки для отправки серверу
`requiressl`		• 1 для запроса установки SSL соединения • 0 для отсутствия запроса
`temp_tablespaces`		Пространство имен для временных таблиц
`default_transaction_isolation`		Режим изоляции транзакции (см. документацию к PostgreSQL)

Техническую информацию можно также найти по адресу https://www.postgresql.org/docs/ .

Взаимодействие Сервера Dr.Web с БД PostgreSQL через UDS

При установке Сервера Dr.Web и БД PostgreSQL на одной машине возможна настройка их взаимодействия через UDS (доменный сокет UNIX).

Чтобы настроить работу через UDS

1. В конфигурационном файле БД PostgreSQL `postgresql.conf` прописать следующую директорию для UDS:

   ```
   unix_socket_directory = '/var/run/postgresql'
   ```

2. Перезапустить PostgreSQL.

Настройка базы данных PostgreSQL

Для увеличения производительности при работе с базой данных PostgreSQL рекомендуется провести настройку на основе информации из официальных руководств по базе данных.

В случае использования базы данных больших размеров и при наличии соответствующих вычислительных ресурсов, рекомендуется настроить следующие параметры в конфигурационном файле `postgresql.conf`:

Минимальная настройка:

```
shared_buffers = 256MB

temp_buffers = 64MB

work_mem = 16MB
```

Расширенная настройка:

```
shared_buffers = 1GB

temp_buffers = 128MB

work_mem = 32MB

fsync = off

synchronous_commit = off

wal_sync_method = fdatasync

commit_delay = 1000

max_locks_per_transaction = 256

max_pred_locks_per_transaction = 256
```

Параметр `fsync = off` значительно повышает производительность, однако может привести к полной потере данных в случае отключения питания или сбоя системы. Отключение параметра `fsync` рекомендуется только при наличии резервной копии базы данных для возможности ее полного восстановления.

Настройка параметра `max_locks_per_transaction` может быть полезна для обеспечения бесперебойной работы при массовом обращении к таблицам базы данных, в частности, при обновлении базы данных до новой версии.

Б4. Использование СУБД MySQL

Общее описание

MySQL — кроссплатформенная свободная реляционная система управления базами данных. СУБД MySQL может быть использована в качестве внешней БД для Dr.Web Enterprise Security Suite.

Чтобы использовать MySQL в качестве внешней БД

1. Установить сервер MySQL.
2. Настроить Сервер Dr.Web на использование соответствующей внешней базы. Это можно сделать в конфигурационном файле или при помощи Центра управления: в меню **Конфигурация Сервера Dr.Web**, на вкладке **База данных**.

Установка и поддерживаемые версии

Dr.Web Enterprise Security Suite поддерживает следующие версии СУБД MySQL:

- MySQL — с версии 5.5.14 до версии 5.7, а также все версии, начиная с 8.0.12
- MariaDB — 10.0, 10.1, 10.2.

После установки СУБД перед созданием новой базы данных необходимо задать следующие настройки в ее конфигурационном файле (за подробностями обратитесь к документации вашей СУБД):

Для MySQL версий 5.X:

```
[mysqld]

innodb_large_prefix = true

innodb_file_format = barracuda

innodb_file_per_table = true

max_allowed_packet = 64M
```

Для MySQL версий 8.X:

```
[mysqld]

innodb_file_per_table = true

max_allowed_packet = 64M
```

Если версия используемой СУБД MariaDB ранее 10.2.4, то в конфигурационном файле также необходимо указать:

```
binlog_format = mixed
```

Приложение B. Аутентификация администраторов

Базовая информация по аутентификации администраторов на Сервере Dr.Web приведена в **Руководстве администратора**, в п. Аутентификация администраторов.

B1. Аутентификация при использовании Active Directory

Конфигурируется только разрешение использования и порядок в списке аутентификаторов: теги `<enabled/>` и `<order/>` в `auth-ads.conf`.

Принцип работы:

1. Администратор задает имя пользователя и пароль в одном из следующих форматов:
   - `username`,
   - `domain\username`,
   - `username@domain`,
   - LDAP DN пользователя.
2. Сервер регистрируется с этим именем и паролем на доменном контроллере по умолчанию (или доменном контроллере для домена, указанного в имени пользователя).
3. Если не удалось зарегистрироваться, осуществляется переход к следующему механизму аутентификации.
4. Определяется LDAP DN зарегистрированного пользователя.
5. У объекта с вычисленным DN читается атрибут `DrWebAdmin`. Если он установлен в `FALSE` — неуспех и переход к следующему механизму аутентификации.
6. Если на этом этапе какие-либо атрибуты не определены, их поиск осуществляется в группах, в которые входит данный пользователь. Для каждой группы просматриваются ее родительские группы (стратегия поиска — вглубь).

В случае любой ошибки осуществляется переход к следующему механизму аутентификации.

Утилита `drweb-12.00.0-<сборка>-esuite-modify-ad-schema-<версия_ОС>.exe` (поставляется отдельно от дистрибутива Сервера) создает новый класс объектов `DrWebEnterpriseUser` для Active Directory и описывает новые атрибуты для данного класса.

Атрибуты имеют следующие OID в Enterprise пространстве:

```
DrWeb_enterprise_OID "1.3.6.1.4.1" // iso.org.dod.internet.private.enterprise
DrWeb_DrWeb_OID DrWeb_enterprise_OID ".29690" // DrWeb
```

```
DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID ".1" // EnterpriseSuite
DrWeb_Alerts_OID DrWeb_EnterpriseSuite_OID ".1" // Alerts
DrWeb_Vars_OID DrWeb_EnterpriseSuite_OID ".2" // Vars
DrWeb_AdminAttrs_OID DrWeb_EnterpriseSuite_OID ".3" // AdminAttrs

// 1.3.6.1.4.1.29690.1.3.1 (AKA
iso.org.dod.internet.private.enterprise.DrWeb.EnterpriseSuite.AdminAttrs.Admin)

DrWeb_Admin_OID DrWeb_AdminAttrs_OID ".1" // R/W admin
DrWeb_AdminReadOnly_OID DrWeb_AdminAttrs_OID ".2" // R/O admin
DrWeb_AdminGroupOnly_OID DrWeb_AdminAttrs_OID ".3" // Group admin
DrWeb_AdminGroup_OID DrWeb_AdminAttrs_OID ".4" // Admin's group
DrWeb_Admin_AttrName "DrWebAdmin"
DrWeb_AdminReadOnly_AttrName "DrWebAdminReadOnly"
DrWeb_AdminGroupOnly_AttrName "DrWebAdminGroupOnly"
DrWeb_AdminGroup_AttrName "DrWebAdminGroup"
```

Редактирование свойств пользователей Active Directory осуществляется вручную на сервере Active Directory (см. в **Руководстве администратора**, в п. Аутентификация администраторов).

Назначение прав администраторам осуществляется согласно общему принципу наследования в иерархической структуре групп, в которые входит администратор.

В2. Аутентификация при использовании LDAP

Настройки приводятся в файле конфигурации `auth-ldap.conf`.

Основные теги конфигурационного файла:

- `<enabled/>` и `<order/>` — аналогично варианту для Active Directory.
- `<server/>` задает адрес LDAP-сервера. Допускается указание нескольких тегов `<server/>` с адресами разных LDAP-серверов, в результате чего будет создан список серверов, на которых можно выполнить аутентификацию. Первым следует указывать адрес главного сервера, на который предполагается основная нагрузка, после которого можно указать адреса резервных серверов. При подключении администратора используется первый доступный LDAP-сервер. В случае неудачи будет предпринята попытка аутентификации на следующем сервере и далее по порядку в той последовательности, в которой адреса LDAP-серверов указаны в файле конфигурации.
- `<user-dn/>` определяет правила трансляции имен в DN с использованием DOS-подобных масок.

  В теге `<user-dn/>` допускается использование символов подстановки:

  - `*` заменяет последовательность любых символов кроме `.` `,` `=` `@` `\` и пробелов;
  - `#` заменяет последовательность любых символов.
- `<user-dn-expr/>` определяет правила трансляции имен в DN с использованием регулярных выражений.

  Например, одно и то же правило в разных вариантах:

```
<user-dn user="*@example.com" dn="CN=\1,DC=example,DC=com"/>
<user-dn-expr user="(.*)@example.com" dn="CN=\1,DC=example,DC=com"/>
```

\1 .. \9 определяют место подстановки в шаблоне значений *, # или выражений в скобках.

Исходя из данного принципа: если указано имя пользователя в виде login@example.com, то после трансляции получится DN: "CN=login,DC=example,DC=com".

- <user-dn-extension-enabled/> разрешает выполнение Lua-скрипта ldap_user_dn_translate.ds (из каталога extensions) для выполнения трансляции имени пользователя в DN. Данный скрипт выполняется после попыток применения всех правил user-dn, user-dn-expr в случае, если не найдено ни одно подходящее правило. У скрипта один параметр — введенное имя пользователя. Скрипт возвращает строку, содержащую либо DN, либо ничего. В случае, если не подошло ни одно правило, и скрипт не разрешен или не вернул ничего, то введенное имя пользователя используется как есть.
- Атрибут LDAP-объекта для DN, полученного в результате трансляции, и его возможные значения могут быть переопределены следующим тегом (указаны значения по умолчанию):

```
<!-- DrWebAdmin attribute equivalent (OID 1.3.6.1.4.1.29690.1.3.1) -->
<admin-attribute-name value="DrWebAdmin" true-value="^TRUE$" false-value="^FALSE$"/>
```

  В качестве значений параметров true-value/false-value задаются регулярные выражения.
- Если остались неопределенные значения атрибута администратора, то в случае задания в конфигурационном файле тега <group-reference-attribute-name value="memberOf"/>, значение атрибута memberOf рассматривается как список DN групп, в которые входит данный администратор, и поиск нужных атрибутов по этим группам ведется также, как в случае с использованием Active Directory.

В3. Аутентификация при использовании LDAP/AD

Конфигурационный файл

Настройки приводятся в файле конфигурации auth-ldap-rfc4515.conf.

Также предоставляются конфигурационные файлы с типовыми настройками:

- auth-ldap-rfc4515-check-group.conf — шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме с проверкой принадлежности к группе Active Directory.
- auth-ldap-rfc4515-check-group-novar.conf — шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме с проверкой принадлежности к группе Active Directory с использованием переменных.

- `auth-ldap-rfc4515-simple-login.conf` — шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме.

Основные теги конфигурационного файла auth-ldap-rfc4515.conf:

- `<server />` — определение LDAP сервера.

Атрибут	Описание	Значение по умолчанию
`base-dn`	DN объекта, относительно которого осуществляется поиск.	Значение атрибута `rootDomainNamingContext` объекта `Root DSE`
`cacertfile`	Файл корневых сертификатов (только UNIX).	–
`host`	Адрес LDAP-сервера.	• Доменный контроллер для сервера под ОС Windows. • `127.0.0.1` для сервера под ОС семейства UNIX. • Допускается указание нескольких тегов `<server />` с адресами разных LDAP-серверов. Первым следует указывать адрес главного сервера, на который предполагается основная нагрузка. В случае неудачи будет предпринята попытка аутентификации на следующем сервере и далее по порядку в указанной последовательности.
`scope`	Область поиска. Допустимые значения: • `sub-tree` — вся область ниже базового DN, • `one-level` — прямые потомки базового DN, • `base` — базовое DN.	`sub-tree`
`tls`	Устанавливать TLS для подключения к LDAP.	`no`
`ssl`	Использовать протокол LDAPS при подключении к LDAP.	`no`

- `<set />` — задание переменных поиском в LDAP.

Атрибут	Описание	Значение по умолчанию
`attribute`	Имя атрибута, значение которого присваивается переменной. Отсутствие недопустимо.	–

Атрибут	Описание	Значение по умолчанию
filter	RFC4515 фильтр поиска в LDAP.	–
scope	Область поиска. Допустимые значения: • sub-tree — вся область ниже базового DN, • one-level — прямые потомки базового DN, • base — базовое DN.	sub-tree
search	DN объекта, относительно которого осуществляется поиск.	При отсутствии используется base-dn тега <server />
variable	Имя переменной. Должно начинаться с буквы и содержать только буквы и цифры. Отсутствие недопустимо.	–

Переменные могут быть использованы в значениях атрибута add тегов <mask /> и <expr />, в значении атрибута value тега <filter /> в форме \varname, а так же в значении атрибута search тега <set />. Допустимый уровень рекурсии при раскрытии переменных — 16.

Если поиск возвращает несколько найденных объектов, то используется только первый.

- <mask /> — шаблоны имени пользователя.

Атрибут	Описание
add	Строка, добавляемая к фильтру поиска по операции И с элементами подстановки.
user	Маска имени пользователя с использование DOS-образных метасимволов * и #. Отсутствие недопустимо.

Например:

```
<mask user="*@#"  add="sAMAccountName=\1" />

<mask user="*\*"  add="sAMAccountName=\2" />
```

\1 и \2 — ссылки на совпадающие маски в атрибуте user.

- <expr /> — шаблоны имени пользователя с использованием регулярных выражений (атрибуты идентичны <mask />).

Например:

```
<expr user="^(.*)@([^.,=@\s\\]+)$"  add="sAMAccountName=\1" />

<expr user="^(.*)\\(.*)"            add="sAMAccountName=\2" />
```

Соответствие масок и регулярных выражений:

Маска	Регулярное выражение
*	.*
#	[^.,=@\s\\]+

- `<filter />` — фильтр поиска в LDAP.

Атрибут	Описание
value	Строка, добавляемая к фильтру поиска по операции И с элементами подстановки.

Конкатенация фильтров

```
<set variable="admingrp"  filter="&amp;(objectclass=group)(cn=ESuite Admin)"
attribute="dn" />
<mask user="*\*" add="sAMAccountName=\2" />
<filter value="&amp;(objectClass=user)(memberOf=\admingrp)" />
```

Если `admingrp` в результате поиска примет значение `"CN=ESuite Admins,OU=some name,DC=example,DC=com"`, а пользователь ввел `domain\user`, тогда в итоге получается фильтр:

```
"(&(sAMAccountName=user)(&(objectClass=user)(memberOf=CN=ESuite
Admins,OU=some name,DC=example,DC=com)))"
```

Пример настройки LDAP/AD-аутентификации

Далее приведен пример типовых настроек для аутентификации с использованием LDAP. Настройки задаются в Центре управления, раздел **Администрирование** → **Аутентификация** → **LDAP/AD-аутентификация** (для варианта **Упрощенные настройки**).

Исходные параметры администраторов, которые должны пройти аутентификацию:

- домен: `dc.test.local`
- группа в Active Directory: `DrWeb_Admins`

Настройки Центра управления:

Название настройки	Значение
Тип сервера	Microsoft Active Directory
Адрес сервера	dc.test.local

Название настройки		Значение
Шаблоны имен пользователей для подтверждения авторизации	Маска учетной записи	test* или *@test.local
	Имя пользователя	\1
Членство пользователей для подтверждения авторизации	Название	DrWeb_Admins
	Тип	группа

В4. Подведомственные разделы прав

Таблица В-1. Список прав администраторов и их особенности

Код	Право	Описание	Раздел Центра управления
Управление группами станций			
1*	**Просмотр свойств групп станций**	Список пользовательских групп, которые администратор видит в антивирусной сети. Все системные группы также отображаются в дереве, но в них видны только станции из указанного списка групп.	Антивирусная сеть Антивирусная сеть → Общие → Свойства
2*	**Редактирование свойств групп станций**	Список пользовательских групп, свойства которых администратор может редактировать. Должен содержать группы из списка права 1.	
3	**Просмотр конфигурации групп станций**	Список пользовательских групп, конфигурация которых доступна для просмотра администратору. Также администратору доступна для просмотра конфигурация станций, для которых группы из списка являются первичными. Должен содержать группы из списка права 1.	Антивирусная сеть Антивирусная сеть → Общие → Запущенные компоненты Антивирусная сеть → Общие → Карантин
4	**Редактирование конфигурации групп станций**	Аналогично праву 3, но с возможностью редактирования. Должен содержать группы из списка права 3.	Страницы из раздела **Конфигурация** управляющего меню

Код	Право	Описание	Раздел Центра управления
5	**Просмотр свойств станций**	Список пользовательских групп, которые являются первичными для станций, свойства которых можно просматривать администратору. Должен содержать группы из списка права 1.	Антивирусная сеть Антивирусная сеть → Общие → Свойства
6	**Редактирование свойств станций**	В том числе ACL, блокировки, допуска и т. д. Аналогично праву 5, но с возможностью редактирования. Должен содержать группы из списка права 5.	
8*	**Помещение станций в группы и удаление станций из групп**	Список пользовательских групп. Должен содержать группы из списка права 1.	Антивирусная сеть
9	**Удаление станций**	Список пользовательских групп, являющихся первичными для станций, которые администратор может удалить. Должен содержать группы из списка права 1.	
10	**Удаленная инсталляция и деинсталляция Агентов**	Список пользовательских групп, для станций которых администратору доступен запуск удаленной установки Агентов с выбранными ID. Данные группы должны быть первичными для устанавливаемых станций. Должен содержать группы из списка права 1. Если есть запрещенные объекты, то пункт в меню не отображается. Установка по сети возможна только из /esuite/network/index.ds при условии, что право 16 разрешено.	
11	**Объединение станций**	Список пользовательских групп, станции из которых можно объединить. Данные группы должны быть первичными для станций. Доступна	

Код	Право	Описание	Раздел Центра управления
		иконка объединения станций на панели инструментов. Должен содержать группы из списка права 1.	
12*	**Просмотр статистических таблиц**	Список пользовательских групп, по которым администратору доступен просмотра статистики. Право дает возможность создать задание в расписании Сервера на получение периодических отчетов. Задается список пользовательских групп, которые админ может указать в этом задании (групп, для станций из которых будут приходить отчеты). Если задана группа Everyone, то отчеты будут приходить по всем группам из списка. Должен содержать группы из списка права 1.	Антивирусная сеть страницы из раздела **Статистика** управляющего меню
23	**Редактирование лицензирования**	Список пользовательских групп, для которых администратор может добавлять/заменять/удалять лицензионный ключ. Данные группы должны быть первичными для станций. Должен содержать группы из списка права 1.	
Управление администраторами			
25	**Создание администраторов, групп администраторов**	Также скрывается соответствующая иконка на панели инструментов.	Администрирование → Конфигурация → Администраторы
26	**Редактирование учетных записей администраторов**	Администратор из группы **Newbies** видит дерево администраторов, корнем которого является группа, в которой он находится, т. е. видит администраторов из своей группы и её подгрупп. Администратор из группы **Administrators** видит всех других администраторов, независимо от их групп.	

Код	Право	Описание	Раздел Центра управления
		Администратор может редактировать учетные записи администраторов из указанных групп. При этом становится доступна соответствующая иконка на панели инструментов.	
27	**Удаление учетных записей администраторов**	Аналогично праву 26.	
28	**Просмотр свойств и конфигурации групп администраторов**	В том числе администраторов в группах и подгруппах. Администратор может выбирать только из подгруппы своей родительской группы.	
39	**Отображение группы администраторов “Newbies”**	Разрешить администратору видеть предустановленную группу **Newbies** в дереве администраторов. Если у администратора нет права на просмотр группы **Newbies**, а сам он находится в этой группе, то видеть он будет только себя.	
29	**Редактирование свойств и конфигурации групп администраторов**	В том числе администраторов в группах и подгруппах. Администратор может выбирать только из подгруппы своей родительской группы. Если данное право не назначено, то администратор не сможет отключить наследование или повысить права администратору в группе, даже если для этой группы назначено право 26.	
Дополнительно			
7	**Создание станций**	При создании станции доступен список групп с правом 8 (для группы, в которую помещаются станции, должно быть назначено право 8). При создании станции первичной должна стать одна из доступных пользовательских групп.	Антивирусная сеть

Код	Право	Описание	Раздел Центра управления
13	**Просмотр аудита**	Аудит доступен для полноправного администратора, а также для объектов с правом 4.	Администрирование → Журналы → Журнал аудита
16	**Запуск Сканера сети**	Если право не назначено, то установка по сети из /esuite/network/index.ds недоступна.	Антивирусная сеть Администрирование → Сканер сети
17	**Подтверждение новичков**	Доступен список групп из права 8. Данное право не может быть предоставлено, если администратору разрешено управление только некоторыми группами, а не всеми объектами антивирусной сети. Т. е. для права 1 (**Просмотр свойств групп станций**) задан набор групп.	Антивирусная сеть
18	**Просмотр расписания Сервера**	Просмотр таблицы **Журнал выполнения заданий**. Если не назначены права 12 и 18, то просмотр страницы с расписанием Сервера запрещен. Если назначено право 12, по при этом право 18 не назначено, то доступен просмотр расписания для статистики. Задание на отправку отчетов для конкретного администратора отображается в зависимости от наличия права 12 и наличия оповещения **Периодический отчет**, даже если право 18 не предоставлено.	Администрирование → Конфигурация → Планировщик заданий Сервера Dr.Web Администрирование → Журналы → Журнал выполнения заданий
19	**Редактирование расписания Сервера**		Администрирование → Конфигурация → Планировщик заданий Сервера Dr.Web
20	**Просмотр конфигурации Сервера и конфигурации репозитория**		Администрирование → Конфигурация → Конфигурация веб-сервера Администрирование → Репозиторий → Состояние репозитория

Код	Право	Описание	Раздел Центра управления
21	**Редактирование конфигурации Сервера и конфигурации репозитория**		Администрирование → Репозиторий → Отложенные обновления Администрирование → Репозиторий → Общая конфигурация репозитория Администрирование → Репозиторий → Детальная конфигурация репозитория Администрирование → Репозиторий → Содержимое репозитория Администрирование → Журналы → Журнал обновлений репозитория Администрирование → Конфигурация → Пользовательские процедуры Администрирование → Сервер Dr.Web → Список версий
22	**Просмотр информации о лицензировании**		Администрирование → Администрирование → Менеджер лицензий
24	**Редактирование конфигурации оповещений**		Администрирование → Оповещения → Конфигурация оповещений Администрирование → Оповещения → Неотправленные оповещения Администрирование → Оповещения → Оповещения веб-консоли
30	**Работа через Web API**		-

Код	Право	Описание	Раздел Центра управления
31	**Просмотр межсерверных связей**		Связи
32	**Редактирование межсерверных связей**		Связи
33	**Использование дополнительных возможностей**	Ограничивает доступ ко всем разделам секции **Дополнительные возможности**, кроме раздела **Утилиты**, который доступен всегда.	Администрирование → Дополнительные возможности
34	**Обновление репозитория**	Обновление репозитория Сервера с ВСО.	Кнопка **Обновить репозиторий** в разделе **Состояние репозитория**
42	**Редактирование собственных настроек**	Право изменять собственные настройки учетной записи администратора.	Администрирование → Конфигурация → Администраторы

* Права 1, 2, 8, 12 определяются для станции по списку групп, в которые она входит, а не по первичной группе станции.

Если станция входит в группу, и для этой группы назначены какие-либо из этих прав, то администратору будет доступен функционал, соответствующий этим правам, независимо от того, является ли разрешенная группа первичной для станции. При этом разрешение является приоритетным: если станция входит одновременно в разрешенную и запрещенную группы, администратору будет доступен функционал, соответствующий правам разрешенной группы.

Приложение Г. Система оповещения

Базовая информация по настройке оповещений администратора приведена в **Руководстве администратора**, в п. Настройка оповещений.

Г1. Описание параметров системы оповещения

Система оповещения о событиях, связанных с работой компонентов антивирусной сети, использует следующие типы отправки оповещений:

- оповещения по электронной почте,
- оповещения через Веб-консоль,
- оповещения через SNMP,
- оповещения через протокол Агента,
- Push-оповещения.

В зависимости от метода отправки оповещений требуются различные наборы параметров в виде ключ → значение. Для каждого метода задаются следующие параметры:

Таблица Г-1. Общие параметры

Параметр	Описание	Значение по умолчанию	Обязательный
`TO`	Множество адресатов оповещения, разделенных символом |		да
`ENABLED`	Включение или выключение оповещения	`true` или `false`	да
`_TIME_TO_LIVE`	Количество попыток повторной отправки оповещения в случае неудачи	10 попыток	нет
`_TRY_PERIOD`	Период в секундах между попытками повторной отправки оповещения	5 мин., (отправка не чаще раза в 5 мин.)	нет

Далее приведены таблицы со списками параметров для различных методов отправки оповещений.

Таблица Г-2. Оповещения по электронной почте

Параметр	Описание	Значение по умолчанию
FROM	Адрес ящика электронной почты отправителя	drwcsd@${имя хоста}
TO	Адреса ящиков электронной почты получателей	-
HOST	Адрес SMTP-сервера	127.0.0.1
PORT	Номер порта SMTP-сервера	• 25, если параметр SSL принимает значение no • 465, если параметр SSL принимает значение yes
USER	Пользователь SMTP-сервера	"" если задан, то требуется включение хотя бы одного метода авторизации, иначе почта не будет передана.
PASS	Пароль пользователя SMTP-сервера	""
STARTTLS	Для шифрованного обмена данными. При этом переключение на защищенное соединение осуществляется через команду STARTTLS. По умолчанию для соединения предусматривается использование 25 порта.	yes
SSL	Для шифрованного обмена данными. При этом будет открыто отдельное защищенное TLS-соединение. По умолчанию для соединения предусматривается использование 465 порта.	no
AUTH-CRAM-MD5	Использовать аутентификацию CRAM-MD5	no
AUTH-PLAIN	Использовать аутентификацию PLAIN	no
AUTH-LOGIN	Использовать аутентификацию LOGIN	no
AUTH-NTLM	Использовать аутентификацию NTLM	no
SSL-VERIFYCERT	Проверять корректность SSL-сертификата сервера	no

Параметр	Описание	Значение по умолчанию
DEBUG	Включить отладочный режим, например, для разбора ситуаций с невозможностью авторизации	-

Таблица Г-3. Оповещения через Веб-консоль

Параметр	Описание	Значение по умолчанию
TO	UUID администраторов, которым будет отправлено данное сообщение	-
SHOW_PERIOD	Время хранения сообщения в секундах, начиная с момента получения сообщения	86400 секунд, т. е. один день.

Таблица Г-4. Оповещения через SNMP

Параметр	Описание	Значение по умолчанию
TO	Принимающая сущность SNMP, например, IP-адрес	-
DOMAIN	Домен	• localhost для ОС Windows, • "" — для ОС семейства UNIX.
COMMUNITY	SNMP-общность или контекст	public
RETRIES	Количество повторных попыток отправки оповещения, предпринимаемых API	5 попыток
TIMEOUT	Время в секундах, после которого API предпримет повторную попытку отправки оповещения	5 секунд

Таблица Г-5. Оповещения через протокол Агента

Параметр	Описание	Значение по умолчанию
TO	UUID принимающих станций	-
SHOW_PERIOD	Время хранения сообщения в секундах, начиная с момента получения сообщения	86400 секунд, т. е. один день.

Таблица Г-6. Push-оповещения

Параметр	Описание	Значение по умолчанию
TO	Токены устройств, которые приложения получают при регистрации на сервере производителя, например Apple	-
SERVER_URL	URL relay сервера, через который оповещения пересылаются на сервер производителя	-

Г2. Параметры шаблонов оповещений

Тексты сообщений генерируются компонентом Сервера, именуемым процессором шаблонов, на основе файлов шаблонов.

Система оповещений по сети Windows функционирует только на ОС Windows с поддержкой сервиса Windows Messenger (Net Send).

ОС Windows Vista и более поздние версии не поддерживают сервис Windows Messenger.

Файл шаблона состоит из текста и переменных, заключенных в фигурные скобки. При редактировании файлов шаблонов можно использовать перечисленные ниже переменные.

Переменные записываются в одной из следующих форм:

- {<*VAR*>} — подставить непосредственно значение переменной <*VAR*>.
- {<*VAR*>:<*N*>} — первые <*N*> символов переменной <*VAR*>.
- {<*VAR*>:<*first*>:<*N*>} — <*N*> символов переменной <*VAR*>, следующих после <*first*> первых (начиная с <*first*>+1-го символа), если остаток меньше — дополняется пробелами справа.
- {<*VAR*>:<*first*>:-<*N*>} — <*N*> символов переменной <*VAR*>, следующих после <*first*> первых (начиная с <*first*>+1-го символа), если остаток меньше — дополняется пробелами слева.
- {<*VAR*>/<*original1*>/<*replace1*>[/<*original2*>/<*replace2*>]} — замена указанных символов переменной <*VAR*> на заданные значения: символы <*original1*> заменяются на символы <*replace1*>, при наличии символы <*original2*> заменяются на символы <*replace2*> и т. д.

  Количество пар подстановки не ограничено.
- {<*VAR*>/<*original1*>/<*replace1*[{<*SUB_VAR*>}]>[/<*original2*>/<*replace2*>]} — аналогично вышеописанным заменам на заданные значения, но с использованием

вложенной переменной <*SUB_VAR*>. Действия с вложенными переменными аналогичны всем действиям с родительскими переменными.

Глубина вложенности при рекурсивных подстановках не ограничена.

- {<*VAR*>/<*original1*>/<*replace1*>/<*original2*>/<*replace2*>/*/<*replace3*>} — аналогично вышеописанным заменам на заданные значения, но также допускается подстановка значения, заданного в <*replace3*>, если ни одно из перечисленных оригинальных значений не совпало. Также если в <*VAR*> не встретилось ни <*original1*>, ни <*original2*>, все значения будут заменены на <*replace3*>.

Таблица Г-7. Форма записи переменных

Переменная	Значение	Выражение	Результат
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35
SYS.TIME	10:35:17:456	{SYS.TIME:3:5}	35:17
SYS.TIME	10:35:17:456	{SYS.TIME:3:-12}	°°°35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:12}	35:17:456°°°
SYS.TIME	10:35:17:456	{SYS.TIME/10/99/35/77}	99:77:17:456

Условные обозначения

° — пробельный символ.

Переменные окружения

Для формирования текстов сообщений вы можете использовать переменные среды окружения процесса Сервера (пользователь **System**).

Переменные среды окружения доступны в редакторе сообщений Центра управления, в выпадающем списке **ENV**. Обратите внимание: переменные необходимо указывать с добавлением префикса `ENV.` (префикс заканчивается на точку).

Системные переменные

- `SYS.BRANCH` — версия Агентов и Сервера,
- `SYS.BUILD` — дата сборки Сервера,
- `SYS.DATE` — текущая системная дата,
- `SYS.DATETIME` — текущие системная дата и время,
- `SYS.HOST` — DNS-имя Сервера,
- `SYS.MACHINE` — сетевой адрес компьютера с установленным Сервером,

- `SYS.OS` — название операционной системы на компьютере с установленным Сервером,
- `SYS.PLATFORM` — платформа Сервера,
- `SYS.PLATFORM.SHORT` — краткий вариант `SYS.PLATFORM`,
- `SYS.SERVER` — название продукта (Dr.Web Server),
- `SYS.TIME` — текущее системное время,
- `SYS.VERSION` — версия Сервера.

Общие переменные для станций

- `GEN.LoginTime` — время подключения станции,
- `GEN.StationAddress` — адрес станции,
- `GEN.StationDescription` — описание станции,
- `GEN.StationID` — уникальный идентификатор станции,
- `GEN.StationLDAPDN` — различающееся имя (distinguished name) станции под ОС Windows. Актуально для станций, входящих в ADS/LDAP-домен,
- `GEN.StationMAC` — MAC-адрес станции,
- `GEN.StationName` — название станции,
- `GEN.StationPrimaryGroupID` — идентификатор первичной группы станции,
- `GEN.StationPrimaryGroupName` — название первичной группы станции,
- `GEN.StationSID` — идентификатор безопасности станции.

Общие переменные для репозитория

- `GEN.CurrentRevision` — текущий идентификатор версии,
- `GEN.Folder` — каталог размещения продукта,
- `GEN.NextRevision` — идентификатор обновленной версии,
- `GEN.Product` — описание продукта.

Параметры и переменные оповещений по типам

Администраторы

Неизвестный администратор

Параметр	Значение
Причина отправки оповещения	Отправляется при попытке авторизации в Центре управления администратора с неизвестным регистрационным именем.

Параметр	Значение	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Login`	регистрационное имя
	`MSG.Address`	сетевой адрес Центра управления

Ошибка авторизации администратора

Параметр	Значение	
Причина отправки оповещения	Отправляется при неуспешной авторизации администратора в Центре управления. Причина ошибки авторизации приводится в тексте оповещения.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Login`	регистрационное имя
	`MSG.Address`	сетевой адрес Центра управления
	`MSG.LoginErrorCode`	числовой код ошибки

Другое

Зафиксировано большое количество аварийно завершенных соединений

Параметр	Значение	
Причина отправки оповещения	Отправляется при наличии большого количества аварийно завершеных соединений с клиентами: станциями, инсталляторами Агента, соседними Серверами, Прокси-серверами.	
Дополнительная настройка	Чтобы иметь возможность отправлять оповещения о множестве аварийно завершенных соединений, необходимо установить флаг **Аварийные завершения соединений** в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Статистика** и задать соответствующие параметры в том же разделе.	
Переменные	`MSG.Total`	количество прерванных соединений
	`MSG.AddrsCount`	количество адресов, с которыми были прерваны соединения

Зафиксировано большое количество блокировок Контролем приложений

Параметр	Значение	
Причина отправки оповещения	Отправляется при наличии большого количества заблокированных приложений на станциях компонентом Контроль приложений.	
Дополнительная настройка	Чтобы иметь возможность отправлять оповещения о большом количестве заблокированных приложений, необходимо установить флаг **Множественные блокировки Контролем приложений** в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Статистика** и задать соответствующие параметры в том же разделе.	
Переменные	`MSG.Total`	общее количество блокировок
	`MSG.Profile`	наиболее распространенные профили, по которым производилась блокировка

Ошибка записи журнала Сервера

Параметр	Значение	
Причина отправки оповещения	Отправляется при возникновении ошибки в процессе записи информации в журнал работы Сервера. Причина ошибки записи в журнал приводится в тексте оповещения.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Error`	текст ошибки

Ошибка ротации журнала Сервера

Параметр	Значение	
Причина отправки оповещения	Отправляется при возникновении ошибки в процессе ротации журнала работы Сервера. Причина ошибки ротации журнала приводится в тексте оповещения.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Error`	текст ошибки

Соседний Сервер давно не подключался

Параметр	Значение	
Причина отправки оповещения	Отправляется согласно заданию в расписании Сервера. Содержит информацию о том, что соседний Сервер давно не подключался к данному Серверу. Дата последнего подключения приводится в тексте оповещения.	
Дополнительная настройка	Длительность периода, в течение которого соседний Сервер должен не выходить на связь, чтобы было отправлено оповещение, задается в задании **Соседний сервер давно не подключался** в расписании Сервера, настраиваемом в разделе **Администрирование → Планировщик задач Сервера Dr.Web**.	
Переменные	`MSG.LastDisconnectTime`	время, когда Сервер был последний раз подключен
	`MSG.StationName`	название соседнего Сервера

Статистический отчет

Параметр	Значение	
Причина отправки оповещения	Отправляется после генерации периодического отчета согласно заданию в расписании Сервера. Также в оповещении приводится путь, по которому можно скачать файл отчета.	
Дополнительная настройка	Отчет создается согласно заданию **Создание статистического отчета** в расписании Сервера, настраиваемом в разделе **Администрирование → Планировщик задач Сервера Dr.Web**.	
Переменные	`MSG.Attachment`	путь к отчету
	`MSG.AttachmentType`	MIME-тип
	`GEN.File`	имя файла отчета

Суммарный отчет превентивной защиты

Параметр	Значение
Причина отправки оповещения	Отправляется при получении большого количества отчетов со станций сети от компонента Превентивная защита.
Дополнительная настройка	Чтобы отправлять единое оповещение об отчете от Превентивной защиты, необходимо установить флаг **Группировать отчеты Превентивной защиты** в разделе **Администрирование → Конфигурация Сервера Dr.Web → Статистика**. Параметры по

Параметр	Значение	
	группировке отчетов задаются в том же разделе.	
Переменные	MSG.AutoBlockedActCount	количество процессов с подозрительной активностью, заблокированных автоматически
	MSG.AutoBlockedProc	процесс с подозрительной активностью, заблокированный автоматически
	MSG.HipsType	тип защищаемого объекта
	MSG.IsShellGuard	разделение по типам реакции Превентивной защиты при автоматической блокировке: • блокировка неавторизованного кода • проверка доступа к защищаемым объектам
	MSG.ShellGuardType	наиболее часто встречающаяся причина блокировки исполнения неавторизованного кода при автоматической блокировке события
	MSG.Total	общее количество событий Превентивной защиты, зафиксированных в сети
	MSG.UserAllowedActCount	количество процессов с подозрительной активностью, разрешенных пользователем
	MSG.UserAllowedHipsType	тип наиболее часто защищаемых объектов, доступ к которым был разрешен пользователем
	MSG.UserAllowedIsShellGuard	разделение по типам реакции Превентивной защиты при разрешении доступа пользователем: • блокировка неавторизованного кода • проверка доступа к защищаемым объектам
	MSG.UserAllowedProc	процесс с подозрительной активностью, разрешенный

Параметр	Значение	
		пользователем
	MSG.UserAllowedShellGuard	наиболее часто встречающаяся причина блокировки исполнения неавторизованного кода при разрешении события пользователем
	MSG.UserBlockedActCount	количество процессов с подозрительной активностью, заблокированных пользователем
	MSG.UserBlockedHipsType	тип наиболее часто защищаемых объектов, доступ к которым был запрещен пользователем
	MSG.UserBlockedIsShellGuard	разделение по типам реакции Превентивной защиты при запрещении доступа пользователем: • блокировка неавторизованного кода • проверка доступа к защищаемым объектам
	MSG.UserBlockedProc	процесс с подозрительной активностью, заблокированный пользователем
	MSG.UserBlockedShellGuard	наиболее часто встречающаяся причина блокировки исполнения неавторизованного кода при блокировке события пользователем

Эпидемия в сети

Параметр	Значение
Причина отправки оповещения	Отправляется при обнаружении эпидемии в антивирусной сети. Это означает, что за заданный промежуток времени было обнаружено более чем заданное количество угроз в сети.
Дополнительная настройка	Чтобы отправлять оповещение об эпидемиях, необходимо установить флаг **Отслеживать эпидемии** в разделе **Администрирование → Конфигурация Сервера Dr.Web → Статистика**. Параметры по определению эпидемии задаются в том

Параметр	Значение	
	же разделе.	
Переменные	`MSG.Infected`	общее количество обнаруженных угроз
	`MSG.Virus`	наиболее распространенные угрозы

Лицензии

Достигнуто лицензионное ограничение по количеству станций в сети

Параметр	Значение	
Причина отправки оповещения	Отправляется, если при подключении станции к Серверу обнаружено, что количество станций в группе, в которую входит подключаемая станция, достигло ограничения в лицензионном ключе, назначенном для этой группы. При этом новая станция не может зарегистрироваться на Сервере.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.ID`	UUID станции
	`MSG.StationName`	название станции
	Также доступны общие переменные для станций, приведенные выше.	

Достигнуто ограничение по количеству переданных лицензий

Параметр	Значение	
Причина отправки оповещения	Отправляется, если для выдачи соседним Серверам было запрошено больше лицензий, чем доступно в лицензионном ключе.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.ObjId`	ID лицензионного ключа

Истек срок передачи лицензий

Параметр	Значение	
Причина отправки оповещения	Отправляется, если истек срок выдачи лицензий соседнему Серверу из лицензионного ключа данного Сервера.	
Дополнительная настройка	Срок выдачи лицензий соседним Серверам задается в разделе **Администрирование → Конфигурация Сервера Dr.Web → Лицензии**.	
Переменные	`MSG.ObjId`	ID лицензионного ключа
	`MSG.Server`	название соседнего Сервера

Количество станций в группе приближается к лицензионному ограничению

Параметр	Значение	
Причина отправки оповещения	Отправляется, если количество станций в группе приближается к лицензионному ограничению в ключе, назначенном для этой группы.	
Дополнительная настройка	Количество свободных лицензий, оставшихся в ключе, при котором отправляется оповещение: либо меньше трех лицензий, либо меньше 5% от общего числа лицензий в ключе.	
Переменные	`MSG.Free`	количество оставшихся свободных лицензий
	`MSG.Licensed`	количество станций, использующих лицензии данной группы
	`MSG.Total`	Общее количество лицензий по всем ключам, назначенным группе. Обратите внимание: лицензионные ключи группы могут быть также назначены на другие объекты лицензирования.
	`GEN.StationPrimaryGroupID`	ID первичной группы
	`GEN.StationPrimaryGroupName`	название первичной группы

Лицензионный ключ автоматически обновлен

Параметр	Значение	
Причина отправки оповещения	Отправляется, если лицензионный ключ был автоматически обновлен. При этом новый ключ успешно загружен и распространен на все объекты старого лицензионного ключа.	
Дополнительная настройка	Для подробной информации по автоматическому обновлению лицензий обратитесь к **Руководству администратора**, п. Автоматическое обновление лицензий.	
Переменные	`MSG.KeyId`	идентификатор старого лицензионного ключа
	`MSG.KeyName`	имя старого лицензионного ключа
	`MSG.NewKeyId`	идентификатор нового лицензионного ключа
	`MSG.NewKeyName`	имя нового лицензионного ключа

Лицензионный ключ заблокирован

Параметр	Значение	
Причина отправки оповещения	Отправляется, если при обновлении репозитория из Всемирной Системы Обновлений Dr.Web была получена информация о том, что лицензионный ключ был заблокирован. Дальнейшее использование этого ключа невозможно.	
Дополнительная настройка	Для получения подробной информации о причине блокировки обратитесь в службу технической поддержки.	
Переменные	`MSG.KeyId`	ID лицензионного ключа
	`MSG.KeyName`	имя пользователя лицензионного ключа

Лицензионный ключ не может быть автоматически обновлен

Параметр	Значение
Причина отправки оповещения	Отправляется, если лицензионный ключ не может быть автоматически обновлен, поскольку состав лицензируемых компонентов у текущего и нового ключей отличается. При этом новый ключ успешно загружен, но не распространен на все

Параметр	Значение	
	объекты старого лицензионного ключа. Необходимо заменить лицензионный ключ вручную.	
Дополнительная настройка	Для подробной информации по автоматическому обновлению лицензий обратитесь к **Руководству администратора**, п. Автоматическое обновление лицензий.	
Переменные	`MSG.ExpirationDate`	дата окончания лицензии
	`MSG.Expired`	• 1 — срок окончания уже наступил • 0 — срок окончания еще не наступил
	`MSG.KeyDifference`	Причина, по которой автоматическая замена ключа невозможна: • 1 — состав лицензируемых компонентов у текущего и нового лицензионных ключей отличается • 2 — у нового лицензионного ключа меньше лицензий, чем у текущего лицензионного ключа
	`MSG.KeyId`	идентификатор старого лицензионного ключа
	`MSG.KeyName`	имя старого лицензионного ключа
	`MSG.NewKeyId`	идентификатор нового лицензионного ключа
	`MSG.NewKeyName`	имя нового лицензионного ключа

Ограничение по количеству лицензий в лицензионном ключе

Параметр	Значение	
Причина отправки оповещения	Отправляется, если при включении Сервера обнаружено, что количество станций в некоторой группе уже превысило количество лицензий в лицензионном ключе, назначенном для этой группы.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.KeyId`	ID лицензионного ключа

Параметр	Значение	
	MSG.KeyName	имя пользователя лицензионного ключа
	MSG.Licensed	количество разрешенных лицензией
	MSG.LicenseLimit	состояние лицензий: • 1 — количество свободных лицензий в лицензионном ключе близко к окончанию, • 2 — количество свободных лицензий в лицензионном ключе закончилось, • 3 — лицензионный ключ был назначен на большее количество объектов, чем разрешено в данном ключе.
	MSG.Licensed	количество объектов, для которых был назначен ключ
	MSG.Total	количество лицензий в ключе

Окончание срока действия лицензионного ключа

Параметр	Значение	
Причина отправки оповещения	Отправляется, если приближается окончание срока действия лицензионного ключа, а автоматическое обновление лицензии недоступно.	
Дополнительная настройка	Не требуется.	
Переменные	MSG.ExpirationDate	дата окончания лицензии
	MSG.Expired	• 1 — срок окончания уже наступил • 0 — срок окончания еще не наступил
	MSG.KeyId	идентификатор лицензионного ключа
	MSG.KeyName	имя лицензионного ключа

Новички

Для сообщений данной группы также доступны общие переменные для станций, приведенные выше.

Станция ожидает подтверждения

Параметр	Значение
Причина отправки оповещения	Отправляется, если новая станция запросила подключение к Серверу, и администратору требуется вручную подтвердить или отказать станции в доступе.
Дополнительная настройка	Ситуация может возникнуть, если в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Общие** для настройки **Режим регистрации новичков** установлено значение **Подтверждать доступ вручную**.
Переменные	Отсутствуют.

Станция отклонена автоматически

Параметр	Значение
Причина отправки оповещения	Отправляется, если новая станция запросила подключение к Серверу и была отклонена Сервером автоматически.
Дополнительная настройка	Ситуация может возникнуть, если в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Общие** для настройки **Режим регистрации новичков** установлено значение **Всегда отказывать в доступе**.
Переменные	Отсутствуют.

Станция отклонена администратором

Параметр	Значение
Причина отправки оповещения	Отправляется, если новая станция запросила подключение к Серверу и была отклонена администратором вручную.
Дополнительная настройка	Ситуация может возникнуть, если в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Общие** для настройки **Режим регистрации новичков** установлено значение **Подтверждать доступ вручную**, и администратор выбрал для станции вариант **Антивирусная сеть** → **Неподтвержденные станции** → **Отказать в доступе выбранным станциям**.

Параметр	Значение	
Переменные	`MSG.AdminAddress`	сетевой адрес Центра управления
	`MSG.AdminName`	имя администратора

Репозиторий

Для сообщений данной группы также доступны общие переменные для репозитория, приведенные выше.

Актуальное состояние продукта в репозитории

Параметр	Значение
Причина отправки оповещения	Отправляется, если при проверке обновлений репозитория было обнаружено, что запрашиваемый продукт находится в актуальном состоянии. Обновление этого продукта с ВСО при этом не требуется.
Дополнительная настройка	Не требуется.
Переменные	Отсутствуют.

Переменные шаблона **Актуальное состояние продукта в репозитории** не включают файлы, помеченные как **игнорируемые при оповещениях** в конфигурационном файле продукта, см. E1. Синтаксис файла конфигурации .config.

Запущено обновление продукта репозитория

Параметр	Значение
Причина отправки оповещения	Отправляется, если при проверке обновлений репозитория было обнаружено, что для запрашиваемых продуктов требуется обновление. При этом запускается обновление с ВСО.
Дополнительная настройка	Не требуется.
Переменные	Отсутствуют.

Недостаточно свободного места на диске

Параметр	Значение
Причина отправки оповещения	Отправляется, если на диске, на котором расположен каталог Сервера `var` с динамическими данными, заканчивается свободное

Параметр	Значение	
	место.	
Дополнительная настройка	Нехватка места на диске определяется, если осталось меньше 315 МБ или меньше 1000 нодов (для ОС семейства UNIX), если эти значения не переопределены переменными окружения.	
Переменные	Общие переменные для репозитория, приведенные выше, недоступны.	
	`MSG.FreeInodes`	число свободных файловых дескрипторов inodes (имеет смысл только для некоторых систем семейства UNIX)
	`MSG.FreeSpace`	свободное место в байтах
	`MSG.Path`	путь к каталогу с малым объемом памяти
	`MSG.RequiredInodes`	необходимое для работы число свободных inodes (имеет смысл только для некоторых систем семейства UNIX)
	`MSG.RequiredSpace`	необходимый для работы объем свободной памяти

Обновление продукта в репозитории заморожено

Параметр	Значение
Причина отправки оповещения	Отправляется, если продукт в репозитории был заморожен администратором. Обновление продукта с ВСО при этом не осуществляется.
Дополнительная настройка	Управлением продуктами репозитория, в том числе заморозкой и снятием заморозки, осуществляется в разделе **Администрирование** → **Детальная конфигурация репозитория**.
Переменные	Отсутствуют.

Обновление репозитория уже запущено

Параметр	Значение
Причина отправки оповещения	Отправляется, если в процессе обновления Сервера было повторно запущено обновление.

Параметр	Значение
Дополнительная настройка	Не требуется.
Переменные	Отсутствуют.

Ошибка обновления репозитория

Параметр	Значение	
Причина отправки оповещения	Отправляется, если при обновлении с ВСО репозитория или какого-либо из продуктов репозитория произошла ошибка. Конкретная причина ошибки, а также название продукта при ошибке обновления продукта, приводятся в тексте оповещения.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Error`	сообщение об ошибке
	`MSG.ExtendedError`	подробное описание ошибки

Продукт в репозитории обновлен

Сообщение	Значение	
Причина отправки оповещения	Отправляется при удачном обновлении репозитория с ВСО.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Added`	список добавленных файлов (каждое наименование на отдельной строке)
	`MSG.AddedCount`	количество добавленных файлов
	`MSG.Deleted`	список удаленных файлов (каждое наименование на отдельной строке)
	`MSG.DeletedCount`	количество удаленных файлов
	`MSG.Replaced`	список замененных файлов (каждое наименование на отдельной строке)
	`MSG.ReplacedCount`	количество замененных файлов

Станции

Для сообщений данной группы также доступны общие переменные для станций, приведенные выше.

В многосерверной сети возможно получение оповещений о событиях на станциях соседних Серверов. Включение данной опции осуществляется при настройке связей с соседними Серверами (см. **Руководство администратора**, раздел Настройка связей между Серверами Dr.Web).

О событиях на соседнем Сервере доступны следующие оповещения: **Обнаружена угроза безопасности**, **Отчет превентивной защиты**, **Ошибка сканирования**, **Статистика сканирования**.

Аварийное завершение соединения

Параметр	Значение	
Причина отправки оповещения	Отправляется при аварийном завершении соединения с клиентом: станцией, инсталлятором Агента, соседним Сервером, Прокси-сервером.	
Дополнительная настройка	Чтобы иметь возможность отправлять оповещения об аварийно завершенных соединениях, необходимо установить флаг **Аварийные завершения соединений** в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Статистика** и задать соответствующие параметры в том же разделе.	
Переменные	`MSG.Total`	количество прерванных соединений
	`MSG.Type`	тип клиента

Контроль приложений заблокировал процесс

Параметр	Значение	
Причина отправки оповещения	Отправляется, если компонентом Контроль приложений было заблокировано приложение на станции.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.AppCtlAction`	примененное действие: • 0 — неизвестно, • 2 — заблокирован, • 3 — заблокирован (не найден в

Параметр	Значение	
		списке доверенных приложений), • 5 — заблокирован запрещающими правилами, • 7 — заблокирован настройками политик.
	MSG.AppCtlType	тип события: • 0 — неизвестен, • 1 — запуск процесса, • 2 — запуск хост-процесса, • 3 — запуск скриптового интерпретатора, • 4 — загрузка модуля, • 5 — загрузка драйвера, • 6 — запуск MSI-установщика, • 7 — создание нового исполняемого файла на диске, • 8 — модификация исполняемого файла на диске.
	MSG.Path	путь к заблокированному процессу
	MSG.Profile	название профиля, по которому произведена блокировка
	MSG.Rule	название правила, по которому произведена блокировка
	MSG.SHA256	хеш заблокированного процесса (SHA-256)
	MSG.StationTime	время на станции, когда процесс был заблокирован
	MSG.Target	путь к заблокированному скрипту в случае хост-процесса
	MSG.TargetSHA256	хеш заблокированного скрипта в случае с хост-процессом (SHA-256)
	MSG.TestMode	включен ли тестовый режим
	MSG.User	пользователь, от имени которого запускался заблокированный объект

Контроль приложений заблокировал процесс из списка известных хешей угроз

Параметр	Значение	
Причина отправки оповещения	Отправляется, если на станции было заблокировано приложение из списка известных хешей угроз компонентом Контроль приложений.	
Дополнительная настройка	Оповещение об обнаружении по списку известных хешей возможно, только если лицензировано использование бюллетеней известных хешей угроз (достаточно лицензии хотя бы в одном из лицензионных ключей, используемых Сервером). Наличие лицензии приводится в информации по лицензионному ключу, которую можно просмотреть в разделе **Менеджер лицензий**, параметр **Разрешенные списки бюллетеней хешей** (если функционал не лицензирован, данный параметр отсутствует).	
Переменные	`MSG.AppCtlAction`	примененное действие: • 0 — неизвестно, • 2 — заблокирован, • 3 — заблокирован (не найден в списке доверенных приложений), • 5 — заблокирован запрещающими правилами, • 7 — заблокирован настройками политик.
	`MSG.AppCtlType`	тип события: • 0 — неизвестен, • 1 — запуск процесса, • 2 — запуск хост-процесса, • 3 — запуск скриптового интерпретатора, • 4 — загрузка модуля, • 5 — загрузка драйвера, • 6 — запуск MSI-установщика, • 7 — создание нового исполняемого файла на диске, • 8 — модификация исполняемого файла на диске.
	`MSG.Document`	бюллетень, содержащий хеш
	`MSG.Path`	путь к заблокированному процессу

Параметр	Значение	
	MSG.Profile	название профиля, по которому произведена блокировка
	MSG.Rule	название правила, по которому произведена блокировка
	MSG.SHA256	хеш заблокированного процесса (SHA-256)
	MSG.StationTime	время на станции, когда процесс был заблокирован
	MSG.Target	путь к заблокированному скрипту в случае хост-процесса
	MSG.TargetSHA256	хеш заблокированного скрипта в случае с хост-процессом (SHA-256)
	MSG.TestMode	включен ли тестовый режим
	MSG.User	пользователь, от имени которого запускался заблокированный объект

Критическая ошибка обновления станции

Параметр	Значение	
Причина отправки оповещения	Отправляется, если со станции получено оповещении об ошибке в процессе обновления антивирусных компонентов с Сервера.	
Дополнительная настройка	Не требуется.	
Переменные	MSG.Product	обновляемый продукт
	MSG.ServerTime	местное время получения сообщения Сервером

Неизвестная станция

Параметр	Значение
Причина отправки оповещения	Отправляется, если новая станция запросила подключение к Серверу, но была не допущена до рассмотрения подтверждения или отказа в регистрации.
Дополнительная настройка	Не требуется.

Параметр	Значение	
Переменные	`MSG.ID`	UUID неизвестной станции
	`MSG.Rejected`	значения: • `rejected` — станции отказано в доступе • `newbie` — сделана попытка перевести станцию в состояние "новичок"
	`MSG.StationName`	название станции

Обнаружена угроза безопасности

Параметр	Значение	
Причина отправки оповещения	Отправляется, если со станции получено оповещении об обнаружении угроз. В оповещении администратору также приводится подробная информация об обнаруженных угрозах.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Action`	действие, предпринятое при обнаружении
	`MSG.Component`	имя компонента
	`MSG.InfectionType`	тип угрозы
	`MSG.ObjectName`	имя инфицированного объекта
	`MSG.ObjectOwner`	владелец инфицированного объекта
	`MSG.RunBy`	пользователь, от имени которого запущен компонент
	`MSG.ServerTime`	время получения события, GMT
	`MSG.Virus`	имя угрозы
	`GEN.ServerRecvLinkID`	UUID последнего соседнего Сервера, от которого было получено данное сообщение об обнаруженной угрозе на подключенных к нему станциях (пустое значение, если обнаружена угроза на станциях, подключенных к данному Серверу)

Параметр	Значение	
	GEN.ServerRecvLinkName	название последнего соседнего Сервера, от которого было получено сообщение об обнаруженной угрозе на подключенных к нему станциях (пустое значение, если обнаружена угроза на станциях, подключенных к данному Серверу)
	GEN.ServerOriginatorID	UUID Сервера, к которому подключена станция, на которой обнаружена угроза
	GEN.ServerOriginatorName	название Сервера, к которому подключена станция, на которой обнаружена угроза

Обнаружена угроза безопасности по известным хешам угроз

Параметр	Значение	
Причина отправки оповещения	Отправляется, если со станции получено оповещении об обнаружении угроз из списка известных хешей угроз. В оповещении администратору также приводится подробная информация об обнаруженных угрозах.	
Дополнительная настройка	Оповещение об обнаружении по списку известных хешей возможно, только если лицензировано использование бюллетеней известных хешей угроз (достаточно лицензии хотя бы в одном из лицензионных ключей, используемых Сервером). Наличие лицензии приводится в информации по лицензионному ключу, которую можно просмотреть в разделе **Менеджер лицензий**, параметр **Разрешенные списки бюллетеней хешей** (если функционал не лицензирован, данный параметр отсутствует).	
Переменные	MSG.Action	действие, предпринятое при обнаружении
	MSG.Component	имя компонента
	MSG.Document	бюллетень, содержащий хеш обнаруженной угрозы
	MSG.InfectionType	тип угрозы
	MSG.ObjectName	имя инфицированного объекта
	MSG.ObjectOwner	владелец инфицированного

Параметр	Значение	
		объекта
	MSG.RunBy	пользователь, от имени которого запущен компонент
	MSG.SHA1	хеш SHA-1 обнаруженного объекта
	MSG.SHA256	хеш SHA-256 обнаруженного объекта
	MSG.ServerTime	время получения события, GMT
	MSG.Virus	имя угрозы
	GEN.ServerRecvLinkID	UUID последнего соседнего Сервера, от которого было получено данное сообщение об обнаруженной угрозе на подключенных к нему станциях (пустое значение, если обнаружена угроза на станциях, подключенных к данному Серверу)
	GEN.ServerRecvLinkName	название последнего соседнего Сервера, от которого было получено сообщение об обнаруженной угрозе на подключенных к нему станциях (пустое значение, если обнаружена угроза на станциях, подключенных к данному Серверу)
	GEN.ServerOriginatorID	UUID Сервера, к которому подключена станция, на которой обнаружена угроза
	GEN.ServerOriginatorName	название Сервера, к которому подключена станция, на которой обнаружена угроза

Отчет Превентивной защиты

Параметр	Значение
Причина отправки оповещения	Отправляется при получении отчета от компонента Превентивная защита со станции этого или соседнего Сервера.

Параметр	Значение	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.AdminName`	администратор, инициировавший действие над подозрительным процессом
	`MSG.Denied`	действие, произведенное над подозрительным процессом: • запрещен • разрешен
	`MSG.HipsType`	тип защищаемого объекта
	`MSG.IsShellGuard`	разделение по типам реакции Превентивной защиты: • блокировка неавторизованного кода • проверка доступа к защищаемым объектам
	`MSG.Path`	путь к процессу с подозрительной активностью
	`MSG.Pid`	идентификатор процесса с подозрительной активностью
	`MSG.ShellGuardType`	причина блокировки исполнения неавторизованного кода
	`MSG.StationTime`	время появления события на станции
	`MSG.Target`	путь к защищаемому объекту, к которому была осуществлена попытка доступа
	`MSG.Total`	количество запретов в случае автоматической реакции Превентивной защиты
	`MSG.User`	пользователь, от имени которого был запущен процесс с подозрительной активностью
	`MSG.UserAction`	инициатор действия над подозрительным процессом: • пользователь • автоматическая реакция Превентивной защиты

Параметр	Значение	
	GEN.ServerRecvLinkID	UUID последнего соседнего Сервера, от которого был получен отчет Превентивной защиты с подключенных к нему станций (пустое значение, если получен отчет со станций, подключенных к данному Серверу)
	GEN.ServerRecvLinkName	название последнего соседнего Сервера, от которого был получен отчет Превентивной защиты с подключенных к нему станций (пустое значение, если получен отчет со станций, подключенных к данному Серверу)
	GEN.ServerOriginatorID	UUID Сервера, к которому подключена станция, с которой получен отчет Превентивной защиты
	GEN.ServerOriginatorName	название Сервера, к которому подключена станция, с которой получен отчет Превентивной защиты

Отчет Превентивной защиты об обнаружении угроз по известным хешам угроз

Параметр	Значение	
Причина отправки оповещения	Отправляется при получении отчета от компонента Превентивная защита со станции этого или соседнего Сервера при обнаружении угроз из списка известных хешей угроз.	
Дополнительная настройка	Оповещение об обнаружении по списку известных хешей возможно, только если лицензировано использование бюллетеней известных хешей угроз (достаточно лицензии хотя бы в одном из лицензионных ключей, используемых Сервером). Наличие лицензии приводится в информации по лицензионному ключу, которую можно просмотреть в разделе **Менеджер лицензий**, параметр **Разрешенные списки бюллетеней хешей** (если функционал не лицензирован, данный параметр отсутствует).	
Переменные	MSG.AdminName	администратор, инициировавший действие над подозрительным процессом

Параметр	Значение	
	MSG.Denied	действие, произведенное над подозрительным процессом: • запрещен • разрешен
	MSG.Document	бюллетень, содержащий хеш обнаруженной угрозы
	MSG.HipsType	тип защищаемого объекта
	MSG.IsShellGuard	разделение по типам реакции Превентивной защиты: • блокировка неавторизованного кода • проверка доступа к защищаемым объектам
	MSG.Path	путь к процессу с подозрительной активностью
	MSG.Pid	идентификатор процесса с подозрительной активностью
	MSG.SHA1	хеш SHA-1 обнаруженного объекта
	MSG.SHA256	хеш SHA-256 обнаруженного объекта
	MSG.ShellGuardType	причина блокировки исполнения неавторизованного кода
	MSG.StationTime	время появления события на станции
	MSG.Target	путь к защищаемому объекту, к которому была осуществлена попытка доступа
	MSG.Total	количество запретов в случае автоматической реакции Превентивной защиты
	MSG.User	пользователь, от имени которого был запущен процесс с подозрительной активностью
	MSG.UserAction	инициатор действия над подозрительным процессом:

Параметр	Значение	
		• пользователь • автоматическая реакция Превентивной защиты
	GEN.ServerRecvLinkID	UUID последнего соседнего Сервера, от которого был получен отчет Превентивной защиты с подключенных к нему станций (пустое значение, если получен отчет со станций, подключенных к данному Серверу)
	GEN.ServerRecvLinkName	название последнего соседнего Сервера, от которого был получен отчет Превентивной защиты с подключенных к нему станций (пустое значение, если получен отчет со станций, подключенных к данному Серверу)
	GEN.ServerOriginatorID	UUID Сервера, к которому подключена станция, с которой получен отчет Превентивной защиты
	GEN.ServerOriginatorName	название Сервера, к которому подключена станция, с которой получен отчет Превентивной защиты

Ошибка авторизации станции

Параметр	Значение	
Причина отправки оповещения	Отправляется, если при попытке подключения к Серверу станция предоставила неверные учетные данные. Дальнейшие действия, зависящие от политики подключения станций, также приводятся в оповещении.	
Дополнительная настройка	Политика подключения станций задается в настройке **Режим регистрации новичков** раздела **Администрирование** → **Конфигурация Сервера Dr.Web** → **Общие**.	
Переменные	MSG.ID	UUID станции
	MSG.Rejected	значения: • rejected — станции отказано

Параметр	Значение	
		в доступе • `newbie` — сделана попытка перевести станцию в состояние "новичок"
	`MSG.StationName`	название станции

Ошибка сканирования

Параметр	Значение	
Причина отправки оповещения	Отправляется, если со станции получено оповещение об ошибке, возникшей при сканировании.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Component`	имя компонента
	`MSG.Error`	сообщение об ошибке
	`MSG.ObjectName`	имя объекта
	`MSG.ObjectOwner`	владелец объекта
	`MSG.RunBy`	пользователь, от имени которого запущен компонент
	`MSG.ServerTime`	время получения события, GMT
	`GEN.ServerRecvLinkID`	UUID последнего соседнего Сервера, от которого была получена информация об ошибке при сканировании подключенных к нему станций (пустое значение, если ошибка сканирования произошла на станциях, подключенных к данному Серверу)
	`GEN.ServerRecvLinkName`	название последнего соседнего Сервера, от которого была получена информация об ошибке при сканировании подключенных к нему станций (пустое значение, если ошибка сканирования произошла на станциях, подключенных к данному Серверу)
	`GEN.ServerOriginatorID`	UUID Сервера, к которому подключена станция, на которой произошла ошибка сканирования

Параметр	Значение	
	GEN.ServerOriginatorName	название Сервера, к которому подключена станция, на которой произошла ошибка сканирования

Ошибка сканирования при обнаружении угрозы по известным хешам угроз

Параметр	Значение	
Причина отправки оповещения	Отправляется, если произошла ошибка сканирования при обнаружении угрозы из списка известных хешей угроз.	
Дополнительная настройка	Оповещение об обнаружении по списку известных хешей возможно, только если лицензировано использование бюллетеней известных хешей угроз (достаточно лицензии хотя бы в одном из лицензионных ключей, используемых Сервером). Наличие лицензии приводится в информации по лицензионному ключу, которую можно просмотреть в разделе **Менеджер лицензий**, параметр **Разрешенные списки бюллетеней хешей** (если функционал не лицензирован, данный параметр отсутствует).	
Переменные	MSG.Component	имя компонента
	MSG.Document	бюллетень, содержащий хеш обнаруженной угрозы
	MSG.Error	сообщение об ошибке
	MSG.ObjectName	имя объекта
	MSG.ObjectOwner	владелец объекта
	MSG.RunBy	пользователь, от имени которого запущен компонент
	MSG.SHA1	хеш SHA-1 обнаруженного объекта
	MSG.SHA256	хеш SHA-256 обнаруженного объекта
	MSG.ServerTime	время получения события, GMT
	GEN.ServerRecvLinkID	UUID последнего соседнего Сервера, от которого была получена информация об ошибке при сканировании подключенных к нему станций (пустое значение, если ошибка сканирования произошла на станциях,

Параметр	Значение	
		подключенных к данному Серверу)
	GEN.ServerRecvLinkName	название последнего соседнего Сервера, от которого была получена информация об ошибке при сканировании подключенных к нему станций (пустое значение, если ошибка сканирования произошла на станциях, подключенных к данному Серверу)
	GEN.ServerOriginatorID	UUID Сервера, к которому подключена станция, на которой произошла ошибка сканирования
	GEN.ServerOriginatorName	название Сервера, к которому подключена станция, на которой произошла ошибка сканирования

Ошибка создания учетной записи станции

Параметр	Значение	
Причина отправки оповещения	Отправляется, если невозможно создать новую учетную запись станции на Сервере. Подробности об ошибке приводятся в файле журнала Сервера.	
Дополнительная настройка	Не требуется.	
Переменные	MSG.ID	UUID станции
	MSG.StationName	название станции

Станция давно не подключалась к Серверу

Параметр	Значение
Причина отправки оповещения	Отправляется согласно заданию в расписании Сервера. Содержит информацию о том, что станция давно не подключался к данному Серверу. Дата последнего подключения приводится в тексте оповещения.
Дополнительная настройка	Длительность периода, в течение которого станция должна не выходить на связь, чтобы было отправлено оповещение, задается в задании **Станция давно не подключалась** в расписании Сервера, настраиваемом в разделе **Администрирование** → **Планировщик задач Сервера Dr.Web**.

Параметр	Значение	
Переменные	Общие переменные для станций, приведенные выше, недоступны.	
	`MSG.DaysAgo`	количество дней с момента последнего подключения к Серверу
	`MSG.LastSeenFrom`	адрес, с которого станция в последний раз подключалась к Серверу
	`MSG.StationDescription`	описание станции
	`MSG.StationID`	UUID станции
	`MSG.StationMAC`	MAC-адрес станции
	`MSG.StationName`	название станции
	`MSG.StationSID`	идентификатор безопасности станции

Станция подтверждена автоматически

Параметр	Значение
Причина отправки оповещения	Отправляется, если новая станция подала запрос на подключение к Серверу и была подтверждена Сервером автоматически.
Дополнительная настройка	Ситуация может возникнуть, если в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Общие** для настройки **Режим регистрации новичков** установлено значение **Автоматически разрешить доступ**.
Переменные	Отсутствуют.

Станция подтверждена администратором

Параметр	Значение
Причина отправки оповещения	Отправляется, если новая станция подала запрос на подключение к Серверу и была подтверждена администратором вручную.
Дополнительная настройка	Ситуация может возникнуть, если в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Общие** для настройки **Режим регистрации новичков** установлено значение **Подтверждать доступ вручную**, и администратор выбрал для станции вариант **Антивирусная сеть** → **Неподтвержденные станции** → **Разрешить доступ выбранным станциям и**

Параметр	Значение	
	назначить первичную группу.	
Переменные	`MSG.AdminAddress`	сетевой адрес Центра управления
	`MSG.AdminName`	имя администратора

Станция уже зарегистрирована

Параметр	Значение	
Причина отправки оповещения	Отправляется, если к Серверу пытается подключиться станция с идентификатором, который совпадает с идентификатором станции уже подключенной к данному Серверу.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.ID`	UUID станции
	`MSG.Server`	ID Сервера, на котором станция зарегистрирована
	`MSG.StationName`	название станции

Статистика сканирования

Параметр	Значение	
Причина отправки оповещения	Отправляется, если со станции получено оповещении о завершении сканирования. В оповещении администратора также приводится краткая статистика сканирования.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Component`	имя компонента, проводившего сканирование
	`MSG.Cured`	количество вылеченных объектов
	`MSG.DeletedObjs`	количество удаленных объектов
	`MSG.Errors`	количество ошибок сканирования
	`MSG.Infected`	количество инфицированных объектов
	`MSG.Locked`	количество заблокированных объектов

Параметр	Значение	
	MSG.Modifications	количество объектов, инфицированных модификациями вирусов
	MSG.Moved	количество объектов, перемещенных в карантин
	MSG.Renamed	количество переименованных объектов
	MSG.RunBy	пользователь, от имени которого запущен компонент
	MSG.Scanned	количество просканированных объектов
	MSG.ServerTime	время получения события, GMT
	MSG.Speed	скорость обработки в КБ/с
	MSG.Suspicious	количество подозрительных объектов
	MSG.VirusActivity	
	GEN.ServerRecvLinkID	UUID последнего соседнего Сервера, от которого была получена статистика сканирования подключенных к нему станций (пустое значение, если получена статистика со станций, подключенных к данному Серверу)
	GEN.ServerRecvLinkName	название последнего соседнего Сервера, от которого была получена статистика сканирования подключенных к нему станций (пустое значение, если получена статистика со станций, подключенных к данному Серверу)
	GEN.ServerOriginatorID	UUID Сервера, к которому подключена станция, с которой получена статистика сканирования
	GEN.ServerOriginatorName	название Сервера, к которому подключена станция, с которой получена статистика сканирования

Требуется перезагрузка станции

Параметр	Значение	
Причина отправки оповещения	Отправляется, если требуется перезагрузка станции по одной из следующих причин: • для завершения лечения, • для применения обновлений, • для изменения состояния аппаратной виртуализации, • для завершения лечения и применения обновлений, • для завершения лечения и изменения состояния, аппаратной виртуализации, • для применения обновлений и изменения состояния аппаратной виртуализации, • для завершения лечения, применения обновлений и изменения состояния аппаратной виртуализации.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Reason`	причина перезагрузки список возможных причин приведен в предустановленном шаблоне

Требуется перезагрузка станции для применения обновлений

Параметр	Значение	
Причина отправки оповещения	Отправляется, если со станции получено оповещение о том, что продукт был установлен или обновлен, и требуется перезагрузка станции.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Product`	обновляемый продукт
	`MSG.ServerTime`	местное время получения сообщения Сервером

Устройство заблокировано

Параметр	Значение
Причина отправки оповещения	Отправляется, если со станции получено оповещение о том, что какое-либо из подключаемых к станции устройств было заблокировано антивирусным компонентом Dr.Web.

Параметр	Значение	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Capabilities`	характеристики устройства
	`MSG.Class`	класс устройства (название родительской группы)
	`MSG.Description`	описание устройства
	`MSG.FriendlyName`	понятное имя устройства
	`MSG.InstanceId`	идентификатор экземпляра устройства
	`MSG.User`	имя пользователя

Установки

Для сообщений данной группы также доступны общие переменные для станций, приведенные выше.

Установка на станции не выполнена

Параметр	Значение	
Причина отправки оповещения	Отправляется в случае возникновения ошибки при установке Агента на станцию. Конкретная причина ошибки приводится в тексте оповещения.	
Дополнительная настройка	Не требуется.	
Переменные	`MSG.Error`	сообщение об ошибке

Установка на станции успешно завершена

Параметр	Значение
Причина отправки оповещения	Отправляется в случае успешной установки Агента на станцию.
Дополнительная настройка	Не требуется.
Переменные	Отсутствуют.

Приложение Д. Спецификация сетевого адреса

В данной спецификации приняты следующие обозначения:

- переменные (поля, подлежащие замене на конкретные значения) заключаются в угловые скобки и пишутся курсивом,
- постоянный текст (сохраняющийся после подстановок) пишется моноширинным шрифтом,
- необязательные элементы заключаются в квадратные скобки,
- слева от последовательности символов `::=` располагается определяемое понятие, а справа — определение (как в форме Бэкуса-Наура).

Д1. Общий формат адреса

Сетевой адрес имеет следующий вид:

`[`*<protocol>*`://][`*<protocol-specific-part>*`]`

По умолчанию *<protocol>* имеет значение `TCP`. Значения по умолчанию *<protocol-specific-part>* определяются приложением.

Также допускается устаревший формат записи адресов:

`[`*<protocol>*`/][`*<protocol-specific-part>*`]`.

Адреса семейства IP

- *<interface>*`::=`*<ip-address>*

  <ip-address> может быть DNS-именем или IP-адресом, разделенным точками (например, `127.0.0.1`).

- *<socket-address>*`::=`*<interface>*`:`*<port-number>*

  <port-number> должен быть задан десятичным числом.

При задании адреса Сервера и адреса Агента существует возможность указать версию используемого протокола. Допускаются следующие варианты:

- *<protocol>*`://`*<interface>*`:`*<port-number>* — использовать IPv4 и IPv6.
- *<protocol>*`://(`*<interface>*`):`*<port-number>* — использовать только IPv4.
- *<protocol>*`://[`*<interface>*`]:`*<port-number>* — использовать только IPv6.

Например:

1. `tcp://127.0.0.1:2193`

   означает протокол `TCP`, порт `2193` на интерфейсе `127.0.0.1`.

2. `tcp://(examle.com):2193`

   означает протокол `TCP`, порт `2193` на IPv4-интерфейсе `example.com`.

3. `tcp://[::]:2193`

   означает протокол `TCP`, порт `2193` на IPv6-интерфейсе `0000.0000.0000.0000.0000.0000.0000.0000`

4. `localhost:2193`

   то же.

5. `tcp://:9999`

   значение для сервера: интерфейс по умолчанию, зависящий от приложения (обычно все доступные интерфейсы), порт `9999`; значение для клиента: связь с хостом по умолчанию, зависящим от приложения (обычно `localhost`), порт `9999`.

6. `tcp://`

   протокол TCP, порт по умолчанию.

Ориентированный на соединение протокол

<protocol>`://`*<socket-address>*

где *<socket-address>* задает локальный адрес сокета для сервера или удаленный сервер для клиента.

Ориентированный на датаграмму протокол

<protocol>`://`*<endpoint-socket-address>*`[-`*<interface>*`]`

Например:

1. `udp://231.0.0.1:2193`

   означает использование multicast-группы `231.0.0.1:2193` на зависящем от приложения интерфейсе по умолчанию.

2. `udp://[ff18::231.0.0.1]:2193`

   означает использование multicast-группы `[ff18::231.0.0.1]` на зависящем от приложения интерфейсе по умолчанию.

3. `udp://`

   зависящий от приложения интерфейс и конечная точка.

4. `udp://255.255.255.255:9999-myhost1`

   использование широковещательных сообщений на порт `9999` на интерфейсе `myhost1`.

Адреса семейства UDS

- Ориентированный на соединение протокол:

  `unx://`*<file_name>*

- Ориентированный на датаграмму протокол:

  `udx://<file_name>`

Например:

```
1. unx://tmp/drwcsd:stream
2. unx://tmp/drwcsd:datagram
```

Адреса семейства SRV

`srv://[<server name>][@<domain name/dot address>]`

Д2. Адреса Агента Dr.Web/ Инсталлятора

Прямое соединение с Сервером Dr.Web

`[<connection-protocol>]://[<remote-socket-address>]`

По умолчанию, в зависимости от <*connection-protocol*>:

- `tcp://127.0.0.1:2193`

  где `127.0.0.1` — loopback, `2193` — порт;
- `tcp://[::1]:2193`

  где `[::1]` — loopback (IPv6), `2193` — порт.

Поиск Сервера <drwcs-name>, использующий указанное семейство протоколов и конечную точку

`[<drwcs-name>]@<datagram-protocol>://[<endpoint-socket-address>[-<interface>]]`

По умолчанию, в зависимости от <*datagram-protocol*>:

- `drwcs@udp://231.0.0.1:2193-0.0.0.0`

  поиск Сервера с именем `drwcs` для TCP-соединения, использующего multicast-группу `231.0.0.1:2193` на всех интерфейсах.

Приложение Е. Управление репозиторием

Рекомендуется осуществлять управление репозиторием через соответствующие настройки Центра управления. Подробнее см. в **Руководстве администратора**, п. Управление репозиторием Сервера Dr.Web.

Настройки репозитория сохраняются в следующие файлы конфигурации репозитория:

- Общие файлы конфигурации расположены в корне каталога репозитория и задают параметры серверов обновлений.
- Файлы конфигурации продуктов расположены в корне каталогов, соответствующих конкретным продуктам репозитория, и задают состав файлов и настройки обновлений продукта, в каталоге которого они находятся.

После редактирования файлов конфигурации требуется перезапуск Сервера.

При настройке межсерверных связей (см. в **Руководстве администратора**, п. Особенности сети с несколькими Серверами) для зеркалирования продуктов следует иметь в виду, что конфигурационные файлы не являются частью продукта и не обрабатываются системой зеркалирования. Чтобы избежать сбоев в работе системы обновления:

- для равноправных Серверов сохраняйте конфигурацию идентичной,
- для подчиненных Серверов отключите синхронизацию компонентов по протоколу HTTP или сохраняйте конфигурацию идентичной.

Е1. Общие файлы конфигурации

.servers

Файл `.servers` содержит список серверов для обновления компонентов Dr.Web Enterprise Security Suite в репозитории Сервера Dr.Web с серверов ВСО.

Серверы в списке опрашиваются последовательно, при успехе обновления процедура опроса завершается.

Например:

```
esuite.geo.drweb.com

esuite.msk3.drweb.com

esuite.msk4.drweb.com
```

```
esuite.msk.drweb.com

esuite.us.drweb.com

esuite.jp.drweb.com
```

.url

Файл `.url` содержит базовый URI зоны обновления — каталога на серверах обновлений, содержащего обновления конкретного продукта Dr.Web.

Например:

```
update
```

.proto

Файл `.proto` содержит название протокола, по которому осуществляется получение обновлений с серверов обновлений.

Может принимать одно из следующих значений: `http | https | ftp | ftps | sftp | scp | smb | smbs | file`.

Протоколы `smb` и `smbs` доступны только для Серверов под ОС семейства UNIX.

Например:

```
https
```

.auth

Файл `.auth` содержит параметры авторизации пользователя на сервере обновлений.

Параметры авторизации задаются в следующем формате:

```
<имя пользователя>

<пароль>
```

Имя пользователя — обязательный параметр, пароль — опциональный.

Например:

```
admin

root
```

.delivery

Файл `.delivery` содержит настройки для передачи обновлений с серверов BCO.

Параметр	Возможные значения	Описание
`cdn`	`on` | `off`	Использование Content Delivery Network при загрузке репозитория: • `on` — использовать CDN, • `off` — не использовать CDN.
`cert`	`drweb` | `valid` | `any` | `custom`	Допустимые SSL-сертификаты серверов обновления, которые будут автоматически приниматься: • `drweb` — принимать только SSL-сертификат компании «Доктор Веб», • `valid` — принимать только действительные SSL-сертификаты, • `any` — принимать любые сертификаты, • `custom` — принимать сертификат, который указал пользователь.
`cert-path`		Путь к пользовательскому сертификату, если указан режим `custom` для параметра `cert`.
`ssh-mode`	`pwd` | `pubkey`	Режим авторизации при использовании протоколов `scp` и `sftp` (основаны на *ssh2*): • `pwd` — авторизация по регистрационному имени пользователя и паролю, • `pubkey` — авторизация по ключам шифрования.
`ssh-pubkey`		Путь к открытому ssh-ключу сервера обновлений.
`ssh-prikey`		Путь к закрытому ssh-ключу сервера обновлений.

Е2. Файлы конфигурации продуктов

.description

Файл .description задает имя продукта. Если файл отсутствует, в качестве имени продукта используется имя соответствующего каталога продукта.

Например:

```
Dr.Web Server
```

.sync-off

Файл отключает обновление продукта. Содержимое не имеет значения.

Файлы исключений при обновлении репозитория Сервера с ВСО

.sync-only

Файл .sync-only содержит регулярные выражения, определяющие список файлов репозитория, которые будут синхронизироваться при обновлении репозитория с ВСО. Файлы репозитория, не заданные в .sync-only, синхронизироваться не будут. Если файл .sync-only отсутствует, то будут синхронизироваться все файлы репозитория кроме файлов, исключенных согласно настройкам в файле .sync-ignore.

.sync-ignore

Файл .sync-ignore содержит в формате регулярных выражений список файлов репозитория, которые будут исключены из синхронизации при обновлении репозитория с ВСО.

Пример файла с исключениями

```
^windows-nt-x64/

^windows-nt/

^windows/
```

Порядок использования файлов конфигурации

Если для продукта присутствуют файлы `.sync-only` и `.sync-ignore`, используется следующая схема действий:

1. Сначала применяется `.sync-only`. Файлы, не перечисленные в `.sync-only`, не обрабатываются.
2. К оставшимся файлам применяется `.sync-ignore`.

Файлы исключений при обновлении Агентов с Сервера

.state-only

Файл `.state-only` содержит регулярные выражения, определяющие список файлов, которые будут синхронизироваться при обновлении Агентов с Сервера. Файлы репозитория, не заданные в `.state-only`, синхронизироваться не будут. Если файл `.state-only` отсутствует, то будет синхронизироваться все файлы репозитория кроме файлов репозитория, исключенных согласно настройкам в файле `.state-ignore`.

.state-ignore

Файл `.state-ignore` содержит регулярные выражения, определяющие список файлов, которые будут исключены из синхронизации при обновлении Агентов с Сервера.

Например:

- не требуется получать немецкий, китайский и испанский языки интерфейса (остальные — получать),
- не требуется получение компонентов, предназначенных для 64-битных ОС Windows.

```
;^common/ru-.*\.dwl$ это будет обновлено

^common/de-.*\.dwl$

^common/cn-.*\.dwl$

^common/es-.*\.dwl$

^win/de-.*

^win/cn-.*

^windows-nt-x64\.*
```

Очередность применения `.state-only` и `.state-ignore` аналогична `.sync-only` и `.sync-ignore`.

Настройки отправки оповещений

Файлы группы `notify` позволяют настроить систему оповещения при удачном обновлении соответствующих продуктов репозитория.

Данные настройки относятся только к оповещению **Продукт обновлен**. На остальные типы оповещений исключения не распространяются.

Настройки системы оповещения описаны в **Руководстве администратора**, п. Настройка оповещений.

.notify-only

Файл `.notify-only` содержит список файлов репозитория, при изменении которых отправляется оповещение.

.notify-ignore

Файл `.notify-ignore` содержит список файлов репозитория, при изменении которых не отправляются оповещения.

Порядок использования файлов конфигурации

Если для продукта присутствуют файлы `.notify-only` и `.notify-ignore`, используется следующая схема действий:

1. При обновлении продукта файлы, обновленные с ВСО, сравниваются со списками исключений.
2. Сначала исключаются файлы, включенные в список `.notify-ignore`.
3. Из оставшихся файлов исключаются файлы, не подпадающие в список `.notify-only`.
4. Если остались файлы, не исключенные на предыдущих шагах, то оповещения отправляются.

Если файлы `.notify-only` и `.notify-ignore` отсутствуют, то оповещения будут отправляться всегда (если они включены на странице **Настройки оповещений** в Центре управления).

Например:

Если в файле `.notify-ignore` задано исключение `^.vdb.lzma$`, то в случае, если обновились только файлы вирусных баз, оповещение отправлено не будет. Если помимо баз обновилось ядро `drweb32.dll`, то оповещение будет отправлено.

Настройки заморозки

.delay-config

Файл `.delay-config` содержит настройки запрета переключения продукта на новую ревизию. Репозиторий продолжает распространение предыдущей ревизии, синхронизация более не осуществляется (состояние продукта "замораживается"). Если администратор сочтет принятую ревизию пригодной для распространения, он должен разрешить ее распространение в Центре управления (см. **Руководство администратора**, п. Управление репозиторием Сервера Dr.Web).

Файл содержит два параметра, независимых от регистра и разделенных точкой с запятой.

Формат файла:

`Delay [ON|OFF]; UseFilter [YES|NO]`

Параметр	Возможные значения	Описание
`Delay`	`ON|OFF`	• `ON` — заморозка обновлений продукта включена. • `OFF` — заморозка обновлений продукта отключена.
`UseFilter`	`YES|NO`	• `Yes` — замораживать обновления только если обновленные файлы соответствуют списку исключений в файле `.delay-only`. • `No` — замораживать обновления в любом случае.

Например:

```
Delay ON; UseFilter NO
```

.delay-only

Файл `.delay-only` содержит список файлов, при изменении которых переключение продукта на новую ревизию запрещается. Список файлов задается в формате регулярных выражений.

Если файл из обновления репозитория совпадает с указанными масками, и настройка `UseFilter` в файле `.sync-only` включена, то ревизия будет заморожена.

.rev-to-keep

Файл `.rev-to-keep` содержит количество хранимых ревизий продукта.

Например:

```
3
```

Приложение Ж. Формат конфигурационных файлов

В данном разделе описывается формат следующих файлов:

Файл	Описание
drwcsd.conf	Конфигурационный файл Сервера Dr.Web.
webmin.conf	Конфигурационный файл Центра управления безопасностью Dr.Web.
download.conf	Конфигурационный файл для настройки загружаемых с Сервера данных.
drwcsd-proxy.conf	Конфигурационный файл Прокси-сервера Dr.Web.
drwreploader.conf	Конфигурационный файл Загрузчика репозитория.

Если на компьютере с соответствующим компонентом установлен Агент со включенной самозащитой, то перед изменением файлов конфигурации необходимо отключить компонент самозащиты Dr.Web Self-protection через настройки Агента.

После сохранения всех внесенных изменений рекомендуется включить компонент Dr.Web Self-protection.

Ж1. Конфигурационный файл Сервера Dr.Web

Конфигурационный файл Сервера Dr.Web `drwcsd.conf` по умолчанию располагается в подкаталоге `etc` корневого каталога Сервера. При запуске Сервера при помощи параметра командной строки может задаваться нестандартное расположение и наименование конфигурационного файла (подробнее см. Приложение 33. Сервер Dr.Web).

Чтобы вручную отредактировать конфигурационный файл Сервера Dr.Web

1. Остановите Сервер (см. в **Руководстве администратора** п. Запуск и останов Сервера Dr.Web).
2. Отключите самозащиту (в случае наличия на компьютере Агента с активной самозащитой — в контекстном меню Агента).
3. Внесите необходимые изменения в конфигурационный файл Сервера.
4. Запустите Сервер (см. в **Руководстве администратора** п. Запуск и останов Сервера Dr.Web).

Формат конфигурационного файла Сервера Dr.Web

Конфигурационный файл Сервера представлен в формате XML.

Описание параметров конфигурационного файла Сервера Dr.Web:

- `<version value="" />`

  Текущая версия конфигурационного файла.

- `<name value="" />`

  Название Сервера Dr.Web или кластера Серверов Dr.Web, по которому будут обращаться при поиске Агенты, инсталляторы Агентов или Центр управления. Оставьте значение параметра пустым ("" — используется по умолчанию), чтобы использовать имя компьютера, на котором установлен Сервер.

- `<id value="" />`

  Уникальный идентификатор Сервера. В предыдущих версиях содержался в лицензионном ключе Сервера. Начиная с версии 10 хранится в конфигурационном файле Сервера.

- `<location city="" country="" department="" floor="" latitude="" longitude="" organization="" province="" room="" street="" />`

  Географическое расположение Сервера.

  Описание атрибутов:

Атрибут	Описание
city	Город
country	Страна
department	Название подразделения
floor	Этаж
latitude	Широта
longitude	Долгота
organization	Название организации
province	Название области
room	Номер комнаты
street	Название улицы

- `<threads count="" />`

  Количество потоков для обработки данных, поступающих от Агентов. Минимальное значение — 5. По умолчанию — 5. Данный параметр влияет на производительность Сервера. Не следует изменять значение параметра без рекомендации службы поддержки.

- `<newbie approve-to-group="" default-rate="" mode="" />`

  Режим доступа новых станций.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`approve-to-group`	-	Группа, которая будет назначена по умолчанию в качестве первичной для новых станции при режиме **Автоматически разрешать доступ** (`mode='open'`).	Пустое значение, что означает назначать первичной группу **Everyone**.
`default-rate`	-	Для AV-Desk. Группа, которая будет назначена по умолчанию в качестве тарифной для новых станции при режиме **Автоматически разрешать доступ** (`mode='open'`).	Пустое значение, что означает назначать тарифной группу **Dr.Web Premium**.
`mode`	• open — автоматически разрешать доступ, • closed — всегда отказывать в доступе, • approval — подтверждать доступ вручную.	Политика подключения новых станций.	-

  Подробнее см. **Руководство администратора**, п. Политика подключения станций.

- `<emplace-auto enabled="" />`

  Режим создания учетных записей станций в Центре управления при установке Агентов из группового инсталляционного пакета, в случае, если недостаточно уже созданных учетных записей.

Атрибут	Допустимые значения	По умолчанию
`enabled`	• `yes` — автоматически создавать недостающие учетные записи станций, • `no` — установка возможна только по количеству уже созданных учетных записей в группе, инсталляционный пакет для станций которой запускается.	`yes`

- `<unauthorized-to-newbie enabled="" />`

  Политика действий над неавторизованными станциями. Допустимые значения атрибута `enabled`:

  - `yes` — станции, не прошедшие авторизацию (например, в случае повреждения базы данных), будут автоматически переводиться в состояние новичков,
  - `no` (по умолчанию) — нормальный режим работы.

- `<maximum-authorization-queue size="" />`

  Максимальное количество станций в очереди для авторизации на Сервере. Не следует изменять значение параметра без рекомендации службы поддержки.

- `<reverse-resolve enabled="" />`

  Заменять IP-адреса DNS-именами компьютеров в файле журнала Сервера Dr.Web. Допустимые значения атрибута `enabled`:

  - `yes` — показывать DNS-имена.
  - `no` (по умолчанию) — показывать IP-адреса.

- `<replace-netbios-names enabled="" />`

  Заменять NetBIOS-имена компьютеров DNS-именем. Допустимые значения атрибута `enabled`:

  - `yes` — показывать DNS-имена.
  - `no` (по умолчанию) — показывать NetBIOS-имена.

- `<dns>`

  Настройки DNS.

  `<timeout value="" />`

  Тайм-аут в секундах для разрешения прямых/обратных DNS-запросов. Оставьте значение пустым, чтобы не ограничивать время ожидания до окончания разрешения.

  `<retry value="" />`

  Максимальное количество повторных DNS-запросов при неуспешном разрешении DNS-запроса.

  `<cache enabled="" negative-ttl="" positive-ttl="" />`

  Время хранения в кеше ответов от DNS-сервера.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание
`enabled`	• `yes` — хранить ответы в кеше, • `no` — не хранить ответы в кеше.	Режим хранения ответов в кеше.
`negative-ttl`	-	Время хранения в кеше (TTL) отрицательных ответов от DNS-сервера в минутах.
`positive-ttl`	-	Время хранения в кеше (TTL) положительных ответов от DNS-сервера в минутах.

  `<servers>`

  Список серверов DNS, заменяющий системный список по умолчанию. Содержит один или несколько дочерних элементов `<server address="" />`, в которых параметр `address` определяет IP-адрес сервера.

<domains>

Список доменов DNS, заменяющий системный список по умолчанию. Содержит один или несколько дочерних элементов <domain name="" />, в которых параметр name определяет имя домена.

- <cache>

  Настройки кеширования.

  Элемент <cache> содержит следующие дочерние элементы:

  - <interval value="" />

    Периодичность полной очистки кеша в секундах.

  - <quarantine ttl="" />

    Периодичность удаления файлов в карантине Сервера в секундах. По умолчанию — 604800 (одна неделя).

  - <download ttl="" />

    Периодичность удаления персональных инсталляционных пакетов. По умолчанию — 604800 (одна неделя).

  - <repository ttl="" />

    Периодичность удаления файлов в кеше репозитория Сервера в секундах.

  - <file ttl="" />

    Периодичность очистки файлового кеша в секундах. По умолчанию — 604800 (одна неделя).

- <replace-station-description enabled="" />

  Синхронизировать описания станций на Сервере Dr.Web с полем **Computer description** на странице **System properties** на станции. Допустимые значения атрибута enabled:

  - yes — заменять описание на Сервере описание со станции.
  - no (по умолчанию) — игнорировать описание на станции.

- <time-discrepancy value="" />

  Допустимая разницу между системным временем Сервера Dr.Web и Агентов Dr.Web в минутах. Если расхождение больше указанного значения, это будет отмечено в статусе станции на Сервере Dr.Web. По умолчанию допускается разница в 3 минуты. Пустое значение или значение 0 означает, что проверка не будет проводиться.

- <encryption mode="" />

  Режим шифрования трафика. Допустимые значения атрибута mode:

  - yes — использовать шифрование,
  - no — не использовать шифрование,
  - possible — шифрование допускается.

  По умолчанию yes.

  Подробнее см. **Руководство администратора**, п. Шифрование и сжатие трафика.

- `<compression level="" mode="" />`

  Режим сжатия трафика.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание
`level`	Целое число от 1 до 9.	Уровень сжатия.
`mode`	• `yes` — использовать сжатие, • `no` — не использовать сжатие, • `possible` — сжатие допускается.	Режим сжатия.

  Подробнее см. **Руководство администратора**, п. Шифрование и сжатие трафика.

- `<track-agent-jobs enabled="" />`

  Разрешить отслеживать и записывать в базу данных Сервера результаты выполнения заданий на станциях. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<track-agent-status enabled="" />`

  Разрешить отслеживать изменения в состоянии станций и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<track-virus-bases enabled="" />`

  Разрешить отслеживать изменения в состоянии (составе, изменении) вирусных баз на станциях и записывать информацию базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`. Параметр игнорируется, если `<track-agent-status enabled="no" />`.

- `<track-agent-modules enabled="" />`

  Разрешить отслеживать версии модулей станций и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<track-agent-components enabled="" />`

  Разрешить отслеживать список установленных на станциях компонентов и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<track-agent-userlogon enabled="" />`

  Разрешить отслеживать сессии пользователей на станциях и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<track-agent-environment enabled="" />`

  Разрешить отслеживать состав аппаратного и программного обеспечения на станциях и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<keep-run-information enabled="" />`

  Разрешить отслеживать информацию о запуске и завершении работы антивирусных компонентов на станциях и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<keep-infection enabled="" />`

  Разрешить отслеживать обнаружение угроз на станциях и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<keep-scan-errors enabled="" />`

  Разрешить отслеживать ошибки при сканировании станций и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<keep-scan-statistics enabled="" />`

  Разрешить отслеживать статистику сканирований станций и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<keep-installation enabled="" />`

  Разрешить отслеживать информацию об установках Агентов на станции и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<keep-blocked-devices enabled="" />`

  Разрешить отслеживать информацию об устройствах, заблокированных компонентом Офисный контроль и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<keep-appcontrol-activity enabled="" />`

  Разрешить отслеживать активность процессов на станциях, зафиксированную Контролем приложений (для наполнения Справочника приложений), и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<keep-appcontrol-block enabled="" />`

  Разрешить отслеживать блокировки процессов на станциях Контролем приложений и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<quarantine enabled="" />`

  Разрешить отслеживать информацию о состоянии Карантина на станциях и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<update-bandwidth queue-size="" value="" />`

  Максимальная ширина полосы пропускания сетевого трафика в КБ/с при передаче обновлений между Сервером и Агентами.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`queue-size`	• целое положительное число,	Максимальное допустимое количество сессий раздачи обновлений, запущенных одновременно с Сервера. При достижении	`unlimited`

Атрибут	Допустимые значения	Описание	По умолчанию
	• unlimited.	указанного ограничения запросы от Агентов размещаются в очереди ожидания. Размер очереди ожидания не ограничен.	
value	• максимальная скорость в КБ/с, • unlimited.	Максимальное значение суммарной скорости при передаче обновлений.	unlimited

- `<install-bandwidth queue-size="" value="" />`

  Максимальная ширина полосы пропускания сетевого трафика в КБ/с при передаче данных с Сервера в процессе установок Агентов на станциях.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
queue-size	• целое положительное число, • unlimited.	Максимальное допустимое количество сессий установки Агента, запущенных одновременно с Сервера. При достижении указанного ограничения запросы от Агентов размещаются в очереди ожидания. Размер очереди ожидания не ограничен.	unlimited
value	• максимальная скорость в КБ/с, • unlimited.	Максимальное значение суммарной скорости при передаче данных в процессе установки Агентов.	unlimited

- `<geolocation enabled="" startup-sync="" />`

  Разрешить синхронизацию географического расположения станций между Серверами Dr.Web.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание
enabled	• yes — разрешить синхронизацию, • no — отключить синхронизацию.	Режим синхронизации.
startup-sync	Целое положительное число.	Количество станций без географических координат, информация о которых запрашивается при установлении соединения между Серверами Dr.Web.

- `<audit enabled="" />`

  Разрешить отслеживать операции администратора в Центре управления безопасностью Dr.Web и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<audit-internals enabled="" />`

  Разрешить отслеживать внутренние операции Сервера Dr.Web и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<audit-xml-api enabled="" />`

  Разрешить отслеживать операции через Web API и записывать информацию в базу данных Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<proxy auth-list="" enabled="" host="" password="" user=""/>`

  Параметры подключений к Серверу Dr.Web через HTTP прокси-сервер.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание

`auth-list`	• `none` — не использовать авторизацию,
	• `any` — любой метод из поддерживаемых,
	• `safe` — любой безопасный метод из поддерживаемых,
	• следующие методы, если несколько, то указывать все необходимые через пробел:
	  ▫ `basic`
	  ▫ `digest`
	  ▫ `digestie`
	  ▫ `ntlmwb`
	  ▫ `ntlm`
	  ▫ `negotiate`
		Тип авторизации на прокси-сервере. По умолчанию - 'any'.

`enabled`	• `yes` — использовать прокси-сервер, • `no` — не использовать прокси-сервер.	Режим подключения к Серверу через HTTP прокси-сервер.
`host`	-	Адрес прокси-сервера.
`password`	-	Пароль пользователя прокси-сервера, если на прокси-сервере требуется авторизация.
`user`	-	Имя пользователя прокси-сервера, если на прокси-сервере требуется авторизация.

При задании списка доступных методов авторизации для прокси-сервера возможно использование метки `only` (добавляется в конце списка через пробел) для изменения алгоритма выбора методов авторизации.

Подробнее см. https://curl.se/libcurl/c/CURLOPT_HTTPAUTH.html.

- `<statistics enabled="" id="" interval="" />`

  Параметры отправки статистики по вирусным событиям в компанию «Доктор Веб» в раздел https://stat.drweb.com/.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
enabled	• yes — отправлять статистику, • no — не отправлять статистику.	Режим отправки статистики в компанию «Доктор Веб».	–
id	–	MD5 лицензионного ключа Агента.	–
interval	Целое положительное число.	Интервал отправки статистики в минутах.	30

- `<cluster>`

  Параметры кластера Серверов Dr.Web для обмена информацией при многосерверной конфигурации антивирусной сети.

  Содержит один или несколько дочерних элементов `<on multicast-group="" port="" interface="" />`.

  Описание атрибутов:

Атрибут	Описание
multicast-group	IP-адрес multicast-группы, через которую Серверы будут осуществлять обмен информацией.
port	Номер порта сетевого интерфейса, к которому привязывается транспортный протокол для передачи информации в multicast-группу.
interface	IP-адрес сетевого интерфейса, к которому привязывается транспортный протокол для передачи информации в multicast-группу.

- `<multicast-updates enabled="" />`

  Настройка передачи групповых обновлений на рабочие станции по multicast-протоколу. Допустимые значения атрибута `enabled`: `yes` или `no`.

  Элемент `<multicast-updates>` содержит ряд дочерних элементов и атрибутов:

Дочерний элемент	Атрибут	Описание	По умолчанию
port	value	Номер порта сетевого интерфейса Сервера Dr.Web, к которому привязывается	2197

Дочерний элемент	Атрибут	Описание	По умолчанию
`<port value="" />`		транспортный multicast-протокол для передачи обновлений. Данный порт будет использоваться всеми multicast-группами. Для групповых обновлений необходимо задавать любой свободный порт, который будет отличаться от порта, назначенного в настройках для работы транспортного протокола самого Сервера.	
ttl `<ttl value="" />`	value	Срок жизни передаваемой UDP-датаграммы. Заданное значение будет использоваться всеми multicast-группами.	8
group `<group address="" />`	address	IP-адрес multicast-группы, через которую станции будут получать групповые обновления.	233.192.86.0 для IPv4 FF0E::176 для IPv6
on `<on interface="" ttl="" />`	interface	IP-адрес сетевого интерфейса Сервера Dr.Web, к которому привязывается транспортный multicast-протокол для передачи обновлений.	–
	ttl	Срок жизни UDP-датаграммы, передаваемой через заданный сетевой интерфейс. Имеет приоритет над общим дочерним элементом `<ttl value="" />`.	8
transfer `<transfer datagram-size="" assembly-timeout="" updates-interval="" chunks-interval="" resend-interval="" silence-interval="" accumulate-interval="" announce-send-times="" />`	datagram-size	Размер UDP-датаграммы — размер в байтах UDP-датаграмм, используемых multicast-протоколом. Допустимый диапазон: 512–8192. Во избежание фрагментации рекомендуется задавать значение меньше MTU (Maximum Transmission Unit) используемой сети.	1400
	assembly-timeout	Время передачи файла (мс.) — в течение заданного интервала осуществляется передача одного файла обновления, после чего Сервер начинает отправку следующего файла. Все файлы, которые не удалось передать на этапе обновления по multicast-протоколу, будут передаваться в процессе стандартного обновления по протоколу TCP.	180000

Дочерний элемент	Атрибут	Описание	По умолчанию
	updates-interval	Длительность групповых обновлений (мс.) — длительность процесса обновления по multicast-протоколу. Все файлы, которые не удалось передать на этапе обновления по multicast-протоколу, будут передаваться в процессе стандартного обновления по протоколу TCP.	600000
	chunks-interval	Интервал отправки пакетов (мс.) — интервал отправки пакетов в multicast-группу. Малое значение интервала может привести к значительным потерям при передаче пакетов и перегрузить сеть. Не рекомендуется изменять этот параметр.	14
	resend-interval	Интервал между запросами на повторную передачу (мс.) — с данным интервалом Агенты отправляют запросы на повторную передачу потерянных пакетов. Сервер Dr.Web накапливает эти запросы, после чего пересылает потерянные блоки.	1000
	silence-interval	Интервал “тишины” на линии (мс.) — в случае завершения передачи файла до истечения отведенного времени, если в течение заданного интервала “тишины” от Агентов не поступило запросов на повторную передачу потерянных пакетов, Сервер Dr.Web считает, что все Агенты успешно получили файлы обновления, и начинает отправку следующего файла.	10000
	accumulate-interval	Интервал накопления запросов на повторную передачу (мс.) — в течение указанного интервала Сервер накапливает запросы от Агентов на повторную передачу потерянных пакетов. Агенты перезапрашивают потерянные пакеты. Сервер накапливает эти запросы в течение указанного времени, после чего пересылает потерянные блоки.	2000
	announce-send-times	Количество анонсов передачи файла — количество раз, которое Сервер	3

Дочерний элемент	Атрибут	Описание	По умолчанию
		анонсирует передачу файла в multicast-группу перед началом передачи обновлений. При анонсе в multicast-группу направляется UDP-датаграмма с метаданными файла. Увеличение количества анонсов способно повысить надежность передачи, но может привести к сокращению объема данных, которые удастся передать за время, отведенное на обновление по multicast-протоколу.	

Элемент **<multicast-updates>** может также опционально содержать дочерний элемент **<acl>**, использующийся для создания списков доступа. Это позволяет ограничить круг TCP-адресов рабочих станций, которые смогут получать групповые обновления по multicast-протоколу с данного Сервера. По умолчанию дочерний элемент **<acl>** отсутствует, что означает отсутствие каких-либо ограничений.

<acl> в составе **<multicast-updates>** содержит следующие дочерние элементы:

- **<priority** mode="" />

  Устанавливает приоритетность списков. Допустимые значения атрибута mode: allow или deny. При значении **<priority** mode="deny" />, список **<deny>** имеет более высокий приоритет, чем список **<allow>**. Адреса, не включенные ни в один из списков или включенные в оба, запрещаются. Разрешаются только адреса, которые включены в список **<allow>** и не включены в список **<deny>**.

  - **<allow>**

    Список TCP-адресов, которым доступны обновления по multicast-протоколу. Элемент **<allow>** содержит один или несколько дочерних элементов **<ip** address="" /> для задания разрешенных адресов в формате IPv4 и **<ip6** address="" /> для задания разрешенных адресов в формате IPv6. В атрибуте address задаются сетевые адреса в формате: <*IP-адрес*>/[<*префикс*>].

  - **<deny>**

    Список TCP-адресов, которым недоступны обновления по multicast-протоколу. Элемент **<deny>** содержит один или несколько дочерних элементов **<ip** address="" /> для задания запрещенных адресов в формате IPv4 и **<ip6** address="" /> для задания запрещенных адресов в формате IPv6. В атрибуте address задаются сетевые адреса в формате: <*IP-адрес*>/[<*префикс*>].

- **<database** connections="" speedup="" />

  Определение базы данных.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`connections`	Целое положительное число.	Максимально допустимое количество соединений базы данных с Сервером. Не следует изменять значение параметра без рекомендации службы поддержки.	2
`speedup`	`yes | no`	Автоматически проводить отложенную очистку базы данных после ее инициализации, обновления и импорта (см. **Руководство администратора**, п. База данных).	`yes`

Элемент `<database>` содержит один из следующих дочерних элементов:

Элемент `<database>` может содержать только один дочерний элемент, определяющий конкретную базу данных.

Атрибуты баз данных, которые могут присутствовать в шаблоне конфигурационного файла, но не приведены в описаниях, не рекомендуется изменять без согласования со службой технической поддержки компании «Доктор Веб».

- `<sqlite dbfile="" cache="" cachesize="" readuncommitted="" precompiledcache="" synchronous="" openmutex="" checkintegrity="" autorepair="" mmapsize="" wal="" wal-max-pages="" wal-max-seconds="" />`

  Определяет встроенную базу данных SQLite3.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`dbfile`		Имя файла базы данных.	`database.sqlite`
`cache`	`SHARED | PRIVATE`	Режим кеширования.	`SHARED`
`cachesize`	Целое положительное число.	Размер кеш-памяти базы данных (в 1,5 Кб страницах).	2048
`precompiledcache`	Целое положительное число.	Размер кеша предкомпилированных sql-операторов в килобайтах.	1024
`synchronous`	• `TRUE` или `FULL` — синхронный • `FALSE` или `NORMAL` — обычный	Режим записи данных.	`FULL`

Атрибут	Допустимые значения	Описание	По умолчанию
	• OFF — асинхронный		
checkintegrity	quick | full | no	Проверка целостности образа базы данных при запуске Сервера Dr.Web.	quick
autorepair	yes | no	Автоматическое восстановление поврежденного образа базы данных при запуске Сервера Dr.Web.	no
mmapsize	Целое положительное число.	Максимальный размер в байтах файла базы данных, который допускается отображать на адресное пространство процесса за один раз.	• для ОС UNIX — 10485760 • для ОС Windows — 0
wal	yes | no	Использование упреждающего журналирования (Write-Ahead Logging).	yes
wal-max-pages		Максимальное число “грязных” страниц, при достижении которого осуществляется запись страниц на диск.	1000
wal-max-seconds		Максимальное время, на которое откладывается запись страниц на диск (в секундах).	30

- `<pgsql dbname="drwcs" host="localhost" port="5432" options="" requiressl="" user="" password="" temp_tablespaces="" default_transaction_isolation="" debugproto ="yes" />`

  Определяет внешнюю базу данных PostgreSQL.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
dbname		Имя файла базы данных.	
host		Адрес сервера PostgreSQL или путь к доменному сокету UNIX.	
port		Номер порта сервера PostgreSQL или расширение имени файла UNIX-сокета.	

Атрибут	Допустимые значения	Описание	По умолчанию
options		Параметры командной строки для отправки на сервер базы данных. Подробнее см. в главе 18 https://www.postgresql.org/docs/9.1/libpq-connect.html	
requiressl	• 1 | 0 (через Центр управления) • y | n • yes | no • on | off	Использовать только SSL-соединения.	• 0 • y • yes • on
user		Имя пользователя базы данных.	
password		Пароль пользователя базы данных.	
temp_tablespaces		Пространство имен для временных таблиц базы данных.	
default_transaction_isolation	• read uncommitted • read committed • repeatable read • serializable	Уровень изоляции транзакций.	read committed

- `<oracle connectionstring="" user="" password="" client="" prefetch-rows="0" prefetch-mem="0" />`

  Определяет внешнюю базу данных Oracle.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
connectionstring		Строка, содержащая Oracle SQL Connect URL или Oracle Net пары ключ-значение.	
user		Регистрационное имя пользователя базы данных.	
password		Пароль пользователя базы данных.	

Атрибут	Допустимые значения	Описание	По умолчанию
client		Путь к клиенту для доступа к БД Oracle (Oracle Instant Client). Сервер Dr.Web поставляется с Oracle Instant Client версии 11. Однако, в случае использования серверов Oracle более поздней версии, либо наличия ошибок в поставляемом драйвере БД Oracle, вы можете скачать соответствующий драйвер с сайта компании Oracle и указать путь до этого драйвера в данном поле.	
prefetch-rows	0-65535	Количество строк для предварительной выборки при выполнении запроса к базе данных.	0 — использовать значение = 1 (умолчание базы данных)
prefetch-mem	0-65535	Объем памяти, выделяемой для предварительной выборки строк при выполнении запроса к базе данных.	0 — не ограничено

- `<odbc dsn="drwcs" user="" pass="" transaction="DEFAULT" />`

  Определяет подключение к внешней базе данных через ODBC.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
dsn		Имя источника данных ODBC.	drwcs
user		Регистрационное имя пользователя базы данных.	drwcs
pass		Пароль пользователя базы данных.	drwcs
limit	Целое положительное число.	Переподключаться к СУБД после указанного количества транзакций.	0 — не переподключаться
transaction	• SERIALIZABLE — упорядочиваемость • READ_UNCOMMITTED — чтение незафиксированных данных • READ_COMMITTED — чтение зафиксированных данных • REPEATABLE_READ — повторяемость чтения	Уровень изоляции транзакций. Некоторые СУБД поддерживают только READ_COMMITTED.	DEFAULT

Атрибут	Допустимые значения	Описание	По умолчанию
	• DEFAULT — равносильно "" — зависит от СУБД.		

- <mysql dbname="drwcs" host="localhost" port="3306" user="" password="" ssl="no" debug="no" />

  Определяет внешнюю базу данных MySQL/MariaDB.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
dbname		Название базы данных.	drwcs
host	Одно из двух.	Адрес сервера базы данных при подключении по TCP/IP.	localhost
		Путь к файлу сокета UNIX при использовании UDS. Если путь не задан, Сервер попытается найти файл в стандартных директориях mysqld.	/var/run/mysqld/
port	Одно из двух.	Номер порта для подключения к базе данных по TCP/IP.	3306
		Имя файла сокета UNIX при использовании UDS.	mysqld.sock
user		Регистрационное имя пользователя базы данных.	""
password		Пароль пользователя базы данных.	""
ssl	yes | любой другой набор символов	Использовать только SSL-соединения.	no
precompiledcache	Целое положительное число.	Размер кеша предкомпилированных sql-операторов в килобайтах.	1024

- <acl>

  Списки контроля доступа. Позволяют настроить ограничения на сетевые адреса, с которых Агенты, сетевые инсталляторы и другие (соседние) Серверы Dr.Web смогут получать доступ к данному Серверу.

  Элемент <acl> содержит следующие дочерние элементы, в которых настраиваются ограничения для соответствующих типов соединений:

  - <install> — список ограничений на IP-адреса, с которых инсталляторы Агентов Dr.Web могут подключаться к данному Серверу.

- <agent> — список ограничений на IP-адреса, с которых Агенты Dr.Web могут подключаться к данному Серверу.
- <links> — список ограничений на IP-адреса, с которых соседние Серверы Dr.Web могут подключаться к данному Серверу.
- <discovery> — список ограничений на IP-адреса, с которых принимаются широковещательные запросы *службой обнаружения Сервера*.

Все дочерние элементы содержат одинаковую структуру вложенных элементов, задающих следующие ограничения:

- <priority mode="" />

  Приоритетность списков. Допустимые значения атрибута `mode`: `allow` или `deny`. При значении <priority mode="deny" />, список <deny> имеет более высокий приоритет, чем список <allow>. Адреса, не включенные ни в один из списков или включенные в оба, запрещаются. Разрешаются только адреса, которые включены в список <allow> и не включены в список <deny>.

  - <allow>

    Список TCP-адресов, с которых доступ разрешен. Элемент <allow> содержит один или несколько дочерних элементов <ip address="" /> для задания разрешенных адресов в формате IPv4 и <ip6 address="" /> для задания разрешенных адресов в формате IPv6. В атрибуте `address` задаются сетевые адреса в формате: <*IP-адрес*>/[<*префикс*>].

  - <deny>

    Список TCP-адресов, с которых доступ запрещен. Элемент <deny> содержит один или несколько дочерних элементов <ip address="" /> для задания запрещенных адресов в формате IPv4 и <ip6 address="" /> для задания запрещенных адресов в формате IPv6. В атрибуте `address` задаются сетевые адреса в формате: <*IP-адрес*>/[<*префикс*>].

- <scripts profile="" stack="" trace="" />

  Настройка параметров профилирования работы скриптов.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`profile`	• `yes`, • `no`.	Записывать в журнал информацию о профилировании работы скриптов Сервера. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости.	`no`
`stack`		Записывать в журнал информацию из стека вызовов при работе скриптов Сервера. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости.	

Атрибут	Допустимые значения	Описание	По умолчанию
trace		Записывать в журнал информацию о трассировке работы скриптов Сервера. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости.	

- **<lua-module-path>**

  Пути для интерпретатора Lua.

  Порядок задания путей имеет значение.

  Элемент **<lua-module-path>** содержит следующие дочерние элементы:

  - **<cpath** root="" **/>** — путь до каталога с бинарными модулями. Допустимые значения атрибута root: home (по умолчанию), var, bin, lib.
  - **<path** value="" **/>** — путь до каталога со скриптами. Если не является дочерним для элемента **<jobs>** или **<hooks>**, то относится к обоим. Пути, задаваемые в атрибуте value, являются относительными от путей, заданных в атрибуте root элемента **<cpath>**.
  - **<jobs>** — пути для заданий из расписания Сервера.

    Элемент **<jobs>** содержит один или несколько дочерних элементов **<path** value="" **/>** для задания пути до каталога со скриптами.
  - **<hooks>** — пути для пользовательских процедур Сервера.

    Элемент **<hooks>** содержит один или несколько дочерних элементов **<path** value="" **/>** для задания пути до каталога со скриптами.

- **<transports>**

  Настройка параметров транспортных протоколов, используемых Сервером для соединения с клиентами. Содержит один или несколько дочерних элементов **<transport** discovery="" ip="" name="" multicast="" multicast-group="" port="" **/>**.

  Описание атрибутов:

Атрибут	Описание	Обязательный	Допустимые значения	По умолчанию
discovery	Определяет, будет ли использоваться служба обнаружения Сервера.	нет, задается только вместе с атрибутом ip.	yes, no	no
• ip • unix	Определяет семейство используемых протоколов и задает адрес интерфейса.	да	–	• 0.0.0.0 • -

Атрибут	Описание	Обязательный	Допустимые значения	По умолчанию
name	Задает имя Сервера для службы обнаружения Сервера.	нет	-	drwcs
multicast	Определяет, входит ли Сервер в multicast-группу.	нет, задается только вместе с атрибутом ip.	yes, no	no
multicast-group	Задает адрес multicast-группы, в которую сходит Сервер.	нет, задается только вместе с атрибутом ip.	-	• 231.0.0.1 • [ff18::231.0.0.1]
port	Прослушиваемый порт.	нет, задается только вместе с атрибутом ip.	-	2193

- **<protocols>**

  Список отключенных протоколов. Содержит один или несколько дочерних элементов **<protocol** enabled="" name="" />.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
enabled	• yes — протокол включен, • no — протокол отключен.	Режим использования протокола.	no
name	• AGENT — протокол взаимодействия Сервера с Агентами Dr.Web. • MSNAPSHV — протокол взаимодействия Сервера с компонентом проверки работоспособности системы Microsoft NAP Validator. • INSTALL — протокол взаимодействия Сервера с инсталляторами Агентов Dr.Web. • CLUSTER — протокол взаимодействия между Серверами в кластерной системе. • SERVER — протокол взаимодействия Сервера Dr.Web с другими Серверами Dr.Web.	Название протокола.	-

- **<plugins>**

  Список отключенных расширений. Содержит один или несколько дочерних элементов **<plugin** enabled="" name="" />.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
enabled	• yes — расширение включено, • no — расширение отключено.	Режим использования расширения.	no
name	• WEBMIN — расширение Центра управления безопасностью Dr.Web для управления Сервером и антивирусной сетью через Центр управления. • FrontDoor — расширение Dr.Web Server FrontDoor, позволяющего подключение утилиты дистанционной диагностики Сервера.	Название расширения.	-

- **<license>**

  Настройки лицензирования.

  Элемент **<license>** содержит следующие дочерние элементы:

  - **<limit-notify** min-count="" min-percent="" />

    Настройки уведомления об ограничении по количеству лицензий в лицензионном ключе.

    Описание атрибутов:

Атрибут	Описание	По умолчанию
min-count	Максимальное количество оставшихся лицензий, при котором будет отправлено уведомление **Ограничение по количеству лицензий в лицензионном ключе**.	3
min-percent	Максимальный процент оставшихся лицензий, при котором будет отправлено уведомление **Ограничение по количеству лицензий в лицензионном ключе**.	5

  - **<license-report** report-period="" active-stations-period="" />

    Настройки для отчета по использованию лицензий.

    Описание атрибутов:

Атрибут	Описание	По умолчанию
report-period	Периодичность, с которой будут создаваться отчеты на Сервере об используемых им лицензионных ключах. Если отчет об использовании лицензий создается подчиненным Сервером, то сразу после создания осуществляется отправка этого отчета на главный Сервер. Созданные отчеты дополнительно отправляются при каждом подключении (в т.ч. перезагрузке) Сервера, а также при	1440

Атрибут	Описание	По умолчанию
	изменении количества выдаваемых лицензий на главном Сервере.	
active-stations-period	Период, в течение которого будет подсчитываться количество активных станций для создания отчета об использовании лицензий. Значение 0 предписывает учитывать в отчете все станции, вне зависимости от статуса их активности.	0

- <exchange>

  Настройки распространения лицензий между Серверами Dr.Web.

  Элемент <exchange> содержит следующие дочерние элементы:

  - <expiration-interval value="" />
  - <prolong-preact value="" />
  - <check-interval value="" />

  Описание элементов:

Элемент	Описание	Значения атрибута value по умолчанию, мин.
expiration-interval	**Срок действия выдаваемых лицензий** — период времени, на который выдаются лицензии из ключа на данном Сервере. Настройка используется, если данный Сервер выдает лицензии соседним Серверам.	1440
prolong-preact	**Период для продления получаемых лицензий** — период до окончания срока действия лицензии, начиная с которого данный Сервер инициирует продление лицензии, полученной от соседнего Сервера. Настройка используется, если данный Сервер получает лицензии от соседних Серверов.	60
check-interval	**Период синхронизации лицензий** — периодичность синхронизации информации о выдаваемых лицензиях между Серверами.	1440

- <email from="" debug="" />

  Настройки параметров отправки электронной почты из Центра управления, например, в качестве оповещений администратора или при рассылке инсталляционных пакетов станций.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
from	-	Адрес ящика электронной почты, от имени которого будут отправляться электронные письма.	drwcs@localhost
debug	• yes — использовать отладочный режим, • no — не использовать отладочный режим.	Использовать отладочный режим для получения детального журнала SMTP-сессии.	no

Элемент <email> содержит следующие дочерние элементы:

- <smtp server="" user="" pass="" port="" start_tls="" auth_plain="" auth_login="" auth_cram_md5="" auth_digest_md5="" auth_ntlm="" conn_timeout="" />

  Настройка параметров SMTP-сервера для отправки электронной почты.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
server	-	Адрес SMTP-сервера, который будет использоваться для отправки электронной почты.	127.0.0.1
user	-	Имя пользователя SMTP-сервера, если SMTP-сервер требует авторизации.	-
pass	-	Пароль пользователя SMTP-сервера, если SMTP-сервер требует авторизации.	-
port	Целое положительное число.	Порт SMTP-сервера, который будет использоваться для отправки электронной почты.	25
start_tls	• yes — использовать этот тип аутентификации, • no — не использовать этот тип аутентификации.	Для шифрованного обмена данными. При этом переключение на защищенное соединение осуществляется через команду STARTTLS. По умолчанию для соединения предусматривается использование 25 порта.	yes
auth_plain		Использование *plain text* аутентификации на почтовом сервере.	no
auth_login		Использование *LOGIN* аутентификации на почтовом сервере.	no

Атрибут	Допустимые значения	Описание	По умолчанию
auth_cram_md5		Использование *CRAM-MD5* аутентификации на почтовом сервере.	no
auth_digest_md5		Использование *DIGEST-MD5* аутентификации на почтовом сервере.	no
auth_ntlm		Использование *AUTH-NTLM* аутентификации на почтовом сервере.	no
conn_timeout	Целое положительное число.	Тайм-аут соединения с SMTP-сервером.	180

- `<ssl enabled="" verify_cert="" ca_certs="" />`

  Настройки параметров SSL-шифрования трафика при отправке писем по электронной почте.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
enabled	• yes — использовать SSL, • no — не использовать SSL.	Режим использования SSL-шифрования.	no
verify_cert	• yes — проверять SSL-сертификат, • no — не проверять SSL-сертификат.	Проверять правильность SSL-сертификата почтового сервера.	no
ca_certs	-	Путь к корневому SSL-сертификату Сервера Dr.Web.	-

- `<track-epidemic enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Настройка параметров отслеживания вирусных эпидемий в сети.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
enabled	yes | no	Разрешает отслеживать множественные события о заражениях станций и иметь	yes

Атрибут	Допустимые значения	Описание	По умолчанию
		возможность отправлять суммарное оповещение администратору.	
aggregation-period	Целое положительное число.	Промежуток времени в секундах после отправки оповещения об эпидемии, в течение которого не будут отправляться оповещения о единичных заражениях станций.	300
check-period		Промежуток времени в секундах, в течение которого должно прийти заданное количество сообщений о зараженных станциях, чтобы отправить оповещение об эпидемии.	3600
threshold		Количество сообщений о заражениях, которые должны прийти за заданный промежуток времени, чтобы Сервер Dr.Web отправлял администратору единое уведомление об эпидемии на все случаи заражения (оповещение **Эпидемия в сети**).	100
most-active		Количество наиболее часто встречающихся угроз, которые необходимо включить в отчет об эпидемиях.	5

- `<track-hips-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Настройка параметров отслеживания множественных событий компонента Превентивная защита.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
enabled	yes | no	Разрешает отслеживать множественные события Превентивной защиты и иметь возможность отправлять суммарное оповещение администратору.	yes
aggregation-period	Целое положительное число.	Промежуток времени в секундах после отправки суммарного отчета о событиях Превентивной защиты, в течение которого не будут	300

Атрибут	Допустимые значения	Описание	По умолчанию
		отправляться оповещения о единичных событиях.	
`check-period`		Промежуток времени в секундах, в течение которого должно произойти заданное количество событий Превентивной защиты, чтобы отправить суммарный отчет.	3600
`threshold`		Количество событий Превентивной защиты, которые должны прийти за заданный промежуток времени, чтобы Сервер Dr.Web отправлял администратору единый суммарный отчет об этих событиях (оповещение **Суммарный отчет Превентивной защиты**).	100
`most-active`		Количество наиболее часто встречающихся процессов, осуществивших подозрительное действие, которые необходимо включить в отчет Превентивной защиты.	5

- `<track-appctl-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Настройка параметров отслеживания множественных событий компонента Контроль приложений.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`enabled`	`yes | no`	Разрешает отслеживать множественные события Контроля приложений и иметь возможность отправлять суммарное оповещение администратору.	`yes`
`aggregation-period`	Целое положительное число.	Промежуток времени в секундах после отправки суммарного отчета о процессах, заблокированных Контролем приложений, в течение которого не будут отправляться оповещения о единичных блокировках.	300

Атрибут	Допустимые значения	Описание	По умолчанию
check-period		Промежуток времени в секундах, в течение которого должно быть заблокировано заданное количество процессов, чтобы отправить суммарный отчет.	3600
threshold		Количество событий о процессах, заблокированных Контролем приложений, которые должны прийти за заданный промежуток времени, чтобы Сервер Dr.Web отправлял администратору единый суммарный отчет об этих событиях (оповещение **Зафиксировано большое количество блокировок Контролем приложений**).	100
most-active		Количество наиболее распространенных профилей, по которым производилась блокировка и которые необходимо включить в оповещение о множественных блокировках.	5

- `<track-disconnect enabled="" aggregation-period="" check-period="" single-alert-threshold="" summary-alert-threshold="" min-session-duration="" />`

  Настройка параметров отслеживания множественных аварийно завершенных соединений с клиентами.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
enabled	yes | no	Разрешает отслеживать аварийно завершенные соединения с клиентами и иметь возможность отправлять соответствующие оповещения администратору.	yes
aggregation-period	Целое положительное число.	Промежуток времени в секундах после отправки оповещения о множественных завершениях соединений, в течение которого не будут отправляться оповещения о единичных завершенных соединениях.	300
check-period		Промежуток времени в секундах, в течение которого должно произойти заданное количество разрывов	3600

Атрибут	Допустимые значения	Описание	По умолчанию
		соединений с клиентами, чтобы отправить соответствующее оповещение.	
`single-alert-threshold`		Минимальное количество соединений, которые должны быть разорваны с одним адресом в течение периода подсчета, чтобы было отправлено оповещение о единичном аварийном завершении соединения (оповещение **Аварийное завершение соединения**).	10
`summary-alert-threshold`		Минимальное количество соединений, которые должны быть разорваны в течение периода подсчета, чтобы было отправлено единое оповещение о множественных аварийных завершениях соединений (оповещение **Зафиксировано большое количество аварийно завершенных соединений**).	1000
`min-session-duration`		Если длительность завершенного соединения с клиентом меньше указанной, то при достижении заданного количества соединений будет отправлено оповещение о единичных завершениях соединений (оповещение **Аварийное завершение соединения**) вне зависимости от периода подсчета. При этом соединение не должно быть прервано в дальнейшем более продолжительными подключениями, и не должно быть отправлено оповещение о множественных аварийных завершениях соединений (оповещение **Зафиксировано большое количество аварийно завершенных соединений**).	300

- `<default-lang value="" />`

  Язык, который используется по умолчанию компонентами и системами Сервера Dr.Web, если не удалось получить настройки языка из базы данных Сервера. В частности используется для Центра управления безопасностью Dr.Web и системы оповещений администратора, если база данных была повреждена, и получить настройки языка не представляется возможным.

Ж2. Конфигурационный файл Центра управления безопасностью Dr.Web

Конфигурационный файл Центра управления `webmin.conf` представлен в формате XML и располагается в подкаталоге `etc` корневого каталога Сервера.

Описание параметров конфигурационного файла Центра управления безопасностью Dr.Web:

`<version value="">`

Текущая версия Сервера Dr.Web.

- `<server-name value=""/>`

  Название Сервера Dr.Web.

  Задается в формате:

  <IP-адрес или DNS-имя Сервера>`[:`*<порт>*`]`

  Если адрес Сервера не задан, то используется имя компьютера, возвращаемое операционной системой или сетевой адрес Сервера: DNS-имя, если доступно, в противном случае — IP-адрес.

  Если номер порта не задан, используется порт, заданный в запросе (например, при обращении к Серверу из Центра управления или через **Web API**). В частности, при запросе из Центра управления — это порт, заданный в адресной строке при подключении Центра управления к Серверу.

- `<document-root value=""/>`

  Путь к каталогу веб-страниц. По умолчанию `value="webmin"`.

- `<ds-modules value=""/>`

  Путь к каталогу модулей. По умолчанию `value="ds-modules"`.

- `<threads value=""/>`

  Количество параллельных запросов, обрабатываемых веб-сервером. Данный параметр влияет на производительность сервера. Не рекомендуется изменять его значение без необходимости.

- `<io-threads value=""/>`

  Количество потоков, обрабатывающих данные, передаваемые по сети. Данный параметр влияет на производительность Сервера. Не рекомендуется изменять его значение без необходимости.

- `<compression value="" max-size="" min-size=""/>`

  Настройки сжатия трафика при передаче данных по каналу связи с веб-сервером через HTTP/HTTPS.

  Описание атрибутов:

Атрибут	Описание	По умолчанию
value	Уровень сжатия данных от 1 до 9, где 1 — минимальный уровень, а 9 — максимальный уровень сжатия.	9
max-size	Максимальный размер HTTP-ответов, которые будут сжиматься. Задайте значение 0, чтобы снять ограничение на максимальный размер HTTP-ответов, подлежащих сжатию.	51200 КБ
min-size	Минимальный размер HTTP-ответов, которые будут сжиматься. Задайте значение 0, чтобы снять ограничение на минимальный размер HTTP-ответов, подлежащих сжатию.	32 байт

- `<keep-alive timeout="" send-rate="" receive-rate=""/>`

  Поддерживать HTTP-сессию активной. Позволяет настроить постоянное соединение для запросов по протоколу HTTP версии 1.X.

  Описание атрибутов:

Атрибут	Описание	По умолчанию
timeout	Тайм-аут HTTP-сессии. При использовании постоянных соединений Сервер разрывает соединение, если в течение указанного времени от клиента не приходят запросы.	15 с
send-rate	Минимальная скорость отправки данных. Если исходящая скорость передачи по сети ниже данного значения, в соединении будет отказано. Задайте значение 0, чтобы снять данное ограничение.	1024 Б/с
receive-rate	Минимальная скорость получения данных. Если входящая скорость передачи по сети ниже данного значения, в соединении будет отказано. Задайте значение 0, чтобы снять данное ограничение.	1024 Б/с

- `<buffers-size send="" receive=""/>`

  Настройка размеров буферов отправки и приема данных.

  Описание атрибутов:

Атрибут	Описание	По умолчанию
send	Размер буферов, используемых при отправке данных. Данный параметр влияет на производительность Сервера. Не рекомендуется изменять его значение без необходимости.	8192 байт
receive	Размер буферов, используемых при получении данных. Данный параметр влияет на производительность Сервера. Не рекомендуется изменять его значение без необходимости.	2048 байт

- `<max-request-length value=""/>`

  Максимально допустимый размер HTTP-запроса в КБ.

- `<reverse-resolve enabled=""/>`

  Заменять IP-адреса DNS-именами компьютеров в файле журнала Сервера. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<script-errors-to-browser enabled=""/>`

  Показывать ошибки скрипта в браузере (500 ошибка). Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости.

- `<trace-scripts enabled=""/>`

  Включить трассировку работы скриптов. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<profile-scripts enabled="" stack=""/>`

  Управление профилированием. Осуществляется измерение производительности — времени исполнения функций и скриптов веб-сервера. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание
`enabled`	• `yes` — включить профилирование, • `no` — отключить профилирование.	Режим профилирования скрипов.
`stack`	• `yes` — записывать данные в журнал, • `no` — не записывать данные в журнал.	Режим записи информации о профилировании (параметры функции и возвращаемые значения) в журнал Сервера.

- `<abort-scripts enabled=""/>`

  Разрешить прерывание работы скриптов, если соединение было прервано клиентом. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<search-localized-index enabled=""/>`

  Использовать локализованные версии страниц. Если режим разрешен, сервер будет искать локализованную версию указанной страницы в соответствии с приоритетом языков, указанных в поле `Accept-Language` заголовка клиента. Допустимые значения атрибута `enabled`: `yes` или `no`.

- `<default-lang value=""/>`

  Язык документов, возвращаемых веб-сервером при отсутствии заголовка `Accept-Language` в HTTP-запросе. Значения атрибута `value` — ISO код языка. По умолчанию — `ru`.

- `<ssl certificate="" private-key="" keep-alive=""/>`

  Настройки SSL-сертификата.

  Описание атрибутов:

Атрибут	Описание	Допустимые значения	По умолчанию
`certificate`	Путь к файлу SSL-сертификата.	-	`certificate.pem`
`private-key`	Путь к файлу закрытого ключа SSL.	-	`private-key.pem`
`keep-alive`	Использовать постоянное соединение для SSL. Устаревшие версии браузеров могут некорректно работать с постоянными SSL-соединениями. Отключите этот параметр, если возникают проблемы с работой по SSL-протоколу.	• `yes`, • `no`.	`yes`

- `<listen>`

  Настройки параметров для прослушивания соединений.

  Элемент `<listen>` содержит следующие дочерние элементы:

  - `<insecure>`

    Список интерфейсов, которые будут прослушиваться для приема незащищенных соединений по протоколу HTTP. По умолчанию используется порт 9080.

    Элемент `<insecure>` содержит один или несколько дочерних элементов `<endpoint address=""/>` для задания разрешенных адресов в формате IPv4 или IPv6. В атрибуте `address` задаются сетевые адреса в формате: *<Протокол>*`://`*<IP-адрес>*.

  - `<secure>`

    Список интерфейсов, которые будут прослушиваться для приема защищенных соединений по протоколу HTTPS. По умолчанию используется порт 9081.

    Элемент `<secure>` содержит один или несколько дочерних элементов `<endpoint address=""/>` для задания разрешенных адресов в формате IPv4 или IPv6. В атрибуте `address` задаются сетевые адреса в формате: *<Протокол>*`://`*<IP-адрес>*.

- `<access>`

  Списки контроля доступа. Позволяют настроить ограничения на сетевые адреса, с которых веб-сервер принимает HTTP и HTTPS запросы.

  Элемент `<access>` содержит следующие дочерние элементы, в которых настраиваются ограничения для соответствующих типов соединений:

  - `<secure priority="">`

    Список интерфейсов, которые будут прослушиваться для приема защищенных соединений по протоколу HTTPS. По умолчанию используется порт 9081.

    Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
priority	allow	Приоритетность разрешения для HTTPS — адреса, не включенные ни в один из списков (или включенные в оба), разрешаются.	deny
	deny	Приоритетность запрета для HTTPS — адреса, не включенные ни в один из списков (или включенные в оба), запрещаются.	

Элемент <secure> содержит один или несколько следующих дочерних элементов: <allow address=""/> и <deny address=""/>.

Описание элементов:

Элемент	Описание	Значения атрибута address по умолчанию
allow	Адреса, с которых будет разрешен доступ по протоколу HTTPS для защищенных соединений.	tcp://127.0.0.1
deny	Адреса, с которых будет запрещен доступ по протоколу HTTPS для защищенных соединений.	-

- <insecure priority="">

Список интерфейсов, которые будут прослушиваться для приема незащищенных соединений по протоколу HTTP. По умолчанию используется порт 9080.

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
priority	allow	Приоритетность разрешения для HTTP — адреса, не включенные ни в один из списков (или включенные в оба), разрешаются.	deny
	deny	Приоритетность запрета для HTTP — адреса, не включенные ни в один из списков (или включенные в оба), запрещаются.	

Элемент <insecure> содержит один или несколько следующих дочерних элементов: <allow address=""/> и <deny address=""/>.

Описание элементов:

Элемент	Описание	Значения атрибута address по умолчанию
allow	Адреса, с которых будет разрешен доступ по протоколу HTTP для незащищенных соединений.	tcp://127.0.0.1

Элемент	Описание	Значения атрибута address по умолчанию
`deny`	Адреса, с которых будет запрещен доступ по протоколу HTTP для незащищенных соединений.	-

Ж3. Конфигурационный файл download.conf

Назначение файла download.conf:

1. При создании и использовании кластерной системы Серверов Dr.Web позволяет распределить нагрузку между Серверами кластеров при подключении большого количества новых станций.
2. В случае использования на Сервере Dr.Web нестандартного порта, позволяет задать этот порт при формировании файла инсталляции Агента.

Файл `download.conf` используется при формировании файла инсталляции Агента для новой станции антивирусной сети. Параметры данного файла позволяют задать адрес Сервера Dr.Web и порт, используемые для подключения инсталлятора Агента к Серверу в формате:

```
download = { server = '<Server_Address>'; port = <port_number> }
```

где:

- <*Server_Address*> — IP-адрес или DNS-имя Сервера.

  При формировании инсталляционного пакета Агента адрес Сервера изначально берется из файла `download.conf`. Если в файле `download.conf` адрес Сервера не задан, то используется значение параметра `ServerName` из файла `webmin.conf`. Иначе — имя компьютера, возвращаемое операционной системой.

- <*port_number*> — порт для подключения инсталлятора Агента к Серверу.

  Если в параметрах файла `download.conf` порт не указан, по умолчанию используется порт 2193 (настраивается в Центре управления в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → вкладка **Сеть** → вкладка **Транспорт**).

По умолчанию параметр `download` в файле `download.conf` закомментирован. Для использования файла `download.conf` необходимо раскомментировать данный параметр, убрав "`--`" в начале строки, и задать соответствующие значения адреса и порта Сервера.

Ж4. Конфигурационный файл Прокси-сервера Dr.Web

Конфигурационный файл Прокси-сервера `drwcsd-proxy.conf` представлен в формате XML и располагается в следующем каталоге:

- ОС Windows: `C:\ProgramData\Doctor Web\drwcs\etc`
- ОС Linux: `/var/opt/drwcs/etc`
- ОС FreeBSD: `/var/drwcs/etc`

Описание параметров конфигурационного файла Прокси-сервера Dr.Web:

- `<listen spec="">`

  Корневой элемент `<drwcsd-proxy>` содержит один или несколько обязательных элементов `<listen>`, определяющих основные настройки для приема соединений Прокси-сервером.

  Элемент `<listen>` содержит единственный обязательный атрибут `spec`, атрибуты которого определяют на каком интерфейсе "слушать" входящие подключения клиентов и запускать ли на этом интерфейсе режим `discovery`.

  Атрибуты элемента `spec`:

Атрибут	Обязательное	Допустимые значения	Описание	По умолчанию
`ip | unix`	да	–	Тип протокола для приема входящих соединений. В качестве параметра указывается адрес, прослушиваемый Прокси-сервером.	`0.0.0.0 | –`
`port`	нет	–	Номер порта, прослушиваемого Прокси-сервером.	`2193`
`discovery`	нет	`yes, no`	Режим имитации Сервера. Позволяет клиентам обнаруживать Прокси-сервер в качестве Сервера Dr.Web в процессе его поиска через широковещательные запросы.	`yes`
`multicast`	нет	`yes, no`	Режим "прослушивания" сети для приема широковещательных запросов Прокси-сервером.	`yes`

Атрибут	Обязательное	Допустимые значения	Описание	По умолчанию

`multicast-group`	нет	–	Многоадресная группа, в которой располагается Прокси-сервер.	`231.0.0.1`
				
				`[ff18::231.0.0.1]`

В зависимости от протокола список необязательных атрибутов, указываемых в атрибуте `spec`, изменяет свой состав.

Список необязательных свойств, которые могут быть заданы (+) или не могут быть заданы (–) в атрибуте `spec` в зависимости от протокола:

Протокол	Наличие свойств			
	port	discovery	multicast	multicast-group
ip	+	+	+	+
unix	+	–	–	–

Включение режима **discovery** необходимо указывать явно в любом случае, даже если уже включен режим **multicast**.

Алгоритм переадресации при наличии списка Серверов Dr.Web приведен в **Руководстве администратора**.

- `<compression mode="" level="">`

Элемент `<compression>` в качестве дочернего для элемента `<listen>` определяет параметры сжатия на каналах клиент — Прокси-сервер.

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`mode`	`yes`	Сжатие включено.	`possible`
	`no`	Сжатие отключено.	
	`possible`	Сжатие возможно.	
`level`	целое число от 1 до 9	Уровень сжатия. Только для канала клиент — Прокси-сервер	8

- `<encryption mode="">`

Элемент `<encryption>` в качестве дочернего для элемента `<listen>` определяет параметры шифрования на каналах клиент — Прокси-сервер.

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
mode	yes	Шифрование включено.	possible
	no	Шифрование отключено.	
	possible	Шифрование возможно.	

- <forward to="" master="">

Задает настройки, определяющие переадресацию входящих соединений. Элемент <forward> является обязательным. Может быть задано несколько элементов <forward> с различными значениями атрибутов.

Описание атрибутов:

Атрибут	Допустимые значения	Описание	Обязательный
to	Адрес задается в соответствии со спецификацией сетевого адреса, в частности, в формате tcp/<*DNS_name*>:<*port*>.	Адрес Сервера Dr.Web, на который будет перенаправлено соединение.	да
master	• yes — Сервер будет безусловным управляющим. • no — Сервер не будет управляющим ни при каких условиях. • possible — Сервер будет управляющим только в том случае, если нет безусловных управляющих (со значением yes для атрибута master).	Атрибут определяет, возможно ли удаленное редактирование настроек Прокси-сервера через Центр управления Сервера Dr.Web, указанного в атрибуте to. Вы можете назначить любое количество Серверов управляющими (значение master="yes"), подключение осуществляется ко всем управляющим Серверам по порядку следования в настройках Прокси-сервера до первого получения валидной (не пустой) конфигурации. Также вы можете не назначать ни один из Серверов управляющим (значение master="no"). В этом случае настройка параметров Прокси-сервера (в том числе назначение управляющих Серверов) возможна только локально через конфигурационный файл Прокси-сервера.	нет

Если для Сервера атрибут `master` отсутствует, то по умолчанию считается, что `master="possible"`.

В конфигурационном файле, созданном инсталлятором при установке Прокси-сервера, атрибут `master` не определен ни для одного из Серверов.

- `<compression mode="" level="">`

Элемент `<compression>` в качестве дочернего для элемента `<forward>` определяет параметры сжатия на каналах Сервер — Прокси-сервер. Атрибуты аналогичны описанным выше.

- `<encryption mode="">`

Элемент `<encryption>` в качестве дочернего для элемента `<listen>` определяет параметры шифрования на каналах Сервер — Прокси-сервер. Атрибуты аналогичны описанным выше.

- `<update-bandwidth value="" queue-size="">`

Элемент `<update-bandwidth>` позволяет установить ограничение скорости при передаче обновлений от Сервера клиентам и количество клиентов, скачивающих обновления одновременно.

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`value`	• КБ/с • `unlimited`	Максимальное значение суммарной скорости при передаче обновлений.	`unlimited`
`queue-size`	• целое положительное число • `unlimited`	Максимальное допустимое количество сессий раздачи обновлений, запущенных одновременно с Сервера. При достижении указанного ограничения запросы от Агентов размещаются в очереди ожидания. Размер очереди ожидания не ограничен.	`unlimited`

- `<bandwidth value="" time-map="">`

У элемента `<update-bandwidth>` может быть один или несколько дочерних элементов `<bandwidth>`. Данный элемент позволяет установить ограничение на скорость передачи данных на заданный промежуток времени.

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`value`	• КБ/с • `unlimited`	Максимальное значение суммарной скорости при передаче данных при обновлении Агента.	`unlimited`

Атрибут	Допустимые значения	Описание	По умолчанию
time-map	–	Маска, указывающая на временной промежуток, в течение которого будет активно ограничение.	–

Значение параметра time-map определяется аналогично расписанию ограничений трафика в настройках Сервера. Генерация time-map вручную на данный момент не предоставляется.

- <install-bandwidth value="" queue-size="">

Элемент <install-bandwidth> позволяет установить ограничение скорости передачи данных при установке Агентов и количество клиентов, скачивающих данные для установки одновременно.

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
value	• КБ/с • unlimited	Максимальное значение суммарной скорости при передаче данных в процессе установки Агентов.	unlimited
queue-size	• целое положительное число • unlimited	Максимальное допустимое количество сессий установки Агента, запущенных одновременно с Сервера. При достижении указанного ограничения запросы от Агентов размещаются в очереди ожидания. Размер очереди ожидания не ограничен.	unlimited

  - <bandwidth value="" time-map="">

У элемента <install-bandwidth> может быть один или несколько дочерних элементов <bandwidth>. Данный элемент позволяет установить ограничение на скорость передачи данных на заданный промежуток времени.

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
value	• КБ/с • unlimited	Максимальное значение суммарной скорости при передаче данных при установке Агента.	unlimited
time-map	–	Маска, указывающая на временной промежуток, в течение которого будет активно ограничение.	–

Значение параметра `time-map` определяется аналогично расписанию ограничений трафика в настройках Сервера. Генерация `time-map` вручную на данный момент не предоставляется.

- `<cache enabled="">`

  Настройки кеша репозитория Прокси-сервера.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`enabled`	`yes | no`	Определяет, включено ли кеширование.	`yes`

  Элемент `<cache>` содержит следующие дочерние элементы:

Элемент	Допустимые значения	Описание	По умолчанию
`<maximum-revision-queue size="">`	целое положительное число	Количество хранимых ревизий.	3
`<clean-interval value="">`	целое положительное число	Временной интервал между очистками старых ревизий в минутах.	60
`<unload-interval value="">`	целое положительное число	Временной интервал между выгрузками из памяти неиспользуемых файлов в минутах.	10
`<repo-check mode="">`	`idle | sync`	Проверка целостности кеша либо при запуске (может занять продолжительное время), либо в фоновом режиме.	`idle`

  - `<synchronize enabled="" schedule="">`

    Настройки синхронизации репозиториев Прокси-сервера и Сервера Dr.Web.

    Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`enabled`	`yes | no`	Определяет, включена ли синхронизация репозиториев.	`yes`
`schedule`	–	Расписание, согласно которому будет осуществляться синхронизация заданных продуктов.	–

Значение параметра `schedule` определяется аналогично расписанию синхронизации в настройках Центра управления. Генерация `schedule` вручную на данный момент не предоставляется.

В качестве дочерних элементов `<product name="">` приводится список продуктов, которые будут синхронизироваться:

- 10-drwbases — вирусные базы,
- 10-drwgatedb — базы SpIDer Gate,
- 10-drwspamdb — базы Антиспама,
- 10-drwupgrade — Модуль обновления Dr.Web,
- 15-drwappcntrl — Доверенные приложения компонента Контроль приложений,
- 15-drwhashdb — Известные хеши угроз,
- 20-drwagent — Агент Dr.Web для Windows,
- 20-drwandroid11 — Агент Dr.Web для Android,
- 20-drwunix — Агент Dr.Web для UNIX,
- 40-drwproxy — Прокси-сервер Dr.Web,
- 70-drwextra — Корпоративные продукты Dr.Web,
- 70-drwutils — Административные утилиты Dr.Web.

- `<events enabled="" schedule="">`

  Настройки кеширования событий, полученных от Агентов.

  Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`enabled`	`yes | no`	Определяет, включено ли кеширование событий. Если включено, то события будут отправляться на Сервер согласно расписанию. Если отключено — события будут отправляться на Сервер сразу после их получения Прокси-сервером.	`yes`
`schedule`	–	Расписание, согласно которому будет осуществляться передача событий, полученных от Агентов.	–

Значение параметра `schedule` определяется аналогично расписанию отправки событий в настройках Центра управления. Генерация `schedule` вручную на данный момент не предоставляется.

- `<update enabled="" schedule="">`

Настройка автоматического обновления Прокси-сервера.

При включенном автоматическом обновлении, если синхронизация включена, то обновления Прокси-сервера будут скачиваться с Сервера согласно расписанию синхронизации (см. выше) и устанавливаться согласно расписанию обновления (по умолчанию без ограничений по времени). Если синхронизация отключена, то скачивание и установка производятся по расписанию обновления (по умолчанию без ограничений по времени).

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`enabled`	`yes | no`	Определяет, включено ли автоматическое обновление.	`yes`
`schedule`	–	Расписание, согласно которому будет осуществляться скачивание (если не задана синхронизация) и установка обновлений.	–

Генерация `schedule` вручную на данный момент не предоставляется. По умолчанию автоматическое обновление разрешено без ограничений по времени.

- `<core-dump enabled="" maximum="">`

Режим сбора и количество дампов памяти в случае возникновения SEH-исключения.

Настройка дампов памяти доступна только для ОС Windows.

Для сбора дампа памяти ОС должна содержать библиотеку `dbghelp.dll`.

Дамп сохраняется в каталоге: `%All Users\Application Data%\Doctor Web\drwcsd-proxy-dump\`

Описание атрибутов:

Атрибут	Допустимые значения	Описание	По умолчанию
`enabled`	`yes | no`	Определяет, включен ли сбор дампов.	`yes`
`maximum`	целое положительное число	Максимальное количество дампов. Более старые удаляются.	10

- `<dns>`

Настройки DNS.

`<timeout value="">`

Тайм-аут в секундах для разрешения прямых/обратных DNS-запросов. Оставьте значение пустым, чтобы не ограничивать время ожидания до окончания разрешения.

<retry value="">

Максимальное количество повторных DNS-запросов при неуспешном разрешении DNS-запроса.

<cache enabled="" negative-ttl="" positive-ttl="">

Время хранения в кеше ответов от DNS-сервера.

Описание атрибутов:

Атрибут	Допустимые значения	Описание
enabled	• yes — хранить ответы в кеше, • no — не хранить ответы в кеше.	Режим хранения ответов в кеше.
negative-ttl	–	Время хранения в кеше (TTL) отрицательных ответов от DNS-сервера в минутах.
positive-ttl	–	Время хранения в кеше (TTL) положительных ответов от DNS-сервера в минутах.

<servers>

Список серверов DNS, заменяющий системный список по умолчанию. Содержит один или несколько дочерних элементов <server address="">, в которых параметр address определяет IP-адрес сервера.

<domains>

Список доменов DNS, заменяющий системный список по умолчанию. Содержит один или несколько дочерних элементов <domain name="">, в которых параметр name определяет имя домена.

Ж5. Конфигурационный файл Загрузчика репозитория

Конфигурационный файл Загрузчика репозитория drwreploader.conf представлен в формате XML и располагается в каталоге etc каталога установки Сервера.

Чтобы использовать конфигурационный файл

- Для консольной утилиты путь до файла должен быть указан в ключе --config.
- Для графической утилиты файл должен располагаться в каталоге размещения самой утилиты. При запуске графической утилиты без конфигурационного файла, он будет создан в каталоге расположения утилиты и будет использоваться при последующих ее запусках.

Описание параметров конфигурационного файла Загрузчика репозитория:

- <mode value="" path="" archive="" key="">

  Описание атрибутов:

Атрибут	Описание	Допустимые значения
value	Режим загрузки обновлений: • repository — осуществляется скачивание репозитория в формате репозитория Сервера. Загруженные файлы могут быть непосредственно импортированы через Центр управления в качестве обновления репозитория Сервера. • mirror — осуществляется скачивание репозитория в формате зоны обновлений ВСО. Загруженные файлы могут быть выложены на зеркало обновлений в вашей локальной сети. В дальнейшем Серверы могут быть настроены на получение обновлений непосредственно с данного зеркала обновлений, содержащего последнюю версию репозитория, а не с серверов ВСО.	repository | mirror
path	Каталог, в который будет осуществляться загрузка репозитория.	–
archive	Автоматически упаковать загруженный репозиторий в zip-архив. Данная опция позволяет получить готовый архивный файл для импорта загруженного репозитория на Сервер при помощи Центра управления, из раздела **Администрирование → Содержимое репозитория**.	yes | no
key	Файл лицензионного ключа Dr.Web. Также можно задать только MD5-хеш лицензионного ключа, который доступен для просмотра в Центре управления, в разделе **Администрирование → Менеджер лицензий**.	–

- `<log path="" verbosity="" rotate="">`

  Настройки ведения журнала работы Загрузчика репозитория.

  Описание атрибутов:

Атрибут	Описание	Допустимые значения
path	Путь к файлу журнала.	–
verbosity	Уровень подробности ведения журнала. По умолчанию — TRACE3.	ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT. Значения ALL и DEBUG3 — синонимы.
rotate	Режим ротации журнала в формате <*N*><*f*>,<*M*><*u*>. Аналогично настройке ротации журнала Сервера. По умолчанию 10,10m, что означает хранить 10 файлов по 10 мегабайт, использовать сжатие.	–

- <update url="" proto="" cdn="" update-key="" version="">

  Общие настройки загрузки репозитория.

  Описание атрибутов:

Атрибут	Описание	Допустимые значения
url	Каталог на серверах ВСО, содержащий обновления продуктов Dr.Web.	–
proto	Тип протокола для получения обновлений с серверов обновлений. Для всех протоколов загрузка обновлений осуществляется согласно настройкам списка серверов ВСО.	http | https | ftp | ftps | sftp | scp | file
cdn	Разрешить использование Content Delivery Network при загрузке репозитория.	yes | no
update-key	Путь до открытого ключа или каталога с открытым ключом для проверки подписи обновлений, загружаемых с ВСО. Открытые ключи для проверки подлинности обновлений update-key-*.upub можно найти на Сервере Dr.Web в каталоге etc.	–
version	Версия Сервера Dr.Web, для которого необходимо скачать обновления.	–

  - <servers>

    Список серверов обновления. Порядок серверов ВСО в списке определяет порядок обращения к ним утилиты при загрузке репозитория.

    Содержит дочерние элементы <server>, в которых указываются серверы обновления.

    - <auth user="" password="">

      Регистрационные данные пользователя для аутентификации на сервере обновлений, если сервер требует аутентификации.

      Описание атрибутов:

Атрибут	Описание
user	Имя пользователя на сервере обновлений.
password	Пароль на сервере обновлений.

    - <proxy host="" port="" user="" password="" />

      Параметры подключения к ВСО через прокси-сервер.

      Описание атрибутов:

Атрибут	Описание
host	Сетевой адрес используемого прокси-сервера.

Атрибут	Описание
port	Номер порта используемого прокси-сервера. По умолчанию — 3128.
user	Имя пользователя на прокси-сервере, если используемый прокси-сервер требует авторизацию.
password	Пароль на прокси-сервере, если используемый прокси-сервер требует авторизацию.

- <ssl cert-mode="" cert-file="">

  Настройки SSL-сертификатов, которые будут автоматически приниматься. Данная настройка используется только для защищенных протоколов, поддерживающих шифрование.

  Описание атрибутов:

Атрибут	Описание	Допустимые значения
cert-mode	Сертификаты, которые будут приниматься автоматически.	▫ any — принимать любые сертификаты, ▫ valid — принимать только проверенные сертификаты, ▫ drweb — принимать только сертификаты Dr.Web, ▫ custom — принимать пользовательские сертификаты.
cert-file	Путь к файлу сертификата.	–

- <ssh mode="" pubkey="" prikey="">

  Тип авторизации на сервере обновлений при обращении по SCP/SFTP.

  Описание атрибутов:

Атрибут	Описание	Допустимые значения
mode	Тип авторизации.	▫ pwd — авторизация по паролю. Пароль задается в теге <auth />. ▫ pubkey — авторизация по открытому ключу. Открытый ключ задается в атрибуте pubkey или извлекается из закрытого ключа, указанного в prikey.
pubkey	Открытый ключ SSH	–
prikey	Закрытый ключ SSH	–

- <products>

  Настройки загружаемых продуктов.

  - <product name="" update="">

    Настройки каждого продукта по отдельности.

    Описание атрибутов:

Атрибут	Описание	Допустимые значения
`name`	Название продукта.	• `05-drwmeta` — данные безопасности Сервера Dr.Web, • `10-drwbases` — вирусные базы, • `10-drwgatedb` — базы SpIDer Gate, • `10-drwspamdb` — базы Антиспама, • `10-drwupgrade` — Модуль обновления Dr.Web, • `20-drwagent` — Агент Dr.Web для Windows, • `20-drwandroid11` — Агент Dr.Web для Android, • `20-drwcs` — Сервер Dr.Web, • `20-drwunix` — Агент Dr.Web для UNIX, • `40-drwproxy` — Прокси-сервер Dr.Web, • `80-drwnews` — новости компании «Доктор Веб».
`update`	Включить загрузку этого продукта.	`yes | no`

- **<schedule>**

  Расписание периодических обновлений. При этом нет необходимости запускать утилиту вручную, загрузка репозитория будет осуществляться автоматически согласно заданным промежуткам времени.

  - **<job period="" enabled="" min="" hour="" day="">**

    Настройки выполнения загрузок по расписанию.

Атрибут	Описание	Допустимые значения
`period`	Периодичность выполнения заданий на загрузку.	• `every_n_min` — каждые N минут, • `hourly` — ежечасно, • `daily` — ежедневно, • `weekly` — еженедельно.
`enabled`	Задание на загрузку включено.	`yes | no`
`min`	Минута выполнения задания.	целые числа от 0 до 59
`hour`	Час выполнения задания. Актуален для периодов `daily` и `weekly`.	целые числа от 0 до 23
`day`	День выполнения задания. Актуален для периода `weekly`.	• `mon` — понедельник, • `tue` — вторник, • `wed` — среда, • `thu` — четверг, • `fri` — пятница, • `sat` — суббота, • `sun` — воскресенье.

Приложение 3. Параметры командной строки программ, входящих в состав Dr.Web Enterprise Security Suite

Параметры командной строки имеют более высокий приоритет, чем настройки по умолчанию или иные постоянные настройки (заданные в конфигурационном файле Сервера, реестре ОС Windows и т. п.). В ряде случаев заданные при запуске параметры также переопределяют постоянные настройки. Такие случаи описаны ниже.

При описании синтаксиса параметров отдельных программ необязательная часть заключается в квадратные скобки `[...]`.

Особенности, описанные ниже в Приложении 3, не относятся к сетевому инсталлятору Агента.

Часть параметров командной строки имеют ключевую форму — начинаются с дефиса. Такие параметры также называются ключами.

Многие ключи могут быть представлены в различных эквивалентных формах. Так, ключи, которые подразумевают логическое значение (да/нет, запретить/разрешить), имеют отрицательный вариант, например, ключ `-admin-rights` имеет парный `-no-admin-rights` с противоположным значением. Они же могут даваться с явным указанием значения, например, `-admin-rights=yes` и `-admin-rights=no`.

Синонимами значения `yes` являются значения `on`, `true`, `OK`. Синонимами `no` являются `off`, `false`.

Если значение ключа содержит пробелы или табуляцию, весь параметр нужно заключить в кавычки, например:

```
"-home=c:\Program Files\DrWeb Server"
```

Названия ключей могут быть сокращены (отбрасыванием последних букв), если при этом сокращенное название не совпадает с начальной частью какого-либо другого ключа.

Если в командной строке присутствует аргумент, который начинается с дефиса, перед ним необходимо ставить знак "--" (двойной минус), например:

```
[--] initdb D:\Keys\agent.key - - <пароль>
```

где:

- `[--]` — отдельностоящий знак, обозначающий конец списка ключей и отделяющий список ключей от списка дополнительных аргументов.
- *<пароль>* — дополнительный аргумент.

Для принудительного выполнения команд с правами администратора в операционных системах семейства Windows может использоваться параметр `elevate`. При этом он указывается перед всеми другими ключами и параметрами, например: `drwcsd elevate start`.

31. Сетевой инсталлятор

Формат команды запуска:

`drwinst.exe [<ключи>]`

Ключи

Ключи командной строки действительны при запуске всех типов инсталляционных файлов Агента.

Ключи запуска сетевого инсталлятора Агента задаются в формате: `/<ключ> <параметр>`.

Все значение параметров указываются через пробел. Например:

`/silent yes`

Если значение ключа содержит пробелы, табуляцию или символ `\`, весь параметр нужно заключить в кавычки. Например:

```
/pubkey "C:\my folder\drwcsd-certificate.pem"
```

Допустимые ключи:

- `/compression` <*режим*> — режим сжатия трафика с Сервером. Параметр <*режим*> может принимать следующие значения:
  - `yes` — использовать сжатие.
  - `no` — не использовать сжатие.
  - `possible` — сжатие возможно. Окончательное решение принимается в зависимости от настроек на стороне Сервера.

  Если ключ не задан, по умолчанию используется значение `possible`.
- `/encryption` <*режим*> — режим шифрования трафика с Сервером. Параметр <*режим*> может принимать следующие значения:
  - `yes` — использовать шифрование.
  - `no` — не использовать шифрование.
  - `possible` — шифрование возможно. Окончательное решение принимается в зависимости от настроек на стороне Сервера.

Если ключ не задан, по умолчанию используется значение `possible`.

- `/excludeFeatures` <*компоненты*> — список компонентов, которые необходимо исключить при установке на станции. При задании нескольких компонентов используйте знак "`,`" в качестве разделителя. Доступные компоненты:
  - `scanner` — Сканер Dr.Web,
  - `spider-mail` — SpIDer Mail,
  - `spider-g3` — SpIDer Guard,
  - `outlook-plugin` — Dr.Web для Microsoft Outlook,
  - `firewall` — Брандмауэр Dr.Web,
  - `spider-gate` — SpIDer Gate,
  - `parental-control` — Офисный контроль,
  - `antispam-outlook` — Антиспам Dr.Web для компонента Dr.Web для Microsoft Outlook,
  - `antispam-spidermail` — Антиспам Dr.Web для компонента SpIDer Mail.

  Для компонентов, не указанных напрямую, сохраняется статус установки, заданный для них по умолчанию.
- `/id` <*идентификатор_станции*> — идентификатор станции, на которую устанавливается Агент.

  Ключ задается вместе с ключом `/pwd` для автоматической авторизации на Сервере. Если параметры авторизации не заданы, решение об авторизации принимается на стороне Сервера.
- `/includeFeatures` <*компоненты*> — список компонентов, которые необходимо установить на станции. При задании нескольких компонентов используйте знак "`,`" в качестве разделителя. Доступные компоненты:
  - `scanner` — Сканер Dr.Web,
  - `spider-mail` — SpIDer Mail,
  - `spider-g3` — SpIDer Guard,
  - `outlook-plugin` — Dr.Web для Microsoft Outlook,
  - `firewall` — Брандмауэр Dr.Web,
  - `spider-gate` — SpIDer Gate,
  - `parental-control` — Офисный контроль,
  - `antispam-outlook` — Антиспам Dr.Web для компонента Dr.Web для Microsoft Outlook,
  - `antispam-spidermail` — Антиспам Dr.Web для компонента SpIDer Mail.

  Для компонентов, не указанных напрямую, сохраняется статус установки, заданный для них по умолчанию.
- `/installdir` <*каталог*> — каталог установки.

Если ключ не задан, по умолчанию установка осуществляется в каталог "`Program Files\DrWeb`" на системном диске.

- `/installtimeout` <*время*> — предельное время ожидания ответа от станции в случае удаленной установки, запущенной из Центра управления. Задается в секундах.

  Если ключ не задан, по умолчанию используется значение 300 секунд.

- `/instMode` <*режим*> — режим запуска инсталлятора. Параметр <*режим*> может принимать следующее значение:

  - `remove` — удалить установленный продукт.

  Если ключ не задан, по умолчанию инсталлятор автоматически определяет режим запуска.

- `/lang` <*код_языка*> — язык инсталлятора и устанавливаемого продукта. Задается в формате ISO-639-1 для кода языка.

  Если ключ не задан, по умолчанию используется системный язык.

- `/pubkey` <*сертификат*> — полный путь к файлу сертфиката Сервера.

  Если сертификат не задан, по умолчанию при запуске локальной установки инсталлятор автоматически подхватывает файл сертификата `*.pem` из каталога своего запуска. В случае размещения файла сертификата в каталоге, отличном от каталога запуска инсталлятора, необходимо вручную задать полный путь до файла сертификата.

  При запуске инсталляционного пакета, созданного в Центре управления, сертификат входит в состав инсталляционного пакета, и дополнительное указание файла сертификата через ключи командной строки не требуется.

- `/pwd` <*пароль*> — пароль Агента для доступа к Серверу.

  Ключ задается вместе с ключом `/id` для автоматической авторизации на Сервере. Если параметры авторизации не заданы, решение об авторизации принимается на стороне Сервера.

- `/regagent` <*режим*> — определяет, будет ли зарегистрирован Агент в списке установленных программ. Параметр <*режим*> может принимать следующие значения:

  - `yes` — зарегистрировать Агент в списке установленных программ.
  - `no` — не регистрировать Агент в списке установленных программ.

  Если ключ не задан, по умолчанию используется значение `no`.

- `/retry` <*количество*> — количество попыток поиска Сервера посредством отправки multicast-запросов. При отсутствии ответа от Сервера по истечении заданного количества попыток, считается, что Сервер не найден.

  Если ключ не задан, по умолчанию осуществляется 3 попытки поиска Сервера.

- `/server [`<*протокол*>`/]`<*адрес_сервера*>`[:`<*порт*>`]` — адрес Сервера, с которого будет осуществляться установка Агента и к которому после установки подключится Агент.

  Если ключ не задан, по умолчанию осуществляется поиск Сервера посредством отправки multicast-запросов.

- `/silent` <*режим*> — определяет, будет ли инсталлятор запущен в фоновом режиме. Параметр <*режим*> может принимать следующие значения:
  - `yes` — запускать инсталлятор в фоновом режиме.
  - `no` — запускать инсталлятор в графическом режиме.

  Если ключ не задан, по умолчанию установка Агента осуществляется в графическом режиме инсталлятора (см. **Руководство по установке**, п. Установка Агента Dr.Web при помощи инсталлятора).
- `/timeout` <*время*> — предельное время ожидания каждого ответа при поиске Сервера. Задается в секундах. Прием ответных сообщений продолжается, пока время ожидания ответа не превышает значение таймаута.

  Если ключ не задан, по умолчанию используется значение 3 секунды.

32. Агент Dr.Web для Windows

Формат команды запуска:

`es-service.exe [`<*ключи*>`]`

Ключи

Каждый из ключей может задаваться в одном из следующих форматов (форматы равнозначны):

`-`<*короткий_ключ*>`[ `<*аргумент*>`]`

или

`--`<*длинный_ключ*>`[=`<*аргумент*>`]`

Ключи могут использоваться одновременно, в том числе короткие и длинные версии.

Если аргумент содержит пробелы, он должен быть заключен в кавычки.

Все ключи выполняются вне зависимости от прав, разрешенных для станции на Сервере. Т. е. даже если права для изменение настроек Агента запрещены на Сервере, вы можете изменить эти настройки при помощи ключей командной строки.

Допустимые ключи:

- Показать справку:
  - `-?`
  - `--help`
- Изменить адрес Сервера, к которому подключается Агент:

- `-e <Сервер>`
- `--esserver=<Сервер>`

Чтобы задать сразу несколько Серверов, необходимо повторить через пробел ключ для каждого адреса Сервера, например:

```
es-service -e 192.168.1.1:12345 -e 192.168.1.2:12345 -e 10.10.1.1:1223
```

или

```
es-service --esserver=10.3.1.1:123 --esserver=10.3.1.2:123 --
esserver=10.10.1.1:123
```

- Добавить открытый ключ шифрования:
  - `-p <ключ>`
  - `--addpubkey=<ключ>`

  Открытый ключ, указанный в качестве аргумента, копируется в каталог Агента (по умолчанию это каталог `%ProgramFiles%\DrWeb`), переименовывается в `drwcsd.pub` (если имя отличалось) и перечитывается сервисом. При этом предыдущий файл открытого ключа, если таковой был найден, переименовывается в `drwcsd.pub.old` и в дальнейшем не используется.

  Все открытые ключи, использованные ранее (ключи, которые были переданы с Сервера и хранятся в реестре), остаются и продолжают использоваться.
- Добавить сертификат Сервера:
  - `-c <сертификат>`
  - `--addcert=<сертификат>`

  Файл сертификата Сервера, указанный в качестве аргумента, копируется в каталог Агента (по умолчанию это каталог `%ProgramFiles%\DrWeb`), переименовывается в `drwcsd-certificate.pem` (если имя отличалось) и перечитывается сервисом. При этом предыдущий файл сертификата, если таковой был найден, переименовывается в `drwcsd-certificate.pem.old` и в дальнейшем не используется.

  Все сертификаты, использованные ранее (сертификаты, которые были переданы с Сервера и хранятся в реестре), остаются и продолжают использоваться.
- Переподключиться к Серверу в качестве новичка:
  - `-w <значение>`
  - `--newbie=<значение>`

  Допустимые значения: `once, always`. При заданном значении `always` при каждом последующем запуске сервиса параметры авторизации Агента будут сбрасываться, в результате чего Агент каждый раз будет подключаться к Серверу в качестве новичка (подробнее см. **Руководство администратора**, п. Политика подключения станций). При заданном значении `once` при следующем запуске сервиса параметры авторизации Агента на Сервере будут сброшены, после чего произойдет однократное подключение Агента к Серверу в качестве новичка.
- Изменить уровень детализации журнала Агента:

- `--change-loglevel=<уровень>`

  Допустимые значения уровня детализации журнала: `err`, `wrn`, `inf`, `dbg`, `all`. Данная команда запускается только с правами администратора. Не требует выключения самозащиты, ручного перезапуска сервиса или ОС.

33. Сервер Dr.Web

Существует несколько вариантов команд запуска Сервера, для удобства они описываются отдельно.

Команды, приведенные в пп. 33.1. Управление Сервером Dr.Web — 33.5. Резервное копирование критичных данных Сервера Dr.Web, являются кроссплатформенными: могут быть использованы как под ОС Windows, так и под ОС семейства UNIX, если не указано обратное.

В случае возникновения ошибок при запуске команд управления Сервером обратитесь к файлу журнала Сервера для поиска возможных причин (см. **Руководство администратора**, п. Журнал работы Сервера Dr.Web).

33.1. Управление Сервером Dr.Web

`drwcsd [<ключи>]` — задать настройки работы Сервера (ключи подробнее описываются ниже).

33.2. Базовые команды

- `drwcsd restart` — сделать полный перезапуск службы Сервера (выполняется как пара `stop` и затем `start`).
- `drwcsd start` — запустить Сервер.
- `drwcsd stop` — нормально завершить работу Сервера.
- `drwcsd stat` — вывод в файл журнала статистики работы: время CPU, использование памяти и т. п. (под ОС семейства UNIX — аналог команды `send_signal WINCH` или `kill SIGWINCH`).
- `drwcsd verifyakey <полное_имя_файла_ключа>` — проверка корректности файла лицензионного ключа (`agent.key`).
- `drwcsd verifyekey <полное_имя_файла_ключа>` — проверка корректности файла лицензионного ключа Сервера (`enterprise.key`). Обратите внимание, лицензионный ключ Сервера более не используется, начиная с версии 10.
- `drwcsd verifyconfig <полное_имя_файла_конфигурации>` — проверка синтаксиса конфигурационного файла Сервера (`drwcsd.conf`).
- `drwcsd verifycache` — проверка корректности содержимого файлового кеша Сервера.

33.3. Команды для управления базой данных

Инициализация базы данных

При инициализации база данных должна отсутствовать или быть пуста.

`drwcsd [<ключи>] initdb [<лицензионный_ключ>|- [<sql_скрипт>|- [<ini_файл>|- [<пароль> [<lua-скрипт>|-]]]]]` — инициализация базы данных.

- *<лицензионный_ключ>* — путь к лицензионному ключу Dr.Web `agent.key`. Если лицензионный ключ не указан, его нужно будет добавить позже из Центра управления, либо получить по межсерверной связи у соседнего Сервера.
- *<sql_скрипт>* — путь к sql-скрипту для инициализации физической структуры БД.
- *<ini_файл>* — предварительно сформированный файл в формате `drweb32.ini`, который будет задавать начальную конфигурацию компонентов ПО Dr.Web (для группы **Everyone**).
- *<пароль>* — начальный пароль администратора Сервера (имя **admin**). По умолчанию **root**.
- *<lua-скрипт>* — путь к Lua-скрипту для инициализации БД (наполнение базы значениями по умолчанию).

Специальное значение "-" (минус) означает не использовать этот параметр.

Знак минус может опускаться, если следующие за ним параметры отсутствуют.

Задание параметров инициализации базы данных

При использовании встроенной БД параметры инициализации могут задаваться через внешний файл. Для этого служит команда:

`drwcsd.exe initdbex` *<response-file>*

<response-file> — файл, в котором записаны параметры инициализации БД, построчно, в том же порядке что и параметры команды `initdb`.

Формат файла:

```
<полное_имя_файла_лицензионного_ключа>

<полное_имя_файла_sql_скрипта>

<полное_имя_ini_файла>
```

```
<пароль_администратора>
```

При использовании под ОС Windows response-файла возможно использование любых символов в пароле администратора.

Хвостовые строки, следующие за необходимым в конкретном случае параметром, необязательны. Если строка представляет собой "-" (один знак минуса), то используется значение по умолчанию (как в `initdb`).

Обновление базы данных

`drwcsd [`*ключи*`] updatedb` *скрипт* — произвести какую-либо манипуляцию с базой данных (например, обновление при смене версии), выполнив SQL- или Lua-скрипт из указанного файла.

Обновление версии базы данных

`drwcsd upgradedb [`*каталог*`]` — запустить Сервер для обновления структуры базы данных при переходе на новую версию из указанного каталога (см. каталог `update-db`) или через внутренние скрипты.

Экспорт базы данных

a) `drwcsd exportdb` *файл* — экспорт базы данных в указанный файл.

Пример для ОС Windows:

```
C:\Program Files\DrWeb Server\bin\drwcsd.exe -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all exportdb "C:\Program Files\DrWeb Server\esbase.es"
```

Под ОС семейства **UNIX** действие выполняется от имени пользователя `drwcs:drwcs` в каталог `$DRWCS_VAR` (кроме ОС **FreeBSD**, которая по умолчанию сохраняет файл в директорию, из которой запущен скрипт; если указать путь явно, то директория должна быть с правами на запись для *пользователя*`:`*группы*, которые были созданы при установке, по умолчанию — `drwcs:drwcs`).

b) `drwcsd xmlexportdb` *xml-файл* — экспорт базы данных в указанный xml-файл.

Если указать расширение файла `gz`, то при экспорте файл базы данных будет упакован в архив gzip.

Если расширение не указать или указать расширение, отличное от `gz`, то файл экспорта не будет архивироваться.

Пример для ОС Windows:

- Для экспорта базы данных в xml-файл без сжатия:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" "-home=C:\Program
Files\DrWeb Server" "-bin-root=C:\Program Files\DrWeb Server" "-var-
root=C:\Program Files\DrWeb Server\var" -verbosity=ALL -rotate=10,10m -
log=export.log xmlexportdb database.db
```

- Для экспорта базы данных в xml-файл, упакованный в архив:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" "-home=C:\Program
Files\DrWeb Server" "-bin-root=C:\Program Files\DrWeb Server" "-var-
root=C:\Program Files\DrWeb Server\var" -verbosity=ALL -rotate=10,10m -
log=export.log xmlexportdb database.gz
```

Пример для ОС семейства UNIX:

- Для экспорта базы данных в xml-файл без сжатия:

```
/etc/init.d/drwcsd xmlexportdb /es/database.db
```

- Для экспорта базы данных в xml-файл, упакованный в архив:

```
/etc/init.d/drwcsd xmlexportdb /es/database.gz
```

Импорт базы данных

a) `drwcsd importdb` <*файл*> — импорт базы данных из указанного файла (старое содержимое БД стирается).

b) `drwcsd upimportdb` <*файл*> `[`<*каталог*>`]` — импорт и обновление базы данных, полученной при экспорте с Сервера предыдущих версий (старое содержимое БД стирается). Также можно указать путь до каталога со скриптами для обновления структуры базы данных при переходе на новую версию (аналогично команде `upgradedb`).

c) `drwcsd xmlimportdb` <*xml-файл*> — импорт базы данных из указанного xml-файла.

d) `drwcsd xmlupimportdb` <*xml-файл*> `[`<*каталог*>`]` — импорт и обновление базы данных, полученной при xml-экспорте с Сервера предыдущих версий. Также можно указать путь до каталога со скриптами для обновления структуры базы данных при переходе на новую версию (аналогично команде `upgradedb`).

e) `drwcsd xmlimportdbnh` <*xml-файл*> — импорт базы данных из указанного xml-файла без учета хеша. Может использоваться, например, если xml-файл базы данных правился вручную, и хеш файла, записанный автоматически при экспорте, стал неактуальным.

Перед использованием команд `upimportdb` и `xmlupimportdb` необходимо выполнить резервное копирование базы данных.

Любые проблемы в процессе выполнения данных команд могут привести к удалению всей информации из базы данных.

Использование команд `upimportdb` и `xmlupimportdb` для импорта с обновлением версии базы данных возможно только в пределах одной СУБД.

Дамп экспорта базы данных

`drwcsd [<ключи>] dumpimportdb <файл_БД> [<файл_SQL> [<фильтр_таблиц>]]` — записать в файл журнала Сервера или SQL-файл подробную информацию о встроенной или внешней базе данных.

Импорт и экспорт базы данных при выполнении команды `dumpimportdb` не производится.

- *<файл_БД>* — файл экспорта базы данных, информация о которой будет записана в журнал Сервера или в *<файл_SQL>*. Файл экспорта может быть получен при помощи команды `exportdb`; также возможно использование файла, полученного при резервном копировании базы данных. XML-файл, полученный при помощи команды `xmlexportdb` не принимается.
- *<файл_SQL>* — файл для записи всех SQL-запросов, которые будут выполняться в случае импорта базы данных из файла, указанного в *<файл_БД>*. Если SQL-файл не указан, запись осуществляется в журнал Сервера (в виде списка таблиц и их полей). Если файл указан - то только в SQL-файл.
- *<фильтр_таблиц>* — список таблиц базы данных, информация о которых будет выведена в *<файл_SQL>*. Список таблиц необходимо указывать через запятую. Названия должны соответствовать названиям таблиц в базе данных. Например: `admins,groups,stations`. Фильтр таблиц действителен только при выводе в SQL-файл. Если список таблиц не указан, выводятся все таблицы.

Проверка базы данных

`drwcsd verifydb` — запустить Сервер для проверки базы данных. Для записи информации о результатах в файл журнала следует вводить команду с ключом `-log`. Подробно особенности использования данного ключа описаны в п. 33.8. Описание ключей.

Ускорение базы данных

`drwcsd [<ключи>] speedupdb` — выполнить команды `VACUUM`, `CLUSTER`, `ANALYZE` для ускорения работы с БД.

Восстановление базы данных

`drwcsd repairdb` — выполнить восстановление поврежденного образа встроенной базы данных **SQLite3** или поврежденных таблиц внешней базы данных **MySQL**.

Восстановление **SQLite3** также может выполняться автоматически при запуске Сервера, если в настройках базы данных **SQLite3** в Центре управления установлен флаг **Восстанавливать поврежденный образ автоматически** (см. **Руководство администратора**, п. Восстановление базы данных).

Очистка базы данных

`drwcsd cleandb` — очистить базу данных Сервера, удалив все таблицы.

33.4. Команды для управления репозиторием

Перед запуском команд `syncrepository`, `restorerepo` и `saverepo` необходимо обязательно остановить Сервер.

- `drwcsd syncrepository` — произвести синхронизацию репозитория с ВСО Dr.Web. Команда запускает процесс Сервера, при этом происходит обращение к ВСО и последующее обновление репозитория в случае наличия обновлений.
- `drwcsd rerepository` — перечитать репозиторий с диска.
- `drwcsd updrepository` — обновить репозиторий с ВСО Dr.Web. Команда отправляет сигнал работающему процессу Сервера для обращения к ВСО и последующего обновления репозитория в случае наличия обновлений. Если Сервер не запущен, обновление репозитория не осуществляется.
- `drwcsd [<ключи>] restorerepo <полное_имя_архива>` — восстановить репозиторий Сервера из заданного zip-архива, созданного при помощи команды `saverepo`.
- `drwcsd [<ключи>] saverepo <полное_имя_архива>` — сохранить весь репозиторий Сервера в указанный zip-архив. Полученный архив может быть импортирован на Сервер при помощи команды `restorerepo`.

Архивы, используемые командами `restorerepo` и `saverepo`, не совместимы с архивами, используемыми для экспорта и импорта репозитория через Центр управления.

33.5. Резервное копирование критичных данных Сервера Dr.Web

Резервная копия критичных данных Сервера (лицензионных ключей, содержимого базы данных, закрытого ключа шифрования, конфигурации Сервера и Центра управления) создается с помощью следующей команды:

`drwcsd -home=<путь> backup [<каталог> [<количество>]]`

- Критичные данные Сервера копируются в указанный *<каталог>*.
- Ключ `-home` задает каталог установки Сервера.
- Параметр *<количество>* — количество сохраняемых копий одного и того же файла.

Пример для ОС Windows:

```
C:\Program Files\DrWeb Server\bin>drwcsd -home="C:\Program Files\DrWeb
Server" backup C:\a
```

Все файлы из резервной копии, кроме содержимого базы данных, готовы к использованию. Резервная копия базы данных сохраняется в формате `.gz`, совместимом с `gzip` и другими архиваторами. Содержимое базы данных можно импортировать из резервной копии в рабочую базу данных Сервера и таким образом восстановить данные (см. п. Восстановление базы данных Dr.Web Enterprise Security Suite).

В процессе работы Сервер Dr.Web регулярно сохраняет резервные копии важной информации в следующих каталогах:

- для ОС **Windows**: *<диск_установки>*`:\DrWeb Backup`
- для ОС **Linux**: `/var/opt/drwcs/backup`
- для ОС **FreeBSD**: `/var/drwcs/backup`

Для выполнения функции резервного копирования в расписание Сервера включено ежедневное задание. Если такое задание в расписании отсутствует, рекомендуется создать его.

33.6. Команды, доступные только под ОС Windows

- `drwcsd [<ключи>] install [<имя_сервиса>]` — установить службу Сервера в системе и назначить заданные ключи для запуска этой службы.

  <имя_сервиса> — суффикс, который добавляется к названию службы по умолчанию, при этом полное имя службы: `DrWebES-`*<имя_сервиса>*. Команда `install` создает (редактирует) службу с заданным именем и автоматически дописывает в ее аргументы ключ `-service=`*<имя_сервиса>*. Существующие службы при этом остаются без изменений.

- `drwcsd uninstall [<имя_сервиса>]` — удалить службу Сервера из системы.

  <имя_сервиса> — суффикс, который добавляется к названию службы по умолчанию, при этом полное имя службы: `DrWebES-<имя_сервиса>`.
- `drwcsd kill` — аварийно завершить службу Сервера (в случае, если нормально не удалось). Данную команду не рекомендуется использовать без крайней необходимости.
- `drwcsd reconfigure` — перечитать конфигурационный файл и перезапуститься (выполняется быстрее — без старта нового процесса).
- `drwcsd silent [<опции>] <команда>` — запретить вывод сообщений от Сервера при запуске команды, заданной в параметре *<команда>*. Используется в частности в командных файлах для отключения интерактивности работы Сервера.
- `drwcsd syncads` — синхронизировать структуру сети: контейнеры Active Directory, содержащие компьютеры, становятся группами антивирусной сети, в которые помещаются рабочие станции.

33.7. Команды, доступные только под ОС семейства UNIX

- `drwcsd config` — аналог команды `reconfigure` или `kill SIGHUP` — перезапуск Сервера.
- `drwcsd interactive` — запускает Сервер, но не передает управление процессу.
- `drwcsd newkey` — генерация новых ключей шифрования `drwcsd.pri` и `drwcsd.pub`, а также сертификата `drwcsd-certificate.pem`.
- `drwcsd readrepo` — перечитать репозиторий с диска. Аналогично команде `rerepository`.
- `drwcsd selfcert [<имя_компьютера>]` — генерация нового сертификата SSL `(certificate.pem)` и закрытого ключа RSA `(private-key.pem)`. Параметр задает имя компьютера с установленным Сервером, для которого будут генерироваться файлы. Если параметр не задан, имя компьютера подставляется автоматически системной функцией.
- `drwcsd shell <имя_файла>` — запуск файла скрипта. Команда запускает `$SHELL` либо `/bin/sh`, передавая ему указанный файл.
- `drwcsd showpath` — показать все пути программы, прописанные в системе.
- `drwcsd status` — показать текущий статус Сервера (запущен, остановлен).

33.8. Описание ключей

Кроссплатформенные ключи:

- `-activation-key=<лицензионный_ключ>` — лицензионный ключ Сервера. По умолчанию файл `enterprise.key`, расположенный в подкаталоге `etc` корневого каталога.

Обратите внимание, лицензионный ключ Сервера более не используется, начиная с версии 10. Ключ `-activation-key` может использоваться при обновлении Сервера с предыдущих версий и при инициализации базы данных: идентификатор Сервера будет взят из указанного лицензионного ключа.

- `-bin-root=<`*каталог*`>` — путь к исполняемым файлам. По умолчанию подкаталог `bin` корневого каталога.
- `-conf=<`*файл*`>` — имя и расположение конфигурационного файла Сервера. По умолчанию файл `drwcsd.conf` в подкаталоге `etc` корневого каталога.
- `-daemon` — для Windows-платформ означает запуск как службы; для платформ UNIX: "демонизация процесса" (перейти в корневой каталог, отсоединиться от терминала и перейти в фоновый режим).
- `-db-verify=on` — при запуске Сервера выполнять проверку целостности БД. Значение по умолчанию. Настоятельно не рекомендуется запускать с явным указанием противоположного значения, за исключением запуска немедленно после проверки БД командой `drwcsd verifydb`, см. выше.
- `-help` — выдать справку. Аналогично описанным выше программам.
- `-hooks` — разрешить выполнение Сервером пользовательских скриптов расширения, находящихся в папке:
  - для ОС Windows: `var\extensions`
  - для ОС FreeBSD: `/var/drwcs/extensions`
  - для ОС Linux: `/var/opt/drwcs/extensions`

  каталога установки Сервера Dr.Web. Скрипты предназначены для автоматизации работы администратора, упрощая и ускоряя выполнение некоторых заданий. Все скрипты по умолчанию отключены.
- `-home=<`*каталог*`>` — каталог установки Сервера (корневой каталог). Структура данного каталога описана в **Руководстве по установке**, п. Установка Сервера Dr.Web для ОС Windows. По умолчанию текущий каталог при запуске.
- `-log=<`*файл_журнала*`>` — активировать ведение журнала Сервера в файл по указанному пути.

  Для Сервера на платформах UNIX вместо имени файла может использоваться "минус", что означает выводить журнал на стандартный вывод.

  По умолчанию: для ОС Windows — `drwcsd.log` в каталоге, указываемом ключом `-var-root`, для ОС семейства UNIX задается ключом `-syslog=user` (см. ниже).
- `-private-key=<`*закрытый_ключ*`>` — закрытый ключ шифрования Сервера. По умолчанию `drwcsd.pri` в подкаталоге `etc` корневого каталога.
- `-rotate=<`*N*`><`*f*`>,<`*M*`><`*u*`>` — режим ротации журнала работы Сервера, где:

Параметр	Описание
<*N*>	Общее количество файлов журнала (включая текущий и архивные).
<*f*>	Формат хранения файлов журнала, возможные значения:

Параметр	Описание
	• z (gzip) — сжимать файлы, используется по умолчанию, • p (plain) — не сжимать файлы.
<*M*>	Размер файла журнала либо время ротации, в зависимости от значения <*u*>;
<*u*>	Единица измерения, возможные значения: • для задания ротации по размеру файла журнала: ▫ k — Кб, ▫ m — Мб, ▫ g — Гб. • для задания ротации по времени: ▫ H — часы, ▫ D — дни, ▫ W — недели.

При задании ротации по времени осуществляется синхронизация вне зависимости от времени запуска команды: для значения H — синхронизация с началом часа, для D — с началом суток, для W — с началом недели (00:00 в понедельник) согласно кратности, указанной в параметре <*u*>.

Начальная точка отсчета — 01 января 01 года н.э., UTC+0.

По умолчанию `10,10m`, что означает хранить 10 файлов по 10 мегабайт, использовать сжатие. Можно также использовать специальный формат `none (-rotate=none)` — это означает "не использовать ротацию, а писать всегда в один и тот же файл неограниченного размера".

При использовании режима ротации используется следующий формат именования файлов: `file.`<*N*>`.log` или `file.`<*N*>`.log.gz`, где <*N*> — порядковый номер: 1, 2, и т. д.

Например, пусть имя файла журнала (см. выше ключ `-log`) задано `file.log`. Тогда:

- `file.log` — текущий файл (в который идет запись),
- `file.1.log` — предыдущий,
- `file.2.log` и так далее — чем больше число, тем более старая версия.

- `-trace` — детально протоколировать место возникновения ошибки.
- `-var-root=`<*каталог*> — путь к каталогу, в который Сервер имеет право записи и который предназначен для хранения изменяемых файлов (например, журналов, а также файлов репозитория). По умолчанию подкаталог `var` корневого каталога.
- `-verbosity=`<*уровень*> — уровень детализации журнала. По умолчанию `WARNING`. Допустимые значения: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Значения `ALL` и `DEBUG3` — синонимы.

При необходимости можно задавать определенные уровни детализации сразу для нескольких источников сообщений в следующем формате:

`-verbosity=<`*источник_сообщения1*`>:<`*уровень1*`>,<`*источник_сообщения2*`>:<`*уровень2*`>,<`*источник_сообщения3*`>:<`*уровень3*`>` и т. д. При этом `<`*уровень*`>` наследуется по общему принципу, т.е. находится ближайший родительский источник с заданным уровнем детализации. Ключ формата `-verbosity=all:all` равносилен ключу `-verbosity=all` (см. также Приложение Л. Формат файлов журнала).

Данный ключ определяет степень подробности записи журнала в файл, заданный следующим после него ключом `-log` (см. выше). В одной команде может быть несколько ключей данного типа.

Ключи `-verbosity` и `-log` позиционно-зависимы.

При использовании этих ключей одновременно, ключ `-verbosity` должен идти перед ключом `-log`: ключ `-verbosity` переопределяет уровень детализации журналов, расположенных по путям, следующим далее в командной строке.

Ключи, доступные только под ОС Windows:

- `-minimized` — минимизировать окно (только если запуск не как службы, а интерактивно).
- `-service=<`*имя_сервиса*`>` — ключ используется запущенным процессом службы для самоидентификации и установки самозащиты на ветку реестра службы Сервера. `<`*имя_сервиса*`>` — суффикс, который добавляется к названию службы по умолчанию, при этом полное имя службы: `DrWebES-<`*имя_сервиса*`>`.

  Ключ используется командой `install`, самостоятельное использование не предусмотрено.
- `-screen-size=<`*размер*`>` — (только если запуск не как службы, а интерактивно) — размер в строках видимого журнала в окне Сервера, по умолчанию 1000.

Ключи, доступные только под ОС семейства UNIX:

- `-etc=<`*путь*`>` — путь к директории `etc` (`<var>/etc`).
- `-keep` — не удалять содержимое временного каталога после установки Сервера.
- `-pid=<`*файл*`>` — файл, в который Сервер записывает идентификатор своего процесса.
- `-syslog=<`*режим*`>` — протоколирование в системный журнал. Возможные режимы: `auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, local0-local7` и для некоторых платформ — `ftp, authpriv` и `console`.

Ключи `-syslog` и `-log` работают совместно. Т. е. при запуске Сервера с ключом `-syslog` (например, `service drwcsd start -syslog=user`), Сервер запустится с

заданным значением для ключа `-syslog` и со значением по умолчанию для ключа `-log`.

- `-user=<пользователь>`, `-group=<группа>` — доступны только для ОС UNIX, при запуске от имени пользователя **root**; означают изменить пользователя или группу процесса и выполняться с правами указанного пользователя (группы).

33.9. Переменные, доступные под ОС семейства UNIX

Для облегчения управления Сервером под ОС семейства UNIX администратору предоставляются переменные, которые располагаются в файле скрипта, хранящегося в следующем каталоге:

- Для ОС Linux: `/etc/init.d/drwcsd`.
- Для ОС FreeBSD: `/usr/local/etc/rc.d/drwcsd` (символьная ссылка на `/usr/local/etc/drweb.com/software/init.d/drwcsd`).

Соответствие между переменными и ключами командной строки для `drwcsd` приведено в Таблице 3-1.

Таблица 3-1.

Ключ	Переменная	Параметры по умолчанию
`-home`	DRWCS_HOME	• `/usr/local/drwcs` — для ОС FreeBSD, • `/opt/drwcs` — для ОС Linux.
`-var-root`	DRWCS_VAR	• `/var/drwcs` — для ОС FreeBSD, • `/var/opt/drwcs` — для ОС Linux.
`-etc`	DRWCS_ETC	`$DRWCS_VAR/etc`
`-rotate`	DRWCS_ROT	`10,10m`
`-verbosity`	DRWCS_LEV	`info`
`-log`	DRWCS_LOG	`$DRWCS_VAR/log/drwcsd.log`
`-conf`	DRWCS_CFG	`$DRWCS_ETC/drwcsd.conf`
`-pid`	DRWCS_PID	
`-user`	DRWCS_USER	
`-group`	DRWCS_GROUP	
`-hooks`	DRWCS_HOOKS	
`-trace`	DRWCS_TRACE	

Переменные DRWCS_HOOKS и DRWCS_TRACE не имеют параметров. При задании переменных соответствующие ключи добавляются при исполнении скрипта. Если переменные не заданы, ключи не будут добавлены.

Прочие переменные приведены в Таблице 3-2.

Таблица 3-2.

Переменная	Параметры по умолчанию	Описание
DRWCS_ADDOPT		Дополнительные ключи командной строки, которые должны быть переданы drwcsd при запуске.
DRWCS_CORE	unlimited	Максимальный размер core-файла.
DRWCS_FILES	131170	Максимальное число файловых дескрипторов, которое сможет открыть Сервер.
DRWCS_BIN	$DRWCS_HOME/bin	Директория, из которой будет запускаться drwcsd.
DRWCS_LIB	$DRWCS_HOME/lib	Директория с библиотеками Сервера.

Значения параметров по умолчанию вступают в силу, если такие переменные не определены в скрипте drwcsd.

Переменные DRWCS_HOME, DRWCS_VAR, DRWCS_ETC, DRWCS_USER, DRWCS_GROUP, DRWCS_HOOKS уже определены в файле скрипта drwcsd.

Если существует файл /var/opt/drwcs/etc/common.conf, то этот файл будет включен в drwcsd, что может переопределить некоторые переменные, однако, если их не экспортировать (при помощи команды export), то они не окажут влияния.

Чтобы задать переменные

1. Добавьте определение переменной в файле скрипта drwcsd.
2. Экспортируйте переменную при помощи команды export (задается там же).
3. При запуске еще одного процесса из этого скрипта, этот процесс считает значения, которые были определены.

33.10. Управление Сервером Dr.Web под ОС семейства UNIX при помощи команды kill

Сервер под ОС UNIX управляется сигналами, посылаемыми процессу Сервера утилитой `kill`.

Подробная справка об утилите `kill` может быть получена при помощи команды `man kill`.

Сигналы утилиты и производимые ими действия:

- `SIGWINCH` — вывод в файл журнала статистики работы (время CPU, использование памяти и т. п.),
- `SIGUSR1` — перечитывание репозитория с диска,
- `SIGUSR2` — перечитывание шаблонов сообщений с диска,
- `SIGHUP` — перезапуск Сервера,
- `SIGTERM` — останов Сервера,
- `SIGQUIT` — останов Сервера,
- `SIGINT` — останов Сервера.

Аналогичные действия для Сервера под ОС Windows реализуются при помощи ключей команды drwcsd, см. Приложение 33.3. Команды для управления базой данных.

34. Сканер Dr.Web для Windows

Данный компонент ПО рабочей станции имеет параметры командной строки, описанные в руководстве пользователя **Агент Dr.Web для Windows**. Единственное отличие состоит в том, что при запуске Сканера Агентом параметры `/go /st` передаются Сканеру автоматически и в обязательном порядке.

35. Прокси-сервер Dr.Web

Для настройки параметров Прокси-сервера запустите с соответствующими ключами исполняемый файл `drwcsd-proxy`, который находится в подкаталоге `bin` каталога установки Прокси-сервера.

Формат команды запуска

`drwcsd-proxy [<ключи>] [<команды> [<аргументы_команд>]]`

Допустимые ключи

Кроссплатформенные ключи:

- `--console=yes|no` — запустить Прокси-сервер в интерактивном режиме. При этом журнал работы Прокси-сервера выводится в консоль.

  По умолчанию: `no`.

- `--etc-root=`*<путь>* — путь к каталогу с конфигурационными файлами (`drwcsd-proxy.conf`, `drwcsd.proxy.auth` и т. д.).

  По умолчанию: `$var/etc`

- `--home=`*<путь>* — путь к каталогу установки Прокси-сервера.

  По умолчанию: `$exe-dir/`

- `--log-root=`*<путь>* — путь к каталогу с файлами журнала работы Прокси-сервера.

  По умолчанию: `$var/log`

- `--pool-size=`*<N>* — количество потоков для работы с клиентами.

  По умолчанию: количество ядер компьютера, на котором установлен Прокси-сервер (но не меньше 2).

- `--rotate=`*<N><f>,<M><u>* — режим ротации журнала работы Прокси-сервера, где:

Параметр	Описание
<N>	Общее количество файлов журнала (включая текущий и архивные).
<f>	Формат хранения файлов журнала, возможные значения: • z (gzip) — сжимать файлы, используется по умолчанию, • p (plain) — не сжимать файлы.
<M>	Размер файла журнала либо время ротации, в зависимости от значения *<u>*;

<u>	Единица измерения, возможные значения:
	• для задания ротации по размеру файла журнала:
	  ▫ k — Кб,
	  ▫ m — Мб,
	  ▫ g — Гб.
	• для задания ротации по времени:
	  ▫ H — часы,
	  ▫ D — дни,
	  ▫ W — недели.

При задании ротации по времени осуществляется синхронизация вне зависимости от времени запуска команды: для значения H — синхронизация с началом часа, для D — с началом суток, для W — с началом недели (00:00 в понедельник) согласно кратности, указанной в параметре <*u*>.

Начальная точка отсчета — 01 января 01 года н.э., UTC+0.

По умолчанию `10,10m`, что означает хранить 10 файлов по 10 мегабайт, использовать сжатие.

- `--trace=yes|no` — включить детальное протоколирование обращений к Прокси-серверу. Доступно только если сборка Прокси-сервера поддерживает детальное протоколирование стека вызовов (в случае возникновения исключения, стек пишется в журнал).

  По умолчанию: `no`.

- `--tmp-root=`<*путь*> — путь к каталогу с временными файлами. Используется при автоматическом обновлении Прокси-сервера.

  По умолчанию: `$var/tmp`.

- `--var-root=`<*путь*> — путь к рабочему каталогу Прокси-сервера для хранения кеша и базы данных.

  По умолчанию:

  - ОС Windows: `%ALLUSERSPROFILE%\Doctor Web\drwcs`
  - ОС Linux: `/var/opt/drwcs`
  - ОС FreeBSD: `/var/drwcs`

- `--verbosity=`<*уровень_подробности*> — уровень детализации журнала. По умолчанию `TRACE`. Допустимые значения: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Значения `ALL` и `DEBUG3` — синонимы.

  При необходимости можно задавать определенные уровни детализации сразу для нескольких источников сообщений в следующем формате:

  `-verbosity=`<*источник_сообщения1*>`:`<*уровень1*>`,`<*источник_сообщения2*>`:`<*уровень2*>`,`<*источник_сообщения3*>`:`<*уровень3*> и т. д. При этом <*уровень*> наследуется по общему принципу, т.е. находится ближайший родительский источник с заданным уровнем детализации. Ключ формата `-verbosity=all:all` равносилен ключу `-verbosity=all` (см. также Приложение Л. Формат файлов журнала).

Все ключи для задания параметров работы Прокси-сервера могут быть указаны одновременно.

Ключи под ОС семейства UNIX:

- `--user` — задать идентификатор пользователя. Ключ актуален как для работы в обычном режиме, так и для работы в режиме демона.

- `--group` — задать идентификатор группы. Ключ актуален как для работы в обычном режиме, так и для работы в режиме демона.
- `--pid=<путь>` — путь к каталогу с идентификатором процесса.

  По умолчанию: `/var/opt/drwcs/run/drwcsd-proxy.pid`

Допустимые команды и их аргументы

Если команда не указана, по умолчанию используется команда `run`.

- `import <путь> [<ревизия>] [<продукты>]` — импортировать файлы из репозитория Dr.Web Сервера в кеш Прокси-сервера.
  - *<путь>* — путь к каталогу с репозиторием Сервера Dr.Web. Репозиторий Сервера должен быть предварительно скачан на компьютер с установленным Прокси-сервером.
  - *<ревизия>* — максимальное количество ревизий, которые нужно импортировать. Если значение не указано, будут импортированы все ревизии.
  - *<продукты>* — список продуктов через пробел, которые нужно импортировать. По умолчанию используется пустой список, т. е. импортировать все продукты репозитория, кроме Сервера Dr.Web. Если задан список, то импортируются только продукты из списка.
- `help` — вывести справку по ключам для настройки Прокси-сервера.
- `run` — запустить Прокси-сервер в обычном режиме.

Команды, доступные только для ОС Windows:

- `install` — установить сервис.
- `start` — запустить установленный сервис.
- `stop` — остановить запущенный сервис.
- `uninstall` — удалить сервис.

Команды, доступные только для ОС семейства UNIX:

- `daemon` — запустить Прокси-сервер в режиме демона (см. также Ключи под ОС семейства UNIX).

Скрипт управления Прокси-сервером и переменные, доступные под ОС семейства UNIX

Для облегчения управления Прокси-сервером под ОС семейства UNIX администратору предоставляются переменные, которые располагаются в файле скрипта `drwcsd-proxy.sh`, расположенного в следующем каталоге:

- **Linux**: `/etc/init.d/dwcp_proxy`
- **FreeBSD**: `/usr/local/etc/rc.d/dwcp_proxy`

Скрипт принимает следующие команды:

- `import <путь> [<ревизия>] [<продукты>]` — импортировать файлы из репозитория Dr.Web Сервера в кеш Прокси-сервера (аналогично команде Прокси-сервера — см. выше).
- `interactive` — запустить Прокси-сервер в интерактивном режиме. При этом журнал работы Прокси-сервера выводится в консоль.
- `start` — запустить Прокси-сервер в режиме демона.
- `status` — проверить, запущен ли демон.
- `stop` — остановить запущенного демона.

Соответствие между переменными и ключами командной строки для `drwcsd-proxy` приведено в Таблице 3-3.

Таблица 3-3.

Ключ	Переменная	Параметры по умолчанию
`--home=<путь>`	`$DRWCS_PROXY_HOME`	`$exe-dir/`
`--var-root=<путь>`	`$DRWCS_PROXY_VAR`	• ОС Linux: `/var/opt/drwcs` • ОС FreeBSD: `/var/drwcs`
`--etc-root=<путь>`	`$DRWCS_PROXY_ETC`	`$var/etc`
`--tmp-root=<путь>`	`$DRWCS_PROXY_TMP`	`$var/tmp`
`--log-root=<путь>`	`$DRWCS_PROXY_LOG`	`$var/log`
–	`$DRWCS_PROXY_LIB`	`$DRWCS_PROXY_HOME/lib`
–	`$DRWCS_PROXY_BIN`	`$DRWCS_PROXY_HOME/bin`
`--verbosity=<уровень_подробности>`	`$DRWCS_PROXY_VERBOSITY`	`INFO`
`--rotate=<N><f>,<M><u>`	`$DRWCS_PROXY_ROTATE`	`10,10m`
`--pid`	`$DRWCS_PROXY_PID`	`/var/opt/drwcs/run/drwcsd-proxy.pid`
-	`$NO_DRWCS_PROXY_USER`	Если присвоено любое значение, то `$DRWCS_PROXY_USER` игнорируется.
`--user`	`$DRWCS_PROXY_USER`	–

Ключ	Переменная	Параметры по умолчанию
-	`$NO_DRWCS_PROXY_GROUP`	Если присвоено любое значение, то `$DRWCS_PROXY_GROUP` игнорируется.
`--group`	`$DRWCS_PROXY_GROUP`	–
-	`$DRWCS_PROXY_FILES`	131170, но не меньше текущего лимита.

36. Инсталлятор Сервера Dr.Web для ОС семейства UNIX

Формат команды запуска:

<название_пакета>`.run [<`*ключи*`>] [--] [<`*аргументы*`>]`

где:

- `[--]` — отдельностоящий необязательный знак, обозначающий конец списка ключей и отделяющий список ключей от списка дополнительных аргументов.
- `[<`*аргументы*`>]` — дополнительные аргументы или встроенные скрипты.

Ключи для получения справки или информации о пакете:

- `--help` — вывести справку по ключам.
- `--info` — вывести расширенную информацию о пакете: название; целевой каталог; размер в распакованном виде; алгоритм сжатия; дата упаковки; версия `makeself`, которым производилась упаковка; команда, которой производилась упаковка; скрипт, который будет запущен после распаковки; будет ли скопировано содержимое архива во временный каталог (если нет, ничего не выводится); является ли целевой каталог постоянным или будет удален после отработки скрипта.
- `--list` — вывести список файлов в установочном пакете.
- `--check` — проверить целостность установочного пакета.

Ключи для запуска пакета:

- `--confirm` — выводить запрос перед запуском встроенного скрипта.
- `--noexec` — не запускать встроенный скрипт.
- `--target <`*каталог*`>` — извлечь установочный пакет в указанный каталог.
- `--tar <`*аргумент_1*`> [<`*аргумент_2*`> ...]` — получить доступ к содержимому установочного пакета при помощи команды `tar`.

Дополнительные аргументы:

- `--help` — вывести справку по дополнительным аргументам.
- `--quiet` — запустить инсталлятор в фоновом режиме. На все следующие вопросы инсталлятора используется утвердительный ответ:
  - принять лицензионное соглашение,
  - задать резервное копирование в каталог по умолчанию,
  - продолжить установку при условии, что установленный в системе дополнительный дистрибутив (extra) будет удален.
- `--clean` — установить пакет с настройками Сервера по умолчанию без использования резервной копии для восстановления настроек предыдущей установки.
- `--preseed` <*путь*> — путь до конфигурационного файла, содержащего предопределенные ответы на вопросы инсталлятора во время установки.

  Переменные для задания предопределенных ответов в конфигурационном файле:
  - `DEFAULT_BACKUP_DIR=`<*путь*> — путь до каталога с резервной копией, которая будет использоваться для восстановления настроек предыдущей версии (не используется, если задана установка с настройками по умолчанию).
  - `QUIET_INSTALL=[0|1]` — определяет использование фонового режима инсталлятора:
    - 0 — запустить инсталлятор в фоновом режиме;
    - 1 — запустить инсталлятор в обычном режиме.
  - `CLEAN_INSTALL=[0|1]` — определяет использование резервной копии при установке:
    - 0 — установка с настройками по умолчанию без восстановления из резервной копии;
    - 1 — установка с восстановлением из резервной копии, расположенной в каталоге из переменной `DEFAULT_BACKUP_DIR`. Если переменная `DEFAULT_BACKUP_DIR` не задана, резервная копия берется из `/var/tmp/drwcs`.
  - `ADMIN_PASSWORD=`<*пароль*> — пароль для учетной записи администратора по умолчанию (**admin**).
    - Если переменная `ADMIN_PASSWORD` задана в файле, ее значение используется как пароль администратора и в конце установки выводится сообщение: `Password specified in the configuration file for the default administrator (admin):` <*пароль*>
    - Если переменная `ADMIN_PASSWORD` не задана в файле, то пароль генерируется автоматически и в конце установки выводится сообщение: `Automatically generated password for the default administrator (admin):` <*пароль*>

Если при использовании ключа `--preseed` в конфигурационном файле не определить запуск инсталлятора в фоновом режиме при помощи переменной `QUIET_INSTALL=0`, то значения остальных переменных конфигурационного файла будут переопределены пользователем в процессе установки.

37. Утилиты

37.1. Утилита генерации цифровых ключей и сертификатов

Предоставляются следующие версии консольной утилиты для генерации цифровых ключей и сертификатов:

Исполняемый файл	Расположение	Описание
`drweb-sign-<ОС>-<разрядность>`	Центр управления, раздел **Администрирование** → **Утилиты**	Независимая версия утилиты. Может запускаться из произвольного каталога и на любом компьютере с соответствующей операционной системой.
	Каталог Сервера `webmin/utilities`	
`drwsign`	Каталог Сервера `bin`	Версия утилиты зависит от наличия серверных библиотек. Может запускаться только из каталога своего расположения.

Версии утилиты `drweb-sign-<ОС>-<разрядность>` и `drwsign` аналогичны по функциональности. Далее в разделе приводится версия `drwsign`, однако все примеры актуальны для обеих версий.

Формат команды запуска

- `drwsign check [-public-key=<открытый_ключ>] <файл>`

  Проверить подпись указанного файла, используя открытый ключ субъекта, подписавшего данный файл.

Параметр ключа	Значение по умолчанию
<открытый_ключ>	`drwcsd.pub`

- `drwsign extract [-private-key=<закрытый_ключ>] [-cert=<сертификат_Сервера>] <открытый_ключ>`

  Извлечь открытый ключ из файла закрытого ключа или из файла сертификата и записать открытый ключ в указанный файл.

  Ключи `-private-key` и `-cert` взаимоисключающие, т. е. может быть задан только один из них; в случае задания обоих ключей одновременно команда завершится с ошибкой.

  Указания параметра для ключей обязательно.

  Если ни один ключ не задан, то будет использован `-private-key=drwcsd.pri` для извлечения открытого ключа из закрытого ключа `drwcsd.pri`.

Параметр ключа	Значение по умолчанию
<*закрытый_ключ*>	drwcsd.pri

- `drwsign genkey [`<*закрытый_ключ*>` [`<*открытый_ключ*>`]]`

  Сгенерировать пару открытый — закрытый ключ и записать их в соответствующие файлы.

Параметр ключа	Значение по умолчанию
<*закрытый_ключ*>	drwcsd.pri
<*открытый_ключ*>	drwcsd.pub

Версия утилиты для платформ Windows (в отличие от версии для ОС UNIX) никак не защищает закрытый ключ от копирования.

- `drwsign gencert [-private-key=`<*закрытый_ключ*>`] [-subj=`<*поля_субъекта*>`] [-days=`<*срок_действия*>`] [`<*самоподписанный_сертификат*>`]`

  Сгенерировать самоподписанный сертификат, используя закрытый ключ Сервера, и записать его в соответствующий файл.

Параметр ключа	Значение по умолчанию
<*закрытый_ключ*>	drwcsd.pri
<*поля_субъекта*>	/CN=<*имя_хоста*>
<*срок_действия*>	3560
<*самоподписанный_сертификат*>	drwcsd-certificate.pem

- `drwsign gencsr [-private-key=`<*закрытый_ключ*>`] [-subj=`<*поля_субъекта*>`] [`<*запрос_на_подпись_сертификата*>`]`

  Сгенерировать запрос на подпись сертификата на основе закрытого ключа и записать этот запрос в соответствующий файл.

  Может быть использовано для подписания сертификата другого сервера, например, для подписания сертификата Прокси-сервера Dr.Web ключом Сервера Dr.Web.

  Для подписания подобного запроса используйте ключ `signcsr`.

Параметр ключа	Значение по умолчанию
<*закрытый_ключ*>	drwcsd.pri
<*поля_субъекта*>	/CN=<*имя_хоста*>

Параметр ключа	Значение по умолчанию
<запрос_на_подпись_сертификата>	`drwcsd-certificate-sign-request.pem`

- `drwsign genselfsign [-show] [-subj=<`*поля_субъекта*`>] [-days=<`*срок_действия*`>] [<`*закрытый_ключ*`> [<`*самоподписанный_сертификат*`>]]`

  Сгенерировать самоподписанный RSA-сертификат и закрытый RSA-ключ для веб-сервера и записать их в соответствующие файлы.

  Ключ `-show` выводит содержимое сертификата в читаемом виде.

Параметр ключа	Значение по умолчанию
<поля_субъекта>	`/CN=<`*имя_хоста*`>`
<срок_действия>	`3560`
<закрытый_ключ>	`private-key.pem`
<самоподписанный_сертификат>	`certificate.pem`

- `drwsign hash-check [-public-key=<`*открытый_ключ*`>] <`*файл_хеша*`> <`*файл_подписи*`>`

  Проверить подпись указанного 256-битного числа в формате клиент-серверного протокола.

  В параметре *<файл_хеша>* задается файл с 256-битным числом, которое необходимо подписать. В файле *<файл_подписи>* — результат подписи (два 256-битных числа).

Параметр ключа	Значение по умолчанию
<открытый_ключ>	`drwcsd.pub`

- `drwsign hash-sign [-private-key=<`*закрытый_ключ*`>] <`*файл_хеша*`> <`*файл_подписи*`>`

  Подписать указанное 256-битное число в формате клиент-серверного протокола.

  В параметре *<файл_хеша>* задается файл с 256-битным числом, которое необходимо подписать. В файле *<файл_подписи>* — результат подписи (два 256-битных числа).

Параметр ключа	Значение по умолчанию
<закрытый_ключ>	`drwcsd.pri`

- `drwsign help [<`*команда*`>]`

  Вывести краткую справку о программе или конкретной команде в формате командной строки.

- `drwsign sign [-private-key=<закрытый_ключ>] <файл>`

  Подписать *<файл>*, используя закрытый ключ.

Параметр ключа	Значение по умолчанию
<закрытый_ключ>	`drwcsd.pri`

- `drwsign signcert [-ca-key=<закрытый_ключ>] [-ca-cert=<сертификат_Сервера>] [-cert=<сертификат_на_подпись>] [-days=<срок_действия>] [<подписанный_сертификат>]`

  Подписать готовый *<сертификат_на_подпись>* закрытым ключом и сертификатом Сервера. Подписанный сертификат сохраняется в отдельном файле.

  Может быть использовано для подписывания сертификата Прокси-сервера Dr.Web ключом Сервера Dr.Web.

Параметр ключа	Значение по умолчанию
<закрытый_ключ>	`drwcsd.pri`
<сертификат_Сервера>	`drwcsd-ca-cerificate.pem`
<сертификат_на_подпись>	`drwcsd-certificate.pem`
<срок_действия>	`3560`
<подписанный_сертификат>	`drwcsd-signed-certificate.pem`

- `drwsign signcsr [-ca-key=<закрытый_ключ>] [-ca-cert=<сертификат_Сервера>] [-csr=<запрос_на_подпись_сертификата>] [-days=<срок_действия>] [<подписанный_сертификат>]`

  Подписать *<запрос_на_подпись_сертификата>*, сгенерированный при помощи команды `gencsr`, закрытым ключом и сертификатом Сервера. Подписанный сертификат сохраняется в отдельный файл.

  Может быть использовано для подписания сертификата другого сервера, например, для подписания сертификата Прокси-сервера Dr.Web ключом Сервера Dr.Web.

Параметр ключа	Значение по умолчанию
<закрытый_ключ>	`drwcsd.pri`
<сертификат_Сервера>	`drwcsd-cerificate.pem`
<запрос_на_подпись_сертификата>	`drwcsd-certificate-sign-request.pem`
<срок_действия>	`3560`
<подписанный_сертификат>	`drwcsd-signed-certificate.pem`

- `drwsign tlsticketkey [<TLS-тикет>]`

  Сгенерировать TLS-тикеты.

  Может быть использовано в кластере Серверов для общих TLS-сессий.

Параметр ключа	Значение по умолчанию
<TLS-тикет>	`tickets-key.bin`

- `drwsign verify [-ss-cert] [-CAfile=<сертификат_Сервера>] [<сертификат_на_проверку>]`

  Проверить валидность сертификата по доверенному сертификату Сервера.

  Ключ `-ss-cert` предписывает игнорировать доверенный сертификат и только проверить корректность самоподписанного сертификата.

Параметр ключа	Значение по умолчанию
<сертификат_Сервера>	`drwcsd-certificate.pem`
<сертификат_на_проверку>	`drwcsd-signed-certificate.pem`

- `drwsign x509dump [<сертификат_на_печать>]`

  Распечатать дамп любого x509 сертификата.

Параметр ключа	Значение по умолчанию
<сертификат_на_печать>	`drwcsd-certificate.pem`

37.2. Утилита администрирования встроенной базы данных

Предоставляются следующие утилиты администрирования встроенной БД:

- `drwidbsh` — для БД IntDB,
- `drwidbsh3` — для БД SQLite3.

Утилиты расположены в следующих директориях:

- для ОС **Linux**: `/opt/drwcs/bin`
- для ОС **FreeBSD**: `/usr/local/drwcs/bin`
- для ОС **Windows**: *<каталог_установки_Сервера>*`\bin`

  (по умолчанию каталог установки Сервера: `C:\Program Files\DrWeb Server`).

Формат команды запуска:

`drwidbsh` *<полное_имя_файла_БД>*

или

`drwidbsh3 <полное_имя_файла_БД>`

Программа работает в текстовом диалоговом режиме, ожидает ввода пользователем команд программы (команды начинаются с точки).

Для справки по другим командам введите `.help`. Будет выдан текст справки.

Для дополнительной информации используйте справочные руководства по языку SQL.

37.3. Утилита дистанционной диагностики Сервера Dr.Web

Утилита дистанционной диагностики Сервера Dr.Web позволяет удаленно подключаться к Серверу Dr.Web для базового управления и просмотра статистики работы. Графическая версия утилиты доступна только под ОС Windows.

Утилита доступна в следующих версиях:

- Для ОС Windows — графическая версия.
- Для ОС семейства UNIX — консольная версия.

Предоставляются следующие версии утилиты дистанционной диагностики Сервера Dr.Web:

Исполняемый файл	Расположение	Описание
`drweb-cntl-<ОС>-<разрядность>`	Центр управления, раздел **Администрирование** → **Утилиты**	Независимая версия утилиты. Может запускаться из произвольного каталога и на любом компьютере с соответствующей операционной системой.
	Каталог Сервера `webmin/utilities`	
`drwcntl`	Каталог Сервера `bin`	Версия утилиты зависит от наличия серверных библиотек. Может запускаться только из каталога своего расположения.

Версии утилиты `drweb-cntl-<ОС>-<разрядность>` и `drwcntl` аналогичны по функциональности. Далее в разделе приводится версия `drwcntl`, однако все примеры актуальны для обеих версий.

Для возможности подключения утилиты дистанционной диагностики Сервера необходимо включить расширение Dr.Web Server FrontDoor. Для этого в разделе **Конфигурация Сервера Dr.Web**, на вкладке **Модули** установите флаг **Расширение Dr.Web Server FrontDoor**.

Для возможности подключения утилиты дистанционной диагностики Сервера необходимо, чтобы для администратора, который подключается через утилиту, было

разрешено право **Использование дополнительных возможностей**. В противном случае доступ к Серверу через утилиту дистанционной диагностики будет запрещен.

Для подключения утилиты (как графической, так и консольной) с использованием TLS необходимо напрямую задавать протокол при указании адреса Сервера: `ssl://<IP-адрес или DNS-имя>`.

Описание настроек Сервера для подключения утилиты дистанционной диагностики Сервера Dr.Web приведены в **Руководстве администратора**, п. Удаленный доступ к Серверу Dr.Web.

Консольная версия утилиты

Формат команды запуска:

`drwcntl [-?|-h|--help] [+<файл_журнала>] [<сервер> [<регистрационное_имя> [<пароль>]]]`

где:

- `-? -h --help` — вывести справку по командам для использования утилиты.
- *<файл_журнала>* — записывать все действия утилиты в файл журнала по заданному пути.
- *<сервер>* — адресная строка Сервера, к которому подключается утилита в формате `[(tcp|ssl)://]`*IP-адрес или DNS-имя*`[:`*порт*`]`.

  Для возможности подключения по одному из поддерживаемых протоколов необходимо выполнение следующих условий:

  a) Для подключения по `ssl` в конфигурационном файле `frontdoor.conf` должен присутствовать тег `<ssl />`. При этом подключение будет возможно только по `ssl`.

  b) Для подключения по `tcp` в конфигурационном файле `frontdoor.conf` должен был отключен (закомментирован) тег `<ssl />`. При этом подключение будет возможно только по `tcp`.

  Если в адресной строке Сервера не заданы параметры подключения, используются следующие значения:

Параметр	Значение по умолчанию
Протокол подключения	`tcp` Для подключения по TCP должен быть снят флаг **Использовать TLS** в Центре управления, в разделе **Администрирование** → **Удаленный доступ к Серверу Dr.Web**. Это отключает тег `<ssl />` в конфигурационном файле `frontdoor.conf`.

Параметр	Значение по умолчанию
IP-адрес или DNS-имя Сервера	Утилита запросит ввести адрес Сервера в соответствующем формате.
Порт	`10101`  На стороне Сервера разрешенный порт задается в разделе **Удаленный доступ к Серверу Dr.Web** и сохраняется в конфигурационный файл `frontdoor.conf`. В случае использования альтернативного порта в данном разделе, необходимо явно указывать этот порт при подключении утилиты.

- <*регистрационное_имя*> — регистрационное имя администратора Сервера.
- <*пароль*> — пароль администратора для доступа к Серверу.

  Если регистрационное имя и пароль администратора не были заданы в строке подключения, утилита запросит ввести соответствующие учетные данные.

Допустимые команды:

- `cache` <*операция*> — работа с файловым кешем. Для запроса конкретной операции используйте следующие команды:
  - `clear` — очистить файловый кеш,
  - `list` — показать все содержимое файлового кеша,
  - `matched` <*регулярное выражение*> — показать содержимое файлового кеша, которое удовлетворяет заданному регулярному выражению,
  - `maxfilesize [`<*размер*>`]` — показать/установить максимальный размер предзагруженных файловых объектов. При запуске без дополнительных параметров показывает текущий размер. Для установки размера задайте требуемый размер в байтах после имени команды.
  - `statistics` — показать статистику использования файлового кеша.
- `calculate` <*функция*> — вычисление заданной последовательности. Для запроса конкретной последовательности используйте следующие команды:
  - `hash [`<*стандарт*>`] [`<*строка*>`]` — вычисление хеша заданной строки. Чтобы задать конкретный стандарт, используйте следующие команды:
    - `gost` — вычисление хеша заданной строки по стандарту ГОСТ,
    - `md5` — вычисление MD5 хеша заданной строки,
    - `sha` — вычисление хеша заданной строки по стандарту SHA,
    - `sha1` — вычисление хеша заданной строки по стандарту SHA1,
    - `sha224` — вычисление хеша заданной строки по стандарту SHA224,
    - `sha256` — вычисление хеша заданной строки по стандарту SHA256,

    - `sha384` — вычисление хеша заданной строки по стандарту SHA384,
    - `sha512` — вычисление хеша заданной строки по стандарту SHA512.
  - `hmac [<стандарт>] [<строка>]` — вычисление HMAC заданной строки. Чтобы задать конкретный стандарт, используйте следующие команды:
    - `md5` — вычисление HMAC-MD5 для заданной строки,
    - `sha256` — вычисление HMAC-SHA256 для заданной строки.
  - `random` — генерация произвольного числа,
  - `uuid` — генерация произвольного уникального идентификатора.
- `clients <операция>` — получение информации и управление клиентами, подключенными к Серверу. Для запроса конкретной функции используйте следующие команды:
  - `addresses [<регулярное выражение>]` — показать сетевые адреса станций, соответствующих заданному регулярному выражению. Если регулярное выражение не задано — показать адреса всех станции.
  - `caddresses [<регулярное выражение>]` — показать количество IP-адресов станций, соответствующих заданному регулярному выражению. Если регулярное выражение не задано — показать количество всех станций.
  - `chosts [<регулярное выражение>]` — показать количество имен компьютеров станций, соответствующих заданному регулярному выражению. Если регулярное выражение не задано — показать количество всех станций.
  - `cids [<регулярное выражение>]` — показать количество идентификаторов станций, соответствующих заданному регулярному выражению. Если регулярное выражение не задано — показать количество всех станций.
  - `cnames [<регулярное выражение>]` — показать количество имен станций, соответствующих заданному регулярному выражению. Если регулярное выражение не задано — показать количество количество всех станции.
  - `disconnect [<регулярное выражение>]` — оборвать текущее активное соединение со станциями, идентификаторы которых соответствуют заданному регулярному выражению. Если регулярное выражение не задано — оборвать соединение со всеми подключенными станциями.
  - `enable [<режим>]` — показать/установить режим подключения клиентов к Серверу. При запуске без дополнительных параметров показывает текущий режим. Для установки режима используйте следующие дополнительные команды:
    - `on` — принимать все соединения с клиентами.
    - `off` — отказывать всем клиентам в подключении.
  - `hosts <регулярное выражение>` — показать имена компьютеров станций, соответствующих заданному регулярному выражению.
  - `ids <регулярное выражение>` — показать идентификаторы станций, соответствующих заданному регулярному выражению.
  - `names <регулярное выражение>` — показать имена станций, соответствующих заданному регулярному выражению.

  - `online` <*регулярное выражение*> — показать длительность подключения станций, идентификатор, имя или адрес которых соответствуют заданному регулярному выражению. Длительность подключения считается с момента последнего подключения станций к Серверу.
  - `statistics` <*регулярное выражение*> — показать статистику по количеству клиентов, соответствующих заданному регулярному выражению.
  - `traffic` <*регулярное выражение*> — показать данные по трафику подключенных в данный момент клиентов, соответствующими заданному регулярному выражению.
- `core` — записать дамп процесса Сервера.
- `cpu` <*параметр*> — показать статистику использования CPU компьютера, на котором установлен Сервер. Для запроса конкретного параметра используйте следующие команды:
  - `clear` — удалить все накопленные статистические данные,
  - `day` — показать график загрузки CPU за текущий день,
  - `disable` — отключить отслеживание загрузки CPU,
  - `enable` — включить отслеживание загрузки CPU,
  - `hour` — показать график загрузки CPU за текущий час,
  - `load` — показать средний уровень загрузки CPU,
  - `minute` — показать график загрузки CPU за прошедшую минуту,
  - `rawd` — показать числовую статистику по загрузке CPU за день,
  - `rawh` — показать числовую статистику по загрузке CPU за последний час,
  - `rawl` — показать числовую статистику по средней загрузке CPU,
  - `rawm` — показать числовую статистику по загрузке CPU за последнюю минуту,
  - `status` — показать статус отслеживания статистики загрузки CPU.
- `debug` <*параметр*> — настройка отладки. Для задания конкретного параметра, используйте дополнительные команды. Для уточнения списка дополнительных команд, можете вызвать справку при помощи команды: `? debug`.

  Команда `debug signal` доступна только для Серверов под ОС семейства UNIX.

- `die` — остановить Сервер и записать дамп процесса Сервера.

  Команда `die` доступна только для Серверов под ОС семейства UNIX.

- `dwcp` <*параметр*> — установить/посмотреть настройки Dr.Web Control Protocol (включает журналы Сервера, Агентов и инсталляторов Агентов). Допустимые параметры:
  - `compression` <*режим*> — установить один из следующих режимов сжатия трафика:

        - `on` — сжатие включено,
        - `off` — сжатие отключено,
        - `possible` — сжатие возможно.
    - `encryption` <*режим*> — установить один из следующих режимов шифрования трафика:
        - `on` — шифрование включено,
        - `off` — шифрование отключено,
        - `possible` — шифрование возможно.
    - `show` — вывести текущие настройки Dr.Web Control Protocol.
- `io` <*параметр*> — показать статистику чтения/записи данных процессом Сервера. Для запроса конкретного параметра используйте следующие команды:
    - `clear` — удалить все накопленные статистические данные,
    - `disable` — отключить отслеживание статистики,
    - `enable` — включить отслеживание статистики,
    - `rawdr` — показать числовую статистику чтения данных за день,
    - `rawdw` — показать числовую статистику записи данных за день,
    - `rawh` — показать числовую статистику за последний час,
    - `rawm` — показать числовую статистику за последнюю минуту,
    - `rday` — показать график статистики чтения данных за день,
    - `rhour` — показать график статистики чтения данных за последний час,
    - `rminute` — показать график статистики чтения данных за последнюю минуту,
    - `status` — показать статус отслеживания статистики,
    - `wday` — показать график статистики записи данных за день,
    - `whour` — показать график статистики записи данных за последний час,
    - `wminute` — показать график статистики записи данных за последнюю минуту.
- `log` <*параметр*> — записать строку в файл журнала Сервера или установить/посмотреть уровень детализации журнала. В зависимости от заданных параметров выполняются следующие действия:
    - `log` <*строка*> — записать в журнал Сервера заданную строку с уровнем детализации `NOTICE`.
    - `log \s [`<*уровень*>`]` — установить/просмотреть уровень детализации журнала. При запуске с ключом `\s` без указания уровня выводится текущий уровень детализации. Допустимые значения уровня детализации: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`.
- `lua` <*скрипт*> — выполнить заданный Lua-скрипт.

- `mallopt` <*параметр*> — задать настройки распределения памяти. Для задания конкретной настройки используйте дополнительные команды. Для уточнения списка дополнительных команд, можете вызвать справку при помощи команды `? mallopt`.

  Команда `mallopt` доступна только для Серверов под ОС семейства Linux.

  Для получения подробностей по особенностям параметров данной команды, ознакомьтесь с описанием функции `mallopt()` из библиотеки `glibc`. Для получения справки по данной функции можете воспользоваться, например, командой `man mallopt`.

- `memory` <*параметр*> — показать статистику использования памяти компьютера, на котором установлен Сервер. Для запроса конкретного параметра используйте следующие команды:
  - `all` — вывести всю информацию и статистические данные,
  - `heap` — вывести информацию по динамической памяти,
  - `malloc` — вывести статистику по размещению памяти,
  - `sizes` — вывести статистику по размерам размещаемой памяти,
  - `system` — вывести информацию по системной памяти.

  Команда `memory` доступна только для Серверов под ОС Windows, ОС семейства Linux и ОС семейства FreeBSD. При этом действуют следующие ограничения на дополнительные параметры команды `memory`:
  - `system` — только для Серверов под ОС Windows, ОС семейства Linux,
  - `heap` — только для Серверов под ОС Windows, ОС семейства Linux,
  - `malloc` — только для Серверов под ОС семейства Linux и ОС семейства FreeBSD,
  - `sizes` — только для Серверов под ОС семейства Linux и ОС семейства FreeBSD.

- `monitoring` <*режим*> — установить/посмотреть режим мониторинга использования ресурсов CPU (ключ `cpu` <*параметр*>) и ввода/вывода (ключ `io` <*параметр*>) процессом Сервера. Допустимые команды:
  - `disable` — отключить мониторинг,
  - `enable` — включить мониторинг,
  - `show` — показать текущий режим.
- `printstat` — записать статистику работы Сервера в журнал.
- `reload` — перезагрузить расширение Dr.Web Server FrontDoor.
- `repository` <*параметр*> — управление репозиторием. Для запроса конкретной функции используйте следующие команды:
  - `all` — вывести список всех продуктов репозитория и количество всех файлов по продуктам,

  - `clear` — очистить содержимое кеша, вне зависимости от значения TTL размещенных в кеше объектов,
  - `fill` — разместить все файлы репозитория в кеше,
  - `keep` — хранить все файлы репозитория, находящиеся в кеше в данный момент, всегда, вне зависимости от их значения TTL,
  - `loaded` — вывести список всех продуктов репозитория и количество всех файлов по продуктам, находящимся в кеше в данный момент,
  - `reload` — перезагрузить репозиторий с диска,
  - `statistics` — показать статистику обновлений репозитория.
- `restart` — перезапустить Сервер.
- `show` <*параметр*> — показать информацию о системе, на которой установлен Сервер. Для задания конкретного параметра, используйте дополнительные команды. Для уточнения списка дополнительных команд, можете вызвать справку при помощи команды `? show`.

  Действуют следующие ограничения на дополнительные параметры команды `show`:

  - `memory` — только для Серверов под ОС Windows, ОС семейства Linux,
  - `mapping` — только для Серверов под ОС Windows, ОС семейства Linux,
  - `limits` — только для Серверов под ОС семейства UNIX,
  - `processors` — только для Серверов под ОС семейства Linux.
- `sql` <*запрос*> — выполнить заданный SQL-запрос.
- `stop` — остановить Сервер.
- `traffic` <*параметр*> — показать статистику по сетевому трафику Сервера. Для запроса конкретного параметра используйте следующие команды:
  - `all` — показать весь объем трафика с начала работы Сервера.
  - `incremental` — показать приращение трафика относительно последнего запуска команды `traffic incremental`.
  - `last` — показать изменение трафика с последней фиксированной точки.
  - `store` — создание фиксированной точки для ключа `last`.
- `update` <*параметр*> — получение информации и управление обновлениями. Для запроса конкретной функции используйте следующие ключи:
  - `active` — показать список Агентов, осуществляющих обновление в данный момент.
  - `agent [`<*режим*>`]` — показать/установить режим обновления Агентов с Сервера. При запуске без дополнительных параметров показывает текущий режим. Для установки режима используйте следующие дополнительные ключи:
    - `on` — включить обновления Агентов.
    - `off` — отключить обновления Агентов.

- `gus` — запустить обновление репозитория с ВСО вне зависимости от состояния процесса обновления с ВСО.
- `http [<режим>]` — показать/установить режим обновлений репозитория Сервера с ВСО. При запуске без дополнительных параметров показывает текущий режим. Для установки режима используйте следующие дополнительные ключи:
  - `on` — включить обновления репозитория с ВСО.
  - `off` — отключить обновления репозитория с ВСО.
- `inactive` — показать список Агентов, которые не осуществляют обновление в данный момент.
- `track [<режим>]` — показать/установить режим отслеживания обновлений Агентов. При запуске без дополнительных параметров показывает текущий режим. Для установки режима используйте следующие дополнительные команды:
  - `on` — включить отслеживание обновлений Агентов.
  - `off` — отключить отслеживание обновлений Агентов. При этом ключ `update active` не будет выводить список обновляемых Агентов.

37.4. Утилита дистанционной диагностики Сервера Dr.Web для работы со скриптами

Утилита дистанционной диагностики Сервера Dr.Web позволяет удаленно подключаться к Серверу Dr.Web для базового управления и просмотра статистики работы. В отличие от drwcntl, утилита `drwcmd` может быть использована при работе со скриптами.

Предоставляются следующие версии консольной утилиты дистанционной диагностики Сервера Dr.Web для работы со скриптами:

Исполняемый файл	Расположение	Описание
`drweb-cmd-<ОС>-<разрядность>`	Центр управления, раздел **Администрирование** → **Утилиты**	Независимая версия утилиты. Может запускаться из произвольного каталога и на любом компьютере с соответствующей операционной системой.
	Каталог Сервера `webmin/utilities`	
`drwcmd`	Каталог Сервера `bin`	Версия утилиты зависит от наличия серверных библиотек. Может запускаться только из каталога своего расположения.

Версии утилиты `drweb-cmd-<ОС>-<разрядность>` и `drwcmd` аналогичны по функциональности. Далее в разделе приводится версия `drwcmd`, однако все примеры актуальны для обеих версий.

Для возможности подключения утилиты дистанционной диагностики Сервера необходимо включить расширение Dr.Web Server FrontDoor. Для этого в разделе **Конфигурация Сервера Dr.Web**, на вкладке **Модули** установите флаг **Расширение Dr.Web Server FrontDoor**.

Для возможности подключения утилиты дистанционной диагностики Сервера необходимо, чтобы для администратора, который подключается через утилиту, было разрешено право **Использование дополнительных возможностей**. В противном случае доступ к Серверу через утилиту дистанционной диагностики будет запрещен.

Описание настроек Сервера для подключения утилиты дистанционной диагностики Сервера Dr.Web приведены в **Руководстве администратора**, п. Удаленный доступ к Серверу Dr.Web.

Формат команды запуска:

`drwcmd [<ключи>] [<файлы>]`

Допустимые ключи

Принцип использования ключей утилитой `drwcmd` подчиняется общим правилам, описанным в разделе Приложение 3. Параметры командной строки программ, входящих в состав Dr.Web Enterprise Security Suite.

- `--?` — вывести справку по ключам.
- `--help` — вывести справку по ключам.
- `--commands=<команды>` — выполнить заданные команды (аналогичны командам утилиты drwcntl). Допускается задание нескольких команд, разделенных знаком `;`.
- `--debug=yes|no` — вести журнала работы утилиты в отладочном режиме (стандартный поток вывода `stderr`). По умолчанию `no`.
- `--files=yes|no` — разрешить выполнение команд (аналогичны командам утилиты drwcntl) из заданных файлов. По умолчанию `yes`.

  Задание команд в файле должно осуществляться по одной команде на строке. Пустые строки игнорируются. В качестве начала комментария допускается использование знака `#`.
- `--keep=yes|no` — поддерживать соединение с Сервером после выполнения последней команды до завершения процесса утилиты. По умолчанию `no`.
- `--output=<файл>` — файл для вывода ответов Сервера. По умолчанию, если файл не указан, используется стандартный поток вывода `stdout`.

  Если имя файла начинается с символа (+), то результат выполнения команд будет добавлен в конец файла, иначе — файл будет перезаписан.

- `--password=<пароль>` — пароль для авторизации на Сервере. Может быть определен в файле, заданном в ключе `--resource`.
- `--read=yes|no` — разрешить чтение параметров подключения к Серверу из ресурсного файла. По умолчанию `yes`.
- `--resource=<файл>` — ресурсный файл с параметрами подключения к Серверу: адресом Сервера и регистрационными данными администратора для авторизации на Сервере. По умолчанию используется файл `.drwcmdrc`, расположенный в следующем каталоге:
  - Для ОС семейства UNIX: `$HOME`
  - Для ОС Windows: `%LOCALAPPDATA%`

  Каждая строка в файле должна представлять из себя 3 слова, разделенных пробелами: *<Сервер> <пользователь> <пароль>*.

  Если нужно использовать в середине слова пробел, то он задается как `%S`. Если требуется знак процента, то он задается как `%P`.

  Например:

```
ssl://127.0.0.1 user1 password1

ssl://127.0.0.1 user2 password2

ssl://127.0.0.1 user pass%Sword
```

  При использовании ключа `--resource` необходимо также указывать ключ `--server`. Подключение осуществляется к Серверу, указанному в ключе `--server`, по регистрационным данным из ресурсного файла, соответствующим адресу этого Сервера.

- `--server=<Сервер>` — адрес Сервера. По умолчанию `ssl://127.0.0.1`. Может быть определен в файле, заданном в ключе `--resource`.
- `--user=<пользователь>` — имя пользователя для авторизации на Сервере. Может быть определено в файле, заданном в ключе `--resource`.
- `--verbose=yes|no` — выводить подробный ответа Сервера (стандартный поток вывода `stdout`). По умолчанию `no`.

Процедура подключения к Серверу:

1. При определении данных подключения к Серверу приоритетными являются значения, заданные в ключах `--server`, `--user` и `--password`.
2. Если ключ `--server` не задан, используется его значение по умолчанию — `ssl://127.0.0.1`.
3. Если ключ `--user` не задан, то в файле `.drwcmdrc` (может быть переопределен в ключе `--resource`) осуществляется поиск нужного Сервера и берется первое по алфавиту имя пользователя.

4. Если ключ `--password` не задан, то в файле `.drwcmdrc` (может быть переопределен в ключе `--resource`) осуществляется поиск по Серверу и имени пользователя.

   Имя пользователя и пароль будут прочитаны из файла `.drwcmdrc` (может быть переопределен в ключе `--resource`), если это не запрещено ключом `--read`.

5. Если имя пользователя и пароль не заданы при помощи ключей или через ресурсный файл, утилита запросит ввод учетных данных через консоль.

Особенности выполнения команд:

- Если в качестве файлов с командами задано пустое значение (–), то читаются команды, введенные через консоль.
- Если одновременно заданы команды в ключе `--commands` и список файлов, то сначала выполняются команды, заданные в ключе `--commands`.
- Если не заданы ни файлы, ни команды в ключе `--commands`, то читаются команды, введенные через консоль.

Например:

Чтобы выполнить команды из ключа `--command`, а затем команды из консоли, введите следующее:

```
drwcmd --commands=<команды> -- -
```

Коды завершения работы

- 0 — успешное выполнение.
- 1 — запрошена справка по ключам: `--help` или `--?`.
- 2 — ошибка разбора командной строки: не заданы параметры авторизации и т. п.
- 3 — ошибка создания файла для вывода ответа Сервера.
- 4 — ошибка авторизации на Сервере: неверные имя и/или пароль администратора.
- 5 — аварийный разрыв соединения с Сервером.
- 127 — неопределенная фатальная ошибка.

37.5. Загрузчик репозитория Dr.Web

Описание графической версии утилиты Загрузчика репозитория приведено в **Руководстве администратора**, в разделе Графическая утилита.

Предоставляются следующие версии консольной утилиты Загрузчик репозитория Dr.Web:

Исполняемый файл	Расположение	Описание
`drweb-reploader-<ОС>-<разрядность>`	Центр управления, раздел **Администрирование** → **Утилиты**	Независимая версия утилиты. Может запускаться из произвольного каталога и на любом компьютере с соответствующей операционной системой.
	Каталог Сервера `webmin/utilities`	
`drwreploader`	Каталог Сервера `bin`	Версия утилиты зависит от наличия серверных библиотек. Может запускаться только из каталога своего расположения.

Версии утилиты `drweb-reploader-<ОС>-<разрядность>` и `drwreploader` аналогичны по функциональности. Далее в разделе приводится версия `drwreploader`, однако все примеры актуальны для обеих версий.

Чтобы упростить задание ключей для запуска консольной утилиты вы можете использовать конфигурационный файл Загрузчика репозитория. В предустановленном конфигурационном файле значения ключей соответствуют значениям по умолчанию, приведенным ниже, кроме ключа `--ssh-auth`: для него в конфигурационном файле переопределяется значение на `pubkey`.

Допустимые ключи

- `--archive` — упаковать репозиторий в архив. По умолчанию: `no`.
- `--auth <аргумент>` — регистрационные данные для авторизации на сервере обновлений в формате `<пользователь>[:<пароль>]`.
- `--cert-file <путь>` — путь к хранилищу корневых сертификатов для SSL-авторизации.
- `--cert-mode [<аргумент>]` — тип SSL-сертификатов, которые будут автоматически приниматься. Данная настройка используется только для защищенных протоколов, поддерживающих шифрование.

  `<аргумент>` может принимать одно из значений:

  - `any` — принимать любые сертификаты,
  - `valid` — принимать только проверенные сертификаты,
  - `drweb` — принимать только сертификаты Dr.Web,
  - `custom` — принимать пользовательские сертификаты.

  По умолчанию используется значение `drweb`.
- `--config <путь>` — путь к конфигурационному файлу Загрузчика репозитория.

- `--cwd <путь>` — путь к текущему рабочему каталогу.
- `--ipc` — включить передачу данных о процессе работы утилиты в поток стандартного вывода. По умолчанию: `no`.
- `--help` — вывести справку по ключам.
- `--license-key <путь>` — путь к файлу лицензионного ключа (должен быть указан ключ или его MD5).
- `--log <путь>` — путь к файлу журнала по процедуре загрузки репозитория.
- `--mode <режим>` — режим загрузки обновлений:
  - `repo` — осуществляется скачивание репозитория в формате репозитория Сервера. Загруженные файлы могут быть непосредственно импортированы через Центр управления в качестве обновления репозитория Сервера. Используется по умолчанию.
  - `mirror` — осуществляется скачивание репозитория в формате зоны обновлений ВСО. Загруженные файлы могут быть выложены на зеркало обновлений в вашей локальной сети. В дальнейшем Серверы могут быть настроены на получение обновлений непосредственно с данного зеркала обновлений, содержащего последнюю версию репозитория, а не с серверов ВСО.
- `--only-bases` — загрузить только вирусные базы. По умолчанию: `no`.
- `--path <аргумент>` — загрузить репозиторий с ВСО в каталог, указанный в параметре <*аргумент*>. При упаковке репозитория в архив при помощи ключа `--archive`, возможно указание пути как до имени каталога, так и до имени файла архива. Если имя архива не указано, будет дано имя по умолчанию — `repository.zip`.
- `--product <аргумент>` — обновляемый продукт. По умолчанию загружается весь репозиторий.
- `--prohibit-cdn` — запретить использовать CDN при загрузке обновлений. По умолчанию: `no`, т. е. разрешено использование CDN.
- `--proto <протокол>` — протокол загрузки обновлений: `file | ftp | ftps | http | https | scp | sftp | smb | smbs`. По умолчанию: `https`.
- `--proxy-auth <аргумент>` — информация для аутентификации на прокси-сервере: регистрационное имя пользователя и пароль в формате <*пользователь*>`[:`<*пароль*>`]`.
- `--proxy-host <аргумент>` — адрес прокси-сервера в формате <*сервер*>`[:`<*порт*>`]`. Порт по умолчанию: `3128`.
- `--rotate <N><f>,<M><u>` — режим ротации журнала работы Загрузчика репозитория. Аналогично настройке ротации журнала Сервера.

  По умолчанию `10,10m`, что означает хранить 10 файлов по 10 мегабайт, использовать сжатие.
- `--servers <аргумент>` — адреса серверов ВСО. Рекомендуется оставить значение по умолчанию: `esuite.geo.drweb.com`.
- `--show-products` — показать список продуктов на ВСО. По умолчанию: `no`.

- `--ssh-auth` <*тип*> — тип авторизации на сервере обновлений при обращении по SCP/SFTP. В качестве параметра <*тип*> допускается одно из следующих значений:
  - `pwd` — авторизация по паролю. Пароль задается в ключе `--auth`.
  - `pubkey` — авторизация по открытому ключу. При этом необходимо задать закрытый ключ через `--ssh-prikey` для извлечения соответствующего открытого ключа.
- `--ssh-prikey` <*путь*> — путь до закрытого ключа SSH.
- `--ssh-pubkey` <*путь*> — путь до открытого ключа SSH.
- `--strict` — остановить загрузку в случае возникновения ошибки. По умолчанию: `no`.
- `--update-key` <*путь*> — путь до открытого ключа или каталога с открытым ключом для проверки подписи обновлений, загружаемых с ВСО. Открытые ключи для проверки подлинности обновлений `update-key-*.upub` можно найти на Сервере Dr.Web в каталоге `etc`.
- `--update-url` <*аргумент*> — каталог на серверах ВСО, содержащий обновления продуктов Dr.Web. Рекомендуется оставить значение по умолчанию — `/update`.
- `--verbosity` <*уровень_подробности*> — уровень детализации журнала. По умолчанию `TRACE3`. Допустимые значения: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Значения `ALL` и `DEBUG3` — синонимы.
- `--version` <*версия*> — версия Сервера, для которого необходимо загрузить обновления в формате <*мажорная_версия*>`.`<*минорная_версия*>. Например, для Сервера версии 11, параметр <*версия*> принимает значение `11.00`.

Особенности использования ключей

При запуске утилиты Загрузчик репозитория обратите внимание на следующие правила:

Ключи должны быть обязательно заданы	**При условии**
`--license-key`	Всегда
`--update-key`	
`--path`	
`--cert-file`	Если следующие ключи принимают одно из значений: • `--cert-mode valid | drweb | custom`, • `--proto https | ftps | smbs`.
`--ssh-prikey`	Если следующие ключи принимают одно из значений: • `--proto sftp | scp`, • `--ssh-auth pubkey`.

Примеры использования

1. Создать импортируемый архив со всеми продуктами:

```
drwreploader.exe --path C:\Temp --archive --license-key C:\agent.key --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc"
```

2. Создать импортируемый архив с вирусными базами:

```
drwreploader.exe --path C:\Temp --archive --license-key "C:\agent.key" --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc" -only-bases
```

3. Создать импортируемый архив только с Сервером:

```
drwreploader.exe --path C:\Temp --archive --license-key "C:\agent.key" --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc" --product=20-drwcs
```

Приложение И. Переменные окружения, экспортируемые Сервером Dr.Web

Для упрощения настройки процессов, запускаемых Сервером Dr.Web по расписанию, требуется информация о размещении каталогов Сервера. С этой целью Сервер экспортирует в окружение запускаемых процессов следующие переменные:

- `DRWCSD_HOME` — путь к корневому каталогу (каталогу установки). Значение ключа `-home`, если он был задан при запуске Сервера, в противном случае текущий каталог при запуске.
- `DRWCSD_BIN` — путь к каталогу для исполняемых файлов. Значение ключа `-bin-root`, если он был задан при запуске Сервера, в противном случае подкаталог `bin` корневого каталога.
- `DRWCSD_VAR` — путь к каталогу, в который Сервер имеет право записи и который предназначен для хранения изменяемых файлов (например, журналов, а также файлов репозитория). Значение ключа `-var-root`, если он был задан при запуске Сервера, в противном случае подкаталог `var` корневого каталога.

Приложение К. Использование регулярных выражений в Dr.Web Enterprise Security Suite

Некоторые параметры Dr.Web Enterprise Security Suite могут задаваться в формате регулярных выражений следующих типов:

- Регулярные выражения языка Lua.

  Используются при настройке автоматического членства станций антивирусной сети в пользовательских группах.

  Подробное описание синтаксиса регулярных выражений языка Lua доступно на сайте http://www.lua.org/manual/5.1/manual.html#5.4.1.

- Регулярные выражения программной библиотеки PCRE.

  Подробное описание синтаксиса библиотеки PCRE доступно на сайте http://www.pcre.org/.

  В данном приложении приведено только краткое описание основных моментов использования регулярных выражений библиотеки PCRE.

К1. Опции регулярных выражений PCRE

Регулярные выражения применяются как в конфигурационном файле Сервера, так и в Центре управления при задании исключаемых из сканирования объектов в настройках Сканера.

Регулярные выражения записываются в следующей форме:

```
qr{EXP}options
```

где `EXP` — собственно выражение, `options` — последовательность опций (строка букв), `qr{}` — литеральные метасимволы. В целом конструкция выглядит, например, так:

`qr{pagefile\.sys}i` — файл подкачки ОС Windows NT

Ниже приведено описание опций и собственно регулярных выражений. Более полное описание см. на http://www.pcre.org/pcre.txt.

- Опция `'a'`, соответствующая `PCRE_ANCHORED`

  С этой настройкой шаблон принудительно "встает на якорь", т. е. ограничивается сопоставлением только с первой искомой позицией в строке, по которой осуществляется поиск ("строка темы"). Это также можно достигнуть с помощью соответствующих конструкций в самом шаблоне.

- Опция `'i'`, соответствующая `PCRE_CASELESS`

  С этой настройкой буквы в шаблоне сопоставляются как с заглавными, так и со строчными буквами. Данная возможность может быть изменена в шаблоне настройкой опции `(?i)`.

- Опция 'x', соответствующая PCRE_EXTENDED

  С этой настройкой пробелы между символами в шаблоне игнорируются, за исключением случаев, когда они предваряются управляющими символами или находятся внутри класса символов. Пробел не включает символ VT (код 11). Кроме того, символы, находящиеся вне класса символов между символом #, не предваренным управляющим символом, и символом новой строки включительно, также игнорируются. Данную опцию можно изменить в шаблоне настройкой опции (?x). Эта настройка дает возможность включать комментарии внутрь сложных шаблонов. Следует обратить внимание, что это применимо только к символам данных. Символы пробела не могут находиться в шаблоне внутри последовательностей специальных символов, например, внутри последовательности (?(, которая вводит условный подшаблон.

- Опция 'm', соответствующая PCRE_MULTILINE

  По умолчанию, PCRE считает, что строка темы состоит из единственной строки с символами (даже если она на самом деле содержит символы перевода строк). Метасимвол "*начала строки*" "^" сопоставляется только в начале строки, в то время как метасимвол "*конец строки*" "$" сопоставляется только в конце строки или перед заключительным переводом строки (если не установлена опция PCRE_DOLLAR_ENDONLY).

  Если установлена опция PCRE_MULTILINE, метасимволы "*начало строки*" и "*конец строки*" привязываются к следующим сразу за ними или перед ними любым переводам строки в строке темы, а также в самом начале и конце строки. Данную опцию можно изменить в шаблоне настройкой опции (?m). Если в тексте нет символов "\n" или если в шаблоне не встречается ^ или $, опция PCRE_MULTILINE не имеет смысла.

- Опция 'u', соответствующая PCRE_UNGREEDY

  Эта опция отменяет "жадность" квантификаторов, так что они становятся "нежадными" по умолчанию, но восстанавливают "жадность", если за ними следует "?". Это также можно настроить опцией (?U) в шаблоне.

- Опция 'd', соответствующая PCRE_DOTALL

  С этой настройкой метасимвол точки в шаблоне сопоставляется со всеми символами, включая символ новой строки. Без него символы новой строки исключаются. Эту опцию можно изменить в шаблоне установкой новой опции (?s). Отрицательный класс, например, [^a], всегда сопоставляется с символом новой строки, независимо от установок этой опции.

- Опция 'e', соответствующая PCRE_DOLLAR_ENDONLY

  С этой настройкой символ доллара в шаблоне сопоставляется только в конце строки темы. Без этой опции доллар также сопоставляется в положении непосредственно перед символом перевода строки в конце строки (но не перед любыми другими символами новой строки). Опция PCRE_DOLLAR_ENDONLY игнорируется, если установлена опция PCRE_MULTILINE.

К2. Особенности регулярных выражений PCRE

Регулярное выражение — это шаблон, сопоставляемый с текстом слева направо. Большинство символов в шаблоне обозначают сами себя и применяются к соответствующим символам в тексте.

Главное преимущество регулярных выражений заключается в возможности включать в шаблон варианты и повторения. Они кодируются с помощью метасимволов, которые не означают сами себя, а наоборот, интерпретируются особым способом.

Существует два различных набора метасимволов: те, которые используются внутри квадратных скобок, и те, которые используются вне квадратных скобок. Рассмотрим их более детально. Вне квадратных скобок используются следующие метасимволы:

Символ	Значение
\	обычный управляющий символ (escape), допускающий несколько вариантов применения
^	объявляет начало строки (или текста в многострочном режиме)
$	объявляет конец строки (или текста в многострочном режиме)
.	соответствует любому символу, кроме символа переноса строки (по умолчанию)
[	начало описания класса символов
]	конец описания класса символов
|	начало альтернативной ветви
(	начало подшаблона
)	конец подшаблона
?	расширяет значение (также квантификатор 0 или 1 также квантификатор-минимизатор
*	0 или более
+	1 или более также "притяжательный квантификатор"
{	начало минимального/ максимального квантификатора

Та часть шаблона, которая находится в квадратных скобках, называется "классом символов". В классе символов метасимволами являются:

Символ	Значение
\	обычный управляющий символ (escape)
^	отрицает класс, но только если в начале класса
-	определяет диапазон символов
[	класс символов POSIX (только если за ним следует синтаксис POSIX)
]	закрывает класс символов

Приложение Л. Формат файлов журнала

Файлы журнала Сервера (см. **Руководство администратора**, п. Журнал работы Сервера Dr.Web) и Агента ведутся в текстовом формате, где каждая строка представляет собой отдельное сообщение.

Формат строки сообщения следующий:

<год><месяц><число>.<час><минута><секунда>.<сотые_секунды> <тип_сообщения> [*<id_процесса>*] *<имя_потока>* [*<источник_сообщения>*] *<сообщение>*

где:

- *<год><месяц><число>.<час><минута><секунда>.<сотые_секунды>* — точная дата записи сообщения в файл журнала.
- *<тип_сообщения>* — уровень ведения журнала:
  - **ftl** (fatal error — фатальная ошибка) — сообщения о критических ошибках функционирования;
  - **err** (error — ошибка) — сообщения об ошибках функционирования;
  - **wrn** (warning — предупреждение) — предупреждения об ошибках;
  - **ntc** (notice — замечание) — важные информационные сообщения;
  - **inf** (info — информация) — информационные сообщения;
  - **tr0..3** (trace0..3 — трассировка) — трассировка происходящих действий с разной степенью детализации (**Трассировка3** — максимальный уровень детализации);
  - **db0..3** (debug0..3 — отладка) — отладочные сообщения с разной степенью детализации (**Отладка3** — максимальный уровень детализации).

  Сообщения с уровнем ведения журнала **tr0..3** (трассировка) и **db0..3** (отладка) ведутся только для разработчиков ПО Dr. Web Enterprise Security Suite.

- [*<id_процесса>*] — уникальный числовой идентификатор процесса, в рамках которого выполнялся поток, записавший сообщение в файл журнала. Под некоторыми ОС [*<id_процесса>*] может быть представлен в виде [*<id_процесса> <id_потока>*].
- *<имя_потока>* — символьное обозначение потока, в рамках которого производилась запись сообщения в файл журнала.
- [*<источник_сообщения>*] — обозначение системы, являющейся инициатором записи сообщения в файл журнала. Источник присутствует не всегда.
- *<сообщение>* — текстовое описание действий в соответствии с уровнем журнала. Может включать в себя как формальное описание сообщения, так и значения некоторых важных для конкретного случая переменных.

Например:

1. `20081023.171700.74 inf [001316] mth:12 [Sch] Job "Purge unsent IS events" said OK`

   где:

   - `20081023` — <*год*><*месяц*><*число*>,
   - `171700` — <*час*><*минута*><*секунда*>,
   - `74` — <*сотые_секунды*>,
   - `inf` — <*тип_сообщения*> — информационное сообщение,
   - `[001316]` — [<*id_процесса*>],
   - `mth:12` — <*имя_потока*>,
   - `[Sch]` — [<*источник_сообщения*>] — планировщик,
   - `Job "Purge unsent IS events" said OK` — <*сообщение*> о корректном выполнении задания **Очистка неотправленных событий**.

2. `20081028.135755.61 inf [001556] srv:0 tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193`

   где:

   - `20081028` — <*год*><*месяц*><*число*>,
   - `135755` — <*час*><*минута*><*секунда*>,
   - `61` — <*сотые_секунды*>,
   - `inf` — <*тип_сообщения*> — информационное сообщение,
   - `[001556]` — [<*id_процесса*>],
   - `srv:0` — <*имя_потока*>,
   - `tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193` — <*сообщение*> об установлении нового соединения через указанный сокет.

Приложение M. Интеграция Web API и Dr.Web Enterprise Security Suite

Описание **Web API** приводится в руководстве **Web API для Dr.Web Enterprise Security Suite**.

Применение

При интеграции **Web API** и Dr.Web Enterprise Security Suite предоставляются функции для операций с учетными записями и автоматизации процесса администрирования пользователей сервиса. Вы можете использовать его, например, при создании динамических страниц для получения от пользователя запроса и выдачи ему установочного файла.

Аутентификация

Для взаимодействия с Сервером Dr.Web используется протокол HTTP(S). **Web API** принимает REST запросы и возвращает XML. Для доступа к Web API используется Basic HTTP-аутентификация (согласно стандарту RFC 2617). При несоблюдении стандарта RFC 2617, HTTP(S) сервер не будет запрашивать учетные данные клиента (регистрационное имя и пароль администратора Dr.Web Enterprise Security Suite).

Приложение H. Лицензии

В данном разделе приведен список сторонних программных библиотек, которые используются ПО Dr.Web Enterprise Security Suite, информация по их лицензированию и адреса проектов разработки.

Сторонняя библиотека	Лицензия	URL проекта
asio	https://www.boost.org/LICENSE_1_0.txt*	https://think-async.com/Asio/
boost	https://www.boost.org/LICENSE_1_0.txt*	https://www.boost.org/
brotli	MIT License**	https://github.com/google/brotli
bsdiff	Custom	http://www.daemonology.net/bsdiff/
c-ares	https://c-ares.haxx.se/license.html*	https://c-ares.org/
cairo	Mozilla Public License** GNU Lesser General Public License**	https://www.cairographics.org/
CodeMirror	MIT License**	https://codemirror.net/
curl	https://curl.se/docs/copyright.html*	https://curl.se/libcurl/
ICU	http://www.unicode.org/copyright.html#License*	https://icu.unicode.org/home
fontconfig	Custom	https://www.freedesktop.org/wiki/Software/fontconfig/
freetype	GNU General Public License** FreeType Project License (BSD like)	https://www.freetype.org/
GCC runtime libraries	GNU General Public License** with exception*	http://gcc.gnu.org/
HTMLayout	Custom	https://terrainformatica.com/a-homepage-section/htmlayout/
jemalloc	https://github.com/jemalloc/jemalloc/blob/dev/COPYING*	https://github.com/jemalloc/jemalloc
jQuery	MIT License** GNU General Public License**	https://jquery.com/
JSON4Lua	MIT License**	https://github.com/craigmj/json4lua

Сторонняя библиотека	Лицензия	URL проекта
Leaflet	BSD License https://github.com/Leaflet/Leaflet/blob/master/LICENSE*	https://leafletjs.com/
libpng	http://libpng.org/pub/png/src/libpng-LICENSE.txt*	http://libpng.org/pub/png/libpng.html
libradius	Juniper Networks, Inc.*	https://www.freebsd.org/
libssh2	3-Clause BSD License** https://github.com/libssh2/libssh2/blob/master/COPYING	https://www.libssh2.org/
libxml2	MIT License**	http://www.xmlsoft.org/
Linenoise NG	3-Clause BSD License**	https://github.com/arangodb/linenoise-ng
lua	MIT License**	http://www.lua.org/
lua-xmlreader	MIT License**	http://asbradbury.org/projects/lua-xmlreader/
lzma	Public Domain	https://www.7-zip.org/sdk.html
ncurses	MIT License**	https://invisible-island.net/ncurses/announce.html
Net-snmp	http://www.net-snmp.org/about/license.html*	http://www.net-snmp.org/
nghttp2	MIT License**	https://nghttp2.org/
Noto Sans CJK	https://scripts.sil.org/cms/scripts/render_download.php?format=file&media_id=OFL_plaintext&filename=OFL.txt*	https://www.google.com/get/noto/help/cjk/
OpenLDAP	https://www.openldap.org/software/release/license.html*	https://www.openldap.org/
OpenSSL	https://www.openssl.org/source/license.html*	https://www.openssl.org/
Oracle Instant Client	https://www.oracle.com/downloads/licenses/instant-client-lic.html*	https://www.oracle.com/index.html
ParaType Free Font	https://www.paratype.ru/public/pt_openlicense_eng.asp*	https://www.paratype.ru/

Сторонняя библиотека	Лицензия	URL проекта
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/
pixman	MIT License**	http://pixman.org/
Prototype JavaScript framework	MIT License**	http://prototypejs.org/assets/2009/8/31/prototype.js
script.aculo.us scriptaculous.js	http://madrobby.github.io/scriptaculous/license/*	http://script.aculo.us/
slt	MIT License**	https://code.google.com/archive/p/slt
SQLite	Public Domain https://www.sqlite.org/copyright.html	https://www.sqlite.org/index.html
wtl	Common Public License** Microsoft Public License**	https://sourceforge.net/projects/wtl/
zlib	http://www.zlib.net/zlib_license.html*	http://www.zlib.net/

* — тексты лицензий приведены далее.

** — тексты базовых лицензий можно найти по следующим адресам:

Лицензия	Адрес
Common Public License	https://opensource.org/licenses/cpl1.0.php
GNU General Public License	https://www.gnu.org/licenses/gpl-3.0.html
GNU Lesser General Public License	https://www.gnu.org/licenses/lgpl-3.0.html
Microsoft Public License	https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649456(v=pandp.10)
MIT License	https://opensource.org/licenses/mit-license.php
Mozilla Public License	https://www.mozilla.org/en-US/MPL/2.0/
3-Clause BSD License	https://opensource.org/licenses/BSD-3-Clause

H1. Boost

```
Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a
copy of the software and accompanying documentation covered by this license (the
"Software") to use, reproduce, display, distribute, execute, and transmit the Software,
and to prepare derivative works of the Software, and to permit third-parties to whom
the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above
license grant, this restriction and the following disclaimer, must be included in all
copies of the Software, in whole or in part, and all derivative works of the Software,
unless such copies or derivative works are solely in the form of machine-executable
object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS
OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY,
WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

H2. C-ares

```
Copyright (c) 2007 - 2018, Daniel Stenberg with many contributors, see AUTHORS file.

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for
any purpose and without fee is hereby granted, provided that the above copyright notice
appear in all copies and that both that copyright notice and this permission notice
appear in supporting documentation, and that the name of M.I.T. not be used in
advertising or publicity pertaining to distribution of the software without specific,
written prior permission. M.I.T. makes no representations about the suitability of this
software for any purpose. It is provided "as is" without express or implied warranty.
```

H3. Curl

```
Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or
without fee is hereby granted, provided that the above copyright notice and this
permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

```
Except as contained in this notice, the name of a copyright holder shall not be used in
advertising or otherwise to promote the sale, use or other dealings in this Software
without prior written authorization of the copyright holder.
```

H4. ICU

```
Copyright © 1991-2018 Unicode, Inc. All rights reserved.

Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the
Unicode data files and any associated documentation (the "Data Files") or Unicode
software and any associated documentation (the "Software") to deal in the Data Files or
Software without restriction, including without limitation the rights to use, copy,
modify, merge, publish, distribute, and/or sell copies of the Data Files or Software,
and to permit persons to whom the Data Files or Software are furnished to do so,
provided that either (a) this copyright and permission notice appear with all copies of
the Data Files or Software, or (b) this copyright and permission notice appear in
associated Documentation.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR
A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE
COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY
SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER
TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE
DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in
advertising or otherwise to promote the sale, use or other dealings in these Data Files
or Software without prior written authorization of the copyright holder.
```

H5. GCC runtime libraries—exception

```
GCC is Copyright (C) 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996,
1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 Free Software
Foundation, Inc.

GCC is free software; you can redistribute it and/or modify it under the terms of the
GNU General Public License as published by the Free Software Foundation; either version
3, or (at your option) any later version.

GCC is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY;
without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR
PURPOSE.  See the GNU General Public License for more details.

Files that have exception clauses are licensed under the terms of the GNU General
Public License; either version 3, or (at your option) any later version.

The following runtime libraries are licensed under the terms of the GNU General Public
License (v3 or later) with version 3.1 of the GCC Runtime Library Exception (included
in this file):
```

```
 - libgcc (libgcc/, gcc/libgcc2.[ch], gcc/unwind*, gcc/gthr*, gcc/coretypes.h,
gcc/crtstuff.c, gcc/defaults.h, gcc/dwarf2.h, gcc/emults.c, gcc/gbl-ctors.h, gcc/gcov-
io.h, gcc/libgcov.c,  gcc/tsystem.h, gcc/typeclass.h).

 - libdecnumber

 - libgomp

 - libssp

 - libstdc++-v3

 - libobjc

 - libmudflap

 - libgfortran

 - The libgnat-4.4 Ada support library and libgnatvsn library.

 - Various config files in gcc/config/ used in runtime libraries.

GCC RUNTIME LIBRARY EXCEPTION

Version 3.1, 31 March 2009

Copyright (C) 2009 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document,
but changing it is not allowed.

This GCC Runtime Library Exception ("Exception") is an additional permission under
section 7 of the GNU General Public License, version 3 ("GPLv3"). It applies to a given
file (the "Runtime Library") that bears a notice placed by the copyright holder of the
file stating that the file is governed by GPLv3 along with this Exception.

When you use GCC to compile a program, GCC may combine portions of certain GCC header
files and runtime libraries with the compiled program. The purpose of this Exception is
to allow compilation of non-GPL (including proprietary) programs to use, in this way,
the header files and runtime libraries covered by this Exception.

0. Definitions.

A file is an "Independent Module" if it either requires the Runtime Library for
execution after a Compilation Process, or makes use of an interface provided by the
Runtime Library, but is not otherwise based on the Runtime Library.

"GCC" means a version of the GNU Compiler Collection, with or without modifications,
governed by version 3 (or a specified later version) of the GNU General Public License
(GPL) with the option of using any subsequent versions published by the FSF.

"GPL-compatible Software" is software whose conditions of propagation, modification and
use would permit combination with GCC in accord with the license of GCC.

"Target Code" refers to output from any compiler for a real or virtual target processor
architecture, in executable form or suitable for input to an assembler, loader, linker
and/or execution phase. Notwithstanding that, Target Code does not include data in any
format that is used as a compiler intermediate representation, or used for producing a
compiler intermediate representation.
```

```
The "Compilation Process" transforms code entirely represented in non-intermediate
languages designed for human-written code, and/or in Java Virtual Machine byte code,
into Target Code. Thus, for example, use of source code generators and preprocessors
need not be considered part of the Compilation Process, since the Compilation Process
can be understood as starting with the output of the generators or preprocessors.

A Compilation Process is "Eligible" if it is done using GCC, alone or with other GPL-
compatible software, or if it is done without using any work based on GCC. For example,
using non-GPL-compatible Software to optimize any GCC intermediate representations
would not qualify as an Eligible Compilation Process.

1. Grant of Additional Permission.

You have permission to propagate a work of Target Code formed by combining the Runtime
Library with Independent Modules, even if such propagation would otherwise violate the
terms of GPLv3, provided that all Target Code was generated by Eligible Compilation
Processes. You may then convey such a combination under terms of your choice,
consistent with the licensing of the Independent Modules.

2. No Weakening of GCC Copyleft.

The availability of this Exception does not imply any general presumption that third-
party software is unaffected by the copyleft requirements of the license of GCC.
```

H6. Jemalloc

```
Unless otherwise specified, files in the jemalloc source distribution are subject to
the following license:

--------------------------------------------------------------------------------

Copyright (C) 2002-2018 Jason Evans <jasone@canonware.com>.

All rights reserved.

Copyright (C) 2007-2012 Mozilla Foundation.  All rights reserved.

Copyright (C) 2009-2018 Facebook, Inc.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice(s), this list
of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice(s), this
list of conditions and the following disclaimer in the documentation and/or other
materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER(S) ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT HOLDER(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
--------------------------------------------------------------------------------
```

H7. Leaflet

```
Copyright (c) 2010-2018, Vladimir Agafonkin

Copyright (c) 2010-2011, CloudMade

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

   1. Redistributions of source code must retain the above copyright notice, this list
of conditions and the following disclaimer.

   2. Redistributions in binary form must reproduce the above copyright notice, this
list of conditions and the following disclaimer in the documentation and/or other
materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

H8. Libpng

```
If you modify libpng you may insert additional notices immediately following this
sentence.

This code is released under the libpng license.

libpng versions 1.0.7, July 1, 2000 through 1.6.32, August 24, 2017 are Copyright (c)
2000-2002, 2004, 2006-2017 Glenn Randers-Pehrson, are derived from libpng-1.0.6, and
are distributed according to the same disclaimer and license as libpng-1.0.6 with the
following individuals added to the list of Contributing Authors:

   Simon-Pierre Cadieux

   Eric S. Raymond

   Mans Rullgard

   Cosmin Truta

   Gilles Vollant

   James Yu

   Mandar Sahastrabuddhe
```

```
   Google Inc.

   Vadim Barkov

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against
infringement.  There is no warranty that our efforts or the library will fulfill any of
your particular purposes or needs.  This library is provided with all faults, and the
entire risk of satisfactory quality, performance, accuracy, and effort is with the
user.

Some files in the "contrib" directory and some configure-generated files that are
distributed with libpng have other copyright owners and are released under other open
source licenses.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c)
1998-2000 Glenn Randers-Pehrson, are derived from libpng-0.96, and are distributed
according to the same disclaimer and license as libpng-0.96, with the following
individuals added to the list of Contributing Authors:

   Tom Lane

   Glenn Randers-Pehrson

   Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996-1997
Andreas Dilger, are derived from libpng-0.88, and are distributed according to the same
disclaimer and license as libpng-0.88, with the following individuals added to the list
of Contributing Authors:

   John Bowler

   Kevin Bracey

   Sam Bushell

   Magnus Holmgren

   Greg Roelofs

   Tom Tanner

Some files in the "scripts" directory have other copyright owners but are released
under this license.

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995-1996
Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as
the following set of individuals:

   Andreas Dilger

   Dave Martindale

   Guy Eric Schalnat

   Paul Schmidt
```

```
   Tim Wegner

The PNG Reference Library is supplied "AS IS".  The Contributing Authors and Group 42,
Inc. disclaim all warranties, expressed or implied, including, without limitation, the
warranties of merchantability and of fitness for any purpose.  The Contributing Authors
and Group 42, Inc. assume no liability for direct, indirect, incidental, special,
exemplary, or consequential damages, which may result from the use of the PNG Reference
Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or
portions hereof, for any purpose, without fee, subject to the following restrictions:

  1. The origin of this source code must not be misrepresented.

  2. Altered versions must be plainly marked as such and must not be misrepresented as
being the original source.

  3. This Copyright notice may not be removed or altered from any source or altered
source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and
encourage the use of this source code as a component to supporting the PNG file format
in commercial products.  If you use this source code in a product, acknowledgment is
not required but would be appreciated.



Glenn Randers-Pehrson

glennrp at users.sourceforge.net

April 1, 2017
```

H9. Libradius

```
 Copyright 1998 Juniper Networks, Inc.

 All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

 1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

 2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3 2012/04/21 18:30:48 melifaro
Exp $
```

H10. Libssh2

```
Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>

Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>

Copyright (c) 2006-2007 The Written Word, Inc.

Copyright (c) 2007 Eli Fant <elifantu@mail.ru>

Copyright (c) 2009-2014 Daniel Stenberg

Copyright (C) 2008, 2009 Simon Josefsson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

Neither the name of the copyright holder nor the names of any other contributors may be
used to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

H11. Linenoise NG

linenoise

```
Copyright (c) 2010, Salvatore Sanfilippo <antirez at gmail dot com>

Copyright (c) 2010, Pieter Noordhuis <pcnoordhuis at gmail dot com>

All rights reserved.
```

```
Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

  * Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

  * Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

  * Neither the name of Redis nor the names of its contributors may be used to endorse
or promote products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

wcwidth

```
Markus Kuhn -- 2007-05-26 (Unicode 5.0)

Permission to use, copy, modify, and distribute this software for any purpose and
without fee is hereby granted. The author disclaims all warranties with regard to this
software.
```

ConvertUTF

```
Copyright 2001-2004 Unicode, Inc.

 Disclaimer

 This source code is provided as is by Unicode, Inc. No claims are made as to fitness
for any particular purpose. No warranties of any kind are expressed or implied. The
recipient agrees to determine applicability of information provided. If this file has
been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any
claim will be exchange of defective media within 90 days of receipt.

 Limitations on Rights to Redistribute This Code

 Unicode, Inc. hereby grants the right to freely use the information supplied in this
file in the creation of products supporting the Unicode Standard, and to make copies of
this file in any form for internal or external distribution as long as this notice
remains attached.
```

H12. Net-snmp

```
Various copyrights apply to this package, listed in various separate parts below.
Please make sure that you read all the parts.
```

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

```
Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or
product names may not be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be
used to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC
```

```
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used
to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

H13. Noto Sans CJK

```
Copyright (c) <dates>, <Copyright Holder> (<URL|email>), with Reserved Font Name
<Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>), with Reserved Font
Name <additional Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>).

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at:

http://scripts.sil.org/OFL

-----------------------------------------------------------

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

-----------------------------------------------------------

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of
collaborative font projects, to support the font creation efforts of academic and
linguistic communities, and to provide a free and open framework in which fonts may be
shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed
freely as long as they are not sold by themselves. The fonts, including any derivative
works, can be bundled, embedded, redistributed and/or sold with any software provided
```

that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A

```
PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT.
IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL
DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE
USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.
```

H14. OpenLDAP

```
The OpenLDAP Public License

  Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with
or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and
notices, this list of conditions, and the following disclaimer in the documentation
and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is
distinguished by a version number. You may use this Software under terms of this
license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND
ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN
NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S)
OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE  POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or
otherwise to promote the sale, use or other dealing in this Software without specific,
written prior permission.  Title to copyright in this Software shall at all times
remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA.  All Rights
Reserved.  Permission to copy and distribute verbatim copies of this document is
granted.
```

H15. OpenSSL

```
Copyright (c) 1998-2018 The OpenSSL Project.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:
```

```
1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

3. All advertising materials mentioning features or use of this software must display
the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL
Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or
promote products derived from this software without prior written permission. For
written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL"
appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL
Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL
PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

====================================================================

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
 This product includes software written by Tim Hudson (tjh@cryptsoft.com).

 Original SSLeay License

 -----------------------

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following
conditions are aheared to.  The following conditions apply to all code found in this
distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code.  The
SSL documentation included with this distribution is covered by the same copyright
terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not
to be removed.
```

```
If this package is used in a product, Eric Young should be given attribution as the
author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation
(online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

3. All advertising materials mentioning features or use of this software must display
the following acknowledgement:

   "This product includes cryptographic software written by Eric Young
(eay@cryptsoft.com)"

   The word 'cryptographic' can be left out if the rouines from the library being used
are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps
directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative
of this code cannot be changed.  i.e. this code cannot simply be copied and put under
another distribution licence [including the GNU Public Licence.]
```

H16. Oracle Instant Client

```
Export Controls on the Programs

Selecting the "Accept License Agreement" button is a confirmation of your agreement
that you comply, now and during the trial term, with each of the following statements:

-You are not a citizen, national, or resident of, and are not under control of, the
government of Cuba, Iran, Sudan, Libya, North Korea, Syria, nor any country to which
the United States has prohibited export.

-You will not download or otherwise export or re-export the Programs, directly or
indirectly, to the above mentioned countries nor to citizens, nationals or residents of
those countries.
```

-You are not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor are you listed on the United States Department of Commerce Table of Denial Orders.

You will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists.

You will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (http://www.oracle.com/products/export).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.

The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to the Software Products referenced below that you wish to download and use and Program documentation. "License" refers to your right to use the Programs and Program documentation under the terms of this Agreement. The substantive and procedural laws of California govern this Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.

Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at
http://www.oracle.com/technetwork/indexes/documentation/index.html.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name,

address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy of the Programs for backup purposes.

You may not:

-use the Programs for any purpose other than as provided above;

-charge your end users for use of the Programs;

-remove or modify any Program markings or any notice of our proprietary rights;

-assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;

-cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;

-disclose results of any Program benchmark tests without our prior consent.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at http://www.oracle.com/products/export/index.html. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Last updated: 01/24/08

H17. ParaType Free Font

LICENSING AGREEMENT

```
for the fonts with Original Name: PT Sans, PT Serif, PT Mono

Version 1.3 - January 20, 2012

GRANT OF LICENSE

ParaType Ltd grants you the right to use, copy, modify the fonts and distribute
modified and unmodified copies of the fonts by any means, including placing on Web
servers for free downloading, embedding in documents and Web pages, bundling with
commercial and non commercial products, if it does not conflict with the conditions
listed below:

- You may bundle the fonts with commercial software, but you may not sell the fonts by
themselves. They are free.

- You may distribute the fonts in modified or unmodified versions only together with
this Licensing Agreement and with above copyright notice. You have no right to modify
the text of Licensing Agreement. It can be placed in a separate text file or inserted
into the font file, but it must be easily viewed by users.

- You may not distribute modified version of the font under the Original name or a
combination of Original name with any other words without explicit written permission
from ParaType.

TERMINATION & TERRITORY

This license has no limits on time and territory, but it becomes null and void if any
of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT.
IN NO EVENT SHALL PARATYPE BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY
TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

ParaType Ltd
```

H18. PCRE

```
PCRE2 is a library of functions to support regular expressions whose syntax and
semantics are as close as possible to those of the Perl 5 language.

Release 10 of PCRE2 is distributed under the terms of the "BSD" licence, as specified
below, with one exemption for certain binary redistributions. The documentation for
PCRE2, supplied in the "doc" directory, is distributed under the same terms as the
software itself. The data in the testdata directory is not copyrighted and is in the
public domain.

The basic library functions are written in C and are freestanding. Also included in the
distribution is a just-in-time compiler that can be used to optimize pattern matching.
This is an optional feature that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS
```

```
--------------------------

Written by:       Philip Hazel

Email local part: ph10

Email domain:     cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2018 University of Cambridge

All rights reserved.

PCRE2 JUST-IN-TIME COMPILATION SUPPORT

-------------------------------------

Written by:       Zoltan Herczeg

Email local part: hzmester

Email domain:     freemail.hu

Copyright(c) 2010-2018 Zoltan Herczeg

All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

--------------------------------

Written by:       Zoltan Herczeg

Email local part: hzmester

Email domain:     freemail.hu

Copyright(c) 2009-2018 Zoltan Herczeg

All rights reserved.

THE "BSD" LICENCE

-----------------

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

 * Redistributions of source code must retain the above copyright notices, this list of
conditions and the following disclaimer.

 * Redistributions in binary form must reproduce the above copyright notices, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.
```

```
  * Neither the name of the University of Cambridge nor the names of any contributors
may be used to endorse or promote products derived from this      software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

EXEMPTION FOR BINARY LIBRARY-LIKE PACKAGES

----------------------------------------

The second condition in the BSD licence (covering binary redistributions) does not
apply all the way down a chain of software. If binary package A includes PCRE2, it must
respect the condition, but if package B is software that includes package A, the
condition is not imposed on package B unless it uses PCRE2 independently.
```

H19. Script.aculo.us

```
Copyright © 2005-2008 Thomas Fuchs (http://script.aculo.us, http://mir.aculo.us)

Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the “Software”), to deal in the Software
without restriction, including without limitation the rights to use, copy, modify,
merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be included in all copies
or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR
THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

H20. Zlib

```
zlib.h -- interface of the 'zlib' general purpose compression library

  version 1.2.11, January 15th, 2017

  Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

  This software is provided 'as-is', without any express or implied warranty.  In no
event will the authors be held liable for any damages arising from the use of this
software.
```

```
  Permission is granted to anyone to use this software for any purpose, including
commercial applications, and to alter it and redistribute it freely, subject to the
following restrictions:

  1. The origin of this software must not be misrepresented; you must not claim that
you wrote the original software. If you use this software in a product, an
acknowledgment in the product documentation would be appreciated but is not required.

  2. Altered source versions must be plainly marked as such, and must not be
misrepresented as being the original software.

  3. This notice may not be removed or altered from any source distribution.

  Jean-loup Gailly        Mark Adler

  jloup@gzip.org          madler@alumni.caltech.edu
```

Глава 3: Часто задаваемые вопросы

Перенос Сервера Dr.Web на другой компьютер (для ОС Windows)

При переносе Сервера на другой компьютер обратите внимание на настройки транспортных протоколов и, при необходимости, внесите соответствующие изменения в разделе **Администрирование** → **Конфигурация Сервера Dr.Web**, на вкладке **Транспорт**.

Процедура запуска и останова Сервера Dr.Web описана в **Руководстве администратора**, в п. Запуск и останов Сервера Dr.Web.

Чтобы перенести Сервер Dr.Web (при установке аналогичной версии Сервера Dr.Web) под ОС Windows

1. Остановите службу Сервера Dr.Web.
2. Запустите из командной строки файл `drwcsd.exe` с ключом `exportdb` для экспорта содержимого базы данных в файл. Полная командная строка для экспорта в версии под ОС Windows будет выглядеть примерно так:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log exportdb <полное_имя_файла>
   ```

3. Сохраните содержимое директории `C:\Program Files\DrWeb Server\etc`, а также ключ `drwcsd.pub` из `C:\Program Files\DrWeb Server\webmin\install`.
4. Удалите Сервер.
5. Установите новый Сервер (пустой, с новой базой) на нужном компьютере. Остановите службу Сервера Dr.Web с помощью средств управления службами ОС Windows или с помощью Центра управления.
6. Скопируйте содержимое сохраненного ранее каталога `etc` в `C:\Program Files\DrWeb Server\etc`, а также ключ `drwcsd.pub` и сертификат `drwcsd-certificate.pem` в `C:\Program Files\DrWeb Server\webmin\install`.
7. Запустите из командной строки файл `drwcsd.exe` с ключом `importdb` для импорта содержимого базы данных из файла. Полная командная строка для импорта в версии под ОС Windows будет выглядеть примерно так:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log importdb <полное_имя_файла>
   ```

8. Запустите службу Сервера Dr.Web.

При использовании встроенной базы данных можно не производить экспорт и импорт БД, а просто сохранить файл встроенной базы `database.sqlite` и заменить новый файл БД на установленном Сервере старым файлом, сохраненным от предыдущего Сервера.

Чтобы перенести Сервер Dr.Web (при установке другой версии Сервера Dr.Web) под ОС Windows

1. Остановите службу Сервера Dr.Web.
2. Сохраните базу данных средствами SQL сервера (если используется встроенная БД, то просто сохраните файл `database.sqlite`).
3. Сохраните содержимое директории `C:\Program Files\DrWeb Server\etc`, а также ключ `drwcsd.pub` из `C:\Program Files\DrWeb Server\webmin\install`.
4. Удалите Сервер.
5. Установите новый Сервер (пустой, с новой базой) на нужном компьютере. Остановите службу Сервера Dr.Web с помощью средств управления службами ОС Windows или с помощью Центра управления.
6. Скопируйте содержимое сохраненного ранее каталога `etc` в `C:\Program Files\DrWeb Server\etc`, а также ключ `drwcsd.pub` и сертификат `drwcsd-certificate.pem` в `C:\Program Files\DrWeb Server\webmin\install`.
7. Восстановите базу данных на новом Сервере, укажите в конфигурационном файле `drwcsd.conf` путь до базы данных.
8. Запустите из командной строки файл `drwcsd.exe` с ключом `upgradedb` для обновления базы данных. Полная командная строка для импорта в версии под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log upgradedb
"C:\Program Files\DrWeb Server\update-db"
```

9. Запустите службу Сервера Dr.Web.

В случае смены имени или IP-адреса при переносе Сервера Dr.Web:

Для возможности перехода Агентов, для которых адрес нового Сервера задается через Центр управления, а не в настройках самого Агента на станции, оставьте включенными оба Сервера до момента завершения процедуры.

1. Осуществите перенос Сервера согласно соответствующей процедуре, описанной выше.
2. Для всех Агентов, которых обслуживал старый Сервер, задайте адрес нового Сервера согласно соответствующей процедуре из раздела Подключение Агента Dr.Web к другому Серверу Dr.Web.

Для Агентов, для которых адрес нового Сервера задавался через Центр управления, а не в настройках самого Агента на станции, на обоих Серверах в настройках Агента должен быть указан адрес нового Сервера.

3. Дождитесь, пока все Агенты перейдут на новый Сервер. После этого можете удалять старый Сервер.

Подключение Агента Dr.Web к другому Серверу Dr.Web

Подключение Агента к другому Серверу возможно выполнить двумя способами:

1. Через Центр управления.

   Удаленная настройка без непосредственного доступа к станции возможна в том случае, если станция все еще подключена к старому Серверу. При этом необходим доступ к Центрам управления как старого, так и нового Серверов.

2. Непосредственно на самой станции.

   Для выполнения действий непосредственно на самой станции требуются права администратора данной станции и права на изменение настроек Агента, устанавливаемые на Сервере. При отсутствии данных прав переподключение к другому Серверу локально на станции возможно только после удаления установленного Агента и установки нового Агента с настройками нового Сервера. В случае отсутствия прав на удаление Агента локально, используйте утилиту Dr.Web Remover для удаление Агента на станции или удалите Агент через Центр управления.

Чтобы переключить Агента Dr.Web на другой Сервер Dr.Web при помощи Центра управления

1. На новом Сервере разрешите станциям с неверными параметрами авторизации запрашивать новые параметры авторизации в качестве новичков. Для этого в Центре управления выберите пункт **Администрирование** главного меню → пункт **Конфигурация Сервера Dr.Web** управляющего меню → вкладка **Общие**:
   a) Установите флаг **Переводить неавторизованных в новички**, если он снят.
   b) Если в выпадающем списке **Режим регистрации новичков** выбран вариант **Всегда отказывать в доступе**, измените его на **Подтверждать доступ вручную** или **Автоматически разрешать доступ**.
   c) Для применения внесенных изменений нажмите кнопку **Сохранить** и перезагрузите Сервер.

   Если политика сети компании не разрешает изменения настроек из шага 1, тогда параметры авторизации станции, соответствующие учетной записи, созданной заранее в Центре управления, необходимо задать непосредственно на станции.

2. На старом Сервере, к которому подключен Агент, задайте параметры нового Сервера. Для этого в Центре управления выберите в главном меню пункт **Антивирусная сеть** → в иерархическом списке сети выберите нужную станцию (или группу для переподключения всех станций этой группы) → в управляющем меню выберите пункт **Параметры подключения**:
   a) Если сертификат нового Сервера не совпадает с сертификатом старого Сервера, в поле **Сертификат** задайте путь до сертификата нового Сервера.
   b) В поле **Сервер** задайте адрес нового Сервера.
   c) Нажмите кнопку **Сохранить**.

Чтобы переключить Агента Dr.Web на другой Сервер Dr.Web непосредственно на самой станции

1. В настройках Агента задайте параметры нового Сервера. Для этого в контекстном меню значка Агента выберите: **Настройки** → вкладка **Основные** → пункт **Сервер** → раздел **Параметры соединения** → кнопка **Изменить настройки**:
   a) Если сертификат нового Сервера не совпадает с сертификатом старого Сервера, по кнопке **Список сертификатов** задайте путь до сертификата нового Сервера.
   b) По кнопке **Добавить** задайте соответствующие параметры нового Сервера.
2. Переведите станцию в новички (сбросьте параметры авторизации на Сервере). Для этого в разделе настроек параметров соединения из шага 1 нажмите следующее: кнопка **Параметры подключения станции** → кнопка **Сбросить параметры и подключиться как новичок** → кнопка **Сбросить параметры**.

Если вам заранее известны ID и пароль для подключения к новому Серверу, вы можете указать их в полях **ID станции** и **Пароль**. При этом нет необходимости переводить станцию в новички.

Смена типа СУБД Dr.Web Enterprise Security Suite

Для ОС Windows

Процедура запуска и останова Сервера Dr.Web описана в **Руководстве администратора**, в п. Запуск и останов Сервера Dr.Web.

1. Остановите службу Сервера Dr.Web.
2. Запустите из командной строки файл `drwcsd.exe` с ключом `exportdb` для экспорта содержимого базы данных в файл. Полная командная строка для экспорта в версии под ОС Windows будет выглядеть примерно так:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log=drwcsd.log exportdb D:\esbase.es
   ```

   В данном примере подразумевается, что Сервер Dr.Web установлен в каталоге `C:\Program Files\DrWeb Server`, а экспорт базы производится в некий файл `esbase.es` в корне диска `D`.

   Если в пути к файлу присутствуют пробелы и/или национальные символы (или имя файла содержит пробелы и/или национальные символы), то путь нужно заключить в кавычки:

   ```
   "D:\<длинное имя>\esbase.es"
   ```

3. Запустите службу Сервера Dr.Web, подключите к нему Центр управления и перенастройте Сервер на использование другой СУБД. Откажитесь от предложения перезапустить Сервер.
4. Остановите службу Сервера Dr.Web.
5. Удалите файл базы данных.
6. Запустите из командной строки файл `drwcsd.exe` с ключом `initdb` для инициализации новой базы данных. Строка инициализации базы данных для версии Сервера под ОС Windows будет выглядеть примерно так:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log=drwcsd.log -- initdb D:\Keys\agent.key - - <пароль>
   ```

   Подразумевается, что Сервер установлен в каталоге `"C:\Program Files\DrWeb Server"`, а агентский ключ `agent.key` лежит в `D:\Keys`.

   Если в пути к файлу присутствуют пробелы и/или национальные символы (или имя файла содержит пробелы и/или национальные символы), то путь нужно заключить в кавычки:

```
"D:\<длинное имя>\agent.key"
```

7. Запустите из командной строки файл `drwcsd.exe` с ключом `importdb` для импорта содержимого базы данных из файла. Полная командная строка для импорта в версии под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log importdb D:\esbase.es"
```

8. Запустите службу Сервера Dr.Web.

Для ОС семейства UNIX

1. Остановите службу Сервера Dr.Web с помощью скрипта:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd stop
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd stop
```

   или с помощью Центра управления.

2. Запустите Сервер с ключом `exportdb` для экспорта содержимого базы данных в файл. Командная строка из каталога установки Сервера будет выглядеть примерно так:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd -log=drwcsd.log exportdb /var/opt/drwcs/esbase.es
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log exportdb /var/drwcs/esbase.es
```

   В данном примере подразумевается, что экспорт базы производится в файл `esbase.es`, расположенный в каталоге пользователя.

3. Запустите службу Сервера Dr.Web с помощью скрипта:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd start
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd start
```

подключите к нему Центр управления и перенастройте Сервер на использование другой СУБД: в меню **Администрирование** → пункт **Конфигурация Сервера Dr.Web** → вкладка **База данных**.

Перенастройку Сервера на использование другой СУБД также можно осуществить, отредактировав напрямую конфигурационный файл Сервера `drwcsd.conf`. Для этого следует закомментировать/удалить запись о текущей БД и прописать новую базу (подробнее см. Приложение Ж1. Конфигурационный файл Сервера Dr.Web).

Откажитесь от предложения перезапустить Сервер.

4. Остановите Сервер Dr.Web (см. шаг **1**).
5. Удалите файл базы данных.
6. Запустите файл `drwcsd` с ключом `initdb` для инициализации новой базы данных. Строка инициализации будет выглядеть примерно так:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd -log=drwcsd.log initdb
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log initdb
```

7. Запустите файл `drwcsd` с ключом `importdb` для импорта содержимого базы данных из файла. Командная строка для импорта будет выглядеть примерно так:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd -log=drwcsd.log importdb /var/opt/drwcs/esbase.es
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log importdb /var/drwcs/esbase.es
```

8. Запустите Сервер Dr.Web (см. шаг **3**).

Если при запуске скрипта Сервера требуется задать параметры (например, указать каталог установки Сервера, изменить уровень подробности лога и т. п.), изменение соответствующих значений производится в стартовом скрипте:

- для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd
```

- для ОС **Linux**:

```
/etc/init.d/drwcsd
```

Восстановление базы данных Dr.Web Enterprise Security Suite

В процессе работы Сервер Dr.Web регулярно сохраняет резервные копии важной информации: лицензионных ключей, содержимого базы данных, закрытого ключа шифрования, конфигурации Сервера и Центра управления.

Резервные копии сохраняются в следующих каталогах:

- для ОС **Windows**: <*диск_установки*>`:\DrWeb Backup`
- для ОС **Linux**: `/var/opt/drwcs/backup`
- для ОС **FreeBSD**: `/var/drwcs/backup`

Для выполнения функции резервного копирования в расписание Сервера включено ежедневное задание. Если такое задание в расписании отсутствует, рекомендуется создать его.

Все файлы из резервной копии, кроме содержимого базы данных, готовы к использованию. Резервная копия базы данных сохраняется в формате `.gz`, совместимом с `gzip` и другими архиваторами. Содержимое базы данных можно импортировать из резервной копии в рабочую базу данных Сервера при помощи команды `importdb` и таким образом восстановить данные.

Для восстановления базы данных также может использоваться резервная копия, созданная администратором вручную через Центр управления в разделе **Администрирование** → **Управление базой данных** → **Экспорт** (только для режима **Экспортировать всю базу данных**). Однако, при этом резервная копия сохраняется в формате xml, и для импорта необходимо использовать команду `xmlimportdb`.

Восстановление БД для различных версий Сервера Dr.Web

Восстановить базу данных можно только из резервной копии, созданной при помощи Сервера с той же мажорной версией, что и версия Сервера, на котором происходит восстановление.

Например:

- БД из резервной копии, созданной при помощи Сервера версии 10, можно восстановить, используя Сервер только версии 10.
- БД из резервной копии, созданной при помощи Сервера версии 5 или 6, нельзя восстановить, используя Сервер версии 10.

Если во время обновления Сервера на версию 12.0 с более ранних версий по каким-либо причинам была повреждена БД, выполните следующее:

1. Удалите Сервер версии 12.0. При этом будут автоматически сохранены резервные копии файлов, используемых Сервером.

2. Установите Сервер той версии, которая стояла до обновления и при помощи которой создавалась резервная копия.

   При этом, согласно штатной процедуре обновления, следует использовать все сохраненные файлы Сервера кроме файла базы данных.

   В процессе установки Сервера создайте новую базу данных.
3. Восстановите базу данных из резервной копии по общим правилам (см. ниже).
4. В настройках Сервера отключите протоколы Агента, Сервера и Сетевого инсталлятора. Для этого выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**, перейдите на вкладку **Модули** и снимите соответствующие флаги.
5. Обновите Сервер до версии 12.0 по общим правилам (см. в **Руководстве администратора** п. Обновление Dr.Web Enterprise Security Suite и его отдельных компонентов).
6. Включите протоколы Агента, Сервера и Сетевого инсталлятора, отключенные на шаге 4.

Для ОС Windows

Процедура запуска и останова Сервера Dr.Web описана в **Руководстве администратора**, в п. Запуск и останов Сервера Dr.Web.

Чтобы восстановить БД из резервной копии

1. Остановите службу Сервера Dr.Web, если она запущена.
2. Импортируйте из соответствующего файла резервной копии содержимое базы данных. Строка импорта выглядит примерно так:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log importdb "<путь_к_бэкап_файлу>\database.gz"
   ```

   Данная команда тоже должна быть набрана в одну строку. В примере подразумевается, что Сервер установлен в каталоге `C:\Program Files\DrWeb Server`.
3. Запустите службу Сервера Dr.Web.

Чтобы восстановить БД из резервной копии при смене версии Сервера Dr.Web (в пределах одной мажорной версии) или порче текущей версии БД

1. Остановите службу Сервера Dr.Web, если она запущена.
2. Удалите содержимое текущей БД. Для этого:

   2.1. При использовании встроенной БД:

a) Удалите файл базы данных `database.sqlite`.

b) Произведите инициализацию новой базы данных. Строка инициализации базы данных в версии Сервера под ОС Windows будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log -- initdb D:\Keys\agent.key - - <пароль>
```

Данная команда должна быть набрана в одну строку (см. также формат команды `drwcsd` с ключом `initdb` в Приложении 33.3. Команды для управления базой данных). В примере подразумевается, что Сервер установлен в каталоге `C:\Program Files\DrWeb Server`, а лицензионный ключ `agent.key` лежит в каталоге `D:\Keys`.

c) После выполнения этой команды в подкаталоге `var` каталога установки Сервера Dr.Web должен появиться новый файл базы `database.sqlite`.

2.2. При использовании внешней БД: произведите очистку БД при помощи команды `cleandb` (см. Приложение 33.3. Команды для управления базой данных).

3. Импортируйте из соответствующего файла резервной копии содержимое базы данных. Строка импорта выглядит примерно так:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log importdb "<путь_к_бэкап_файлу>\database.gz"
```

Данная команда тоже должна быть набрана в одну строку. В примере подразумевается, что Сервер установлен в каталоге `C:\Program Files\DrWeb Server`.

4. Запустите службу Сервера Dr.Web.

Для ОС семейства UNIX

1. Остановите Сервер Dr.Web (если он запущен):

- для ОС **Linux**:

```
/etc/init.d/drwcsd stop
```

- для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd stop
```

2. Удалите файл базы данных `database.sqlite` из следующей директории каталога установки Сервера Dr.Web:

- для ОС **Linux**: `/var/opt/drwcs/`
- для ОС **FreeBSD**: `/var/drwcs/`

При использовании внешней БД ее очистка осуществляется при помощи команды `cleandb` (см. Приложение 33.3. Команды для управления базой данных).

3. Инициализируйте базу данных Сервера. Для этого служит следующая команда:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd -log=drwcsd.log initdb
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log initdb
```

4. После выполнения этой команды в папке `var` каталога установки Сервера Dr.Web должен появиться новый файл базы `database.sqlite`.
5. Импортируйте из соответствующего файла резервной копии содержимое базы данных. Строка импорта выглядит примерно так:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd -log=drwcsd.log importdb
"<путь_к_бэкап_файлу>/database.gz"
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log importdb
"<путь_к_бэкап_файлу>/database.gz"
```

6. Запустите Сервер Dr.Web.
   - для ОС **Linux**:

```
/etc/init.d/drwcsd start
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd start
```

Если при запуске скрипта Сервера требуется задать параметры (например, указать каталог установки Сервера и т. п.), изменение соответствующих значений производится в стартовом скрипте:

- для ОС FreeBSD: `/usr/local/etc/rc.d/drwcsd`;
- для ОС Linux: `/etc/init.d/drwcsd`.

Если требуется изменить уровень подробности журнала Сервера, для этого используйте файл `local.conf`:

- для ОС Linux: `/var/opt/drwcs/etc/local.conf`;
- для ОС FreeBSD: `/var/drwcs/etc/local.conf`.

Если какие-либо Агенты были установлены после создания последней резервной копии, они не смогут подключиться к Серверу после восстановления базы данных из этой резервной копии. Такие станции можно дистанционно перевести в режим новичков. В разделе **Администрирование** → **Конфигурация Сервера Dr.Web** на вкладке **Общие** установите флаг **Переводить неавторизованных в новички**. В выпадающем списке **Режим регистрации новичков** выберите вариант **Автоматически разрешать доступ**. Нажмите **Сохранить** и перезагрузите Сервер.

После того как все станции благополучно подключатся к новому Серверу, измените данные настройки Сервера на настройки, принятые в соответствии с политикой вашей компании.

После восстановления базы рекомендуется подключиться к Серверу через Центр управления, открыть раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web** и проверить в нем наличие задания **Резервное копирование критичных данных сервера**. Если такое задание отсутствует, рекомендуется его создать.

Обновление Агентов на серверах ЛВС

При обновлении Агентов, установленных на серверах ЛВС, могут быть нежелательны перезагрузки станций или остановы сетевого ПО, работающего на таких станциях.

Во избежание функционального простоя станций, выполняющих важные функции ЛВС, предлагается следующий режим обновления Агентов и антивирусного ПО:

1. В расписании Сервера изменить стандартные задания для обновления всех компонентов на обновление только вирусных баз.
2. Создать новое задание на обновление всех компонентов в удобное время, когда это не скажется критически на работе серверов ЛВС.

   Создание и редактирование заданий в расписании Сервера приведено в **Руководстве администратора** п. Настройка расписания Сервера Dr.Web.

На серверы, выполняющие важные сетевые функции (домен-контроллеры, серверы раздачи лицензий и т. д.), не рекомендуется устанавливать компоненты SpIDer Gate, SpIDer Mail и Брандмауэр Dr.Web во избежание возможных конфликтов сетевых сервисов и внутренних компонентов антивируса Dr.Web.

Восстановление пароля администратора Dr.Web Enterprise Security Suite

В случае, если пароль администратора для доступа к Серверу Dr.Web был утерян, существует возможность его просмотра или изменения с использованием прямого доступа к базе данных Сервера:

a) При использовании встроенной базы для просмотра и смены пароля администратора используется утилита `drwidbsh`, входящая в дистрибутив Сервера (см. п. 37.2. Утилита администрирования встроенной базы данных).

b) Для внешней БД используйте соответствующий sql-клиент.

> Параметры учетных записей администраторов хранятся в таблице `admins`.

Пример использования утилиты drwidbsh:

1. Запустите утилиту `drwidbsh3` с указанием пути до файла БД:
   - Для встроенной БД под ОС Linux:

```
/opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite
```

   - Для встроенной БД под ОС Windows:

```
"C:\Program Files\DrWeb Server\bin\drwidbsh3" "C:\Program Files\DrWeb Server\var\database.sqlite"
```

> Если используется встроенная база данных старого формата IntDB, например, в случае обновления Сервера с версии 6, то имя базы данных по умолчанию — `dbinternal.dbs`, а утилита для управления базой данных — `drwidbsh`.

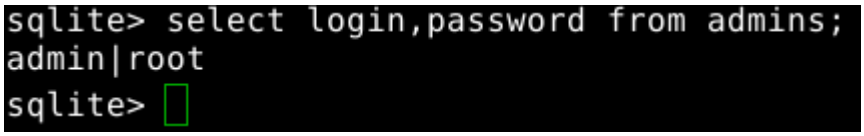
2. Для просмотра всех данных, хранящихся в таблице `admins`, выполните команду:

```
select * from admins;
```

3. Для просмотра имен и паролей для всех учетных записей администраторов выполните команду:

```
select login,password from admins;
```

4. Результат для варианта, когда существует только одна учетная запись с именем `admin` и у нее пароль `root`, приведен на скриншоте:



5. Для изменения пароля используйте команду `update`. Пример команды, изменяющей пароль от учетной записи `admin` на `qwerty`:

```
update admins set password='qwerty' where login='admin';
```

6. Для выхода из утилиты выполните команду:

```
.exit
```

Описание работы утилиты `drwidbsh` приведено в приложении 37.2. Утилита администрирования встроенной базы данных.

Использование DFS при установке Агента через Active Directory

При установке Агента Dr.Web через Active Directory возможно использование службы распределенной файловой системы (DFS).

Данный подход может быть удобен, например, при наличии в ЛВС нескольких контроллеров домена.

Чтобы установить Агент Dr.Web в сети с несколькими контроллерами домена

1. На каждом из контроллеров домена создать по каталогу с одинаковым именем.
2. При помощи DSF объединить созданные каталоги в один корневой целевой каталог.
3. Осуществить административную установку пакета `*.msi` в созданный целевой каталог (см. **Руководство по установке**, п. Установка Агента Dr.Web с использованием службы Active Directory).
4. Полученный целевой каталог использовать при назначении пакета в редакторе объектов групповой политики.

   При этом использовать сетевое имя вида: `\\`<*domain*>`\`<*folder*>

   где: <*domain*> — имя домена, <*folder*> — название целевого каталога.

Восстановление антивирусной сети после отказа Сервера Dr.Web

В случае фатального отказа Сервера Dr.Web рекомендуется воспользоваться приведенными процедурами для восстановления работоспособности антивирусной сети без переустановки Агентов на станциях.

Подразумевается, что новый Сервер Dr.Web будет установлен на компьютере с тем же IP-адресом и DNS-именем.

Восстановление при наличии резервной копии Сервера Dr.Web

В процессе работы Сервер Dr.Web регулярно сохраняет резервные копии важной информации: лицензионных ключей, содержимого базы данных, закрытого ключа шифрования, конфигурации Сервера и Центра управления.

Резервные копии сохраняются в следующих каталогах:

- для ОС **Windows**: <*диск_установки*>`:\DrWeb Backup`
- для ОС **Linux**: `/var/opt/drwcs/backup`
- для ОС **FreeBSD**: `/var/drwcs/backup`

Для выполнения функции резервного копирования в расписание Сервера включено ежедневное задание. Если такое задание в расписании отсутствует, рекомендуется создать его.

Все файлы из резервной копии, кроме содержимого базы данных, готовы к использованию. Резервная копия базы данных сохраняется в формате `.gz`, совместимом с `gzip` и другими архиваторами. Содержимое базы данных можно импортировать из резервной копии в рабочую базу данных Сервера при помощи команды `upimportdb` и таким образом восстановить данные.

Для восстановления базы данных также может использоваться резервная копия, созданная администратором вручную через Центр управления в разделе **Администрирование** → **Управление базой данных** → **Экспорт** (только для режима **Экспортировать всю базу данных**). Однако, при этом резервная копия сохраняется в формате xml, и для импорта необходимо использовать команду `xmlupimportdb`.

Также рекомендуется хранить на другом ПК создаваемые резервные копии и другие важные для вас файлы. Таким образом, вы сможете избежать потери данных при повреждении ПК, на котором установлен Сервер Dr.Web, и полностью восстановить данные и функциональность Сервера. В случае утраты лицензионных ключей их можно запросить заново, как указано в **Руководстве администратора**, п. Лицензирование.

Чтобы восстановить Сервер после отказа, если сохранилась резервная копия данных Сервера

1. Выберите компьютер, на который будет устанавливаться новый Сервер Dr.Web. Изолируйте данный компьютер от работающих Агентов: отключите его от сети, в которой установлены Агенты, или временно измените его IP-адрес, или воспользуйтесь любым другим наиболее удобным для вас способом.
2. Установите новый Сервер Dr.Web.
3. В разделе **Администрирование** → **Менеджер лицензий** добавьте лицензионный ключ от предыдущей установки Сервера и распространите его на соответствующие группы, в частности на группу **Everyone**. Шаг обязателен, если при установке Сервера не был задан лицензионный ключ.
4. Обновите репозиторий установленного Сервера с ВСО:
   a) Откройте раздел Центра управления **Администрирование** → **Состояние репозитория**.
   b) Нажмите кнопку **Проверить обновления** для проверки наличия обновлений всех продуктов на ВСО и загрузки имеющихся обновлений с серверов ВСО.
5. При наличии новых версий ПО Сервера, произведите обновление до последней версии:
   a) Откройте раздел Центра управления **Администрирование** → **Сервер Dr.Web**.
   b) Для перехода к списку версий Сервера нажмите на текущую версию Сервера или на кнопку **Список версий**. Откроется раздел **Обновления Сервера Dr.Web** со списком доступных обновлений и резервных копий Сервера.
   c) Для перехода к новой версии Сервера установите опцию напротив последней версии в списке **Все версии**. Нажмите кнопку **Сохранить**.
   d) Дождитесь завершения процесса обновления Сервера.
6. Остановите Сервер.
7. Для получения открытого ключа шифрования из резервной копии закрытого ключа воспользуйтесь утилитой `drwsign`, находящейся в подкаталоге `\bin` каталога установки Сервера:

   `drwsign extract [-private-key=<`*закрытый_ключ*`>] <`*открытый_ключ*`>`

   В качестве <*закрытый_ключ*> и <*открытый_ключ*> укажите соответствующие пути, по которым расположен закрытый ключ, а также куда следует разместить созданный открытый ключ.
8. Замените критичные данные Сервера на данные, полученные из резервной копии:

Операционная система	Открытый ключ шифрования	Конфигурационные файлы
Windows	`webmin\install` в каталоге установки Сервера	`etc` в каталоге установки Сервера

Операционная система	Открытый ключ шифрования	Конфигурационные файлы
Linux	`/opt/drwcs/webmin/install`	`/var/opt/drwcs/etc`
FreeBSD	`/usr/local/drwcs/webmin/install`	`/var/drwcs/etc`

9. Настройте базу данных.

   a) Внешняя база данных:

   Дальнейших действий по подключению базы данных к Серверу не требуется (при условии, что сохранен конфигурационный файл Сервера).

   Если версия Сервера, установленная из последних обновлений, позднее версии утраченного Сервера, произведите обновление внешней базы данных при помощи команды `upgradedb`:

   - для ОС Windows:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log
   upgradedb
   ```

   - для ОС Linux:

   ```
   /etc/init.d/drwcsd -log=drwcsd.log upgradedb
   ```

   - для ОС FreeBSD:

   ```
   /usr/local/etc/rc.d/drwcsd -log=drwcsd.log upgradedb
   ```

   b) Резервная копия базы данных внешней или встроенной:

   При использовании внешней базы данных предварительно произведите ее очистку при помощи команды `cleandb` (см. Приложение 33.3. Команды для управления базой данных).

   Импортируйте базу данных из соответствующего файла резервной копии с обновлением формата базы данных до версии установленного Сервера при помощи команды `upimportdb`:

   - для ОС Windows:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log=drwcsd.log upimportdb
   "<путь_к_бэкап_файлу>\database.gz"
   ```

   - для ОС Linux:

   ```
   /etc/init.d/drwcsd -log=drwcsd.log upimportdb
   "<путь_к_бэкап_файлу>/database.gz"
   ```

   - для ОС FreeBSD:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log upimportdb
"<путь_к_бэкап_файлу>/database.gz"
```

На все замененные файлы Сервера необходимо установить те же системные права, что были выбраны при предыдущей (утраченной) установке Сервера.

Для ОС семейства UNIX: `rw` для `drwcs:drwcs`.

10. Запустите Сервер.
11. Убедитесь в сохранности и актуальности данных, полученных из резервной копии базы данных: настроек Агентов, состояния дерева антивирусной сети и т. п.
12. Восстановите доступность Сервера для Агентов, исходя из способа изоляции Сервера, выбранного на шаге 1.

Если какие-либо Агенты были установлены после создания последней резервной копии, они не смогут подключиться к Серверу после восстановления базы данных из этой резервной копии. Такие станции можно дистанционно перевести в режим новичков. В разделе **Администрирование** → **Конфигурация Сервера Dr.Web** на вкладке **Общие** установите флаг **Переводить неавторизованных в новички**. В выпадающем списке **Режим регистрации новичков** выберите вариант **Автоматически разрешать доступ**. Нажмите **Сохранить** и перезагрузите Сервер.

После того, как все станции благополучно подключатся к новому Серверу, измените данные настройки Сервера, на настройки, принятые в соответствии с политикой вашей компании.

Восстановление при отсутствии резервной копии Сервера Dr.Web

Чтобы восстановить Сервер после отказа, если не сохранилось никаких резервных копий

1. Выберите компьютер, на который будет устанавливаться новый Сервер Dr.Web. Изолируйте данный компьютер от работающих Агентов: отключите его от сети, в которой установлены Агенты, или временно измените IP-адрес, или воспользуйтесь любым другим наиболее удобным для вас способом.
2. Установите новый Сервер Dr.Web.
3. В разделе **Администрирование** → **Менеджер лицензий** добавьте лицензионный ключ от предыдущей установки Сервера и распространите его на соответствующие группы, в частности на группу **Everyone**. Шаг обязателен, если при установке Сервера не был задан лицензионный ключ.
4. Обновите репозиторий установленного Сервера с ВСО:
   a) Откройте раздел Центра управления **Администрирование** → **Состояние репозитория**.

b) Нажмите кнопку **Проверить обновления** для проверки наличия обновлений всех продуктов на ВСО и загрузки имеющихся обновлений с серверов ВСО.

5. При наличии новых версий ПО Сервера, произведите обновление до последней версии:
   a) Откройте раздел Центра управления **Администрирование** → **Сервер Dr.Web**.
   b) Для перехода к списку версий Сервера нажмите на текущую версию Сервера или на кнопку **Список версий**. Откроется раздел **Обновления Сервера Dr.Web** со списком доступных обновлений и резервных копий Сервера.
   c) Для перехода к новой версии Сервера установите опцию напротив последней версии в списке **Все версии**. Нажмите кнопку **Сохранить**.
   d) Дождитесь завершения процесса обновления Сервера.
6. Измените настройки подключения станций в конфигурации Сервера:
   a) Откройте раздел **Администрирование** → **Конфигурация Сервера Dr.Web**.
   b) На вкладке **Общие** установите флаг **Переводить неавторизованных в новички**.
   c) На вкладке **Общие** в выпадающем списке **Режим регистрации новичков** выберите вариант **Автоматически разрешать доступ**.
   d) Нажмите **Сохранить** и перезагрузите Сервер.
7. В разделе **Антивирусная сеть** Центра управления создайте пользовательские группы в дереве антивирусной сети по аналогии с предыдущей версией. При необходимости создайте автоматические правила членства для станций в созданных пользовательских группах.
8. При необходимости задайте настройки Агентов и настройки Сервера (кроме временных настроек из шага 6) по аналогии с предыдущей версией.
9. При необходимости измените настройки репозитория в разделе **Администрирование** → **Детальная конфигурация репозитория**.
10. Восстановите доступность Сервера для Агентов, исходя из способа изоляции Сервера, выбранного на шаге 1.
11. Замените открытый ключ шифрования на всех станциях сети, которые должны будут подключиться к новому Серверу.
    - При включенной самозащите скопируйте на станцию открытый ключ, созданный при установке нового Сервера, и выполните следующую команду:

      ```
      es-service.exe -p <ключ>
      ```

      или

      ```
      es-service.exe --addpubkey=<ключ>
      ```

      В качестве *<ключ>* укажите путь к скопированному открытому ключу шифрования.

      В результате открытый ключ будет скопирован в каталог установки Агента. По умолчанию это каталог `%ProgramFiles%\DrWeb` (подробнее см. Приложение 32. Агент Dr.Web для Windows).
    - Если на станции отключена самозащита, можете взять открытый ключ, созданный при установке нового Сервера, и разместить его в указанный выше каталог.

12. После того, как все станции благополучно подключатся к новому Серверу, измените настройки Сервера, заданные на шаге 5, на настройки, принятые в соответствии с политикой вашей компании.

Управление уровнем ведения журнала Сервера Dr.Web под ОС Windows

Изменить уровень детализации журнала Сервера под ОС Windows можно одним из следующих способов:

- При помощи раздела **Конфигурация Сервера Dr.Web → Журнал** в Центре управления.

  Данный способ является предпочтительным. В разделе **Журнал** вы можете задать любой возможный уровень детализации журнала Сервера, а также некоторые другие его настройки.

  Подробная информация приведена в **Руководстве администратора**, в разделе Настройка конфигурации Сервера Dr.Web → Журнал.

- При помощи консольной команды:

  ```
  drwcsd [<ключи>] install
  ```

  Вы можете задать любой возможный уровень детализации журнала Сервера при помощи ключа `--verbosity`.

  Подробная информация по ключам командной строки для управления Сервером приведена в разделе 33.8. Описание ключей.

  Пример команды для установки уровня ведения журнала **Детальный**:

  ```
  drwcsd --daemon "--home=C:\Program Files\DrWeb Server" "--bin-root=C:
  \Program Files\DrWeb Server" "--var-root=C:\Program Files\DrWeb Server\var"
  --verbosity=ALL --log=drwcsd.log --rotate=10,50m install
  ```

  Остальные ключи являются обязательными, в частности, если были переопределены стандартные пути установки Сервера и его рабочих каталогов.

  После изменения уровня ведения журнала необходимо перезапустить Сервер:

  ```
  drwcsd restart
  ```

- При помощи команд, расположенных в главном меню ОС Windows **Пуск**.

  При этом доступны только два возможных уровня детализации журнала: **Детальный** или **Стандартный**:

  a) **Программы → Управление сервером → Детальный журнал**
  или
  Программы → Управление сервером → Стандартный журнал

  b) **Программы → Управление сервером → Перезапустить**.

Автоматическое определение местоположения станции под ОС Android

Dr.Web Enterprise Security Suite позволяет автоматически предоставлять информацию администратору о географическом местоположении защищаемых мобильных устройств под ОС Android.

Чтобы определить местоположение мобильного устройства

1. Настройте передачу данных о местоположении защищаемого мобильного устройства на Сервер Dr.Web:
   a) В Центре управления безопасностью Dr.Web, в разделе **Антивирусная сеть**, в дереве сети выберите интересующую вас станцию или группу станций под управлением ОС Android.
   b) Выберите пункт управляющего меню **Dr.Web для Android**.
   c) На вкладке **Общие** установите флаг **Отслеживать местоположение**. В выпадающем списке **Периодичность передачи координат** выберите значение, в соответствии с которым будут обновляться данные о местоположении устройства.
   d) Сохраните внесенные изменения.
2. Автоматическое определение местоположения осуществляется одним из следующих способов:
   - В случае, если на мобильном устройстве пользователя включены провайдеры местоположения (GPS, мобильные сети) и при наличии стабильного сигнала, определение местоположения осуществляется средствами самого мобильного устройства.
   - В случае, если на мобильном устройстве пользователя отключены провайдеры местоположения (GPS, мобильные сети) или отсутствует GPS-сигнал, Dr.Web Enterprise Security Suite предоставляет возможность использовать технологию Яндекс.Локатор для определения местоположения мобильного устройства по координатам вышек мобильной связи (GSM, 3D, LTE) и WiFi ID.
     Для настройки технологии Яндекс.Локатор необходимо активировать и настроить **Расширение Yandex.Locator**:
     a) Получите API-ключ на сайте компании Яндекс по адресу: https://yandex.ru/dev/locator/keys/get/.
     b) В Центре управления безопасностью Dr.Web, в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Модули** установите флаг **Расширение Yandex.Locator**.
     c) В поле **API-ключ** введите ключ, полученный на шаге a).
     d) Сохраните внесенные изменения и перезагрузите Сервер Dr.Web.

Использование WiFi ID возможно только для мобильных устройств под ОС Android 5.1 и более ранних версий.

3. Чтобы просмотреть местоположение станции в Центре управления безопасностью Dr.Web:
   a) В разделе **Антивирусная сеть**, в дереве сети выберите станцию, для которой были заданы соответствующие настройки на шаге 1.
   b) В свойствах станции, в разделе **Расположение** будут автоматически заполняться географические координаты, полученные с мобильного устройства.
   c) Нажмите **Показать на карте**, чтобы просмотреть географическое местоположение мобильного устройства на OpenStreetMap согласно полученным координатам.

Примеры обращения к базе данных Сервера Dr.Web

Далее приводятся примеры SQL-запросов к базе данных PostgreSQL. Запросы к другим базам данных могут содержать некоторые отличия, обусловленные особенностями самой базы данных и тонкостями её использования.

Возможности языка SQL не позволяют учитывать в запросах иерархию групп и станций.

Чтобы обратиться напрямую к базе данных

1. Откройте Центр управления вашего Сервера.
2. Перейдите в раздел **Администрирование** → **SQL-консоль**.
3. Введите необходимый SQL-запрос. Примеры запросов приведены далее.
4. Нажмите кнопку **Выполнить**.

Примеры SQL-запросов

1. Найти станции, на которых установлена серверная версия ОС Windows и на которых вирусные базы старее, чем 2019.07.04-00:00:00 UTC (12.0).

```
SELECT
  stations.name Station,
  groups_list.name OS,
  station_products.crev Bases
FROM
  stations
  INNER JOIN groups_list ON groups_list.platform =(
    CAST(stations.lastos AS INTEGER) & ~15728640
  )
  AND (
    (
      CAST(stations.lastos AS INTEGER) & 2130706560
    ) = 33554560
  )
  INNER JOIN station_products ON station_products.id = stations.id
  AND station_products.product = '10-drwbases'
  AND station_products.crev < 12020190704000000;
```

2. Найти станции, имеющие в разделе **Антивирусная сеть** → **Статистика** → **Состояние** записи с серьезностью **Высокая** или **Максимальная**.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id IN (
    SELECT
      DISTINCT id
    FROM
```

```
      station_status
    WHERE
      severity >= 1342177280
  );
```

3. Получить соответствие статусов и количества станций, имеющих эти статусы.

```
SELECT
  code Code,
  COUNT(code) Num
FROM
  (
    SELECT
      DISTINCT id,
      code
    FROM
      station_status
  ) AS t
GROUP BY
  Code
ORDER BY
  Code;
```

4. Получить 10 наиболее популярных угроз, обнаруженных с 2019.06.01 по 2019.07.01 на станциях, входящих в группу с идентификатором '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5' или в любые вложенные в неё группы.

```
SELECT
  cat_virus.str Threat,
  COUNT(cat_virus.str) Num
FROM
  station_infection
  INNER JOIN cat_virus ON cat_virus.id = station_infection.virus
WHERE
  station_infection.infectiontime BETWEEN 20190601000000000
  AND 20190701000000000
  AND station_infection.id IN (
    SELECT
      sid
    FROM
      station_groups
    WHERE
      gid = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      OR gid IN (
        SELECT
          child
        FROM
          group_children
        WHERE
          id = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      )
  )
GROUP BY
  cat_virus.str
ORDER BY
  Num DESC
LIMIT
  10;
```

5. Получить 10 наиболее заражаемых станций.

```
SELECT
  Station,
  Grp,
  Num
FROM
  (
    SELECT
      stations.id,
      groups_list.id,
      stations.name Station,
      groups_list.name Grp,
      COUNT(stations.id) Num
    FROM
      station_infection
      INNER JOIN stations ON station_infection.id = stations.id
      INNER JOIN groups_list ON groups_list.id = stations.gid
    GROUP BY
      stations.id,
      groups_list.id,
      stations.name,
      groups_list.name
    ORDER BY
      Num DESC
    LIMIT
      10
  ) AS t;
```

6. Удалить членство всех станций из пользовательских групп, которые не являются первичными для этих станций.

```
DELETE FROM
  station_groups;
INSERT INTO station_groups(sid, gid)
SELECT
  stations.id,
  groups_list.id
FROM
  stations
  INNER JOIN groups_list ON stations.gid = groups_list.id
  AND groups_list.type NOT IN(1, 4);
```

7. Найти объекты антивирусной сети, в которых указанный домен присутствует в белом списке компонента SplDer Gate, в персональных настройках.

```
SELECT
  stations.name Station
FROM
  station_cfg
  INNER JOIN stations ON stations.id = station_cfg.id
WHERE
  station_cfg.component = 38
  AND station_cfg.name = 'WhiteVirUrlList'
  AND station_cfg.value = 'domain.tld';
SELECT
  groups_list.name Grp
FROM
  group_cfg
  INNER JOIN groups_list ON groups_list.id = group_cfg.id
WHERE
  group_cfg.component = 38
```

```
  AND group_cfg.name = 'WhiteVirUrlList'
  AND group_cfg.value = 'domain.tld';
SELECT
  policy_list.name Policy
FROM
  policy_cfg
  INNER JOIN policy_list ON policy_list.id = policy_cfg.id
WHERE
  policy_cfg.component = 38
  AND policy_cfg.name = 'WhiteVirUrlList'
  AND policy_cfg.value = 'domain.tld';
```

8. Получить из аудита события неудачного входа администраторов в Центр управления с соответствующими кодами ошибки авторизации.

```
SELECT
  admin_activity.login Login,
  admin_activity.address Address,
  activity_data.value ErrorCode,
  admin_activity.createtime EventTimestamp
FROM
  admin_activity
  INNER JOIN activity_data ON admin_activity.record = activity_data.record
WHERE
  admin_activity.oper = 10100
  AND admin_activity.status != 1
  AND activity_data.item = 'Error';
```

9. Найти станции под ОС Windows, на которых не установлены необходимые исправления безопасности.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id NOT IN (
    SELECT
      station_env_kb.id
    FROM
      station_env_kb
      INNER JOIN stations ON stations.id = station_env_kb.id
    WHERE
      (
        CAST(stations.lastos AS INTEGER) & 2130706432
      )= 33554432
      AND station_env_kb.name IN (
        SELECT
          id
        FROM
          env_strings
        WHERE
          str IN(
            'KB4012212', 'KB4012213', 'KB4012214',
            'KB4012215', 'KB4012216', 'KB4012217',
            'KB4012598'
          )
      )
  );
```

Критерии функционального анализа

Критерии функционального анализа позволяют выстроить максимальную защиту, поэтому их необходимо задавать при настройке функционального анализа.

В разделе **Критерии функционального анализа** указаны категории, которые вы можете использовать для защиты профиля. Выбор категории зависит от необходимого вам уровня безопасности и особенностей системы.

Категории критериев функционального анализа

1. **Запуск приложений**:
   - *Запрещать запуск приложений, подписанных сертификатами, известными в "Доктор Веб" как сертификаты для рекламных программ.*
     Блокирует запуск приложений, которые могут распространять рекламу.
   - *Запрещать запуск приложений, подписанных сертификатами, известными в "Доктор Веб" как серые.*
     Блокирует запуск приложений, которые подписаны "серыми" сертификатами. Такие сертификаты часто используются для подписи небезопасных приложений.
   - *Запрещать запуск приложений, подписанных сертификатами, известными в "Доктор Веб" как сертификаты для взлома программ.*
     Блокирует запуск приложений, которые подписаны сертификатами, использующимися для взлома программ. Использование данного критерия рекомендовано.
   - *Запрещать запуск приложений, подписанных поддельными/поврежденными сертификатами.*
     Блокирует запуск вредоносных приложений, которые подписаны недействительными сертификаты. Использование данного критерия рекомендовано.
   - *Запрещать запуск приложений, подписанных сертификатами, известными в "Доктор Веб" как сертификаты для вредоносных программ.*
     Блокирует запуск приложений, которые подписаны скомпрометированными сертификатами. Использование данного критерия рекомендовано.
   - *Запрещать запуск приложений, подписанных отозванными сертификатами.*
     Блокирует запуск приложений, которые подписаны украденными или скомпрометированными сертификатами. Использование данного критерия рекомендовано, так как он позволяет превентивно пресекать запуск потенциально вредоносных приложений.
   - *Запрещать запуск приложений, подписанными самоподписными сертификатами.*
     Блокирует нелицензионное ПО, которое может оказаться вредоносным.
   - *Запрещать запуск неподписанных приложений.*
     Блокирует запуск потенциально вредоносных и ненадежных приложений, источник происхождения которых неизвестен.

- *Запрещать запуск утилит от Sysinternals*.
  Защищает от компрометации системы через утилиты Sysinternals.

Если на вкладке **Разрешения** стоит флаг **Разрешать запуск системных приложений и приложений от компании Microsoft**, утилиты Sysinternals будут запускаться даже при запрете за запуск.

- *Запрещать запуск приложений из альтернативных потоков NTFS (ADS)*.
  Приложения из альтернативных потоков NTFS (ADS) зачастую являются вредоносными, поэтому использование данного критерия является обязательным.
- *Запрещать запуск приложений из сети и общих ресурсов*.
  Запуск приложений из сети и общих ресурсов является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.
- *Запрещать запуск приложений со сменных носителей*.
  Запуск приложений со сменных носителей является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.
- *Запрещать запуск приложений из временных каталогов*.
  Блокирует запуск приложений из временных каталогов.
- *Запрещать запуск Windows/Microsoft Store приложений (только для Windows 8 и выше)*.
  Блокирует запуск приложений, загруженных из Windows/Microsoft Store.
- *Запрещать запуск приложений с двойным/нетипичным расширением*.
  Блокирует запуск подозрительных файлов с нестандартным расширением (например, `*.jpg.exe`).
- *Запрещать запуск bash-оболочек и WSL-приложений (только для Windows 10 и выше)*.
  Блокирует запуск командных оболочек Bash и WSL-приложений.

2. **Загрузка и исполнение модулей**. Критерии могут работать в двух режимах:
   - *Загрузка всех модулей*.
     Данный режим является ресурсозатратным, поэтому его рекомендуется использовать только при необходимости повышенного контроля.
   - *Контролировать загрузку и исполнение модулей в хост-приложениях*.
     Данный режим является менее ресурсозатратным. Контролирует работу модулей только в процессах, которые используются для компрометации системы или для проникновения вредоносного ПО под видом системного или доверенного файла. При отсутствии необходимости повышенного контроля следует использовать данный режим.

   Рекомендации по использованию критериев **Загрузка и исполнение модулей** аналогичны рекомендациям по использованию критериев Запуска приложений.
3. **Запуск скриптовых интерпретаторов**:

- *Запрещать запуск CMD/BAT-сценариев*.
  Блокирует запуск файлов с расширениями `cmd` и `bat`.
- *Запрещать запуск HTA-сценариев*.
  Блокирует запуск HTA-сценариев. Такие сценарии могут обрабатывать вредоносные скрипты и скачивать на компьютер исполняемые файлы, которые могут нанести вред системе.
- *Запрещать запуск VBScript/JavaScript*.
  Блокирует запуск приложений, написанных на скриптовых языках VBScript и JavaScript. Такие приложения могут обрабатывать вредоносные скрипты и скачивать на компьютер исполняемые файлы, которые могут нанести вред системе.
- *Запрещать запуск PowerShell-сценариев*.
  Блокирует запуск сценариев, написанных на скриптовом языке PowerShell. Такие сценарии могут обрабатывать вредоносные скрипты и скачивать на компьютер исполняемые файлы, которые могут нанести вред системе.
- *Запрещать запуск REG-сценариев*.
  Блокирует запуск реестровых скриптов (файлов с расширением `reg`). Такие файлы могут быть использованы для добавления или изменения значений в реестре.
- *Запрещать запуск сценариев из альтернативных потоков NTFS (ADS)*.
  Блокирует запуск сценариев из альтернативных потоков NTFS (ADS). Такие сценарии зачастую являются вредоносными, поэтому данный критерий рекомендован к использованию.
- *Запрещать запуск сценариев из сети и общих ресурсов*.
  Запуск сценариев из сети и общих ресурсов является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.
- *Запрещать запуск сценариев со сменных носителей*.
  Запуск сценариев со сменных носителей является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.
- *Запускать запуск сценариев из временных каталогов*.
  Запуск сценариев из временных каталогов является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.

4. **Загрузка драйверов**.
   - *Запрещать загрузку неподписанных драйверов*.
     Блокирует загрузку руткитов и буткитов. Блокирует использование уязвимостей ПО и ОС.
     Данный режим рекомендовано использовать на 64-разрядных версиях ОС. Использование режима также допустимо на 32-разрядных версиях ОС при отсутствии в системе неподписанных драйверов.
   - *Запрещать загрузку уязвимых версий драйверов популярного ПО*.
     Блокирует загрузку небезопасных версий драйверов популярного ПО.

Запрет на загрузку уязвимых версий драйверов популярного ПО не может быть перекрыт исключениями.

Остальные рекомендации по использованию критериев **Загрузка драйверов** аналогичны рекомендациям по использованию критериев Запуска приложений.

5. **Установка MSI-пакетов**.

   Рекомендации по использованию критериев **Установка MSI-пакетов** аналогичны рекомендациям по использованию критериев Запуска приложений.

6. **Целостность исполняемых файлов**.

   - *Запрещать создание новых исполняемых файлов*.
     Блокирует попытки создания новых исполняемых файлов.
   - *Запрещать модификацию исполняемых файлов*.
     Блокирует попытки изменения исполняемых файлов.

   Критерии **Целостность исполняемых файлов** используются только в системах, работающих в режиме доверенной среды. В подобных системах все процессы контролируются администратором (например, банкоматы и иные системы).

   При использовании критериев **Целостность исполняемых файлов** в других системах поведение непредсказуемо, вплоть до выхода станции из строя.

Критерии **Целостность исполняемых файлов** не могут быть перекрыты правилами.

Глава 4: Устранение неполадок

Диагностика проблем удаленной установки

Принцип установки:

1. Сервер Dr.Web подключается к ресурсу `ADMIN$` на удаленной машине (`\\<`*удаленная_машина*`>\ADMIN$\Temp`) и копирует сетевой инсталлятор `drwinst.exe`, расположенный в каталоге `webmin\install\windows` каталога установки Сервера, и SSL-сертификат `drwcsd-certificate.pem`, расположенный в каталоге `etc` каталога установки Сервера, в каталог `\\<`*удаленная_машина*`>\ADMIN$\Temp`.
2. Сервер запускает файл `drwinst.exe` на удаленной машине с ключами командной строки, соответствующими настройкам в Центре управления.

Для успешной установки необходимо, чтобы на Сервере, с которого происходит установка:

1. Был доступен ресурс `ADMIN$\Temp` на удаленной машине.

   Доступность можно проверить следующим образом:

   Введите в адресную строку приложения `Windows Explorer`:

   `\\<`*удаленная_машина*`>\ADMIN$\Temp`

   Должно появиться приглашение на ввод пользователя и пароля для доступа к этому ресурсу. Введите учетные данные, которые были указаны на странице инсталляции.

   Ресурс `ADMIN$\Temp` может быть недоступен по следующим причинам:

   a) учетная запись не имеет прав администратора;

   b) машина отключена или межсетевой экран блокирует доступ к порту 445;

   c) ограничения удаленного доступа к ресурсу `ADMIN$\Temp` на ОС Windows Vista и выше в случае, если они не входят в домен;

   d) отсутствует владелец каталога или недостаточно прав на каталог у пользователя или группы.
2. Был доступ к файлам `drwinst.exe` и `drwcsd.pub`.

В Центре управления отображается расширенная информация (этап и код ошибки), помогающая диагностировать причину ошибки.

Список ошибок удаленной установки Агента Dr.Web

Этап	Ошибка	Причина
Подключение по SMB к станции <*host*>	Неверный адрес станции <*host*>	IP-адрес станции, заданный для установки Агента, не является корректным адресом IPv4/IPv6 или не удалось преобразовать DNS-имя в адрес: такого DNS-имени не существует, либо неправильно настроен сервер имен.

	Ошибка подключения по SMB к станции <*host*>	Не удалось подключиться к станции по SMB. Возможные причины:
		• на станции отключена служба сервера;
		• недоступен 445 TCP-порт на удаленной машине, возможные причины:
		  ▫ машина отключена;
		  ▫ межсетевой экран блокирует указанный порт;
		  ▫ на удаленной машине установлена ОС, отличная от ОС Windows;
		• не настроена модель совместного доступа и безопасности для локальных учетных записей;
		• недоступен сервер авторизации (контроллер домена);
		• неизвестный пользователь или неверный пароль.

	Недостаточно прав для открытия разделяемого ресурса <*share*> на станции <*host*>	Не существует ресурса `ADMIN$` на удаленной машине, либо не хватает прав на его открытие.
Отправка файлов на станцию <*host*>	Не найден путь <*path*> в разделяемом ресурсе <*share*> на станции <*host*>	Отсутствует директория `ADMIN$/TEMP`.
	Не удалось создать временный каталог <*path*> в разделяемом ресурсе <*share*> на станции <*host*>	Не удалось создать временную директорию в `ADMIN$/TEMP`, например, не хватило прав на запись.
	Не удалось удалить временный каталог <*path*> в разделяемом ресурсе <*share*> на станции <*host*>	Не удалось удалить директорию в `ADMIN$/TEMP` после завершения процедуры. Например, если не дождались завершения службы, либо кто-то открыл файл в этой директории.

Этап	Ошибка	Причина
	Не удалось открыть файл для чтения <*path*> на Сервере Не удалось прочитать файл <*path*> на Сервере	Отсутствует файл установщика на самом Сервере, либо заданы неверные права на файл установщика.
	Не удалось открыть файл для записи <*path*> в разделяемом ресурсе <*share*> на станции <*host*> Не удалось записать файл <*path*> в разделяемом ресурсе <*share*> на станции <*host*>	Недостаточно прав для чтения/записи соответствующих файлов или в соответствующих директориях.
Создание сервиса на станции <*host*>	Ошибка подключения к серверной службе (srvsvc RPC) на станции <*host*>	Недоступно удаленное управление службами.
	Ошибка подключения к SCM на станции <*host*> Не удалось создать сервис на станции <*host*> Не удалось запустить сервис на станции <*host*> Не удалось остановить сервис на станции <*host*> Не удалось удалить сервис на станции <*host*>	Недостаточно прав на управление службами.
Исполнение сервиса на станции <*host*>	Не удалось получить статус сервиса на станции <*host*>	Возможно, ошибка с SCM.
	Установка прервана по таймауту на станции <*host*>	Установщик не успел установить Агента за указанный период времени. Возможные причины: медленный канал между станцией и Сервером, не хватило времени для загрузки необходимых данных.
	Не удалось получить локальный путь к разделяемому ресурсу <*share*> на станции <*host*>	Не удалось определить путь на станции до ресурса `ADMIN$`.
	Сервис завершил выполнение с ошибкой на станции <*host*>. Статус завершения: <*state*>. Код ошибки: <*rc*>.	Ошибки установщика Агента.

Устранение ошибки службы BFE при установке Агента Dr.Web для Windows

Для функционирования некоторых компонентов Антивируса Dr.Web для Windows необходимо наличие запущенной службы базового модуля фильтрации (BFE). В случае, если данная служба отсутствует или повреждена, установка Агента Dr.Web для Windows будет невозможна. Повреждение или отсутствие службы BFE может указывать на наличие угроз безопасности станции.

Если попытка установки Агента Dr.Web для Windows завершилась с ошибкой службы BFE, выполните следующие действия:

1. Просканируйте систему станции при помощи лечащей утилиты CureNet! от компании «Доктор Веб».

   Демо-версию (диагностика без функции лечения) утилиты можно запросить здесь: https://download.drweb.com/curenet/.

   Ознакомиться с условиями использования и стоимостью полной версии утилиты можно здесь: https://estore.drweb.com/utilities/.
2. Вручную запустите или перезапустите службу BFE. Если запустить службу BFE не удалось или служба отсутствует в списке, обратитесь в службу технической поддержки компании Microsoft.
3. Запустите установщик Агента Dr.Web для Windows и произведите установку согласно штатной процедуре, приведенной в **Руководстве по установке**.

   Если проблема не устранена, обратитесь в службу технической поддержки компании «Доктор Веб».

Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

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

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

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

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

Предметный указатель

© «Доктор Веб», 2021