Dr.WEB

Enterprise Security Suite

# Приложения

**Dr.Web Enterprise Security Suite**
**Версия 13.0**
**Приложения**
**27.05.2025**

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 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**

   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**

   Адресовано *администратору антивирусной сети* — сотруднику организации, которому поручено руководство антивирусной защитой компьютеров (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**

   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 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 структуре базы данных Сервера Dr.Web**

   Содержит описание внутренней структуры базы данных Сервера Dr.Web и примеров ее 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, 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:

- 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,
- ACL — списки контроля доступа (Access Control List),
- CDN — сеть доставки контента (Content Delivery Network),
- DFS — распределенная файловая система (Distributed File System),
- DN — отличительное имя, уникальный идентификатор записи в дереве LDAP (Distinguished Name),
- 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).

# Глава 2: Приложения

## Приложение A. Настройки для использования СУБД. Параметры драйверов СУБД

**Структура базы данных Сервера Dr.Web** доступна в виде отдельного одноименного руководства. Документ можно открыть из раздела **Поддержка** в Центре управления безопасностью Dr.Web.

В качестве базы данных Сервера Dr.Web может использоваться:

- встроенная БД;
- внешняя СУБД.

### Встроенная БД

При настройке обращения к встроенной БД для хранения и обработки данных используются параметры, приведенные в таблице ниже.

**Параметры встроенной БД**

| Имя | Значение по умолчанию | Описание |
|---|---|---|
| DBFILE | database.sqlite | Путь к файлу базы данных |
| CACHESIZE | 2048 | Размер кеша базы данных в страницах |
| PRECOMPILEDCACHE | 1048576 | Размер кеша предкомпилированных SQL-операторов в байтах |
| MMAPSIZE | • для ОС UNIX — 10485760,<br>• для ОС Windows — 0 | Максимальный размер файла базы данных в байтах, который допускается отображать на адресное пространство процесса за один раз. |
| CHECKINTEGRITY | QUICK | Проверка целостности образа базы данных при запуске Сервера Dr.Web:<br>• FULL — полная проверка на предмет ошибок, связанных с ограничениями вида UNIQUE, CHECK и NOT NULL, неупорядоченных записей, пропущенных страниц и некорректных индексов,<br>• QUICK — быстрый вариант проверки, без отслеживания ошибок ограничений и некорректных индексов,<br>• NO — проверка не выполняется. |

| | | |
|---|---|---|
| AUTOREPAIR | NO | Автоматическое восстановление поврежденного образа базы данных при запуске Сервера Dr.Web:<br>• YES — восстановление образа базы данных запускается каждый раз при запуске Сервера Dr.Web,<br>• NO — автоматическое восстановление отключено. |
| WAL | YES | Использование упреждающего журналирования (Write-Ahead Logging):<br>• YES — журналирование включено,<br>• NO — журналирование не используется. |
| WAL-MAX-PAGES | 1000 | Максимальное число “грязных” страниц, при достижении которого осуществляется запись страниц на диск. |
| WAL-MAX-SECONDS | 30 | Максимальное время, на которое откладывается запись страниц на диск (в секундах). |
| SYNCHRONOUS | FULL | Режим синхронной записи изменений в базе данных на диск:<br>• FULL — полностью синхронная запись на диск,<br>• NORMAL — синхронная запись критичных данных,<br>• OFF — асинхронная запись. |

В качестве встроенной БД предоставляется SQLite3.

### Внешняя СУБД

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

- СУБД MySQL, MariaDB. Описание настроек приведено в A4. Использование СУБД MySQL.
- СУБД Oracle. Описание настройки приведено в A2. Настройка драйвера БД для Oracle.
- СУБД PostgreSQL. Описание настроек приведено в A3. Использование СУБД PostgreSQL.

  Поддерживаются СУБД, основанные на PostgreSQL (PostgreSQL Pro, Jatoba и другие).

- 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 A1. Настройка ODBC-драйвера).

  Поддерживается использование Microsoft SQL Server 2008 или 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 Dr.Web, 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://learn.microsoft.com/en-US/troubleshoot/sql/releases/download-and-install-latest-updates.

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 встроенной БД и внешних СУБД

Встроенная БД рассчитана на подключение к Серверу Dr.Web порядка 400–600 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен Сервер Dr.Web, и нагрузка по прочим задачам, выполняемым на данном компьютере, возможно подключение порядка 1000–1500 станций.

В противном случае необходимо использовать внешнюю БД. В зависимости от конфигурации и нагрузки на компьютер, выполняющий функции Сервера Dr.Web, внешняя БД может быть размещена на этом же или на специально выделенном компьютере.

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

- процессор с частотой 3ГГц,
- от 6 ядер процессора,
- 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 БД:

- В больших антивирусных сетях (свыше 400–600 станций) рекомендуется использовать внешнюю БД, более устойчивую к сбоям, чем встроенная 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.

## A1. Настройка ODBC-драйвера

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

**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`:<br>• `SERIALIZABLE`<br>• `READ_UNCOMMITTED`<br>• `READ_COMMITTED`<br>• `REPEATABLE_READ`<br>• `DEFAULT`<br>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`).

---

Нежелательно употреблять следующие символы: пробел, "`{`", "`;`" и "`}`", подробнее см. https://learn.microsoft.com/en-us/sql/odbc/reference/syntax/sqldriverconnect-function?redirectedfrom=MSDN&view=sql-server-ver15.

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 https://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 (SQL Server Native Client), крайне не рекомендовано.

Исключением являются БД, поставляемые Microsoft без ODBC-драйвера. Если Вы используете СУБД MS SQL, необходимо установить и использовать актуальную версию ODBC-драйвера с сайта Microsoft.

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 Dr.Web, 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**.

## A2. 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**.

   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 ниже.

### 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) |

**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 Dr.Web.

## А3. 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) 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 базы данных.

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 ниже.

**Параметры СУБД PostgreSQL**

| Имя | Значение по умолчанию | Описание |
|---|---|---|
| `host` | *<Локальный UNIX-сокет>* | Хост сервера PostgreSQL |
| `port` | | Порт сервера PostgreSQL или расширение имени файла сокета |

| Имя | Значение по умолчанию | Описание |
|---|---|---|
| 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<br>• 0 для отсутствия запроса |
| temp_tablespaces | | Пространство имен для временных таблиц |
| default_transaction_isolation | | Режим изоляции транзакции (см. документацию к PostgreSQL) |

Допускается указание любого из режимов изоляции транзакции, поддерживаемых PostgreSQL, однако корректная работа Сервера Dr.Web при режиме **Repeatable read** не гарантируется.

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

work_mem = 16MB
```

Расширенная настройка:

```
shared_buffers = 1GB

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.

## A4. 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 — все версии, начиная с 8.0.12,

Убедитесь, что для пользователя, через которого осуществляется подключение к MySQL версии 8.X, тип аутентификации соответствует `caching_sha2_password`. Данный параметр задается при установке и становится параметром по умолчанию для каждого пользователя или настраивается вручную для каждого пользователя.

- MariaDB — все версии, начиная с 10.5.

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 8.X:

```
[mysqld]

innodb_file_per_table = true

max_allowed_packet = 64M
```

## Параметры

При настройке обращения к СУБД MySQL используются параметры, описываемые в таблице ниже.

**Параметры СУБД MySQL**

| Имя | Значение по умолчанию | Описание |
|---|---|---|
| `HOST` | localhost | • При подключении к базе данных по TCP/IP — адрес сервера базы данных. |

| | | |
|---|---|---|
| | | • При использовании UDS — путь к файлу сокета UNIX. Если путь не задан, Сервер Dr.Web попытается найти файл в стандартных директориях mysqld. |
| PORT | 3306 | • При подключении к базе данных по TCP/IP — номер порта для подключения.<br>• При использовании UDS — имя файла сокета UNIX. |
| DBNAME | | Название базы данных |
| USER | | Регистрационное имя пользователя базы данных |
| PASSWORD | QUICK | Пароль пользователя базы данных |
| PRECOMPILEDCACHE | 1048576 | Размер кеша предкомпилированных sql-операторов в байтах |
| SSL | NO | Использовать только SSL-соединения:<br>• YES — подключаться к базе данных только при условии использования протокола SSL,<br>• NO — протокол SSL при подключении к базе данных не обязателен. |

# Приложение Б. Аутентификация администраторов

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

## Б1. 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 Dr.Web 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-modify-ad-schema-<версия_пакета>-<сборка>-<версия_ОС>.exe` (поставляется отдельно от дистрибутива Сервера Dr.Web) создает новый класс объектов `DrWebEnterpriseUser` для Active Directory и описывает новые атрибуты для данного класса.

Атрибуты имеют следующие OID:

```
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.

## Б2. 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, если не найдено ни одно подходящее правило. У скрипта один параметр — введенное имя пользователя. Скрипт возвращает строку, содержащую либо DN, либо ничего. 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.

## Б3. 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.<br>• `127.0.0.1` для сервера под ОС семейства UNIX.<br>• Допускается указание нескольких тегов `<server />` с адресами разных LDAP-серверов. Первым следует указывать адрес главного сервера, на который предполагается основная нагрузка. Если сервер недоступен, то будет предпринята попытка аутентификации на следующем сервере и далее по порядку в указанной последовательности. Если сервер доступен, то поиск учетной записи будет осуществляться только на данном сервере. Вне зависимости от результата аутентификации в этом случае подключение к следующим серверам производится не будет. |
| `scope` | Область поиска. Допустимые значения:<br>• `sub-tree` — вся область ниже базового DN,<br>• `one-level` — прямые потомки базового DN,<br>• `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. | – |
| `filter` | RFC4515 фильтр поиска в LDAP. | – |
| `scope` | Область поиска. Допустимые значения:<br>• `sub-tree` — вся область ниже базового DN,<br>• `one-level` — прямые потомки базового DN,<br>• `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. | – |

Для корректной аутентификации все группы, для которых настроено членство пользователей в группах в Центре управления (**Администрирование → Аутентификация → Настройки LDAP/AD аутентификации → Членство пользователей в группах**), т.е. для которых в теге `<set />` есть соответствующие записи, должны фактически присутствовать в домене Active Directory.

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. |

- <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 (пользовательская процедура Трансляция имен пользователей в LDAP DN) для выполнения трансляции имени пользователя в DN. Данный скрипт выполняется после попыток применения всех правил user-dn, user-dn-expr, если не найдено ни одно подходящее правило. У скрипта один параметр — введенное имя пользователя. Скрипт возвращает строку, содержащую либо DN, либо

ничего. Если не подошло ни одно правило и скрипт не разрешен или не вернул ничего, то введенное имя пользователя используется как есть.

- `<bind dn/>` определяет DN пользователя, который используется для подключения к серверу LDAP, и `<bind password/>` определяет пароль пользователя, который используется для подключения к серверу LDAP (возможны пустые `DN` и `password` для анонимного подключения).

  Например:

```
<bind dn="CN=some dn,OU=some name,DC=example,DC=com" password="***" />
```

> Если одновременно заданы отдельный аккаунт для поиска Bind DN (в т.ч. анонимный) и правила трансляции логина DN, то приоритет отдается первому, а второе игнорируется.

### 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 |

| Название настройки | | Значение |
|---|---|---|
| Адрес сервера | | dc.test.local |
| 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 |

## Б4. Подведомственные разделы прав

### Список прав администраторов и их особенностей

| 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.<br><br>Если право предоставлено только для отдельных групп, а не всей антивирусной сети, пункт меню **Администрирование** → **Установки** → **Установка по сети** недоступен. | Антивирусная сеть<br><br>Антивирусная сеть → Общие → Свойства |
| 2* | **Редактирование свойств групп станций** | Список пользовательских групп, свойства которых администратор может редактировать.<br><br>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. | Антивирусная сеть<br><br>Антивирусная сеть → Общие → Запущенные компоненты<br><br>Антивирусная сеть → Общие → Карантин |

| Код | Право | Описание | Раздел Центра управления |
|---|---|---|---|
| | | Должен содержать группы из списка права 1. | |
| 4 | **Редактирование конфигурации групп станций** | Аналогично праву 3, но с возможностью редактирования.<br><br>Должен содержать группы из списка права 3. | Страницы из раздела **Конфигурация** управляющего меню |
| 5 | **Просмотр свойств станций** | Список пользовательских групп, которые являются первичными для станций, свойства которых можно просматривать администратору.<br><br>Должен содержать группы из списка права 1. | Антивирусная сеть |
| 6 | **Редактирование свойств станций** | В том числе ACL, блокировки, допуска и т. д.<br><br>Аналогично праву 5, но с возможностью редактирования.<br><br>Должен содержать группы из списка права 5. | Антивирусная сеть → Общие → Свойства |
| 8* | **Помещение станций в группы и удаление станций из групп** | Список пользовательских групп.<br><br>Должен содержать группы из списка права 1. | |
| 9 | **Удаление станций** | Список пользовательских групп, являющихся первичными для станций, которые администратор может удалить.<br><br>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 Dr.Web с выбранными ID. Данные группы должны быть первичными для устанавливаемых станций.<br><br>Должен содержать группы из списка права 1. | Антивирусная сеть |

| Код | Право | Описание | Раздел Центра управления |
|---|---|---|---|
| | | Если есть запрещенные объекты, то пункт в меню не отображается.<br><br>Установка по сети возможна только из /esuite/network/index.ds при условии, что право 16 предоставлено. | |
| 11 | **Объединение станций** | Список пользовательских групп, станции из которых можно объединить. Данные группы должны быть первичными для станций. Доступна иконка объединения станций на панели инструментов.<br><br>Должен содержать группы из списка права 1. | |
| 12* | **Просмотр статистических таблиц** | Список пользовательских групп, по которым администратору доступен просмотр статистики.<br><br>Право дает возможность создать задание в расписании Сервера Dr.Web на получение периодических отчетов. Задается список пользовательских групп, которые администратор 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.<br><br>Должен содержать группы из списка права 1. | Антивирусная сеть<br><br>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.<br><br>Должен содержать группы из списка права 1. | Антивирусная сеть → Конфигурация → Лицензионные ключи |
| 40 | **Запуск и прерывание компонентов** | Запуск и прерывание компонентов, установленных на станции. | Антивирусная сеть → кнопка **Управление компонентами** на панели инструментов → кнопка **Прервать запущенные компоненты** |

| Код | Право | Описание | Раздел Центра управления |
|---|---|---|---|
| | | | Антивирусная сеть → Общие → Компоненты защиты → кнопки **Прервать выбранные компоненты**, **Запустить выбранные компоненты** на панели инструментов<br><br>Антивирусная сеть → кнопка **Сканировать** на панели инструментов → кнопки **Быстрое сканирование**, **Полное сканирование**, **Выборочное сканирование**<br><br>Антивирусная сеть → Общие → Карантин → кнопки **Удалить файлы**, **Экспорт**, **Восстановить файлы**, **Сканировать файлы** на панели инструментов |
| 48 | **Просмотр отчетов для технической поддержки** | Создание и просмотр системных журналов компонентов защиты, установленных на станции. | Антивирусная сеть → Общие → Отчеты для технической поддержки |
| **Управление администраторами** | | | |
| 18 | **Просмотр расписания Сервера Dr.Web** | Просмотр таблицы **Журнал выполнения заданий**. Для просмотра доступны задания, созданные администратором, а также администраторами из выбранной группы.<br><br>Если не предоставлены права 12 и 18, то просмотр страницы с расписанием Сервера Dr.Web запрещен.<br><br>Если предоставлено 12 и не предоставлено 18, то доступен просмотр расписания для статистики.<br><br>Задание на отправку отчетов для конкретного администратора отображается в зависимости от | Администрирование → Конфигурация → Планировщик заданий Сервера Dr.Web<br><br>Администрирование → Журналы → Журнал выполнения заданий |

| Код | Право | Описание | Раздел Центра управления |
|---|---|---|---|
| | | наличия права 12 и наличия оповещения **Периодический отчет**, даже если право 18 не предоставлено. | |
| 19 | **Редактирование расписания Сервера Dr.Web** | Для редактирования доступны задания, созданные администратором, а также администраторами из выбранной группы. | Администрирование → Конфигурация → Планировщик заданий Сервера Dr.Web |
| 24 | **Редактирование конфигурации оповещений** | | Администрирование → Оповещения → Конфигурация оповещений<br><br>Администрирование → Оповещения → Неотправленные оповещения<br><br>Администрирование → Оповещения → Оповещения веб-консоли |
| 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 ее подгрупп. Администратор из группы **Administrators** видит всех других администраторов, независимо от их групп.<br><br>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. | |

| Код | Право | Описание | Раздел Центра управления |
|---|---|---|---|
| 28 | **Просмотр свойств и конфигурации групп администраторов** | В том числе администраторов в группах и подгруппах.<br><br>Администратор может выбирать только из подгруппы своей родительской группы. | |
| 29 | **Редактирование свойств и конфигурации групп администраторов** | В том числе администраторов в группах и подгруппах.<br><br>Администратор может выбирать только из подгруппы своей родительской группы.<br><br>Если данное право не предоставлено, то даже если право 26 предоставлено для этой группы, администратор не сможет отключить наследование или повысить права администратору в группе. | |
| 39 | **Отображение группы администраторов “Newbies”** | Разрешить администратору видеть предустановленную группу **Newbies** в дереве администраторов.<br><br>Если у администратора нет права на просмотр группы **Newbies**, а сам он находится в этой группе, то видеть он будет только себя. | |
| 41 | **Редактирование административных оповещений** | Редактирование конфигурации оповещений администраторов. | |
| **Дополнительно** | | | |
| 7 | **Создание станций** | При создании станции доступен список групп с правом 8 (у группы, в которую помещаются станции, должно быть право 8).<br><br>При создании станции первичной должна стать одна из доступных пользовательских групп. | Антивирусная сеть |
| 13 | **Просмотр аудита** | Аудит доступен для полноправного администратора, а также для объектов с правом 4. | Администрирование → Журналы → Журнал аудита |

| Код | Право | Описание | Раздел Центра управления |
|---|---|---|---|
| 16 | **Запуск Сканера сети** | Если право не назначено, то установка по сети из /esuite/network/index.ds недоступна. | Антивирусная сеть<br><br>Администрирование → Сканер сети |
| 17 | **Подтверждение новичков** | Доступен список групп из права 8.<br><br>Данное право не может быть назначено, 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 |
| 20 | **Просмотр конфигурации Сервера Dr.Web и конфигурации репозитория** | | Администрирование → Конфигурация → Конфигурация веб-сервера<br><br>Администрирование → Репозиторий → Состояние репозитория<br><br>Администрирование → Репозиторий → Отложенные обновления<br><br>Администрирование → Репозиторий → Общая конфигурация репозитория<br><br>Администрирование → Репозиторий → Детальная конфигурация репозитория<br><br>Администрирование → Репозиторий → Содержимое репозитория<br><br>Администрирование → Журналы → Журнал обновлений репозитория<br><br>Администрирование → Конфигурация → Пользовательские процедуры |

| Код | Право | Описание | Раздел Центра управления |
|---|---|---|---|
| 21 | **Редактирование конфигурации Сервера Dr.Web и конфигурации репозитория** | | Администрирование → Сервер Dr.Web → Список версий |
| 22 | **Просмотр информации о лицензировании** | | Администрирование → Администрирование → Менеджер лицензий |
| 30 | **Работа через Web API** | | - |
| 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 Dr.Web с ВСО. | Кнопка **Обновить репозиторий** в разделе **Состояние репозитория** |
| 42 | **Редактирование собственных настроек** | Право изменять собственные настройки учетной записи администратора. | Администрирование → Конфигурация → Администраторы |
| 43 | **Просмотр Прокси-серверов Dr.Web** | Право просматривать настройки Прокси-серверов Dr.Web (если просмотр выключен, то редактирование автоматически отключается тоже). | Антивирусная сеть → Прокси |
| 44 | **Редактирование Прокси-серверов Dr.Web** | Право изменять настройки Прокси-серверов Dr.Web. | Антивирусная сеть → Прокси |
| 45 | **Просмотр свойств и конфигурации политик** | Если просмотр выключен, то редактирование автоматически отключается тоже. | Антивирусная сеть → Политики |

| Код | Право | Описание | Раздел Центра управления |
|---|---|---|---|
| 46 | **Редактирование свойств и конфигурации политик** | | Антивирусная сеть → Политики |
| 47 | **Редактирование правил членства** | Право изменять правила членства пользовательских групп. | Антивирусная сеть |

* 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 предоставлены какие-либо из этих прав, то администратору будет доступен набор функций, 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 B. Система оповещения

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

## B1. 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 Dr.Web,
- push-оповещения,
- оповещения через Syslog-протокол.

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

**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 | 300 сек, (отправка не чаще раза в 300 сек) | нет |

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

### Оповещения по электронной почте

| Параметр | Описание | Значение по умолчанию |
|---|---|---|
| FROM | Адрес ящика электронной почты отправителя | drwcs@${<*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<br>• 465, если параметр SSL принимает значение yes |
| USER | Пользователь SMTP-сервера | ""<br><br>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 порта 25. | yes |
| SSL | Для шифрованного обмена данными. При этом будет открыто отдельное защищенное TLS-соединение. По умолчанию для соединения предусматривается использование порта 465. | 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 | - |

### 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. |

### Оповещения через SNMP

| Параметр | Описание | Значение по умолчанию |
|---|---|---|
| TO | Принимающая сущность SNMP, например, IP-адрес | - |
| DOMAIN | Домен | • `localhost` для ОС Windows,<br>• "" 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 |

### 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. |

### 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 | - |

### Оповещения через Syslog-протокол

| Параметр | Описание | Значение по умолчанию |
|---|---|---|
| TO | Адрес получателя оповещения по протоколу Syslog. Протокол передачи TCP или UDP. | UDP, порт 514 |
| FORMAT | Формат оповещения: RFC 5424 или CEF (Common Event Format). | RFC 5424 |
| TIMEOUT | Период в секундах, в течение которого Сервер Dr.Web осуществляет попытку соединения с получателем оповещения по протоколу TCP. | 5 сек. |
| FACILITY | Категория сформировавшего оповещение процесса (например, ядра, почтовой системы). Принимает значения в пределах от 0 до 23. | 14 |
| HOSTNAME | Отправитель. Идентификатор Сервера Dr.Web (полное доменное имя, имя хоста, IP-адрес). | - |

## В2. Параметры шаблонов оповещений

Тексты сообщений генерируются компонентом Сервера Dr.Web, 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*>.

**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 Dr.Web (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 Dr.Web и Сервера Dr.Web,
- `SYS.BUILD` — дата сборки Сервера Dr.Web,
- `SYS.DATE` — текущая системная дата,
- `SYS.DATETIME` — текущие системная дата и время,
- `SYS.HOST` — DNS-имя Сервера Dr.Web,
- `SYS.MACHINE` — сетевой адрес компьютера с установленным Сервером Dr.Web,
- `SYS.OS` — название операционной системы на компьютере с установленным Сервером Dr.Web,
- `SYS.PLATFORM` — платформа Сервера Dr.Web,
- `SYS.PLATFORM.SHORT` — краткий вариант `SYS.PLATFORM`,
- `SYS.SERVER` — название продукта (Dr.Web Server),
- `SYS.TIME` — текущее системное время,
- `SYS.VERSION` — версия Сервера Dr.Web.

## 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. | |
| 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 Dr.Web, 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 Dr.Web

| Параметр | Значение |
|---|---|
| Причина отправки | Отправляется при возникновении ошибки в процессе записи |

| Параметр | Значение | |
|---|---|---|
| оповещения | информации в журнал работы Сервера Dr.Web. Причина ошибки записи в журнал приводится в тексте оповещения. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | `MSG.Error` | текст ошибки |

### Ошибка ротации журнала Сервера Dr.Web

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

### Соседний Сервер Dr.Web давно не подключался

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

| Параметр | Значение | |
|---|---|---|
| | приводится путь, по которому можно скачать файл отчета. | |
| Дополнительная настройка | Отчет создается согласно заданию **Создание статистического отчета** в расписании Сервера Dr.Web, 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 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:<br>• блокировка неавторизованного кода<br>• проверка доступа к защищаемым объектам |
| | `MSG.ShellGuardType` | наиболее часто встречающаяся причина блокировки исполнения неавторизованного кода при автоматической блокировке события |

| Параметр | Значение | |
|---|---|---|
| | 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:<br>• блокировка неавторизованного кода<br>• проверка доступа к защищаемым объектам |
| | MSG.UserAllowedProc | процесс с подозрительной активностью, разрешенный 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:<br>• блокировка неавторизованного кода<br>• проверка доступа к защищаемым объектам |

| Параметр | Значение | |
|---|---|---|
| | `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 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 Dr.Web обнаружено, что количество станций в группе, в которую входит подключаемая станция, достигло ограничения в лицензионном ключе, назначенном для этой группы.<br><br>При этом новая станция не может зарегистрироваться на Сервере Dr.Web. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | `MSG.ID` | UUID станции |

| Параметр | Значение | |
|---|---|---|
| | `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 Dr.Web 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 Dr.Web из лицензионного ключа данного Сервера Dr.Web. | |
| Дополнительная настройка | Срок выдачи лицензий соседним Серверам Dr.Web задается в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Лицензии**. | |
| Переменные | `MSG.ObjId` | ID лицензионного ключа |
| | `MSG.Server` | название соседнего Сервера Dr.Web |

### 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 доступных 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 |

| Параметр | Значение | |
|---|---|---|
| | | доступных лицензий |
| | MSG.Licensed | количество станций, использующих лицензии данной группы |
| | MSG.Total | общее количество лицензий по всем ключам, назначенным группе.<br><br>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 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<br>• 0 — срок окончания еще не наступил |
| | `MSG.KeyDifference` | Причина, по которой автоматическая замена ключа невозможна:<br>• 1 — состав лицензируемых компонентов у текущего и нового лицензионных ключей отличается<br>• 2 — у нового лицензионного ключа меньше лицензий, чем у текущего лицензионного ключа |

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

| Параметр | Значение | |
|---|---|---|
| | `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<br>• 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 Dr.Web, 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 Dr.Web и была отклонена Сервером Dr.Web 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 Dr.Web 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**. | |
| 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. |

| Параметр | Значение |
|---|---|
| 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. Д1. Общие файлы конфигурации.

### 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 Dr.Web `var` с динамическими данными, заканчивается свободное 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 |

| Параметр | Значение | |
|---|---|---|
| | | 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 Dr.Web было повторно запущено обновление. |
| 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 Dr.Web. Включение данной опции осуществляется при настройке связей с соседними Серверами Dr.Web (см. **Руководство администратора**, раздел Настройка связей между Серверами Dr.Web).

О событиях на соседнем Сервере Dr.Web 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 Dr.Web, Прокси-сервером. |

| Параметр | Значение | |
|---|---|---|
| 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 приложение на станции было заблокировано компонентом Контроль приложений. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | `MSG.AppCtlAction` | примененное действие:<br>• 0 — неизвестно,<br>• 2 — заблокирован,<br>• 3 — заблокирован (не найден в списке доверенных приложений),<br>• 5 — заблокирован запрещающими правилами,<br>• 7 — заблокирован настройками политик. |
| | `MSG.AppCtlType` | тип события:<br>• 0 — неизвестен,<br>• 1 — запуск процесса,<br>• 2 — запуск хост-процесса,<br>• 3 — запуск скриптового интерпретатора,<br>• 4 — загрузка модуля,<br>• 5 — загрузка драйвера,<br>• 6 — запуск MSI-установщика,<br>• 7 — создание нового исполняемого файла на диске,<br>• 8 — модификация исполняемого файла на диске. |

| Параметр | Значение | |
|---|---|---|
| | 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 Dr.Web).<br><br>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:<br>• 0 — неизвестно,<br>• 2 — заблокирован,<br>• 3 — заблокирован (не найден в |

| Параметр | Значение | |
|---|---|---|
| | | списке доверенных приложений),<br>• 5 — заблокирован запрещающими правилами,<br>• 7 — заблокирован настройками политик. |
| | MSG.AppCtlType | тип события:<br>• 0 — неизвестен,<br>• 1 — запуск процесса,<br>• 2 — запуск хост-процесса,<br>• 3 — запуск скриптового интерпретатора,<br>• 4 — загрузка модуля,<br>• 5 — загрузка драйвера,<br>• 6 — запуск MSI-установщика,<br>• 7 — создание нового исполняемого файла на диске,<br>• 8 — модификация исполняемого файла на диске. |
| | MSG.Document | бюллетень, содержащий хеш |
| | 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 |

| Параметр | Значение | |
|---|---|---|
| | | 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 Dr.Web. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | `MSG.Product` | обновляемый продукт |
| | `MSG.ServerTime` | время получения события, GMT |

### Неизвестная станция

| Параметр | Значение | |
|---|---|---|
| Причина отправки оповещения | Отправляется, если новая станция запросила подключение к Серверу Dr.Web, но была не допущена до рассмотрения подтверждения или отказа в регистрации. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | `MSG.ID` | UUID неизвестной станции |
| | `MSG.Rejected` | значения:<br>• `rejected` — станции отказано в доступе<br>• `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. |

| Параметр | Значение | |
|---|---|---|
| Дополнительная настройка | Не требуется. | |
| Переменные | MSG.Action | действие, предпринятое при обнаружении |
| | MSG.Component | имя компонента |
| | MSG.InfectionType | тип угрозы |
| | MSG.ObjectName | имя зараженного объекта |
| | MSG.ObjectOwner | владелец 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 Dr.Web, 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 Dr.Web) |
| | GEN.ServerRecvLinkName | название последнего соседнего Сервера Dr.Web, от которого было получено сообщение об обнаруженной угрозе на подключенных к нему станциях (пустое значение, если обнаружена угроза на станциях, подключенных к данному Серверу Dr.Web) |
| | GEN.ServerOriginatorID | UUID Сервера Dr.Web, к которому подключена станция, на которой обнаружена угроза |
| | GEN.ServerOriginatorName | название Сервера Dr.Web, 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 Dr.Web).<br><br>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 зараженного 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 |
| | `MSG.Virus` | имя угрозы |
| | `GEN.ServerRecvLinkID` | UUID последнего соседнего Сервера Dr.Web, от которого было получено данное сообщение об обнаруженной угрозе на подключенных к нему станциях (пустое значение, если |

| Параметр | Значение | |
|---|---|---|
| | | обнаружена угроза на станциях, подключенных к данному Серверу Dr.Web) |
| | GEN.ServerRecvLinkName | название последнего соседнего Сервера Dr.Web, от которого было получено сообщение об обнаруженной угрозе на подключенных к нему станциях (пустое значение, если обнаружена угроза на станциях, подключенных к данному Серверу Dr.Web) |
| | GEN.ServerOriginatorID | UUID Сервера Dr.Web, к которому подключена станция, на которой обнаружена угроза |
| | GEN.ServerOriginatorName | название Сервера Dr.Web, 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 Dr.Web. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | MSG.AdminName | администратор, инициировавший действие над подозрительным процессом |
| | MSG.Denied | действие, произведенное над подозрительным процессом:<br>• запрещен<br>• разрешен |
| | MSG.HipsType | тип защищаемого объекта |
| | MSG.IsShellGuard | разделение по типам реакции Превентивной защиты:<br>• блокировка неавторизованного кода<br>• проверка доступа к защищаемым объектам |

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

| Параметр | Значение | |
|---|---|---|
| | | получен отчет Превентивной защиты |
| | GEN.ServerOriginatorName | название Сервера Dr.Web, 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 Dr.Web 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 Dr.Web).<br><br>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 |
| | MSG.Denied | действие, произведенное над подозрительным процессом:<br>• запрещен<br>• разрешен |
| | MSG.Document | бюллетень, содержащий хеш обнаруженной угрозы |
| | MSG.HipsType | тип защищаемого объекта |
| | MSG.IsShellGuard | разделение по типам реакции Превентивной защиты:<br>• блокировка неавторизованного кода<br>• проверка доступа к защищаемым объектам |
| | MSG.Path | путь к процессу с подозрительной |

| Параметр | Значение | |
|---|---|---|
| | | 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:<br>• пользователь<br>• автоматическая реакция Превентивной защиты |
| | GEN.ServerRecvLinkID | UUID последнего соседнего Сервера Dr.Web, от которого был получен отчет Превентивной защиты с подключенных к нему станций (пустое значение, если получен отчет со станций, подключенных к данному Серверу Dr.Web) |
| | GEN.ServerRecvLinkName | название последнего соседнего Сервера Dr.Web, от которого был получен отчет Превентивной защиты с подключенных к нему станций (пустое значение, если получен отчет со станций, |

| Параметр | Значение | |
|---|---|---|
| | | подключенных к данному Серверу Dr.Web) |
| | GEN.ServerOriginatorID | UUID Сервера Dr.Web, к которому подключена станция, с которой получен отчет Превентивной защиты |
| | GEN.ServerOriginatorName | название Сервера Dr.Web, 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 Dr.Web 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:<br>• rejected — станции отказано в доступе<br>• 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 |

| Параметр | Значение | |
|---|---|---|
| | 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 Dr.Web, 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 Dr.Web) |
| | GEN.ServerRecvLinkName | название последнего соседнего Сервера Dr.Web, 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 Dr.Web) |
| | GEN.ServerOriginatorID | UUID Сервера Dr.Web, к которому подключена станция, на которой произошла ошибка сканирования |
| | GEN.ServerOriginatorName | название Сервера Dr.Web, 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 |

| Параметр | Значение | |
|---|---|---|
| | лицензионных ключей, используемых Сервером Dr.Web).<br><br>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 Dr.Web, 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 Dr.Web) |
| | `GEN.ServerRecvLinkName` | название последнего соседнего Сервера Dr.Web, 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 Dr.Web) |
| | `GEN.ServerOriginatorID` | UUID Сервера Dr.Web, к которому подключена станция, на которой |

| Параметр | Значение | |
|---|---|---|
| | | произошла ошибка сканирования |
| | GEN.ServerOriginatorName | название Сервера Dr.Web, 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 Dr.Web. Подробности об ошибке приводятся в файле журнала Сервера Dr.Web. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | MSG.ID | UUID станции |
| | MSG.StationName | название станции |

### Станция давно не подключалась к Серверу Dr.Web

| Параметр | Значение | |
|---|---|---|
| Причина отправки оповещения | Отправляется согласно заданию в расписании Сервера Dr.Web. Содержит информацию о том, что станция давно не подключался к данному Серверу Dr.Web. 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 Dr.Web, настраиваемом в разделе **Администрирование** → **Планировщик задач Сервера Dr.Web**. | |
| Переменные | Общие переменные для станций, приведенные выше, недоступны. | |
| | MSG.DaysAgo | количество дней с момента последнего подключения к Серверу Dr.Web |
| | MSG.LastSeenFrom | адрес, с которого станция в последний раз подключалась к Серверу Dr.Web |
| | MSG.StationDescription | описание станции |

| Параметр | Значение | |
|---|---|---|
| | 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 Dr.Web и была подтверждена Сервером Dr.Web 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 Dr.Web 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 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 Dr.Web пытается подключиться станция с идентификатором, который совпадает с идентификатором станции уже подключенной к данному Серверу Dr.Web. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | `MSG.ID` | UUID станции |
| | `MSG.Server` | ID Сервера Dr.Web, 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 вредоносных объектов |
| | `MSG.Locked` | количество заблокированных объектов |
| | `MSG.Modifications` | количество объектов, инфицированных модификациями вирусов |
| | `MSG.Moved` | количество объектов, перемещенных в карантин |
| | `MSG.Renamed` | количество переименованных объектов |

| Параметр | Значение | |
|---|---|---|
| | 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 | количество обнаруженных угроз |
| | GEN.ServerRecvLinkID | UUID последнего соседнего Сервера Dr.Web, от которого была получена статистика сканирования подключенных к нему станций (пустое значение, если получена статистика со станций, подключенных к данному Серверу Dr.Web) |
| | GEN.ServerRecvLinkName | название последнего соседнего Сервера Dr.Web, от которого была получена статистика сканирования подключенных к нему станций (пустое значение, если получена статистика со станций, подключенных к данному Серверу Dr.Web) |
| | GEN.ServerOriginatorID | UUID Сервера Dr.Web, к которому подключена станция, с которой получена статистика сканирования |
| | GEN.ServerOriginatorName | название Сервера Dr.Web, 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:<br>• для завершения лечения, |

| Параметр | Значение | |
|---|---|---|
| | • для применения обновлений,<br>• для изменения состояния аппаратной виртуализации,<br>• для завершения лечения и применения обновлений,<br>• для завершения лечения и изменения состояния, аппаратной виртуализации,<br>• для применения обновлений и изменения состояния аппаратной виртуализации,<br>• для завершения лечения, применения обновлений и изменения состояния аппаратной виртуализации. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | `MSG.Reason` | причина перезагрузки<br><br>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` | время получения события, GMT |

### 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. | |
| Дополнительная настройка | Не требуется. | |
| Переменные | `MSG.Capabilities` | характеристики устройства |
| | `MSG.Class` | класс устройства (название родительской группы) |

| Параметр | Значение | |
|---|---|---|
| | 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 Г. 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).

## Г1. 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 Dr.Web и адреса Агента Dr.Web 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://(example.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. udx://tmp/drwcsd:datagram
```

### Адреса семейства SRV

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

## Г2. Форматы адресов, используемые Агентами Dr.Web и их инсталляторами

В данном разделе описаны форматы адресации Сервера Dr.Web для подключения к нему или обнаружения его со стороны Агента Dr.Web или инсталлятора Агента Dr.Web. Приведенные ниже форматы и настройки по умолчанию (при пустых значениях) применяются на стороне Агентов Dr.Web или их инсталляторов.

### Прямое соединение с Сервером Dr.Web

`[tcp://]<remote-socket-address>`

Например:

`tcp://192.168.1.42:2193`

где `192.168.1.42` — адрес Сервера Dr.Web, `2193` — порт.

По умолчанию (если адрес не задан) применяются следующие значения:

`tcp://127.0.0.1:2193`

где `127.0.0.1` — адрес Сервера Dr.Web, `2193` — порт.

Информация о прямых соединениях представлена в **Руководстве администратора**, в разделе Прямые соединения.

### Поиск Сервера Dr.Web через Службу обнаружения Сервера Dr.Web с указанием семейства протоколов и конечной точки

*<drwcs-name>*`@udp://<endpoint-socket-address>[-<interface>]`

По умолчанию (если адрес не задан) применяются следующие значения:

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

При данных значениях выполняется поиск Сервера Dr.Web с именем `drwcs` по протоколу UDP с использованием multicast-группы `231.0.0.1:2193` на всех интерфейсах.

Информация о Службе обнаружения Сервера Dr.Web представлена в **Руководстве администратора**, в разделе Служба обнаружения Сервера Dr.Web.

# Приложение Д. 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 Dr.Web.

При настройке межсерверных связей (см. в **Руководстве администратора**, п. Особенности сети с несколькими Серверами Dr.Web) 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 Dr.Web сохраняйте конфигурацию идентичной,
- для подчиненных Серверов Dr.Web отключите синхронизацию компонентов по протоколу HTTP или сохраняйте конфигурацию идентичной.

## Д1. 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
```

## .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 Dr.Web под ОС семейства Unix. Поддержка протокола SMB осуществлена при помощи `curl` (поддерживает только SMBv1).

**Например:**

```
https
```

## .auth

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

Параметры аутентификации задаются в следующем формате:

```
<метод аутентификации>

<имя пользователя>

<пароль>
```

В качестве метода аутентификации может быть указано одно из следующих значений: `none | any | safe | basic | digest | digestie | ntlm | ntlmwb | negotiate`. Значения соответствуют значениям выпадающего списка **Метод авторизации** в разделе **Администрирование** → **Общая конфигурация репозитория** → **BCO Dr.Web** в Центре управления.

Имя пользователя — обязательный параметр, пароль — опциональный.

**Например:**

```
safe

admin

root
```

## .version

Файл `.version` содержит версию сервера, с зоны которого должны быть скачаны обновления. Используется в отладочных целях, по умолчанию соответствует текущей версии сервера в формате MM.mm.

## .max-retry

Файл `.max-retry` содержит максимальное количество попыток при ошибках скачивания с каждого из серверов обновления.

## .cdn-mode

Файл `.cdn-mode` содержит настройки для использования Content Delivery Network (CDN) при загрузке репозитория.

Может принимать одно из следующих значений:

- `on` — использовать CDN,
- `off` — не использовать CDN.

## .cert-mode

Файл `.cert-mode` содержит настройки для допустимых SSL-сертификатов серверов обновления, которые будут автоматически приниматься.

Может принимать одно из следующих значений:

- `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-file

Файл `.cert-file` содержит путь к пользовательскому сертификату, если указан режим `custom` для параметра `cert`.

### .ssh-mode

Файл `.ssh-mode` содержит настройки режима авторизации при использовании протоколов SCP и SFTP (основаны на SSH2).

Может принимать одно из следующих значений:

- `pwd` — авторизация по регистрационному имени пользователя и паролю,
- `pubkey` — авторизация по ключам шифрования.

### .ssh-pubkey

Файл `.ssh-pubkey` содержит путь к открытому SSH-ключу сервера обновлений.

### .ssh-prikey

Файл `.ssh-prikey` содержит путь к закрытому SSH-ключу сервера обновлений.

### .sync-ignore-flavoured

Файл `.sync-ignore-flavoured` содержит перечень тех защитных компонентов, которые не будут синхронизироваться с зоны обновлений в локальный репозиторий.

## Д2. 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
```

### ..languages

Файл `..languages` содержит список кодов языков, для которых настроено обновление. Если файл отсутствует или пустой, обновление не настроено ни для каких языков и производиться не будет.

### ..platforms

Файл `..platforms` содержит полные коды платформ, использующиеся в продукте, для которых настроено обновление. Если файл отсутствует или пустой, обновление не настроено ни для каких платформ и производиться не будет.

### ..formats

Файл `..formats` содержит форматы файлов, для которых настроено обновление, например, форматы документов (html, pdf). Если файл отсутствует или пустой, обновление не настроено ни для каких форматов и производиться не будет.

### ..items

Файл `..items` определяет, какие именно административные утилиты или корпоративные продукты подлежат обновлению. Если файл отсутствует или пустой, обновление не настроено ни для каких утилит или продуктов и производиться не будет.

### .sync-off

Файл `.sync-off` отключает обновление продукта. Содержимое не имеет значения.

### .deleted

Файл `.deleted` отмечает продукт, как удалённый. Все ревизии из него будут удалены, синхронизация с ВСО отключена.

## Файлы исключений при обновлении репозитория Сервера Dr.Web 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 регулярные выражения, определяющие 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 Dr.Web с Сервера Dr.Web

### .state-only

Файл `.state-only` содержит регулярные выражения, определяющие список файлов, которые будут синхронизироваться при обновлении Агентов Dr.Web с Сервера Dr.Web. Файлы репозитория, не заданные в `.state-only`, синхронизироваться не будут. Если файл `.state-only` отсутствует, то будут 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 Dr.Web с Сервера Dr.Web.

**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 обновления только файлов 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|APPROVAL]; UseFilter [YES|NO]
```

| Параметр | Возможные значения | Описание |
|---|---|---|
| `Delay` | `ON\|OFF\|APPROVAL` | • `ON` — заморозка обновлений продукта включена.<br>• `OFF` — заморозка обновлений продукта отключена.<br>• `APPROVAL` — заморозка обновлений продукта до подтверждения администратором. |
| `UseFilter` | `YES\|NO` | • `Yes` — замораживать обновления только если обновленные файлы соответствуют списку исключений в файле `.delay-only`.<br>• `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
```

## .on-demand

Наличие файла означает, что включена синхронизация продукта по требованию, т.е. при наличии клиентов, запрашивающих данный продукт.

## .is-sync-off-in

Наличие файла означает, что отключено получение обновлений продукта через межсерверные связи.

### .is-sync-off-out

Наличие файла означает, что отключена раздача обновлений продукта через межсерверные связи.

### .no-platform

Наличие файла означает, что директории верхнего уровня в ревизии продукта не считаются платформами, то есть ревизия распространяется на любые платформы.

## Приложение Е. 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 Dr.Web данных. |
| drwcsd-proxy.conf | Конфигурационный файл Прокси-сервера Dr.Web. |
| drwreploader.conf | Конфигурационный файл Загрузчика репозитория. |
| share.conf | Конфигурационный файл разделяемого ресурса. |

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

После сохранения всех внесенных изменений рекомендуется включить компонент **Самозащита**.

## Е1. Конфигурационный файл Сервера Dr.Web

Конфигурационный файл Сервера Dr.Web `drwcsd.conf` по умолчанию располагается в подкаталоге `etc` корневого каталога Сервера Dr.Web. При запуске Сервера Dr.Web при помощи параметра командной строки может задаваться нестандартное расположение и

наименование конфигурационного файла (подробнее см. Приложение Ж3. Сервер Dr.Web).

**Чтобы вручную отредактировать конфигурационный файл Сервера Dr.Web**

1. Остановите Сервер Dr.Web (см. **Руководство администратора**, п. Сервер Dr.Web).
2. Отключите Самозащиту (в случае наличия на компьютере Агента Dr.Web с активной Самозащитой — в контекстном меню Агента Dr.Web).
3. Внесите необходимые изменения в конфигурационный файл Сервера Dr.Web.
4. Запустите Сервер Dr.Web (см. **Руководство администратора**, п. Сервер Dr.Web).

## Формат конфигурационного файла Сервера Dr.Web

Конфигурационный файл Сервера Dr.Web 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 Dr.Web, инсталляторы Агентов Dr.Web или Центр управления. Оставьте значение параметра пустым ("" — используется по умолчанию), чтобы использовать имя компьютера, на котором установлен Сервер Dr.Web.

  В качестве адреса Сервера Dr.Web рекомендуется использовать имя Сервера Dr.Web в формате FQDN, предварительно зарегистрированное в службе DNS. Это упростит процесс настройки антивирусной сети, связанный с процедурой переустановки Сервера Dr.Web на другой компьютер. В таком случае при смене адреса Сервера Dr.Web достаточно будет изменить его в настройках DNS-сервера для имени компьютера с Сервером Dr.Web, чтобы все агенты автоматически подключились к новому серверу.

  1. Если в сети функционирует локальный DNS-сервер, необходимо создать в нём отдельное имя для Сервера Dr.Web, а также для Прокси-сервера Dr.Web (например, `drwebes.company.lan`).
  2. В настройках Агентов Dr.Web следует указывать имя Dr.Web Сервера в формате FQDN.
  3. Дополнительно к имени в формате FQDN в настройках Агента Dr.Web рекомендуется добавить также адрес Сервера Dr.Web и поддерживать этот адрес в актуальном состоянии при его изменении. В этом случае при невозможности работы с именем сервера агент выполнит попытку подключения по адресу сервера.

- `<id value="" />`

  Уникальный идентификатор Сервера Dr.Web. До 10 версии содержался в лицензионном ключе Сервера Dr.Web. Хранится в конфигурационном файле Сервера Dr.Web.

- `<passwd-salt value="" />`

  Криптографическая соль. Строка случайных данных, которая добавляется к паролю администратора, после чего объединенное значение обрабатывается хеш-функцией и хранится в виде единого хеша в базе данных, для защиты пароля от взлома путем перебора возможных вариантов. Генерируется по умолчанию при установке или обновлении Сервера Dr.Web с предыдущих версий.

  В дополнение к статической соли, для каждого пароля генерируется также динамическая соль. В качестве кода аутентификации HMAC при расчете отпечатка соленого пароля используется стандарт формирования ключа на основе пароля PBKDF2. Таким образом, объединение пароля и соли с последующим хешированием проводится многократно. Статическая соль по умолчанию отключена, динамическая соль используется всегда.

  

  При наличии соли просмотр и изменение пароля администратора с помощью предоставляемой утилиты для работы с базой данных Сервера Dr.Web (`drwidbsh3`) становится невозможным.

  

  При использовании кластера Серверов Dr.Web необходимо вручную задать одно и то же значение соли на всех Серверах Dr.Web, входящих в кластер.

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

  Географическое расположение Сервера Dr.Web.

  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 клиентов Сервера Dr.Web (Агентов Dr.Web и их инсталляторов, соседних Серверов Dr.Web, Прокси-серверов Dr.Web). Минимальное значение — 5. По умолчанию — 5.

  Данный параметр влияет на производительность Сервера Dr.Web. При использовании встроенной базы данных менять значение по умолчанию не рекомендуется. При использовании внешней базы данных может потребоваться большее значение параметра (см. раздел Нагрузка на Сервер Dr.Web и рекомендуемые параметры настройки). При работе в сети с большим количеством подключений клиентов к Серверу Dr.Web перед изменением значения рекомендуется получить консультацию в службе технической поддержки компании «Доктор Веб».

- `<newbie approve-to-group="" 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**. |
| `mode` | • `open` — автоматически разрешать доступ,<br>• `closed` — всегда отказывать в доступе,<br>• `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 Dr.Web из группового инсталляционного пакета, если уже созданных учетных записей недостаточно.

| Атрибут | Допустимые значения | По умолчанию |
|---|---|---|
| `enabled` | • `yes` — автоматически создавать недостающие учетные записи станций,<br>• `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 Dr.Web. Не следует изменять значение параметра без рекомендации службы поддержки «Доктор Веб».

- <reverse-resolve enabled="" />

  Заменять IP-адреса на DNS-имена компьютеров в полях с адресами рабочих станций в Центре управления. Допустимые значения атрибута enabled:

  - yes — использовать DNS-имена,
  - no (по умолчанию) — использовать IP-адреса.

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

  Заменять имена компьютеров на DNS-имена в Центре управления.

  Описание атрибутов:

| Атрибут | Допустимые значения | Описание |
|---|---|---|
| enabled | • yes — заменять,<br>• no — не заменять. Будут применяться настройки <agent-host-names />. | Режим замены имен. |
| host | • yes — отображать частично определенные DNS-имена (до точки в FQDN),<br>• no — отображать полностью определенные DNS-имена (FQDN). | Формат отображаемого имени после замены. |

- <agent-host-names mode="" />

  Формат, в котором имена станций антивирусной сети передаются Агентами Dr.Web на Сервер Dr.Web и отображаются в каталоге антивирусной сети Центра управления. Данная настройка игнорируется, если у параметра <replace-netbios-names /> атрибут enabled имеет значение yes.

  Допустимые значения атрибута mode:

  - netbios — NetBIOS-имена (используется по умолчанию при пустом значении атрибута или отсутствии параметра целиком),
  - fqdn — полностью определенные DNS-имена (FQDN),
  - host — частично определенные DNS-имена (до точки в FQDN).

- <dns>

  Настройки DNS.

- <timeout value="" />

  Тайм-аут в секундах для разрешения прямых/обратных DNS-запросов. Установите значение 0, 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,<br>• 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 Dr.Web 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 Dr.Web 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 Dr.Web описанием со станции,
  - no (по умолчанию) — игнорировать описание на станции.

- <time-discrepancy value="" />

  Допустимая разница 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,<br>• no — не использовать сжатие,<br>• 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 Dr.Web 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 Dr.Web. 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 Dr.Web. 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 Dr.Web. 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 Dr.Web. Допустимые значения атрибута enabled: yes или no.

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

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

- <keep-infection enabled="" />

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

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

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

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

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

- <keep-installation enabled="" />

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

- `<quarantine enabled="" />`

  Разрешить отслеживать информацию о состоянии Карантина на станциях и записывать информацию в базу данных Сервера Dr.Web. 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 Dr.Web и Агентами Dr.Web.

  Описание атрибутов:

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| `queue-size` | • целое положительное число,<br>• `unlimited`. | Максимальное допустимое количество сессий раздачи обновлений, запущенных одновременно с Сервера Dr.Web. При достижении указанного ограничения запросы от Агентов Dr.Web размещаются в очереди ожидания. Размер очереди ожидания не ограничен. | `unlimited` |
| `value` | • максимальная скорость в КБ/с,<br>• `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 Dr.Web в процессе установок Агентов Dr.Web на станциях.

  Описание атрибутов:

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

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

  Разрешить синхронизацию географического расположения станций между Серверами Dr.Web.

  Описание атрибутов:

| Атрибут | Допустимые значения | Описание |
|---|---|---|
| enabled | • yes — разрешить синхронизацию,<br>• 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 Dr.Web. Допустимые значения атрибута enabled: yes или no.

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

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

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

  Разрешить отслеживать операции через Web API и записывать информацию в базу данных Сервера Dr.Web. 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,<br>• any — любой метод из поддерживаемых,<br>• safe — любой безопасный метод из поддерживаемых,<br>• следующие методы, если несколько, то указывать все необходимые через пробел:<br>▫ basic<br>▫ digest<br>▫ digestie<br>▫ ntlmwb<br>▫ ntlm<br>▫ negotiate | Тип авторизации на прокси-сервере. По умолчанию — any. |
| enabled | • yes — использовать прокси-сервер,<br>• no — не использовать прокси-сервер. | Режим подключения к Серверу Dr.Web 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 обнаруженным угрозам в компанию «Доктор Веб» в раздел https://stat.drweb.com/.

  Описание атрибутов:

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| enabled | • yes — отправлять статистику, | Режим отправки статистики в компанию «Доктор Веб». | – |

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| | • `no` — не отправлять статистику. | | |
| `id` | – | MD5 лицензионного ключа Агента Dr.Web. | – |
| `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 Dr.Web 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`<br><br>`<port value="" />` | `value` | Номер порта сетевого интерфейса Сервера Dr.Web, к которому привязывается транспортный multicast-протокол для передачи обновлений. Данный порт будет использоваться всеми multicast-группами.<br><br>Для групповых обновлений необходимо задавать любой свободный порт, который будет отличаться от порта, назначенного в настройках для работы транспортного протокола самого Сервера Dr.Web. | 2197 |

| Дочерний элемент | Атрибут | Описание | По умолчанию |
|---|---|---|---|
| ttl<br><br><ttl value="" /> | value | Срок жизни передаваемой UDP-датаграммы. Заданное значение будет использоваться всеми multicast-группами. | 8 |
| group<br><br><group address="" /> | address | IP-адрес multicast-группы, через которую станции будут получать групповые обновления. | 233.192.86.0 для IPv4<br><br>FF0E::176 для IPv6 |
| on<br><br><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<br><br><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.<br><br>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 Dr.Web начинает отправку следующего файла.<br><br>Все файлы, которые не удалось передать на этапе обновления по multicast-протоколу, будут передаваться в процессе стандартного обновления по протоколу TCP. | 180000 |
| | updates-interval | Длительность групповых обновлений (мс.) — длительность процесса обновления по multicast-протоколу.<br><br>Все файлы, которые не удалось передать на этапе обновления по multicast-протоколу, будут передаваться в процессе стандартного обновления по протоколу TCP. | 600000 |

| Дочерний элемент | Атрибут | Описание | По умолчанию |
|---|---|---|---|
| | chunks-interval | Интервал отправки пакетов (мс.) — интервал отправки пакетов в multicast-группу.<br><br>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 Dr.Web отправляют запросы на повторную передачу потерянных пакетов.<br><br>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 Dr.Web не поступило запросов на повторную передачу потерянных пакетов, Сервер Dr.Web считает, что все Агенты Dr.Web успешно получили файлы обновления, и начинает отправку следующего файла. | 10000 |
| | accumulate-interval | Интервал накопления запросов на повторную передачу (мс.) — в течение указанного интервала Сервер Dr.Web накапливает запросы от Агентов Dr.Web на повторную передачу потерянных пакетов.<br><br>Агенты Dr.Web перезапрашивают потерянные пакеты. Сервер Dr.Web накапливает эти запросы в течение указанного времени, после чего пересылает потерянные блоки. | 2000 |
| | announce-send-times | Количество анонсов передачи файла — количество раз, которое Сервер Dr.Web анонсирует передачу файла в multicast-группу перед началом передачи обновлений.<br><br>При анонсе в multicast-группу направляется UDP-датаграмма с метаданными файла. Увеличение количества анонсов способно повысить надежность передачи, но может | 3 |

| Дочерний элемент | Атрибут | Описание | По умолчанию |
|---|---|---|---|
| | | 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 Dr.Web. 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 Dr.Web.<br><br>При использовании встроенной базы данных значение по умолчанию менять не рекомендуется. | 2 |

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| | | При использовании внешней базы данных может потребоваться большее значение атрибута (см. раздел Нагрузка на Сервер Dr.Web и рекомендуемые параметры настройки). При работе в сети с большим количеством подключений клиентов к Серверу Dr.Web перед изменением значения рекомендуется получить консультацию в службе технической поддержки компании «Доктор Веб». | |
| 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="" 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 |
| readuncommitted | on \| off | Переход на уровень изоляции транзакции READ UNCOMMITTED (чтение данных, которые были | off |

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| | | изменены или удалены, но не зафиксированы другой транзакцией). | |
| precompiledcache | Целое положительное число. | Размер кеша предкомпилированных SQL-операторов в байтах. | 1048576 |
| synchronous | • TRUE или FULL — синхронный<br>• FALSE или NORMAL — обычный<br>• OFF — асинхронный | Режим записи данных. | FULL |
| 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 семейства Unix — 10485760<br>• 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. | – |
| options | – | Параметры командной строки для отправки на сервер базы данных.<br><br>Подробнее см. в главе 18 https://www.postgresql.org/docs/9.1/libpq-connect.html | – |
| requiressl | • 1 \| 0 (через Центр управления)<br>• y \| n<br>• yes \| no<br>• on \| off | Использовать только SSL-соединения. | • 0<br>• y<br>• yes<br>• 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<br>• read committed<br>• repeatable read<br>• serializable | Уровень изоляции транзакций. | read committed |
| debugproto | • yes \| no<br>• on \| off | Вести отладочный журнал работы СУБД. | • yes<br>• on |

- `<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 пары ключ-значение Oracle Net. | – |
| user | – | Регистрационное имя пользователя базы данных. | – |
| password | – | Пароль пользователя базы данных. | – |
| client | – | Путь к клиенту для доступа к БД Oracle (Oracle Instant Client). Сервер Dr.Web поставляется с Oracle Instant Client версии 11. 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 (значение по умолчанию 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="" limit="" 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 |

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| transaction | • SERIALIZABLE — упорядочиваемость<br>• READ_UNCOMMITTED — чтение незафиксированных данных<br>• READ_COMMITTED — чтение зафиксированных данных<br>• REPEATABLE_READ — повторяемость чтения<br>• DEFAULT — равносильно "" — зависит от СУБД. | Уровень изоляции транзакций.<br>Некоторые СУБД поддерживают только READ_COMMITTED. | DEFAULT |

- `<mysql dbname="drwcs" host="localhost" port="3306" user="" password="" ssl="no" precompiledcache="" 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 Dr.Web 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 | Размер кеша предкомпилированных SQL- | 1048576 |

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| | число. | операторов в байтах. | |
| debug | • yes \| no<br>• on \| off | Вести отладочный журнал работы СУБД. | • no<br>• off |

- **<acl>**

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

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

  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`,<br>• `no`. | Записывать в журнал информацию о профилировании работы скриптов Сервера Dr.Web. 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 Dr.Web. Данный параметр используется службой технической поддержки и разработчиками. Не рекомендуется изменять его значение без необходимости. | |
| `trace` | | Записывать в журнал информацию о трассировке работы скриптов Сервера Dr.Web. 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 Dr.Web.

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

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

- <transports>

  Настройка параметров транспортных протоколов, используемых Сервером Dr.Web 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 Dr.Web. | нет, задается только вместе с атрибутом ip. | yes, no | no |
| ip \| unix | Определяет семейство используемых протоколов (IP или Unix-сокет) и задает адрес интерфейса. | да | – | 0.0.0.0 \| – |
| name | Задает имя Сервера Dr.Web для службы обнаружения Сервера Dr.Web. | нет | – | drwcs |
| multicast | Определяет, входит ли Сервер Dr.Web в multicast-группу. Данная настройка доступна только при включении службы обнаружения Сервера Dr.Web (параметр discovery): если он выключен, то multicast запросы прослушиваться не будут. | нет, задается только вместе с атрибутом ip. | yes, no | no |
| multicast-group | Задает адрес multicast-группы, в которую входит Сервер Dr.Web. | нет, задается только вместе с атрибутом ip. | – | • 231.0.0.1<br>• [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,<br>• no — протокол отключен. | Режим использования протокола. | no |
| name | • AGENT — протокол взаимодействия Сервера Dr.Web с Агентами Dr.Web.<br>• MSNAPSHV — протокол взаимодействия Сервера Dr.Web с компонентом проверки работоспособности системы Microsoft NAP Validator.<br>• INSTALL — протокол взаимодействия Сервера Dr.Web с инсталляторами Агентов Dr.Web.<br>• CLUSTER — протокол взаимодействия между Серверами Dr.Web в кластерной системе.<br>• 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,<br>• no — расширение отключено. | Режим использования расширения. | no |
| name | • WEBMIN — расширение Центра управления безопасностью Dr.Web для управления Сервером Dr.Web и антивирусной сетью через Центр управления.<br>• FrontDoor — расширение Dr.Web Server FrontDoor, позволяющего подключение утилиты дистанционной диагностики Сервера Dr.Web. | Название расширения. | – |

- **<license>**

  Настройки лицензирования.

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

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

    Настройки оповещения об ограничении по количеству лицензий в лицензионном ключе.

    Описание атрибутов:

| Атрибут | Описание | По умолчанию |
|---|---|---|
| min-count | Максимальное количество оставшихся лицензий, при котором будет отправлено оповещение **Ограничение по количеству лицензий в лицензионном ключе**. | 3 |
| min-percent | Максимальный процент оставшихся лицензий, при котором будет отправлено оповещение **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 Dr.Web об используемых им лицензионных ключах.<br><br>Если отчет об использовании лицензий создается подчиненным Сервером Dr.Web, то сразу после создания осуществляется отправка этого отчета на главный Сервер Dr.Web.<br><br>Созданные отчеты дополнительно отправляются при каждом подключении (в т.ч. перезагрузке) Сервера Dr.Web, а также при изменении количества выдаваемых лицензий на главном Сервере Dr.Web. | 1440 |
| 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 Dr.Web. Настройка используется, если данный Сервер Dr.Web выдает лицензии соседним Серверам Dr.Web. | 1440 |
| `prolong-preact` | **Период для продления получаемых лицензий** — период до окончания срока действия лицензии, начиная с которого данный Сервер Dr.Web инициирует продление лицензии, полученной от соседнего Сервера Dr.Web. Настройка используется, если данный Сервер Dr.Web получает лицензии от соседних Серверов Dr.Web. | 60 |
| `check-interval` | **Период синхронизации лицензий** — периодичность синхронизации информации о выдаваемых лицензиях между Серверами Dr.Web. | 1440 |

- `<auth-flood count="" only-failed="" period="" />`

  Настройки авторизации. При превышении указанного числа попыток авторизация будет невозможна в течение определенного времени.

  Описание атрибутов:

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| `count` | – | Количество попыток авторизации. | `5` |
| `only-failed` | • `yes` — учитывать только неуспешные авторизации,<br>• `no` — учитывать как неуспешные, так и успешные авторизации. | Учитывать только неуспешные авторизации. | `yes` |
| `period` | – | Период времени, в течение которого авторизация будет невозможна. | 60 секунд |

- `<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,<br>• 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,<br>• 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,<br>• no — не использовать SSL. | Режим использования SSL-шифрования. | no |
| verify_cert | • yes — проверять SSL-сертификат,<br>• 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 эпидемий угроз в сети.

  Описание атрибутов:

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| enabled | yes \| no | Разрешает отслеживать множественные события о заражениях станций и иметь возможность отправлять суммарное оповещение администратору. | yes |
| 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 оповещение 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 отправляться оповещения о единичных событиях. | 300 |

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| 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 |
| 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 | 100 |

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| | | отчет об этих событиях (оповещение **Зафиксировано большое количество блокировок Контролем приложений**). | |
| 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 соединений с клиентами, чтобы отправить соответствующее оповещение. | 3600 |
| 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 | 1000 |

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| | | **Зафиксировано большое количество аварийно завершенных соединений**). | |
| `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 Dr.Web. 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.

- `<security-through-obscurity="" />`

  Настройка параметров безопасности, позволяющих усилить безопасность за счет сокрытия или намеренного искажения некоторых данных.

  Элемент `<security-through-obscurity>` содержит следующие дочерние элементы:

  - `<server-header enabled="" />`
  - `<lower-case-uri enabled="" />`
  - `<hacker-misleading enabled="" />`

  Описание атрибутов:

| Атрибут | Допустимые значения атрибута enabled | Описание | Значение атрибута enabled по умолчанию |
|---|---|---|---|
| `server-header` | `yes \| no` | Позволяет не показывать строку с данными сервера (версией Сервера Dr.Web, версией ОС, используемыми библиотеками), что усложняет задачу по поиску известных уязвимостей.<br><br>Соответствует настройке **Возвращать подробный заголовок** в конфигурации веб-сервера. | `no` |

| Атрибут | Допустимые значения атрибута enabled | Описание | Значение атрибута enabled по умолчанию |
|---|---|---|---|
| `lower-case-uri` | `yes \| no` | При включении опция преобразует URI в нижний регистр.<br><br>Соответствует настройке **Преобразовывать URI в нижний регистр** в конфигурации веб-сервера. | `no` |
| `hacker-misleading` | `yes \| no` | При включении в ответ на запросы файлов вида `/etc/passwd`, `/etc/hosts` и пр. (в расчете на наличие уязвимости класса Path/Directory Traversal) возвращает им поддельные `passwd`, `hosts` и пр.<br><br>Соответствующей настройки в конфигурации веб-сервера на данный момент не имеет. | `yes` |

## E2. 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 Dr.Web.

**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 Dr.Web>*`[:`*<порт>*`]`

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

  Если номер порта не задан, используется порт, заданный в запросе (например, при обращении к Серверу Dr.Web 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 Dr.Web.

- `<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 Dr.Web. 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 Dr.Web 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 | 1024 Б/с |

| Атрибут | Описание | По умолчанию |
|---|---|---|
| | будет отказано. Задайте значение 0, чтобы снять данное ограничение. | |

- `<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 Dr.Web. Не рекомендуется изменять его значение без необходимости. | 8192 байт |
| `receive` | Размер буферов, используемых при получении данных. Данный параметр влияет на производительность Сервера Dr.Web. Не рекомендуется изменять его значение без необходимости. | 2048 байт |

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

  Максимально допустимый размер HTTP-запроса в КБ.

- `<xheaders>`

  Параметр для добавления пользовательских HTTP-заголовков. По умолчанию уже заведены три заголовка, призванные защитить от сетевых атак:

  - `<xheader name="X-XSS-Protection" value="1; mode=block"/>`

    Заголовок управляет поведением веб-браузера при обнаружении кода, встроенного в атакуемую страницу (так называемая «XSS-атака»). Возможные значения:

| Значение | Поведение браузера |
|---|---|
| `0` | XSS-фильтр отключен. |
| `1` | XSS-фильтр включен. При обнаружении XSS-атаки веб-браузер удалит встроенный код. |
| `1; mode=block` | XSS-фильтр включен. При обнаружении XSS-атаки веб-браузер не будет загружать скомпрометированную страницу. Используется по умолчанию. |
| `1; report=`*<сетевой-адрес>* | XSS-фильтр включен. При обнаружении XSS-атаки веб-браузер удалит встроенный код и отправит отчет на указанный адрес. Поддерживается только в веб-браузерах на основе Chromium. |

  - `<xheader name="X-Content-Type-Options" value="nosniff"/>`

    При значении по умолчанию (`nosniff`) заголовок запрещает браузеру определять MIME-тип содержимого независимо от указанного в `Content-Type` типа и обрабатывать его соответствующим образом (так называемый «MIME-сниффинг»).

- `<xheader name="X-Frame-Options" value="SAMEORIGIN"/>`

  Заголовок управляет поведением веб-браузера при обнаружении попытки встроить веб-страницу в сторонний фрейм (так называемый «кликджекинг»). Возможные значения:

| Значение | Поведение браузера |
|---|---|
| DENY | Запрещает веб-браузеру загружать страницу во фрейме. |
| SAMEORIGIN | Разрешает веб-браузеру загружать страницу во фрейме, если у страницы и фрейма один источник (домен, порт и протокол). Используется по умолчанию. |
| ALLOW-FROM <сетевой-адрес> | Разрешает веб-браузеру загружать страницу во фрейме только при условии, что страница находится указанному адресу. |

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

  Заменять IP-адреса DNS-именами компьютеров в файле журнала Сервера Dr.Web. 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,<br>• no — отключить профилирование. | Режим профилирования скрипов. |
| stack | • yes — записывать данные в журнал,<br>• no — не записывать данные в журнал. | Режим записи информации о профилировании (параметры функции и возвращаемые значения) в журнал Сервера Dr.Web. |

- `<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="" ciphers="" />`

  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`,<br>• `no`. | `yes` |
| `ciphers` | Список и настройки используемых шифров. | Подробное описание см. в документации для OpenSSL, раздел **CIPHER LIST FORMAT**. | `HIGH:!aNULL:!RC4:@STRENGTH` |

- `<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 |
| deny | Адреса, с которых будет запрещен доступ по протоколу HTTP для незащищенных соединений. | - |

## Е3. Конфигурационный файл download.conf

**Назначение файла download.conf:**

1. При создании и использовании кластерной системы Серверов Dr.Web позволяет распределить нагрузку между Серверами Dr.Web 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 Dr.Web.

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

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

где:

- <*Server_Address*> — доменное имя или IP-адрес Сервера Dr.Web.

  

  В качестве адреса Сервера Dr.Web рекомендуется использовать имя сервера в формате FQDN.

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

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

  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 Dr.Web.

## E4. 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 обнаружения Прокси-сервера Dr.Web. Позволяет клиентам обнаруживать функционирующий Прокси-сервер в процессе его поиска через широковещательные запросы. | yes |
| multicast | нет | yes, no | Режим "прослушивания" сети для приема широковещательных запросов Прокси-сервером. | yes |
| multicast-group | нет | – | Многоадресная группа, в которой располагается Прокси-сервер. | 231.0.0.1<br>[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:<br>• *<protocol>*://*<interface>*:*<port-number>* — использовать IPv4 и IPv6.<br>• *<protocol>*://(*<interface>*):*<port-number>* — использовать только IPv4. | Адрес Сервера Dr.Web, на который будет перенаправлено соединение. | да |

| Атрибут | Допустимые значения | Описание | Обязательный |
|---|---|---|---|
| | • *<protocol>*://[*<interface>*]:*<port-number>* — использовать только IPv6. | | |
| master | • yes — Сервер Dr.Web будет безусловным управляющим.<br>• no — Сервер Dr.Web не будет управляющим ни при каких условиях.<br>• possible — Сервер Dr.Web 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 Dr.Web через Центр управления Сервера Dr.Web, указанного в атрибуте to.<br><br>Вы можете назначить любое количество Серверов Dr.Web управляющими (значение master="yes"), подключение осуществляется ко всем управляющим Серверам Dr.Web по порядку следования в настройках Прокси-сервера Dr.Web до первого получения валидной (не пустой) конфигурации.<br><br>Также вы можете не назначать ни один из Серверов Dr.Web управляющим (значение master="no"). В этом случае настройка параметров Прокси-сервера Dr.Web (в том числе назначение управляющих Серверов Dr.Web) возможна только локально через конфигурационный файл Прокси-сервера Dr.Web. | нет |

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

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

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

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

- <encryption mode="">

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

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

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

Описание атрибутов:

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| value | • максимальная скорость в КБ/с,<br>• unlimited | Максимальное значение суммарной скорости при передаче обновлений. | unlimited |
| queue-size | • целое положительное число,<br>• unlimited | Максимальное допустимое количество сессий раздачи обновлений, запущенных одновременно с Сервера Dr.Web. При достижении указанного ограничения запросы от Агентов Dr.Web 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 | • максимальная скорость в КБ/с,<br>• unlimited | Максимальное значение суммарной скорости при передаче данных при обновлении Агента Dr.Web. | unlimited |
| time-map | – | Маска, указывающая на временной промежуток, в течение которого будет активно ограничение. | – |

Значение атрибута time-map задается автоматически после указания соответствующей настройки в веб-интерфейсе Центра управления (см. **Руководство администратора**, раздел Удаленная настройка Прокси-сервера). Задать time-map вручную через конфигурационный файл удобным способом на данный момент нельзя.

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

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

Описание атрибутов:

| Атрибут | Допустимые значения | Описание | По умолчанию |
|---|---|---|---|
| value | • максимальная скорость в КБ/с,<br>• unlimited | Максимальное значение суммарной скорости при передаче данных в процессе установки Агентов Dr.Web. | unlimited |
| queue-size | • целое положительное число,<br>• unlimited | Максимальное допустимое количество сессий установки Агента Dr.Web, запущенных одновременно с Сервера Dr.Web. При достижении указанного ограничения запросы от Агентов Dr.Web 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 | • максимальная скорость в КБ/с,<br>• unlimited | Максимальное значение суммарной скорости при передаче данных при установке Агента Dr.Web. | unlimited |
| time-map | – | Маска, указывающая на временной промежуток, в течение которого будет активно ограничение. | – |

Значение атрибута time-map задается автоматически после указания соответствующей настройки в веб-интерфейсе Центра управления (см. **Руководство администратора**, раздел Удаленная настройка Прокси-сервера). Задать time-map вручную через конфигурационный файл удобным способом на данный момент нельзя.

- <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 атрибута schedule задается автоматически после указания соответствующей настройки в веб-интерфейсе Центра управления (см. **Руководство администратора**, раздел Удаленная настройка Прокси-сервера). Задать schedule вручную через конфигурационный файл удобным способом на данный момент нельзя.

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

- 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,
- 15-drwhashdb — известные хеши угроз,

- 20-drwagent — Агент Dr.Web для Windows,
- 20-drwandroid11 — вирусные базы для Android,
- 20-drwcs — Сервер Dr.Web,
- 20-drwunix — базы контент-фильтров для UNIX,
- 25-drwcsdoc — документация,
- 40-drwproxy — Прокси-сервер Dr.Web,
- 70-drwextra — корпоративные продукты Dr.Web,
- 70-drwutils — административные утилиты Dr.Web,
- 80-drwnews — новости компании «Доктор Веб».

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

  Настройки кеширования событий, полученных от Агентов Dr.Web.

  Описание атрибутов:

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

Значение атрибута `schedule` задается автоматически после указания соответствующей настройки в веб-интерфейсе Центра управления (см. **Руководство администратора**, раздел Удаленная настройка Прокси-сервера). Задать `schedule` вручную через конфигурационный файл удобным способом на данный момент нельзя.

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

  Настройка автоматического обновления Прокси-сервера.

  При включенном автоматическом обновлении, если синхронизация включена, то обновления Прокси-сервера будут скачиваться с Сервера Dr.Web 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. | – |

Значение атрибута schedule задается автоматически после указания соответствующей настройки в веб-интерфейсе Центра управления (см. **Руководство администратора**, раздел Удаленная настройка Прокси-сервера). Задать schedule вручную через конфигурационный файл удобным способом на данный момент нельзя.

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: %APPDATA%\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,<br>• `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.

## E5. Конфигурационный файл Загрузчика репозитория

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

**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 \| mirror` |

| Атрибут | Описание | Допустимые значения |
|---|---|---|
| | • `repository` — осуществляется скачивание репозитория в формате репозитория Сервера Dr.Web. Загруженные файлы могут быть непосредственно импортированы через Центр управления в качестве обновления репозитория Сервера Dr.Web.<br>• `mirror` — осуществляется скачивание репозитория в формате зоны обновлений ВСО. Загруженные файлы могут быть выложены на зеркало обновлений в вашей локальной сети. В дальнейшем Серверы Dr.Web могут быть настроены на получение обновлений непосредственно с данного зеркала обновлений, содержащего последнюю версию репозитория, а не с серверов ВСО. | |
| `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 Dr.Web 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 Dr.Web.<br><br>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,<br>▫ valid — принимать только проверенные сертификаты,<br>▫ drweb — принимать только сертификаты Dr.Web,<br>▫ 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 />.<br>▫ 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,<br>• `10-drwbases` — вирусные базы,<br>• `10-drwgatedb` — базы SpIDer Gate,<br>• `10-drwspamdb` — базы Антиспама,<br>• `10-drwupgrade` — Модуль обновления Dr.Web,<br>• `15-drwhashdb` — известные хеши угроз,<br>• `20-drwagent` — Агент Dr.Web для Windows,<br>• `20-drwandroid11` — вирусные базы для Android,<br>• `20-drwcs` — Сервер Dr.Web,<br>• `20-drwunix` — базы контент-фильтров для UNIX,<br>• `25-drwcsdoc` — документация,<br>• `40-drwproxy` — Прокси-сервер Dr.Web,<br>• `70-drwextra` — корпоративные продукты Dr.Web,<br>• `70-drwutils` — административные утилиты Dr.Web,<br>• `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,<br>• `hourly` — ежечасно,<br>• `daily` — ежедневно,<br>• `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 |

| Атрибут | Описание | Допустимые значения |
|---|---|---|
| `day` | День выполнения задания. Актуален для периода `weekly`. | • `mon` — понедельник,<br>• `tue` — вторник,<br>• `wed` — среда,<br>• `thu` — четверг,<br>• `fri` — пятница,<br>• `sat` — суббота,<br>• `sun` — воскресенье. |

## Е6. Конфигурационный файл share.conf

По умолчанию при установке Сервера Dr.Web для Windows создается разделяемый ресурс `DRWESI$`.

Его настройки хранятся в файле `/etc/share.conf`. По умолчанию содержимое файла включает в себя две строки:

1. Адрес разделяемого ресурса: `%ProgramFiles%\DrWeb Server\webmin\install`.
2. Имя разделяемого ресурса: по умолчанию `DRWESI$` (может быть изменено при установке).

**Чтобы изменить имя разделяемого ресурса**

1. Создайте новый разделяемый ресурс в настройках **Средства администрирования Windows**: откройте **Управление компьютером** → **Общие папки** → **Общие ресурсы**, в контекстном меню выберите пункт **Новый общий ресурс**.
2. Укажите имя нового ресурса в конфигурационном файле `share.conf`.

**Чтобы отключить разделяемый ресурс**

1. Отключите его в настройках **Средства администрирования Windows**: откройте **Управление компьютером** → **Общие папки** → **Общие ресурсы**, в контекстном меню ресурса выберите пункт **Прекратить общий доступ**.
2. Удалите конфигурационный файл `share.conf`.

# Приложение Ж. 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 Dr.Web, 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, не относятся к сетевому инсталлятору Агента Dr.Web.

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.

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`.

## Ж1. Сетевой инсталлятор

**Формат команды запуска:**

```
drwinst.exe [<ключи>]
```

### Ключи

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

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

Все значения 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 Dr.Web. 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 Dr.Web.

  Если ключ не задан, по умолчанию используется значение `possible`.
- `/encryption` <*режим*> — режим шифрования трафика с Сервером Dr.Web. 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 Dr.Web.

  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` — SplDer Mail,
  - `spider-g3` — SplDer Guard,
  - `outlook-plugin` — Dr.Web для Microsoft Outlook,
  - `firewall` — Брандмауэр Dr.Web,
  - `spider-gate` — SplDer Gate,
  - `parental-control` — Офисный контроль,
  - `antispam-outlook` — Антиспам Dr.Web для компонента Dr.Web для Microsoft Outlook,
  - `antispam-spidermail` — Антиспам Dr.Web для компонента SplDer Mail.

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

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

- `/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 следующие значения:
  - `change` — изменить список установленных компонентов продукта;
  - `remove` — удалить установленный продукт;
  - `recovery` — восстановить установленный продукт, если некоторые его компоненты были повреждены.

  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 сертификата Сервера Dr.Web.

  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 Dr.Web для доступа к Серверу Dr.Web.

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

- `/regagent` <*режим*> — определяет, будет ли зарегистрирован Агент Dr.Web в списке установленных программ. Параметр <*режим*> может принимать следующие значения:
  - `yes` — зарегистрировать Агент Dr.Web в списке установленных программ.
  - `no` — не регистрировать Агент Dr.Web в списке установленных программ.

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

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

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

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

  Если ключ не задан, по умолчанию осуществляется поиск Сервера Dr.Web 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 Dr.Web 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 Dr.Web. Задается в секундах. Прием ответных сообщений продолжается, пока время ожидания ответа не превышает значение тайм-аута.

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

## Ж2. 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. Короткие ключи могут принимать значения без разделительного пробела, например:

```
es-service -e192.168.1.1:12345
```

---

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

**Допустимые ключи:**

- Показать справку:
  - `-?`
  - `--help`
- Изменить адрес Сервера Dr.Web, к которому подключается Агент Dr.Web:
  - `-e <Сервер Dr.Web>`
  - `--esserver=<Сервер Dr.Web>`

  Чтобы задать сразу несколько Серверов Dr.Web, необходимо повторить через пробел ключ для каждого адреса Сервера Dr.Web, 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 Dr.Web (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 Dr.Web и хранятся в реестре), остаются и продолжают использоваться.

- Добавить сертификат Сервера Dr.Web:
  - `-c <`*сертификат*`>`
  - `--addcert=<`*сертификат*`>`

  Файл сертификата Сервера Dr.Web, указанный в качестве аргумента, копируется в каталог Агента Dr.Web (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 Dr.Web 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 Dr.Web будут сбрасываться, в результате чего Агент Dr.Web 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 Dr.Web на Сервере будут сброшены, после чего произойдет однократное подключение Агента Dr.Web к Серверу в качестве новичка.
- Изменить уровень детализации журнала Агента Dr.Web:
  - `--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.

## Ж3. Сервер Dr.Web

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

Ряд команд требует наличия в командной строке обязательных ключей `modexec` или `modexecdb` для исполнения Lua-модулей и, при необходимости, передачи набора вспомогательных параметров. Команда в этом случае строится следующим образом:

`drwcsd [<ключи>] modexec [<имя_функции>@]<название_модуля> [<параметры>]`

- *<имя_функции>* — имя конкретной функции, которую нужно исполнить в Lua-модуле.
- *<название_модуля>* — название исполняемого Lua-модуля.

Команды, приведенные в пп. Ж3.1. Управление Сервером Dr.Web — Ж3.5. 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 Dr.Web обратитесь к файлу журнала Сервера Dr.Web для поиска возможных причин (см. **Руководство администратора**, п. Журнал Сервера Dr.Web).

## Ж3.1. Управление Сервером Dr.Web

`drwcsd [<ключи>]` — задать настройки работы Сервера Dr.Web (ключи подробнее описываются в Приложении Ж3.8).

По умолчанию в ОС Windows файл `drwcsd.exe` расположен в каталоге `C:\Program Files\DrWeb Server\bin`.

В ОС Linux и FreeBSD рекомендуется использовать скрипты, по умолчанию расположенные в следующих каталогах:

- Linux: `/etc/init.d/drwcsd`
- FreeBSD: `/usr/local/etc/rc.d/drwcsd`

## Ж3.2. Базовые команды

- `drwcsd restart` — сделать полный перезапуск службы Сервера Dr.Web (выполняется как пара `stop` и затем `start`).
- `drwcsd start` — запустить Сервер Dr.Web.
- `drwcsd stop` — нормально завершить работу Сервера Dr.Web.
- `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 modexec agent@verify-key` *<полное_имя_файла_ключа>* — проверка корректности файла лицензионного ключа (`agent.key`).
- `drwcsd modexec enterprise@verify-key` *<полное_имя_файла_ключа>* — проверка корректности файла лицензионного ключа Сервера Dr.Web

(`enterprise.key`). Обратите внимание, лицензионный ключ Сервера Dr.Web более не используется, начиная с версии 10.

- `drwcsd verifyconfig` *<полное_имя_файла_конфигурации>* — проверка синтаксиса конфигурационного файла Сервера Dr.Web (`drwcsd.conf`).
- `drwcsd verifycache` — проверка корректности содержимого файлового кеша Сервера Dr.Web.
- `drwcsd syncads` — синхронизировать структуру сети: контейнеры Active Directory, содержащие компьютеры, становятся группами антивирусной сети, в которые помещаются рабочие станции.
- `drwcsd modexec restore@repository-server-update` — восстановить Сервер Dr.Web из ревизии (откатить к состоянию текущей ревизии без сохранения резервной копии, обновления базы данных и конфигурационных файлов. При отсутствии данной ревизии в репозитории восстановление невозможно.

Данное действие записывается в журнал аудита.

- `update@repository-server-update [<revision-to>]` — обновление Сервера Dr.Web. Если не указана ревизия, до которой следует обновиться, сервер будет обновлен до самой последней ревизии.
- `revert@repository-server-update <revision-to>` — откат Сервера Dr.Web к определенной ревизии.

Последние два действия записываются в журнал аудита.

Обновление и откат Сервера Dr.Web описаны в документации администратора, разделе Обновление Сервера Dr.Web и восстановление из резервной копии.

## Ж3.3. Команды для управления базой данных

### Инициализация базы данных

При инициализации база данных должна отсутствовать или быть пуста.

Значения для флагов должны быть указаны в формате `%true` и `%false`, либо `1` и `0`.

`drwcsd [<ключи>] modexecdb database-init [<лицензионный_ключ> [<пароль>]]` — 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 Dr.Web.
- *<пароль>* — начальный пароль администратора Сервера Dr.Web (имя **admin**). По умолчанию **root**.

> Если требуется пропустить один или несколько параметров при написании команды, вместо каждого из них следует использовать специальное значение `%nil`.
>
> `%nil` 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 modexecdb database-init@`*<response-file>*

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

Формат файла:

```
<полное_имя_файла_лицензионного_ключа>

<пароль_администратора>
```

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

Если в строке указано значение `%nil`, будет использоваться значение по умолчанию (как в `database-init`).

### Обновление версии базы данных

`drwcsd modexecdb database-upgrade [pretend] [upgrade_ver_flag]` — запустить Сервер Dr.Web для обновления структуры базы данных при переходе на новую версию через внутренние скрипты.

- `pretend=%false` — значение по умолчанию. Предписывает обновить базу данных. Если указать значение `%true`, будет выполняться только проверка актуальности базы данных вместо фактического ее обновления.

- `upgrade_ver_flag=%true` — если указано значение `%true`, во время обновления версия базы данных и данные в базе фиксируются при каждом успешном обновлении до следующей версии схемы базы. Значение по умолчанию — `%false`.

Вместо значений параметров `%true` или `%false` допускается использовать равнозначные им 1 или 0.

## Экспорт базы данных

a) `drwcsd modexecdb database-export` <*файл*> `[ignore_tables]` — экспорт базы данных в указанный файл.

- <*файл*> — путь к файлу, в который будет выполнен экспорт базы данных.
- `ignore_tables` — позволяет указать строку или таблицу строк с названиями таблиц базы данных, которые не подлежат экспорту. Формат таблиц строк выглядит следующим образом: `%{"table1","table2"}`. В случае указания строки — `table1`.

**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=trace -log="C:\Program Files\DrWeb Server\var\exportdb.log"
modexecdb database-export "C:\Program Files\DrWeb Server\esbase.es"
alert_unsent
```

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 modexecdb database-export-xml` <*xml-файл*> `[ignore_tables]` — экспорт базы данных в указанный XML-файл.

- <*xml-файл*> — путь к XML-файлу, в который будет выполнен экспорт базы данных.
- `ignore_tables` — позволяет указать строку или таблицу строк с названиями таблиц базы данных, которые не подлежат экспорту. Формат таблиц строк выглядит следующим образом: `%{"table1","table2"}`. В случае указания строки — `table1`.

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=trace -rotate=10,10m -
log="C:\Program Files\DrWeb Server\var\exportxmldb.log" modexecdb
database-export-xml 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=trace -rotate=10,10m -
log="C:\Program Files\DrWeb Server\var\exportxmldb.log" modexecdb
database-export-xml database.gz
```

**Пример для ОС семейства UNIX**:

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

```
/etc/init.d/drwcsd modexecdb database-export-xml /es/database.db
```

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

```
/etc/init.d/drwcsd modexecdb database-export-xml /es/database.gz
```

### Импорт базы данных

a) `drwcsd modexecdb database-import` <*файл*> `[ignore_tables]` — импорт базы данных из указанного файла. При этом удаляются все записи из всех таблиц, сами же таблицы не удаляются - в них переносятся записи из экспорта.

- <*файл*> — путь к файлу, из которого будет выполнен импорт базы данных.
- `ignore_tables` — позволяет указать строку или таблицу строк с названиями таблиц базы данных, которые не подлежат импорту. Формат таблиц строк выглядит следующим образом: `%{"table1","table2"}`. В случае указания строки — `table1`.

b) `drwcsd modexecdb database-import-and-upgrade` <*файл*> `[import_only_flag] [upgrade_ver_flag] [ignore_tables]` — импорт и обновление базы данных, полученной при экспорте с Сервера Dr.Web предыдущих версий. При этом удаляются сами таблицы, новые таблицы создаются по описанию из экспорта. В них переносятся записи из экспорта, после чего запускается процедура обновления.

- <*файл*> — путь к файлу, из которого будет выполнен импорт базы данных.
- `import_only_flag` — если указано значение `%true`, обновление и верификация базы данных производиться не будут, будет осуществлен только импорт. Значение по умолчанию — `%false`.
- `upgrade_ver_flag` — если указано значение `%true`, во время обновления базы версия базы данных и данные в ней фиксируются при каждом успешном обновлении до следующей версии схемы базы. Значение по умолчанию — `%false`.

- `ignore_tables` — позволяет указать строку или таблицу строк с названиями таблиц базы данных, которые не подлежат импорту. Формат таблиц строк выглядит следующим образом: `%{"table1","table2"}`. В случае указания строки — `table1`.

При указании параметров, предыдущие должны быть обязательно выставлены, например: при указании `ignore_tables` параметры `import_only_flag` и `upgrade_ver_flag` должны быть обязательно выставлены (то есть оба флага должны быть указаны перед `ignore_tables`).

Перед использованием команды `database-import-and-upgrade` необходимо выполнить резервное копирование базы данных.

Любые проблемы в процессе выполнения данной команды могут привести к удалению всей информации из базы данных.

---

Использование команды `database-import-and-upgrade` для импорта с обновлением версии базы данных возможно только в пределах одной БД.

## Проверка базы данных

`drwcsd modexecdb database-verify [full [ignore-version]]` — запустить Сервер Dr.Web для проверки базы данных и восстановления недостающей информации. Для записи информации о результатах в файл журнала следует вводить команду с ключом `-log`. Подробно особенности использования данного ключа описаны в п. Ж3.8. Описание ключей.

- `full=%false` — определяет режим проверки. При значении по умолчанию (`%false`) выполняется быстрая проверка, при значении `%true` — полная.
- `ignore-version=%false` — определяет, нужно ли игнорировать версию схемы базы данных при проверке. По умолчанию `%false`. Если указано значение `%true`, проверка продолжится даже в случае неправильной версии схемы.

### Пример

- При выполнении данной команды будет выполнена полная проверка базы данных даже в случае неправильной версии схемы базы данных.

```
drwcsd modexecdb database-verify %true %true
```

Проверку базы данных нельзя проводить на запущенном Сервере Dr.Web.

### Ускорение базы данных

`drwcsd [<ключи>] modexecdb database-speedup` — выполнить команды `VACUUM`, `CLUSTER`, `ANALYZE` для ускорения работы с базой данных.

### 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 Dr.Web, если в настройках базы данных **SQLite3** в Центре управления установлен флаг **Восстанавливать поврежденный образ автоматически** (см. **Руководство администратора**, п. Восстановление баз данных).

### Очистка базы данных

`drwcsd modexecdb database-clean` — очистить базу данных Сервера Dr.Web, удалив все таблицы.

### Смена пароля администратора

`drwcsd modexecdb set-admin-password <регистрационное_имя> <новый_пароль>` — задать новый пароль для указанной учетной записи администратора.

## Ж3.4. Команды для управления репозиторием

Перед запуском команд `syncrepository`, `restorerepo` и `saverepo` необходимо обязательно завершить работу Сервера Dr.Web.

- `drwcsd syncrepository` — произвести синхронизацию репозитория с ВСО Dr.Web. Команда запускает процесс Сервера Dr.Web, 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 Dr.Web для обращения к ВСО и последующего обновления репозитория в случае наличия обновлений. Если Сервер Dr.Web не запущен, обновление репозитория не осуществляется.
- `drwcsd [<ключи>] restorerepo <полное_имя_архива>` — восстановить репозиторий Сервера Dr.Web из заданного zip-архива, созданного при помощи команды `saverepo`.

- `drwcsd [<ключи>] saverepo <полное_имя_архива>` — сохранить весь репозиторий Сервера Dr.Web в указанный zip-архив. Полученный архив может быть импортирован на Сервер Dr.Web при помощи команды `restorerepo`.

Архивы, используемые командами `restorerepo` и `saverepo`, не совместимы с архивами, используемыми для экспорта и импорта репозитория через Центр управления.

## Ж3.5. Резервное копирование критичных данных Сервера Dr.Web

Резервная копия критичных данных Сервера Dr.Web (лицензионных ключей, содержимого базы данных, закрытого ключа шифрования, конфигурации Сервера Dr.Web и Центра управления) создается с помощью следующей команды:

- в ОС Windows: `drwcsd -home=<путь> backup [<каталог> [<количество>]]`
- в ОС Linux, FreeBSD: `drwcsd backup [<каталог> [<количество>]]`

где:

- ключ `-home` задает каталог установки Сервера Dr.Web,
- критичные данные Сервера Dr.Web копируются в указанный *<каталог>*,
- параметр *<количество>* — количество сохраняемых копий одного и того же файла.

**Пример для ОС Windows:**

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -verbosity=all -log="C:\Program Files\DrWeb Server\var\backup.log" backup "C:\DrWeb Backup"
```

**Пример для ОС Linux:**

```
/etc/init.d/drwcsd backup /tmp/backup/ -verbosity=all -log=/tmp/backup/backup.log
```

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 Dr.Web и таким образом восстановить данные (см. п. Восстановление базы данных).

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 Dr.Web включено ежедневное задание. Если такое задание в расписании отсутствует, рекомендуется создать его.

## Ж3.6. Команды, доступные только под ОС Windows

- `drwcsd [<ключи>] install [<имя_сервиса>]` — установить службу Сервера Dr.Web 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 Dr.Web 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 Dr.Web (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 Dr.Web при запуске команды, заданной в параметре *<команда>*. Используется в частности в командных файлах для отключения интерактивности работы Сервера Dr.Web.

## Ж3.7. Команды, доступные только под ОС семейства UNIX

- `drwcsd cacherepo` — создать или восстановить файловый кеш репозитория Сервера Dr.Web.
- `drwcsd config` — аналог команды `reconfigure` или `kill SIGHUP` — перезапуск Сервера Dr.Web.
- `drwcsd interactive` — запускает Сервер Dr.Web, 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 Dr.Web, 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 Dr.Web (запущен, остановлен).

## Ж3.8. Описание ключей

Ключи, описанные в этом разделе, допускают две равнозначные формы записи: с одним дефисом (`-<ключ>`) или двумя (`--<ключ>`).

**Кроссплатформенные ключи:**

- `-activation-key=<лицензионный_ключ>` — лицензионный ключ Сервера Dr.Web. По умолчанию файл `enterprise.key`, расположенный в подкаталоге `etc` корневого каталога.

  Обратите внимание, лицензионный ключ Сервера Dr.Web более не используется, начиная с версии 10. Ключ `-activation-key` может использоваться при обновлении Сервера Dr.Web с предыдущих версий и при инициализации базы данных: идентификатор Сервера Dr.Web 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 Dr.Web. 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 Dr.Web 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 modexecdb database-verify`, см. выше.
- `-help` — выдать справку. Аналогично описанным выше программам.
- `-hooks` — разрешить выполнение Сервером Dr.Web пользовательских скриптов расширения, находящихся в следующем подкаталоге каталога установки Сервера Dr.Web:
  - для ОС Windows: `var\extensions`
  - для ОС FreeBSD: `/var/drwcs/extensions`
  - для ОС Linux: `/var/opt/drwcs/extensions`

Скрипты предназначены для автоматизации работы администратора, упрощая и ускоряя выполнение некоторых заданий. Все скрипты по умолчанию отключены.

- `-home=<каталог>` — каталог установки Сервера Dr.Web (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 Dr.Web в файл по указанному пути.

  Для Сервера Dr.Web на платформах UNIX вместо имени файла может использоваться "минус", что означает выводить журнал на стандартный вывод. Операции на платформах UNIX выполняются от имени пользователя drwcs, и если у него нет прав на запись в каталог файла журнала, то возникнет ошибка.

  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 Dr.Web. По умолчанию `drwcsd.pri` в подкаталоге `etc` корневого каталога.
- `-rotate=<N><f>,<M><u>` — режим ротации журнала работы Сервера Dr.Web, где:

| Параметр | Описание |
|---|---|
| <*N*> | Общее количество файлов журнала (включая текущий и архивные). |
| <*f*> | Формат хранения файлов журнала, возможные значения:<br>• z (gzip) — сжимать файлы, используется по умолчанию,<br>• p (plain) — не сжимать файлы. |
| <*M*> | Размер файла журнала либо время ротации, в зависимости от значения <*u*>; |
| <*u*> | Единица измерения, возможные значения:<br>• для задания ротации по размеру файла журнала:<br>  ▫ k — Кб,<br>  ▫ m — Мб,<br>  ▫ g — Гб.<br>• для задания ротации по времени:<br>  ▫ H — часы,<br>  ▫ D — дни,<br>  ▫ 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.

Минимальный размер файла журнала — 1 МБ.

По умолчанию `10z,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.

Ключи `-rotate` и `-log` позиционно-зависимы.

При использовании этих ключей одновременно ключ `-rotate` должен идти перед ключом `-log`: ключ `-rotate` определяет режим ротации журналов, расположенных по путям, следующим далее в командной строке.

- `-trace` — детально протоколировать место возникновения ошибки.
- `-var-root=`<*каталог*> — путь к каталогу, в который Сервер Dr.Web 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 К. 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 Dr.Web. *<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 Dr.Web, 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 Dr.Web.
- `-pid=<`*файл*`>` — файл, в который Сервер Dr.Web 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 Dr.Web с ключом `-syslog` (например, `service drwcsd start -syslog=user`), Сервер Dr.Web 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).

## Ж3.9. Переменные, доступные под ОС семейства UNIX

Для облегчения управления Сервером Dr.Web под ОС семейства UNIX администратору предоставляются переменные, которые располагаются в файле скрипта:

- 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 ниже.

**Ключи командной строки для drwcsd и соответствующие переменные**

| Ключ | Переменная | Параметры по умолчанию |
|---|---|---|
| `-home` | DRWCS_HOME | • `/usr/local/drwcs` — для ОС FreeBSD,<br>• `/opt/drwcs` — для ОС Linux. |
| `-var-root` | DRWCS_VAR | • `/var/drwcs` — для ОС FreeBSD,<br>• `/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 ниже.

**Переменные без соответствий ключам командной строки**

| 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 Dr.Web. |
| DRWCS_BIN | `$DRWCS_HOME/bin` | Директория, из которой будет запускаться `drwcsd`. |
| DRWCS_LIB | `$DRWCS_HOME/lib` | Директория с библиотеками Сервера Dr.Web. |

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.

## Ж3.10. Управление Сервером Dr.Web под ОС семейства UNIX при помощи команды kill

Сервер Dr.Web под ОС UNIX управляется сигналами, посылаемыми процессу Сервера Dr.Web 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 Dr.Web,
- `SIGTERM` — завершение работы Сервера Dr.Web,
- `SIGQUIT` — завершение работы Сервера Dr.Web,
- `SIGINT` — завершение работы Сервера Dr.Web.

Аналогичные действия для Сервера Dr.Web под ОС Windows реализуются при помощи ключей команды drwcsd, см. Приложение Ж3.3. Команды для управления базой данных.

## Ж4. Сканер Dr.Web для Windows

Данный компонент ПО рабочей станции имеет параметры командной строки, описанные в **Руководстве пользователя Агента Dr.Web для Windows**. Единственное отличие состоит в том, что при запуске Сканера Агентом Dr.Web параметры `/go /st` передаются Сканеру автоматически и в обязательном порядке.

## Ж5. 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:<br>• z (gzip) — сжимать файлы, используется по умолчанию,<br>• p (plain) — не сжимать файлы. |
| <*M*> | Размер файла журнала либо время ротации, в зависимости от значения <*u*>; |
| <*u*> | Единица измерения, возможные значения:<br>• для задания ротации по размеру файла журнала:<br>  ▫ k — Кб,<br>  ▫ m — Мб,<br>  ▫ g — Гб.<br>• для задания ротации по времени:<br>  ▫ H — часы,<br>  ▫ D — дни,<br>  ▫ 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 К. 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 Сервера Dr.Web в кеш Прокси-сервера.

- <*путь*> — путь к каталогу с репозиторием Сервера Dr.Web. Репозиторий Сервера Dr.Web 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 Dr.Web под ОС семейства UNIX администратору предоставляются переменные, которые располагаются в файле скрипта `drwcsd-proxy.sh`, выполняемого с помощью скриптов инициализации:

- **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 Сервера Dr.Web 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 ниже.

**Ключи командной строки для drwcsd-proxy и соответствующие переменные**

| Ключ | Переменная | Параметры по умолчанию |
|---|---|---|
| `--home=<путь>` | `$DRWCS_PROXY_HOME` | `$exe-dir/` |
| `--var-root=<путь>` | `$DRWCS_PROXY_VAR` | • ОС Linux: `/var/opt/drwcs`<br>• ОС FreeBSD: `/var/drwcs` |
| `--etc-root=<путь>` | `$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` | `$DRWCS_PROXY_USER` | – |
| – | `$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. |

## Ж6. 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.
- `--lsm` — вывести содержание встроенной LSM-записи с базовой информацией о пакете: название, версия, описание, автор, и т. д. Если LSM-запись не заполнялась, будет выведено соответствующее сообщение.
- `--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.
- `--keep` — не удалять указанный каталог после выполнения встроенного скрипта.
- `--nox11` — не запускать эмулятор терминала `xterm` по завершении установки.
- `--nochown` — не назначать владельцем извлеченных файлов пользователя, который инициирует установку.
- `--log <`*путь*`>` — вести журнал установки в файле по указанному пути.
- `--nolog` — не вести журнал установки.
- `--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 Dr.Web 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.

# Ж7. Утилиты

## Ж7.1. 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 Dr.Web `webmin/utilities` | |
| `drwsign` | Каталог Сервера Dr.Web `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_Dr.Web>] <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 Dr.Web, и записать его в соответствующий файл.

| Параметр ключа | Значение по умолчанию |
|---|---|
| <*закрытый_ключ*> | `drwcsd.pri` |
| <*поля_субъекта*> | `/CN=`<*имя_хоста*> |
| <*срок_действия*> | `1095` |
| <*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*> |
| <*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>* | `730` |
| *<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_Dr.Web>] [-cert=<сертификат_на_подпись>] [-days=<срок_действия>] [-eku=<предназначение>] [<подписанный_сертификат>]`

  Подписать готовый *<сертификат_на_подпись>* закрытым ключом и сертификатом Сервера Dr.Web. Подписанный сертификат сохраняется в отдельном файле.

  Может быть использовано для подписывания сертификата Прокси-сервера Dr.Web ключом Сервера Dr.Web.

  Возможны следующие значения ключа `-eku` (расширение Extended Key Usage):

  - `drwebServerAuth` — аутентификация Сервера/Прокси-сервера Агентом Dr.Web,
  - `drwebMeshDAuth` — аутентификация Сканирующего сервера Виртуальным агентом.

| Параметр ключа | Значение по умолчанию |
|---|---|
| *<закрытый_ключ>* | `drwcsd.pri` |
| *<сертификат_Сервера_Dr.Web>* | `drwcsd-ca-cerificate.pem` |
| *<сертификат_на_подпись>* | `drwcsd-certificate.pem` |
| *<срок_действия>* | `365` |
| *<предназначение>* | `drwebServerAuth` |
| *<подписанный_сертификат>* | `drwcsd-signed-certificate.pem` |

- `drwsign signcsr [-ca-key=<закрытый_ключ>] [-ca-cert=<сертификат_Сервера_Dr.Web>] [-csr=<запрос_на_подпись_сертификата>] [-days=<срок_действия>] [-eku=<предназначение>] [<подписанный_сертификат>]`

  Подписать *<запрос_на_подпись_сертификата>*, сгенерированный при помощи команды `gencsr`, закрытым ключом и сертификатом Сервера Dr.Web. 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.

  Возможны следующие значения ключа `-eku` (расширение Extended Key Usage):

  - `drwebServerAuth` — аутентификация Сервера/Прокси-сервера Агентом Dr.Web,
  - `drwebMeshDAuth` — аутентификация Сканирующего сервера Виртуальным агентом.

| Параметр ключа | Значение по умолчанию |
|---|---|
| *<закрытый_ключ>* | `drwcsd.pri` |
| *<сертификат_Сервера_Dr.Web>* | `drwcsd-cerificate.pem` |
| *<запрос_на_подпись_сертификата>* | `drwcsd-certificate-sign-request.pem` |

| Параметр ключа | Значение по умолчанию |
|---|---|
| <*срок_действия*> | 365 |
| <*предназначение*> | drwebServerAuth |
| <*подписанный_сертификат*> | drwcsd-signed-certificate.pem |

- `drwsign tlsticketkey [<`*TLS-тикет*`>]`

  Сгенерировать TLS-тикеты.

  Может быть использовано в кластере Серверов Dr.Web для общих TLS-сессий.

| Параметр ключа | Значение по умолчанию |
|---|---|
| <*TLS-тикет*> | tickets-key.bin |

- `drwsign verify [-ss-cert] [-CAfile=<`*сертификат_Сервера_Dr.Web*`>] [<`*сертификат_на_проверку*`>]`

  Проверить валидность сертификата по доверенному сертификату Сервера Dr.Web.

  Ключ `-ss-cert` предписывает игнорировать доверенный сертификат и только проверить корректность самоподписанного сертификата.

| Параметр ключа | Значение по умолчанию |
|---|---|
| <*сертификат_Сервера_Dr.Web*> | 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 |

- `drwsign version`

  Вывести информацию о версии утилиты.

## Ж7.2. Утилита администрирования встроенной базы данных

Для администрирования встроенной БД (SQLite3) предоставляется утилита `drwidbsh3`.

Утилита расположена в следующих директориях:

- для ОС **Linux**: `/opt/drwcs/bin`
- для ОС **FreeBSD**: `/usr/local/drwcs/bin`
- для ОС **Windows**: <*каталог_установки_Сервера_Dr.Web*>`\bin`

(по умолчанию каталог установки Сервера Dr.Web: `C:\Program Files\DrWeb Server`).

**Формат команды запуска:**

`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.

## Ж7.3. 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 Dr.Web `webmin/utilities` | |
| `drwcntl` | Каталог Сервера Dr.Web `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 Dr.Web

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 Dr.Web необходимо, чтобы для администратора, который подключается через утилиту, было разрешено право **Использование дополнительных возможностей**. В противном случае доступ к Серверу Dr.Web 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 Dr.Web: `ssl://`<*IP-адрес или DNS-имя*>.

Описание настроек Сервера Dr.Web 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 Dr.Web, 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 Dr.Web не заданы параметры подключения, используются следующие значения:

| Параметр | Значение по умолчанию |
|---|---|
| Протокол подключения | `tcp`<br>  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`. |
| IP-адрес или DNS-имя Сервера Dr.Web | Утилита запросит ввести адрес Сервера Dr.Web в соответствующем формате. |
| Порт | `10101`<br>  На стороне Сервера Dr.Web 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 Dr.Web.
- <*пароль*> — пароль администратора для доступа к Серверу Dr.Web.

  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 Dr.Web. 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 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 Dr.Web. 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 Dr.Web.
    - `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 Dr.Web.
- `cpu` <*параметр*> — показать статистику использования CPU компьютера, на котором установлен Сервер Dr.Web. 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 Dr.Web под ОС семейства UNIX.

- `die` — завершить работу Сервера Dr.Web и записать дамп процесса Сервера Dr.Web.

Команда `die` доступна только для Серверов Dr.Web под ОС семейства UNIX.

- `dwcp` <*параметр*> — установить/посмотреть настройки Dr.Web Control Protocol (включает журналы Сервера Dr.Web, Агентов Dr.Web и инсталляторов Агентов Dr.Web). 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 Dr.Web. 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 Dr.Web или установить/посмотреть уровень детализации журнала. В зависимости от заданных параметров выполняются следующие действия:
  - `log` <*строка*> — записать в журнал Сервера Dr.Web 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 Dr.Web 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 Dr.Web. 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 Dr.Web под ОС Windows, ОС семейства Linux и ОС семейства FreeBSD. При этом действуют следующие ограничения на дополнительные параметры команды `memory`:
  - `system` — только для Серверов Dr.Web под ОС Windows, ОС семейства Linux,
  - `heap` — только для Серверов Dr.Web под ОС Windows, ОС семейства Linux,
  - `malloc` — только для Серверов Dr.Web под ОС семейства Linux и ОС семейства FreeBSD,
  - `sizes` — только для Серверов Dr.Web 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 Dr.Web. Допустимые команды:
  - `disable` — отключить мониторинг,
  - `enable` — включить мониторинг,
  - `show` — показать текущий режим.

- `printstat` — записать статистику работы Сервера Dr.Web 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 Dr.Web.
- `show` <*параметр*> — показать информацию о системе, на которой установлен Сервер Dr.Web. 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 Dr.Web под ОС Windows, ОС семейства Linux,
  - `mapping` — только для Серверов Dr.Web под ОС Windows, ОС семейства Linux,
  - `limits` — только для Серверов Dr.Web под ОС семейства UNIX,
  - `processors` — только для Серверов Dr.Web под ОС семейства Linux.
- `sql` <*запрос*> — выполнить заданный SQL-запрос.
- `stop` — завершить работу Сервера Dr.Web.
- `traffic` <*параметр*> — показать статистику по сетевому трафику Сервера Dr.Web. Для запроса конкретного параметра используйте следующие команды:
  - `all` — показать весь объем трафика с начала работы Сервера Dr.Web.
  - `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 Dr.Web, осуществляющих обновление в данный момент.
- `agent [<режим>]` — показать/установить режим обновления Агентов Dr.Web с Сервера Dr.Web. При запуске без дополнительных параметров показывает текущий режим. Для установки режима используйте следующие дополнительные ключи:
  - `on` — включить обновления Агентов Dr.Web.
  - `off` — отключить обновления Агентов Dr.Web.
- `gus` — запустить обновление репозитория с ВСО вне зависимости от состояния процесса обновления с ВСО.
- `http [<режим>]` — показать/установить режим обновлений репозитория Сервера Dr.Web 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 Dr.Web, которые не осуществляют обновление в данный момент.
- `track [<режим>]` — показать/установить режим отслеживания обновлений Агентов Dr.Web. При запуске без дополнительных параметров показывает текущий режим. Для установки режима используйте следующие дополнительные команды:
  - `on` — включить отслеживание обновлений Агентов Dr.Web.
  - `off` — отключить отслеживание обновлений Агентов Dr.Web. При этом ключ `update active` не будет выводить список обновляемых Агентов Dr.Web.

- `version` — вывести информацию о версии утилиты.

## Ж7.4. 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 Dr.Web `webmin/utilities` | |

| Исполняемый файл | Расположение | Описание |
|---|---|---|
| `drwcmd` | Каталог Сервера Dr.Web `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 Dr.Web 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 Dr.Web необходимо, чтобы для администратора, который подключается через утилиту, было разрешено право **Использование дополнительных возможностей**. В противном случае доступ к Серверу Dr.Web через утилиту дистанционной диагностики будет запрещен.

Описание настроек Сервера Dr.Web 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 Ж. 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 журнал 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 Dr.Web после выполнения последней команды до завершения процесса утилиты. По умолчанию `no`.

- `--output=<`*файл*`>` — файл для вывода ответов Сервера Dr.Web. 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 Dr.Web. Может быть определен в файле, заданном в ключе `--resource`.

- `--read=yes|no` — разрешить чтение параметров подключения к Серверу Dr.Web из ресурсного файла. По умолчанию `yes`.

- `--resource=<`*файл*`>` — ресурсный файл с параметрами подключения к Серверу Dr.Web: адресом Сервера Dr.Web и регистрационными данными администратора для авторизации на Сервере Dr.Web. 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_Dr.Web>* *<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 Dr.Web, указанному в ключе `--server`, по регистрационным данным из ресурсного файла, соответствующим адресу этого Сервера Dr.Web.

- `--server=<`*Сервер_Dr.Web*`>` — адрес Сервера Dr.Web. По умолчанию `ssl://127.0.0.1`. Может быть определен в файле, заданном в ключе `--resource`.

- `--user=<`*пользователь*`>` — имя пользователя для авторизации на Сервере Dr.Web. Может быть определено в файле, заданном в ключе `--resource`.

- `--verbose=yes|no` — выводить подробный ответа Сервера Dr.Web (стандартный поток вывода `stdout`). По умолчанию `no`.
- `--version` — вывести информацию о версии утилиты.

**Процедура подключения к Серверу Dr.Web:**

1. При определении данных подключения к Серверу Dr.Web 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 Dr.Web 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 Dr.Web 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 Dr.Web.
- 4 — ошибка авторизации на Сервере Dr.Web: неверные имя и/или пароль администратора.
- 5 — аварийный разрыв соединения с Сервером Dr.Web.
- 127 — неопределенная фатальная ошибка.

## Ж7.5. 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 Dr.Web `webmin/utilities` | |
| `drwreploader` | Каталог Сервера Dr.Web `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

Значения ключей можно указывать через пробел или знак «=».

- `--archive` — упаковать репозиторий в архив.
- `--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.
- `--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 Dr.Web. Загруженные файлы могут быть непосредственно импортированы через Центр управления в качестве обновления репозитория Сервера Dr.Web. 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 Dr.Web 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.
- `--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>` — загрузить указанный продукт. Для загрузки нескольких продуктов укажите несколько пар «ключ — значение» подряд, например: `--product=20-drwcs --product=40-drwproxy`, или несколько значений ключа через запятую, например: `--product 20-drwcs,40-drwproxy`. По умолчанию загружается весь репозиторий.

- `--prohibit-cdn` — запретить использовать CDN при загрузке обновлений. По умолчанию использование CDN разрешено.
- `--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 Dr.Web.

  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.
- `--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.
- `--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 следующие значения:
  - для несертифицированных версий продукта — `/update`;
  - для сертифицированных версий продукта — значение параметра **Базовый URI**, указанное в Центре управления в разделе **Администрирование** → **Общая конфигурация репозитория** → **ВСО Dr.Web**.
- `--V` — вывести информацию о версии утилиты.
- `--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 Dr.Web, для которого необходимо загрузить обновления в формате *<мажорная_версия>*`.`*<минорная_версия>*. Например, для Сервера Dr.Web версии 13, параметр *<версия>* принимает значение `13.00`. Состав продуктов, для которых доступны обновления, может различаться в зависимости от версии Сервера Dr.Web. Уточнить состав доступных продуктов можно, например, проверив описание параметра `<products>` для конфигурационного файла Загрузчика репозитория в руководстве к интересующей вас версии.

## 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:<br>• `--cert-mode valid \| drweb \| custom`<br>• `--proto https \| ftps \| smbs` |
| `--ssh-prikey` | Если следующие ключи принимают одно из значений:<br>• `--proto sftp \| scp`<br>• `--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. Загрузить только базы SpIDer Gate и Сервер Dr.Web:

```
drwreploader.exe --path C:\Temp --license-key C:\agent.key --update-key
"C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program Files\DrWeb
Server\etc" --product 10-drwgatedb,20-drwcs
```

3. Загрузить только вирусные базы для создания зеркала обновлений:

```
drwreploader.exe --path C:\Temp --license-key C:\agent.key --update-key
"C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program Files\DrWeb
Server\etc" --mode mirror --only-bases
```

# Ж7.6. Утилита удаленной установки Агента Dr.Web для UNIX

Утилита удаленной установки Агента Dr.Web для UNIX позволяет дистанционно установить Агент Dr. Web на защищаемые станции антивирусной сети, работающие под управлением операционной системы семейства UNIX. При необходимости с помощью данной утилиты можно также установить Dr.Web Server Security Suite (Unix).

Утилита работает в режиме командной строки и доступна в следующих версиях:

| Исполняемый файл | Расположение | Описание |
|---|---|---|
| `drweb-unix-install-<ОС>-<разрядность>` | Центр управления, раздел **Администрирование** → **Утилиты** | Независимая версия утилиты. Может запускаться из произвольного каталога и на любом компьютере с соответствующей операционной системой. Обновляется при обновлении репозитория или Сервера Dr.Web. |
| | Каталог Сервера Dr.Web `webmin/utilities` | |
| `drwunixinstall` | Каталог Сервера Dr.Web `bin` | Версия утилиты зависит от наличия серверных библиотек. Может запускаться только из каталога своего расположения. Обновляется только при обновлении Сервера Dr.Web. |

Версии утилиты `drweb-unix-install-<ОС>-<разрядность>` и `drwunixinstall` аналогичны по функциональности. Далее в разделе приводится версия `drwunixinstall`, однако формат и допустимые ключи актуальны для обеих версий.

**Формат команды запуска:**

`drwunixinstall [<ключи>] <IP-адрес_станции_1>[:<порт_SSH>[^<имя_пользователя>[^<пароль>]]] <IP-адрес_станции_2>[:<порт_SSH>[^<имя_пользователя>[^<пароль>]]] ...`

## Допустимые ключи

Принцип использования ключей утилитой `drwunixinstall` подчиняется общим правилам, описанным в разделе Приложение Ж. Параметры командной строки программ, входящих в состав Dr.Web Enterprise Security Suite.

- `--help` — вывести справку по ключам.
- `--ak <параметры_авторизации>` — задать параметры альтернативной авторизации на удаленных станциях с использованием ключей шифрования в следующем формате:

```
<имя_пользователя>
^<путь_к_закрытому_ключу_Сервера_Dr.Web>
^<путь_к_открытому_ключу_Сервера_Dr.Web>[^<пароль_закрытого_ключа>]
```

Если при формировании команды задать одновременно параметры стандартной авторизации по паре *<имя_пользователя>*^*<пароль>* и альтернативной авторизации по ключам шифрования, первыми при запуске утилиты будут использоваться параметры с ключами.

- `--ap` *<имя_пользователя>*^*<пароль>* — использовать режим авторизации на удаленных станциях с многократным вводом пароля (keyboard-interactive).
- `--certificate` *<путь>* — задать путь к файлу сертификата Сервера Dr.Web. По умолчанию `webmin/install/unix/workstation/drwcsd-certificate.pem`.
- `--cpus` *<количество>* — задать количество ядер процессора, используемых при удаленной установке. По умолчанию `4`.
- `--ctimeout` *<время>* — задать предельное время ожидания завершения процесса передачи установочных пакетов на удаленные станции. Задается в секундах, по умолчанию `600`.
- `--debug` — вести журнал работы утилиты в отладочном режиме. По умолчанию `no`.
- `--esuite` *<адрес_сервера>* — ввести адрес Сервера Dr.Web, с которого будет производиться удаленная установка и к которому по завершении установки подключится Агент Dr.Web. Формат: `[udp://]`*<IP-адрес или DNS-имя>*`[:`*<порт>*`]`
- `--etimeout` *<время>* — задать предельное время ожидания завершения установки пакетов на удаленных станциях. Задается в секундах, по умолчанию `900`.
- `--from` *<путь>* — задать путь к каталогу с установочными пакетами на Сервере Dr.Web. По умолчанию `webmin/install/unix`.
- `--long` — вести журнал работы утилиты с указанием временных меток. По умолчанию `no`.
- `--pwd` *<пароль>* — пароль для авторизации на удаленных станциях при использовании команды `su` и/или `sudo`.
- `--remote-temp` *<путь>* — задать путь к каталогу на удаленных станциях для временного хранения дистрибутива и сертификата Сервера Dr.Web. По умолчанию используется каталог, заданный в системе.
- `--server` — установить продукт Dr.Web Server Security Suite (Unix) вместо Агента Dr.Web. По умолчанию `no`.
- `--simultaneously` *<количество>* — задать максимальное количество станций, на которые будет одновременно устанавливаться Агент Dr.Web.
- `--sshdebug` — вести журнал работы утилиты в отладочном режиме, с указанием деталей по всем операциям, использующим протокол SSH. По умолчанию `no`.

- `--sshwaitdebug` — вести журнал работы утилиты в отладочном режиме, с указанием деталей по всем операциям, использующим протокол SSH, а также таймерным операциям. По умолчанию `no`.
- `--stimeout` <*время*> — задать предельное время ожидания ввода пароля для использования команды `su` и/или `sudo` на удаленных станциях. Задается в секундах, по умолчанию `10`.
- `--su` — использовать команду `su` во время установки для повышения прав до уровня суперпользователя на удаленных станциях. По умолчанию `no`.
- `--sudo` — использовать команду `sudo` во время установки для повышения прав до уровня суперпользователя на удаленных станциях. По умолчанию `no`.
- `--temp` <*путь*> — задать путь к каталогу на Сервере Dr.Web для временного хранения сертификата. По умолчанию используется каталог, заданный в системе.
- `--timeout` <*время*> — задать предельное время ожидания установки соединения и аутентификации на удаленных станциях. Задается в секундах, по умолчанию `30`.
- `--verbosity` <*уровень*> — задать уровень детализации журнала работы утилиты. По умолчанию `info`. Допустимые значения: `all`, `debug3`, `debug2`, `debug1`, `debug`, `trace3`, `trace2`, `trace1`, `trace`, `info`, `notice`, `warning`, `error`, `crit`. Значения `all` и `debug3` — синонимы.
- `--version` — вывести информацию о версии утилиты.

## Ж7.7. Утилита удаленной установки Агента Dr.Web для Windows

Утилита удаленной установки Агента Dr.Web для Windows позволяет дистанционно установить Агент Dr. Web на защищаемые станции антивирусной сети, работающие под управлением операционной системы Windows.

Утилита работает в режиме командной строки и доступна в следующих версиях:

| Исполняемый файл | Расположение | Описание |
|---|---|---|
| `drweb-windows-install-`<*ОС*>`-`<*разрядность*> | Центр управления, раздел **Администрирование** → **Утилиты** | Независимая версия утилиты. Может запускаться из произвольного каталога и на любом компьютере с соответствующей операционной системой. Обновляется при обновлении репозитория или Сервера Dr.Web. |
| | Каталог Сервера Dr.Web `webmin/utilities` | |
| `drwwindowsinstall` | Каталог Сервера Dr.Web `bin` | Версия утилиты зависит от наличия серверных библиотек. Может запускаться только из каталога своего расположения. Обновляется только при обновлении Сервера Dr.Web. |

Версии утилиты `drweb-windows-install-<ОС>-<разрядность>` и `drwwindowsinstall` аналогичны по функциональности. Далее в разделе приводится версия `drwwindowsinstall`, однако формат и допустимые ключи актуальны для обеих версий.

**Формат команды запуска:**

`drwwindowsinstall <ключи>`

## Допустимые ключи

Принцип использования ключей утилитой `drwwindowsinstall` подчиняется общим правилам, описанным в разделе Приложение Ж. Параметры командной строки программ, входящих в состав Dr.Web Enterprise Security Suite.

- `--help` — вывести справку по ключам.
- `--console=yes|no` — выводить журнал работы утилиты в консоль. По умолчанию `no`.
- `--disable-v1=yes|no` — отключить протокол SMB версии 1 (SMBv1) на время работы утилиты. По умолчанию `no`.
- `--distribution <имя_файла>` — задать вручную имя файла инсталлятора Агента Dr.Web, который будет запускаться на удаленных станциях. По умолчанию `drwinst.exe`.
- `--install-address <IP-адрес_станции>` — ввести адрес удаленной станции, на которую будет установлен Агент Dr.Web. При одновременном указании нескольких станций их адреса следует разделять запятой (`,`) или точкой с запятой (`;`), без пробелов.
- `--install-certificate <путь>` — задать путь к файлу сертификата Сервера Dr.Web.
- `--install-clients <количество>` — задать максимальное количество станций, на которые будет одновременно устанавливаться Агент Dr.Web. По умолчанию `8`.
- `--install-compression <режим>` — установить режим сжатия трафика при соединении Сервера Dr.Web с удаленными станциями: `on` — сжатие включено, `off` — сжатие отключено, `possible` — сжатие возможно. Последнее означает, что режим зависит от настроек на Сервере Dr.Web. По умолчанию `possible`.
- `--install-encryption <режим>` — установить режим шифрования трафика при соединении Сервера Dr.Web с удаленными станциями: `on` — шифрование включено, `off` — шифрование отключено, `possible` — шифрование возможно. Последнее означает, что режим зависит от настроек на Сервере Dr.Web. По умолчанию `possible`.
- `--install-language <код_языка>` — задать язык интерфейса устанавливаемого Агента Dr.Web в виде двухбуквенного кода согласно стандарту ISO 639-1. Если ключ не

задан или Агент Dr.Web на заданном языке не доступен, используется системный язык на удаленной станции.

- `--install-path` <*путь*> — задать путь к каталогу установки Агента Dr.Web на удаленных станциях. По умолчанию `%ProgramFiles%\DrWeb`.
- `--install-register=yes|no` — зарегистрировать Агент Dr.Web в списке установленных программ по завершении установки. По умолчанию `no`.
- `--install-server` <*адрес_сервера*> — ввести адрес Сервера Dr.Web, с которого будет производиться удаленная установка и к которому по завершении установки подключится Агент. Формат: `[udp://]`<*IP-адрес_или_DNS-имя*>`[:`<*порт*>`]`.
- `--install-timeout` <*время*> — задать предельное время ожидания завершения установки Агента Dr.Web на удаленных станциях. Задается в секундах, по умолчанию `300`.
- `--install-user` <*имя_пользователя*>`@`<*домен*>`:`<*пароль*> или <*домен*>`\`<*имя_пользователя*>`:`<*пароль*> — задать имя пользователя и пароль для авторизации на удаленных станциях.
- `--log` <*путь*> — задать путь к файлу журнала работы утилиты. По умолчанию `drwsmb.log` в подкаталоге `var` каталога установки Сервера Dr.Web.
- `--machine` <*название*> — задать название, которое будет присвоено удаленной станции в антивирусной сети Dr.Web Enterprise Security Suite, по завершении установки Агента Dr.Web и подключении к Серверу Dr.Web. По умолчанию используется зарегистрированное в операционной системе имя компьютера.
- `--rotate=`<*N*><*f*>`,`<*M*><*u*> — установить режим ротации журнала работы утилиты. Формат идентичен аналогичному ключу, который используется для управления ротацией журнала Сервера Dr.Web. По умолчанию `10,10m`.
- `--service-id` <*название_в_реестре*> — задать название, которое будет присвоено разделу службы удаленной установки Агента Dr.Web в реестре Windows. По умолчанию `DrWebRsvcRunner`.
- `--service-name` <*отображаемое_имя*> — задать имя службы удаленной установки Агента Dr.Web, отображаемое в оснастке Services. По умолчанию `Dr.Web Remote Runner Service`.
- `--target-root` <*имя_каталога*> — задать имя каталога в общем административном ресурсе на удаленной станции, откуда будет запускаться скопированный с Сервера Dr.Web инсталлятор Агента Dr.Web. По умолчанию `TEMP`.
- `--target-volume` <*имя_ресурса*> — задать имя общего административного ресурса, в котором будут размещаться файлы установки Агента Dr.Web. По умолчанию `ADMIN$`.
- `--threads` <*количество*> — задать количество потоков ввода-вывода в пуле. По умолчанию `2`.
- `--verbosity` <*уровень*> — задать уровень детализации журнала работы утилиты. По умолчанию `trace`. Допустимые значения: `all`, `debug3`, `debug2`, `debug1`, `debug`, `trace3`, `trace2`, `trace1`, `trace`, `info`, `notice`, `warning`, `error`, `crit`. Значения `all` и `debug3` — синонимы.
- `--version` — вывести информацию о версии утилиты.

# Приложение 3. Переменные окружения, экспортируемые Сервером Dr.Web

Для упрощения настройки процессов, запускаемых Сервером Dr.Web по расписанию, требуется информация о размещении каталогов Сервера Dr.Web. С этой целью Сервер Dr.Web 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 Dr.Web, 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 Dr.Web, в противном случае подкаталог `bin` корневого каталога.
- `DRWCSD_VAR` — путь к каталогу, в который Сервер Dr.Web 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 Dr.Web, в противном случае подкаталог `var` корневого каталога.

# Приложение И. 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 https://www.lua.org/manual/5.1/manual.html.

- Регулярные выражения программной библиотеки PCRE.

  Подробное описание синтаксиса библиотеки PCRE доступно на сайте https://www.pcre.org/.

  В данном приложении приведено только краткое описание основных моментов использования регулярных выражений библиотеки PCRE.

## И1. Опции регулярных выражений PCRE

Регулярные выражения применяются как в конфигурационном файле Сервера Dr.Web, так и в Центре управления при задании исключаемых из сканирования объектов в настройках Сканера Dr.Web.

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 https://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.

## И2. 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 (<br>также квантификатор 0 или 1<br>также квантификатор-минимизатор |
| * | 0 или более |
| + | 1 или более<br>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 К. Формат файлов журнала

Файлы журнала Сервера Dr.Web (см. **Руководство администратора**, п. Журнал Сервера Dr.Web) и Агента Dr.Web 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 Л. 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 М. 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/ |
| Base58 | https://github.com/leafo/lua-base58/blob/master/LICENSE | https://github.com/leafo/lua-base58 |
| 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.org/license.html* | https://c-ares.org/ |
| cairo | Mozilla Public License**<br>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/ |
| fontconfig | Custom | https://www.freedesktop.org/wiki/Software/fontconfig/ |
| freetype | GNU General Public License**<br>FreeType Project License (BSD like) | https://freetype.org/ |
| GCC runtime libraries | GNU General Public License** with exception* | https://gcc.gnu.org/ |
| HTMLayout | Custom | https://terrainformatica.com/a-homepage-section/htmlayout/ |
| ICU | https://www.unicode.org/copyright.html#License* | https://icu.unicode.org/home |
| jemalloc | https://github.com/jemalloc/jemalloc/blob/dev/COPYING* | https://github.com/jemalloc/jemalloc |
| jQuery | MIT License** | https://jquery.com/ |

| Сторонняя библиотека | Лицензия | URL проекта |
|---|---|---|
| | GNU General Public License** | |
| JSON | https://github.com/nlohmann/json/blob/develop/LICENSE.MIT | https://github.com/nlohmann/json |
| JSON4Lua | MIT License** | https://github.com/craigmj/json4lua |
| Leaflet | BSD License<br><br>https://github.com/Leaflet/Leaflet/blob/main/LICENSE* | https://leafletjs.com |
| libipeg turbo | https://github.com/libjpeg-turbo/libjpeg-turbo/blob/main/LICENSE.md | https://libjpeg-turbo.org/ |
| 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<br><br>https://github.com/libssh2/libssh2/blob/master/COPYING* | https://libssh2.org/ |
| libxml2 | MIT License** | https://gitlab.gnome.org/GNOME/libxml2/-/wikis/home |
| Linenoise NG | BSD license* | https://github.com/arangodb/linenoise-ng |
| lua | MIT License** | https://www.lua.org/ |
| lua-xmlreader | MIT License** | https://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://github.com/notofonts/noto-fonts/blob/main/LICENSE* | https://fonts.google.com/noto/use |
| OpenLDAP | https://www.openldap.org/software/release/license.html* | https://www.openldap.org |

| Сторонняя библиотека | Лицензия | URL проекта |
|---|---|---|
| OpenSSL | https://openssl-library.org/source/license/index.html* | https://www.openssl.org/ |
| Oracle Instant Client | https://www.oracle.com/downloads/licenses/instant-client-lic.html* | https://www.oracle.com |
| ParaType Free Font | https://www.paratype.ru/eula* | https://www.paratype.ru |
| pcre | https://www.pcre.org/licence.txt* | https://www.pcre.org/ |
| pixman | MIT License** | https://pixman.org/ |
| Prototype JavaScript framework | MIT License** | http://prototypejs.org/assets/2009/8/31/prototype.js |
| quirc | https://github.com/dlbeer/quirc/blob/master/LICENSE | https://github.com/dlbeer/quirc/ |
| QR Code generator | https://github.com/nayuki/QR-Code-generator | https://www.nayuki.io/page/qr-code-generator-library |
| script.aculo.us scriptaculous.js | https://madrobby.github.io/scriptaculous/license/* | http://script.aculo.us/ |
| slt | MIT License** | https://code.google.com/archive/p/slt |
| SQLite | Public Domain<br>https://www.sqlite.org/copyright.html | https://www.sqlite.org/index.html |
| wtl | Common Public License**<br>Microsoft Public License** | https://sourceforge.net/projects/wtl/ |
| zlib | https://www.zlib.net/zlib_license.html* | https://www.zlib.net/ |

* — тексты лицензий приведены далее.

** — тексты базовых лицензий можно найти по следующим адресам:

| Лицензия | Адрес |
|---|---|
| Common Public License | https://opensource.org/license/cpl1-0-txt |
| GNU General Public License | https://www.gnu.org/licenses/gpl-3.0.html |

| Лицензия | Адрес |
|---|---|
| GNU Lesser General Public License | https://www.gnu.org/licenses/lgpl-3.0.html |
| Microsoft Public License | https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff649456(v=pandp.10) |
| MIT License | https://opensource.org/license/mit |
| Mozilla Public License | https://www.mozilla.org/en-US/MPL/2.0/ |
| 3-Clause BSD License | https://opensource.org/license/bsd-3-clause |

## M1. Base58

```
The MIT License (MIT)


Copyright (c) 2015 leaf


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.
```

## M2. 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.
```

## M3. 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.
```

## M4. 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.
```

## M5. 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.
```

## M6. 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.
```

## M7. 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.
```

```
--------------------------------------------------------------------------------
```

## M8. JSON

```
MIT License


Copyright (c) 2013-2022 Niels Lohmann


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.
```

## M9. 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.
```

## M10. libjpeg turbo

```
libjpeg-turbo note:  This file has been modified by The libjpeg-turbo
Project

to include only information relevant to libjpeg-turbo, to wordsmith certain

sections, and to remove impolitic language that existed in the libjpeg v8

README.  It is included only for reference.  Please see README.md for

information specific to libjpeg-turbo.



The Independent JPEG Group's JPEG software

==========================================



This distribution contains a release of the Independent JPEG Group's free
JPEG

software.  You are welcome to redistribute this software and to use it for
any

purpose, subject to the conditions under LEGAL ISSUES, below.



This software is the work of Tom Lane, Guido Vollbeding, Philip Gladstone,
```

```
Bill Allombert, Jim Boucher, Lee Crocker, Bob Friesenhahn, Ben Jackson,
Julian Minguillon, Luis Ortiz, George Phillips, Davide Rossi, Ge' Weijers,
and other members of the Independent JPEG Group.

IJG is not affiliated with the ISO/IEC JTC1/SC29/WG1 standards committee
(also known as JPEG, together with ITU-T SG16).



DOCUMENTATION ROADMAP
=====================

This file contains the following sections:

OVERVIEW            General description of JPEG and the IJG software.
LEGAL ISSUES        Copyright, lack of warranty, terms of distribution.
REFERENCES          Where to learn more about JPEG.
ARCHIVE LOCATIONS   Where to find newer versions of this software.
FILE FORMAT WARS    Software *not* to get.
TO DO               Plans for future IJG releases.

Other documentation files in the distribution are:

User documentation:
  usage.txt         Usage instructions for cjpeg, djpeg, jpegtran,
                    rdjpgcom, and wrjpgcom.
  *.1               Unix-style man pages for programs (same info as
usage.txt).
  wizard.txt        Advanced usage instructions for JPEG wizards only.
  change.log        Version-to-version change highlights.
```

```
Programmer and internal documentation:

  libjpeg.txt       How to use the JPEG library in your own programs.

  example.txt       Sample code for calling the JPEG library.

  structure.txt     Overview of the JPEG library's internal structure.

  coderules.txt     Coding style rules --- please read if you contribute
code.


Please read at least usage.txt.  Some information can also be found in the
JPEG

FAQ (Frequently Asked Questions) article.  See ARCHIVE LOCATIONS below to
find

out where to obtain the FAQ article.


If you want to understand how the JPEG code works, we suggest reading one or

more of the REFERENCES, then looking at the documentation files (in roughly

the order listed) before diving into the code.



OVERVIEW

========


This package contains C software to implement JPEG image encoding, decoding,

and transcoding.  JPEG (pronounced "jay-peg") is a standardized compression

method for full-color and grayscale images.  JPEG's strong suit is
compressing

photographic images or other types of images that have smooth color and

brightness transitions between neighboring pixels.  Images with sharp lines
or

other abrupt features may not compress well with JPEG, and a higher JPEG

quality may have to be used to avoid visible compression artifacts with such

images.
```

```
JPEG is lossy, meaning that the output pixels are not necessarily identical
to

the input pixels.  However, on photographic content and other "smooth"
images,

very good compression ratios can be obtained with no visible compression

artifacts, and extremely high compression ratios are possible if you are

willing to sacrifice image quality (by reducing the "quality" setting in the

compressor.)


This software implements JPEG baseline, extended-sequential, and progressive

compression processes.  Provision is made for supporting all variants of
these

processes, although some uncommon parameter settings aren't implemented yet.

We have made no provision for supporting the hierarchical or lossless

processes defined in the standard.


We provide a set of library routines for reading and writing JPEG image
files,

plus two sample applications "cjpeg" and "djpeg", which use the library to

perform conversion between JPEG and some other popular image file formats.

The library is intended to be reused in other applications.


In order to support file conversion and viewing software, we have included

considerable functionality beyond the bare JPEG coding/decoding capability;

for example, the color quantization modules are not strictly part of JPEG

decoding, but they are essential for output to colormapped file formats or

colormapped displays.  These extra functions can be compiled out of the

library if not required for a particular application.
```

```
We have also included "jpegtran", a utility for lossless transcoding between
different JPEG processes, and "rdjpgcom" and "wrjpgcom", two simple
applications for inserting and extracting textual comments in JFIF files.


The emphasis in designing this software has been on achieving portability
and
flexibility, while also making it fast enough to be useful.  In particular,
the software is not intended to be read as a tutorial on JPEG.  (See the
REFERENCES section for introductory material.)  Rather, it is intended to
be reliable, portable, industrial-strength code.  We do not claim to have
achieved that goal in every aspect of the software, but we strive for it.


We welcome the use of this software as a component of commercial products.
No royalty is required, but we do ask for an acknowledgement in product
documentation, as described under LEGAL ISSUES.



LEGAL ISSUES
============


In plain English:


1. We don't promise that this software works.  (But if you find any bugs,
   please let us know!)
2. You can use this software for whatever you want.  You don't have to pay
us.
3. You may not pretend that you wrote this software.  If you use it in a
   program, you must acknowledge somewhere in your documentation that
   you've used the IJG code.
```

```
In legalese:

The authors make NO WARRANTY or representation, either express or implied,
with respect to this software, its quality, accuracy, merchantability, or
fitness for a particular purpose.  This software is provided "AS IS", and
you,
its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2020, Thomas G. Lane, Guido Vollbeding.
All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this
software (or portions thereof) for any purpose, without fee, subject to
these
conditions:
(1) If any part of the source code for this software is distributed, then
this
README file must be included, with this copyright and no-warranty notice
unaltered; and any additions, deletions, or changes to the original files
must be clearly indicated in accompanying documentation.
(2) If only executable code is distributed, then the accompanying
documentation must state that "this software is based in part on the work of
the Independent JPEG Group".
(3) Permission for use of this software is granted only if the user accepts
full responsibility for any undesirable consequences; the authors accept
NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG
code,
```

```
not just to the unmodified library.  If you use our work, you ought to
acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company
name
in advertising or publicity relating to this software or products derived
from
it.  This software may be referred to only as "the Independent JPEG Group's
software".

We specifically permit and encourage the use of this software as the basis
of
commercial products, provided that all warranty or liability claims are
assumed by the product vendor.



REFERENCES
==========

We recommend reading one or more of these references before trying to
understand the innards of the JPEG software.

The best short technical introduction to the JPEG compression algorithm is
        Wallace, Gregory K.  "The JPEG Still Picture Compression Standard",
        Communications of the ACM, April 1991 (vol. 34 no. 4), pp. 30-44.
(Adjacent articles in that issue discuss MPEG motion picture compression,
applications of JPEG, and related topics.)  If you don't have the CACM issue
handy, a PDF file containing a revised version of Wallace's article is
available at http://www.ijg.org/files/Wallace.JPEG.pdf.  The file (actually
a preprint for an article that appeared in IEEE Trans. Consumer Electronics)
```

```
omits the sample images that appeared in CACM, but it includes corrections
and some added material.  Note: the Wallace article is copyright ACM and
IEEE,
and it may not be used for commercial purposes.


A somewhat less technical, more leisurely introduction to JPEG can be found
in
"The Data Compression Book" by Mark Nelson and Jean-loup Gailly, published
by
M&T Books (New York), 2nd ed. 1996, ISBN 1-55851-434-1.  This book provides
good explanations and example C code for a multitude of compression methods
including JPEG.  It is an excellent source if you are comfortable reading C
code but don't know much about data compression in general.  The book's JPEG
sample code is far from industrial-strength, but when you are ready to look
at a full implementation, you've got one here...


The best currently available description of JPEG is the textbook "JPEG Still
Image Data Compression Standard" by William B. Pennebaker and Joan L.
Mitchell, published by Van Nostrand Reinhold, 1993, ISBN 0-442-01272-1.
Price US$59.95, 638 pp.  The book includes the complete text of the ISO JPEG
standards (DIS 10918-1 and draft DIS 10918-2).


The original JPEG standard is divided into two parts, Part 1 being the
actual
specification, while Part 2 covers compliance testing methods.  Part 1 is
titled "Digital Compression and Coding of Continuous-tone Still Images,
Part 1: Requirements and guidelines" and has document numbers ISO/IEC IS
10918-1, ITU-T T.81.  Part 2 is titled "Digital Compression and Coding of
Continuous-tone Still Images, Part 2: Compliance testing" and has document
numbers ISO/IEC IS 10918-2, ITU-T T.83.
```

```
The JPEG standard does not specify all details of an interchangeable file
format.  For the omitted details, we follow the "JFIF" conventions, revision
1.02.  JFIF version 1 has been adopted as ISO/IEC 10918-5 (05/2013) and
Recommendation ITU-T T.871 (05/2011): Information technology - Digital
compression and coding of continuous-tone still images: JPEG File
Interchange
Format (JFIF).  It is available as a free download in PDF file format from
https://www.iso.org/standard/54989.html and http://www.itu.int/rec/T-REC-
T.871.
A PDF file of the older JFIF 1.02 specification is available at
http://www.w3.org/Graphics/JPEG/jfif3.pdf.


The TIFF 6.0 file format specification can be obtained from
http://mirrors.ctan.org/graphics/tiff/TIFF6.ps.gz.  The JPEG incorporation
scheme found in the TIFF 6.0 spec of 3-June-92 has a number of serious
problems.  IJG does not recommend use of the TIFF 6.0 design (TIFF
Compression
tag 6).  Instead, we recommend the JPEG design proposed by TIFF Technical
Note
#2 (Compression tag 7).  Copies of this Note can be obtained from
http://www.ijg.org/files/.  It is expected that the next revision
of the TIFF spec will replace the 6.0 JPEG design with the Note's design.
Although IJG's own code does not support TIFF/JPEG, the free libtiff library
uses our library to implement TIFF/JPEG per the Note.



ARCHIVE LOCATIONS
=================
```

```
The "official" archive site for this software is www.ijg.org.
The most recent released version can always be found there in
directory "files".

The JPEG FAQ (Frequently Asked Questions) article is a source of some
general information about JPEG.  It is available at
http://www.faqs.org/faqs/jpeg-faq.



FILE FORMAT COMPATIBILITY
=========================

This software implements ITU T.81 | ISO/IEC 10918 with some extensions from
ITU T.871 | ISO/IEC 10918-5 (JPEG File Interchange Format-- see REFERENCES).
Informally, the term "JPEG image" or "JPEG file" most often refers to JFIF
or
a subset thereof, but there are other formats containing the name "JPEG"
that
are incompatible with the DCT-based JPEG standard or with JFIF (for
instance,
JPEG 2000 and JPEG XR).  This software therefore does not support these
formats.  Indeed, one of the original reasons for developing this free
software
was to help force convergence on a common, interoperable format standard for
JPEG files.

JFIF is a minimal or "low end" representation.  TIFF/JPEG (TIFF revision 6.0
as
modified by TIFF Technical Note #2) can be used for "high end" applications
that need to record a lot of additional data about an image.
```

```
TO DO

=====


Please send bug reports, offers of help, etc. to jpeg-info@jpegclub.org.
```

```
Copyright (C)2009-2022 D. R. Commander. All Rights Reserved.

Copyright (C)2015 Viktor Szathmáry. 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 libjpeg-turbo Project 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.
```

```
Copyright (c) <year> <copyright holders>


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.
```

## M11. 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
```

## M12. 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 $
```

## M13. Libssh2



## M14. Linenoise NG

### linenoise

```
  * 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.
```

## M15. 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:
```

```
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.
```

## M16. 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.

## M17. 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.
```

## M18. 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.]
```

## M19. 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

## M20. 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
```

## M21. 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.
```

## M22. QR Code Gnerator

```
Copyright © 2022 Project Nayuki. (MIT License)

https://www.nayuki.io/page/qr-code-generator-library



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.
```

## M23. quirc

```
quirc -- QR-code recognition library

Copyright (C) 2010-2012 Daniel Beer <dlbeer@gmail.com>
```

```
ISC License

==========

Permission to use, copy, modify, and/or 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" AND THE AUTHOR DISCLAIMS ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE
AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, 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 THIS SOFTWARE.
```

## M24. 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.
```

## M25. 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
```

# Приложение Н. Пользовательские процедуры

В данном разделе описываются следующие категории пользовательских процедур:

| Процедура | Описание |
|---|---|
| Администраторы | управление авторизацией администраторов |
| Группа | управление группами |
| Доступ | управление доступом |
| Другое | разное |
| Новички | управление новыми станциями |
| Связи | управление связями с соседними Серверами Dr.Web |
| Сервер | управление Сервером Dr.Web |
| Соединения | управление соединениями с клиентами |
| Станции | управление станциями |

| Процедура | Описание |
|---|---|
| Ldap | трансляция имен пользователей |

# H1. Администраторы

## Администратор авторизован

Вызывается при успешной аутентификации администратора в Центре управления безопасностью.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `address` — сетевой адрес, с которого авторизовался администратор,<br>• `subsys` — подсистема Сервера Dr.Web (см. файл `adm-subsys.ds`),<br>• `id` — ID администратора,<br>• `authorizer` — название модуля авторизации (база данных, LDAP, AD),<br>• `language` — код языка административной учетной записи,<br>• `date_format` — формат даты административной учетной записи | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when Administrator authorize successfully

Database:
  available

Parameters:
  login              Administrator`s login name
  address            Administrator`s network address
  subsys             Server subsystem (see adm-subsys.ds)
  id                 Administrator`s ID
  authorizer         Authorizer name (database, LDAP, AD)
  language           Administrator`s language code
  date_format        Administrator`s date format

Returned value:
  ignored
```

```
]]

local args = ... -- args.login, args.address, args.subsys, args.error, args.id,
args.authorizer,
                 -- args.language, args.date_format
```

## Администратор авторизован с помощью Microsoft Active Directory Service

Вызывается при успешной аутентификации администратора с помощью Microsoft Active Directory Service (MSAD).

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `address` — сетевой адрес, с которого авторизовался администратор,<br>• `is_secure` — администратор использует защищенное соединение HTTPS (`true` \| `false`),<br>• `name` — LDAP-имя администратора,<br>• `DN` — LDAP DN администратора,<br>• `SID` — идентификатор безопасности Windows (SID) администратора,<br>• `GUID` — глобальный уникальный идентификатор (GUID) администратора,<br>• `primary_group` — имя первичной группы администратора,<br>• `primary_group_DN` — LDAP DN первичной группы администратора,<br>• `primary_group_SID` — идентификатор безопасности (SID) первичной группы администратора,<br>• `primary_group_GUID` — глобальный уникальный идентификатор (GUID) первичной группы администратора,<br>• `groups` — таблица, содержащая имена группы администратора (включенные в атрибут MSAD),<br>• `groups_DN` — таблица, содержащая DN-имена группы администратора (в том же порядке, что и группы),<br>• `groups_SID` — таблица, содержащая идентификаторы безопасности (SID) группы администратора (в том же порядке, что и группы),<br>• `groups_GUID` — таблица, содержащая глобальные уникальные идентификаторы (GUID) группы администратора (в том же порядке, что и группы) | • `nil` — ничего не делать,<br>• `string` — empty ничего не делать,<br>• `not-empty` — установить в качестве группы администратора группу с ID, соответствующим данной строке |

**Текст процедуры:**

```
--[[
Called:
  when the external administrator was authorized successfully using Microsoft Active
Directory Service

Database:
  available

Parameters:
  login              Administrator's login name
  address            Administrator's network address
  is_secure          Is true if administrator uses HTTPS connection
  name               Administrator's LDAP name
  DN                 Administrator's LDAP distinguished name
  SID                Administrator's Windows security identifier
  GUID               Administrator's GUID
  primary_group      Administrator's primary group name
  primary_group_DN   Administrator's primary group LDAP distinguished name
  primary_group_SID  Administrator's primary group SID
  primary_group_GUID Administrator's primary group GUID
  groups             Table containg Administrator's group names (memberOf MSAD
attribute)
  groups_DN          Table containg Administrator's group distinguished names (in the
same order as groups)
  groups_SID         Table containg Administrator's group SIDs (in the same order as
groups)
  groups_GUID        Table containg Administrator's group GUIDs (in the same order as
groups)

Returned value:
             nil        do nothing
  string     empty      do nothing
             not-empty  set administrator group to this string (group ID)

]]

local args = ... -- args.is_secure, args.login, args.address,
                 -- args.name, args.DN, args.SID, args.GUID,
                 -- args.primary_group, args.primary_group_DN, args.primary_group_SID,
args.primary_group_GUID,
                 -- args.groups, args.groups_DN, args.groups_SID, args.groups_GUID
```

## Администратор не авторизован

Вызывается при ошибке авторизации администратора в Центре управления безопасностью.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `address` — сетевой адрес администратора, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `subsys` — подсистема Сервера Dr.Web (см. файл adm-subsys.ds),<br>• `error` — код ошибки (см. файл auth-error.ds) | |

**Текст процедуры:**

```
--[[
Called:
  when Administrator authorization failed

Database:
  available

Parameters:
  login              Administrator`s login name
  address            Administrator`s network address
  subsys             Server subsystem (see adm-subsys.ds)
  error              Error code (see auth-error.ds)

Returned value:
  ignored

]]

local args = ... -- args.login, args.address, args.subsys, args.error
```

# H2. Группа

## Группа создана

Вызывается после создания новой группы.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна, если процедура не запущена функцией `drwcs.new_group()` | • `login` — регистрационное имя администратора,<br>• `id` — ID группы,<br>• `name` — название группы,<br>• `pid` — ID родительской группы | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when new group created
```

```
Database:
  available

Parameters:
  login      administrator`s login name
  id         group ID
  name       group name
  pid        parent group ID

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.pid
```

## Группа удалена

Вызывается после удаления группы.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `id` — ID группы,<br>• `name` — название группы | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when group deleted

Database:
  available

Parameters:
  login      administrator`s login name
  id         group ID
  name       group name

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name
```

## Свойства группы изменены

Вызывается после изменения свойств группы.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `id` — ID группы,<br>• `name` — название группы,<br>• `descr` — описание группы,<br>• `pid` — ID родительской группы | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when group properties changed

Database:
  available

Parameters:
  login      administrator`s login name
  id         group ID
  name       group name
  descr      group description
  pid        parent group ID

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.descr, args.pid
```

## H3. Доступ

### Доступ запрещен

Вызывается при запрете доступа согласно настройкам ACL или по результату выполнения процедуры `access_check`.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — временный ID клиента (для новичков/Серверов Dr.Web),<br>• `address` — сетевой адрес клиента,<br>• `station` — NetBIOS-имя клиента. Не задается для Серверов Dr.Web и не заменяется на DNS-имя,<br>• `type` — “station”, “installer”, “newbie”, “server”, “proxy”, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `description` — описание станции | |

**Текст процедуры:**

```
--[[
Called:
  when access denied according ACLs settings or result
  of 'access_check' procedure

Database:
  available

Parameters:
  id              station (temporary for newbie/server) ID
  address         station network address
  station         station name (undefined for servers)
                  this is NetBIOS station name (not replaced by DNS one)
  type            one of 'station' | 'installer' | 'newbie' | 'server' | 'proxy'
  description     station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.type, args.description

-- no return => `nil' value
```

## Проверка доступа

Вызывается перед проверкой доступа по соответствующим ACL (Access Control List - списки контроля доступа).

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — временный ID клиента (для новичков/Серверов Dr.Web),<br>• `address` — сетевой адрес клиента,<br>• `station` — NetBIOS-имя клиента. Не задается для Серверов Dr.Web и не заменяется на DNS-имя,<br>• `type` — “station”, “installer”, “newbie”, “server”, “proxy” | • `nil` — проверять адреса через заданные ACL,<br>• `boolean` — не проверять адреса через ACL, для всех:<br>  ▫ `true` — разрешать доступ, |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | | ▫ `false` — запрещать доступ |

**Текст процедуры**

```
--[[
Called:
  before check access against appropriate ACL

Database:
  available

Parameters:
  id              station ID (temporary for newbie/server)
  address         station network address
  station         station name (undefined for servers)
                  this is NetBIOS station name (not replaced by DNS one)
  type            one of 'station | installer | newbie | server | proxy'

Returned value:
              nil         check address against configured ACLs
  boolean     true        allow access, do not check agains ACLs
              false       reject access, do not check agains ACLs

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.address, args.station, args.type

-- no return => `nil' value
```

## H4. Другое

### Автоматическое обновление лицензионного ключа

Вызывается при окончании срока действия лицензионного ключа.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `event` — тип события:<br>▫ `expire` — истекает срок действия лицензионного ключа, автоматическое обновление недоступно<br>▫ `diff` — загружен новый лицензионный ключ, но состав лицензируемых компонентов у текущего и нового ключей отличается. Лицензионный ключ должен быть заменен вручную | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | ▫ `renew` — лицензионный ключ был автоматически обновлен<br>• `old_key` — содержимое старого лицензионного ключа<br>• `new_key` — содержимое нового лицензионного ключа. Доступно, если тип события `diff` или `renew` | |

**Текст процедуры:**

```
--[[
Called:
  when license key expire or have been renewed

Database:
  available

Parameters:
  event       event type: "expire" - license key expires or have done it
                          "diff"   - received new key, but components differs from
current one
                          "renew"  - current key have been renewed, old one was deleted

  old_key     content of old license key
  new_key     content of renew license key, available at event type "diff" or "renew"

Returned value:
  ignored

]]

local args = ... -- args.event, args.old_key, args.new_key
```

## Обнаружена эпидемия

Вызывается при обнаружении эпидемии угроз безопасности в сети.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `virus` — наиболее распространенная угроза,<br>• `total` — общее количество обнаруженных угроз | игнорируется |

**Текст процедуры:**

```
--[[
Called:
```

```
  when virus epidemic has been detected by the server

Database:
  available

Parameters:
  total            total count of viruses
  virus            most frequently detected virus name

Returned value:
  ignored

]]

local args = ... -- args.total, args.virus
```

## Отчет Контроля приложений

Вызывается при получении отчета Контроля приложений со станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — сетевой адрес станции,<br>• `station` — название станции,<br>• `time` — время наступления события (время станции),<br>• `sid` — SID станции,<br>• `user` — пользователь, который запустил процесс с подозрительной активностью,<br>• `type` — тип события,<br>• `action` — примененное действие,<br>• `policy_type` — тип сработавшей политики,<br>• `policy_mask` — маска сработавшей политики,<br>• `test_mode` — событие произошло в тестовом режиме,<br>• `profile_id` — UUID профиля, по которому произведена блокировка,<br>• `profile_name` — название профиля, по которому произведена блокировка,<br>• `rule_id` — UUID правила, по которому произведена блокировка (если существует),<br>• `rule_name` — название правила, по которому произведена блокировка (если существует),<br>• `process_path` — путь к заблокированному процессу,<br>• `process_file_sha256` — SHA-256 файла процесса, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • process_file_version — версия файла процесса,<br>• process_file_description — описание файла процесса,<br>• process_file_origname — исходное имя файла процесса,<br>• process_file_prodname — название продукта файла процесса,<br>• process_file_prodver — версия продукта файла процесса,<br>• process_file_company — название компании файла процесса,<br>• process_cert_thumbprint — отпечаток сертификата (SHA-1), которым подписан процесс (если существует),<br>• process_cert_serial — серийный номер сертификата, которым подписан процесс (если существует)<br>• process_cert_issuer — издатель сертификата, которым подписан процесс (если существует),<br>• process_cert_subject — субъект сертификата, которым подписан процесс (если существует),<br>• process_cert_timestamp — время выдачи сертификата, которым подписан процесс (если существует),<br>• process_cert_not_before — время начала действия сертификата, которым подписан процесс (если существует),<br>• process_cert_not_after — время окончания действия сертификата, которым подписан процесс (если существует),<br>• process_hashdb — бюллетень, содержащий хеш файла процесса,<br>• object_path — путь к заблокированному скрипту или пустое значение,<br>• object_file_sha256 — SHA-256 файла скрипта (если существует),<br>• object_file_version — версия файла скрипта (если существует),<br>• object_file_description — описание файла скрипта (если существует),<br>• object_file_origname — исходное имя файла скрипта (если существует), | |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `object_file_prodname` — название продукта файла скрипта (если существует),<br>• `object_file_prodver` — версия продукта файла скрипта (если существует),<br>• `object_file_company` — название компании файла скрипта (если существует),<br>• `object_cert_thumbprint` — отпечаток сертификата (SHA-1), которым подписан скрипт (если существует),<br>• `object_cert_serial` — серийный номер сертификата, которым подписан скрипт (если существует),<br>• `object_cert_issuer` — издатель сертификата, которым подписан скрипт (если существует),<br>• `object_cert_subject` — субъект сертификата, которым подписан скрипт (если существует),<br>• `object_cert_timestamp` — время выдачи сертификата, которым подписан скрипт (если существует),<br>• `object_cert_not_before` — время начала действия сертификата, которым подписан скрипт (если существует),<br>• `object_cert_not_after` — время окончания действия сертификата, которым подписан скрипт (если существует),<br>• `object_hashdb` — бюллетень, содержащий хеш файла скрипта | |

### Текст процедуры:

```
--[[
Called:
  when application control event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  time              station time
  sid               SID of user initiated activity
  user              name of user initiated activity
  type              event type
  action            applied action
  policy_type       matched policy type
  policy_mask       matched policy mask
```

```
  test_mode           event occured in test mode
  profile_id          profile UUID used for activity blocking
  profile_name        profile name used for activity blocking
  rule_id             rule UUID used for activity blocking (if exist)
  rule_name           rule name used for activity blocking (if exist)

  process_path                path to affected process file
  process_file_sha256         process file SHA-256
  process_file_version        process file version
  process_file_description    process file description
  process_file_origname       process file original name
  process_file_prodname       process file product name
  process_file_prodver        process file product version
  process_file_company        process file company name
  process_cert_thumbprint     process file signing certificate thumbprint (SHA-1) (if
exist)
  process_cert_serial         process file signing certificate serial number (if exist)
  process_cert_issuer         process file signing certificate issuer (if exist)
  process_cert_subject        process file signing certificate subject (if exist)
  process_cert_timestamp      process file signing certificate sign issuance timestamp
(if exist)
  process_cert_not_before     process file signing certificate NotBefore timestamp (if
exist)
  process_cert_not_after      process file signing certificate NotAfter timestamp (if
exist)
  process_hashdb              hash database containing process file

  object_path                 path to affected object file (script, etc) or empty
  object_file_sha256          object file SHA-256 (if exist)
  object_file_version         object file version (if exist)
  object_file_description     object file description (if exist)
  object_file_origname        object file original name (if exist)
  object_file_prodname        object file product name (if exist)
  object_file_prodver         object file product version (if exist)
  object_file_company         object file company name (if exist)
  object_cert_thumbprint      object file signing certificate thumbprint (SHA-1) (if
exist)
  object_cert_serial          object file signing certificate serial number (if exist)
  object_cert_issuer          object file signing certificate issuer (if exist)
  object_cert_subject         object file signing certificate subject (if exist)
  object_cert_timestamp       object file signing certificate sign issuance timestamp (if
exist)
  object_cert_not_before      object file signing certificate NotBefore timestamp (if
exist)
  object_cert_not_after       object file signing certificate NotAfter timestamp (if
exist)
  object_hashdb               hash database containing object file

Returned value:
  ignored

]]

local args = ...
```

## Отчет Контроля приложений с соседнего Сервера

Вызывается при получении отчета Контроля приложений для станции от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `event_time` — время появления события на станции,<br>• `sid` — SID станции,<br>• `user` — пользователь, который запустил процесс с подозрительной активностью,<br>• `type` — тип события,<br>• `action` — примененное действие,<br>• `policy_type` — тип сработавшей политики,<br>• `policy_mask` — маска сработавшей политики,<br>• `test_mode` — событие произошло в тестовом режиме,<br>• `profile_id` — UUID профиля, по которому произведена блокировка,<br>• `profile_name` — название профиля, по которому произведена блокировка,<br>• `rule_id` — UUID правила, по которому произведена блокировка (если существует),<br>• `rule_name` — название правила, по которому произведена блокировка (если существует),<br>• `process_path` — путь к заблокированному процессу,<br>• `process_file_sha256` — SHA-256 файла процесса,<br>• `process_file_version` — версия файла процесса,<br>• `process_file_description` — описание файла процесса,<br>• `process_file_origname` — исходное имя файла процесса,<br>• `process_file_prodname` — название продукта файла процесса,<br>• `process_file_prodver` — версия продукта файла процесса, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • process_file_company — название компании файла процесса,<br>• process_cert_thumbprint — отпечаток сертификата (SHA-1), которым подписан процесс (если существует),<br>• process_cert_serial — серийный номер сертификата, которым подписан процесс (если существует),<br>• process_cert_issuer — издатель сертификата, которым подписан процесс (если существует),<br>• process_cert_subject — субъект сертификата, которым подписан процесс (если существует),<br>• process_cert_timestamp — время выдачи сертификата, которым подписан процесс (если существует),<br>• process_cert_not_before — время начала действия сертификата, которым подписан процесс (если существует),<br>• process_cert_not_after — время окончания действия сертификата, которым подписан процесс (если существует),<br>• process_hashdb — бюллетень, содержащий хеш файла процесса,<br>• object_path — путь к заблокированному скрипту или пустое значение,<br>• object_file_sha256 — SHA-256 файла скрипта (если существует),<br>• object_file_version — версия файла скрипта (если существует),<br>• object_file_description — описание файла скрипта (если существует),<br>• object_file_origname — исходное имя файла скрипта (если существует),<br>• object_file_prodname — название продукта файла скрипта (если существует),<br>• object_file_prodver — версия продукта файла скрипта (если существует),<br>• object_file_company — название компании файла скрипта (если существует),<br>• object_cert_thumbprint— отпечаток сертификата (SHA-1), которым подписан скрипт (если существует), | |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • object_cert_serial — серийный номер сертификата, которым подписан скрипт (если существует),<br>• object_cert_issuer — издатель сертификата, которым подписан скрипт (если существует),<br>• object_cert_subject — субъект сертификата, которым подписан скрипт (если существует),<br>• object_cert_timestamp — время выдачи сертификата, которым подписан скрипт (если существует),<br>• object_cert_not_before — время начала действия сертификата, которым подписан скрипт (если существует),<br>• object_cert_not_after — время окончания действия сертификата, которым подписан скрипт (если существует),<br>• object_hashdb — бюллетень, содержащий хеш файла скрипта | |

**Текст процедуры:**

```
--[[
Called:
  when application control event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  event_time          station time
  recv_time           server originator time
  sid                 SID of user initiated activity
  user                name of user initiated activity
  type                event type
  action              applied action
  policy_type         matched policy type
  policy_mask         matched policy mask
  test_mode           event occured in test mode
  profile_id          profile UUID used for activity blocking
  profile_name        profile name used for activity blocking
  rule_id             rule UUID used for activity blocking (if exist)
  rule_name           rule name used for activity blocking (if exist)
```

```
  process_path               path to affected process file
  process_file_sha256        process file SHA-256
  process_file_version       process file version
  process_file_description   process file description
  process_file_origname      process file original name
  process_file_prodname      process file product name
  process_file_prodver       process file product version
  process_file_company       process file company name
  process_cert_thumbprint    process file signing certificate thumbprint (SHA-1) (if
exist)
  process_cert_serial        process file signing certificate serial number (if exist)
  process_cert_issuer        process file signing certificate issuer (if exist)
  process_cert_subject       process file signing certificate subject (if exist)
  process_cert_timestamp     process file signing certificate sign issuance timestamp
(if exist)
  process_cert_not_before    process file signing certificate NotBefore timestamp (if
exist)
  process_cert_not_after     process file signing certificate NotAfter timestamp (if
exist)
  process_hashdb             hash database containing process file

  object_path                path to affected object file (script, etc) or empty
  object_file_sha256         object file SHA-256 (if exist)
  object_file_version        object file version (if exist)
  object_file_description    object file description (if exist)
  object_file_origname       object file original name (if exist)
  object_file_prodname       object file product name (if exist)
  object_file_prodver        object file product version (if exist)
  object_file_company        object file company name (if exist)
  object_cert_thumbprint     object file signing certificate thumbprint (SHA-1) (if
exist)
  object_cert_serial         object file signing certificate serial number (if exist)
  object_cert_issuer         object file signing certificate issuer (if exist)
  object_cert_subject        object file signing certificate subject (if exist)
  object_cert_timestamp      object file signing certificate sign issuance timestamp (if
exist)
  object_cert_not_before     object file signing certificate NotBefore timestamp (if
exist)
  object_cert_not_after      object file signing certificate NotAfter timestamp (if
exist)
  object_hashdb              hash database containing object file

Returned value:
  ignored

]]

local args = ...
```

## Прокси-сервер Dr.Web создан

Вызывается при завершении создания Прокси-сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `id` — ID Прокси-сервера Dr.Web,<br>• `name` — название Прокси-сервера Dr.Web,<br>• `state` — статус завершения операции:<br>▫ `0` — успешно создан,<br>▫ `1` — ошибка при выполнении операции (ошибка базы данных),<br>▫ `2` — время ожидания операции истекло (база данных перегружена),<br>▫ `4` — Прокси-сервер Dr.Web уже существует | |

**Текст процедуры:**

```
--[[
Called:
  when proxy create completed

Database:
  available

Parameters:
  login         administrator`s login name
  id            proxy ID
  name          proxy name
  state         operation completion state:
                  0  created successfully
                  1  operation failed (database error)
                  2  operation timed out (database overloaded)
                  4  already exists

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.state
```

## Прокси-сервер Dr.Web удален

Вызывается при удалении Прокси-сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `id` — ID Прокси-сервера Dr.Web,<br>• `name` — название Прокси-сервера Dr.Web, | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when proxy deleted

Database:
  available

Parameters:
  login     administrator`s login name
  id        proxy id
  name      proxy name

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name
```

## H5. Новички

### Новичок зарегистрирован

После предоставления доступа новичку, но перед занесением соответствующей информации в базу данных.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — временный/постоянный ID станции,<br>• `address` — сетевой адрес станции,<br>• `station` — название станции,<br>• `existing` — подтвердить для существующей станции | игнорируется |

**Текст процедуры:**

```
--[[
Database:
  available

Called:
  when newbie access granted but before information stored in database

Parameters:
  id              station temporary/permanent ID
  address         station network address
  station         station name
  existing        approved using existing station
```

```
Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station
```

## Новичок подключается к Серверу Dr.Web

Вызывается при подключении новичка к Серверу Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — временный ID станции,<br>• `address` — сетевой адрес станции,<br>• `station` — название станции,<br>• `description` — описание станции (только для клиентов под ОС Windows),<br>• `ldapdn` — LDAP DN станции (только для клиентов под ОС Windows),<br>• `sid` — SID станции,<br>• `mac` — MAC-адрес станции | • `nil` — использовать настройки по умолчанию как при стандартной работе Сервера Dr.Web,<br>• `boolean` — действие Сервера Dr.Web:<br>▫ `true` — запросить ручное подтверждение (аналогично `Newbie approval`),<br>▫ `false` — запретить доступ (аналогично `Newbie closed`),<br>• `string` — первичная группа при подтверждении:<br>▫ `empty` — подтвердить, установить группу `Everyone` в качестве первичной (аналогично `Newbie open`),<br>▫ `not-empty` — подтвердить доступ и установить в качестве первичной группу с ID, |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | | соответствующим данной строке. Внимание! Существование данного ID будет проверено и, в случае если он не существует, первичной будет назначена группа `Everyone`,<br>• `vector` — подтверждать по умолчанию, содержит следующие команды и необязательные аргументы:<br>▫ `pgroup` —задать первичную группу, далее должен следовать ID группы,<br>▫ `rate` —задать тарифную группу, далее должен следовать ID тарифной группы,<br>▫ `id` —задать ID станции, далее должен следовать ID станции<br>▫ approve — запросить подтверждение вручную вместо автоматического подтверждения,<br>▫ `into` — подтвердить в существующую станцию, далее должен следовать ID существующей станции |

**Текст процедуры:**

```
--[[
Called:
  when newbie connected

Database:
  available

Parameters:
  id              station temporary ID
  address         station network address
  station         station name
  description     station description (Windows client only)
  ldapdn          station LDAP DN (Windows client only)
  sid             station computer SID
  mac             station computer MAC

Returned value:
              nil         default, standard server operation according settings
  boolean     true        request approval (like 'Newbie approval' does)
              false       reject access (like 'Newbie closed' does)
  string      empty       accept, set primary group to 'Everyone'
                            (like 'Newbie open' does)
              not-empty   accept, set primary group to this string (ID) (substring after
space treated as rate group id)
                          Attention! Existence of This ID will be checked and
                          if it does not exist it will be replaced by `Everyone'
  vector                  accept by default, must contain commands and optional arguments:
                          "pgroup"  - set primary group, must be followed by group id
                          "rate"    - set rate group, must be followed by rate group id
                          "id"      - set station id, must be followed by station id
                          "approve" - request approval instead of accepting
                          "into"    - accept into existing station, must be followed by
existing station id


Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.address, args.station

-- place my station (named ADMINISTRATOR) into `Everyone' group ignoring newbie policy
and newbie's preference
if string.upper( args.station ) == 'ADMINISTRATOR' then
  return ''
end

-- set new UUID for any station with this id and request for manual approve, useful for
cloned stations
if args.id == '01234567-89ab-cdef-0123-456789abcdef' then
  return { "id", dwcore.get_uuid(), "approve" }
end

-- no return => `nil' value => according server settings
```

## Новичок принят

Вызывается при предоставлении доступа новичку, успешной его авторизации и создании станции в базе данных.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — временный ID станции,<br>• `address` — сетевой адрес станции,<br>• `station` — название станции,<br>• `compsid` — SID станции,<br>• `compmac` — MAC-адрес станции,<br>• `description` — описание станции | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when newbie access granted, authorization is successfull
  and station created in database

Database:
  available

Parameters:
  id              station temporary ID
  address         station network address
  station         station name
  compsid         station UID (SID on Windows)
  compmac         station MAC address
  description     station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.compsid, args.compmac,
args.description
```

## Н6. Связи

### Завершение работы компонента на станции соседнего Сервера Dr.Web

Вызывается при получении события `component completed` от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • neighborname — название соседнего Сервера Dr.Web,<br>• originatorid — ID Сервера Dr.Web, который является источником события,<br>• originatorname — название Сервера Dr.Web, который является источником события,<br>• stationid — ID станции,<br>• stationname — название станции,<br>• eventid — ID события,<br>• component — номер компонента,<br>• pid — ID процесса,<br>• infections — обнаружены угрозы,<br>• errors — обнаружены ошибки доступа,<br>• exitcode — код завершения компонента,<br>• time — время завершения (время станции) | |

**Текст процедуры:**

```
--[[
Called:
  when "component completed" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  infections          infections found
  errors              access errors detected
  exitcode            component exit code
  time                end time (station time)

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
```

```
                -- args.stationname, args.time
                -- args.component, args.pid, args.infections
                -- args.errors, args.exitcode
```

## Запуск компонента на станции соседнего Сервера Dr.Web

Вызывается при получении события `component started` от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `component` — номер компонента,<br>• `pid` — ID процесса,<br>• `engine` — версия поискового движка,<br>• `records` — количество записей об угрозах,<br>• `user` — имя пользователя и группа владельца процесса,<br>• `time` — время начала (время станции) | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "component started" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
```

```
  pid                process ID
  engine             virus-finding engine version
  records            virus records number
  user               user name and group (process owner)
  time               start time (station time)

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.engine
                 -- args.records, args.user, args.time
```

## Изменились координаты соседнего Сервера Dr.Web или станции соседнего Сервера Dr.Web

Вызывается при получении события `geolocation` от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `latitude` — широта в формате DD.DDDDDD,<br>• `longitude` — долгота в формате DD.DDDDDD | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "geolocation" event received from neighbor server

Database:
  available

Parameters:
  neighborid         neighbor server ID which the event received from
```

```
  neighborname       neighbor server name
  originatorid       ID of the event server originator
  originatorname     name of the event server originator
  stationid          station ID
  stationname        station name
  latitude           latitude in DD.DDDDDD format
  longitude          longitude in DD.DDDDDD format

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.latidue,args.longitude
                 -- ...
```

## Изменились оборудование и программы станции соседнего сервера

Вызывается при получении события `environment changed` от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `group_name` — название первичной группы станции,<br>• `category` — категория объекта окружения | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "environment changed" event recived from neighbor server

Database:
  available
```

```
Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  group_name          station primary group name
  category            environment category

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,args.stationname,
                 -- args.group_name, args.category
```

## Обнаружена угроза безопасности на станции соседнего Сервера Dr.Web

Вызывается при получении события `virus detected` от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `component` — номер компонента,<br>• `pid` — ID процесса,<br>• `time` — время наступления события (время станции),<br>• `user` — имя пользователя и группа владельца процесса,<br>• `object` — путь к объекту в файловой системе,<br>• `owner` — имя пользователя и группа владельца объекта,<br>• `action` — код действия, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `objecttype` — тип объекта:<br>  ▫ `-1` неизвестен<br>  ▫ `0` файл<br>  ▫ `1` загрузочный сектор<br>  ▫ `2` блок памяти или процесс<br>  ▫ `3` вредоносная активность<br>• `infectiontype` — тип угрозы (см. Dr.Web API),<br>• `sha1` — хеш SHA-1 обнаруженного объекта,<br>• `sha256` — хеш SHA-256 обнаруженного объекта,<br>• `hashdb` — бюллетень, содержащий хеш | |

**Текст процедуры:**

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  time                event time (station time)
  user                user name and group (process owner)
  object              filesystem object path
  owner               object owner (user name and group)
  action              action code (see Dr.Web API; only errors bit set)
  objecttype          object type
                        -1    unknown
                         0    file
                         1    boot sector
                         2    memory block / process
                         3    virus like activity
  infectiontype       infection type (see Dr.Web API)
  sha1                object SHA-1 hash
  sha256              object SHA-256 hash
  hashdb              hash database containing object

Returned value:
  ignored

]]
```

```
local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.object, args.owner,
                 -- args.action, args.objecttype, args.infectiontype,
                 -- args.sha1, args.sha256, args.hashdb
```

## Отчет Превентивной защиты с соседнего Сервера

Вызывается при получении отчета Превентивной защиты для станции от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `pid` — ID процесса,<br>• `path` — путь к исполняемому файлу процесса с подозрительной активностью,<br>• `target_path` — путь к защищаемому объекту, к которому была осуществлена попытка доступа,<br>• `hips_type` — тип защищаемого объекта (числовое значение),<br>• `shell_guard_type` — причина блокировки неавторизованного кода (числовое значение),<br>• `denied` — доступ был запрещен (`true` \| `false`),<br>• `is_user_action` — действие было запрошено у пользователя (`true` \| `false`),<br>• `event_count` — количество автоматически запрещенных событий (только если для `is_user_action` значение `false`),<br>• `event_user` — пользователь, который запустил процесс с подозрительной активностью, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • action_user — пользователь, который задал реакцию на подозрительную активность процесса (только если для is_user_action значение true),<br>• event_time — время появления события на станции,<br>• recv_time — время получения отчета соседним Сервером Dr.Web,<br>• sha1 — хеш SHA-1 обнаруженного объекта,<br>• sha256 — хеш SHA-256 обнаруженного объекта,<br>• hashdb — бюллетень, содержащий хеш | |

**Текст процедуры:**

```
--[[
Called:
  when HIPS event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  pid                 numeric,process id
  path                process file path
  target_path         affected resource path
  hips_type           numeric, HIPS type
  shell_guard_type    numeric, Shell Guard event type
  denied              boolean, access was denied
  is_user_action      boolean, user was asked
  event_count         event number (for accumulation period - if is_user_action is false)
  event_user          user which initiated the suspicious activity
  action_user         user which allowed or denied the activity (non-empty only if
is_user_action is true)
  event_time          station time
  recv_time           server originator time
  sha1                process file SHA-1 hash
  sha256              process file SHA-256 hash
  hashdb              hash database containing process file

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname, args.originatorid,
args.originatorname,
```

```
                -- args.stationid, args.stationname, args.eventid
                -- args.pid, args.path, args.target_path, args.hips_type,
args.shell_guard_type,
                -- args.denied, args.is_user_action, args.event_count, args.event_user,
args.action_user
                -- args.event_time, args.recv_time, args.sha1, args.sha256, args.hashdb
```

## Ошибка авторизации на соседнем Сервере Dr.Web

Вызывается после отказа соединения с соседним Сервером Dr.Web вследствие ошибки авторизации.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID Сервера Dr.Web,<br>• `address` — адрес Сервера Dr.Web,<br>• `name` — название Сервера Dr.Web,<br>• `reason` — причина сбоя | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  just after server connection rejected due (authorization) error

Database:
  available

Parameters:
  id          server ID
  address     server address
  name        server name
  reason      failure reason

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.reason
```

## Ошибка сканирования на станции соседнего Сервера Dr.Web

Вызывается при получении события `scan error` от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `component` — номер компонента,<br>• `pid` — ID процесса<br>• `time` — время наступления события (время станции),<br>• `user` — имя пользователя и группа владельца процесса,<br>• `object` — путь к объекту в файловой системе,<br>• `owner` — имя пользователя и группа владельца объекта,<br>• `action` — код действия,<br>• `sha1` — хеш SHA-1 обнаруженного объекта,<br>• `sha256` — хеш SHA-256 обнаруженного объекта,<br>• `hashdb` — бюллетень, содержащий хеш | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  time                event time (station time)
  user                user name and group (process owner)
```

```
  object              filesystem object path
  owner               object owner (user name and group)
  action              action code (error bit(s) set)
  sha1                object SHA-1 hash
  sha256              object SHA-256 hash
  hashdb              hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.object, args.owner, args.action,
                 -- args.sha1, args.sha256, args.hashdb
```

## Соседний Сервер Dr.Web подключен

Вызывается при соединении с соседним Сервером Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID Сервера Dr.Web,<br>• `address` — адрес Сервера Dr.Web,<br>• `name` — название Сервера Dr.Web | игнорируется |

### Текст процедуры:

```
--[[
Called:
  when server connected

Database:
  available

Parameters:
  id          server ID
  address     server address
  name        server name

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name
```

## Состояние станции соседнего Сервера Dr.Web

Вызывается, когда соседний Сервер Dr.Web сообщает состояние станции, включающее состояние компонентов, вирусных баз и некоторые локальные политики (отправка событий, прием обновлений и заданий).

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `count` — количество различных кодов статуса,<br>• `state_0` — значение состояния,<br>• `number_0` — количество станций в `state_0` | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  count               number of different status code
  state_0             state value
  number_0            number of the stations in 'state_0'

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
```

```
                -- args.stationname,
                -- args.count,
                -- args.state_0, args.number_0
                -- args.state_1, args.number_1
                -- ...
```

## Станция соседнего Сервера Dr.Web удалена

Вызывается при удалении станции на соседнем Сервере Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when station was deleted on neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname
                 -- ...
```

## Статистика сканирования станции соседнего Сервера Dr.Web

Вызывается при получении события `scan statistics` от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `component` — номер компонента,<br>• `pid` — ID процесса,<br>• `user` — имя пользователя и группа владельца процесса,<br>• `time` — время наступления события (время станции),<br>• `size` — суммарный размер всех просканированных объектов,<br>• `elapsedtime` — затраченное время,<br>• `scanned` — количество просканированных объектов,<br>• `infected` — количество объектов, инфицированных известным вирусом,<br>• `modifications` — количество объектов, инфицированных модификацией вируса,<br>• `suspicious` — количество подозрительных объектов,<br>• `cured` — количество вылеченных файлов,<br>• `deleted` — количество удаленных файлов,<br>• `renamed` — количество переименованных файлов,<br>• `moved` — количество файлов, перемещенных в карантин,<br>• `locked` — количество заблокированных файлов (только SpIDer Guard),<br>• `errors` — количество файлов, не просканированных из-за ошибки доступа | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "scan statistics" event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           number of component
  pid                 process ID
  user                user name and group (process owner)
  time                event time (station time)
  size                summary size of all scanned objects
  elapsedtime         elapsed time
  scanned             number of scanned objects
  infected            number of objects infected by known virus
  modifications       number of objects infected by virus modification
  suspicious          number of suspicious objects
  cured               number of cured files
  deleted             number of deleted files
  renamed             number of renamed files
  moved               number of quarantined files
  locked              number of locked files (SpIDer Guard only)
  errors              number of not scanned files (due access error)

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.scanned, args.infected, args.modifications,
                 -- args.suspicious, args.cured, args.deleted, args.renamed,
                 -- args.moved, args.locked, args.errors, args.size, args.elapsedtime
```

## Установка Агента с соседнего Сервера Dr.Web

Вызывается при получении события `installation` от соседнего Сервера Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `neighborid` — ID соседнего Сервера Dr.Web, от которого получено событие,<br>• `neighborname` — название соседнего Сервера Dr.Web,<br>• `originatorid` — ID Сервера Dr.Web, который является источником события,<br>• `originatorname` — название Сервера Dr.Web, который является источником события,<br>• `stationid` — ID станции,<br>• `stationname` — название станции,<br>• `eventid` — ID события,<br>• `event` — тип события:<br>  ▫ `0` — установка началась,<br>  ▫ `1` — установка успешно завершена,<br>  ▫ `2` — отказ,<br>  ▫ `3` — время истекло,<br>  ▫ `4` — неуспешно,<br>  ▫ `5` — не завершено<br>• `message` — сообщение об ошибке (или пустое, если не было ошибки),<br>• `address` — адрес станции,<br>• `begtime` — время начала,<br>• `endtime` — время окончания | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "installation" event recived from neighbor server

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  event               event type:
                        0   installation begin
                        1   successully completed
                        2   rejected
                        3   timed out
                        4   failed
                        5   incomplete
  message             error message (or empty if there is no error)
  address             station address
  begtime             begin time
  endtime             end time

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.event, args.message, args.address
                 -- args.begtime, args.endtime
```

# H7. Сервер

## Бинарный файл Сервера Dr.Web загружен

Вызывается после загрузки бинарного файла Сервера Dr.Web для исполнения некоторых служебных функций (Сервер Dr.Web не будет обслуживать клиентов).

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | нет | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when server binary file loaded for execute some service function
  (the server will not serve clients)
```

```
Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

## Верификация БД завершена

Вызывается после завершения верификации базы данных.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | • `state` — статус завершения:<br>▫ `true` — успешно,<br>▫ `false` — неуспешно | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when database verification completed

Database:
  NOT available

Parameters:
  state     true   success
                   failed

Returned value:
  ignored

]]

local args = ... -- args.state
```

## Достигнуто лицензионное ограничение (соединение не установлено)

Вызывается когда невозможно установить соединение с клиентом из-за лицензионного ограничения. После разрыва соединения вызывается `bad_connection.ds`.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `reason` — причина ошибки соединения: | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | ▫ `connection` — нет доступных лицензий,<br>▫ `database` — ошибка создания новой станции в БД поскольку не осталось доступных лицензий | |

**Текст процедуры:**

```
--[[
Called:
  when new client connection cannot be established due license limitation

Database:
  available

Parameters:
  reason     "connection"   no free license
             "database"     cannot create new station in database due
                            no free license

Returned value:
  ignored

]]

local args = ... -- args.reason
```

## Завершение некоторых функций Сервера Dr.Web

Вызывается после завершения выполнения некоторых служебных функций Сервером Dr.Web (Сервер Dr.Web не обслуживал клиентов).

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | нет | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when server completed execute some service function
  (the server did not serve clients)

Database:
  NOT available

Parameters:
  none
```

```
Returned value:
  ignored

]]
```

## Загрузка драйвера БД завершена

Вызывается после завершения процесса загрузки драйвера базы данных.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | • `state` — статус завершения:<br>  ▫ `true` — успешная загрузка,<br>  ▫ `false` — ошибка загрузки,<br>• `driver` — название драйвера базы данных,<br>• `library` — полный путь до библиотеки драйвера базы данных,<br>• `message` — текст сообщение об ошибке при статусе `false` | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when database driver load process completed

Database:
  NOT available

Parameters:
  state     true     successful load
            false    load failed
  driver             database driver name
  library            full path to database driver library
  message            error message text when state is 'false'

Returned value:
  ignored

]]

local args = ... -- args.state, args.driver, args.library, args.message
```

## Задание на Сервере Dr.Web выполнено

Вызывается после выполнения задания на Сервере Dr.Web.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID Сервера Dr.Web,<br>• `done` — статус завершения:<br>  ▫ `true` — выполнено успешно,<br>  ▫ `false` — сбой при выполнении,<br>• `time` — время завершения задания,<br>• `name` — название задания,<br>• `error` — сообщение из журнала выполнения | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when job executed on the server

Database:
  available

Parameters:
  id                server ID
  done      true    executed successfully
            false   execution failed
  time              job completion time
  name              job name
  error             error or other message

Returned value:
  ignored

]]

local args = ... -- args.id, args.done, args.name, args.time, args.error
```

## Модуль протокола выгружен

Вызывается при выгрузке модуля протокола.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | • `name` — внутреннее название протокола, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `path` — путь к файлу модуля протокола | |

**Текст процедуры:**

```
--[[
Called:
  when protocol module unloaded

Database:
  NOT available

Parameters:
  name                    protocol name
  path                    path to protocol module file

Returned value:
  ignored

]]

local args = ... -- args.path
```

## Модуль протокола загружен

Вызывается после загрузки модуля протокола.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| не определено | • `path` — путь к файлу модуля протокола,<br>• `name` — внутреннее название протокола,<br>• `desc` — описание модуля протокола,<br>• `state` — состояние:<br>  ▫ `loaded` — модуль протокола удачно загружен,<br>  ▫ `disabled` — модуль протокола отключен в файле `drwcsd.conf`,<br>• `error` — текст сообщение об ошибке при статусе `invalid` | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when protocol module loaded

Parameters:
  path                    path to protocol module file
  name                    internal protocol name
  desc                    protocol module description string
  state      "loaded"     protocol module loaded successfully
             "disabled"   protocol module is disabled in drwcsd.conf
             "invalid"    invalid protocol module format
  error                   error message if state is "invalid"

Returned value:
  ignored

]]

local args = ... -- args.state, args.path, args.name
```

## Расширение выгружено

Вызывается при выгрузке модуля расширения.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | • `name` — название расширения,<br>• `path` — путь к файлу расширения | игнорируется |

### Текст процедуры:

```
--[[
Called:
  when plugin module unloaded

Database:
  NOT available

Parameters:
  name                    plugin name
  path                    path to plugin file

Returned value:
  ignored

]]

local args = ... -- args.name, yargs.path
```

## Расширение загружено

Вызывается после загрузки модуля расширения.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | • `path` — путь к файлу расширения,<br>• `name` — внутреннее название расширения,<br>• `desc` — описание расширения,<br>• `state` — состояние:<br>▫ `loaded` — расширение успешно загружено,<br>▫ `disabled` — использование расширения отключено в файле `drwcsd.conf`,<br>▫ `invalid` — некорректный формат расширения,<br>• `error` — текст сообщение об ошибке при статусе `invalid` | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when plugin module loaded

Database:
  NOT available

Parameters:
  path                    path to plugin file
  name                    internal plugin name
  desc                    plugin description string
  state      "loaded"     plugin loaded successfully
             "disabled"   plugin is disabled in drwcsd.conf
             "invalid"    invalid plugin format
  error                   error message if state is "invalid"

Returned value:
  ignored

]]


local args = ... -- args.state, args.path, args.name, args.error
```

## Резервное копирование

Вызывается после завершения резервного копирования файлов, но перед удалением файлов предыдущего резервного копирования.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `state` — статус завершения:<br>▫ `true` — успешно,<br>▫ `false` — неуспешно | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when backup completed but before deleting previous backup files

Database:
  available

Parameters:
  state  true  successful
         false failed

Returned value:
  ignored

]]

local args = ... -- args.state
```

## Сервер Dr.Web завершает обслуживание

Вызывается когда Сервер Dr.Web завершает обслуживание клиентов.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | нет | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when server completed serve clients

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored
```

```
]]
```

## Сервер Dr.Web запущен и готов

Вызывается при запуске Сервера Dr.Web и его готовности обслуживать клиентов.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| недоступна | нет | игнорируется |

### Текст процедуры:

```
--[[
Called:
  when server started and going to serve clients

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

# H8. Соединения

## Достигнуто лицензионное ограничение (в соединении отказано)

Вызывается при отказе соединения согласно ограничениям в лицензионном соглашении.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — сетевой адрес станции,<br>• `station` — NetBIOS-имя станции. Не заменяется на DNS-имя,<br>• `type` — тип `station` | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when connection denied according license limitation

Database:
  available

Parameters:
  id              station ID
  address         station network address
  station         station name
                  this is NetBIOS station name (not replaced by DNS one)
  type            one of 'station'

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.type

-- no return => `nil' value
```

## Ошибка соединения

Вызывается при невозможности установления соединения с новым клиентом.

Возможные причины: закончились лицензии (при этом сначала вызывается `license_error.ds`), нет связи с БД, ошибка БД, превышено число станций, ожидающих авторизации, перегружен сервер или БД.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна, если причина `no license`, и потенциально доступна, если причина `overload` (БД в это время использовать не рекомендуется) | • `address` — адрес клиента,<br>• `reason` — причина ошибки соединения:<br>  ▫ `no database` — не установлено соединение с базой данных,<br>  ▫ `overload` — база данных перегружена,<br>  ▫ `no license` — не осталось доступных лицензий для принятия соединения | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when new client connection cannot be established

Database:
  available if reason is "no license" and potentialy available if
  reason is "overload" (but it is not recommended to use DB that time)

Parameters:
  address                  client address
  reason   "no database"   no established database connection
           "overload"      database is overloaded
           "no license"    no free license to accept connection

Returned value:
  ignored

]]

local args = ... -- args.address, args.reason
```

## Получен PONG от клиента

Вызывается при получении PONG от клиента.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID клиента,<br>• `address` — сетевой адрес клиента,<br>• `station` — название клиента (для Агента, Сервера, Инсталлятора),<br>• `time` — время возврата (round-trip) пакета | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when 'PONG' received from client

Database:
  available

Parameters:
  id         client ID
  address    network address
  station    station name (for Agent, Server, Installer)
  time       packet round-trip time in milliseconds

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station,
                 -- args.time
```

## Соединение с клиентом разорвано

Вызывается после разрыва соединения с клиентом.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID клиента,<br>• `address` — сетевой адрес клиента,<br>• `type` — тип клиента: `unknown`, `station`, `console`, `server`, `installer`, `newbie`<br>• `station` — название станции (только для Агента),<br>• `bytesin` — получено байт без сжатия,<br>• `bytesout` — отправлено байт без сжатия,<br>• `totalbytesin` — получено байт со сжатием,<br>• `totalbytesout` — отправлено байт со сжатием,<br>• `reason` — причина разъединения | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when client disconnected

Database:
  available

Parameters:
  id              client ID
  address         network address
  type            client type: "unknown", "station", "proxy",
                               "server", "installer", "newbie"
  station         station name (only for Agent)
  bytesin         bytes received
  bytesout        bytes sent
  totalbytesin    compressed bytes received
  totalbytesout   compressed bytes sent
  reason          disconnect reason

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.type, args.station
                 -- args.bytesin, args.bytesout
                 -- args.totalbytesin, args.totalbytesout
                 -- args.reason
```

# H9. Станции

## Агент деинсталлирован

Вызывается после завершения удаления Агента.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `state` — статус завершения:<br>  ▫ `true` — успешно,<br>  ▫ `false` — неуспешно,<br>• `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `message` — пустое, если статус `true`, в противном случае содержит сообщение об ошибке | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when deinstallation of Agent completed

Database:
  available

Parameters:
  login           login name of administrator
  state           true    success
                  false   failed
  id                      station ID
  address                 station address
  station                 station name
  message                 empty if state is 'true' or contains error message

Returned value:
  ignored

]]

local args = ... -- args.login, args.state, args.id
                 -- args.address, args.station, args.message
```

## Завершение работы компонента на станции

Вызывается при получении события `component completed` от Агента.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `component` — номер компонента,<br>• `pid` — ID процесса,<br>• `infections` — обнаружены угрозы,<br>• `errors` — обнаружены ошибки доступа,<br>• `exitcode` — код завершения компонента, | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "component completed" event received from Agent

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  component   component number
  pid         process ID
  infections  infections found
  errors      access errors detected
  exitcode    component exit code

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.exitcode, args.infections, args.errors
```

## Задание выполнено

Вызывается при получении от Агента события `job executed`.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `done` — статус выполнения:<br>  ▫ `true` — выполнено успешно,<br>  ▫ `false` — сбой при выполнении,<br>• `time` — время завершения задания,<br>• `name` — название задания,<br>• `error` — сообщение об ошибке или состоянии | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "job executed" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  done      true    executed successfully
            false   execution failed
  time              job completion time
  name              job name
  job               job ID (empty for Agent prior version 11 (protocol 3.1+))
  error             error or other message

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.done,
                 -- args.name, args.job, args.time, args.error
```

## Запуск компонента на станции

Вызывается при получении события `component started` от Агента.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `component` — номер компонента,<br>• `pid` — ID процесса,<br>• `engine` — версия поискового движка,<br>• `records` — количество записей об угрозах,<br>• `user` — имя пользователя и группа владельца процесса,<br>• `time` — время начала (время станции) | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when "component started" event received from Agent

Database:
  available

Parameters:
  id         station ID
  address    station address
  station    station name
  component  component number
  pid        process ID
  engine     virus-finding engine version
  records    virus records number
  user       user name and group (process owner)
  time       start time (station time)

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.records, args.user, args.time, args.engine
```

## Изменилось географическое положение станции

Вызывается при изменении географического местоположения станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `latitude` — широта станции в формате DD.DDDDDD,<br>• `longitude` — долгота станции в формате DD.DDDDDD | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when agent geolocation changed

Database:
  available

Parameters:
  id         station ID
  address    station address
  station    station name
  latitude   station latitude in DD.DDDDDD format
  longitude  station longitude in DD.DDDDDD format

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.latitude, args.longitude
```

## Необходима перезагрузка станции

Вызывается после получения Сервером Dr.Web сообщения `reboot required` от станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — сетевой адрес станции,<br>• `station` — NetBIOS-имя станции. Не заменяется на DNS-имя,<br>• `product` — ID продукта, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `description` — описание продукта,<br>• `from_revision` — номер текущей ревизии,<br>• `to_revision` — номер новой ревизии,<br>• `from_revision_date` — дата текущей ревизии,<br>• `to_revision_date` — дата новой ревизии | |

**Текст процедуры:**

```
--[[
Called:
  after server received 'reboot required' station message.

Database:
  available

Parameters:
  id                  station ID
  address             station network address
  station             station name (this is NetBIOS station name not replaced by DNS
one)
  product             product ID
  description         product description
  from_revision       current revision number
  to_revision         new revision number
  from_revision_date  current revision date
  to_revision_date    new revision date

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.product, args.description,
args.from_revision, args.to_revision, args.from_revision_date, args.to_revision_date
```

## Обнаружена угроза безопасности станции

Вызывается при получении события `virus detected` от Агента.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `component` — номер компонента,<br>• `pid` — ID процесса,<br>• `time` — время наступления события (время станции),<br>• `user` — имя пользователя и группа владельца процесса,<br>• `object` — путь к объекту в файловой системе,<br>• `owner` — имя пользователя и группа владельца объекта,<br>• `virus` — название угрозы,<br>• `action` — код действия,<br>• `objecttype` — тип объекта:<br>  ▫ `-1` неизвестен,<br>  ▫ `0` файл,<br>  ▫ `1` —загрузочный сектор,<br>  ▫ `2` —блок памяти или процесс,<br>  ▫ `3` —вредоносная активность<br>• `infectiontype` — тип угрозы (см. Dr.Web API),<br>• `compsid` — SID станции,<br>• `compmac` — MAC-адрес станции,<br>• `description` — описание станции,<br>• `compdn` — LDAP DN станции (только для клиентов под ОС Windows),<br>• `sha1` — хеш SHA-1 обнаруженного объекта,<br>• `sha256` — хеш SHA-256 обнаруженного объекта,<br>• `hashdb` — бюллетень, содержащий хеш | |

**Текст процедуры:**

```
--[[
```

```
Called:
  when "virus detected" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  component         component number
  pid               process ID
  time              event time (station time)
  user              user name and group (process owner)
  object            filesystem object path
  owner             object owner (user name and group)
  virus             virus name
  action            action code (see Dr.Web API; only errors bit set)
  objecttype        object type
                      -1    unknown
                       0    file
                       1    boot sector
                       2    memory block / process
                       3    virus like activity
  infectiontype     infection type (see Dr.Web API)
  compsid           computer sid
  compmac           computer MAC
  description       computer description
  compdn            computer LDAP DN
  sha1              object SHA-1 hash
  sha256            object SHA-256 hash
  hashdb            hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.object, args.owner,
                 -- args.virus, args.action, args.objecttype, args.infectiontype
                 -- args.compsid, args.compmac, args.description, args.compdn
                 -- args.sha1, args.sha256, args.hashdb
```

## Отчет Превентивной защиты

Вызывается при получении отчета Превентивной защиты со станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `time` — время появления события на станции, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `pid` — ID процесса,<br>• `path` — путь к исполняемому файлу процесса с подозрительной активностью,<br>• `target_path` — путь к защищаемому объекту, к которому была осуществлена попытка доступа,<br>• `hips_type` — тип защищаемого объекта (числовое значение),<br>• `shell_guard_type` — причина блокировки неавторизованного кода (числовое значение),<br>• `denied` — доступ был запрещен (true \| false),<br>• `is_user_action` — действие было запрошено у пользователя (`true` \| `false`),<br>• `event_count` — количество автоматически запрещенных событий (только если для `is_user_action` значение `false`),<br>• `event_user` — пользователь, который запустил процесс с подозрительной активностью,<br>• `action_user` — пользователь, который задал реакцию на подозрительную активность процесса (только если для `is_user_action` значение `true`),<br>• `sha1` — хеш SHA-1 обнаруженного объекта,<br>• `sha256` — хеш SHA-256 обнаруженного объекта,<br>• `hashdb` — бюллетень, содержащий хеш | |

**Текст процедуры:**

```
--[[
```

```
Called:
  when HIPS event received from Agent

Database:
  available

Parameters:
  id                  station ID
  address             station address
  station             station name
  time                station time
  pid                 numeric,process id
  path                process file path
  target_path         affected resource path
  hips_type           numeric, HIPS type
  shell_guard_type    numeric, Shell Guard event type
  denied              boolean, access was denied
  is_user_action      boolean, user was asked
  event_count         event number (for accumulation period - if is_user_action is false)
  event_user          user which initiated the suspicious activity
  action_user         user which allowed or denied the activity (non-empty only if
is_user_action is true)
  sha1                process file SHA-1 hash
  sha256              process file SHA-256 hash
  hashdb              hash database containing process file

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.time,
                 -- args.pid, args.path, args.target_path, args.hips_type,
args.shell_guard_type,
                 -- args.denied, args.is_user_action, args.event_count, args.event_user,
args.action_user
                 -- args.sha1, args.sha256, args.hashdb
```

## Ошибка авторизации станции

Вызывается после отказа соединения с Агентом вследствие ошибки авторизации.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `reason` — причина сбоя,<br>• `type` — один из `station`, `installer`, `proxy`,<br>• `compsid` — SID станции,<br>• `compmac` — MAC-адрес станции, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `description` — описание станции | |

**Текст процедуры:**

```
--[[
Called:
  just after Agent connection rejected due authorization error

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  reason      failure reason
  type        one of 'station' | 'installer' | 'proxy'
  compsid     station UID (SID on Windows)
  compmac     station MAC address
  description station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.reason, args.type,
args.compsid, args.compmac, args.description
```

## Ошибка даты/времени на станции

Вызывается при обнаружении некорректных времени/даты на станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `now` — время на Сервере Dr.Web (в миллисекундах),<br>• `time` — время на станции (в миллисекундах),<br>• `valid_delta` — допустимая разница времени (в миллисекундах) | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when invalid station time/date detected

Database:
  available

Parameters:
  id              station ID
  address         station address
  station         station name
  now             server time (in milliseconds)
  time            station time (in milliseconds)
  valid_delta     valid time delta (in milliseconds)

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station
                 -- args.now, args.date, args.valid_delta
```

## Ошибка обновления станции

Вызывается после получения Сервером Dr.Web сообщения `update failed` от станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — сетевой адрес станции,<br>• `station` — NetBIOS-имя станции. Не заменяется на DNS-имя,<br>• `product` — ID продукта,<br>• `description` — описание продукта,<br>• `from_revision` — номер текущей ревизии,<br>• `to_revision` — номер новой ревизии,<br>• `from_revision_date` — дата текущей ревизии,<br>• `to_revision_date` — дата новой ревизии | игнорируется |

### Текст процедуры:

```
--[[
```

```
Called:
  after server received 'update failed' station message.

Database:
  available

Parameters:
  id                  station ID
  address             station network address
  station             station name (this is NetBIOS station name not replaced by DNS
one)
  product             product ID
  description         product description
  from_revision       current revision number
  to_revision         new revision number
  from_revision_date  current revision date
  to_revision_date    new revision date

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.product, args.description,
args.from_revision, args.to_revision, args.from_revision_date, args.to_revision_date
```

## Ошибка сканирования станции

Вызывается при получении события `scan error` от Агента.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `component` — номер компонента,<br>• `pid` — ID процесса,<br>• `time` — время наступления события (время станции),<br>• `user` — имя пользователя и группа владельца процесса,<br>• `object` — путь к объекту в файловой системе,<br>• `owner` — имя пользователя и группа владельца объекта,<br>• `action` — код действия,<br>• `compsid` — SID станции,<br>• `compmac` — MAC-адрес станции, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `description` — описание станции,<br>• `ldapdn` — LDAP DN станции (только для клиентов под ОС Windows),<br>• `sha1` — хеш SHA-1 обнаруженного объекта,<br>• `sha256` — хеш SHA-256 обнаруженного объекта,<br>• `hashdb` — бюллетень, содержащий хеш | |

**Текст процедуры:**

```
--[[
Called:
  when "scan error" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  component         component number
  pid               process ID
  time              event time (station time)
  user              user name and group (process owner)
  object            filesystem object path
  owner             object owner (user name and group)
  action            action code (error bit(s) set)
  compsid           computer SID
  compmac           computer MAC
  description       computer description
  ldapdn            computer LDAP DN
  sha1              object SHA-1 hash
  sha256            object SHA-256 hash
  hashdb            hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.object, args.owner,
                 -- args.action, args.compsid, args.compmac, args.description,
args.ldapdn
                 -- args.sha1, args.sha256, args.hashdb
```

## Получен список компонентов

Вызывается при сообщении Агентом списка установленных компонентов.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `count` — количество заявленных компонентов,<br>• `component_0` — название компонента,<br>• `time_0` — время установки,<br>• `from_0` — источник установки (адрес Сервера Dr.Web, MSI и т.п.),<br>• `path_0` — путь установки | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when Agent reported installed components

Database:
  available

Parameters:
  id                  station ID
  address             station address
  station             station name
  count               number of components reported
  component_0         component name
  time_0              installation time
  from_0              installation source (server address, MSI, etc)
  path_0              installation path

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.count
                 -- args.component_0, args.time_0, args.from_0, args.path_0
                 -- args.component_1, args.time_1, args.from_1, args.path_1
                 -- ...
```

## Получена информация о вирусных базах

Вызывается при отправке Агентом информации о вирусных базах.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `count` — количество вирусных баз,<br>• `name_0` — название файла вирусной базы,<br>• `md5_0` — MD5 файла вирусной базы,<br>• `version_0` — версия вирусной базы,<br>• `issued_0` — дата и время выпуска вирусной базы,<br>• `records_0` — количество записей в вирусной базе,<br>• `type_0` — тип вирусной базы | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when Agent sent virus bases information

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  count       number of found virus bases
  name_0      virus base file name
  md5_0       virus base file MD5
  version_0   virus base version
  issued_0    virus base issue date and time
  records_0   number of records
  type_0      virus base type

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.count,
                 -- args.name_0, args.md5_0, args.version_0,
                 -- args.issued_0, args.records_0, args.type_0,
                 -- args.name_1, args.md5_1, args.version_1,
```

```
                -- args.issued_1, args.records_1, args.type_1,
                -- ...
```

## Состояние станции

Вызывается при сообщении Агентом состояния компонентов, вирусных баз и некоторых локальных политик (отправка событий, прием обновлений и заданий).

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `events` — сообщение о событиях:<br>▫ `true` — Агент отправляет информацию о событиях,<br>▫ `false` — Агент не отправляет информацию о событиях,<br>• `jobs` — прием заданий (по расписанию и удаленные сканирования):<br>▫ `true` — Агент принимает задания,<br>▫ `false` — Агент не принимает задания,<br>• `updates` — прием обновлений:<br>▫ `true` — Агент принимает обновления,<br>▫ `false` — Агент не принимает обновления | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when Agent report its local policy

Database:
  available

Parameters:
  events    true     Agent send events
            false    Agent do not send events
  jobs      true     Agent accept jobs (schedule & remote scan)
            false    Agent do not accept jobs
  updates   true     Agent accept updates
            false    Agent do not accept updates
```

```
Returned value:
  ignored

]]

local args = ... -- args.events, args.jobs, args.updates
```

## Станция в процессе авторизации

Вызывается при попытке авторизации станции (ID и пароль уже проверены, валидны и известны).

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `connected` — проверка наличия станций с данным ID, уже подключенных к Серверу Dr.Web:<br>  ▫ `true` — другая станция с данным ID уже подключена к Серверу Dr.Web,<br>  ▫ `false` — нет других подключенных станций с данным ID,<br>• `current_address` — сетевой адрес уже подключенной станции с данным ID (не пустой, только если `connected` принимает значение `true`),<br>• `current_name` — название уже подключенной станции с данным ID,<br>• `last_address` — сетевой адрес станции с данным ID во время ее последнего подключения,<br>• `last_time` — время последнего появления станции с данным ID,<br>• `last_server` — Сервер Dr.Web станции с данным ID во время ее последнего подключения,<br>• `new_name` — название подключающейся станции, | • `string` — результат запроса на подключение станции<br>• `nil` — поведение Сервера Dr.Web по умолчанию<br>• `deny` — отказать станции в авторизации<br>• `force` — разрешить авторизацию, даже если другая станция с этим ID уже подключена (отключить подключенную станцию)<br>• `newbie` — сбросить станцию в новички |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `new_address` — сетевой адрес подключающейся станции | |

**Текст процедуры:**

```
--[[
Called:
  when station tries to authorize (id and password already checked, valid and known)

Database:
  available

Parameters:
  id                      station ID
  connected       true    station with same ID already connected to server
                  false   no any station with same ID connected
  current_address         already connected station network address (not empty only if
'connected' is true)
  current_name            last connected station name
  last_address            last disconnected station network address
  last_time               last disconnected station seen time
  last_server             last connected station server
  new_name                now connecting station name
  new_address             now connecting station network address

Returned value:
          nil             default server behavior
  string  'deny'          deny authorization for station
          'force'         allow authorization even if other station with same ID already
connected (by disconnecting it)
          'newbie'        reset station to newbie

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.connected, args.current_address, args.current_name,
args.last_address,
                 -- args.last_time, args.last_server, args.new_name, args.new_address

-- no return => `nil' value
```

## Станция подключена

Вызывается при удачном подключении Агента.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | • `os` — ОС станции,<br>• `platform` — платформа станции,<br>• `compsid` — SID станции,<br>• `compmac` — MAC-адрес станции,<br>• `description` — описание станции | |

**Текст процедуры:**

```
--[[
Called:
  when Agent connected successfully

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  os          station os
  platform    station platform
  compsid     station UID (Security ID on Windows)
  compmac     station MAC address
  description station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.os, args.platform,
args.compsid, args.compmac, args.description
```

## Станция создана

Вызывается при завершении создания станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `id` — ID станции,<br>• `name` — название станции,<br>• `state` — статус завершения операции: | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | ▫ `0` — успешно создана,<br>▫ `1` — ошибка при выполнении операции (ошибка базы данных),<br>▫ `2` — время ожидания операции истекло (база данных перегружена),<br>▫ `3` — нет доступных лицензий,<br>▫ `4` — станция уже существует | |

**Текст процедуры:**

```
--[[
Called:
  when station create completed

Database:
  available

Parameters:
  login         administrator`s login name
  id            station ID
  name          station name
  state         operation completion state:
                  0  created successfully
                  1  operation failed (database error)
                  2  operation timed out (database overloaded)
                  3  no free license
                  4  already exists

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.state
```

## Станция удалена

Вызывается при удалении станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `login` — регистрационное имя администратора,<br>• `id` — ID станции | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when station deleted

Database:
  available

Parameters:
  login     administrator`s login name
  id        station id

Returned value:
  ignored

]]

local args = ... -- args.login, args.id
```

## Статистика сканирования станции

Вызывается при получении события `scan statistics` от Агента.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `component` — номер компонента,<br>• `pid` — ID процесса,<br>• `user` — имя пользователя и группа владельца процесса,<br>• `time` — время наступления события (время станции),<br>• `size` — суммарный размер всех просканированных объектов,<br>• `elapsedtime` — затраченное время,<br>• `scanned` — количество просканированных объектов,<br>• `infected` — количество объектов, инфицированных известным вирусом,<br>• `modifications` — количество объектов, | игнорируется |

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| | инфицированных модификацией вируса,<br>• `suspicious` — количество подозрительных объектов,<br>• `cured` — количество вылеченных файлов,<br>• `deleted` — количество удаленных файлов,<br>• `renamed` — количество переименованных файлов,<br>• `moved` — количество файлов, перемещенных в карантин,<br>• `locked` — количество заблокированных файлов (только SplDer Guard),<br>• `errors` — количество файлов, не просканированных из-за ошибки доступа | |

**Текст процедуры:**

```
--[[
Called:
  when "scan statistics" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  component         number of component
  pid               process ID
  user              user name and group (process owner)
  time              event time (station time)
  size              summary size of all scanned objects
  elapsedtime       elapsed time
  scanned           number of scanned objects
  infected          number of objects infected by known virus
  modifications     number of objects infected by virus modification
  suspicious        number of suspicious objects
  cured             number of cured files
  deleted           number of deleted files
  renamed           number of renamed files
  moved             number of quarantined files
  locked            number of locked files (SpIDer Guard only)
  errors            number of not scanned files (due access error)

Returned value:
  ignored
```

```
]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.scanned,
                 -- args.infected, args.modifications, args.suspicious,
                 -- args.cured, args.deleted, args.renamed, args.moved,
                 -- args.locked, args.errors, args.size, args.elapsedtime
```

## Установка Агента

Вызывается после получения события `installation`.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID инсталляции (внимание: это не ID станции),<br>• `address` — адрес станции,<br>• `station` — название станции,<br>• `event` — тип события:<br>  ▫ `0` — начало инсталляции,<br>  ▫ `1` — завершено успешно,<br>  ▫ `2` — отказ,<br>  ▫ `3` — время истекло,<br>  ▫ `4` — неуспешно,<br>  ▫ `5` — не завершено<br>• `message` — сообщение об ошибке (или пустое, если не было ошибки),<br>• `sessionid` — ID сессии инсталляции | игнорируется |

### Текст процедуры:

```
--[[
Called:
  when "installation" event occured

Database:
  available

Parameters:
  id                installation ID (not station!)
  address           station address
  station           station name
  event             event type:
                      0   installation begin
                      1   successully completed
                      2   rejected
```

```
                      3   timed out
                      4   failed
                      5   incomplete
  message           error message (or empty if there is no error)
  sessionid         installation session ID

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station
                 -- args.event, args.message, args.sessionid
```

## Устройство заблокировано

Вызывается при блокировке устройства на станции.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `id` — ID станции,<br>• `address` — адрес станции,<br>• `name` — название станции,<br>• `user` — имя пользователя,<br>• `instance_id` — идентификатор экземпляра устройства,<br>• `friendly_name` — понятное имя устройства,<br>• `description` — описание устройства,<br>• `guid` — GUID устройства,<br>• `class` — класс устройства (название родительской группы) | игнорируется |

**Текст процедуры:**

```
--[[
Called:
  when device on station blocked

Database:
  available

Parameters:
  id              station ID
  address         station address
  station         station name
  user            user name
  instance_id     device instance id
  friendly_name   device friendly name
  description     device description
  guid            device guid
  class           device group class guid
  blocktime       time when station was blocked
  blockrcvtime    time when server received alert

Returned value:
  ignored

]]

local args = ... -- args.id args.address args.station args.user args.instance_id
                 -- args.friendly_name args.description args.guid args.class
                 -- args.station_time args.args.recv_time
```

# H10. Ldap

## Трансляция имен пользователей в LDAP DN

Вызывается при трансляции имен пользователей в LDAP DN.

| База данных | Параметры | Возвращаемое значение |
|---|---|---|
| доступна | • `user` — имя пользователя | • `nil` — неизвестный пользователь<br>• `string` — информация о пользователе:<br>▫ `empty` — неизвестный пользователь<br>▫ `non-empty` — DN пользователя |

### Текст процедуры

```
--[[

Called:
  when AuthLDAP module translates user name to DN
```

```
Database:
  available

Parameters:
  user           username

Returned value:
             nil         unknown user
  string     empty       unknown user
             non-empty   DN of user

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.user

-- example code:
-- if args.user == 'super-admin' then return 'CN=super,DC=example,DC=com' end

-- no return => `nil' value
```

# Глава 3: Часто задаваемые вопросы

## Перенос Сервера Dr.Web на другой компьютер (для ОС Windows)

Описанные процедуры переноса Сервера Dr.Web предполагают, что на компьютере, на который переносится Сервер Dr.Web, будет установлен Сервер Dr.Web той же мажорной версии, что и на исходном компьютере.

---

При переносе Сервера Dr.Web 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 завершения работы Сервера Dr.Web описана в **Руководстве администратора**, в подразделах:

- Запуск и завершение работы Сервера Dr.Web под ОС Windows,
- Запуск и завершение работы Сервера Dr.Web под ОС семейства UNIX.

Процедуры переноса различаются в зависимости от ОС исходного компьютера:

- Перенос с компьютера под управлением ОС Windows на компьютер под управлением ОС Windows.
- Перенос с компьютера под управлением ОС семейства UNIX на компьютер под управлением ОС Windows.

После завершения процедуры переноса в обоих случаях проверьте работоспособность нового Сервера Dr.Web и обеспечьте подключение к нему станций.

**Чтобы перенести Сервер Dr.Web с компьютера под управлением ОС Windows на другой компьютер под ОС Windows**

1. Установите новый Сервер Dr.Web (пустой, с новой базой) той же мажорной версии на нужном компьютере (установка подробно описана в **Руководстве по установке**, Установка Сервера Dr.Web для ОС Windows).

Если вы планируете переносить старый Сервер Dr.Web с сохранением IP-адреса, назначьте новому Серверу Dr.Web временный IP-адрес, чтобы станции могли взаимодействовать со старым Сервером Dr.Web во время переноса.

2. В веб-интерфейсе нового Сервера Dr.Web перейдите в раздел **Администрирование** → **Менеджер лицензий**, добавьте ключ вашей действующей лицензии `agent.key` и распространите его на группу **Everyone**.

3. Перейдите в раздел **Состояние репозитория** и убедитесь, что репозиторий обновляется без ошибок.

   Если в таблице со списком продуктов в графе **Состояние** имеются сообщения об ошибках, обратитесь в техническую поддержку. К запросу прикрепите файл `drwcsd.log`. Не следует выполнять какие-либо дальнейшие действия из инструкций до получения обратной связи в запросе.

4. Перейдите в раздел **Сервер Dr.Web** и убедитесь, что в этом разделе отображается дата, которая совпадает с датой текущей ревизии Сервера Dr.Web в разделе **Состояние репозитория**. Если дата не совпадает и имеется сообщение о наличии обновлений, нажмите на кнопку **Посмотреть список версий** и обновите Сервер Dr.Web до актуальной версии.

5. Остановите службу нового Сервера Dr.Web с помощью средств управления службами ОС Windows, Центра управления или меню **Пуск** → **Все программы** → **Dr.Web Server** → **Остановить**.

6. Остановите службу старого Сервера Dr.Web.

7. Проверьте целостность базы данных на старом Сервере Dr.Web с помощью команды `drwcsd modexecdb database-verify`. Полная командная строка для проверки базы данных будет выглядеть примерно так:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=trace -log="C:
   \Program Files\DrWeb Server\var\verifydb.log" modexecdb database-verify
   ```

   Если после выполнения этой команды в файле `verifydb.log` появится сообщение об ошибке, обратитесь в техническую поддержку.

8. Выполните экспорт базы данных старого Сервера Dr.Web в файл с помощью команды `drwcsd modexecdb database-export`. Полная командная строка для экспорта будет выглядеть примерно так:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=trace -log="C:
   \Program Files\DrWeb Server\var\exportdb.log" modexecdb database-export
   <полное_имя_файла>
   ```

9. Запустите службу старого Сервера Dr.Web, чтобы он продолжал обслуживать клиентов, с помощью средств управления службами ОС Windows или меню **Пуск** → **Все программы** → **Dr.Web Server** → **Запустить**.

10. Замените содержимое каталогов `%programfiles%\DrWeb Server\etc` и `%programfiles%\DrWeb Server\var\extensions` на новом Сервере Dr.Web содержимым аналогичных каталогов со старого Сервера Dr.Web.

11. Замените файл сертификата `drwcsd-certificate.pem` в каталоге `%programfiles%\DrWeb Server\webmin\install\windows` на новом Сервере Dr.Web аналогичным файлом со старого Сервера Dr.Web.

12. Если вы используете встроенную базу данных, замените файл базы данных `database.sqlite` в каталоге `%programfiles%\DrWeb Server\var` на новом Сервере Dr.Web аналогичным файлом со старого Сервера Dr.Web.

13. Запустите службу нового Сервера Dr.Web.

14. Войдите в веб-интерфейс нового Сервера Dr.Web с теми же логином и паролем, что и на старом Сервере Dr.Web.
15. Перейдите в раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web** и выберите задание **Backup sensitive data** (Резервное копирование критичных данных). Нажмите на значок ; в окне для редактирования задания выберите вкладку **Действие**. Убедитесь, что в поле **Путь** не указан путь к каталогу на старом Сервере Dr.Web. Очистите это поле и оставьте это поле пустым (в этом случае для хранения резервных копий будет использоваться каталог по умолчанию — `%programfiles%\DrWeb Server\var\backup`) или укажите путь к каталогу на новом Сервере Dr.Web. Проделайте то же самое с заданием **Backup repository** (Резервное копирование репозитория), а также с иными заданиями с действиями **Резервное копирование критичных данных** и **Резервное копирование репозитория** (при наличии таких заданий).

    Если в расписании присутствуют задания с действием **Запуск программы**, отредактируйте их в соответствии с набором ПО, установленного на новом компьютере, или удалите их из расписания.
16. Проверьте работоспособность нового Сервера Dr.Web и обеспечьте подключение к нему станций.
17. Остановите службу старого Сервера Dr.Web и удалите его (см. **Руководство по установке**, Удаление Сервера Dr.Web для ОС Windows).

**Чтобы перенести Сервер Dr.Web с компьютера под управлением ОС семейства UNIX на компьютер под ОС Windows**

В инструкции приведены примеры команд для ОС Linux. Обратите внимание, что пути для ОС FreeBSD отличаются:

- `/etc/init.d/` → `/usr/local/etc/rc.d/`
- `/var/opt/drwcs/` → `/var/drwcs/`
- `/opt/drwcs/` → `/usr/local/drwcs/`

1. Установите новый Сервер Dr.Web (пустой, с новой базой) той же мажорной версии на нужном компьютере (установка подробно описана в **Руководстве по установке**, Установка Сервера Dr.Web для ОС Windows).

   Если вы планируете переносить старый Сервер Dr.Web с сохранением IP-адреса, назначьте новому Серверу Dr.Web временный IP-адрес, чтобы станции могли взаимодействовать со старым Сервером Dr.Web во время переноса.
2. В веб-интерфейсе нового Сервера Dr.Web перейдите в раздел **Администрирование** → **Менеджер лицензий**, добавьте ключ вашей действующей лицензии `agent.key` и распространите его на группу **Everyone**.
3. Перейдите в раздел **Состояние репозитория** и убедитесь, что репозиторий обновляется без ошибок.

Если в таблице со списком продуктов в графе **Состояние** имеются сообщения об ошибках, обратитесь в техническую поддержку. К запросу прикрепите файл `drwcsd.log`. Не следует выполнять какие-либо дальнейшие действия из инструкций до получения обратной связи в запросе.

4. Перейдите в раздел **Сервер Dr.Web** и убедитесь, что в этом разделе отображается дата, которая совпадает с датой текущей ревизии Сервера Dr.Web в разделе **Состояние репозитория**. Если дата не совпадает и имеется сообщение о наличии обновлений, нажмите на кнопку **Посмотреть список версий** и обновите Сервер Dr.Web до актуальной версии.
5. Остановите службу нового Сервера Dr.Web с помощью средств управления службами ОС Windows, Центра управления или меню **Пуск** → **Все программы** → **Dr.Web Server** → **Остановить**.
6. Замените следующие файлы на новом Сервере Dr.Web файлами со старого Сервера Dr.Web:
   - файл сертификата `drwcsd-certificate.pem` в каталоге `%programfiles%\DrWeb Server\webmin\install\windows` нового Сервера Dr.Web соответствующим файлом из каталога `/opt/drwcs/webmin/install/windows` старого Сервера Dr.Web;
   - содержимое каталога `%programfiles%\DrWeb Server\var\extensions` (пользовательские процедуры) нового Сервера Dr.Web содержимым каталога `/var/opt/drwcs/extensions` старого Сервера Dr.Web;
   - конфигурационный файл `drwcsd.conf`, файл закрытого ключа `drwcsd.pri` и вторую копию сертификата `drwcsd-certificate.pem` в каталоге `%programfiles%\DrWeb Server\etc` нового Сервера Dr.Web соответствующими файлами из каталога `/var/opt/drwcs/etc` старого Сервера Dr.Web.

   

   Проверьте содержимое файла `drwcsd.conf` на предмет наличия путей, свойственных ОС семейства UNIX. Если таковые имеются, требуется исправить их вручную перед переносом.

7. Остановите старый Сервер Dr.Web через консоль с помощью команды:

```
# /etc/init.d/drwcsd stop
```

8. Проверьте целостность базы данных на старом Сервере Dr.Web с помощью команды:

```
# /etc/init.d/drwcsd modexecdb database-verify
```

Если после выполнения этой команды в файле `drwcsd.log` появится сообщение об ошибке, обратитесь в техническую поддержку.

9. Выполните экспорт базы данных старого Сервера Dr.Web в файл с помощью команды `drwcsd modexecdb database-export`. Полная командная строка для экспорта будет выглядеть примерно так:

```
# /etc/init.d/drwcsd modexecdb database-export <полное_имя_файла>
```

10. Запустите старый Сервер Dr.Web, чтобы он продолжал обслуживать клиентов, через консоль с помощью команды:

```
# /etc/init.d/drwcsd start
```

11. Если вы используете встроенную базу данных, замените файл базы данных `database.sqlite` в каталоге `%programfiles%\DrWeb Server\var` на новом Сервере Dr.Web аналогичным файлом из каталога `/var/opt/drwcs/` старого Сервера Dr.Web.
12. Запустите службу нового Сервера Dr.Web с помощью средств управления службами ОС Windows или меню **Пуск** → **Все программы** → **Dr.Web Server** → **Запустить**.
13. Войдите в веб-интерфейс нового Сервера Dr.Web с теми же логином и паролем, что и на старом Сервере Dr.Web.
14. Перейдите в раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web** и выберите задание **Backup sensitive data** (Резервное копирование критичных данных). Нажмите на значок ; в окне для редактирования задания выберите вкладку **Действие**. Убедитесь, что в поле **Путь** не указан путь к каталогу на старом Сервере Dr.Web. Очистите это поле и оставьте это поле пустым (в этом случае для хранения резервных копий будет использоваться каталог по умолчанию — `%programfiles%\DrWeb Server\var\backup`) или укажите путь к каталогу на новом Сервере Dr.Web. Проделайте то же самое с заданием **Backup repository** (Резервное копирование репозитория), а также с иными заданиями с действиями **Резервное копирование критичных данных** и **Резервное копирование репозитория** (при наличии таких заданий).

    Если в расписании присутствуют задания с действием **Запуск программы**, отредактируйте их в соответствии с набором ПО, установленного на новом компьютере, или удалите их из расписания.
15. Проверьте работоспособность нового Сервера Dr.Web и обеспечьте подключение к нему станций.
16. Остановите службу старого Сервера Dr.Web и удалите его (см. **Руководство по установке**, Удаление Сервера Dr.Web для ОС семейства UNIX).

**Чтобы проверить работоспособность нового Сервера Dr.Web после переноса**

1. Войдите в веб-интерфейс нового Сервера Dr.Web. Убедитесь, что все Агенты Dr.Web корректно отображаются в списке антивирусной сети.
2. Перейдите в раздел **Администрирование** → **Состояние репозитория** и убедитесь, что репозиторий на новом Сервере Dr.Web обновляется без ошибок. Если в таблице со списком продуктов в графе **Состояние** имеются сообщения об ошибках, обратитесь в техническую поддержку. К запросу прикрепите файл `drwcsd.log`. Не следует выполнять какие-либо дальнейшие действия из инструкций до получения обратной связи в запросе.

### Чтобы обеспечить подключение станций к новому Серверу Dr.Web

Для возможности перехода Агентов Dr.Web, для которых адрес нового Сервера Dr.Web задается через Центр управления, а не в настройках самого Агента Dr.Web на станции, оставьте включенными оба Сервера Dr.Web до момента завершения процедуры.

В качестве адреса Сервера Dr.Web рекомендуется использовать имя сервера в формате FQDN.

- Если у нового Сервера Dr.Web будет свой IP-адрес:
  a) Для всех Агентов Dr.Web, которых обслуживал старый Сервер Dr.Web, задайте адрес нового Сервера Dr.Web согласно соответствующей процедуре из раздела Подключение Агента Dr.Web к другому Серверу Dr.Web.

     Для Агентов Dr.Web, для которых адрес нового Сервера Dr.Web задавался через Центр управления, а не в настройках самого Агента Dr.Web на станции, на обоих Серверах Dr.Web в настройках Агента Dr.Web должен быть указан адрес нового Сервера Dr.Web.
  b) Дождитесь, пока все Агенты Dr.Web перейдут на новый Сервер Dr.Web.
- Если требуется сохранить для нового Сервера Dr.Web старый IP-адрес:
  a) Остановите старый Сервер Dr.Web.
  b) Назначьте новому Серверу Dr.Web IP-адрес старого Сервера Dr.Web.
  c) Перезапустите новый Сервер Dr.Web, чтобы измененные сетевые настройки вступили в силу.

# Перенос Сервера Dr.Web на другой компьютер (для ОС семейства UNIX)

Описанные процедуры переноса Сервера Dr.Web предполагают, что на компьютере, на который переносится Сервер Dr.Web, будет установлен Сервер Dr.Web той же мажорной версии, что и на исходном компьютере.

---

При переносе Сервера Dr.Web 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 завершения работы Сервера Dr.Web описана в **Руководстве администратора**, в подразделах:

- Запуск и завершение работы Сервера Dr.Web под ОС Windows,
- Запуск и завершение работы Сервера Dr.Web под ОС семейства UNIX.

Процедуры переноса различаются в зависимости от ОС исходного компьютера:

- Перенос с компьютера под управлением ОС семейства UNIX на компьютер под управлением ОС семейства UNIX.
- Перенос с компьютера под управлением ОС Windows на компьютер под управлением ОС семейства UNIX.

После завершения процедуры переноса в обоих случаях проверьте работоспособность нового Сервера Dr.Web и обеспечьте подключение к нему станций.

### Чтобы перенести Сервер Dr.Web с компьютера под управлением ОС семейства UNIX на другой компьютер под ОС семейства UNIX

#### Способ 1:

В инструкции приведены примеры команд для ОС Linux. Обратите внимание, что пути для ОС FreeBSD отличаются:

- `/etc/init.d/ → /usr/local/etc/rc.d/`
- `/var/opt/drwcs/ → /var/drwcs/`
- `/opt/drwcs/ → /usr/local/drwcs/`

1. Установите новый Сервер Dr.Web (пустой, с новой базой) на нужном компьютере (установка подробно описана в **Руководстве по установке**, Установка Сервера Dr.Web для ОС семейства UNIX).

Если вы планируете переносить старый Сервер Dr.Web с сохранением IP-адреса, назначьте новому Серверу Dr.Web временный IP-адрес, чтобы станции могли взаимодействовать со старым Сервером Dr.Web во время переноса.

2. В веб-интерфейсе нового Сервера Dr.Web перейдите в раздел **Администрирование** → **Менеджер лицензий**, добавьте ключ вашей действующей лицензии `agent.key` и распространите его на группу **Everyone**.
3. Перейдите в раздел **Состояние репозитория** и убедитесь, что репозиторий обновляется без ошибок.

Если в таблице со списком продуктов в графе **Состояние** имеются сообщения об ошибках, обратитесь в техническую поддержку. К запросу прикрепите файл `drwcsd.log`. Не следует выполнять какие-либо дальнейшие действия из инструкций до получения обратной связи в запросе.

4. Перейдите в раздел **Сервер Dr.Web** и убедитесь, что в этом разделе отображается дата, которая совпадает с датой текущей ревизии Сервера Dr.Web в разделе **Состояние репозитория**. Если дата не совпадает и имеется сообщение о наличии обновлений, нажмите на кнопку **Посмотреть список версий** и обновите Сервер Dr.Web до актуальной версии.
5. Остановите новый Сервер Dr.Web через веб-интерфейс или через консоль с помощью команды:

```
# /etc/init.d/drwcsd stop
```

6. Для переноса пользовательских процедур на новом Сервере Dr.Web замените каталог `/var/opt/drwcs/extensions/` на аналогичный каталог со всем содержимым со старого Сервера Dr.Web.
7. Из каталога `/opt/drwcs/webmin/install/windows` на новом Сервере Dr.Web удалите файл сертификата `drwcsd-certificate.pem`:

```
# rm /opt/drwcs/webmin/install/windows/drwcsd-certificate.pem
```

8. На новом Сервере Dr.Web замените конфигурационный файл `drwcsd.conf`, файл закрытого ключа `drwcsd.pri` и вторую копию сертификата `drwcsd-certificate.pem` в каталоге `var/opt/drwcs/etc/` соответствующими файлами со старого Сервера Dr.Web.
9. Остановите старый Сервер Dr.Web через веб-интерфейс или через консоль с помощью команды:

```
# /etc/init.d/drwcsd stop
```

10. Проверьте целостность базы данных на старом Сервере Dr.Web с помощью команды:

```
# /etc/init.d/drwcsd modexecdb database-verify
```

Если после выполнения этой команды в файле `drwcsd.log` появится сообщение об ошибке, обратитесь в техническую поддержку.

11. Выполните экспорт базы данных старого Сервера Dr.Web в файл с помощью команды `drwcsd modexecdb database-export`. Полная командная строка для экспорта будет выглядеть примерно так:

```
# /etc/init.d/drwcsd modexecdb database-export <полное_имя_файла>
```

12. Если вы используете встроенную базу данных, замените файл базы данных `/var/opt/drwcs/database.sqlite` на новом Сервере Dr.Web аналогичным файлом со старого Сервера Dr.Web.
13. Запустите старый Сервер Dr.Web, чтобы он продолжал обслуживать клиентов, через консоль с помощью команды:

```
# /etc/init.d/drwcsd start
```

14. На новом Сервере Dr.Web назначьте пользователя `drwcs` владельцем каталога размещения базы данных `/var/opt/drwcs`, а также владельцем файлов `/var/opt/drwcs/etc/drwcsd.pri`, `/var/opt/drwcs/etc/drwcsd.conf` и `/var/opt/drwcs/etc/drwcsd-certificate.pem`:

```
# chown -R drwcs:drwcs /var/opt/drwcs

# chown drwcs:drwcs /var/opt/drwcs/etc/drwcsd*
```

15. Скопируйте сертификат `drwcsd-certificate.pem` в каталог `/opt/drwcs/webmin/install/windows`:

```
# cp /var/opt/drwcs/etc/drwcsd-
certificate.pem /opt/drwcs/webmin/install/windows
```

16. Запустите новый Сервер Dr.Web с помощью команды:

```
# /etc/init.d/drwcsd start
```

17. Войдите в веб-интерфейс нового Сервера Dr.Web с теми же логином и паролем, что и на старом Сервере Dr.Web.
18. Перейдите в раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web** и выберите задание **Backup sensitive data** (Резервное копирование критичных данных). Нажмите на значок  ; в окне для редактирования задания выберите вкладку **Действие**. Убедитесь, что в поле **Путь** не указан путь к каталогу на старом Сервере Dr.Web. Очистите это поле и оставьте это поле пустым (в этом случае для хранения резервных копий будет использоваться каталог по умолчанию — `/var/opt/drwcs/backup`) или укажите путь к каталогу на новом Сервере Dr.Web. Проделайте то же самое с заданием **Backup repository** (Резервное копирование репозитория), а также с иными заданиями с действиями **Резервное копирование критичных данных** и **Резервное копирование репозитория** (при наличии таких заданий).

Если в расписании присутствуют задания с действием **Запуск программы**, отредактируйте их в соответствии с набором ПО, установленного на новом компьютере, или удалите их из расписания.

19. Проверьте работоспособность нового Сервера Dr.Web и обеспечьте подключение к нему станций.
20. Остановите службу старого Сервера Dr.Web и удалите его (см. **Руководство по установке**, Удаление Сервера Dr.Web для ОС семейства UNIX).

**Способ 2:**

Данный способ предполагает недоступность Сервера Dr.Web на период его переноса. Во избежание перерыва в обслуживании клиентов Сервером Dr.Web рекомендуется пользоваться способом переноса 1.

В инструкции приведены примеры команд для ОС Linux. Обратите внимание, что пути для ОС FreeBSD отличаются:

`/etc/init.d/ → /usr/local/etc/rc.d/`

1. Остановите старый Сервер Dr.Web через веб-интерфейс или через консоль с помощью команды:

```
# /etc/init.d/drwcsd stop
```

2. Выполните экспорт базы данных старого Сервера Dr.Web в файл с помощью команды `drwcsd modexecdb database-export`. Полная командная строка для экспорта будет выглядеть примерно так:

```
# /etc/init.d/drwcsd modexecdb database-export <полное_имя_файла>
```

3. Удалите старый Сервер Dr.Web (см. **Руководство по установке**, Удаление Сервера Dr.Web для ОС семейства UNIX). В процессе удаления будет создана резервная копия критичных данных (в каталоге `/var/tmp/drwcs/` по умолчанию).
4. Перенесите содержимое каталога резервной копии на компьютер, где будет установлен новый Сервер Dr.Web.
5. Запустите установку Сервера Dr.Web той же мажорной версии на новом компьютере (подробно описана в **Руководстве по установке**, Установка Сервера Dr.Web для ОС семейства UNIX). На шаге выбора источника резервной копии укажите путь к каталогу с резервной копией. Дождитесь успешного завершения установки.
6. Запустите новый Сервер Dr.Web с помощью команды:

```
# /etc/init.d/drwcsd start
```

7. Войдите в веб-интерфейс нового Сервера Dr.Web с теми же логином и паролем, что и на старом Сервере Dr.Web.

8. Перейдите в раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web** и выберите задание **Backup sensitive data** (Резервное копирование критичных данных). Нажмите на значок  ; в окне для редактирования задания выберите вкладку **Действие**. Убедитесь, что в поле **Путь** не указан путь к каталогу на старом Сервере Dr.Web. Очистите это поле и оставьте это поле пустым (в этом случае для хранения резервных копий будет использоваться каталог по умолчанию — `/var/opt/drwcs/backup`) или укажите путь к каталогу на новом Сервере Dr.Web. Проделайте то же самое с заданием **Backup repository** (Резервное копирование репозитория), а также с иными заданиями с действиями **Резервное копирование критичных данных** и **Резервное копирование репозитория** (при наличии таких заданий).

   Если в расписании присутствуют задания с действием **Запуск программы**, отредактируйте их в соответствии с набором ПО, установленного на новом компьютере, или удалите их из расписания.

9. Проверьте работоспособность нового Сервера Dr.Web и обеспечьте подключение к нему станций.

**Чтобы перенести Сервер Dr.Web с компьютера под управлением ОС Windows на компьютер под ОС семейства UNIX**

В инструкции приведены примеры команд для ОС Linux. Обратите внимание, что пути для ОС FreeBSD отличаются:

- `/etc/init.d/ → /usr/local/etc/rc.d/`
- `/var/opt/drwcs/ → /var/drwcs/`
- `/opt/drwcs/ → /usr/local/drwcs/`

1. Установите новый Сервер Dr.Web (пустой, с новой базой) той же мажорной версии на нужном компьютере в соответствии с инструкцией, описанной в **Руководстве по установке**, Установка Сервера Dr.Web для ОС семейства UNIX.

Если вы планируете переносить старый Сервер Dr.Web с сохранением IP-адреса, назначьте новому Серверу Dr.Web временный IP-адрес, чтобы станции могли взаимодействовать со старым Сервером Dr.Web во время переноса.

2. В веб-интерфейсе нового Сервера Dr.Web перейдите в раздел **Администрирование** → **Менеджер лицензий**, добавьте ключ вашей действующей лицензии `agent.key` и распространите его на группу **Everyone**.
3. Перейдите в раздел **Состояние репозитория** и убедитесь, что репозиторий обновляется без ошибок.

   Если в таблице со списком продуктов в графе **Состояние** имеются сообщения об ошибках, обратитесь в техническую поддержку. К запросу прикрепите файл `drwcsd.log`. Не следует выполнять какие-либо дальнейшие действия из инструкций до получения обратной связи в запросе.

4. Перейдите в раздел **Сервер Dr.Web** и убедитесь, что в этом разделе отображается дата, которая совпадает с датой текущей ревизии Сервера Dr.Web в разделе **Состояние репозитория**. Если дата не совпадает и имеется сообщение о наличии обновлений, нажмите на кнопку **Посмотреть список версий** и обновите Сервер Dr.Web до актуальной версии.
5. Остановите новый Сервер Dr.Web через веб-интерфейс или через консоль с помощью команды:

```
# /etc/init.d/drwcsd stop
```

6. На новом Сервере Dr.Web удалите следующие файлы:
   - файл сертификата `drwcsd-certificate.pem`:

```
# rm /opt/drwcs/webmin/install/windows/drwcsd-certificate.pem
```

   - конфигурационный файл `drwcsd.conf`, файл закрытого ключа `drwcsd.pri` и вторую копию сертификата `drwcsd-certificate.pem`:

```
#
rm /var/opt/drwcs/etc/drwcsd.conf /var/opt/drwcs/etc/drwcsd.pri /var/opt/d
rwcs/etc/drwcsd-certificate.pem
```

   - пользовательские процедуры из каталога `/var/opt/drwcs/extensions/`.
7. Остановите старый Сервер Dr.Web через веб-интерфейс или меню **Пуск** → **Все программы** → **Dr.Web Server** → **Остановить**.
8. Проверьте целостность базы данных на старом Сервере Dr.Web с помощью команды `drwcsd modexecdb database-verify`. Полная командная строка для проверки базы данных будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=trace -log="C:
\Program Files\DrWeb Server\var\verifydb.log" modexecdb database-verify
```

   Если после выполнения этой команды в файле `verifydb.log` появится сообщение об ошибке, обратитесь в техническую поддержку.
9. Выполните экспорт базы данных старого Сервера Dr.Web в файл с помощью команды `drwcsd modexecdb database-export`. Полная командная строка для экспорта будет выглядеть примерно так:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=trace -log="C:
\Program Files\DrWeb Server\var\exportdb.log" modexecdb database-export
<полное_имя_файла>
```

10. Скопируйте следующие файлы со старого Сервера Dr.Web на новый:
    - содержимое каталога `%programfiles%\DrWeb Server\var\extensions` (пользовательские процедуры) старого Сервера Dr.Web в каталог `/var/opt/drwcs/extensions/` нового Сервера Dr.Web;
    - конфигурационный файл `drwcsd.conf`, закрытый ключ `drwcsd.pri` и сертификат `drwcsd-certificate.pem` из каталога `%programfiles%\DrWeb Server\etc` на

старом Сервере Dr.Web в каталог `/var/opt/drwcs/etc/` на новом Сервере Dr.Web.

Проверьте содержимое файла `drwcsd.conf` на предмет наличия путей, свойственных Windows. Если таковые имеются, требуется исправить их вручную перед переносом.

11. Если вы используете встроенную базу данных, замените файл базы данных `database.sqlite` в каталоге `/var/opt/drwcs/` на новом Сервере Dr.Web аналогичным файлом из каталога `%programfiles%\DrWeb Server\var` старого Сервера Dr.Web.
12. Запустите старый Сервер Dr.Web, чтобы он продолжал обслуживать клиентов, с помощью средств управления службами ОС Windows или меню **Пуск** → **Все программы** → **Dr.Web Server** → **Запустить.**
13. На новом Сервере Dr.Web назначьте пользователя `drwcs` владельцем каталога размещения базы данных `/var/opt/drwcs`, а также владельцем файлов `/var/opt/drwcs/etc/drwcsd.pri`, `/var/opt/drwcs/etc/drwcsd.conf` и `/var/opt/drwcs/etc/drwcsd-certificate.pem`:

```
# chown -R drwcs:drwcs /var/opt/drwcs

# chown drwcs:drwcs /var/opt/drwcs/etc/drwcsd*
```

14. Скопируйте сертификат `drwcsd-certificate.pem` в каталог `/opt/drwcs/webmin/install/windows`:

```
# cp /var/opt/drwcs/etc/drwcsd-
certificate.pem /opt/drwcs/webmin/install/windows
```

15. Запустите новый Сервер Dr.Web с помощью команды:

```
# /etc/init.d/drwcsd start
```

16. Войдите в веб-интерфейс нового Сервера Dr.Web с теми же логином и паролем, что и на старом Сервере Dr.Web.
17. Перейдите в раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web** и выберите задание **Backup sensitive data** (Резервное копирование критичных данных). Нажмите на значок  ; в окне для редактирования задания выберите вкладку **Действие**. Убедитесь, что в поле **Путь** не указан путь к каталогу на старом Сервере Dr.Web. Очистите это поле и оставьте это поле пустым (в этом случае для хранения резервных копий будет использоваться каталог по умолчанию — `/var/opt/drwcs/backup`) или укажите путь к каталогу на новом Сервере Dr.Web. Проделайте то же самое с заданием **Backup repository** (Резервное копирование репозитория), а также с иными заданиями с действиями **Резервное копирование критичных данных** и **Резервное копирование репозитория** (при наличии таких заданий).

Если в расписании присутствуют задания с действием **Запуск программы**, отредактируйте их в соответствии с набором ПО, установленного на новом компьютере, или удалите их из расписания.

18. Проверьте работоспособность нового Сервера Dr.Web и обеспечьте подключение к нему станций.
19. Остановите старый Сервер Dr.Web и удалите его (см. **Руководство по установке**, Удаление Сервера Dr.Web для ОС Windows).

**Чтобы проверить работоспособность нового Сервера Dr.Web после переноса**

1. Войдите в веб-интерфейс нового Сервера Dr.Web. Убедитесь, что все Агенты Dr.Web корректно отображаются в списке антивирусной сети.
2. Перейдите в раздел **Администрирование** → **Состояние репозитория** и убедитесь, что репозиторий на новом Сервере Dr.Web обновляется без ошибок. Если в таблице со списком продуктов в графе **Состояние** имеются сообщения об ошибках, обратитесь в техническую поддержку. К запросу прикрепите файл `drwcsd.log`. Не следует выполнять какие-либо дальнейшие действия из инструкций до получения обратной связи в запросе.

**Чтобы обеспечить подключение станций к новому Серверу Dr.Web**

Для возможности перехода Агентов Dr.Web, для которых адрес нового Сервера Dr.Web задается через Центр управления, а не в настройках самого Агента Dr.Web на станции, оставьте включенными оба Сервера Dr.Web до момента завершения процедуры.

В качестве адреса Сервера Dr.Web рекомендуется использовать имя сервера в формате FQDN.

- Если у нового Сервера Dr.Web будет свой IP-адрес:
  a) Для всех Агентов Dr.Web, которых обслуживал старый Сервер Dr.Web, задайте адрес нового Сервера Dr.Web согласно соответствующей процедуре из раздела Подключение Агента Dr.Web к другому Серверу Dr.Web.

  Для Агентов Dr.Web, для которых адрес нового Сервера Dr.Web задавался через Центр управления, а не в настройках самого Агента Dr.Web на станции, на обоих Серверах Dr.Web в настройках Агента Dr.Web должен быть указан адрес нового Сервера Dr.Web.

  b) Дождитесь, пока все Агенты Dr.Web перейдут на новый Сервер Dr.Web.
- Если требуется сохранить для нового Сервера Dr.Web старый IP-адрес:
  a) Остановите старый Сервер Dr.Web.
  b) Назначьте новому Серверу Dr.Web IP-адрес старого Сервера Dr.Web.

c) Перезапустите новый Сервер Dr.Web, чтобы измененные сетевые настройки вступили в силу.

## Подключение Агента Dr.Web к другому Серверу Dr.Web

Подключение Агента Dr.Web к другому Серверу Dr.Web может быть необходимо в случае, если агенты подключены к Серверу Dr.Web, адрес которого изменился, или если Сервер Dr.Web был переустановлен без использования сертификата предыдущего сервера.

Подключение Агента Dr.Web к другому Серверу Dr.Web 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 Dr.Web. При этом необходим доступ к Центрам управления как старого, так и нового Серверов Dr.Web.

2. Непосредственно на самой станции.

   Для выполнения действий непосредственно на самой станции требуются права администратора данной станции и, в случае их изменения через интерфейс агента, права на изменение настроек Агента Dr.Web, устанавливаемые на Сервере Dr.Web (раздел **Антивирусная сеть** → **Конфигурация** → **Права** → вкладка **Общие** → **Изменение конфигурации Агента Dr.Web**). При отсутствии данных прав переподключение к другому Серверу Dr.Web возможно только после удаления установленного агента из Центра управления и установки нового Агента Dr.Web с настройками нового Сервера Dr.Web.

Изменить ряд настроек подключения можно из командной строки от имени администратора станции:

- ОС Windows:

`"%ProgramFiles%\DrWeb\es-service.exe" --esserver=<адрес_сервера> --addcert=<путь_к_сертификату>`

- ОС UNIX:

`drweb-ctl esdisconnect && drweb-ctl esconnect <адрес_сервера> --Certificate <путь_к_сертификату>`

<*адрес_сервера*> — если изменился адрес сервера,

<*путь_к_сертификату*> — если сервер был переустановлен без использования сертификата от предыдущего сервера.

Сертификат сервера доступен в Центре управления, в разделе **Администрирование** → **Ключи шифрования**.

**Чтобы переключить Агент Dr.Web на другой Сервер Dr.Web при помощи Центра управления**

1. На новом Сервере Dr.Web 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 Dr.Web.

   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 Dr.Web, к которому подключен Агент Dr.Web, задайте параметры нового Сервера Dr.Web. 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 Dr.Web не совпадает с сертификатом старого Сервера Dr.Web, в поле **Сертификат** задайте путь до сертификата нового Сервера Dr.Web.
   b) В поле **Сервер** задайте адрес нового Сервера Dr.Web.

   В качестве адреса Сервера Dr.Web рекомендуется использовать имя сервера в формате FQDN.

   c) Нажмите кнопку **Сохранить**.

**Чтобы переключить Агент Dr.Web на другой Сервер Dr.Web непосредственно на самой станции**

1. В настройках Агента Dr.Web задайте параметры нового Сервера Dr.Web. Для этого через контекстное меню значка Агента Dr.Web откройте **Центр безопасности** → нажмите на замок  , если он еще не открыт, для доступа к расширенным настройкам → кнопка  для доступа к настройкам → пункт **Сервер** → кнопка **Изменить настройки**:
   a) Если сертификат нового Сервера Dr.Web не совпадает с сертификатом старого Сервера Dr.Web, по кнопке **Список сертификатов** задайте путь до сертификата нового Сервера Dr.Web.

b) По кнопке **Добавить** задайте соответствующие параметры нового Сервера Dr.Web.

2. Переведите станцию в новички (сбросьте параметры авторизации на Сервере Dr.Web). 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 Dr.Web, вы можете указать их в полях **ID станции** и **Пароль**. При этом нет необходимости переводить станцию в новички.

## Нагрузка на Сервер Dr.Web и рекомендуемые параметры настройки

При использовании внешней базы данных в антивирусных сетях большого размера для обеспечения работоспособности Сервера Dr.Web может потребоваться изменить значения следующих параметров:

- **Администрирование** → **Конфигурация Сервера Dr.Web** → **База данных** → **Количество соединений** (параметр `database connections=""` в конфигурационном файле Сервера Dr.Web) — максимально допустимое количество соединений Сервера Dr.Web с базой данных.
- **Администрирование** → **Конфигурация Сервера Dr.Web** → **Общие** → **Количество параллельных запросов от клиентов** (параметр `threads count=""` в конфигурационном файле Сервера Dr.Web) — количество потоков для обработки данных, поступающих от клиентов: Агентов Dr.Web, инсталляторов Агентов, соседних Серверов Dr.Web, Прокси-серверов Dr.Web.

Данные параметры влияют на производительность Сервера Dr.Web. Не меняйте их значения без необходимости. Чтобы определить потребность в их изменении, обратитесь к таблице взаимосвязей между размерами антивирусной сети, аппаратными возможностями Сервера Dr.Web и оптимальными значениями параметров:

| Количество подключений клиентов к Серверу Dr.Web | Количество ядер процессора Сервера Dr.Web | Количество соединений с базой данных (database connections) | Количество параллельных запросов от клиентов (threads count) |
|---|---|---|---|
| до 500 | 2 | 2 (значение по умолчанию) | 5 (значение по умолчанию) |
| 500–1500 | 3–5 | 3–5 | 6–10 |
| более 1500 | 5–8 | 5–8 | 10–14 |

Значение параметра **Количество параллельных запросов от клиентов** (`threads count`) не должно превышать количество ядер процессора на компьютере, выполняющем функции Сервера Dr.Web, более чем в два раза.

---

При использовании встроенной базы данных менять значения по умолчанию не рекомендуется.

При работе в сети с большим количеством подключений перед изменением значений приведенных параметров рекомендуется получить консультацию в службе технической поддержки компании «Доктор Веб».

# Увеличение дискового пространства для нужд Сервера Dr.Web

В каталоге Сервера Dr.Web `/var/opt/drwcs/` в ОС Linux и `/var/drwcs/` в ОС FreeBSD (далее в этом разделе — **var**) хранятся резервные копии базы данных, основные конфигурационные файлы компонентов антивирусной сети, репозиторий установочных пакетов и другие необходимые файлы. В процессе работы Сервера Dr.Web размер данного каталога может существенно увеличиться. В случае ограниченного свободного пространства на диске установки Сервера Dr.Web рекомендуется смонтировать данный каталог на отдельный диск. Это можно выполнить как при первичной установке Сервера Dr.Web, так и после его установки.

В инструкциях ниже приведены примеры команд для ОС Linux. Обратите внимание, что пути для ОС FreeBSD отличаются:

- `/var/opt/drwcs/ → /var/drwcs/`
- `/etc/init.d/ → /usr/local/etc/rc.d/`

## При первичной установке Сервера Dr.Web

Чтобы избежать потенциальных проблем с нехваткой дискового пространства, до установки Сервера Dr.Web следует предварительно смонтировать новый диск как каталог **var**.

### Чтобы смонтировать новый диск как каталог var в ОС Linux

1. Создайте каталог **var**:

   ```
   # mkdir /var/opt/drwcs/
   ```

2. Смонтируйте новый диск (например, `/dev/sdXY`) в каталог **var**:

   ```
   # mount /dev/sdXY /var/opt/drwcs/
   ```

   где `/var/opt/drwcs/` — точка монтирования нового диска.

3. При необходимости внесите соответствующие изменения в файл `/etc/fstab`.

После выполнения этих шагов установите Сервер Dr.Web согласно инструкции, приведенной в **Руководстве по установке** в разделе Установка Сервера Dr.Web для ОС семейства UNIX.

## После установки Сервера Dr.Web

Во избежание нехватки дискового пространства на диске установки Сервера Dr.Web каталог **var** можно перенести на отдельный диск.

### Чтобы перенести каталог var на отдельный диск в ОС Linux

1. Остановите Сервер Dr.Web с помощью команды:

```
# /etc/init.d/drwcsd stop
```

2. Создайте новый каталог, куда в дальнейшем будет скопировано содержимое каталога **var**, например:

```
# mkdir /mnt/var/opt/drwcs/
```

3. Смонтируйте новый диск (например, `/dev/sdXY`) в созданный каталог:

```
# mount /dev/sdXY /mnt/var/opt/drwcs/
```

где `/mnt/var/opt/drwcs/` — точка монтирования нового диска.

4. Скопируйте содержимое каталога **var** на примонтированный диск:

```
#cp -apx /var/opt/drwcs/* /mnt/var/opt/drwcs/
```

5. Удалите содержимое исходного каталога **var**:

```
# rm -R /var/opt/drwcs/*
```

6. Отмонтируйте диск, смонтированный в созданный каталог:

```
# umount /dev/sdXY
```

7. Примонтируйте диск в каталог **var**:

```
# mount /dev/sdXY /var/opt/drwcs/
```

8. Назначьте для каталога **var** права пользователя `drwcs`, входящего в группу `drwcs`:

```
# chown -R drwcs:drwcs /var/opt/drwcs
```

9. Запустите Сервер Dr.Web:

```
# /etc/init.d/drwcsd start
```

10. При необходимости внесите соответствующие изменения в файл `/etc/fstab`.

# Смена типа базы данных

## Для ОС Windows

Процедура запуска и завершения работы Сервера Dr.Web описана в **Руководстве администратора**, в п. Запуск и завершение работы Сервера Dr.Web.

1. Остановите службу Сервера Dr.Web.
2. Запустите из командной строки файл `drwcsd.exe` с ключом `modexecdb database-export` 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=trace -log="C:\Program Files\DrWeb Server\var\exportdb.log"
   modexecdb database-export 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 Dr.Web на использование другой БД. Откажитесь от предложения перезапустить Сервер Dr.Web.
4. Остановите службу Сервера Dr.Web.
5. Переместите файл базы данных в какой-либо временный каталог, пока не убедитесь, что смена типа БД прошла успешно.
6. Запустите из командной строки файл `drwcsd.exe` с ключом `modexecdb database-init` для инициализации новой базы данных. Строка инициализации базы данных для версии Сервера Dr.Web 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="C:\Program Files\DrWeb Server\var\initdb.log"
   modexecdb database-init
   ```

   Подразумевается, что Сервер Dr.Web установлен в каталоге `"C:\Program Files\DrWeb Server"`.

7. Запустите из командной строки файл `drwcsd.exe` с ключом `modexecdb database-import` 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=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import 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 Dr.Web с ключом `modexecdb database-export` для экспорта содержимого базы данных в файл. Командная строка из каталога установки Сервера Dr.Web будет выглядеть примерно так:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd modexecdb database-export /var/opt/drwcs/esbase.es
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-export /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 Dr.Web на использование другой БД: в меню **Администрирование** → пункт **Конфигурация Сервера Dr.Web** → вкладка **База данных**.

Перенастройку Сервера Dr.Web на использование другой БД также можно осуществить, отредактировав напрямую конфигурационный файл Сервера Dr.Web `drwcsd.conf`. Для этого следует закомментировать/удалить запись о текущей БД и прописать новую базу (подробнее см. E1. Конфигурационный файл Сервера Dr.Web).

Откажитесь от предложения перезапустить Сервер Dr.Web.

4. Остановите Сервер Dr.Web (см. шаг **1**).
5. Переместите файл базы данных в какой-либо временный каталог, пока не убедитесь, что смена типа БД прошла успешно.
6. Запустите файл `drwcsd` с ключом `modexecdb database-init` для инициализации новой базы данных. Строка инициализации будет выглядеть примерно так:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd modexecdb database-init
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-init
```

7. Запустите файл `drwcsd` с ключом `modexecdb database-import` для импорта содержимого базы данных из файла. Командная строка для импорта будет выглядеть примерно так:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd modexecdb database-import /var/opt/drwcs/esbase.es
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import /var/drwcs/esbase.es
```

8. Запустите Сервер Dr.Web (см. шаг **3**).

Если при запуске скрипта Сервера Dr.Web требуется задать параметры (например, указать каталог установки Сервера Dr.Web, 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

В процессе работы Сервер Dr.Web регулярно сохраняет резервные копии важной информации: лицензионных ключей, содержимого базы данных, закрытого ключа шифрования, конфигурации Сервера Dr.Web 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 Dr.Web 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 Dr.Web при помощи команды `modexecdb database-import` 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**).

Восстановить базу данных можно только из резервной копии, созданной при помощи Сервера Dr.Web с той же мажорной версией, что и версия Сервера Dr.Web, на котором происходит восстановление. Например, БД из резервной копии, созданной при помощи Сервера Dr.Web версии 13, можно восстановить, используя Сервер Dr.Web только версии 13.

**Если во время обновления Сервера Dr.Web до версии 13 с более ранних версий по каким-либо причинам была повреждена БД, выполните следующее:**

1. Удалите Сервер Dr.Web версии 13. При этом будут автоматически сохранены резервные копии файлов, используемых Сервером Dr.Web.
2. Установите Сервер Dr.Web 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 Dr.Web кроме файла базы данных.

   В процессе установки Сервера Dr.Web создайте новую базу данных.

3. Восстановите базу данных из резервной копии по общим правилам (см. ниже).
4. В настройках Сервера Dr.Web отключите протоколы Агента Dr.Web, Сервера Dr.Web 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 Dr.Web до версии 13 по общим правилам (см. в **Руководстве администратора** п. Глава 11: Обновление компонентов Dr.Web Enterprise Security Suite в процессе работы).
6. Включите протоколы Агента Dr.Web, Сервера Dr.Web и Сетевого инсталлятора, отключенные на шаге 4.

## Восстановление БД под ОС Windows

Процедура запуска и завершения работы Сервера Dr.Web описана в **Руководстве администратора**, в п. Запуск и завершение работы 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=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import "<путь_к_бэкап_файлу>\database.gz"
```

   Данная команда тоже должна быть набрана в одну строку. В примере подразумевается, что Сервер Dr.Web 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. Произведите инициализацию новой базы данных.
   - При использовании встроенной БД:
     a) Переместите файл базы данных `database.sqlite` в какой-либо временный каталог, пока не убедитесь, что восстановление БД прошло успешно.
     b) Строка инициализации базы данных в версии Сервера Dr.Web 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="C:\Program Files\DrWeb Server\var\initdb.log"
modexecdb database-init
```

Данная команда должна быть набрана в одну строку (см. также формат команды `drwcsd` с ключом `modexecdb database-init` в Приложении Ж3.3. Команды для управления базой данных). В примере подразумевается, что Сервер Dr.Web установлен в каталоге `C:\Program Files\DrWeb Server`.

c) После выполнения этой команды в подкаталоге `var` каталога установки Сервера Dr.Web должен появиться новый файл базы `database.sqlite`.

- При использовании внешней БД:

a) экспортируйте файл базы данных в какой-либо временный каталог, пока не убедитесь, что восстановление БД прошло успешно.

b) произведите очистку БД при помощи команды `modexecdb database-clean` (см. Приложение Ж3.3. 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=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import "<путь_к_бэкап_файлу>\database.gz"
```

Данная команда тоже должна быть набрана в одну строку. В примере подразумевается, что Сервер Dr.Web установлен в каталоге `C:\Program Files\DrWeb Server`.

4. Запустите службу Сервера Dr.Web.

## Восстановление БД под 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. Переместите файл базы данных в какой-либо временный каталог, пока не убедитесь, что восстановление БД прошло успешно. Файл базы данных `database.sqlite` находится в 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 `modexecdb database-clean` (см. Приложение Ж3.3. Команды для управления базой данных).

3. Инициализируйте базу данных Сервера Dr.Web. Для этого служит следующая команда:
   - для ОС **Linux**:

```
/etc/init.d/drwcsd modexecdb database-init
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-init
```

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 modexecdb database-import
"<путь_к_бэкап_файлу>/database.gz"
```

   - для ОС **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import
"<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 Dr.Web требуется задать параметры (например, указать каталог установки Сервера Dr.Web 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 Dr.Web, 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 Dr.Web были установлены после создания последней резервной копии, они не смогут подключиться к Серверу Dr.Web 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 Dr.Web.

После того как все станции благополучно подключатся к новому Серверу Dr.Web, измените данные настройки Сервера Dr.Web на настройки, принятые в соответствии с политикой вашей компании.

---

После восстановления базы рекомендуется подключиться к Серверу Dr.Web через Центр управления, открыть раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web** и проверить в нем наличие задания **Резервное копирование критичных данных Сервера Dr.Web**. Если такое задание отсутствует, рекомендуется его создать.

# Обновление Агентов Dr.Web на серверах ЛВС

При обновлении Агентов Dr.Web, установленных на серверах ЛВС, могут быть нежелательны перезагрузки станций или завершение работы сетевого ПО, работающего на таких станциях.

Во избежание функционального простоя станций, выполняющих важные функции ЛВС, предлагается следующий режим обновления Агентов Dr.Web и антивирусного ПО:

1. В расписании Сервера Dr.Web 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 Dr.Web 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.

# Использование DFS при установке Агента Dr.Web 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 DFS 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 Dr.Web 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 Dr.Web 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 Dr.Web 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 Dr.Web при помощи команды `modexecdb database-import-and-upgrade` 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**).

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 Dr.Web. В случае утраты лицензионных ключей их можно запросить заново, как указано в **Руководстве администратора**, п. Лицензирование.

**Чтобы восстановить Сервер Dr.Web после отказа, если сохранилась резервная копия данных Сервера Dr.Web**

1. Выберите компьютер, на который будет устанавливаться новый Сервер Dr.Web. Изолируйте данный компьютер от работающих Агентов Dr.Web: отключите его от сети, в которой установлены Агенты Dr.Web, 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 Dr.Web и распространите его на соответствующие группы, в частности на группу **Everyone**. Шаг обязателен, если при установке Сервера Dr.Web не был задан лицензионный ключ.
4. Обновите репозиторий установленного Сервера Dr.Web 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 Dr.Web произведите обновление до последней версии:
   a) Откройте раздел Центра управления **Администрирование** → **Сервер Dr.Web**.
   b) Для перехода к списку версий Сервера Dr.Web нажмите на текущую версию Сервера Dr.Web или на кнопку **Список версий**. Откроется раздел **Обновления Сервера Dr.Web** со списком доступных обновлений и резервных копий Сервера Dr.Web.
   c) Для перехода к новой версии Сервера Dr.Web установите флаг напротив последней версии в списке **Все версии**. Нажмите кнопку **Применить**.
   d) Дождитесь завершения процесса обновления Сервера Dr.Web.
6. Остановите Сервер Dr.Web.
7. Замените критичные данные Сервера Dr.Web на данные, полученные из резервной копии:

| **Операционная система** | **Конфигурационные файлы** |
|---|---|
| Windows | `etc` в каталоге установки Сервера Dr.Web |
| Linux | `/var/opt/drwcs/etc` |
| FreeBSD | `/var/drwcs/etc` |

8. Настройте базу данных.
   a) Внешняя база данных:

   Дальнейших действий по подключению базы данных к Серверу Dr.Web не требуется (при условии, что сохранен конфигурационный файл Сервера Dr.Web).

Если версия Сервера Dr.Web, установленная из последних обновлений, позднее версии утраченного Сервера Dr.Web, произведите обновление внешней базы данных при помощи команды `modexecdb database-upgrade`:

- для ОС Windows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=all -log="C:
\Program Files\DrWeb Server\var\upgradedb.log" modexecdb database-
upgrade
```

- для ОС Linux:

```
/etc/init.d/drwcsd modexecdb database-upgrade
```

- для ОС FreeBSD:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-upgrade
```

b) Резервная копия базы данных внешней или встроенной:

При использовании внешней базы данных предварительно произведите ее очистку при помощи команды `modexecdb database-clean` (см. Приложение Ж3.3. Команды для управления базой данных).

Импортируйте базу данных из соответствующего файла резервной копии с обновлением формата базы данных до версии установленного Сервера Dr.Web при помощи команды `modexecdb database-import-and-upgrade`:

- 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=trace -log="C:\Program Files\DrWeb
Server\var\importupgradedb.log" modexecdb database-import-and-upgrade
"<путь_к_бэкап_файлу>\database.gz"
```

- для ОС Linux:

```
/etc/init.d/drwcsd modexecdb database-import-and-upgrade
"<путь_к_бэкап_файлу>/database.gz"
```

- для ОС FreeBSD:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import-and-upgrade
"<путь_к_бэкап_файлу>/database.gz"
```

На все замененные файлы Сервера Dr.Web необходимо установить те же системные права, что были выбраны при предыдущей (утраченной) установке Сервера Dr.Web.

Для ОС семейства UNIX: `rw` для `drwcs:drwcs`.

9. Запустите Сервер Dr.Web.

10. Убедитесь в сохранности и актуальности данных, полученных из резервной копии базы данных: настроек Агентов Dr.Web, состояния дерева антивирусной сети и т. п.
11. Восстановите доступность Сервера Dr.Web для Агентов Dr.Web, исходя из способа изоляции Сервера Dr.Web, выбранного на шаге 1.

Если какие-либо Агенты Dr.Web были установлены после создания последней резервной копии, они не смогут подключиться к Серверу Dr.Web 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 Dr.Web.

После того как все станции благополучно подключатся к новому Серверу Dr.Web, измените данные настройки Сервера Dr.Web, 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. Восстанавливать подключение к серверу можно как на тот же компьютер (с тем же адресом), так и на другой (изменив в настройках Агентов Dr.Web адрес для подключения к Серверу Dr.Web).

   Для того чтобы можно было выполнить первоначальные настройки Сервера Dr.Web и антивирусной сети перед подключением Агентов Dr.Web, изолируйте данный компьютер от работающих Агентов Dr.Web: при установке временно измените порт на отличный от дефолтного порта 2193 (позже его можно будет изменить обратно на дефолтный). После первоначальной настройки проверьте подключение к Серверу Dr.Web на примере одного-двух Агентов Dr.Web.

   Возможно восстанавливать Сервер как на тот же компьютер (с тем же адресом), так и на другой, изменив в настройках Агентов Dr.Web адрес для подключения к серверу.
2. Установите новый Сервер Dr.Web.
3. В разделе **Администрирование** → **Менеджер лицензий** добавьте лицензионный ключ от предыдущей установки Сервера Dr.Web и распространите его на соответствующие группы, в частности на группу **Everyone**. Шаг обязателен, если при установке Сервера Dr.Web не был задан лицензионный ключ.
4. Обновите репозиторий установленного Сервера Dr.Web 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 Dr.Web произведите обновление до последней версии:
   a) Откройте раздел Центра управления **Администрирование** → **Сервер Dr.Web**.
   b) Для перехода к списку версий Сервера Dr.Web нажмите на текущую версию Сервера Dr.Web или на кнопку **Список версий**. Откроется раздел **Обновления Сервера Dr.Web** со списком доступных обновлений и резервных копий Сервера Dr.Web.
   c) Для перехода к новой версии Сервера Dr.Web установите флаг напротив последней версии в списке **Все версии**. Нажмите кнопку **Сохранить**.
   d) Дождитесь завершения процесса обновления Сервера Dr.Web.
6. Измените настройки подключения станций в конфигурации Сервера Dr.Web:
   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 Dr.Web.
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 Dr.Web и настройки Сервера Dr.Web (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 Dr.Web для Агентов Dr.Web, исходя из способа изоляции Сервера Dr.Web, выбранного на шаге 1.
11. Замените сертификат на всех станциях сети, которые должны будут подключиться к новому Серверу Dr.Web. Скачать сертификат можно в разделе **Администрирование** → **Ключи шифрования**.
    - При включенной самозащите скопируйте на станцию сертификат, созданный при установке нового Сервера Dr.Web, и выполните следующую команду:

      `%ProgramFiles%\DrWeb\es-service.exe -c <`*сертификат*`>`

      или

      `%ProgramFiles%\DrWeb\es-service.exe --addcert=<`*сертификат*`>`

      В качестве <*сертификат*> укажите путь к скопированному сертификату сервера.

      В результате сертификат будет скопирован в каталог установки Агента Dr.Web. По умолчанию это каталог `%ProgramFiles%\DrWeb` (подробнее см. Приложение Ж2. Агент Dr.Web для Windows).

- Если на станции отключена самозащита, можете взять сертификат, созданный при установке нового Сервера Dr.Web, и разместить его в указанный выше каталог.

12. Если вы восстанавливали подключение к Серверу Dr.Web на другой компьютер, измените адрес для подключения к серверу в настройках Агентов Dr.Web.

Для выполнения действий непосредственно на самой станции требуются права администратора данной станции и, в случае их изменения через интерфейс Агента Dr.Web, право на изменение настроек Агента Dr.Web, устанавливаемое на Сервере Dr.Web (раздел **Антивирусная сеть** → **Конфигурация** → **Права** → вкладка **Общие** → **Изменение конфигурации Агента Dr.Web**). При отсутствии данных прав переподключение к другому Серверу Dr.Web возможно только после удаления установленного Агента Dr.Web из Центра управления и установки нового Агента Dr.Web с настройками нового Сервера Dr.Web.

В качестве адреса Сервера Dr.Web рекомендуется использовать имя сервера в формате FQDN.

13. После того как все станции благополучно подключатся к новому Серверу Dr.Web, измените настройки Сервера Dr.Web, заданные на шаге 6, на настройки, принятые в соответствии с политикой вашей компании.

## Восстановление узла кластера Серверов Dr.Web

Если один из Серверов Dr.Web кластера по какой-либо причине не работает, Агенты Dr.Web, потерявшие соединение с ним, подключатся к другому узлу кластера. В случае фатального отказа Сервера Dr.Web необходимо его восстановить: установить ПО Сервера Dr.Web и добавить его заново в кластер.

### Установка Сервера Dr.Web для последующего добавления его в кластер

Для возможности работы с одной базой данных все Серверы Dr.Web должны быть одинаковой версии.

Вы можете воспользоваться резервной копией вышедшего из строя Сервера Dr.Web при ее наличии для упрощения процедуры восстановления узла кластера. Резервная копия содержит настройки репозитория, конфигурационные файлы, ключи шифрования, сертификаты, резервную копию внутренней базы данных.

При установке Сервера Dr.Web на замену вышедшему из строя узлу кластера придерживайтесь предписаний ниже.

#### Установка Сервера на ОС семейства UNIX

Следуйте инструкциям из **Руководства по установке**, раздела Установка Сервера Dr.Web для ОС семейства UNIX. Вы можете установить новый Сервер Dr.Web или

воспользоваться резервной копией вышедшего из строя Сервера Dr.Web, входившего в кластер.

По умолчанию резервные копии хранятся в следующих каталогах:

- для Сервера Dr.Web под ОС Linux — `/var/opt/drwcs/backup`,
- для Сервера Dr.Web под ОС FreeBSD — `/var/drwcs/backup`.

Установленный из резервной копии Сервер Dr.Web будет использовать общую базу данных, к которой обращаются узлы кластера.

При установке без использования резервной копии Сервер Dr.Web будет использовать встроенную базу данных. После завершения процесса установки необходимо будет переключить Сервер Dr.Web на общую базу данных, используемую кластером.

### Установка Сервера Dr.Web на ОС Windows

Вы можете установить новый Сервер Dr.Web или воспользоваться резервной копией вышедшего из строя Сервера Dr.Web, входившего в кластер. По умолчанию резервные копии хранятся в каталоге <*диск_установки*>`:\DrWeb Backup`.

Следуйте инструкциям из **Руководства по установке**, раздела Установка Сервера Dr.Web для ОС Windows, обращая внимание на следующие моменты:

- Установка с подключением к внешней базе данных не рекомендуется, поскольку при подключении Сервера Dr.Web к кластеру возможна потеря данных, хранящихся в базе.
- При установке из резервной копии укажите следующие параметры конфигурации:
  - **Драйвер базы данных**: выберите опцию **SQLite (встроенная база данных)**. Оставлять внешнюю базу данных не рекомендуется, поскольку это может привести к потере данных при подключении Сервера Dr.Web к кластеру. Подключить внешнюю базу данных, используемую в кластере, необходимо уже после завершения установки Сервера Dr.Web.
  - **Конфигурация сети**: укажите актуальные значения полей **Интерфейс** и **Порт**. Если флаг **Включить службу обнаружения Сервера Dr.Web** не установлен, установите его, чтобы Сервер Dr.Web мог обмениваться информацией с другими узлами кластера при помощи multicast-группы. Ниже укажите параметры multicast-группы, используемой Серверами Dr.Web в кластере.

  Для остальных параметров значения могут быть установлены согласно разделу **Установка Сервера Dr.Web для ОС Windows**.
- При установке нового Сервера Dr.Web укажите следующие параметры конфигурации:
  - **Конфигурация Сервера Dr.Web**: укажите пути к конфигурационному файлу `drwcsd.conf` и закрытому ключу шифрования, использовавшимся вышедшим из строя Сервером Dr.Web, при их наличии. В ином случае оставьте поля незаполненными, чтобы создать новые ключи шифрования, сертификат и конфигурационный файл с настройками по умолчанию. Значения этих параметров необходимо будет изменить после установки Сервера Dr.Web.

- **Драйвер базы данных**: выберите опцию **SQLite (встроенная база данных)**. Подключить внешнюю базу данных, используемую в кластере, необходимо уже после завершения установки Сервера Dr.Web.
- **Конфигурация сети**: укажите актуальные значения полей **Интерфейс** и **Порт**. Установите флаг **Включить службу обнаружения Сервера Dr.Web**, чтобы Сервер Dr.Web мог обмениваться информацией с другими узлами кластера при помощи multicast-группы. Ниже укажите параметры multicast-группы, используемой Серверами Dr.Web в кластере.

Для остальных параметров значения могут быть установлены согласно разделу **Установка Сервера Dr.Web для ОС Windows**.

### Введение Сервера Dr.Web в кластер

Чтобы подключить установленный Сервер Dr.Web к кластеру, следуйте предписаниям, приведенным в **Руководстве администратора**, в разделе Кластер Серверов Dr.Web.

## Управление уровнем ведения журнала Сервера Dr.Web под ОС Windows

**Изменить уровень детализации журнала Сервера Dr.Web 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 Dr.Web, 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 Dr.Web при помощи ключа `--verbosity`.

  Подробная информация по ключам командной строки для управления Сервером Dr.Web приведена в разделе Ж3.8. Описание ключей.

  Пример команды для установки уровня ведения журнала **Трассировка**:

  ```
  drwcsd --daemon "--home=C:\Program Files\DrWeb Server" "--bin-root=C:
  \Program Files\DrWeb Server" "--var-root=C:\Program Files\DrWeb Server\var"
  --verbosity=trace --log="C:\Program Files\DrWeb Server\var\install.log" --
  rotate=10,50m install
  ```

Остальные ключи являются обязательными, в частности, если были переопределены стандартные пути установки Сервера Dr.Web и его рабочих каталогов.

После изменения уровня ведения журнала необходимо перезапустить Сервер Dr.Web:

```
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** → **Dr.Web Server** → **Детальный журнал** или **Программы** → **Dr.Web Server** → **Стандартный журнал**

  b) **Программы** → **Dr.Web Server** → **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 Mobile Security Suite (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:
   - Если на мобильном устройстве пользователя включены провайдеры местоположения (GPS, мобильные сети) и сигнал стабилен, определение местоположения осуществляется средствами самого мобильного устройства.
   - 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/.

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.

# 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. Значение всех параметров по умолчанию — **Отключено**.

# Категории критериев функционального анализа

## Запуск приложений

Включает контроль запускаемых процессов для списка доверенных 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 программ взлома.*

  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 сертификатами (поврежденными или прикрепленными к бинарному файлу, чтобы не дать определить угрозу - например, сертификатами легального ПО). Также это может помочь при попытках модифицировать легальный файл или заразить вирусом. 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 самоподписанными сертификатами.*

  Блокирует нелицензионное ПО, которое может оказаться вредоносным. Вредоносные программы могут добавлять к своим бинарным файлам поддельную подпись с известным именем (например, Microsoft) и/или добавлять в систему корневой сертификат, чтобы данный файл показывался и распознавался ОС как легально подписанный.

- *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 на 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.

Исключения из блокировок выше:

- *Разрешать запуск системных приложений и приложений от компании Microsoft.*

- *Разрешать запуск приложений, известных/доверенных «Доктор Веб»*.

  Если включено, то разрешена работа приложений, которые подписаны доверенным сертификатом.

  

  Если данная опция включена, то разрешается работа приложений, которые подписаны доверенным сертификатом. Данная функция позволяет не создавать излишнее количество правил, основываясь на уже проверенных Dr.Web данных. Доверие в данном случае основывается на криптографии, обширной и постоянно пополняющейся базе.

## Загрузка и исполнение модулей

Включает контроль загружаемых модулей. Критерии могут работать в двух режимах:

- *Контролировать загрузку и исполнение всех модулей*.

  Глобальная опция, которая включает контроль модулей для доверенных приложений. 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. В данном режиме вы можете:

  - *Запрещать загрузку и исполнение модулей, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для рекламных программ*.

    Блокирует запуск модулей, которые могут распространять рекламу.

  - *Запрещать загрузку и исполнение модулей, подписанных сертификатами, известными в «Доктор Веб» как серые*.

    Блокирует запуск модулей, которые подписаны "серыми" сертификатами. Такие сертификаты часто используются для подписи небезопасных приложений.

  - *Запрещать загрузку и исполнение модулей, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для программ взлома*.

    Блокирует запуск модулей, которые подписаны сертификатами, использующимися для взлома программ. Использование данного критерия рекомендовано.

  - *Запрещать загрузку и исполнение модулей, подписанных поддельными/поврежденными сертификатами*.

    Блокирует запуск вредоносных модулей, которые подписаны недействительными сертификатами (поврежденными или прикрепленными к бинарному файлу, чтобы не дать определить угрозу - например, сертификатами легального ПО). Также это может помочь при попытках модифицировать легальный файл или заразить вирусом. Использование данного критерия рекомендовано.

- *Запрещать загрузку и исполнение модулей, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для вредоносных программ.*

  Блокирует запуск модулей, которые подписаны скомпрометированными сертификатами. Использование данного критерия рекомендовано.

- *Запрещать загрузку и исполнение модулей, подписанных отозванными сертификатами.*

  Блокирует запуск модулей, которые подписаны украденными или скомпрометированными сертификатами. Использование данного критерия рекомендовано, так как он позволяет превентивно пресекать запуск потенциально вредоносных приложений.

- *Запрещать загрузку и исполнение модулей, подписанных самоподписанными сертификатами.*

  Блокирует нелицензионное ПО, которое может оказаться вредоносным. Вредоносные программы могут добавлять к своим бинарным файлам поддельную подпись с известным именем (например, Microsoft) и/или добавлять в систему корневой сертификат, чтобы данный файл показывался и распознавался ОС как легально подписанный.

- *Запрещать загрузку и исполнение неподписанных модулей.*

  Блокирует запуск потенциально вредоносных и ненадежных модулей, источник происхождения которых неизвестен.

- *Запрещать загрузку и исполнение модулей из альтернативных потоков NTFS (ADS).*

  Модули из альтернативных потоков NTFS (ADS) зачастую являются вредоносными, поэтому использование данного критерия является обязательным.

- *Запрещать загрузку и исполнение модулей из сети и общих ресурсов.*

  Запуск модулей из сети и общих ресурсов является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.

- *Запрещать загрузку и исполнение модулей со сменных носителей.*

  Запуск модулей со сменных носителей является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.

- *Запрещать загрузку и исполнение модулей из временных каталогов.*

  Блокирует запуск модулей из временных каталогов.

- *Запрещать загрузку и исполнение модулей с двойным/нетипичным расширением.*

  Блокирует запуск подозрительных модулей с нестандартным расширением (например, *.jpg.exe).

Исключения из блокировок выше:

- *Разрешать загрузку и исполнение системных модулей и модулей от компании Microsoft.*
- *Разрешать загрузку и исполнение модулей, известных/доверенных «Доктор Веб».*

Если включено, разрешена работа модулей, подписанных доверенным сертификатом.

## Запуск скриптовых интерпретаторов

Включает контроль запускаемых скриптовых сценариев для списка доверенных приложений.

- *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).*

  Приложения из альтернативных потоков NTFS (ADS) зачастую являются вредоносными, поэтому использование данного критерия является обязательным.

- *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.

- *Запрещать запуск сценариев из временных каталогов.*

  Блокирует запуск сценариев из временных каталогов.

Исключения из блокировок выше:

- *Разрешать запуск системных сценариев и сценариев от компании Microsoft.*
- *Разрешать запуск сценариев, известных/доверенных «Доктор Веб».*

  Если включено, разрешен запуск сценариев, подписанных доверенным сертификатом.

## Загрузка драйверов

Включает контроль загружаемых драйверов для списка доверенных приложений.

- *Запрещать загрузку драйверов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для рекламных программ.*

  Блокирует запуск драйверов, которые могут распространять рекламу.

- *Запрещать загрузку драйверов, подписанных сертификатами, известными в «Доктор Веб» как серые.*

  Блокирует запуск драйверов, которые подписаны "серыми" сертификатами. Такие сертификаты часто используются для подписи небезопасных приложений.

- *Запрещать загрузку драйверов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для программ взлома.*

  Блокирует запуск драйверов, которые подписаны сертификатами, использующимися для взлома программ. Использование данного критерия рекомендовано.

- *Запрещать загрузку драйверов, подписанных поддельными/поврежденными сертификатами.*

  Блокирует запуск вредоносных драйверов, которые подписаны недействительными сертификатами (поврежденными или прикрепленными к бинарному файлу, чтобы не дать определить угрозу - например, сертификатами легального ПО). Также это может помочь при попытках модифицировать легальный файл или заразить вирусом. Использование данного критерия рекомендовано.

- *Запрещать загрузку драйверов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для вредоносных программ.*

  Блокирует запуск драйверов, которые подписаны скомпрометированными сертификатами. Использование данного критерия рекомендовано.

- *Запрещать загрузку драйверов, подписанных отозванными сертификатами.*

  Блокирует запуск драйверов, которые подписаны украденными или скомпрометированными сертификатами. Использование данного критерия рекомендовано, так как он позволяет превентивно пресекать запуск потенциально вредоносных приложений.

- *Запрещать загрузку драйверов, подписанных самоподписанными сертификатами.*

  Блокирует нелицензионное ПО, которое может оказаться вредоносным. Вредоносные программы могут добавлять к своим бинарным файлам поддельную подпись с известным именем (например, Microsoft) и/или добавлять в систему корневой сертификат, чтобы данный файл показывался и распознавался ОС как легально подписанный.

- *Запрещать загрузку неподписанных драйверов.*

  Блокирует запуск потенциально вредоносных и ненадежных драйверов, источник происхождения которых неизвестен.

- *Запрещать загрузку драйверов из альтернативных потоков NTFS (ADS).*

Приложения из альтернативных потоков NTFS (ADS) зачастую являются вредоносными, поэтому использование данного критерия является обязательным.

- *Запрещать загрузку драйверов из сети и общих ресурсов.*

  Загрузка драйверов из сети и общих ресурсов является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.

- *Запрещать загрузку драйверов со сменных носителей.*

  Загрузка драйверов со сменных носителей является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.

- *Запрещать загрузку драйверов из временных каталогов.*

  Блокирует запуск драйверов из временных каталогов.

- *Запрещать загрузку уязвимых версий драйверов популярного ПО.*

  Блокирует загрузку небезопасных версий драйверов популярного ПО. Драйвера легального ПО, например, VirtualBox, Asus и т.п., могут быть использованы для проникновения в систему через RDP. При включении этой опции небезопасные версии этих драйверов будут блокироваться при загрузке.

  

  Запрет на загрузку уязвимых версий драйверов популярного ПО не может быть перекрыт исключениями.

- *Запрещать запуск драйверов с двойным / не типичным расширением.*

  Блокирует запуск подозрительных драйверов с нестандартным расширением (например, *.jpg.exe).

Исключения из блокировок выше:

- *Разрешать загрузку системных драйверов и драйверов от компании Microsoft.*
- *Разрешать загрузку драйверов, известных/доверенных «Доктор Веб».*

  Если включено, то разрешена загрузка драйверов, которые подписаны доверенным сертификатом.

## Установка MSI-пакетов

Включает контроль запускаемых MSI-пакетов для списка доверенных приложений.

- *Запрещать установку пакетов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для рекламных программ.*

  Блокирует запуск пакетов, которые могут распространять рекламу.

- *Запрещать установку пакетов, подписанных сертификатами, известными в «Доктор Веб» как серые.*

  Блокирует запуск пакетов, которые подписаны "серыми" сертификатами. Такие сертификаты часто используются для подписи небезопасных приложений.

- *Запрещать установку пакетов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для программ взлома*.

  Блокирует запуск пакетов, которые подписаны сертификатами, использующимися для взлома программ. Использование данного критерия рекомендовано.

- *Запрещать установку пакетов, подписанных поддельными/поврежденными сертификатами*.

  Блокирует запуск вредоносных пакетов, которые подписаны недействительными сертификатами (поврежденными или прикрепленными к бинарному файлу, чтобы не дать определить угрозу - например, сертификатами легального ПО). Также это может помочь при попытках модифицировать легальный файл или заразить вирусом. Использование данного критерия рекомендовано.

- *Запрещать установку пакетов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для вредоносных программ*.

  Блокирует запуск пакетов, которые подписаны скомпрометированными сертификатами. Использование данного критерия рекомендовано.

- *Запрещать установку пакетов, подписанных отозванными сертификатами*.

  Блокирует запуск пакетов, которые подписаны украденными или скомпрометированными сертификатами. Использование данного критерия рекомендовано, так как он позволяет превентивно пресекать запуск потенциально вредоносных приложений.

- *Запрещать установку пакетов, подписанных самоподписанными сертификатами*.

  Блокирует нелицензионное ПО, которое может оказаться вредоносным. Вредоносные программы могут добавлять к своим бинарным файлам поддельную подпись с известным именем (например, Microsoft) и/или добавлять в систему корневой сертификат, чтобы данный файл показывался и распознавался ОС как легально подписанный.

- *Запрещать установку неподписанных пакетов*.

  Блокирует запуск потенциально вредоносных и ненадежных пакетов, источник происхождения которых неизвестен.

- *Запрещать установку пакетов из альтернативных потоков NTFS (ADS)*.

  Приложения из альтернативных потоков NTFS (ADS) зачастую являются вредоносными, поэтому использование данного критерия является обязательным.

- *Запрещать установку пакетов из сети и общих ресурсов*.

  Установка пакетов из сети и общих ресурсов является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.

- *Запрещать установку пакетов со сменных носителей*.

  Установка пакетов со сменных носителей является нетипичным сценарием и несет угрозу безопасности системы. Данный критерий рекомендован к использованию.

- *Запрещать установку пакетов из временных каталогов*.

  Блокирует установку пакетов из временных каталогов.

Исключения из блокировок выше:

- *Разрешать установку системных пакетов и пакетов от компании Microsoft.*
- *Разрешать установку пакетов, известных/доверенных «Доктор Веб».*

  Если включено, то разрешена установка пакетов, которые подписаны доверенным сертификатом.

### Целостность исполняемых файлов

Включает контроль целостности 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.

- *Запрещать создание новых исполняемых файлов.*

  Блокирует попытки создания новых исполняемых файлов на диске.
- *Запрещать модификацию исполняемых файлов.*

  Блокирует попытки изменения существующих исполняемых файлов на диске.

Исключения из блокировок выше:

- *Разрешать создание и модификацию исполняемых файлов подписанным системным приложениям и приложениям от компании Microsoft.*
- *Разрешать создание и модификацию исполняемых файлов подписанным приложениям, известным/доверенным «Доктор Веб».*

  Если включено, то разрешена установка пакетов, которые подписаны доверенным сертификатом.

Критерии **Целостность исполняемых файлов** не могут быть перекрыты разрешающими/запрещающими правилами.

## 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 ее использования.

Для облегчения понимания примеры составлены без учета иерархии групп и станций, а также используют менее оптимальные с точки зрения производительности, но более простые для восприятия конструкции.

**Чтобы обратиться напрямую к базе данных**

1. Откройте Центр управления вашего Сервера Dr.Web.
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 под управлением серверных версий ОС Windows, на которых установлены вирусные базы, выпущенные до 2024.07.16-00:00:00 UTC.

```
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 < 13020240716000000;
```

Данные о платформах станций антивирусной сети хранятся в виде числовых кодов.

**Чтобы получить соответствие кода и названия платформы станции**

1. Откройте Центр управления вашего Сервера Dr.Web.
2. Перейдите в раздел **Администрирование** → **SQL-консоль**.
3. Введите следующую команду:

   ```
   SELECT DISTINCT lastos FROM stations
   ```

4. Нажмите кнопку **Выполнить**.

   Вы увидите список кодов платформ, которые были распознаны на станциях данной антивирусной сети.

5. Сохраните результат выполнения запроса в файл с помощью кнопок на панели инструментов или оставьте вкладку открытой для последующего использования полученных данных.
6. Откройте раздел **Администрирование** → **Lua-консоль**.
7. Введите команду следующего вида:

   ```
   return { ['<код>'] = dwcore.platform_str(<код>)}
   ```

   где *<код>* — один из числовых кодов, полученных с помощью SQL-запроса.

8. Нажмите кнопку **Выполнить**.

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
  );
```

Данные о серьезности состояния станций хранятся в виде числовых кодов:

`0` — минимальная,

`268435456` — низкая,

`805306368` — средняя,

`1342177280` — высокая,

`1879048192` — максимальная.

Вы также можете проверить коды состояния станций следующим способом:

1. Откройте Центр управления вашего Сервера Dr.Web.
2. Перейдите в раздел **Администрирование** → **Lua-консоль**.
3. Введите следующую команду:
   `require 'statusmessages' return statusmessages.severity`
4. Нажмите кнопку **Выполнить**.

3. Получить соответствие сообщений о состоянии станции и количества станций в каждом из этих состояний.

```
SELECT
  code Code,
  COUNT(code) Num
FROM
  (
    SELECT
      DISTINCT id,
      code
    FROM
      station_status
  ) AS t
GROUP BY
  Code
ORDER BY
  Code;
```

Данные о сообщениях о состоянии станций хранятся в виде числовых кодов.

**Чтобы получить соответствие кодов и сообщений о состоянии станции**

1. Откройте Центр управления вашего Сервера Dr.Web.
2. Перейдите в раздел **Администрирование** → **Lua-консоль**.
3. Введите следующий код:

```
local sm = require 'statusmessages'
local messageByCode = require 'stats/message_by_code'
local codes = {}
for _,v in pairs(sm) do
  local n = tonumber(v)
  if n ~= nil then
    code = sm.get_code( n )
    codes[code] = messageByCode( code )
  end
end
return codes
```

4. Нажмите кнопку **Выполнить**.

4. Получить 10 наиболее популярных угроз, обнаруженных с 2024.06.01 по 2024.07.01 на станциях, входящих в группу с идентификатором '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5' или в любые вложенные в нее 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 20240601000000000
  AND 20240701000000000
  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 SpIDer 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.

   Вариант 1:

```
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'
```

```
        )
    )
);
```

Данные о платформах станций антивирусной сети хранятся в виде числовых кодов.

Вариант 2, где '24e27d73-d21d-b211-a78c-85419c46f0e6' — UUID системной группы **Windows**:

```
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
      stations.osgroup IN
      (
        SELECT
          child
        FROM
          group_children
        WHERE
          id='24e27d73-d21d-b211-a78c-85419c46f0e6'
        UNION ALL
        SELECT
          '24e27d73-d21d-b211-a78c-85419c46f0e6'
      )
      AND station_env_kb.name IN (
        SELECT
          id
        FROM
          env_strings
        WHERE
          str IN(
            'KB4012212', 'KB4012213', 'KB4012214',
            'KB4012215', 'KB4012216', 'KB4012217',
            'KB4012598'
          )
      )
  );
```

# 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 Dr.Web, и SSL-сертификат `drwcsd-certificate.pem`, расположенный в каталоге `etc` каталога установки Сервера Dr.Web, в каталог `\\<`*удаленная_машина*`>\ADMIN$\Temp`.
2. Сервер Dr.Web запускает файл `drwinst.exe` на удаленной машине с ключами командной строки, соответствующими настройкам в Центре управления.

**Для успешной установки необходимо, чтобы на Сервере Dr.Web, 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 имени 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 брандмауэр блокирует доступ к порту 445;

   c) ограничения удаленного доступа к ресурсу `ADMIN$\Temp` на ОС Windows Vista и выше, если они не входят в домен;

   d) отсутствует владелец каталога или недостаточно прав на каталог у пользователя или группы.
2. Был доступ к файлу `drwinst.exe` и сертификату `*.pem`.

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 Dr.Web, 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:<br>• на станции отключена служба сервера;<br>• недоступен 445 TCP-порт на удаленной машине, возможные причины:<br>  ▫ машина отключена;<br>  ▫ брандмауэр блокирует указанный порт;<br>  ▫ на удаленной машине установлена ОС, отличная от ОС Windows;<br>• не настроена модель совместного доступа и безопасности для локальных учетных записей;<br>• недоступен сервер авторизации (контроллер домена);<br>• 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 Dr.Web<br><br>Не удалось прочитать файл <*path*> на Сервере Dr.Web | Отсутствует файл установщика на самом Сервере Dr.Web, либо заданы неверные права на файл установщика. |
| | Не удалось открыть файл для записи <*path*> в разделяемом ресурсе <*share*> на станции <*host*><br><br>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*><br><br>Не удалось создать сервис на станции <*host*><br><br>Не удалось запустить сервис на станции <*host*><br><br>Не удалось остановить сервис на станции <*host*><br><br>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 тайм-ауту на станции <*host*> | Установщик не успел установить Агента Dr.Web за указанный период времени. Возможные причины: медленный канал между станцией и Сервером Dr.Web, 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 Dr.Web. |

# 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). 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:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. 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»:

1. Заполните веб-форму в соответствующей секции раздела https://support.drweb.com/.
2. 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/.