Dr.WEB

Enterprise Security Suite

附录



© Doctor Web, 2022. 版权所有

本手册是关于手册所涉及的Dr.Web家族软件产品的信息性介绍和帮助手册。本手册不可成为全面判断Dr.Web家族软件产品具备或不具备某些功能和/或技术参数的依据，亦不可用于判定Dr.Web家族软件产品是否符合某些要求、技术任务和/或参数以及其他第三方文件。

本手册中的所有资料为Doctor Web公司所有并只能为产品购买者个人使用。本手册的任何部分均不得复制、转载于网络资源或利用通讯渠道或在大众媒体加以传播，不得以个人使用以外的任何其他方式不指明出处加以利用。

商标

Dr.Web、SpIDer Mail、SpIDer Guard、CureIt!、CureNet!、AV-Desk、KATANA和徽标Dr.WEB是Doctor Web公司在俄罗斯以及/或者其他国家的注册商标。本文档中提及的其他注册商标、徽标和公司名称为其所有人所有。

免责声明

任何情况下Doctor Web公司及其经销商对本文档可能的任何错误和/或遗漏以及因其导致的产品购买方损失（直接或间接损失，包括未得利益）均不承担任何责任。

Dr.Web Enterprise Security Suite
版本 **13.0**
附录
2022/3/11

Doctor Web有限公司 俄罗斯总公司
地址：125124，亚姆斯基场3道街2-12A
网址：https://www.drweb.com/
电话：+7(495)789-45-87
公司在其他地区和国家分支机构的相关信息见公司官网。

Doctor Web

Doctor Web公司是俄罗斯信息安全产品厂商。

Doctor Web公司为国家机关和大型企业以及个人用户提供高效反病毒和反垃圾邮件解决方案。

Dr.Web家族反病毒解决方案的研发始于1992年，一直以来展示着卓越的恶意软件侦测能力，符合国际安全标准。

各种证书与奖项以及用户遍布全球是对我公司产品无比信任的见证。

感谢用户对Dr.Web家族反病毒解决方案的支持！

内容

第一章、导言 **7**

文档用途 **7**

标志与缩写 **8**

第二章、应用程序 **10**

附录**A.** 产品支持的所有操作系统列表 **10**

附录**B. DBMS**使用设置**. DBMS**驱动程序参数 **15**

B1. ODBC驱动程序设置 17

B2. Oracle数据库驱动程序设置 19

B3. 使用 PostgreSQL DBMS 21

B4. 使用MySQL DBMS 23

附录**C.** 管理员身份验证 **26**

C1. 使用Active Directory认证 26

C2. 使用LDAP认证 27

C3. 使用LDAP/AD身份验证 28

C4. 权限分支部分 31

附录**D.** 系统通知 **36**

D1. 通知系统参数 36

D2. 通知模板参数 38

附录**E.** 网络地址特点 **67**

E1. 地址常规格式 67

E2. Dr.Web代理端/安装程序地址 69

附录**F.** 库的管理 **70**

F1. 常规配置文件 70

F2. 产品配置文件 72

附录**G.** 配置文件格式 **76**

G1. Dr.Web服务器配置文件 76

G2. Dr.Web安全管理中心配置文件 97

G3. 配置文件download.conf 101

G4. Dr.Web代理服务器配置文件 102

G5. 库加载器配置文件 108

附录**H. Dr.Web Enterprise Security Suite**所含软件命令行参数 **113**

H1. 网络安装程序 113

H2. Windows操作系统Dr.Web代理端 116

H3. Dr.Web服务器 117
H4. 用于Windows的Dr.Web扫描仪 127
H5. Dr.Web代理服务器 128
H6. UNIX家族操作系统Dr.Web服务器安装程序 131
H7. 工具 134
附录**I. Dr.Web**服务器导出的环境变量 **155**
附录**J. Dr.Web Enterprise Security Suite** 中正则表达式的使用 **156**
J1. PCRE正则表达式选项 156
J2. PCRE正则表达式特点 157
附录**K.** 日志文件格式 **159**
附录**L. Web API** 和**Dr.Web Enterprise Security Suite**的整合 **161**
附录**M.** 授权 **162**
M1. Boost 164
M2. C-ares 165
M3. Curl 165
M4. ICU 165
M5. GCC runtime libraries—exception 166
M6. Jemalloc 168
M7. Leaflet 168
M8. Libpng 169
M9. Libradius 171
M10. Libssh2 171
M11. Linenoise NG 172
M12. Net-snmp 173
M13. Noto Sans CJK 178
M14. OpenLDAP 180
M15. OpenSSL 180
M16. Oracle Instant Client 182
M17. ParaType Free Font 186
M18. PCRE 187
M19. Script.aculo.us 189
M20. Zlib 189
第三章、常见问题 **191**
将**Dr.Web**服务器迁至另一台计算机（**OS Windows**） **191**
将**Dr.Web**代理端连接到另一**Dr.Web**服务器 **193**
更换**Dr.Web Enterprise Security Suite DBMS**类型 **195**

恢复**Dr.Web Enterprise Security Suite**数据库 **198**
更新局域网服务器上的客户端 **203**
使用**DFS**通过**Active Directory**安装代理端 **204**
Dr.Web服务器出现事故后恢复反病毒网络 **205**
具备Dr.Web服务器备份的情况下进行还原 205
不具备Dr.Web服务器备份的情况下进行还原 207
管理**Windows**操作系统**Dr.Web**服务器的日志记录等级 **208**
自动确定**OS Android**工作站位置 **209**
访问**Dr.Web**服务器数据库示例 **210**
第四章、问题和解除方法 **214**
远程安装问题诊断 **214**
消除安装**Windows**操作系统**Dr.Web**代理端时的**BFE**服务错误 **217**
技术支持 **218**
索引 **219**

第一章、导言

文档用途

Dr.Web Enterprise Security Suite反病毒网络管理员手册包含利用 Dr.Web Enterprise Security Suite建立企业计算机网络全面反病毒保护网络的总体原则以及具体实施细则。

反病毒网络管理员手册由以下几部分组成：

1. **安装手册**

   将有助于企业领导作出购买、安装反病毒全面保护系统的决定。

   安装手册介绍反病毒网络部署流程和基本组件安装流程。

2. **管理员手册**

   供*反病毒网络管理员*使用，该管理员的职责是对企业网络中计算机（工作站和服务器）的反病毒保护进行管理。

   反病毒网络管理员应具备系统管理员的职能或者与内网管理员协作，应掌握反病毒保护策略并熟知适用于内网中各操作系统的Dr.Web反病毒软件包。

3. **附录**

   包含技术信息，介绍设置反病毒软件组件使用的参数以及运用参数的规则和各规则的含义。



上述各文档间存在交叉索引。将文档加载到本地计算机时，只有当所有文件处于同一目录且保留原有名称的情况下，交叉索引才可正常使用。

随附手册还包括：

1. **反病毒网络部署说明**

   内容为反病毒网络组件安装和初步设置的简短介绍。详细信息请查阅管理员手册。

2. **工作站管理手册**

   介绍反病毒管理员如何通过Dr.Web安全管理中心统一设置工作站上安装的反病毒软件。

3. **用户手册**

   介绍可直接在受保护工作站上进行的Dr.Web反病毒解决方案的设置。

4. **Web API手册**

   为利用Web API将Dr.Web Enterprise Security Suite与第三方软件集成的技术信息。

5. **Dr.Web服务器数据库手册**

   是对Dr.Web服务器数据库内部结构的介绍以及使用示例

所有上述手册作为Dr.Web Enterprise Security Suite组成，可通过Dr.Web安全管理中心打开。

在阅读手册前请确认您使用的产品当前版本的相应手册的最新版本。手册内容不断更新，您可在Doctor Web公司官方网站获取手册的最新版本https://download.drweb.com/doc/。

标志与缩写

标志说明

本手册中使用以下标志：

标志	说明
	重要说明或指令
	可能出现错误的情况或需要特别注意的重要环节。
反病毒网络	新的专有名词或描述中所含专有名词。
<IP-address>	用实际值代替名称的占位符
保存	按钮、窗口、菜单选项或其他程序界面元素的名称
CTRL	键盘按键名称
C:\Windows\	文件和文件夹以及部分程序代码的名称
附录 A	手册章节的交叉链接或外部资源的超链接

缩写

本手册中可能出现以下缩写：

- ACL——访问控制列表（Access Control List），
- CDN——内容分发网络（Content Delivery Network），
- DFS——分布式文件系统（Distributed File System），
- DNS——域名系统（Domain Name System），
- FQDN——全限定域名（Fully Qualified Domain Name），
- GUI——图形用户界面（Graphical User Interface），GUI-程序版本——使用GUI的版本，
- MIB——管理信息库（Management Information Base），
- MTU——最大传输单元（Maximum Transmission Unit），
- NAP——Network Access Protection，
- TTL——数据包生存时间（Time To Live），
- UDS——UNIX域套接字（UNIX Domain Socket），
- DB、DBMS——数据库、数据库管理系统，
- GUS Dr.Web——全球更新系统 Dr.Web，
- LAN——局域网，

- OS——操作系统。
-

第二章、应用程序

附录A. 产品支持的所有操作系统列表

用于Dr.Web服务器和Dr.Web代理服务器

UNIX家族操作系统

Linux，需具备glibc 2.13或更高版本，包括：

- ALT Linux 8
- ALT Linux 9
- Astra Linux Special Edition (Smolensk) 1.5 （带累积补丁包20201201SE15）
- Astra Linux 1.6 （带累积补丁包20200722SE16）
- Astra Linux 1.7
- Astra Linux Common Edition 2.12 Orel
- ALT 8 SP
- Goslinux IC6



ALT 8 Sp和Goslinux IC6操作系统下不支持强制访问级别。

FreeBSD11.3或更高版本。

OS Windows

- 32 bit:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

- 64 bit:

- Windows Server 2008 R2
- Windows 7
- Windows Server 2012
- Windows Server 2012 R2
- Windows 8
- Windows 8.1

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

用于Dr.Web扫描服务器

安装扫描服务器的虚拟机需符合以下要求：

组件	系统要求
管理程序	**VMware**、**Hyper-V**、**Xen**、**KVM**
操作系统	**Linux**、**FreeBSD** 支持的操作系统列表与UNIX操作系统反病毒软件包的列表相同。
处理器	处理器架构和指令系统 • Intel/AMD：32位（IA-32, x86）和64位（x86_64, x64, amd64）；
内存	可用内存不少于500MB（推荐为1GB或更多）。
硬盘空间	不少于1GB的磁盘可用空间。
网络连接	必需的网络连接： • 连接互联网，以便更新病毒库和内置过滤器数据库。 • 用于服务虚拟机代理端申请的连接。

用于Dr.Web代理端和反病毒软件包

UNIX家族操作系统

组件	系统要求
平台	支持的处理器架构和指令系统： • **Intel/AMD**：为32位（*IA-32, x86*）；64位（*x86-64, x64, amd64*） • **ARM64** • **E2K**（*Elbrus*）
内存	可用内存不少于500MB（推荐为1GB或更多）。
硬盘空间	应用目录所在卷可用磁盘空间不少于2GB。
操作系统	• **FreeBSD**11,12. • **Linux**，内核版本2.6.37或更新版本，使用库**glibc**版本2.13或更新版本。

组件	系统要求
	产品支持的**Linux**软件列表见下。 操作系统应支持身份验证机制**PAM**。 SpIDer Gate正常运行要求操作系统内核配置时启用以下选项： • *CONFIG_NETLINK_DIAG*、*CONFIG_INET_TCP_DIAG;* • *CONFIG_NF_CONNTRACK_IPV4*、*CONFIG_NF_CONNTRACK_IPV6*、*CONFIG_NF_CONNTRACK_EVENTS;* • *CONFIG_NETFILTER_NETLINK_QUEUE*、*CONFIG_NETFILTER_NETLINK_QUEUE_CT*、*CONFIG_NETFILTER_XT_MARK*。 上面所列选项具体情况取决于所使用的**GNU/Linux**操作系统软件。
其它	必需的网络连接： • 连接互联网，以便更新病毒库和应用组件。 • 在统一保护模式下只需在局域网连接所使用的服务器，不需要连接互联网。

使用64位版本操作系统时，必须启用对32位应用程序的支持。

对于**FreeBSD**操作系统只可从全能数据包安装应用。

产品支持以下**Linux**软件：

平台	支持的**Linux**软件
x86_64	• Astra Linux Special Edition (Smolensk) 1.5（带累积补丁包20201201SE15）、1.6（带累积补丁包20201201SE16）、1.7 • Astra Linux Common Edition 2.12 Orel • Debian 9、10 • Fedora 31、32 • CentOS 7、8 • Ubuntu 18.04、20.04 • ALT工作站8、9 • ALT服务器8、9 • ALT 8 SP • RED OS MUROM 7.2、7.3 • Goslinux IC6

平台	支持的**Linux**软件
	• SUSE Linux Enterprise Server 12SP3 • Red Hat Enterprise Linux 7、8
x86	• CentOS 7 • Debian 10 • ALT 8 SP • ALT工作站9
ARM64	• Ubuntu 18.04 • CentOS 7、8 • ALT工作站9 • ALT服务器9 • ALT 8 SP • Astra Linux Special Edition (Novorossiysk) 4.11
E2K	• Astra Linux Special Edition (Leningrad) 8.1（带累积补丁包20200429SE81） • ALT 8 SP • Elbrus-D МЦСТ 1.4 • OPO VK Elbrus-8.32 TVGI.00311-28



ALT 8 SP、Astra Linux Special Edition (Novorossiysk) 4.11和Goslinux IC6操作系统下不支持强制访问级别。

其他符合相应要求的**OS Linux**版本不能完全保证与应用完全兼容。如出现与您所使用的软件的兼容问题，请联系技术支持。

OS Windows

- 32 bit:

- Windows XP c SP2
- Windows Vista SP2
- Windows 7 SP1
- Windows 8
- Windows 8.1
- Windows 10版本21H2或更早版本
- Windows Server 2003 SP1
- Windows Server 2008 SP2

- 64 bit:

- Windows Vista SP2
- Windows 7 SP1
- Windows 8

- Windows 8.1
- Windows 10版本21H2或更早版本
- Windows 11
- Windows Server 2008 SP2
- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

由于Microsoft公司已经终止对SHA-1哈希算法的支持，在将Dr.Web代理端安装到Windows Vista、Windows 7、Windows Server 2008或Windows Server 2008 R2之前请确认操作系统支持SHA-256哈希算法。支持这一算法需安装Windows更新中心建议安装的所有更新。相关的更新补丁包的详细信息请参阅Doctor Web公司官网。

无法在操作系统为Windows Starter和Home的工作站进行Dr.Web代理端的远程安装。

macOS

OS X 10.11 El Capitan
macOS 10.12 Sierra
macOS 10.13 High Sierra
macOS 10.14 Mojave
macOS 10.15 Catalina
macOS 11.5 BigSur
macOS 12 Monterey

OS Android

Android 4.4
Android 5.0
Android 5.1
Android 6.0
Android 7.0
Android 7.1
Android 8.0
Android 8.1
Android 9.0

Android 10.0
Android 11.0

附录B. DBMS使用设置. DBMS驱动程序参数

Dr.Web服务器数据库结构可在同名手册查看。可在Dr.Web安全管理中心支持部分打开此文档。

Dr.Web服务器数据库可以是：

- 内设DBMS；
- 外设DBMS。

内设DBMS

内设DBMS进行数据保存和处理使用的设置参数见表**B-1**。

表**B-1**。内设**DBMS**

名称	默认值	描述
DBFILE	database.sqlite	数据库文件路径
CACHESIZE	2048	数据库缓存大小（页数）
PRECOMPILEDCACHE	1048576	预编译sql缓存大小（以字节计）
MMAPSIZE	• 对于OS UNIX——10485760， • 对于Windows操作系统——0	一次允许显示到进程地址空间的数据库文件最大大小，以字节计。
CHECKINTEGRITY	QUICK	启动Dr.Web服务器时检查数据库的完整性： • FULL——完全检查，检查与UNIQUE、CHECK和NOT NULL类限制相关以及与无序记录、跳过页以及无效指数相关的错误， • QUICK——快速检查，不追踪与限制和无效指数相关的错误， • NO——不进行检查。
AUTOREPAIR	NO	启动Dr.Web服务器时自动还原数据库镜像： • YES ——每次启动Dr.Web服务器时都还原数据库镜像， • NO——停用自动还原。
WAL	YES	使用主动记录（Write-Ahead Logging）：

		• yes——启用记录， • NO——不进行记录。
WAL-MAX-PAGES	1000	"脏"页数量上限，达到此限后将页记录到磁盘。
WAL-MAX-SECONDS	30	延迟磁盘记录页的最长时间（以秒计）。
SYNCHRONOUS	FULL	数据库更改磁盘同步写入模式： • FULL——全部同步写入到磁盘， • NORMAL——同步写入重要数据， • OFF——异步写入。

版本10以上Dr.Web服务器支持的内设DBM为SQLite3。

外设DBMS

Dr.Web服务器外设数据库可以是：

- Oracle DBMS。设置描述见附录B2.Oracle数据库驱动程序设置。
- PostgreSQL DBMS。PostgreSQL DBMS设置描述见附录B3. PostgreSQL DBMS的使用。
- Microsoft SQL Server/Microsoft SQL Server Express。访问DBMS数据可以所有ODBC驱动程序（Windows操作系统下ODBC驱动程序参数设置见附录B1. DBMS驱动程序设置）。

支持使用Microsoft SQL Server 2008或更高版本。建议使用Microsoft SQL Server 2014及更高版本。

不建议在工作站数量较大的反病毒网络（超过100台工作站）使用Microsoft SQL Server Express数据库。

Microsoft SQL Server作为外设数据库连接UNIX家族操作系统Dr.Web服务器时不能保证ODBC可与FreeTDS正常运行。

如果Dr.Web服务器通过ODBC运行Microsoft SQL Server数据管理系统出现预警或错误，请检查使用的是否是数据管理系统最新版本。

可打开Microsoft公司的这一网页检查是否有更新：https://docs.microsoft.com/en-US/troubleshoot/sql/general/determine-version-edition-update-level。

为减少使用DBMS Microsoft SQL Server默认交易隔离等级(READ COMMITTED)时出现的阻止数量，建议执行以下SQL指令来启用参数READ_COMMITTED_SNAPSHOT：

```
ALTER DATABASE <数据库名称>
SET READ_COMMITTED_SNAPSHOT ON;
```

此指令需在隐式交易模式下且与数据库为单一连接时执行。

内设和外设DBMS对比



连接Dr.Web服务器工作站数量不超过200–300台时可使用内设数据库。如果安装Dr.Web服务器的计算机硬件配置以及该计算机执行的其它任务负载允许，可以增加到1000台。

如不允许则必须使用外设数据库。

使用外设数据库且连接Dr.Web服务器的计算机超过10000台时建议达到以下最低要求：

- 处理器频率为3GHz，
- 内存——Dr.Web服务器为4GB以上，数据库服务器为8GB以上，
- UNIX家族操作系统

在选择使用内设数据库或外设数据库时需考虑每种DBMS具备的一些参数：

- 在大型反病毒网络（超过200–300台工作站）建议使用外设数据库，外设数据库比内设数据库运行更为稳定。
- 使用内设数据库不需要安装其他厂商的产品。建议在常规情况下使用。
- 内设数据库不需要管理员具备DBMS操作技能，是中小企业的最佳选择。
- 如需要直接访问数据库、对DBMS进行单独操作则应考虑使用外设数据库。可使用常规API访问数据库，如：OLE DB, ADO.NET或ODBC。

B1. ODBC驱动程序设置

外设DBMS进行数据保存和处理使用的设置参数见表**B-2**（具体参数值仅为示例）。

表B-2. 用于DBMS连接的参数

名称	说明	描述
DSN	drwcs	数据收集名称
USER	drwcs	用户名
PASS	fUqRbrmlvI	密码
TRANSACTION	DEFAULT	TRANSACTION的参数值可以是： • SERIALIZABLE • READ_UNCOMMITTED • READ_COMMITTED • REPEATABLE_READ • DEFAULT 默认值DEFAULT表示“默认使用SQL-服务器”。交易隔离等级详细信息参见相应DBMS的说明文档。

为避免出现编码问题，必须关闭ODBC驱动程序的以下参数：

- **输入货币、数值、日期和时间使用本地设置**——可能导致数字参数格式化出错。
- **执行符号数据翻译**——启用此项可能导致数据库数据在管理中心显示乱码，此选项设定符号显示将取决于不使用Unicode的程序的语言设置。

在Microsoft SQL DBMS创建新数据库时必须指定排序要考虑大小写（后缀_CS）和区别标记（后缀_AS）。

使用上述参数在SQL服务器预先建立数据库。

必须为安装有Dr.Web服务器的计算机进行ODBC-驱动程序设置。

UNIX家族操作系统下ODBC驱动程序设置信息参见http://www.unixodbc.org/的**Manuals**。

OS Windows的ODBC驱动程序设置

设置ODBC驱动程序参数

1. 在OS Windows**控制面板**选择**管理工具**，在打开的窗口双击**数据源（ODBC）**图标。打开**ODBC数据源管理器**。进入**系统DSN**标签。
2. 点击**添加**按钮。打开驱动程序选择窗口。
3. 选择用于此数据库的ODBC驱动程序，然后点击**完成**按钮。打开数据库服务器访问设置的第一个窗口。

使用外设DBMS Oracle必须安装和此DBMS一起供应的最新版本的ODBC-驱动程序。不建议使用和OS Windows一起提供的 ODBC-驱动程序。由Microsoft提供的不带ODBC-驱动程序的数据库除外。

4. 输入与Dr.Web服务器设置中指定的参数相符的数据源访问参数。如果数据库服务器与Dr.Web服务器安装于不同的计算机，需在**服务器**一栏输入数据库服务器的IP地址或名称。点击**下一步**。
5. 选择**检查SQL Server账户真实性**后指定用户访问数据库的账户信息。点击**下一步**。
6. 在**默认使用数据库**下拉列表选择Dr.Web服务器使用的数据库。必须是Dr.Web服务器数据库名称，而非**Default**值。

   确认已勾选以下选项：**引号内识别码使用ANSI格式**、**null值、模板和预警使用ANSI格式**。点击**下一步**。

如果设置ODBC-驱动程序时可以更改SQL-服务器系统通知语言，必须设定为英语。

7. 结束设置后点击**完成**按钮。打开已设定参数信息窗口。
8. 点击**检查数据源**按钮检查设置是否正确。得到已通过检查的通知后点击**确定**按钮。

B2. Oracle数据库驱动程序设置

概述

Oracle Database（或Oracle DBMS）——对象关系型数据库管理系统。Oracle可作为Dr.Web Enterprise Security Suite外设数据库。

Dr.Web服务器可在所有平台使用DBMS Oracle作为外设数据库，只有FreeBSD除外（参见安装和支持的版本）。

使用Oracle DBMS

1. 安装一个编码为AL32UTF8的Oracle数据库。也可使用此编码的现有数据库。
2. 将数据库驱动程序设置为使用相应的外设数据库。可利用配置文件进行设置或利用管理中心：**Dr.Web服务器配置**菜单的**数据库**标签。

如果计划使用ODBC接通Oracle作为外设数据库，则在安装（更新）Dr.Web服务器时，需在安装程序设置中取消安装Oracle DBMS内置客户端（在**支持数据库 → Oracle数据库驱动程序**）。

否则将出现库冲突而无法通过ODBC使用Oracle数据库。

禁止以系统用户SYS和SYSTEM和使用优先权SYSDBA和SYSOPER连接Oracle数据库。

安装和支持的版本

使用Oracle数据库作为外设数据库必须安装一个Oracle数据库并将其编码设置为AL32UTF8（CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16）。可使用以下方法设置：

1. 使用Oracle数据库安装程序（使用数据库高级安装和配置模式）。
2. 使用SQL指令CREATE DATABASE。

建立、配置数据库详细信息见Oracle数据库说明文档。

如编码有别于上述编码，本国语言符号显示会出现问题。

Dr.Web Enterprise Security Suite安装包保含数据库客户端（Oracle Instant Client）。

Oracle DBMS支持的平台参见厂商网站。

Oracle Client支持的平台参见厂商网站。

Dr.Web Enterprise Security Suite支持Oracle DBMS版本11及更高版本。

使用Oracle外设数据库时请注意对Dr.Web服务器的系统要求（参见安装手册的系统要求）。

参数

Oracle DBMS访问设置使用的参数见表**B-3**。

表B-3. Oracle DBMS参数

参数	描述
drworacle	驱动程序名称
User	数据库用户名称（必填项）
Password	用户密码（必填项）
ConnectionString	数据库连接行（必填项）

Oracle DBMS 连接行格式：

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

其中：

- *<host>*——Oracle服务器IP地址或名称；
- *<port>*——服务器监听的端口；
- *<service name>*——需连接的数据库名称。

例如：

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

其中：

- myserver111——Oracle服务器名称。
- 1521——服务器监听的端口。
- bjava21——需连接的数据库名称。

Oracle DBMS驱动程序配置

使用DBMS Oracle时必须利用下面一种方法更改数据库驱动程序的确定和设置：

- 在管理中心：主菜单**管理**选项→控制菜单的**Dr.Web服务器配置**选项→**数据库**标签 → 在**数据库**下拉列表选择**Oracle**，按照上面所列格式进行设置。
- 在Dr.Web服务器配置文件。

B3. 使用 PostgreSQL DBMS

概述

PostgreSQL——对象关系型数据库管理系统。为自由软件数据库系统，可替代商业DBMS（如Oracle Database, Microsoft SQL Server等等）使用。在大型反病毒网络中可以使用PostgreSQL DBMS作为Dr.Web Enterprise Security Suite外设数据库。

使用**PostgreSQL**作为外设数据库

1. 安装PostgreSQL服务器或Postgres Pro。
2. 设置Dr.Web服务器使用相应的外设数据库。可利用配置文件进行设置或利用管理中心：**Dr.Web服务器配置**菜单的**数据库**标签。



连接PostgreSQL数据库时只可使用trust、password和MD5身份验证。

安装和支持的版本

1. 下载免费产品PostgreSQL最新版本（PostgreSQL服务器和相应的ODBC驱动程序），至少不应使用早于**8.4**的版本，Postgres Pro不低于11.4.1。
2. 用以下一种方式创建PostgreSQL数据库：
   a) 使用`pgAdmin`图形界面。
   b) 使用SQL指令`CREATE DATABASE`。



建立数据库使用的编码应为UTF8。

更换为外设服务器的操作见更换Dr.Web Enterprise Security Suite DBMS类型。

使用PostgreSQL外设数据库时请注意对Dr.Web服务器的系统要求（参见**安装手册**的系统要求）。

参数

PostgreSQL数据库访问设置使用参数见表**B-4**。

表B-4。PostgreSQL

名称	默认值	描述
`host`	*<local UNIX socket>*	PostgreSQL服务器主机

名称	默认值	描述
port		PostgreSQL服务器端口或套接字文件扩展名
dbname	drwcs	数据库名称
user	drwcs	用户名
password	drwcs	密码
options		用于向服务器发送的调试/追踪项
requiressl		• 1为请求安装 SSL连接 • 0为无请求
temp_tablespaces		临时表格名称空间
default_transaction_isolation		交易间隔模式（见PostgreSQL帮助文档）

相关技术信息见https://www.postgresql.org/docs/。

Dr.Web 服务器与PosrtgreSQL数据库通过 UDS 的交互作用

如Dr.Web 服务器和PostgreSQL数据库安装在同一台计算机，可设置使用UDS（UNIX域名套接字）进行交互作用。

通过UDS设置运行

1. 在PostgreSQL数据库配置文件postgresql.conf中为UDS指定以下目录：

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

2. 重新启动PostgreSQL。

PostgreSQL数据库驱动程序设置

使用PostgreSQL数据库时，建议按照数据库官方手册进行设置，以便提高运行能力。

使用大型数据库且具备相应的运算资源时，建议设置配置文件postgresql.conf中的以下参数：

最基本的设置：

```
shared_buffers = 256MB

temp_buffers = 64MB

work_mem = 16MB
```

高级设置：

```
shared_buffers = 1GB

temp_buffers = 128MB

work_mem = 32MB

fsync = off

synchronous_commit = off

wal_sync_method = fdatasync

commit_delay = 1000

max_locks_per_transaction = 256

max_pred_locks_per_transaction = 256
```



参数fsync = off可大大提高运行能力，但如出现断电或系统故障会导致数据全部丢失。建议只有在具备数据库备份并可利用备份完全恢复数据库的情况下才可停用参数fsync。

参数设置max_locks_per_transaction可保证大量调用数据库表时运行不出现故障，如在讲数据库更新为新版本时。

B4. 使用MySQL DBMS

概述

MySQL——跨平台关系型数据库管理系统。MySQL DBMS可作为Dr.Web Enterprise Security Suite外设数据库。

使用**MySQL**作为外设数据库

1. 安装MySQL服务器。
2. 设置Dr.Web服务器使用相应的外设数据库。可利用配置文件进行设置或利用管理中心：**Dr.Web**服务器配置菜单的数据库标签。

安装和支持的版本

Dr.Web Enterprise Security Suite支持以下版本的MySQL DBMS：

- MySQ——从版本5.5.14至版本5.7，以及自8.0.12后的所有版本，
- MariaDB——10.0、10.1、10.2、10.3、10.4。

安装DBMS后在创建新数据库前必须在配置文件进行以下设置（详情请参阅您所使用的DBMS的帮助文档）：

MySQL版本5.X：

```
[mysqld]

innodb_large_prefix = true

innodb_file_format = barracuda

innodb_file_per_table = true

max_allowed_packet = 64M
```

MySQL版本8.X：

```
[mysqld]

innodb_file_per_table = true

max_allowed_packet = 64M
```

如所使用的MariaDB的DBMS版本早于10.2.4，则需在配置文件中指明：

```
binlog_format = mixed
```

参数

MySQL DBMS访问设置使用的参数见表**B-5**。

表B-5. MySQL DBMS参数

名称	默认值	描述
HOST	localhost	• 按TCP/IP连接数据库时——数据库服务器地址 • 使用UDS时——UNIX套接字文件路径。如未给出，Dr.Web服务器会尝试在常规目录mysqld查找文件。
PORT	3306	• 按TCP/IP连接数据库时——连接端口。 • 使用UDS时——UNIX套接字文件名称。
DBNAME		数据库名称
USER		数据库用户的注册名
PASSWORD	QUICK	数据库用户密码

PRECOMPILEDCACHE	1048576	预编译sql缓存大小（以字节计）
SSL	NO	只使用SSL连接： • YES——只在使用SSL的情况下才连接数据库， • NO——连接数据库不要求必须是SSL协议。

附录C. 管理员身份验证

Dr.Web服务器管理员身份验证的基本信息见**管理员手册**中的管理员身份验证。

C1. 使用Active Directory认证

只可设置允许使用以及被认证人名单次序：auth-radius.conf中的标签 <enabled/>和 <order/> 。

运行原则：

1. 管理员使用以下一种格式设定用户名和密码：
   - username，
   - domain\username，
   - username@domain，
   - 用户LDAP DN。
2. Dr.Web服务器在域控制器默认使用此用户名和密码（或在域控制器的用户名所指定的域）注册。
3. 如未能注册，则转到下一认证机制。
4. 确定注册用户的LDAP DN。
5. 为确定DN的对象读取属性DrWebAdmin。如属性为FALSE——未成功，转到下一认证机制。
6. 如果在此阶段有属性未确定，则在此用户所属组进行搜索。为每一组查看其所有父组（搜索原则——依次深入）。

出现任何错误都转至下一认证机制。

工具drweb-13.00.0-*<编号>*-esuite-modify-ad-schema-*<操作系统版本>*.exe（与Dr.Web服务器软件分开供应）可为Active Directory建立新的对象类DrWebEnterpriseUser，并为此对象类设定新的属性。

属性在Enterprise空间的OID为：

```
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"
```

编辑Active Directory用户属性需在Active Directory服务器手动进行（参见管理员手册中的管理员身份验证）。

管理员权限的指定遵循管理员所属组分层结构的继承原则。

C2. 使用LDAP认证

在配置文件auth-ldap.conf进行设置。

配置文件主要标签：

- <enabled/>和<order/>——同Active Directory。
- <server/>指定的是LDAP服务器地址。可给出多个标识符<server/>标志不同的LDAP服务器地址，也就是创建一个需要执行身份认证的服务器列表。表中第一个应该是承担主要负载的主服务器，其后可以给出几个备用服务器。管理员试图登录时会首先使用第一个可以访问的LDAP服务器。如未能连接会按照配置文件中指定的列表依次访问服务器。
- <user-dn/>使用DOS类通配符确定将用户名转为DN的规则。

  在标签<user-dn/>中允许使用的替代符号：
  - *替代所有符号串，但 . , = @ \ 和空格除外；
  - #替代所有符号串。
- <user-dn-expr/>使用正则表达式确定将用户名转为DN的规则。

  示例：同一规则的两种设定方式：

  ```
  <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确定模板中*、# 或括号中表达式的替代位置。

  根据此规则：如用户名为login@example.com，则转换后的DN为："CN=login,DC=example,DC=com"。
- <user-dn-extension-enabled/>允许执行Lua脚本ldap_user_dn_translate.ds（从目录extensions）来将用户名转换为DN。此脚本在尝试user-dn、user-dn-expr所有规则失败后启用。脚本只有一个参数——输入的用户名。脚本执行后或返回DN，或返回为空。如所有规则失败，而不允许执行脚本或脚本执行后返回为空，则按原样使用输入的用户名。
- 转换后获得的LDAP对象DN属性和其可能值可用标签重新定义（以下为默认值）：

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

  true-value/false-value参数值使用正则表达式。

- 如有未确定的管理员属性值，而配置文件设置有<group-reference-attribute-name value="memberOf"/>标签，则memberOf属性值视为此管理员所属DN组列表，在这些组中搜索所需属性与使用Active Directory时相同。

C3. 使用LDAP/AD身份验证

配置文件

在配置文件auth-ldap-rfc4515.conf进行设置。

还提供包含标准设置的配置文件：

- auth-ldap-rfc4515-check-group.conf——通过LDAP进行管理员外部身份验证的配置文件，采用简易方式，检查是否属于Active Directory组。
- auth-ldap-rfc4515-check-group-novar.conf——通过LDAP进行管理员外部身份验证的配置文件，采用简易方式，检查是否属于Active Directory组，并使用变量。
- auth-ldap-rfc4515-simple-login.conf——通过LDAP进行管理员外部身份验证的配置文件，采用简易方式。

配置文件**auth-ldap-rfc4515.conf**主要标签：

- <server />——确定LDAP服务器。

属性	描述	默认值
base-dn	DN对象，相对于此对象进行搜索。	对象Root DSE的rootDomainNamingContext参数的参数值
cacertfile	根证书文件（仅限UNIX）。	–
host	LDAP服务器地址。	• 用于OS Windows服务器的域控制器。 • 127.0.0.1用于UNIX家族操作系统服务器。 • 可给出多个标识符<server/>标志不同的LDAP服务器地址。表中第一个应该是承担主要负载的主服务器。如未能连接会按照配置文件中指定的列表依次访问服务器。
scope	搜索区域。有效值可为： • sub-tree——所有低于基础DN的区域， • one-level——基础DN的直接子域， • base——基础DN。	sub-tree
tls	安装TLS来连接LDAP服务器。	no

属性	描述	默认值
ssl	使用LDAPS协议连接LDAP服务器。	no

- <set />——指定在LDAP搜索的变量。

属性	描述	默认值
attribute	其参数值被确定为变量的参数名称。不可空缺。	–
filter	在LDAP的RFC4515搜索过滤器。	–
scope	搜索区域。有效值可为： • sub-tree——所有低于基础DN的区域， • one-level——基础DN的直接子域， • base——基础DN。	sub-tree
search	DN对象，相对于此对象进行搜索。	空缺时使用标签<server />的base-dn
variable	变量名称。应以字母开始并指包含字母和数字。不可空缺。	–

变量可用于标签 <mask />和<expr />的参数add，标签<filter />的参数value，格式为\varname，还可用于标签<set />的参数search。打开变量时的最大递归等级为16。

如搜索返回多个找到的对象，则只使用第一个。

- <mask />——用户名模板。

属性	描述
add	添加到按操作且包含可替代元素进行搜索的过滤器的行。
user	使用DOS形元字符*和#的用户名通配符。不可空缺。

例如：

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

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

\1和\2——user属性中相符通配符链接。

- <expr />——使用正则表达式的用户名模板（属性同<mask />）。

例如：

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

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

通配符与正则表达式的对应关系：

通配符	正则表达式
*	.*
#	[^.,=@\s\\]+

- `<filter />`——在LDAP的搜索过滤器。

属性	描述
value	添加到按操作且包含可替代元素进行搜索的过滤器的行。

隔离区串联

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

如admingrp在搜索结果中的值变为"CN=ESuite Admins,OU=some name,DC=example,DC=com"，而用户输入的是domain\user，最终获得的过滤器为：

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

LDAP/AD身份验证设置示例

下例为使用LDAP进行身份验证的标准设置。设置在管理中心**管理** → **身份验证** → **LDAP/AD身份验证**部分指定（如为**简明设置**）。

需进行身份验证的管理员的初始参数：

- 域名：dc.test.local
- 在Active Directory的组：DrWeb_Admins

管理中心设置：

设置名称		值
服务器类型		Microsoft Active Directory
服务器地址		dc.test.local
用于确认登录的用户名模板	账户通配符	test*或*@test.local
	用户名	\1
用于确认登录的用户组籍	名称	DrWeb_Admins

设置名称		值
	类型	组

C4. 权限分支部分

表 C-1. 管理员权限列表及其特点

编码	权限	描述	管理中心部分
管理工作站组			
1*	查看组属性	管理员在反病毒网络中可以看到的用户组列表。反病毒网络树结构中会包含所有系统组，但这些组中只显示可查看的用户组。	反病毒网络
2*	编辑工作站组属性	管理员可以编辑其属性的用户组列表。 应包含权限1列表中的组。	反病毒网络→常规→属性
3	查看工作站组配置	管理员可以查看其配置的用户组列表。还可以查看这些用户组为基组的工作站的配置。 应包含权限1列表中的组。	反病毒网络 反病毒网络→常规→已启用的组件
4	编辑工作站组配置	同权限3，但可以进行编辑。 应包含权限3列表中的用户组。	反病毒网络→常规→隔离区 控制菜单**配置**部分的页面
5	查看组属性	作为管理员可查看其属性的工作站的基组的用户组列表。 应包含权限1列表中的组。	反病毒网络
6	编辑工作站属性	包括ACL、阻止、访问等等。 同权限5，但可以进行编辑。 应包含权限5列表中的用户组。	反病毒网络→常规→属性
8*	将工作站添加到组或将工作站从组中删除	用户组列表。 应包含权限1列表中的组。	反病毒网络
9	删除工作站	作为管理员可以删除的工作站的基组的用户组列表。	

编码	权限	描述	管理中心部分
		应包含权限1列表中的组。	
10	代理端远程安装和卸载	管理员可利用所选ID启动其工作站代理端远程安装的用户组列表。这些组应是需安装的工作站的基组。 应包含权限1列表中的组。 如存在被禁止的对象，则菜单不显示此项。 提供权限16后只可从/esuite/network/index.ds进行网络安装。	
11	合并工作站	其工作站可合并的用户组列表。这些组应是工作站基组。在工具面板可选择工作站合并图标。 应包含权限1列表中的组。	
12*	查看统计报表	管理员可查看其统计信息的用户组列表。 此权限允许在Dr.Web服务器日程指定获取定期报表的任务。需给出管理员可以在此任务中选择的用户组（将获得其工作站统计报表的工作站）。如指定Everyone组，则将获得表中所有组的报表。 应包含权限1列表中的组。	反病毒网络 控制菜单**统计信息**部分的页面
23	编辑授权	管理员可添加/更换/删除其授权密钥的用户组列表。这些组应是工作站的基组。 应包含权限1列表中的组。	
管理管理员			
25	创建管理员、管理员组	将隐藏工具面板的相应图标。	管理→配置→管理员
26	编辑管理员账户	**Newbies**组管理员可以看到树结构根组为其所在组，也就是只能看到本组和其子组。**Administrators**组的管理员能够看到所有组的管理员。 管理员可以编辑指定组的工作站的账户。这时工具面板将显示相应图标。	

编码	权限	描述	管理中心部分
27	删除管理员账户	同权限26。	
28	查看管理员组属性和配置	包括组和子组中的管理员属性及配置。 管理员只可从其父组的子组中选择。	
39	显示管理员组**"Newbies"**	允许管理员在管理员树结构查看预设组**Newbies**。 如管理员没有查看**Newbies**组的权限，但包含于此组中，则只可看到自己的账户。	
29	编辑管理员组属性和配置	包括组和子组中的管理员属性及配置。 管理员只可从其父组的子组中选择。 如未提供此权限，则即便是对此组提供了权限26，管理员也不可以为组中管理员禁止继承或提高其权限。	
高级			
7	创建工作站	创建工作站时可访问具备权限8的组列表（向其添加工作站的组应具备权限8）。 创建工作站时其基组应是可分为的一个用户组。	反病毒网络
13	查看审计	全权管理员可查看审计，以及具备权限4的对象。	管理→日志→审计日志
16	启动网络搜索仪	如此权限未指定，则不可以从 /esuite/network/index.ds进行网络安装。	反病毒网络 管理→网络搜索仪
17	批准新工作站	可使用权限8的组列表。 不可指定此权限，如果管理员只有权管理某些组，而不是管理反病毒网络所有对象，也就是权限1（**查看工作站组属性**）指定了具体的组。	反病毒网络
18	查看**Dr.Web**服务器日程	查看**任务执行日志**报表。 如未提供权限12和18，则禁止查看Dr.Web服务器日程页面。	管理→配置→Dr.Web服务器任务计划器 管理→日志→任务执行日志

编码	权限	描述	管理中心部分
		如提供了12但未提供18，则可以查看统计信息日程。 对于具体的管理员，发送报告任务是否显示取决于是否具备权限12和是否有**定期报告**通知，即便是未提供权限18。	
19	编辑**Dr.Web**服务器日程		管理→配置→Dr.Web服务器任务计划器
20	查看**Dr.Web**服务器配置和库配置		管理→配置→Web服务器配置
21	编辑**Dr.Web**服务器配置和库配置		管理→库→库状态 管理→库→推迟的更新 管理→库→库常规配置 管理→库→库详细配置 管理→库→库内容 管理→日志→库更新日志 管理→配置→自定义钩子 管理 → Dr.Web服务器→版本列表
22	查看授权相关信息		管理→管理→授权管理器
24	编辑通知配置		管理→通知→通知配置 管理→通知→未发送的通知 管理→通知→Web控制台通知
30	利用**Web API**		-
31	查看服务器间连接		邻居
32	编辑服务器间连接		邻居
33	使用高级功能	限制访问**高级功能**部分所有选项，只有**工具**部分总是可以访问。	管理→高级功能
34	更新库	从GUS更新Dr.Web服务器。	**更新库**按钮在**库状态**部分

编码	权限	描述	管理中心部分
42	编辑自身设置	管理员更改自身账户的权限。	管理→配置→管理员

*权限1、2、8、12按照工作站所属组列表指定，而不是按照工作站基组指定。

如果工作站为组成员，而为此组提供了上述一些权限，则管理员可以使用与权限对应的功能，不论允许的组是否是工作站基组。这时为允许优先，如果工作站同时在权限允许组和权限禁止组，则管理员可以使用允许组权限对应的功能。

附录D. 系统通知

管理员通知设置相关信息见管理员手册的通知设置。

D1. 通知系统参数

反病毒网络通知系统使用的通知发送类型：

- 利用电子邮箱发送通知；
- 使用Web控制台发送通知；
- 使用SNMP发送通知；
- 使用代理端日志发送通知；
- push通知。

不同的通知发送方式需设置相应的参数，格式为参数 → 参数值。需为每种方式设置以下参数：

表D-1. 常规参数

参数	描述	默认值	必填项
TO	地址使用 | 隔开		是
ENABLED	启用或停用通知	true或false	是
_TIME_TO_LIVE	发送失败是重复发送的次数	10次	否
_TRY_PERIOD	重复发送的时间间隔	5分钟（5分钟内只发送一次）	否

以下为不同发送方式各自的参数表。

表D-2. 利用电子邮箱发送通知

参数	描述	默认值
FROM	发件人电子邮箱地址	drwcsd@${主机名称}
TO	收件人电子邮箱地址	-
HOST	SMTP服务器地址	127.0.0.1
PORT	SMTP服务器的端口号	• 25，如参数SSL为no • 465，如参数SSL为yes
USER	SMTP服务器用户	""

参数	描述	默认值
		如指定，则必须启用至少一种身份验证方式，负责不会发送邮件。
PASS	SMTP服务器用户密码	""
STARTTLS	用于交换数据时加密。这时通过指令STARTTLS转为受保护的连接。默认连接使用的端口为25。	yes
SSL	用于交换数据时加密。这时会开通单独的TLS受保护连接。默认连接使用的端口为465。	no
AUTH-CRAM-MD5	使用RAM-MD5身份验证	no
AUTH-PLAIN	使用PLAIN身份验证	no
AUTH-LOGIN	使用LOGIN身份验证	no
AUTH-NTLM	使用NTLM身份验证	no
SSL-VERIFYCERT	检查服务器SSL证书	no
DEBUG	启用调试模式，如在需要确定无法登录的原因时	-

表D-3. 利用Web控制台发送通知

参数	描述	默认值
TO	需向其发送此通知的管理员UUID	-
SHOW_PERIOD	通知保存时长，以秒计，自接收通知起计时	86400秒，即保存一天

表D-4. 利用SNMP发送通知

参数	描述	默认值
TO	SNMP接收实体，如IP地址	-
DOMAIN	域名	• localhost用于OS Windows • ""——用于UNIX家族操作系统。
COMMUNITY	SNMP社区或上下文	public

参数	描述	默认值
RETRIES	API重复发送通知的尝试次数	5次
TIMEOUT	API重复发送通知的的时间间隔，以秒计	5秒

表**D-5.** 利用代理端协议发送通知

参数	描述	默认值
TO	接收通知的工作站的UUID	-
SHOW_PERIOD	通知保存时长，以秒计，自接收通知起计时	86400秒，即保存一天

表**D-6. Push**通知

参数	描述	默认值
TO	应用程序在厂商（如Apple）服务器注册时获得的设备令牌	-
SERVER_URL	通知转发至厂商服务器所使用的URL relay服务器	-

D2. 通知模板参数

通知文本由Dr.Web服务器的组件以模板文件为基础生成，该组件名称为模板处理器。

Windows网络通知系统只限支持 Windows Messenger（Net Send）服务的Windows操作系统。

OS Windows Vista及更高版本不支持Windows Messenger服务。

模板文件由文字和括号中的变量组成。编辑模板文件时可以使用以下变量。

变量采用下述一种方式写入：

- {*<VAR>*}——直接替代为变量值*<VAR>*。
- {*<VAR>*: *<N>*}——变量*<VAR>*开始的*<N>*个符号。
- {*<VAR>*: *<first>*: *<N>*}——变量*<VAR>*开始的*<N>*个符号，在*<first>*个符号之后（从第*<first>*+1个符号开始），如剩余符号数量不够，右侧添加空格。
- {*<VAR>*: *<first>*: -*<N>*}——变量*<VAR>*开始的*<N>*个符号，在*<first>*个符号之后（从第*<first>*+1个符号开始）的，如剩余符号数量不够，左侧添加空格。
- {*<VAR>*/ *<original1>*/ *<replace1>*[/ *<original2>*/ *<replace2>*]}——将变量*<VAR>*指定符号替换为设定值：符号*<original1>* 替换为*<replace1>*，存在符号*<original2>*时替换为*<replace2>*，以此类推。

替换对数量不限。

- {*<VAR>*/*<original1>*/*<replace1*[{*<SUB_VAR>*}]>[/*<original2>*/*<replace2>*]}——与上面介绍的替换为指定值类似，但使用的内嵌变量为*<SUB_VAR>*。带内嵌变量的操作与带父变量的所有操作类似。

  递归替换时内嵌深度不限。

- {*<VAR>*/*<original1>*/*<replace1>*/*<original2>*/*<replace2>*/*/*<replace3>*}——与上面介绍的替换为指定值类似，但可以替换*<replace3>*的指定值，如某原值不符。如*<VAR>*中既没有*<original1>*，也没有*<original2>*，所有值都会替换为*<replace3>*。

表**D-7.** 变量写入格式

变量	说明	表达式	结果
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

标志说明

°——空格符号。

环境变量

编写通知内容可使用Dr.Web服务器进程的环境变量（用户**System**）。

环境变量在管理中心通知编辑器的**ENV**下拉列表。请注意：环境变量必须添加前缀ENV.（前缀以点结束）。

系统变量

- SYS.BRANCH——代理端和Dr.Web服务器版本，
- SYS.BUILD——Dr.Web服务器的组装日期，
- SYS.DATE——当前系统日期，
- SYS.DATETIME——当前系统日期和时间，
- SYS.HOST——Dr.Web服务器的DNS名称，
- SYS.MACHINE——安装Dr.Web服务器的计算机的网络地址，
- SYS.OS——安装Dr.Web服务器的计算机操作系统名称，
- SYS.PLATFORM——Dr.Web服务器平台，
- SYS.PLATFORM.SHORT——SYS.PLATFORM简称，

- SYS.SERVER——产品名称（Dr.Web Server），
- SYS.TIME——当前系统时间，
- SYS.VERSION——Dr.Web服务器版本。

工作站常规变量

- GEN.LoginTime——工作站连接时间，
- GEN.StationAddress——工作站地址，
- GEN.StationDescription——工作站描述，
- GEN.StationID——工作站独有识别码，
- GEN.StationLDAPDN——OS Windows工作站区分名称（distinguished name）。ADS/LDAP域包含的工作站具备此名称。
- GEN.StationMAC——工作站MAC地址，
- GEN.StationName——工作站名称，
- GEN.StationPrimaryGroupID——工作站基组识别码，
- GEN.StationPrimaryGroupName——工作站基组名称，
- GEN.StationSID——工作站安全识别码。

库常规变量

- GEN.CurrentRevision——当前版本识别码，
- GEN.Folder——产品所在的目录，
- GEN.NextRevision——已更新版本识别码，
- GEN.Product——产品描述。

各类型通知的参数和变量

管理员

管理员身份验证出错

参数	说明	
发送通知的原因	管理员未能成功登录管理中心时发送。通知内容为登录出错的原因。	
高级设置	不需指定。	
变量	MSG.Login	注册用户名
	MSG.Address	管理中心网络地址
	MSG.LoginErrorCode	错误数字代码

未知管理员

参数	说明	
发送通知的原因	使用管理员未知注册名试图登录管理中心时发送。	
高级设置	不需指定。	
变量	MSG.Login	注册用户名
	MSG.Address	管理中心网络地址

安装

此组通知还可使用工作站常规变量，见上。

未能在工作站完成安装

参数	说明	
发送通知的原因	工作站安装代理端出错时发送此通知。通知中包含错误原因。	
高级设置	不需指定。	
变量	MSG.Error	出错通知

已在工作站成功完成安装

参数	说明
发送通知的原因	工作站已成功安装代理端时发送此通知。
高级设置	不需指定。
变量	无。

授权

组中工作站数量已接近授权上限

参数	说明
发送通知的原因	组中工作站数量已接近为此组指定的授权上限时发送此通知。
高级设置	发送此通知时密钥剩余授权的数量为：或少于三个授权，或低于密钥授权总量的5%。

参数	说明	
变量	MSG.Free	剩余可用授权的数量
	MSG.Licensed	使用此组授权的工作站数量
	MSG.Total	指定给此组的所有密钥的授权数量总计。 请注意：组授权密钥有可能同时指定给其他授权对象。
	GEN.StationPrimaryGroupID	基组ID
	GEN.StationPrimaryGroupName	基组名称

网络中工作站数量已达到授权上限

参数	说明	
发送通知的原因	工作站连接Dr.Web服务器时发现此工作站所在组中的工作站数量已超出为其指定的授权密钥规定的数量时发送。 这时新工作站无法在Dr.Web服务器注册。	
高级设置	不需指定。	
变量	MSG.ID	工作站UUID
	MSG.StationName	工作站名称
	还有工作站常规变量，见上。	

授权密钥无法自动更新

参数	说明	
发送通知的原因	无法自动更新授权时发送此通知。无法自动更新的原因是当前授权组件有别于新授权。这时新密钥已成功加载，但没有分发到原授权中的对象。必须手动更换授权密钥。	
高级设置	自动更新授权的详细信息参见管理员手册中的自动更新授权。	
变量	MSG.ExpirationDate	授权到期日期
	MSG.Expired	• 1——已到期 • 0——未到期
	MSG.KeyDifference	无法自动更换密钥的原因： • 1——当前密钥与新密钥授权

参数	说明	
		组件不同 • 2——新授权数量少于当前授权
	MSG.KeyId	原授权密钥识别码
	MSG.KeyName	原授权密钥名称
	MSG.NewKeyId	新授权密钥识别码
	MSG.NewKeyName	新授权密钥名称

授权密钥自动更新

参数	说明	
发送通知的原因	授权密钥自动更新后发送此通知。这时新密钥已成功加载并分发到原授权密钥的所有对象。	
高级设置	自动更新授权的详细信息参见管理员手册中的自动更新授权。	
变量	MSG.KeyId	原授权密钥识别码
	MSG.KeyName	原授权密钥名称
	MSG.NewKeyId	新授权密钥识别码
	MSG.NewKeyName	新授权密钥名称

授权密钥已被锁

参数	说明	
发送通知的原因	从Dr.Web全球更新系统更新库时获得授权密钥已被锁的信息时发送此通知。这一密钥无法继续使用。	
高级设置	了解被锁原因详细信息请联系技术支持部门。	
变量	MSG.KeyId	授权密钥ID
	MSG.KeyName	授权密钥用户名

已达到传送授权数量限制

参数	说明
发送通知的原因	给Dr.Web邻居服务器分发的授权数量超过授权密钥允许的数量时发送。

参数	说明	
高级设置	不需指定。	
变量	MSG.ObjId	授权密钥ID

授权传送期超时

参数	说明	
发送通知的原因	从此Dr.Web服务器授权密钥向Dr.Web邻居服务器分发授权的分发期限到期时发送。	
高级设置	向Dr.Web邻居服务器分发授权的分发期限在**管理** → **Dr.Web服务器配置** → **授权**中给出。	
变量	MSG.ObjId	授权密钥ID
	MSG.Server	Dr.Web邻居服务器名称

授权密钥中的授权数量限制

参数	说明	
发送通知的原因	打开Dr.Web服务器是发现某组中的工作站数量已超出为其指定的授权密钥中的授权数量时发送。	
高级设置	不需指定。	
变量	MSG.KeyId	授权密钥ID
	MSG.KeyName	授权密钥用户名
	MSG.Licensed	允许的授权数量
	MSG.LicenseLimit	授权状态： • 1——授权密钥中可用授权数量剩余不多， • 2——授权密钥中可用授权已用完， • 3——授权密钥指定的对象数量已超过此密钥的允许值。
	MSG.Licensed	授权密钥指定的对象数量
	MSG.Total	密钥中的授权数量

授权密钥到期

参数	说明	
发送通知的原因	授权密钥即将到期且不可自动更新时发送此通知。	
高级设置	不需指定。	
变量	MSG.ExpirationDate	授权到期日期
	MSG.Expired	• 1——已到期 • 0——未到期
	MSG.KeyId	授权密钥识别码
	MSG.KeyName	授权密钥名称

新工作站

此组通知还可使用工作站常规变量，见上。

工作站在等待确认

参数	说明
发送通知的原因	新工作站申请连接Dr.Web服务器后管理员需手动确认或拒绝工作站访问时发送。
高级设置	出现这种情况的条件是管理 → **Dr.Web**服务器配置 → 常规部分的新工作站注册模式设置为手动确认。
变量	无。

工作站已被自动拒绝

参数	说明
发送通知的原因	新工作站申请连接Dr.Web服务器并得到Dr.Web服务器自动拒绝时发送。
高级设置	出现这种情况的条件是管理 → **Dr.Web**服务器配置 → 常规部分的新工作站注册模式设置为总是拒绝访问。
变量	无。

工作站已被管理员拒绝

参数	说明	
发送通知的原因	新工作站申请连接Dr.Web服务器后被管理员手动拒绝时发送。	
高级设置	出现这种情况的条件是**管理** → **Dr.Web服务器配置** → **常规**部分的**新工作站注册模式**设置为**手动确认**，而管理员为工作站选择了**反病毒网络** → 未确认的工作站 → 拒绝所选工作站访问。	
变量	MSG.AdminAddress	管理中心网络地址
	MSG.AdminName	管理员姓名

库

此组通知还可使用库常规变量，见上。

库产品更新已被冻结

参数	说明
发送通知的原因	库中产品被管理员冻结时发送此通知。这时不从全球更新系统进行产品更新。
高级设置	管理库中产品，包括冻结或解除冻结利用的是**管理** → **库详细配置**。
变量	无。

已启动库中产品更新

参数	说明
发送通知的原因	检查库更新如发现要更新的产品需要最新时发送此通知。启动从全球更新系统的产品更新。
高级设置	不需指定。
变量	无。

已启动库更新

参数	说明
发送通知的原因	在Dr.Web服务器更新过程中二次启动更新时发送。

参数	说明
高级设置	不需指定。
变量	无。

库更新出错

参数	说明	
发送通知的原因	库中某产品从全球更新系统更新库或更新某产品出错时发送此通知。通知中包含产品名称和产品更新出错具体原因。	
高级设置	不需指定。	
变量	MSG.Error	出错通知
	MSG.ExtendedError	错误详细描述

库中产品当前状态

参数	说明
发送通知的原因	检查库更新如发现要更新的产品为最新状态时发送此通知。不需要从全球更新系统更新此产品。
高级设置	不需指定。
变量	无。



库中产品当前状态模板的变量不包括在产品配置文件中被标为**通知时忽略**的文件，参见F1.配置文件.config句法。

库产品已更新

通知	说明	
发送通知的原因	库从全球更新系统成功更新时发送此通知。	
高级设置	不需指定。	
变量	MSG.Addded	已添加文件列表（每行单列一个名称）
	MSG.AddedCount	已添加文件的数量
	MSG.Deleted	已删除文件列表（每行单列一个名称）

通知	说明	
	MSG.DeletedCount	已删除文件数量
	MSG.Replaced	已更换文件列表（每行单列一个名称）
	MSG.ReplacedCount	已更换文件的数量

磁盘空间不足

参数	说明	
发送通知的原因	Dr.Web服务器动态数据目录var所在磁盘可用空间剩余有限时发送。	
高级设置	如不是有环境变量预定，磁盘剩余空间小于315MB或低于1000点（对于UNIX家族操作系统）时为磁盘空间不足。	
变量	库常规变量，见上，不可用。	
	MSG.FreeInodes	自由文件句柄inodes数量（只针对某些UNIX操作系统）
	MSG.FreeSpace	可用空间字节数
	MSG.Path	占用少量内存的目录的路径
	MSG.RequiredInodes	运行所需自由inodes数量（只针对某些UNIX操作系统）
	MSG.RequiredSpace	运行所需可用内存空间

其它

记录到应用程序监控多次阻止

参数	说明	
发送通知的原因	工作站组件应用程序监控大量阻止应用时发送。	
高级设置	发送大量阻止应用通知需在**管理** → **Dr.Web服务器配置** → **统计信息**部分勾选**应用程序监控大量阻止**一项，同时可设置相应参数。	
变量	MSG.Total	阻止总量
	MSG.Profile	阻止依据最多的模式

记录连接意外结束的日志

参数	说明	
发送通知的原因	记录到与客户端有大量非正常连接中断时发送，包括与工作站、代理端安装程序、Dr.Web邻居服务器、代理服务器的连接。	
高级设置	发送大量连接非正常结束通知需在**管理** → **Dr.Web服务器配置** → **统计信息**部分勾选**连接非正常结束**一项，同时可设置相应参数。	
变量	MSG.Total	中断的连接数量
	MSG.AddrsCount	出现连接中断的地址数量

Dr.Web服务器日志轮循出错

参数	说明	
发送通知的原因	Dr.Web服务器运行日志轮循过程出错时发送通知。通知内容为日志轮循出错的原因。	
高级设置	不需指定。	
变量	MSG.Error	错误内容

Dr.Web服务器日志写入出错

参数	说明	
发送通知的原因	Dr.Web服务器运行日志信息记录出错时发送通知。通知内容为日志记录出错的原因。	
高级设置	不需指定。	
变量	MSG.Error	错误内容

网络病毒流行

参数	说明
发送通知的原因	发现反病毒网络出现病毒流行后发送。这表明在指定时间段侦测到的威胁数量超过了设定值。
高级设置	发送病毒流行通知需在**管理** → **Dr.Web服务器配置** → **统计信息**部分勾选**追踪病毒流行**一项。同时可设置判断出现病毒流行的参数。

参数	说明	
变量	MSG.Infected	侦测到的威胁总数
	MSG.Virus	最常见的威胁

Dr.Web邻居服务器久未连接

参数	说明	
发送通知的原因	按照Dr.Web服务器任务日程中的任务发送。内容是通知Dr.Web邻居服务器很长时间未连接本Dr.Web服务器。通知中有上次连接的日期。	
高级设置	Dr.Web邻居服务器未连接的时长，达到此时限发送通知，此参数在**管理 → Dr.Web服务器任务计划器**的Dr.Web服务器日程**Dr.Web邻居服务器久未连接**这一任务中指定。	
变量	MSG.LastDisconnectTime	Dr.Web服务器上次连接的时间
	MSG.StationName	邻居服务器名称

统计报告

参数	说明	
发送通知的原因	按照Dr.Web服务器日程中的任务生成定期报告后发送。通知中包含下载报告文件的路径。	
高级设置	创建报告按照在**管理 → Dr.Web服务器任务计划器**设置的Dr.Web服务器日程中的**创建统计报告**这一任务。	
变量	MSG.Attachment	报告路径
	MSG.AttachmentType	MIME类型
	GEN.File	日志文件名称

预防性保护汇总报告

参数	说明	
发送通知的原因	从网络工作站预防性保护组件获得大量报告时发送。	
高级设置	发送预防性保护汇总报告需在**管理 → Dr.Web服务器配置 → 统计信息**部分勾选**汇总预防性保护报告**一项。同时可设置汇总报告的参数。	
变量	MSG.AutoBlockedActCount	被自动阻止的可疑进程的数量

参数	说明	
	MSG.AutoBlockedProc	被自动阻止的可疑进程
	MSG.HipsType	受保护对象类型
	MSG.IsShellGuard	按照自动阻止进程时预防性保护的反应类型区分： • 阻止未验证码 • 检查对受保护对象的访问
	MSG.ShellGuardType	自动阻止事件时最常见的阻止未验证码执行的原因
	MSG.Total	预防性保护在网络记录到的事件的数量
	MSG.UserAllowedActCount	被用户允许的可疑进程的数量
	MSG.UserAllowedHipsType	被用户允许访问的最常受到保护的对象类型
	MSG.UserAllowedIsShellGuard	按照被用户允许访问时预防性保护的反应类型区分： • 阻止未验证码 • 检查对受保护对象的访问
	MSG.UserAllowedProc	被用户允许的可疑进程
	MSG.UserAllowedShellGuard	用户允许事件时最常见的阻止未验证码执行的原因
	MSG.UserBlockedActCount	被用户阻止的可疑进程的数量
	MSG.UserBlockedHipsType	被用户禁止访问的最常受到保护的对象类型
	MSG.UserBlockedIsShellGuard	按照被用户禁止访问时预防性保护的反应类型区分： • 阻止未验证码 • 检查对受保护对象的访问
	MSG.UserBlockedProc	被用户阻止的可疑进程
	MSG.UserBlockedShellGuard	用户阻止事件时最常见的阻止未验证码执行的原因

工作站

此组通知还可使用工作站常规变量，见上。

在对服务器网络可以获取邻居服务器下属工作站的时间通知。可在设置与Dr.Web邻居服务器时启用此选项（参见管理员手册的设置Dr.Web服务器间连接）。

可收到Dr.Web邻居服务器的以下事件通知：发现安全威胁、预防性保护报告、扫描错误、扫描统计信息。

预防性保护报告

参数	说明	
发送通知的原因	获得来自工作站或Dr.Web邻居服务器的预防性保护报告时发送。	
高级设置	不需指定。	
变量	MSG.AdminName	对可疑进程采取操作的管理员
	MSG.Denied	对可疑进程采取的操作 • 禁止 • 允许
	MSG.HipsType	受保护对象类型
	MSG.IsShellGuard	按照预防性保护的反应类型区分： • 阻止未验证码 • 检查对受保护对象的访问
	MSG.Path	可疑进程路径
	MSG.Pid	可疑进程识别码
	MSG.ShellGuardType	阻止执行未验证码的原因
	MSG.StationTime	工作站出现事件的时间
	MSG.Target	被企图访问的受保护对象路径
	MSG.Total	预防性保护自动反应时禁止的数量
	MSG.User	用户名，可疑进程以其名义启动
	MSG.UserAction	对可疑进程采取的操作的发起人： • 用户 • 预防性保护的自动反应
	GEN.ServerRecvLinkID	上次收到其下属工作站预防性保护报告的Dr.Web邻居服务器的UUID（如报告来自与本Dr.Web服

参数	说明	
		务器直接连接的工作站则词参数为空）。
	GEN.ServerRecvLinkName	上次收到其下属工作站预防性保护报告的Dr.Web邻居服务器的名称（如报告来自与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerOriginatorID	收到其下属工作站预防性保护报告的Dr.Web服务器的UUID。
	GEN.ServerOriginatorName	收到其下属工作站预防性保护报告的Dr.Web服务器的名称。

预防性保护的根据已知威胁哈希值侦测威胁报告

参数	说明	
发送通知的原因	按已知哈希列表侦测到威胁后获得来自工作站或Dr.Web邻居服务器的预防性保护报告时发送。	
高级设置	按已知哈希列表侦测到威胁的通知可以使用的前提是已授权使用已知威胁哈希值公报（Dr.Web服务器使用的授权密钥中的一个授权包含此授权即可）。 是否存在此授权见授权没有信息，可在**授权管理器**查看是否有参数**允许的哈希公报列表**（如没有此功能授权，则没有这一参数）。	
变量	MSG.AdminName	对可疑进程采取操作的管理员
	MSG.Denied	对可疑进程采取的操作 • 禁止 • 允许
	MSG.Document	包含所发现的威胁的哈希值的公报
	MSG.HipsType	受保护对象类型
	MSG.IsShellGuard	按照预防性保护的反应类型区分： • 阻止未验证码 • 检查对受保护对象的访问
	MSG.Path	可疑进程路径
	MSG.Pid	可疑进程识别码

参数	说明	
	MSG.SHA1	侦测到的对象的哈希值SHA-1
	MSG.SHA256	侦测到的对象的哈希值SHA-256
	MSG.ShellGuardType	阻止执行未验证码的原因
	MSG.StationTime	工作站出现事件的时间
	MSG.Target	被企图访问的受保护对象路径
	MSG.Total	预防性保护自动反应时禁止的数量
	MSG.User	用户名，可疑进程以其名义启动
	MSG.UserAction	对可疑进程采取的操作的发起人： • 用户 • 预防性保护的自动反应
	GEN.ServerRecvLinkID	上次收到其下属工作站预防性保护报告的Dr.Web邻居服务器的UUID（如报告来自与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerRecvLinkName	上次收到其下属工作站预防性保护报告的Dr.Web邻居服务器的名称（如报告来自与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerOriginatorID	收到其下属工作站预防性保护报告的Dr.Web服务器的UUID。
	GEN.ServerOriginatorName	收到其下属工作站预防性保护报告的Dr.Web服务器的名称。

设备已被锁

参数	说明	
发送通知的原因	从工作站接收到连接工作站的设备已被Dr.Web组件阻止时发送此通知。	
高级设置	不需指定。	
变量	MSG.Capabilities	设备特征
	MSG.Class	设备等级（父组名称）

参数	说明	
	MSG.Description	设备描述
	MSG.FriendlyName	设备可识别的名称
	MSG.InstanceId	一个设备的识别码
	MSG.User	用户名

应用程序监控已阻止已知威胁哈希列表中的进程

参数	说明	
发送通知的原因	某工作站应用程序监控组件阻止威胁已知哈希值列表中的应用时发送。	
高级设置	按已知哈希列表侦测到威胁的通知可以使用的前提是已授权使用已知威胁哈希值公报（Dr.Web服务器使用的授权密钥中的一个授权包含此授权即可）。 是否存在此授权见授权没有信息，可在**授权管理器**查看是否有参数**允许的哈希公报列表**（如没有此功能授权，则没有这一参数）。	
变量	MSG.AppCtlAction	所采取的操作： • 0——未知， • 2——已阻止， • 3——已阻止（不在可信任应用列表）， • 5——已根据禁止性规则阻止， • 7——已根据策略设置阻止。
	MSG.AppCtlType	事件类型： • 0——未知， • 1——启动进程， • 2——启动主机进程， • 3——启动脚本解释器， • 4——加载模块， • 5——加载驱动程序， • 6——启动MSI安装器， • 7——在磁盘创建新的可执行文件， • 8——在磁盘更改可执行文件，
	MSG.Document	显示哈希值的公报

参数	说明	
	MSG.Path	被阻止进程的路径
	MSG.Profile	阻止依据的模式的名称
	MSG.Rule	按期进行阻止的规则的名称
	MSG.SHA256	被阻止进程的哈希值（SHA-256）
	MSG.StationTime	进程被阻止的工作站时间
	MSG.Target	进程为主机进程时被阻止脚本的路径
	MSG.TargetSHA256	进程为主机进程时被阻止脚本的哈希值（SHA-256）
	MSG.TestMode	是否启用测试状态
	MSG.User	以其账户启动被阻止对象的用户

应用程序监控已阻止进程

参数	说明	
发送通知的原因	某工作站上的应用被应用程序监控组件阻止时发送。	
高级设置	不需指定。	
变量	MSG.AppCtlAction	所采取的操作： • 0——未知， • 2——已阻止， • 3——已阻止（不在可信任应用列表）， • 5——已根据禁止性规则阻止， • 7——已根据策略设置阻止。
	MSG.AppCtlType	事件类型： • 0——未知， • 1——启动进程， • 2——启动主机进程， • 3——启动脚本解释器， • 4——加载模块， • 5——加载驱动程序， • 6——启动MSI安装器，

参数	说明	
		• 7——在磁盘创建新的可执行文件， • 8——在磁盘更改可执行文件，
	MSG.Path	被阻止进程的路径
	MSG.Profile	阻止依据的模式的名称
	MSG.Rule	按期进行阻止的规则的名称
	MSG.SHA256	被阻止进程的哈希值（SHA-256）
	MSG.StationTime	进程被阻止的工作站时间
	MSG.Target	进程为主机进程时被阻止脚本的路径
	MSG.TargetSHA256	进程为主机进程时被阻止脚本的哈希值（SHA-256）
	MSG.TestMode	是否启用测试状态
	MSG.User	以其账户启动被阻止对象的用户

侦测到安全威胁

参数	说明	
发送通知的原因	从工作站接收到发现威胁时发送此通知。通知中包含侦测到的威胁的详细信息。	
高级设置	不需指定。	
变量	MSG.Action	侦测后所采取的操作
	MSG.Component	组件名称
	MSG.InfectionType	威胁类型
	MSG.ObjectName	已感染对象名称
	MSG.ObjectOwner	已感染对象所有人
	MSG.RunBy	以其账户启动组件的用户
	MSG.ServerTime	获取事件时间，GMT
	MSG.Virus	威胁名称

参数	说明	
	GEN.ServerRecvLinkID	上次收到其下属工作站侦测到威胁报告的Dr.Web邻居服务器的UUID（如威胁侦测报告来自与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerRecvLinkName	上次收到其下属工作站侦测到威胁报告的Dr.Web邻居服务器的名称（如威胁侦测报告来自与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerOriginatorID	收到其下属工作站侦测到威胁报告的Dr.Web服务器的UUID。
	GEN.ServerOriginatorName	收到其下属工作站侦测到威胁报告的Dr.Web服务器的名称。

根据已知威胁哈希值发现安全威胁

参数	说明	
发送通知的原因	从工作站接收到根据已知威胁哈希值发现威胁时发送此通知。发给管理员的通知中包含侦测到的威胁的详细信息。	
高级设置	按已知哈希列表侦测到威胁的通知可以使用的前提是已授权使用已知威胁哈希值公报（Dr.Web服务器使用的授权密钥中的一个授权包含此授权即可）。 是否存在此授权见授权没有信息，可在**授权管理器**查看是否有参数**允许的哈希公报列表**（如没有此功能授权，则没有这一参数）。	
变量	MSG.Action	侦测后所采取的操作
	MSG.Component	组件名称
	MSG.Document	包含所发现的威胁的哈希值的公报
	MSG.InfectionType	威胁类型
	MSG.ObjectName	已感染对象名称
	MSG.ObjectOwner	已感染对象所有人
	MSG.RunBy	以其账户启动组件的用户
	MSG.SHA1	侦测到的对象的哈希值SHA-1
	MSG.SHA256	侦测到的对象的哈希值SHA-256

参数	说明	
	MSG.ServerTime	获取事件时间，GMT
	MSG.Virus	威胁名称
	GEN.ServerRecvLinkID	上次收到其下属工作站侦测到威胁报告的Dr.Web邻居服务器的UUID（如威胁侦测报告来自与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerRecvLinkName	上次收到其下属工作站侦测到威胁报告的Dr.Web邻居服务器的名称（如威胁侦测报告来自与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerOriginatorID	收到其下属工作站侦测到威胁报告的Dr.Web服务器的UUID。
	GEN.ServerOriginatorName	收到其下属工作站侦测到威胁报告的Dr.Web服务器的名称。

工作站登录出错

参数	说明	
发送通知的原因	工作站尝试连接Dr.Web服务器时提供的账户信息有误时发送。通知中还包含按照工作站连接策略所应采取的操作。	
高级设置	工作站连接策略在管理 → **Dr.Web服务器配置** → 常规部分的新工作站注册模式设置。	
变量	MSG.ID	工作站UUID
	MSG.Rejected	数值： • rejected——工作站被拒绝登录 • newbie——已尝试将工作站转为"新工作站"状态；
	MSG.StationName	工作站名称

创建工作站账户出错

参数	说明
发送通知的原因	如无法在Dr.Web工作站创建新的工作站账户时发送。错误相关选项会记录到Dr.Web服务器日志。

参数	说明	
高级设置	不需指定。	
变量	MSG.ID	工作站UUID
	MSG.StationName	工作站名称

扫描进程出错

参数	说明	
发送通知的原因	从工作站接收到扫描出错信息时发送此通知。	
高级设置	不需指定。	
变量	MSG.Component	组件名称
	MSG.Error	出错通知
	MSG.ObjectName	对象名称
	MSG.ObjectOwner	对象所有人
	MSG.RunBy	以其账户启动组件的用户
	MSG.ServerTime	获取事件时间，GMT
	GEN.ServerRecvLinkID	上次收到其下属工作站扫描尺寸的Dr.Web邻居服务器的UUID（如扫描出错的是与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerRecvLinkName	上次收到其下属工作站扫描尺寸的Dr.Web邻居服务器的名称（如扫描出错的是与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerOriginatorID	收到其下属工作站扫描出错的Dr.Web服务器的UUID。
	GEN.ServerOriginatorName	收到其下属工作站扫描出错的Dr.Web服务器的名称。

工作站更新出现重大错误

参数	说明
发送通知的原因	从工作站获得从Dr.Web服务器获得反病毒组件更新的过程出错通知时发送。

参数	说明	
高级设置	不需指定。	
变量	MSG.Product	可更新产品
	MSG.ServerTime	Dr.Web获得通知的本地时间

根据已知威胁哈希值侦测威胁时扫描出错

参数	说明	
发送通知的原因	根据已知威胁哈希值侦测威胁如扫描出错则发送此通知。	
高级设置	按已知哈希列表侦测到威胁的通知可以使用的前提是已授权使用已知威胁哈希值公报（Dr.Web服务器使用的授权密钥中的一个授权包含此授权即可）。 是否存在此授权见授权没有信息，可在**授权管理器**查看是否有参数**允许的哈希公报列表**（如没有此功能授权，则没有这一参数）。	
变量	MSG.Component	组件名称
	MSG.Document	包含所发现的威胁的哈希值的公报
	MSG.Error	出错通知
	MSG.ObjectName	对象名称
	MSG.ObjectOwner	对象所有人
	MSG.RunBy	以其账户启动组件的用户
	MSG.SHA1	侦测到的对象的哈希值SHA-1
	MSG.SHA256	侦测到的对象的哈希值SHA-256
	MSG.ServerTime	获取事件时间，GMT
	GEN.ServerRecvLinkID	上次收到其下属工作站扫描尺寸的Dr.Web邻居服务器的UUID（如扫描出错的是与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerRecvLinkName	上次收到其下属工作站扫描尺寸的Dr.Web邻居服务器的名称（如扫描出错的是与本Dr.Web服务器直接连接的工作站则词参数为空）。
	GEN.ServerOriginatorID	收到其下属工作站扫描出错的

参数	说明	
		Dr.Web服务器的UUID。
	GEN.ServerOriginatorName	收到其下属工作站扫描出错的Dr.Web服务器的名称。

扫描统计信息

参数	说明	
发送通知的原因	从工作站接收到结束扫描信息时发送此通知。通知中包含简短的扫描结果统计信息。	
高级设置	不需指定。	
变量	MSG.Component	进行扫描的组件名称
	MSG.Cured	已清除的对象数量
	MSG.DeletedObjs	已删除的对象数量
	MSG.Errors	扫描错误数量
	MSG.Infected	已感染对象数量
	MSG.Locked	已阻止对象数量
	MSG.Modifications	被病毒变种感染的对象数量
	MSG.Moved	已隔离对象数量
	MSG.Renamed	已重命名对象数量
	MSG.RunBy	以其账户启动组件的用户
	MSG.Scanned	已扫描对象数量
	MSG.ServerTime	获取事件时间，GMT
	MSG.Speed	处理速度（KB/秒）
	MSG.Suspicious	可疑对象数量
	MSG.VirusActivity	侦测到的病毒总数
	GEN.ServerRecvLinkID	上次收到其下属工作站扫描统计信息的Dr.Web邻居服务器的UUID（如扫描信息来自与本Dr.Web服务器直接连接的工作站，则此参数为空）。
	GEN.ServerRecvLinkName	上次收到其下属工作站扫描统计

参数	说明	
		信息的Dr.Web邻居服务器的名称（如扫描信息来自与本Dr.Web服务器直接连接的工作站，则此参数为空）。
	GEN.ServerOriginatorID	收到其下属工作站扫描统计信息的Dr.Web服务器的UUID。
	GEN.ServerOriginatorName	收到其下属工作站扫描统计信息的Dr.Web服务器的名称。

未知工作站

参数	说明	
发送通知的原因	新工作站申请连接Dr.Web服务器但在确认前无法访问会被拒绝时发送。	
高级设置	不需指定。	
变量	MSG.ID	未知工作站的UUID
	MSG.Rejected	数值： • rejected——工作站被拒绝登录 • newbie——已尝试将工作站转为"新工作站"状态；
	MSG.StationName	工作站名称

连接错误结束

参数	说明	
发送通知的原因	与客户端错误中断连接是发送，客户端包括：工作站、代理端安装程序、Dr.Web邻居服务器、代理服务器。	
高级设置	发送连接非正常结束通知需在**管理** → **Dr.Web服务器配置** → **统计信息**部分勾选**连接非正常结束**一项，同时可设置相应参数。	
变量	MSG.Total	中断的连接数量
	MSG.Type	客户端类型

工作站已注册

参数	说明	
发送通知的原因	此通知在试图连接Dr.Web服务器的工作站识别码与已连接此Dr.Web服务器的工作站识别码相同时发送。	
高级设置	不需指定。	
变量	MSG.ID	工作站UUID
	MSG.Server	已注册工作站的Dr.Web服务器的ID
	MSG.StationName	工作站名称

工作站久未连接Dr.Web服务器

参数	说明	
发送通知的原因	按照Dr.Web服务器任务日程中的任务发送。内容是通知工作站很长时间未连接本Dr.Web服务器。通知中有上次连接的日期。	
高级设置	工作站未连接的时长，达到此时限发送通知，此参数在**管理** → **Dr.Web服务器任务计划器**的Dr.Web服务器日程**工作站久未连接**这一任务中指定。	
变量	工作站常规变量，见上，不可用。	
	MSG.DaysAgo	上次连接Dr.Web服务器后已过天数
	MSG.LastSeenFrom	工作站上次连接Dr.Web服务器使用的地址
	MSG.StationDescription	工作站描述
	MSG.StationID	工作站UUID
	MSG.StationMAC	工作站MAC地址
	MSG.StationName	工作站名称
	MSG.StationSID	工作站安全识别码

必须重启工作站

参数	说明
发送通知的原因	因以下原因必须重启工作站时发送此通知： • 完成清除，

参数	说明	
	• 应用更新， • 更改硬件虚拟化状态， • 完成清除并应用更新， • 完成清除并更改硬件虚拟化状态， • 应用更新并更改硬件虚拟化状态， • 完成更新、应用更新并更改硬件虚拟化状态。	
高级设置	不需指定。	
变量	MSG.Reason	重启原因 可能原因列表包含于预设面板

工作站已自动确认

参数	说明
发送通知的原因	新工作站申请连接Dr.Web服务器并得到Dr.Web服务器自动确认时发送。
高级设置	出现这种情况的条件是**管理** → **Dr.Web服务器配置** → **常规**部分的**新工作站注册模式**设置为**自动允许访问**。
变量	无。

工作站已由管理员确认

参数	说明	
发送通知的原因	新工作站申请连接Dr.Web服务器并得到管理员手动确认时发送。	
高级设置	出现这种情况的条件是**管理** → **Dr.Web服务器配置** → **常规**部分的**新工作站注册模式**设置为**手动确认**，而管理员为工作站选择了**反病毒网络** → **未确认的工作站** → **允许所选工作站访问且指定基组**。	
变量	MSG.AdminAddress	管理中心网络地址
	MSG.AdminName	管理员姓名

应用更新必须重启工作站

参数	说明
发送通知的原因	从工作站接收到产品已安装或更新且必须重启工作站时发送此通知。

参数	说明	
高级设置	不需指定。	
变量	MSG.Product	可更新产品
	MSG.ServerTime	Dr.Web服务器获得通知的本地时间

附录E. 网络地址特点

本节使用以下约定符号：

- 变量（实际值替代项）在尖括号中，为斜体；
- 固定文字（不替换）为等宽字体；
- 非必须元素在方括号中；
- 符号串::=左侧为被定义概念，右侧为定义（同巴科斯-诺尔范式）。

E1. 地址常规格式

网络地址的格式为：

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

默认情况下 *<protocol>*值为TCP。 *<protocol-specific-part>*默认值由应用程序指定。

> 也可使用老的地址记录格式：
>
> [*<protocol>*/] [*<protocol-specific-part>*]。

IP地址

- *<interface>*: :=*<ip-address>*
  *<ip-address>*可以是DNS名称或以点隔开的IP地址（如127.0.0.1）。
- *<socket-address>*: :=*<interface>*: *<port-number>*
  <port-number> 应为十进制数字。

指定Dr.Web服务器地址和代理端地址时可以给出所使用的协议版本。可采用以下方案：

- *<protocol>*: / / *<interface>*: *<port-number>*——使用IPv4和IPv6。
- *<protocol>*: / / (*<interface>*) : *<port-number>*——只使用IPv4。
- *<protocol>*: / / [*<interface>*] : *<port-number>*——只使用IPv6。

例如：

1. tcp://127.0.0.1:2193
   代表TCP协议，端口号2193，在接口 127.0.0.1。
2. tcp://(examle.com):2193
   代表TCP协议，端口号2193，在IPv4接口 example.com。
3. tcp://[::]:2193
   代表TCP协议，IPv6接口 0000.0000.0000.0000.0000.0000.0000.0000的端口号2193。
4. localhost:2193
   同上。

5. tcp://:9999

   对于服务器：取决于应用程序的默认接口（一般为所有可用接口），端口9999；对于客户端：与取决于应用程序的默认主机连接（一般为localhost），端口9999。

6. tcp://

   TCP协议。默认端口。

使用连接协议

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

其中*<socket-address>*为服务器套接字本地地址或客户端远程服务器。

使用数据报协议

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

例如：

1. udp://231.0.0.1:2193

   表示在应用程序默认接口使用multicast-组231.0.0.1:2193。

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

   表示在应用程序默认接口使用multicast-组 [ff18::231.0.0.1]。

3. udp://

   应用程序默认接口和终点。

4. udp://255.255.255.255:9999-myhost1

   在接口myhost1使用端口9999广播。

UDS地址

- 使用连接协议：

  unx://*<file_name>*

- 使用数据报协议：

  udx://*<file_name>*

例如：

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

SRV地址

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

E2. Dr.Web代理端/安装程序地址

直接连接Dr.Web服务器

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

取决于不同的*<connection-protocol>*默认值为：

- `tcp://127.0.0.1:2193`
  其中`127.0.0.1`——loopback，`2193`——端口；
- `tcp://[::1]:2193`
  其中`[::1]`——loopback (IPv6)，`2193`——端口。

使用指定协议和终点搜索Dr.Web服务器<drwcs-name>

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

取决于不同的*<datagram-protocol>*默认值为：

- `drwcs@udp://231.0.0.1:2193-0.0.0.0`
  搜索名称为`drwcs`的Dr.Web服务器，实现在所有接口使用multicast-组`231.0.0.1:2193`的TCP连接。

附录F. 库的管理

建议利用管理中心的相应设置来对库进行管理。参见管理员手册中的Dr.Web服务器库的管理。

库设置保存与以下库配置文件：

- 常规配置文件位于库根目录，设定服务器更新参数。
- 产品配置文件位于对应库中具体产品的根目录，设定相应产品的文件组成和更新设置。

对配置文件进行编辑后需要重新启动Dr.Web服务器。

设置服务器间连接时（参见管理员手册中的多Dr.Web服务器网络特点）建立产品镜像需注意，配置文件不是产品的组成部分，镜像系统不能对配置文件进行处理。为避免更新系统运行出现问题：

- 需为同级Dr.Web服务器保存相同的配置；
- 关闭Dr.Web子服务器使用HTTP协议进行组件同步或保存相同的配置。

F1. 常规配置文件

.servers

文件.servers中是从全球更新系统服务器更新Dr.Web服务器库中Dr.Web Enterprise Security Suite组件的服务器列表。

依次请求列表中服务器，成功更新时结束请求。

例如：

```
esuite.geo.drweb.com
```

.url

文件.url中是更新区基本URI——更新服务器上内含Dr.Web具体产品更新的目录。

例如：

```
update
```

.proto

文件.proto中是从更新服务器获取更新使用的协议名称。

可以是：http | https | ftp | ftps | sftp | scp | smb | smbs | file。



协议smb和smbs只可用于UNIX家族操作系统的Dr.Web服务器。

例如：

```
https
```

.auth

文件.auth包含登录更新服务器的参数。

登录参数格式为：

```
<用户名>
<密码>
```

用户名为必填参数，密码为可选参数。

例如：

```
admin
root
```

.delivery

文件.auth中是从全球更新系统服务器获取更新的设置。

参数	可用参数值	描述
cdn	on | off	加载库时使用Content Delivery Network： • on——使用CDN， • off——不使用CDN。
cert	drweb | valid | any | custom	允许的更新服务器SSL证书，自动接受： • drweb——只接受Doctor Web公司SSL证书，

参数	可用参数值	描述
		• valid——只接受有效的SSL证书， • any——接受所有证书， • custom——接受用户指定的证书。
cert-path		用户证书路径，如参数cert设为custom模式。
ssh-mode	pwd | pubkey	使用scp和sftp（基于*ssh2*）时的身份验证模式： • pwd——根据注册的用户名和密码进行身份验证， • pubkey——根据加密密钥进行身份验证。
ssh-pubkey		更新服务器ssh公钥路径。
ssh-prikey		更新服务器ssh私钥路径。

F2. 产品配置文件

.description

文件.description指定产品名称。 如无此文件，则使用产品相应目录名称作为产品名称。

例如：

```
Dr.Web Server
```

.sync-off

此文件停用产品更新。文件内容对功能没有影响。

从全球更新系统更新Dr.Web服务器库时的排除项文件

.sync-only

文件.sync-only含正则表达式，确定从GUS更新库时库中需同步的文件列表。.sync-only未指定的库中文件不进行同步。如.sync-only文件不存在，则同步库中所有文件，只有文件.sync-ignore中设置为排除的文件不同步。

.sync-ignore

文件.sync-ignore含库文件名称正则表达式，这些文件在从GUS更新库时不进行同步。

排除项文件示例

```
^windows-nt-x64/

^windows-nt/

^windows/
```

配置文件使用流程

如对于某产品同时存在文件.sync-only和.sync-ignore，执行操作的流程为：

1. 首先应用.sync-only。.sync-only中不包含的文件不进行处理。
2. 对其它文件应用.sync-ignore。

从Dr.Web服务器更新代理端时的排除项文件

.state-only

文件.state-only含正则表达式，确定从Dr.Web服务器更新代理端时需同步的文件列表。.state-only未指定的库中文件不进行同步。如.state-only文件不存在，则同步库中所有文件，只有文件.sync-ignore中设置为排除的文件不同步。

.state-ignore

文件.state-ignore含正则表达式，确定从Dr.Web服务器更新代理端时不需同步的文件列表。

例如：

- 不需要接收德语、汉语和西班牙语界面语言（其它语言界面接收），
- 不需要接收用于OS Windows 64位系统的组件。

```
;^common/ru-.*\.dwl$ 将更新

^common/de-.*\.dwl$

^common/cn-.*\.dwl$

^common/es-.*\.dwl$

^win/de-.*

^win/cn-.*

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

.state-only和.state-ignore与.sync-only和.sync-ignore的应用次序相同。

通知发送设置

使用文件notify可设置在成功更新库中相应产品时发送的通知。

> 这些设置只针对**产品已更新**这一通知。不适用其他类型通知。
>
> 通知系统设置相关信息见**管理员手册**的通知设置。

.notify-only

文件.notify-only包含库文件列表，这些文件发生变化时发送通知。

.notify-ignore

文件.notify-ignore包含库文件列表，这些文件发生变化时不发送通知。

配置文件使用流程

如对于某产品同时存在文件.notify-only和.notify-ignore，执行操作的流程为：

1. 从GUS更新的产品时将更新了的文件与排除列表进行对比。
2. 首先排除.notify-ignore列表包含的文件。
3. 剩下的文件中排除.notify-only列表不包含的文件。
4. 如有文件没有被排除，则发送通知。

如没有.notify-only和.notify-ignore文件，则总是发送通知（如果管理中心的**通知设置**页面启用了这些通知）。

例如：

如文件.notify-ignore指定排除^.vdb.lzma$，则只更新了病毒库时不发送通知。如果除了病毒库，还更新了引擎drweb32.dll，则发送通知。

设置冻结

.delay-config

文件.delay-config含禁止产品转至新校检的设置。库将继续分发前一校检，不再进行同步（产品状态"冻结"）。如管理员认为新接收的校检可以分发，需在管理中心允许分发（参见**管理员手册**的Dr.Web服务器库管理）。

文件含两个参数，不计大小写，用分号隔开。

文件格式：

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

参数	可用参数值	描述
Delay	ON|OFF	• ON——启用产品更新冻结。 • OFF——停用产品更新冻结。
UseFilter	YES|NO	• Yes——只有当更新文件符合文件.delay-only中的排除列表时才冻结更新。 • No——任何情况下都冻结更新。

例如：

```
Delay ON; UseFilter NO
```

.delay-only

文件.delay-only中设定的文件如发生变化会禁止产品转为新校检。文件列表采用正则表达式。

如库更新的文件与所设定的通配符相符，且文件.sync-only中的UseFilter为启用，则校检将被冻结。

.rev-to-keep

文件.rev-to-keep是保存的产品校检的数量。

例如：

```
3
```

附录G. 配置文件格式

本节介绍以下文件的格式：

文件	描述
drwcsd.conf	Dr.Web服务器配置文件。
webmin.conf	Dr.Web安全管理中心配置文件。
download.conf	用于设置从Dr.Web服务器加载的数据的配置文件。
drwcsd-proxy.conf	Dr.Web代理服务器配置文件。
drwreploader.conf	库加载器配置文件。



如果在安装有相应组件的计算机上安装有代理端，且代理端自我保护为开启状态，在修改配置文件必须通过代理端设置关闭自我保护组件Dr.Web Self-protection。

保存修改后应启用组件Dr.Web Self-protection。

G1. Dr.Web服务器配置文件

Dr.Web服务器配置文件drwcsd.conf默认情况下位于Dr.Web服务器根目录的etc子目录。利用命令行参数启动Dr.Web服务器时可以指定另一路径和另一文件名称（详见附录H3. Dr.Web服务器）。

手动编辑Dr.Web服务器配置文件

1. 停止Dr.Web服务器（参见管理员手册中的启动和停止Dr.Web服务器）。
2. 停用自我保护（如计算机上安装有代理端并启用自我保护——在代理端菜单停用自我保护）。
3. 对Dr.Web服务器配置文件进行更改。
4. 启动Dr.Web服务器（参见管理员手册中的启动和停止Dr.Web服务器）。

Dr.Web服务器配置文件格式

Dr.Web服务器配置文件为XML格式文件。

Dr.Web服务器配置文件参数介绍：

- `<version value="" />`

  配置文件当前版本。

- `<name value="" />`

  代理端、代理端安装程序或管理中心进行搜索时使用的Dr.Web服务器或Dr.Web服务器群集名称。如参数为空（""——默认使用）。则使用安装Dr.Web服务器的计算机的名称。

- `<id value="" />`

  Dr.Web服务器识别码。在之前的版本中保存在Dr.Web服务器密钥，自版本10起保存于Dr.Web服务器配置文件。

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

  加盐加密。为添加到管理员密码后的随机字符串，之后经哈希功能整体处理后以一个哈希值的形式保存于数据库，用以防止利用轮选方式破解管理员密码。默认是在安装或升级Dr.Web服务器时生成。参数值为空则不进行密码加密（不建议留空）。

  使用加盐加密后无法使用Dr.Web服务器数据库运行工具（drwidbsh3）来查看和更改管理员密码。

  使用Dr.Web服务器群集时必须在群集中的所有Dr.Web服务器手动指定同一盐值。

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

  Dr.Web服务器地理位置。

  属性介绍：

属性	描述
city	城市
country	国家
department	部门名称
floor	楼层
latitude	纬度
longitude	经度
organization	单位名称
province	省份名称
room	办公室编号
street	街道名称

- `<threads count="" />`

  用于处理代理端发来的数据的线程数量。最小值为5。默认为5。此参数影响Dr.Web服务器的性能。没有接到技术支持部门建议的情况下不可对此参数进行修改。

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

  新工作站访问模式

  属性介绍：

属性	有效值	描述	默认值
approve-to-group	-	自动允许访问（mode='open'）模式下默认设为新工作站基组的工作站组。	此值为空时表示将**Everyone**组设为基组。
mode	• open——自动允许访问， • closed——总是拒绝访问， • approval——手动确认。	新工作站连接策略	-

  详见管理员手册中的 工作站连接策略。

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

  此模式是从组安装包安装代理端时如账户不足，管理中心会自动创建工作站账户。

属性	有效值	默认值
enabled	• yes——工作站账户不足时自动创建， • no——只可按照启动安装包的组中已创建的账户数量进行安装。	yes

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

  对未登录工作站采取的操作。enabled允许值为：

  - yes——表示没有通过验证的工作站（如数据库受损时）将自动转为新工作站状态。
  - no（默认值）——代表一般运行模式。

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

  登录Dr.Web服务器的等候列队中工作站最多数量。没有接到技术支持部门建议的情况下不可对此参数进行修改。

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

  在Dr.Web服务器日志文件将计算机IP地址更换为DNS名称。enabled允许值为：

  - yes——显示DNS名称。
  - no（默认值）——显示IP地址。

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

  将计算机NetBIOS名称替换为DNS名称。

  属性介绍：

属性	有效值	描述
enabled	• yes——替换， • no——不替换，将应用设置<**agent-host-names** />。	NetBIOS名称替换模式。

属性	有效值	描述
host	• yes——部分显示确定的DNS名称（FQDN中点之前的部分）， • no——完整显示确定的DNS名称（FQDN）。	替换后名称的格式。

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

  反病毒网络计算机访问Dr.Web服务器时名称的显示模式。属性 mode可用值有：

  - netbios——显示NetBIOS名称（属性值为空或无此参数时默认使用），
  - fqdn——完整显示确定的DNS名称（FQDN）。
  - host——部分显示确定的DNS名称（FQDN中点之前的部分）。

- `<dns>`

  DNS设置。

  `<timeout value="" />`

  允许正向/反向DNS请求的超时时限（以秒计）。为空时不限定等待允许的时间。

  `<retry value="" />`

  未能成功允许DNS请求时重复DNS请求的最多次数。

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

  缓存保存DNS服务器响应的时限。

  属性介绍：

属性	有效值	描述
enabled	• yes——缓存中保存回应， • no——缓存中不保存回应。	缓存回应的模式。
negative-ttl	-	在缓存（TTL）保存DNS服务器负响应的时限，以分钟计。
positive-ttl	-	在缓存（TTL）保存DNS服务器正响应的时限，以分钟计。

  `<servers>`

  包含一个或多个子元素`<server address="" />`，其中参数address确定服务器IP地址。替代系统默认列表的DNS服务器列表。

  `<domains>`

  包含一个或多个子元素 `<domain name="" />`，其中参数name确定域名。替代系统默认列表的DNS服务器列表。

- `<cache>`

  缓存设置。

  元素`<cache>` 包含以下子元素：

- <interval value="" />

  全部清空缓存的周期，以秒计。

- <quarantine ttl="" />

  删除Dr.Web服务器隔离区文件的周期，以秒计。默认值为604800（一个星期）。

- <download ttl="" />

  删除个人安装包的周期，以秒计。默认值为604800（一个星期）。

- <repository ttl="" />

  删除Dr.Web服务器库缓存文件时间间隔，以秒计。

- <file ttl="" />

  清空缓存区文件的周期，以秒计。默认值为604800（一个星期）。

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

  将Dr.Web服务器上的工作站描述与工作站**System properties**页面的**Computer description**栏进行同步。enabled允许值为：

  - yes——将Dr.Web服务器上的描述替换为工作站上的描述。
  - no（默认值）——忽略工作站上的描述。

- <time-discrepancy value="" />

  允许的Dr.Web服务器系统时间与Dr.Web代理端系统时间的差别，以分钟计。如超出此允许值，则在服务器的工作站状态作出标记。默认为3分钟。值为空或为0表示不进行系统时间比照。

- <encryption mode="" />

  流量加密模式。mode允许值为：

  - yes——使用加密，
  - no——不使用加密，
  - possible——可使用加密。

  默认为yes。

  详见管理员手册中的流量的加密和压缩。

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

  流量压缩模式。

  属性介绍：

属性	有效值	描述
level	1至9的整数。	压缩等级。
mode	• yes——使用压缩， • no——不使用压缩， • possible——可使用压缩。	压缩模式

  详见管理员手册中的流量的加密和压缩。

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

  允许跟踪任务执行结果并记录到Dr.Web服务器数据库。enabled允许值为：yes或no。

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

  允许跟踪工作站状态变化并将信息记录到Dr.Web服务器数据库。enabled允许值为: yes或no。

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

  允许跟踪工作站病毒库状态变化（组成、变化）并将信息记录到Dr.Web服务器数据库。enabled允许值为：yes或no。 忽略此参数，如<track-agent-status enabled="no" />。

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

  允许跟踪工作站模块版本并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  允许跟踪工作站安装的组件列表并将信息记录到Dr.Web服务器数据库。enabled允许值为：yes或no。

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

  允许跟踪工作站用户对话并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  允许跟踪工作站硬软件组成并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  允许跟踪工作反病毒组件启动与结束运行并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

- <keep-infection enabled="" />

  允许跟踪工作站的威胁侦测并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  允许跟踪工作站扫描错误并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  允许跟踪工作站扫描统计信息并将信息记录到Dr.Web服务器数据库。enabled允许值为：yes或no。

- <keep-installation enabled="" />

  允许跟踪工作站代理端安装信息并将信息记录到Dr.Web服务器数据库。enabled允许值为：yes或no。

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

  允许跟踪组件办公控制阻止的设备的信息并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  允许跟踪工作站应用程序监控阻止的进程的活动（用于填写应用程序目录），并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  允许跟踪工作站应用程序监控阻止进程，并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

- <quarantine enabled="" />

  允许跟踪工作站隔离区状态并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  Dr.Web服务器和代理端间传递更新时的最大网络流量带宽（KB/秒）。

  属性介绍：

属性	有效值	描述	默认值
queue-size	• 正整数 • unlimited.	同时从Dr.Web服务器启动的更新分发对话最大数量。达到这一限量时代理端请求将列入等待队列。等待队列长度不限。	unlimited
value	• 最大速度KB/秒 • unlimited.	传输更新时总传速上限。	unlimited

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

  安装代理端过程在从Dr.Web服务器传递数据的最大网络流量带宽（KB/秒）。

  属性介绍：

属性	有效值	描述	默认值
queue-size	• 正整数 • unlimited.	同时从Dr.Web服务器启动的代理端安装对话最大数量。达到这一限量时代理端请求将列入等待队列。等待队列长度不限。	unlimited
value	• 最大速度KB/秒 • unlimited.	安装代理端时数据传输总传速上限。	unlimited

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

  允许在Dr.Web服务器间同步工作站的地理位置。

  属性介绍：

属性	有效值	描述
enabled	• yes——允许同步， • no——停用同步。	同步模式
startup-sync	正整数	在Dr.Web服务器间建立连接时询问工作站地理坐标时无此信息的工作站数量。

- <audit enabled="" />

  允许跟踪管理员在Dr.Web安全管理中心的操作并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  允许跟踪Dr.Web服务器内部操作并将信息记录到Dr.Web服务器数据库。enabled允许值为：yes或no。

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

  允许跟踪通过Web API进行的操作并将信息记录到Dr.Web服务器数据库。enabled允许值为： yes或no。

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

  通过HTTP代理服务器连接Dr.Web服务器的密码。

  属性介绍：

属性	有效值	描述
auth-list	• none——不使用身份验证， • any——支持的任一方式， • safe——支持的任一安全方式， • 以下方式如使用多个，则需要指定所有必要的方式，用空格隔开： ▫ basic ▫ digest ▫ digestie ▫ ntlmwb ▫ ntlm ▫ negotiate	代理服务器身份认证类型。默认设置为'any'。
enabled	• yes——使用代理服务器， • no——不使用代理服务器。	通过HTTP代理服务器连接Dr.Web服务器的模式。
host	-	代理服务器地址。
password	-	代理服务器用户密码，如在代理服务器要求进行身份验证。
user	-	代理服务器用户名，如在代理服务器要求进行身份验证。

  指定代理服务器登录身份验证方式时可以使用标记only（使用空格后添加在方式列表最后），此标记用于更改身份验证方式选择算法。

  详见https://curl.se/libcurl/c/CURLOPT_HTTPAUTH.html。

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

  向Doctor Web公司https://stat.drweb.com/发送病毒事件统计信息的相关参数。

  属性介绍：

属性	有效值	描述	默认值
enabled	• yes——发送统计信息， • no——不发送统计信息。	向Doctor Web公司发送统计信息的模式。	–
id	–	代理端MD5授权密钥	–
interval	正整数	发送统计信息的时间间隔，以分钟计。	30

- **<cluster>**

  反病毒网络多服务器配置时Dr.Web服务器群集用于交换信息的参数。

  包含一个或多个子元素<on multicast-group="" port="" interface="" />。

  属性介绍：

属性	描述
multicast-group	Dr.Web服务器交换信息使用的multicast组的IP地址。
port	将信息发送给multicast组使用的传输协议捆绑的网络接口的端口号。
interface	将信息发送给multicast组使用的传输协议捆绑的网络接口的IP地址。

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

  使用multicast协议向工作站发送组更新的设置。属性enabled允许值为： yes 或 no。

  元素<multicast-updates>包含多个子元素和属性：

子元素	属性	描述	默认值
port <port value="" />	value	发送更新multicast传输协议捆绑Dr.Web服务器网络接口的端口号。所有multicast组都将使用此端口。 进行组更新必须指定一个可用的端口，要不同于Dr.Web服务器本身运行传输协议设置中的端口。	2197
ttl <ttl value="" />	value	可传递UDP数据报生命期。此设置值用于所有multicast组。	8
-group <group address="" />	address	工作站获得组更新使用的multicast组的IP地址。	233.192.86.0用于IPv4 FF0E::176用于IPv6
on	interface	发送更新multicast传输协议捆绑Dr.Web服务器网络接口的IP地址。	–

子元素	属性	描述	默认值
<on interface="" ttl="" />	ttl	通过指定网络接口传递的UDP数据报生命期。相比常规子元素<ttl value="" />具有优先权。	8
transfer <transfer datagram-size="" assembly-timeout="" updates-interval="" chunks-interval="" resend-interval="" silence-interval="" accumulate-interval="" announce-send-times="" />	datagram-size	UDP数据报大小——multicast协议使用的UDP数据报大小，以字节计。 可用值区间为512–8192。为避免分节，建议设置的数值要小于所使用网络的MTU（Maximum Transmission Unit）。	1400
	assembly-timeout	文件传输时长（毫秒）——在指定时间段内传输一个更新文件，之后Dr.Web服务器开始传输下一个文件。 所有在使用multicast协议更新时未能传输的文件将在进行常规更新时使用TCP协议传输。	180000
	updates-interval	组更新长度（毫秒）——使用multicast协议更新的时长。 所有在使用multicast协议更新时未能传输的文件将在进行常规更新时使用TCP协议传输。	600000
	chunks-interval	数据包发送的时间间隔（毫秒）——向multicast组发送数据包的时间间隔。 过小的时间间隔可能导致传输过程中数据包丢失并造成网络超负载。不建议更改此参数。	14
	resend-interval	申请重发的时间间隔（毫秒）——代理端以此时间间隔发出要求重新发送丢失的数据包的申请。 Dr.Web服务器收集这些申请，之后重发丢失的数据。	1000
	silence-interval	"静候"时长（毫秒）——在指定时间前结束文件发送时，如在"静候"时长内没有收到代理端要求重发丢失的数据包的申请，则Dr.Web服务器认为所有代理端都已接收到更新文件，并开始发送下一个文件。	10000
	accumulate-interval	收集重发申请的时长（毫秒）——在指定时长内Dr.Web服务器收集代理端发出的要求重发丢失的数据包的申请。 代理端再次要求重发丢失的数据包。Dr.Web服务器收集这些申请，之后重发丢失的数据。	2000

子元素	属性	描述	默认值
	announce-send-times	文件传输预通知次数——Dr.Web服务器开始传递更新前向multicast组发送文件传输预通知的次数。 预通知时向multicast组发送有元数据文件的UDP数据报。增加预通知次数可以提高传递的可靠性，但可能会导致按照multicast协议进行更新的时间段内能够传输的数据量下降。	3

元素 <multicast-updates> 可以含有子元素<acl>，用于创建权限列表。使用这一子元素可以限制从此Dr.Web服务器按照multicast协议获取组更新的工作站的TCP地址范围。默认没有子元素<acl> ，也就是没有任何限制。

<multicast-updates>中的<acl>包含以下子元素：

- <priority mode="" />

  确定列表优先级。属性mode允许值为：allow或deny。值为<priority mode="deny"/>时，列表<deny>优先级高于列表<allow>。未列入任何列表或两个列表都列入的地址为禁止。只允许列表<allow>中包含且不包含于列表<deny >的地址。

- <allow>

  可按照multicast协议更新的TCP地址列表。元素<allow> 包含一个或几个子元素<ip address="" />，用于设定IPv4格式的允许的地址，和<ip6 address="" />，用于设定IPv6格式的允许的地址。属性address中输入网络地址，格式为：*<IP地址>*/[*<前缀>*]。

- <deny>

  不可按照multicast协议更新的TCP地址列表。元素<deny> 包含一个或几个子元素<ip address="" />，用于设定IPv4格式的允许的地址，和<ip6 address="" />，用于设定IPv6格式的允许的地址。属性address中输入网络地址，格式为：*<IP地址>*/[*<前缀>*]。

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

  确定数据库。

  属性介绍：

属性	有效值	描述	默认值
connections	正整数。	数据库与Dr.Web服务器的连接数量上限。没有接到技术支持部门建议的情况下不可对此参数进行修改。	2
speedup	yes | no	在结束初始化、更新和导入后自动执行推迟的数据库清空（详见管理员手册中的数据库）。	yes

元素<database> 包含以下一个子元素：



元素<database>只包含一个确定具体数据库的子元素。

数据库属性，可能包含于配置文件面板，但没有列入描述，未得到Doctor Web公司技术支持部门同意的情况下不应进行更改。

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

  确定内设数据库SQLite3。

  属性介绍：

属性	有效值	描述	默认值
dbfile		数据库文件名称。	database.sqlite
cache	SHARED | PRIVATE	缓存模式	SHARED
cachesize	正整数。	数据库缓存大小 (以1.5Kb页面计)。	2048
precompiledcache	正整数。	预编译sql缓存大小（以字节计）。	1048576
synchronous	• TRUE或FULL——同步 • FALSE或NORMAL——常规 • OFF——异步	数据写入模式。	FULL
checkintegrity	quick | full | no	启动Dr.Web服务器时检查数据库的完整性。	quick
autorepair	yes | no	启动Dr.Web服务器时自动还原数据库镜像。	no
mmapsize	正整数	一次允许显示到进程地址空间的数据库文件最大大小，以字节计。	• 对于OS UNIX——10485760 • 对于Windows操作系统——0
wal	yes | no	使用主动记录（Write-Ahead Logging）。	yes
wal-max-pages		"脏"页数量上限，达到此限后将页记录到磁盘。	1000
wal-max-seconds		延迟磁盘记录页的最长时间（以秒计）。	30

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

  确定外设数据库PostgreSQL。

属性介绍：

属性	有效值	描述	默认值
dbname		数据库文件名称。	
host		PostgreSQL服务器地址或UNIX域套接字路径。	
port		PostgreSQL服务器端口或UNIX套接字文件扩展名。	
options		用于发送至数据库服务器命令行参数。 详见第18章 https://www.postgresql.org/docs/9.1/libpq-connect.html	
requiressl	• 1 | 0（利用管理中心） • y | n • yes | no • on | off	只使用SSL连接。	• 0 • y • yes • on
user		数据库用户名	
password		数据库用户密码	
temp_tablespaces		数据库临时表格名称空间	
default_transaction_isolation	• read uncommitted • read committed • repeatable read • serializable	交易隔绝程度。	read committed

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

  确定外设Oracle数据库。

  属性介绍：

属性	有效值	描述	默认值
connectionstring		此行包含Oracle SQL Connect URL或Oracle Net参数对值。	
user		数据库用户注册名	
password		数据库用户密码	

属性	有效值	描述	默认值
client		Oracle数据库访问客户端路径（Oracle Instant Client）。Dr.Web服务器与Oracle Instant Client版本11一起供货。如使用的是更高版本的Oracle服务器或Oracle数据库驱动程序存在错误，可从Oracle公司官网下载相应的驱动程序后再此栏输入驱动程序路径。	
prefetch-rows	0-65535	执行数据库请求预选行数。	0——使用值 = 1（数据库默认）
prefetch-mem	0-65535	执行数据库请求预选占用的内存大小。	0——不限

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

  确定通过ODBC连接外设数据库。

  属性介绍：

属性	有效值	描述	默认值
dsn		ODBC的数据源名称。	drwcs
user		数据库用户注册名	drwcs
pass		数据库用户密码	drwcs
limit	正整数	在达到指定交易数后转接至DBMS。	0——不转接
transaction	• SERIALIZABLE——有序性 • READ_UNCOMMITTED——读取未固定数据 • READ_COMMITTED——读取固定数据 • REPEATABLE_READ——读取可重复性 • DEFAULT——同于 ""——取决于DBMS。	交易隔绝程度。 某些DBMS只包含READ_COMMITTED。	DEFAULT

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

  确定外设数据库MySQL/MariaDB。

  属性介绍：

属性	有效值	描述	默认值
dbname		数据库名称	drwcs
host	二选一。	按照TCP/IP连接时数据库服务器地址。	localhost

属性	有效值	描述	默认值
		使用UDS时UNIX套接字文件路径。如未给出，Dr.Web服务器会尝试在常规目录mysqld查找文件。	/var/run/mysqld/
port	二选一。	按照TCP/IP连接数据库使用的端口号。	3306
		使用UDS时UNIX套接字文件名称。	mysqld.sock
user		数据库用户注册名	""
password		数据库用户密码	""
ssl	yes | 任意另一字符串	只使用SSL连接。	no
precompiledcache	正整数。	预编译sql缓存大小（以字节计）。	1048576

- **<acl>**

  访问限制列表。用于限制代理端、网络安装程序和其它（"邻居"）服务器访问此Dr.Web服务器使用的网络地址。

  元素<acl>包含以下子元素，限制相应类型的连接：

  - <install>——Dr.Web代理端安装程序连接此Dr.Web服务器使用的IP地址限制列表。
  - <agent>——Dr.Web代理端连接此Dr.Web服务器使用的IP地址限制列表。
  - <links>——邻居Dr.Web服务器连接此Dr.Web服务器使用的IP地址限制列表。
  - <discovery>——*Dr.Web服务器发现服务*接收多播请求使用的IP地址限制列表。

  所有自元素包含相同的内部元素组成，内部元素指定以下限制：

  - <priority mode="" />

    列表优先级。属性mode允许值为：allow或deny。值为<priority mode="deny"/>时，列表<deny>优先级高于列表<allow>。未列入任何列表或两个列表都列入的地址为禁止。只允许列表<allow>中包含且不包含于列表<deny >的地址。

  - <allow>

    允许访问的TCP地址列表。元素<allow> 包含一个或几个子元素<ip address="" />，用于设定IPv4格式的允许的地址，和<ip6 address="" />，用于设定IPv6格式的允许的地址。属性address中输入网络地址，格式为：*<IP地址>*/[*<前缀>*]。

  - <deny>

    禁止其访问的TCP地址列表。元素<deny> 包含一个或几个子元素<ip address="" />，用于设定IPv4格式的允许的地址，和<ip6 address="" />，用于设定IPv6格式的允许的地址。属性address中输入网络地址，格式为：*<IP地址>*/[*<前缀>*]。

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

  脚本运行剖析参数设置。

  属性介绍：

属性	有效值	描述	默认值
profile	• yes， • no。	将Dr.Web服务器脚本运行剖析信息写入日志。此参数供技术支持和研发人员使用。如无特殊需要，不建议更改。	no
stack		将Dr.Web服务器脚本运行时调用堆栈信息写入日志。此参数供技术支持和研发人员使用。如无特殊需要，不建议更改。	
trace		将Dr.Web服务器脚本运行追踪信息写入日志。此参数供技术支持和研发人员使用。如无特殊需要，不建议更改。	

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

  Lua解释器路径。

  > 指定路径的顺序有影响。

  元素<lua-module-path>包含以下子元素：

  - <cpath root="" />——到二进制模块目录的路径。属性root允许值为：home（默认值）、var、bin、lib。
  - <path value="" />——到脚本目录的路径。如不是元素<jobs>或<hooks>的子元素，则同时应用于两个元素。在属性value中给出的路径相对于属性root的元素<cpath>中给出的路径。
  - <jobs>——Dr.Web服务器日程中任务的路径。

    元素<jobs>包含一个或多个子元素<path value="" />，用于指定到脚本目录的路径。
  - <hooks>——Dr.Web服务器用户进程路径。

    元素<hooks>包含一个或多个子元素<path value="" />，用于指定到脚本目录的路径。

- **<transports>**

  Dr.Web服务器连接客户端使用的传输协议参数设置。包含一个或几个子元素<transport discovery="" ip="" name="" multicast="" multicast-group="" port="" />。

  属性介绍：

属性	描述	必填项	有效值	默认值
discovery	确定是否使用Dr.Web服务器发现服务。	否，只能同ip一同设置。	yes,no	no
• ip • unix	确定所使用的协议家族和接口地址。	是	-	• 0.0.0.0 • -
name	为Dr.Web服务器发现服务指定Dr.Web服务器名称。	否	-	drwcs
multicast	确定Dr.Web服务器是否列入multicast组。	否，只能同ip一同设置。	yes,no	no

属性	描述	必填项	有效值	默认值
multicast-group	指定Dr.Web服务器所属multicast组的地址。	否，只能同ip一同设置。	-	• 231.0.0.1 • [ff18::231.0.0.1]
port	监听的端口号	否，只能同ip一同设置。	-	2193

- **<protocols>**

  停用协议列表。包含一个或多个子元素<protocol enabled="" name="" />。

  属性介绍：

属性	有效值	描述	默认值
enabled	• yes——协议为启用， • no——协议为停用。	协议使用模式。	no
name	• AGENT——Dr.Web服务器与Dr.Web代理端的交互作用协议。 • MSNAPSHV——Dr.Web服务器与Microsoft系统运行性能检查组件 NAP Validator的交互作用协议。 • INSTALL——Dr.Web服务器与Dr.Web代理端安装程序的交互作用协议。 • CLUSTER——群集系统中各Dr.Web服务器间的交互作用协议。 • SERVER——Dr.Web服务器与其他Dr.Web服务器的交互作用协议。	日志名称	-

- **<plugins>**

  停用插件列表。包含一个或多个子元素<plugin enabled="" name="" />。

  属性介绍：

属性	有效值	描述	默认值
enabled	• yes——插件为启用， • no——插件为停用。	插件使用模式。	no
name	• WEBMIN——Dr.Web安全管理中心通过管理中心管理Dr.Web服务器和反病毒网络的插件。 • FrontDoor——插件Dr.Web Server FrontDoor，用于连接Dr.Web服务器远程诊断工具。	插件名称	-

- **<license>**

  授权设置。

  元素<license>包含以下子元素：

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

    设置已超过授权数量限制的通知

    属性介绍：

属性	描述	默认值
min-count	剩余授权数量降为此值时会发送已超过授权数量限制的通知	3
min-percent	剩余授权数量降至此比例时会发送已超过授权数量限制的通知	5

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

  设置授权使用情况报告。

  属性介绍：

属性	描述	默认值
report-period	按照此周期在Dr.Web服务器创建服务器已使用授权密钥报告。 如在Dr.Web子服务器创建，会在创建后立即将报告发送至Dr.Web主服务器。 此外每次连接Dr.Web服务器（包括重启）以及Dr.Web主服务器分发的授权数量发生变化时都会发送报告。	1440
active-stations-period	在此周期内计算活跃工作站的数量，以发送授权使用报告。0值表示报告将统计所有工作站，不论是否处于活跃状态。	0

- `<exchange>`

  在Dr.Web服务器间分发授权的设置。

  元素`<exchange>`包含以下子元素：

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

  元素描述：

元素	描述	属性**value**默认值，分钟
expiration-interval	**分发出去的授权的有效期**——从此Dr.Web服务器密钥分发出去的授权的有效期。如此Dr.Web服务器向Dr.Web邻居服务器分发授权，则使用此设置。	1440
prolong-preact	**接收的授权延期期限**——授权有效期剩余期限，自此期限起此Dr.Web服务器请求延长从Dr.Web邻居服务器接收的授权。如此Dr.Web服务器从Dr.Web邻居服务器接收授权，则使用此设置。	60
check-interval	**授权同步周期**——Dr.Web服务器间分发的授权进行信息同步的时间间隔。	1440

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

  设置从管理中心发送邮件的参数，如发送管理员通知或群发工作站安装包。

  属性介绍：

属性	有效值	描述	默认值
from	-	邮件发件人电子邮箱地址。	drwcs@localhost
debug	• yes——使用调试模式， • no——不使用调试模式。	调试模式用于获得SMTP对话过程详细日志。	no

  元素<email> 包含以下子元素：

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

    在SMTP-服务器发送邮件邮件参数设置。

    属性介绍：

属性	有效值	描述	默认值
server	-	SMTP服务器地址，用于发送邮件。	127.0.0.1
user	-	SMTP服务器用户名，如SMTP服务器要求身份验证。	-
pass	-	SMTP服务器用户密码，如SMTP服务器要求身份验证。	-
port	正整数	用于发送邮件的SMTP服务器的端口。	25
start_tls	• yes——使用此类型的身份验证， • no——不使用此类型的身份验证。	用于交换数据时加密。这时通过指令STARTTLS转为受保护的连接。默认连接使用的端口为25。	yes
auth_plain		在邮件服务器使用*plain text*身份验证。	no
auth_login		在邮件服务器使用*LOGIN*身份验证。	no
auth_cram_md5		在邮件服务器使用*CRAM-MD5*身份验证。	no
auth_digest_md5		在邮件服务器使用*DIGEST-MD5*身份验证。	no
auth_ntlm		在邮件服务器使用*AUTH-NTLM*身份验证。	no
conn_timeout	正整数	与SMTP服务器连接的超时时限。	180

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

  发送邮件时SSL加密参数设置。

  属性介绍：

属性	有效值	描述	默认值
enabled	• yes——使用SSL， • no——不使用SSL。	SSL加密使用模式。	no
verify_cert	• yes——检查SSL证书， • no——不检查SSL证书。	检查邮件服务器的SSL证书。	no
ca_certs	-	Dr.Web服务器SSL根证书路径。	-

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

  跟踪网络病毒流行的参数设置。

  属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	允许追踪工作站感染多次事件，并可将汇总通知发送给管理员。	yes
aggregation-period	正整数。	发送病毒流行的通知后不再发送个别感染事件通知的时间段，以秒计。	300
check-period		在此时段内如发生一定数量的感染，则发送病毒流行通知，以秒计。	3600
threshold		通知数量，在指定时间段内如果收到的感染通知达到此数量，则Dr.Web服务器会向管理员发送一个病毒流行汇总通知（通知网络病毒流行）。	100
most-active		病毒流行报告必须记录的最常见的威胁的数量。	5

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

  追踪预防性保护组件多次性事件的参数设置。

  属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	允许追踪预防性保护多次事件，并可将汇总通知发送给管理员。	yes
aggregation-period	正整数。	发送预防性保护事件汇总通知后不再发送个别事件通知的时间段，以秒计。	300

属性	有效值	描述	默认值
check-period		在此时段内如发生一定数量的预防性保护事件，则发送汇总通知，以秒计。	3600
threshold		如在指定时间间隔出现此数量的预防性保护事件，Dr.Web服务器会向管理员发送包含所有事件的汇总通知（通知**预防性保护汇总报告**）。	100
most-active		预防性保护报告必须记录的最常见的进行可疑操作的进程的数量。	5

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

  追踪应用程序监控组件多次性事件的参数设置。

  属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	允许追踪应用程序监控组件多次事件，并可将汇总通知发送给管理员。	yes
aggregation-period	正整数	发送应用程序监控阻止进程汇总通知后不再发送个别阻止通知的时间段，以秒计。	300
check-period		在此时段内如一定数量的进程被阻止，则发送汇总通知，以秒计。	3600
threshold		如在指定时间间隔内应用程序监控阻止的进程达到此数量，Dr.Web服务器会向管理员发送包含所有事件的汇总通知（通知**记录到应用程序监控大量阻止进程**）。	100
most-active		阻止依据最多的模式数量，大量阻止通知中必须列入这些模式。	5

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

  追踪与客户端连接大量非正常中断的参数设置。

  属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	允许追踪与客户端连接的非正常中断，并可向管理员发送相应通知。	yes
aggregation-period	正整数。	发送连接大量中断的通知后不再发送连接中断个别通知的时间段，以秒计。	300
check-period		在此时段内如与客户端的连接发生一定数量的中断，则发送相应通知，以秒计。	3600

属性	有效值	描述	默认值
single-alert-threshold		与同一地址在计数时段内出现连接中断数量达到这一最低值后发送连接非正常结束个别通知（通知**连接非正常结束**）。	10
summary-alert-threshold		与同一地址在计数时段内出现连接中断数量达到这一最低值后发送多起连接非正常结束通知（通知**记录到多起连接非正常结束**）。	1000
min-session-duration		如与客户端连接时长低于此值，则只要达到指定的连接数量值就会发送个别连接结束通知（通知**连接非正常结束**），不再取决于计算结束的连接的时段。此后连接不应以更长时间的连接尝试中断，已不应发送多起连接非正常结束通知（通知**记录到多起连接非正常结束**）。	300

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

  如果未能从Dr.Web服务器数据库获得语言设置，Dr.Web服务器系统和组件使用的默认语言。包括因数据库受损无法获得语言设置时Dr.Web安全管理中心和管理员通知系统使用的语言。

G2. Dr.Web安全管理中心配置文件

管理中心配置文件webmin.conf为XML格式，位于Dr.Web服务器根目录的etc子目录。

Dr.Web安全管理中心配置文件参数介绍：

- **<version** value="">

  Dr.Web服务器当前版本。

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

  Dr.Web服务器名称。

  格式为：

  <服务器IP地址或DNS名称>[:*<端口>*]

  如未给出Dr.Web服务器地址，则使用操作系统返回的计算机名称或Dr.Web服务器网络地址：DNS名称（如有），或IP地址。

  如果未给出端口号，则使用申请中的端口（如从管理中心或通过**Web API**访问Dr.Web服务器时）。从管理中心访问时是管理中心连接Dr.Web服务器时地址行中给出的端口。

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

  Web页面目录路径。默认为value="webmin"。

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

  模块目录路径。默认为value="webmin"。

- **<threads** value=""/>

  Web服务器处理的平行申请数量。此参数影响服务器性能。无特殊情况不建议更改。

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

  处理网络传输数据的线程数量。此参数影响Dr.Web服务器性能。无特殊情况不建议更改。

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

  按照HTTP/HTTPS通过与Web服务器连接通道传输数据时的流量压缩设置。

  属性介绍：

属性	描述	默认值
value	压缩等级为1到9，1为最低，9为最高。	9
max-size	需压缩的HTTP回应最大大小。设置为0时取消对应压缩的HTTP回应最大大小的限制。	51200KB
min-size	需压缩的HTTP回应大小的最小值。设置为0时取消对应压缩的HTTP回应最大大小的限制。	32字节

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

  支持HTTP对话。用于设置使用HTTP1.X.版本的不间断的连接。

  属性介绍：

属性	描述	默认值
timeout	HTTP对话超时时限。使用不间断连接时如在此时限内没有接到客户端请求，Dr.Web服务器会中断连接。	15秒
send-rate	发送数据的最低速度。如网络出港传输速度低于此值则拒绝连接。设置为0时取消限制。	1024字节/秒
receive-rate	接收数据的最低速度。如网络进港传输速度低于此值则拒绝连接。设置为0时取消限制。	1024字节/秒

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

  发送和接收数据缓存大小设置。

  属性介绍：

属性	描述	默认值
send	用于发送数据的缓存区大小。此参数影响Dr.Web服务器性能。无特殊情况不建议更改。	8192字节
receive	用于接收数据的缓存区大小。此参数影响Dr.Web服务器性能。无特殊情况不建议更改。	2048字节

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

  HTTP请求大小上限（KB）。

- `<xheaders>`

  用于添加自定义HTTP头信息的参数。默认已存在三个头信息，用于抵御网络进攻：

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

    头信息在侦测到页面受到攻击（如 "XSS进攻"）后的内嵌代码时控制浏览器的行为。可用值为：

值	浏览器行为
0	XSS过滤器已停用。
1	XSS过滤器已启用。侦测到XSS进攻时浏览器会删除内嵌代码。
1; mode=block	XSS过滤器已启用。侦测到XSS进攻时浏览器不会加载被解锁的页面，为默认使用。
1; report=<网络地址>	XSS过滤器已启用。侦测到XSS进攻时浏览器会删除内嵌代码并像指定地址发送报告。只支持以Chromium为基础的浏览器。

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

  默认值（nosniff）情况下头信息禁止浏览器执行替换MIME格式的文件。

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

  头信息在侦测到将网页内置到他方框架（"点击劫持"攻击）时控制浏览器的行为。可用值为：

值	浏览器行为
DENY	头信息禁止浏览器在架构加载页面。
SAMEORIGIN	允许浏览器在架构加载页面，如页面和框架同源（域名、端口和协议相同），为默认使用。
ALLOW-FROM <网络地址>	只有当页面符合指定的地址时才允许浏览器在架构加载页面。

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

  在Dr.Web服务器日志文件将计算机IP地址更换为DNS名称。enabled允许值为：yes或no。

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

  在浏览器显示脚本错误（错误500）。此参数供技术支持和研发人员使用。如无特殊需要，不建议更改。

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

  启动脚本运行追踪。此参数供技术支持和研发人员使用。如无特殊需要，不建议更改。
  enabled允许值为：yes或no。

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

  管理剖析。将测量性能——Web服务器脚本和功能执行时长。此参数供技术支持和研发人员使用。如无特殊需要，不建议更改。

  属性介绍：

属性	有效值	描述
enabled	• yes——启用剖析， • no——停用剖析。	脚本剖析模式。
stack	• yes——将数据写入日志， • no——不将数据写入日志。	将剖析信息（功能参数和反馈值）写入Dr.Web服务器日志。

- <abort-scripts enabled=""/>

  允许在客户端中断连接时中断脚本运行。此参数供技术支持和研发人员使用。如无特殊需要，不建议更改。enabled允许值为：yes或no。

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

  使用页面本地版本。如允许此模式，服务器会根据客户端Accept-Language一栏的优先语言搜索页面的本地版本。enabled允许值为：yes或no。

- <default-lang value=""/>

  HTTP请求中没有Accept-Language时Web服务器返回的文件的语言。属性value值为语言的ISO码。默认为ru。

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

  SSL证书设置。

  属性介绍：

属性	描述	有效值	默认值
certificate	SSL证书文件路径	-	certificate.pem
private-key	SSL私钥文件路径	-	private-key.pem
keep-alive	使用SSL不间断连接。老版本的浏览器可能不支持不间断的SSL连接。如运行SSL协议出现问题，请停用此参数。	• yes， • no。	yes

- <listen>

  监听连接参数设置。

  元素<listen> 包含以下子元素：

  - <insecure>

    接收HTTP协议未加密连接时监听的接口列表。默认为9080。

    元素<insecure>包含一个或几个子元素<endpoint address=""/>，用于设定IPv4和IPv6格式的允许的地址。属性address中输入网络地址，格式为：*<协议>://<IP地址>*。

  - <secure>

    接收HTTPS协议加密连接时监听的接口列表。默认为9081。

    元素<secure > 包含一个或几个子元素<endpoint address="" />，用于设定IPv4和IPv6格式的允许的地址。属性address中输入网络地址，格式为：*<协议>://<IP地址>*。

- <access>

  访问限制列表。用于限制Web服务器接收HTTP和HTTPS请求使用的网络地址。

  元素<access > 包含以下子元素，限制相应类型的连接：

  - <secure priority="">

    接收HTTPS协议加密连接时监听的接口列表。默认为9081。

    属性介绍：

属性	有效值	描述	默认值
priority	allow	HTTPS允许优先——未列入任何列表（或两个列表都包含的）地址为允许使用的地址。	deny

属性	有效值	描述	默认值
	deny	HTTPS禁止优先——未列入任何列表（或两个列表都包含的）地址为禁止使用的地址。	

元素<secure >包含一个或几个以下子元素：<allow address=""/>和<deny address=""/>。

元素描述：

元素	描述	属性address默认值
allow	允许按照HTTPS协议加密连接进行访问的地址。	tcp://127.0.0.1
deny	禁止按照HTTPS协议加密连接进行访问的地址。	-

- <insecure priority="">

接收HTTP协议未加密连接时监听的接口列表。默认为9080。

属性介绍：

属性	有效值	描述	默认值
priority	allow	HTTP允许优先——未列入任何列表（或两个列表都包含的）地址为允许使用的地址。	deny
	deny	HTTP禁止优先——未列入任何列表（或两个列表都包含的）地址为禁止使用的地址。	

元素<insecure >包含一个或几个以下子元素：<allow address=""/>和<deny address=""/>。

元素描述：

元素	描述	属性address默认值
allow	允许按照HTTP协议未加密连接进行访问的地址。	tcp://127.0.0.1
deny	禁止按照HTTP协议未加密连接进行访问的地址。	-

G3. 配置文件download.conf

文件**download.conf** 的用途：

1. 建立Dr.Web服务器群集系统可在群集的Dr.Web服务器间分配负载，以接通更多数量的新工作站。
2. 在Dr.Web服务器使用非标准端口，可以为生成代理端安装文件指定这一端口。

文件download.conf用于为反病毒网络新工作站生成代理端安装文件。利用该文件参数可以设定代理端安装程序接通Dr.Web服务器所使用的Dr.Web服务器地址和端口，格式为：

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

其中：

- *<Server_Address>*——Dr.Web服务器IP地址或DNS名称。

  生成代理端安装包时首先从download.conf文件提取Dr.Web服务器地址。如果文件download.conf中未指定Dr.Web服务器地址，则使用webmin.conf文件中的参数值ServerName。或者使用由操作系统返回的计算机名称。

- *<port_number>*——代理端安装程序接通Dr.Web服务器使用的端口。

  如果文件download.conf中未指定端口，则默认情况下使用端口2193（设置于管理中心**管理部分 → Dr.Web服务器配置→ 的网络 → 标签传输**标签）。

默认情况下download.conf中注释参数download。使用download.conf文件必须取消这一参数的注释：去掉行首的"--"，然后设定相应的Dr.Web服务器地址和端口号。

G4. Dr.Web代理服务器配置文件

代理服务器配置文件drwcsd-proxy.conf为XML格式文件，位置在：

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

Dr.Web代理服务器配置文件参数说明：

- <listen spec="">

  根元素 <drwcsd-proxy > 含一个或几个必需元素 <listen >，确定代理服务器接收连接的主要设置。

  元素<listen > 含一个必需的属性spec，用于确定在哪一接口"监听"客户端传入连接以及是否在此接口启用discovery模式。

  元素spec属性值：

属性	必需属性	有效值	描述	默认值
ip |unix	是	–	接收传入连接使用的协议类型。参数值为代理服务器监听的地址。	0.0.0.0 | -
port	否	–	代理服务器监听的端口号。	2193
discovery	否	yes, no	Dr.Web服务器仿真模式。允许客户端将代理服务器作为Dr.Web服务器进行多播搜索。	yes
multicast	否	yes, no	代理服务器接收多播申请的"监听"模式。	yes
multicast-group	否	–	代理服务器所在的多播组。	231.0.0.1 [ff18::231.0.0.1]

取决于不同协议，属性spec所包含非必需属性列表的会发生变化。
不同协议下属性spec中可以指定（+）或不可以指定（–）的非必需属性列表：

协议	属性值			
	port	**discovery**	**multicast**	**multicast-group**
ip	+	+	+	+
unix	+	–	–	–



如何情况下都必须明指启用**discovery**模式，包括已启用**multicast**模式的情况。

存在Dr.Web服务器名单时的地址重定向方式见管理员手册。

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

元素<**compression** >作为元素<**listen** >的子元素确定客户端-代理服务器间通道的压缩参数。
属性介绍：

属性	有效值	描述	默认值
mode	yes	启用压缩。	possible
	no	停用压缩。	
	possible	可能压缩。	
level	1至9的整数	压缩等级。只适用于客户端—代理服务器通道	8

- **<encryption** mode="">

元素<**encryption** >作为元素<**listen** >的子元素确定客户端—代理服务器间通道的加密参数。
属性介绍：

属性	有效值	描述	默认值
mode	yes	启用加密。	possible
	no	停用加密。	
	possible	可能加密。	

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

指定重定向进港连接的设置。元素 <**forward** > 为必需项。而且可指定几个参数值不同的 <**forward** > 元素。
属性介绍：

属性	有效值	描述	必填项
to	地址需按照 网络地址特点给出，如以格式 tcp/*<DNS_name>*:*<port>* 给出。	将向其重定向连接的Dr.Web服务器地址。	是
master	• yes——Dr.Web服务器将是无条件的控制服务器。 • no——Dr.Web服务器任何情况下都不会是控制服务器。 • possible——只有没有绝对控制服务器（属性master值为yes的服务器）时此Dr.Web服务器才作为控制服务器。	此属性确定是否可以从to指定分Dr.Web服务器管理中心远程编辑代理服务器设置。 可将任意数量的Dr.Web服务器指定为控制服务器（参数值master="yes"），按照代理服务器设置依次连接所有Dr.Web控制服务器，直至第一次获取非空白配置。 也可以不将任何一个Dr.Web服务器指定为控制服务器（参数值master="no"）。这时只可通过代理服务器配置文件对代理服务器参数进行设置（包括指定Dr.Web控制服务器）。	否

如Dr.Web服务器的属性master缺省，默认认为master="possible"。

在安装代理服务器时由安装程序创建的配置文件中不指定任何Dr.Web服务器的master属性。

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

元素<**compression** >作为元素<**forward** />的子元素确定Dr.Web服务器—代理服务器间通道的压缩参数。属性同上。

- <**encryption** mode="">

元素<**encryption** >作为元素<**listen** >的子元素确定Dr.Web服务器—代理服务器间通道的加密参数。属性同上。

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

元素<**update-bandwidth** >用于限制Dr.Web服务器向客户端发送更新的传输速度以及同时下载更新的客户端数量。

属性介绍：

属性	有效值	描述	默认值
value	• KB/s • unlimited	传输更新时总传速上限。	unlimited
queue-size	• 正整数 • unlimited	同时从Dr.Web服务器启动的更新分发对话最大数量。达到这一限量时代理端请求将列入等待队列。等待队列长度不限。	unlimited

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

元素<**update-bandwidth** >可以有一个或几个子元素<**bandwidth** >。此元素可以设定指定时间段内的数据传速上限。

属性介绍：

属性	有效值	描述	默认值
value	• KB/s • unlimited	更新代理端时传输数据时总传速上限。	unlimited
time-map	–	限制生效的时间段的通配符。	–

在管理中心Web界面指定相应设置后会自动给出属性值time-map（参见管理员手册的远程设置代理服务器）。目前尚未有方便的方式通过配置文件来手动设置time-map。

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

元素<install-bandwidth/>用于限制安装代理端时数据传输速度以及同时下载安装数据的客户端数量。

属性介绍：

属性	有效值	描述	默认值
value	• KB/s • unlimited	安装代理端时数据传输总传速上限。	unlimited
queue-size	• 正整数 • unlimited	同时从Dr.Web服务器启动的代理端安装对话最大数量。达到这一限量时代理端请求将列入等待队列。等待队列长度不限。	unlimited

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

元素<install-bandwidth >可以有一个或几个子元素<bandwidth >。此元素可以设定指定时间段内的数据传速上限。

属性介绍：

属性	有效值	描述	默认值
value	• KB/s • unlimited	安装代理端时传输数据时总传速上限。	unlimited
time-map	–	限制生效的时间段的通配符。	–

在管理中心Web界面指定相应设置后会自动给出属性值time-map（参见管理员手册的远程设置代理服务器）。目前尚未有方便的方式通过配置文件来手动设置time-map。

- <cache enabled="">

设置代理服务器库缓存。

属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	确定是否已启用缓存。	yes

元素<cache> 包含以下子元素：

元素	有效值	描述	默认值
<maximum-revision-queue size="">	正整数	保存的校检数量。	3
<clean-interval value="">	正整数	清空校检记录时间间隔，以分钟计。	60
<unload-interval value="">	正整数	从内存卸载未使用文件的时间间隔，以分钟计。	10
<repo-check mode="">	idle | sync	或在启动时检查缓存完整性（需占用较长时间），或以背景模式检查。	idle

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

代理服务器和Dr.Web服务器库同步设置。

属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	确定是否启用库同步。	yes
schedule	–	进行所选产品同步的日程。	–

在管理中心Web界面指定相应设置后会自动给出属性值schedule（参见管理员手册的远程设置代理服务器）。目前尚未有方便的方式通过配置文件来手动设置schedule。

子元素 <product name="">为将进行同步的产品列表：

- 05-drwmeta——Dr.Web服务器安全数据，
- 10-drwbases——病毒库，
- 10-drwgatedb——SpIDer Gate库，
- 10-drwspamdb——反垃圾邮件库，
- 10-drwupgrade——Dr.Web更新模块，
- 15-drwhashdb——已知威胁哈希值，
- 20-drwagent——用于Windows操作系统的Dr.Web代理端，
- 20-drwandroid11——用于Android操作系统的Dr.Web数据库，
- 20-drwcs——Dr.Web服务器，
- 20-drwunix——用于UNIX操作系统的Dr.Web代理端，
- 20-drwcsdoc——帮助文档，
- 40-drwproxy——Dr.Web代理服务器，
- 70-drwextra——Dr.Web企业产品，
- 70-drwutils——Dr.Web管理员工具，
- 80-drwnews——Doctor Web公司新闻。

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

缓存从代理端获取的事件的设置。

属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	确定是否已启用事件缓存。 如启用将按照日程向Dr.Web服务器发送事件。如果停用缓存，则代理服务器接收到事件后会立即发送给Dr.Web服务器。	yes
schedule	–	发送从代理端接收的事件的日程。	–



在管理中心Web界面指定相应设置后会自动给出属性值schedule（参见管理员手册的远程设置代理服务器）。目前尚未有方便的方式通过配置文件来手动设置schedule。

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

代理服务器的自动更新设置。

启用了自动更新时如启用了同步，则按照同步日程（见上）从Dr.Web服务器加载代理服务器更新，并按照更新日程安装（默认为无时间限制）。如停用同步，则按照更新日程加载和安装（默认为无时间限制）。

属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	确定是否启用自动更新。	yes
schedule	–	加载（如未指定同步）并安装更新的日程。	–



在管理中心Web界面指定相应设置后会自动给出属性值schedule（参见管理员手册的远程设置代理服务器）。目前尚未有方便的方式通过配置文件来手动设置schedule。

默认为允许自动更新，无时间限制。

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

出现SEH排除项时收集内存转储的模式和数量。



仅可在Windows操作系统下设置内存转储。

收集内存转储OS需存在库dbghelp.dll。

转储保存于目录：%APPDATA%\Doctor Web\drwcsd-proxy\dump\

属性介绍：

属性	有效值	描述	默认值
enabled	yes | no	确定是否启用收集转储。	yes

属性	有效值	描述	默认值
maximum	正整数	最多转储数量。删除更早的转储。	10

- <dns>

  DNS设置。

  <timeout value="">

  允许正向/反向DNS请求的超时时限（以秒计）。为空时不限定等待允许的时间。

  <retry value="">

  未能成功允许DNS请求时重复DNS请求的最多次数。

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

  缓存保存DNS服务器响应的时限。

  属性介绍：

属性	有效值	描述
enabled	• yes——缓存中保存回应， • no——缓存中不保存回应。	缓存回应的模式。
negative-ttl	–	在缓存（TTL）保存DNS服务器负响应的时限，以分钟计。
positive-ttl	–	在缓存（TTL）保存DNS服务器正响应的时限，以分钟计。

  <servers>

  包含一个或多个子元素 <server address="">，其中参数address确定服务器IP地址。替代系统默认列表的DNS服务器列表。

  <domains>

  替代系统默认列表的DNS服务器列表。包含一个或多个子元素 <domain name=""/>，其中参数name确定域名。

G5. 库加载器配置文件

库加载器配置文件drwreploader.conf为XML格式，位于Dr.Web服务器安装目录的etc子目录。

使用配置文件

- 控制台工具中文件路径应在参数--config指定。
- 图形工具中文件应位于工具本身所在目录。无配置文件启动图形工具时会在工具本身所在目录创建配置文件，并在之后启动时使用。

库加载器配置文件参数说明：

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

  属性介绍：

属性	描述	有效值
value	加载更新的模式： • repository——以Dr.Web服务器库格式加载库。加载的文件可直接利用管理中心导入，用于更新Dr.Web服务器库。 • mirror——以GUS更新区格式加载库。加载的文件可置于本地网络的更新镜像。之后可将Dr.Web服务器设置为直接从此更新镜像获取最新版本的库，而不是从GUS服务器获取。	repository | mirror
path	加载库的目录。	–
archive	自动将加载的库压缩为zip压缩文件。使用此选项获得的文件可通过管理中心的管理→库内容导入到Dr.Web服务器。	yes | no
key	Dr.Web授权密钥。也可只指定密钥的MD5哈希，可在管理中心的管理→授权管理器查看。	–

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

  库加载器运行日志设置：

  属性介绍：

属性	描述	有效值
path	日志文件路径。	–
verbosity	日志记录的详细等级。默认为TRACE3。	ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRIT。参数值ALL和DEBUG3意义相同。
rotate	格式为 *<N><f>, <M><u>*的日志轮循模式。设置同Dr.Web服务器日志轮循。 默认值为10，10m，即保存10个大小为10MB的文件，使用压缩。	–

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

  库加载器常规设置。

  属性介绍：

属性	描述	有效值
url	GUS服务器包含Dr.Web产品更新的目录。	–
proto	从更新服务器获取更新使用的协议类型。所有协议下更新加载都遵循GUS服务器列表设置。	http | https | ftp | ftps | sftp | scp | file
cdn	允许在加载库时使用Content Delivery Network。	yes | no
update-key	用于检查从GUS加载的更新签名的公钥路径或公钥目录路径。用于检查更新真实性的公钥update-key-*.upub在Dr.Web服务器的etc目录。	–
version	需加载更新的Dr.Web服务器版本。	–

- <servers>

更新服务器列表。表中GUS服务器顺序确定加载库时加载器的访问次序。

所含子元素<server>指定更新服务器。

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

如服务器要求进行身份验证，登录更新服务器的用户身份验证信息。

属性介绍：

属性	描述
user	登录更新服务器的用户名。
password	登录更新服务器的密码。

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

通过代理服务器连接GUS的连接参数。

属性介绍：

属性	描述
host	所使用的代理服务器的网络地址。
port	所使用的代理服务器的端口。默认为3128。
user	登录代理服务器的用户名，如代理服务器要求进行身份验证。
password	登录代理服务器的用密码，如代理服务器要求进行身份验证。

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

可自动接受的SSL证书设置。此设置只用于支持加密的安全协议。

属性介绍：

属性	描述	有效值
cert-mode	将自动接受的证书。	▫ any——接受所有证书， ▫ valid——只接受有效的SSL证书，

属性	描述	有效值
		▫ drweb——只接受Dr.Web证书， ▫ custom——接受自定义证书。
cert-file	证书文件路径。	–

▫ <ssh mode="" pubkey="" prikey="">

按照SCP/SFTP连接时在更新服务器进行身份验证的类型。

属性介绍：

属性	描述	有效值
mode	身份验证类型。	▫ pwd——使用密码登录。密码在<auth />指定。 ▫ pubkey——按照公钥进行身份验证。公钥在属性pubkey给出或者从prikey指定的私钥提取。
pubkey	SSH公钥	–
prikey	SSH私钥	–

- <products>

可加载产品设置。

▫ <product name="" update="">

分别设置每一产品。

属性介绍：

属性	描述	有效值
name	产品名称。	• 05-drwmeta——Dr.Web服务器安全数据， • 10-drwbases——病毒库， • 10-drwgatedb——SpIDer Gate库， • 10-drwspamdb——反垃圾邮件库， • 10-drwupgrade——Dr.Web更新模块， • 15-drwhashdb——已知威胁哈希值， • 20-drwagent——用于Windows操作系统的Dr.Web代理端， • 20-drwandroid11——用于Android操作系统的Dr.Web数据库， • 20-drwcs——Dr.Web服务器， • 20-drwunix——用于UNIX操作系统的Dr.Web代理端， • 20-drwcsdoc——帮助文档， • 40-drwproxy——Dr.Web代理服务器， • 70-drwextra——Dr.Web企业产品， • 70-drwutils——Dr.Web管理员工具， • 80-drwnews——Doctor Web公司新闻。

属性	描述	有效值
update	启动这一产品的加载。	yes | no

- <schedule>

  定期更新日程。这时不需要手动启动加载器，库加载器将按照指定的时间间隔自动启动。

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

    设置按日程进行加载。

属性	描述	有效值
period	加载任务执行周期。	• every_n_min——每N分钟， • hourly——每小时， • daily——每日， • weekly——每周。
enabled	已启用加载任务。	yes | no
min	开始执行任务的分钟。	从0到59的整数
hour	开始执行任务的整点。适用于daily和weekly。	从0到23的整数
day	周几执行任务。适用于weekly。	• mon——星期一， • tue——星期二， • wed——星期三， • thu——星期四， • fri——星期五， • sat——星期六， • sun——星期日。

附录H. Dr.Web Enterprise Security Suite所含软件命令行参数

命令行参数比默认设置或其它长期设置（Dr.Web服务器配置文件、OS Windows注册表中的设置等等）更为优先。在某些情况下启动时指定的参数还会取代永久设置。详情见下。

在介绍部分程序参数语法时非必需部分使用方括号[...]。



附录H所介绍的特点不适用于代理端网络安装程序。

部分命令行参数以连字符开始。此类参数称为钥匙。

有许多命令参数有不同的格式。如表示逻辑意义（是/否、禁止/允许）的参数有否定格式：例如参数-admin-rights和其对应的意义相反的参数-no-admin-rights为一个参数对。也可明指参数值，如 -admin-rights=yes和-admin-rights=no。



参数值yes的同义词为on、true、OK。no的同义词为off、false。

如参数值含空格会制表符，整个参数都需使用括号，例如：

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



参数名称可以简略（省去后面的字母），但省略后的名称不可与任何一个其它参数的名称出现重复。

在Windows操作系统可以使用参数elevate来强行执行管理员权限指令。具体操作是将此参数加到其他参数之前，例如：drwcsd elevate start.

H1. 网络安装程序

启动命令格式：

```
drwinst.exe [<参数>]
```

参数



命令行参数在启动所有类型的代理端安装文件是都有效。

代理端网络安装程序启动参数格式为：/<*参数*> <*值*>。

所有参数值前为空格。如：

```
/silent yes
```

如参数值含空格、制表符或符号\，整个参数值都需使用引号，例如：

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

可用参数：

- /compression <*模式*>——与Dr.Web服务器流量的压缩模式。<*模式*>可为：
  - yes——使用压缩。
  - no——不使用压缩。
  - possible——可能压缩。最终是否压缩取决于Dr.Web服务器端的设置。

  如未给出参数，默认值为possible。
- /encryption <*模式*>——与Dr.Web服务器流量的加密模式。<*模式*>可为：
  - yes——使用加密。
  - no——不使用加密。
  - possible——可能加密。最终是否加密取决于Dr.Web服务器端的设置。

  如未给出参数，默认值为possible。
- /excludeFeatures <*组件*>——在工作中安装时必须排除的组件列表。指定多个组件时中间用 ","隔开。可指定为不安装的组件有：
  - scanner——Dr.Web扫描仪，
  - spider-mail——SpIDer Mail，
  - spider-g3——SpIDer Guard，
  - outlook-plugin——Dr.Web for Microsoft Outlook，
  - firewall——Dr.Web防火墙，
  - spider-gate——SpIDer Gate，
  - parental-control——办公控制，
  - antispam-outlook——Dr.Web反垃圾邮件，用于组件Dr.Web for Microsoft Outlook，
  - antispam-spidermail——Dr.Web反垃圾邮件，用于组件SpIDer Mail。

  未明指的组件遵照其默认安装模式。
- /id <*工作站识别码*>——安装代理端的工作站的识别码。

  此参数和Dr.Web服务器自动登录参数/pwd一同给出。如未给出登录参数，是否允许登录取决于Dr.Web服务器端。
- /includeFeatures <*组件*>——在工作中安装时必须安装的组件列表。指定多个组件时中间用 ","隔开。可指定为必须安装的组件有：
  - scanner——Dr.Web扫描仪，
  - spider-mail——SpIDer Mail，
  - spider-g3——SpIDer Guard，

- outlook-plugin——Dr.Web for Microsoft Outlook，
- firewall——Dr.Web防火墙，
- spider-gate——SpIDer Gate，
- parental-control——办公控制，
- antispam-outlook——Dr.Web反垃圾邮件，用于组件Dr.Web for Microsoft Outlook，
- antispam-spidermail——Dr.Web反垃圾邮件，用于组件SpIDer Mail。

未明指的组件遵照其默认安装模式。

- /installdir *<目录>*——安装目录。

  如未给出参数，默认情况下是系统盘的文件夹"Program Files\DrWeb"。
- /installtimeout *<时间>*——从管理中心远程安装时等待工作站响应的超时时限，以秒计。

  如未给出参数，默认值为300秒。
- /instMode *<模式>*——安装文件启动模式。*<模式>*可为：
  - remove——删除已安装产品。

  如未给出参数，默认安装程序自动确定启动模式。
- /lang *<语言代码>*——安装程序和所安装的产品的语言。语言代码格式为ISO-639-1。

  如未给出参数，默认使用系统语言。
- /pubkey *<证书>*——Dr.Web服务器证书文件完整路径。

  如证书未给出，默认情况下启动本地安装时安装程序自动从其启动目录调出证书文件*.pem。如证书文件不在安装程序启动目录，需手动给出证书文件的完整路径。

  启动在管理中心创建的安装包时，安装包包含证书，不需要通过命令行参数给出证书。
- /pwd *<密码>*——代理端登录Dr.Web服务器使用的密码。

  此参数和Dr.Web服务器自动登录参数/id一同给出。如未给出登录参数，是否允许登录取决于Dr.Web服务器端。
- /regagen*<模式>*——确定代理端是否注册到在已安装程序列表。*<模式>*可为：
  - yes——在已安装程序列表中注册代理端。
  - no——不在已安装程序列表中注册代理端。

  如未给出参数，默认值为no。
- /retry *<数量>*——利用发送多播请求搜索Dr.Web服务器的尝试次数。如尝试次数达到此限量而Dr.Web服务器未响应，则认为未找到Dr.Web服务器。

  如未给出参数，默认Dr.Web服务器搜索次数为3次。
- /server [*<协议>*/]*<服务器地址>*[:*<端口>*]——Dr.Web服务器地址，从此服务器安装代理端，代理端安装后连接到此服务器。

  如未给出参数，默认使用多播请求搜索Dr.Web服务器。
- /silent *<模式>*——确定是否以背景模式启动安装程序。*<模式>*可为：
  - yes——以背景模式启动安装程序。
  - no——以图形模式启动安装程序。

  如未给出参数，默认以图形模式安装代理端（参见 **安装手册** 的利用安装程序安装Dr.Web代理端）。

- `/timeout` *<时间>*——搜索Dr.Web服务器时等待每一响应的超时时限，以秒计。未超过此时限时继续接收响应。

  如未给出参数，默认值为3秒。

H2. Windows操作系统Dr.Web代理端

启动命令格式：

`es-service.exe [<参数>]`

参数

每一参数可用以下一种格式给出：

`-<短参数>[ <值>]`

或

`-<长参数>[ <值>]`

不同参数可同时使用，包括同时使用短参数和长参数。



如参数值包含空格，需使用引号将参数值引上。

所有参数的执行不取决于Dr.Web服务器上为工作站开通的权限。也就是说如果Dr.Web服务器上禁止更改代理端设置，您也可利用命令行参数更改这些设置。

可用参数：

- 显示帮助文档：
  - `-?`
  - `--help`
- 更改代理端连接的Dr.Web服务器地址：
  - `-e` *<Dr.Web服务器>*
  - `--esserver=`*<Dr.Web服务器>*

  同时指定多个Dr.Web服务器，需为每一Dr.Web服务器重复参数，用空格隔开，例如：

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

  或

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

- 添加加密公钥：
  - `-p` *<密钥>*

- --addpubkey=*<密钥>*

作为参数指定的公钥复制到代理端目录（默认为目录%ProgramFiles%\DrWeb），重命名为drwcsd.pub（如名称有别），并重读。这时如找到上一公钥文件，则重命名为drwcsd.pub.old且不再使用。

所有之前使用的公钥（包括之前从Dr.Web服务器接收和保存在注册表的密钥）将保存，如需可以使用。

- 添加Dr.Web服务器证书：
  - -c *<证书>*
  - --addcert=*<证书>*

作为参数指定的Dr.Web服务器证书复制到代理端目录（默认为目录%ProgramFiles%\DrWeb），重命名为drwcsd-certificate.pem（如名称有别），并重读。这时如找到上一公钥文件，则重命名为drwcsd-certificate.pem.old且不再使用。

所有之前使用的证书（包括之前从Dr.Web服务器接收和保存在注册表的证书）将保存，如需可以使用。

- 作为新工作站连接服务器：
  - -w *<值>*
  - --newbie=*<值>*

有效值：once，always。如指定为always则每次启动服务时都会清空代理端登录参数，也就是说每次代理端都要作为新工作站连接服务器（详见**管理员手册**中的工作站连接策略）。如指定为once则下一次启动服务时都会清空代理端登录参数，之后代理端要作为新工作站连接服务器，清空和重新连接都只进行一次。

- 更改代理端日志详细等级：
  - --change-loglevel=*<等级>*

日志详细等级有效值：err、 wrn、 inf、 dbg、 all。 启动此指令需使用管理员权限。不需要停用自我保护以及手动重启服务或操作系统。

H3. Dr.Web服务器

存在几种用于启动Dr.Web服务器的命令，将分别加以介绍。

有些指令要求命令行中必须有参数modexec或modexecdb来执行Lua模块或是传输辅助参数。这时指令的格式为：

drwcsd [*<参数>*] modexec [*<功能名称>*@] *<模块名称>* [*<参数>*]

- *<功能名称>*——需在Lua模块执行的具体功能的名称。
- *<模块名称>*——可执行Lua模块的名称。

H3.1. Dr.Web服务器的管理——H3.5. Dr.Web服务器关键数据备份所列命令为跨平台命令，如无特殊说明，即可用于OS Windows，也可用于UNIX家族操作系统。



启用Dr.Web服务器控制指令时如出现错误请查看Dr.Web服务器日志文件寻找原因（参见**管理员手册**中的Dr.Web服务器运行日志）。

H3.1. Dr.Web服务器的管理

`drwcsd [<参数>]`——用于Dr.Web服务器运行设置（参数介绍见下）。

H3.2. 基本指令

- `drwcsd restart`——执行Dr.Web服务器服务的完全重启（先执行`stop`，然后执行`start`）。
- `drwcsd start`——启动Dr.Web服务器。
- `drwcsd stop`——正常结束Dr.Web服务器运行。
- `drwcsd stat`——将运行统计信息，包括CPU时间、内存占用等等写入日志文件（UNIX家族操作系统下类似指令`send_signal WINCH`或`kill SIGWINCH`）。
- `drwcsd modexec agent@verify-key` *<密钥文件完整名称>*——检查授权密钥（`agent.key`）是否有效。
- `drwcsd modexec enterprise@verify-key` *<密钥文件完整名称>*——检查Dr.Web服务器授权密钥（`enterprise.key`）的正确性。注意，从版本10开始，不再使用Dr.Web服务器授权密钥。
- `drwcsd verifyconfig` *<配置文件完整名称>*——检查Dr.Web服务器配置文件（`drwcsd.conf`）的语法。
- `drwcsd verifycache`——检查Dr.Web服务器缓存文件内容的有效性。
- `drwcsd syncads`——同步网络结构：Active Directory计算机容器转变为反病毒网络工作站组。

H3.3. 数据库管理指令

数据库初始化



进行初始化时应没有数据库或数据库为空。

`drwcsd [<参数>] modexecdb database-init [<授权密钥> [<密码>]]`——数据库初始化

- *<授权密钥>*——授权密钥Dr.Web `agent.key`的路径。如未指定授权密钥，需之后在管理中心添加，或者利用服务器间连接从Dr.Web邻居服务器获取。
- *<密码>*——Dr.Web服务器管理员初始密码（用户名为**admin**）。默认为**root**。



编写指令时如需跳过一个或多个参数，需使用专用参数值`%nil`取代。

`%nil`后如再无参数，可略去。

指定数据库初始化参数

使用内设数据库时可通过外部文件指定初始化参数，指令为：

`drwcsd.exe modexecdb database-init@<response-file>`

<response-file>——记录数据库初始化参数的文件，参数分行写入，顺序同`database-init`指令参数。

文件格式：

```
<授权密钥文件完整名称>
<管理员密码>
```



OS Windows下使用response文件时可在管理员密码中使用任何符号。

如命令行中有`%nil`，将使用默认值（与`database-init`相同）。

更新数据库版本

`drwcsd modexecdb database-upgrade [pretend=false]`——利用内部脚本升级时启动Dr.Web服务器更新数据库结构。

- `pretend=false`——是否只检查数据库结构是否为最新，而不是进行实际更新。默认为`false`。如设为`true`，则只检查数据库结构是否为最新。

导出数据库

a) `drwcsd modexecdb database-export <文件>`——将数据库导出到指定文件。

Windows操作系统下示例：

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

OS **UNIX**下以用户`drwcs:drwcs`名义执行操作至目录`$DRWCS_VAR`（OS **FreeBSD**除外，此系统下默认为将文件保存到启动脚本的目录。如明确指定路径，则安装时创建的*<用户>:<组>*应具备写入此目录的权限，默认为`drwcs:drwcs`）。

b) `drwcsd modexecdb database-export-xml <xml文件>`——将数据库导出到指定的xml文件。

如文件扩展名为`gz`，则导出数据库文件时压缩为gzip文档。

如不指定扩展名或扩展名不是`gz`，则导出文件时不压缩。

Windows操作系统下示例：

- 将数据库导出至xml文件，不压缩：

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

- 将数据库导出至xml压缩文件：

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

UNIX家族操作系统示例：

- 将数据库导出至xml文件，不压缩：

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

- 将数据库导出至xml压缩文件：

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

导入数据库

a) `drwcsd modexecdb database-import` *<文件>*——从指定文件导入数据库（覆盖原数据库内容）。

b) `drwcsd modexecdb database-import-and-upgrade` *<文件>* [<目录>]——导入并更新从上一版本Dr.Web服务器导出的数据库（数据库原有内容删除）。还可指定脚本目录，用于转用新版本时更新数据库结构（与指令upgradedb类似）。



使用指令database-import-and-upgrade前必须进行数据库备份。

执行这一指令过程中出现的任何问题都可能导致数据库全部信息被删除。

只能在同一DBMS内使用指令database-import-and-upgrade导入来更新数据库版本。

检查数据库

`drwcsd modexecdb database-verify [full=false [ignore-version=false]]`——启动Dr.Web服务器检查数据库。将检查结果信息记录到日志需在指令中加入参数`-log`。此参数使用说明见H3.8. 参数介绍。

- `full=false`——确定扫描模式。按照默认设置（`false`）进行快速扫描，设为`true`则进行完全扫描。
- `ignore-version=false`——确定执行扫描时是否忽略数据库结构版本。默认为`false`。设为`true`则即便是结构版本错误也同样执行扫描。

数据库运行提速

`drwcsd [<参数>] modexecdb database-speedup` ——执行指令VACUUM、CLUSTER、ANALYZE，加快运行数据库的速度。

恢复数据库

`drwcsd repairdb`——执行受损内设数据**SQLite3**的还原或外设数据库**MySQL**受损表格的还原。

启动Dr.Web服务器时可自动恢复**SQLite3**，如管理中心数据库**SQLite3**设置中勾选了**自动恢复受损镜像**（参见**管理员手册**中的恢复数据库）。

清空数据库

`drwcsd modexecdb database-clean`——清空Dr.Web服务器数据库，删除所有列表。

更换管理员密码

`drwcsd modexecdb set-admin-password` *<注册名>* *<新密码>* ——为相应的管理员账户指定新密码。

H3.4. 库管理指令



启用指令syncrepository、restorerepo和saverepo前必须停止Dr.Web服务器运行。

- `drwcsd syncrepository`——从Dr.Web GUS进行库同步。此命令启动Dr.Web服务器进程，连接GUS，如有更新则会随后更新库。
- `drwcsd rerepository`——从磁盘重读库。
- `drwcsd syncrepository`——从Dr.Web GUS进行库同步。此命令启动Dr.Web服务器进程，连接GUS，如有更新则会随后更新库。如Dr.Web服务器未启动，不进行库更新。
- `drwcsd [<参数>] restorerepo` *<压缩文件完整名称>*——从利用saverepo指令创建的指定zip压缩文件还原Dr.Web服务器库。
- `drwcsd [<参数>] saverepo` *<压缩文件完整名称>*——将整个Dr.Web服务器库保存到指定的zip压缩文件。此压缩文件可利用指令restorerepo导入Dr.Web服务器。



指令restorerepo和saverepo使用的压缩文件与通过管理中心导出和导入所使用的压缩文件不兼容。

H3.5. Dr.Web服务器关键数据备份

利用以下指令进行Dr.Web服务器重要数据（数据库内容、授权密钥文件、私钥、Dr.Web服务器和管理中心配置文件）备份：

```
drwcsd -home=<路径> backup [<目录> [<数量>]]
```

- Dr.Web服务器重要数据备份到指定的*<目录>*。
- 参数-home指定为Dr.Web服务器安装目录。
- 参数*<数量>*——同一文件的备份数量。

Windows操作系统下示例：

```
C:\Program Files\DrWeb Server\bin>drwcsd -home="C:\Program Files\DrWeb
Server" backup C:\a
```

备份中所有文件可使用，只有数据库内容除外。数据库备份保存为.gz格式，与gzip和其他存档兼容。可将数据库内容从备份导入到Dr.Web服务器工作数据库来恢复数据（参见恢复Dr.Web Enterprise Security Suite数据库）。

Dr.Web服务器运行过程中会定期在以下命令备份重要信息：

- OS **Windows**：*<安装磁盘>*:\DrWeb Backup
- OS **Linux**：/var/opt/drwcs/backup
- OS **FreeBSD**：/var/drwcs/backup

进行定期备份需在Dr.Web服务器日程中启用每日任务。如日志中暂无此任务，建议新建。

H3.6. 只可在OS Windows下使用的指令

- drwcsd [*<参数>*] install[*<服务名称>*]——在系统中安装Dr.Web服务器服务。

  <服务名称>——默认添加到服务名称的后缀，完整名称为：DrWebES-*<服务名称>*。指令install 创建（编辑）指定名称的服务并自动在其属性添写参数-service=*<服务名称>*。现有服务不会发生更改。
- drwcsd uninstall[*<服务名称>*]——从系统中删除Dr.Web服务器服务。

  。 *<服务名称>*——默认添加到服务名称的后缀，完整名称为：DrWebES-*<服务名称>*。
- drwcsd kill——紧急结束Dr.Web服务器服务（如未能正常结束）。除了紧急情况不要使用这一指令。
- drwcsd reconfigure——重读配置文件并重启（不需启动新进程，执行速度更快）。
- drwcsd silent[*<选项>*] *<指令>*——在运行*<指令>*所设指令时禁止Dr.Web服务器导出通知。可在命令文件使用，用于关闭Dr.Web服务器运行互动模式。

H3.7. 只可在UNIX下使用的指令

- drwcsd cacherepo——创建或还原Dr.Web服务器库文件缓存。
- drwcsd config——类似reconfigure或kill SIGHUP——重启Dr.Web服务器。

- drwcsd interactive——启动Dr.Web服务器，但不向进程转交管理权。
- drwcsd newkey——生成新的加密密钥drwcsd.pri和drwcsd.pub，以及证书drwcsd-certificate.pem。
- drwcsd readrepo——从磁盘重读库。与指令rerepository类似。
- drwcsd selfcert [*<计算机名称>*]——生成新的SSL证书 (certificate.pem) 和私钥RSA (private-key.pem)。参数是为其生成文件的Dr.Web服务器所在计算机名称。如未给出参数，由系统功能自动给出计算机名称。
- drwcsd shell *<文件名称>*——运行脚本文件。指令命令启动$SHELL或/bin/sh，传递所指定的文件。
- drwcsd showpath——显示系统记录的所有软件路径。
- drwcsd status——显示Dr.Web服务器当前状态（已启动、已停止）。

H3.8. 参数介绍

跨平台参数：

- -activation-key=*<授权密钥>*——Dr.Web服务器授权密钥。默认情况下为文件enterprise.key，在根目录中的etc子目录。

  注意，从版本10开始，不再使用Dr.Web服务器授权密钥。 从上一版本更新Dr.Web服务器和进行数据库初始化时会用到密钥-activation-key：需从这一密钥提取Dr.Web服务器识别码。
- -bin-root=*<目录>*——可执行文件路径。默认为根目录的bin子目录。
- -conf=*<文件>*——Dr.Web服务器配置文件名称和位置。默认情况下为文件drwcsd.conf，在根目录中的etc子目录。
- -daemon——Windows平台下表示作为服务启动。UNIX平台下："作为守护进程"（转为根目录、与终端断开、转为背景模式）。
- -db-verify=on——在启动Dr.Web服务器时检查数据库的完整性。为默认设置。特别强调不应以反义参数启动，只有使用drwcsd modexecdb database-verify命令检查数据库（见上）后立即启动的情况除外。
- -help——显示帮助文档。与上述程序的使用相同。
- -hooks——允许Dr.Web服务器执行以下文件夹中的用户扩展脚本：
  - OS Windows：var\extensions
  - OS FreeBSD：/var/drwcs/extensions
  - OS Linux：/var/opt/drwcs/extensions

  Dr.Web服务器安装目录。脚本用于使管理员的操作自动化，能简化和加快某些任务的完成。所有脚本默认为禁用。
- -home=*<目录>*——Dr.Web服务器安装目录（根目录）。目录结构见**安装手册**中的OS Windows下Dr.Web服务器的安装。默认为启动的当前目录。
- -log=*<日志文件>*——将Dr.Web服务器日志记录到指定路径的文件。

  UNIX平台Dr.Web服务器可用"减号"代替名称，表示常规显示日志。

  默认：Windows平台下drwcsd.log在参数-var-root指定的目录，UNIX平台下由参数-syslog=user指定（见下）。

- -private-key=*<私钥>*——Dr.Web服务器私钥。默认情况下drwcsd.pri在根目录中的etc子目录。
- -rotate=*<N><f>*, *<M><u>*——Dr.Web服务器运行日志轮值模式。

参数	描述
<N>	日志文件总数（包括当前文件和归档文件）。
<f>	日志文件保存格式，可用参数值： • z (gzip)——压缩文件，为默认设置， • p (plain)——不压缩文件。
<M>	日志文件大小或轮循时间，取决于*<u>*值；
<u>	衡量单位，可用参数值： • 按照日志文件大小轮询时： ▫ k——Kb， ▫ m——Mb， ▫ g——Gb， • 按照时间轮询时： ▫ H——小时， ▫ D——天， ▫ W——星期。



按照时间轮循时，不论启用命令是在什么时间，都进行同步：H——与小时开始之时同步，D——与一天的零点同步，W——与周一零点同步，依照*<u>*值中指定的次数。

起始时间为公元01年1月01日，UTC+0。

默认值为10z，10m，即保存10个大小为10MB的文件，使用压缩。也可利用特殊格式：none (-rotate=none)——表示"不使用轮循，总是记录到同一个文件，文件大小不限"。

使用轮循模式时使用的日志文件名称格式：file.*<N>*.log或file.*<N>*.log.dz，其中*<N>*——排序编号：1、2等等。

如日志文件名称（见上-log参数）指定为file.log，则：

- file.log——当前文件（进行写入的文件），
- file.1.log——上一个文件，
- file.2.log等等——数字越大，日志文件越陈旧。

- -trace——详细记录出现错误的地方。
- -var-root=*<目录>*——Dr.Web服务器有权写入的目录路径，用于保存可更改文件（如日志以及库文件）。默认是根目录的var子目录。
- --verbosity=*<等级>*——日志详细等级。默认值为WARNING。允许值为：ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRIT。参数值ALL和DEBUG3意义相同。

  如需可以为多个消息源指定详细等级，格式为：

-verbosity=*<消息源1>*:*<等级1>*, *<消息源2>*:*<等级2>*, *<消息源3>*:*<等级3>*等等。这时*<等级>*按照常规来继承，也就是找到最近的指定有详细等级的父源。格式中的-verbosity=all:all 等于-verbosity=all （参见附录K. 日志文件格式）。

此参数确定其后参数-log（见上）所指定的文件记录详细等级。一个指令可包含多个此类参数。

参数-verbosity 和 -log相互位置十分重要。

同时使用这两个参数时，参数-verbosity应在参数-log之前：参数-verbosity决定其后参数所指路径的日志文件详细等级。

只可在**OS Windows**下使用的参数：

- -minimized——窗口最小化（不是作为服务启动，而为互动模式启动的情况下）。
- -service=*<服务名称>*——启动的服务进程利用这一参数进行自身身份验证，并将自我保护安装到Dr.Web服务器服务注册表分支。 *<服务名称>* ——默认添加到服务名称的后缀：DrWebES-*<服务名称>*。

  此参数由指令install使用，不单独使用。
- -screen-size=*<大小>*——（不是作为服务启动，而为互动模式）——Dr.Web服务器窗口可见日志行大小，默认为1000。

只可在**UNIX**家族操作系统下使用的参数：

- -etc=*<路径>*——目录etc路径（<var>/etc）。
- -keep——安装Dr.Web服务器后不清空临时目录。
- -pid=*<文件>*——Dr.Web服务器用于记录进程识别码的文件。
- -syslog=*<模式>*——记录到系统日志。可用模式：auth、cron、daemon、kern、lpr、mail、news、syslog、user、uucp、local0-local7，某些平台下为ftp，authpriv和console。

参数-syslog和-log同时起作用。即如果启动Dr.Web服务器使用的参数是-syslog（例如service drwcsd start -syslog=user），Dr.Web服务器以-syslog参数值和-log默认值启动。

- -user=*<用户>*, -group=*<组>*——只用于OS UNIX，且使用用户名**root**启动时；表示更改进程的用户或组，以所指定的用户（组）权限执行。

H3.9. UNIX家族操作系统下的变量

为方便对UNIX家族操作系统Dr.Web服务器的管理，管理员可使用脚本文件中的变量，脚本保存在以下目录：

- OS Linux：/etc/init.d/drwcsd。
- OS FreeBSD：/usr/local/etc/rc.d/drwcsd（符号链接/usr/local/etc/drweb.com/software/init.d/drwcsd）。

变量对应的drwcsd命令行参数见表H-1.

表H-1.

参数	变量	默认参数
-home	DRWCS_HOME	• /usr/local/drwcs——用于OS FreeBSD， • /opt/drwcs——用于OS Linux。
-var-root	DRWCS_VAR	• /var/drwcs——用于OS FreeBSD， • /var/opt/drwcs——用于OS 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	

变量DRWCS_HOOKS和DRWCS_TRACE没有参数值。指定变量后执行脚本时添加相应的参数。不指定变量时不添加参数。

其他变量见表H-2.

表H-2.

变量	默认参数	描述
DRWCS_ADDOPT		命令行高级参数，启动时会传递给drwcsd。
DRWCS_CORE	unlimited	core文件最大大小。
DRWCS_FILES	131170	Dr.Web服务器可以打开的文件描述符最大数量。
DRWCS_BIN	$DRWCS_HOME/bin	启动drwcsd的目录。

变量	默认参数	描述
DRWCS_LIB	$DRWCS_HOME/lib	Dr.Web服务器库目录。

默认情况下如drwcsd脚本中未确定相应变量，则参数值生效。



变量DRWCS_HOME、DRWCS_VAR、DRWCS_ETC、DRWCS_USER、DRWCS_GROUP、DRWCS_HOOKS已在drwcsd脚本文件中确定。

如果存在文件/var/opt/drwcs/etc/common.conf，则此文件会列入drwcsd，并会重新确定某些变量，但如果不导出这些变量（使用指令export），则不产生影响。

指定变量

1. 将变量定义添加到drwcsd脚本文件。
2. 使用export指令导出变量（同时给出）。
3. 从此脚本启动另一进程时，进程将读取已确定的值。

H3.10. 利用指令kill管理UNIX操作系统Dr.Web服务器

UNIX操作系统Dr.Web服务器对工具kill发给Dr.Web服务器进程的信号进行管理。



可利用指令man kill调出工具kill的帮助文档。

工具信号及其执行的操作：

- SIGWINCH——将运行统计信息（CPU时间、内存占用等等）写入日志文件。
- SIGUSR1——从磁盘重读库，
- SIGUSR2——从磁盘重读通知模板，
- SIGHUP——重新启动Dr.Web服务器，
- SIGTERM——停止Dr.Web服务器，
- SIGQUIT——停止Dr.Web服务器，
- SIGINT——停止Dr.Web服务器。

在Windows操作系统Dr.Web服务器执行以上操作使用drwcsd指令，见附录 H3.3. 数据库管理指令。

H4. 用于Windows的Dr.Web扫描仪

工作站软件这一组件所使用的命令行参数见**Windows操作系统Dr.Web代理端**用户手册。唯一的区别是代理端启动扫描仪时参数/go /st一定会自动传递给扫描仪。

H5. Dr.Web代理服务器

设置代理服务器参数需使用相应参数运行执行文件drwcsd-proxy。该执行文件的位置在代理服务器安装目录的子目录bin。

启动命令格式

drwcsd-proxy[*<参数>*] [*<指令>* [*<指令参数>*]]

可用参数

跨平台参数：

- --console=yes|no——以对话窗口模式启动代理服务器。此时代理服务器运行日志记录到控制台。

  默认为no。
- --etc-root=*<路径>*——配置文件所在目录的路径（drwcsd-proxy.conf、drwcsd.proxy.auth等等）。

  默认为$var/etc
- --home=*<路径>*——代理服务器安装目录。

  默认为$exe-dir/
- --log-root=*<路径>*——代理服务器运行日志文件所在目录的路径。

  默认为$var/log
- --pool-size=*<N>*——与代理端交互作用的线程数量。

  默认为安装代理服务器的电脑的内核数量（但不小于2）。
- -rotate=*<N><f>*, *<M><u>*——代理服务器运行日志轮循模式，其中：

参数	描述
<N>	日志文件总数（包括当前文件和归档文件）。
<f>	日志文件保存格式，可用参数值： • z (gzip)——压缩文件，为默认设置， • p (plain)——不压缩文件。
<M>	日志文件大小或轮循时间，取决于*<u>*值；

<u>	衡量单位，可用参数值：
	• 按照日志文件大小轮询时：
	  ▫ k——Kb，
	  ▫ m——Mb，
	  ▫ g——Gb，
	• 按照时间轮询时：
	  ▫ H——小时，

参数	描述
	▫ D——天， ▫ W——星期。



按照时间轮循时，不论启用命令是在什么时间，都进行同步：H——与小时开始之时同步，D——与一天的零点同步，W——与周一零点同步，依照*<u>*值中指定的次数。

起始时间为公元01年1月01日，UTC+0。

默认值为10，10m，即保存10个大小为10MB的文件，使用压缩。

- --trace=yes|no——启用代理服务器调用详细日志记录。只有代理服务器支持调用堆栈详细日志记录时才可使用此参数。

  默认为no。

- --tmp-root=*<路径>*——临时文件目录的路径。自动更新代理服务器时使用。

  默认为$var/tmp。

- --var-root=*<路径>*——代理服务器工作目录路径，用于缓存和保存数据库。

  默认为：

  ▫ OS Windows：%ALLUSERSPROFILE%\Doctor Web\drwcs

  ▫ OS Linux：/var/opt/drwcs

  ▫ OS FreeBSD：/var/drwcs

- --verbosity=*<详细等级>*——日志详细等级。默认值为TRACE。允许值为：ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRIT。参数值ALL和DEBUG3意义相同。

  如需可以为多个消息源指定详细等级，格式为：

  -verbosity=*<消息源1>*:*<等级1>*,*<消息源2>*:*<等级2>*,*<消息源3>*:*<等级3>*等等。这时*<等级>*按照常规来继承，也就是找到最近的指定有详细等级的父源。格式中的-verbosity=all:all 等于-verbosity=all （参见附录K. 日志文件格式）。



代理服务器所有运行参数参数可同时给出。

UNIX®家族操作系统参数：

- --user——指定用户识别码。一般模式下运行和以守护进程模式运行都需要此参数。
- --group——指定组识别码。一般模式下运行和以守护进程模式运行都需要此参数。
- --pid=*<路径>*——进程识别码所在目录的路径。

  默认为：/var/opt/drwcs/run/drwcsd-proxy.pid

可用指令及其参数

如未给出指令，默认使用指令run。

- import *<路径>* [*<校检>*] [*<产品>*]——将Dr.Web服务器库文件导入到代理服务器缓存。
  - *<路径>*——Dr.Web服务器库所在目录的路径。需预先将Dr.Web服务器库下载到安装代理服务器的电脑。
  - *<校检>*——可导入的校检数量上限。如未指定，则导入所有校检。
  - *<产品>*——需导入的产品，用空格隔开。默认使用空白列表，即导入Dr.Web服务器之外的所有产品。如给出列表，则只导入列表中的产品。
- help——显示代理服务器设置参数说明文档。
- run——以常规模式启动代理服务器。

仅限**Windows**操作系统的指令：

- install——安装服务。
- start——启动已安装的服务。
- stop——停止已启动的服务。
- uninstall——删除服务。

仅限**UNIX**家族操作系统的指令：

- daemon——以守护进程模式启动代理服务器（参见UNIX®家族操作系统参数）。

代理服务器控制脚本和UNIX家族操作系统下可使用的变量

为方便对UNIX家族操作系统代理服务器的管理，管理员可使用脚本文件drwcsd-proxy.sh中的变量，脚本保存在以下目录：

- **Linux**：/etc/init.d/dwcp_proxy
- **FreeBSD**：/usr/local/etc/rc.d/dwcp_proxy

脚本接收以下指令：

- import *<路径>* [*<校检>*] [*<产品>*]——将Dr.Web服务器库文件导入到代理服务器缓存（与代理服务器指令类似，见上）。
- interactive——以对话窗口模式启动代理服务器。此时代理服务器运行日志记录到控制台。
- start——以守护进程模式启动代理服务器。
- status——检查守护进程是否已启动。
- stop——停止已启动的守护进程。

变量对应的drwcsd-proxy命令行参数见表H-3。

表H-3

参数	变量	默认参数
--home=*<路径>*	$DRWCS_PROXY_HOME	$exe-dir/
--var-root=*<路径>*	$DRWCS_PROXY_VAR	• OS Linux：/var/opt/drwcs • OS FreeBSD：/var/drwcs
--etc-root=*<路径>*	$DRWCS_PROXY_ETC	$var/etc
--tmp-root=*<路径>*	$DRWCS_PROXY_TMP	$var/tmp
--log-root=*<路径>*	$DRWCS_PROXY_LOG	$var/log
-	$DRWCS_PROXY_LIB	$DRWCS_PROXY_HOME/lib
-	$DRWCS_PROXY_BIN	$DRWCS_PROXY_HOME/bin
--verbosity=*<详细等级>*	$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
-	$NO_DRWCS_PROXY_USER	如为任意值，则忽略$DRWCS_PROXY_USER。
--user	$DRWCS_PROXY_USER	-
-	$NO_DRWCS_PROXY_GROUP	如为任意值，则忽略$DRWCS_PROXY_GROUP。
--group	$DRWCS_PROXY_GROUP	-
-	$DRWCS_PROXY_FILES	131170，但不低于当前额度。

H6. UNIX家族操作系统Dr.Web服务器安装程序

启动命令格式：

<数据包名称>.run [*<参数>*] [--] [*<值>*]

其中：

- [--]——独立分非必需符号，表示参数列表结尾，将参数列表与补充值列表分开。
- [*<值>*]——补充值或内嵌脚本。

可使用以下参数获取帮助文档或数据包信息：

- `--help`——显示参数说明文档。
- `--info`——显示数据包详细信息：名称；目标目录；解压后大小；压缩算法；打包日期；打包使用的`makeself`版本；打包使用的指令；解压后启动的脚本；是否会将压缩包内容复制到临时目录（如不复制，不做任何显示）；目标目录是否是永久目录或是在处理脚本后会被删除。
- `--lsm`——显示数据包基本信息内置LSM记录内容：名称、版本、描述、作者等等。如未记录LSM，会显示相应通知。
- `--list`——导出安装包文件列表。
- `--check`——检查安装包的完整性。

安装包启动参数：

- `--confirm`——在启动内嵌脚本时显示申请。
- `--noexec`——不启动内嵌脚本。
- `--keep`——在执行内嵌脚本后不删除指定目录。
- `--nox11`——在结束安装后不启动终端模拟器`xterm`。
- `--nochown`——不将发起安装的用户指定为所提取文件的所有人。
- `--log` *<路径>*——按照指定路径记录安装日志文件。
- `--nolog`——不记录安装日志。
- `--target` *<目录>*——将安装包解压至指定目录。
- `--tar` *<值_1>* `[`*<值_2>* `...]`——利用指令`tar`访问安装包内容。

补充参数：

- `--help`——显示补充参数说明文档。
- `--quite`——以背景模式启动安装程序。对安装程序提示的问题都作出肯定的回答：
  - 接受许可协议，
  - 在默认文件夹进行备份，
  - 在删除已安装在系统的补充软件（extra）后再继续进行安装。
- `--clean`——以Dr.Web服务器默认设置安装软件包，不使用备份恢复上一次安装的设置。
- `--preseed` *<路径>*——包含安装程序在安装过程中所提问题预设回答方式的配置文件路径。

  配置文件中预设回答方式的变量：
  - `DEFAULT_BACKUP_DIR=`*<路径>*——用于恢复上次安装设置的备份所在目录路径（如指定使用默认设置安装，则不使用此备份）。
  - `QUIET_INSTALL=[0|1]`——指定使用安装程序背景模式：
    - 0——以背景模式启动安装程序；
    - 1——以一般模式启动安装程序。
  - `CLEAN_INSTALL=[0|1]`——指定安装时使用备份：
    - 0——使用默认设置安装，不使用备份恢复原设置；

- 1——安装使用备份恢复原设置，备份所在目录由变量DEFAULT_BACKUP_DIR指定。如未指定变量DEFAULT_BACKUP_DIR，使用/var/tmp/drwcs中的备份。

- ADMIN_PASSWORD=*<密码>*——管理员账户默认（**admin**）。
  - 如文件中给出了ADMIN_PASSWORD变量，则会用作管理员密码，安装结束时会显示通知：
    Password specified in the configuration file for the default administrator (admin): *<密码>*
  - 如文件中未给出ADMIN_PASSWORD变量，则会自动生成密码，安装结束时会显示通知：
    Automatically generated password for the default administrator (admin): *<密码>*



如使用参数--preseed时配置文件没有利用变量QUIET_INSTALL=0指定以背景模式启动安装程序，则配置文件中所有其他变量均由用户在安装过程中给出。

H7. 工具

H7.1. 数字密钥和证书生成工具

提供以下数字密钥和证书生成工具控制台版本：

可执行文件	位置	描述
drweb-sign-*<操作系统>-<位数>*	管理中心的管理→工具部分	为工具的独立版本。可从自定义目录启动，可用于相应操作系统的任一计算机。
	Dr.Web服务器目录 webmin/utilities	
drwsign	Dr.Web服务器目录bin	此工具版本取决于是否具备服务器库。只能从所在目录启动。



工具版本drweb-sign-*<操作系统>-<位数>*和drwsign功能相同。以下介绍的是为drwsign版本，但所有示例同样适用于另一版本。

启动命令格式

- drwsign check [-public-key=*<公钥>*] *<文件>*

  检查此文件签名，使用<公钥>作为该文件签名者的公钥。

密钥参数	默认值
<公钥>	drwcsd.pub

- drwsign extract [-private-key=*<私钥>*] [-cert=*<Dr.Web服务器证书>*] *<公钥>*

  从私钥文件或证书文件提取公钥，将公钥写入指定文件。

  密钥-private-key和-cert不可并用，也就是说只能指定其中一个；同时指定会导致指令执行出错。

  必须为密钥指定参数。

  如未给出任何密钥，则使用-private-key=drwcsd.pri，从私钥 drwcsd.pri提取公钥。

密钥参数	默认值
<私钥>	drwcsd.pri

- drwsign genkey [*<私钥>* [*<公钥>*]]

  生成一对公—私钥并将其写入相应文件。

密钥参数	默认值
<私钥>	drwcsd.pri

密钥参数	默认值
<公钥>	drwcsd.pub



用于Windows平台的工具版本（有别于用于UNIX操作系统的版本）不能保护私钥不被复制。

- drwsign gencert [-private-key=*<私钥>*] [-subj=*<主体栏>*] [-days=*<有效期>*] [*<自签名证书>*]

  使用Dr.Web服务器私钥生成自签名证书并将证书写入相应文件。

密钥参数	默认值
<私钥>	drwcsd.pri
<主体栏>	/CN=*<主机名称>*
<有效期>	3560
<自签名证书>	drwcsd-certificate.pem

- drwsign gencsr [-private-key=*<私钥>*] [-subj=*<主体栏>*] [*<证书签名申请>*]

  在私钥基础上生成证书签名申请并将申请写入相应文件。

  可利用另一服务器进行证书签名，例如，使用Dr.Web服务器密钥为Dr.Web代理服务器进行证书签名。

  为此类申请签名使用的密钥是signcsr。

密钥参数	默认值
<私钥>	drwcsd.pri
<主体栏>	/CN=*<主机名称>*
<证书签名申请>	drwcsd-certificate-sign-request.pem

- drwsign genselfsign [-show] [-subj=*<主体栏>*] [-days=*<有效期>*] [*<私钥>* [*<自签名证书>*]]

  为Web服务器生成RSA自签名证书和RSA私钥并将其写入相应文件。

  参数-show将证书内容导出为可读模式。

密钥参数	默认值
<主体栏>	/CN=*<主机名称>*
<有效期>	3560
<私钥>	private-key.pem

密钥参数	默认值
<自签名证书>	certificate.pem

- drwsign hash-check [-public-key=*<公钥>*] *<哈希文件>* *<签名文件>*

  检查客户端-服务器协议格式中指定的256字节数字签名。

  在*<哈希文件>*给出需进行签名的256字节数字文件。*<签名文件>*是签名结果（两个256字节数字）。

密钥参数	默认值
<公钥>	drwcsd.pub

- drwsign hash-sign [-private-key=*<私钥>*] *<哈希文件>* *<签名文件>*

  为客户端-服务器协议格式中指定的256字节数字签名。

  在*<哈希文件>*给出需进行签名的256字节数字文件。*<签名文件>*是签名结果（两个256字节数字）。

密钥参数	默认值
<私钥>	drwcsd.pri

- drwsign help [*<指令>*]

  调查程序简要帮助文档或命令行格式具体指令说明。

- drwsign sign [-private-key=*<私钥>*] *<文件>*

  使用私钥为*<文件>*签名。

密钥参数	默认值
<私钥>	drwcsd.pri

- drwsign signcert [-ca-key=*<私钥>*] [-ca-cert=*<Dr.Web服务器证书>*] [-cert=*<需签名的证书>*] [-days=*<有效期>*] [-eku=*<用途>*] [*<已签名证书>*]

  使用Dr.Web服务器私钥和证书为准备好的*<需签名的证书>*签名。签名后的证书另存为新文件。

  可用于Dr.Web服务器密钥为Dr.Web代理服务器证书签名。

  密钥-eku（全名Extended Key Usage）有效值：

  - drwebServerAuth——由代理端验证服务器/代理服务器，
  - drwebMeshDAuth——由虚拟代理端验证扫描服务器

密钥参数	默认值
<私钥>	drwcsd.pri
<Dr.Web服务器证书>	drwcsd-ca-cerificate.pem
<需签名的证书>	drwcsd-certificate.pem

密钥参数	默认值
<有效期>	3560
<用途>	drwebServerAuth
<已签名证书>	drwcsd-signed-certificate.pem

- drwsign signcsr [-ca-key=*<私钥>*] [-ca-cert=*<Dr.Web服务器证书>*] [-csr=*<证书签名申请>*] [-days=*<有效期>*] [-eku=*<用途>*] [*<已签名证书>*]

  使用Dr.Web服务器私钥和证书为指令gencsr生成的*<证书签名申请>*签名。签名后的证书另存为新文件。

  可利用另一服务器进行证书签名，例如，使用Dr.Web服务器密钥为Dr.Web代理服务器进行证书签名。

  密钥-eku（全名Extended Key Usage）有效值：

  - drwebServerAuth——由代理端验证服务器/代理服务器，
  - drwebMeshDAuth——由虚拟代理端验证扫描服务器

密钥参数	默认值
<私钥>	drwcsd.pri
<Dr.Web服务器证书>	drwcsd-cerificate.pem
<证书签名申请>	drwcsd-certificate-sign-request.pem
<有效期>	3560
<用途>	drwebServerAuth
<已签名证书>	drwcsd-signed-certificate.pem

- drwsign tlsticketkey [*<TLS标签>*]

  生成TLS标签。

  可用于Dr.Web服务器群集共享TLS对话。

密钥参数	默认值
<TLS标签>	tickets-key.bin

- drwsign verify [-ss-cert] [-CAfile=*<Dr.Web服务器证书>*] [*<需检查的证书>*]

  根据Dr.Web服务器可信任证书检查证书合法性。

  参数-ss-cert指定忽略可信任证书，只检查自签名证书的有效性。

密钥参数	默认值
<Dr.Web服务器证书>	drwcsd-certificate.pem
<需检查的证书>	drwcsd-signed-certificate.pem

- `drwsign x509dump [<需打印的证书>]`

  打印任一x509证书转储。

密钥参数	默认值
<需打印的证书>	`drwcsd-certificate.pem`

- `drwsign version`

  导出工具版本信息。

H7.2. 内设数据库管理工具

工具`drwidbsh3`用于管理内设数据库(SQLite3)。

工具所在目录：

- OS **Linux**：`/opt/drwcs/bin`
- OS **FreeBSD**：`/usr/local/drwcs/bin`
- OS **Windows**：*<Dr.Web服务器安装目录>*`\bin`
  （默认Dr.Web服务器安装目录：`C:\Program Files\DrWeb Server`）。

启动命令格式：

`drwidbsh3` *<数据库文件完整名称>*

程序以文本对话模式运行，等待用户输入程序命令（命令以点开始）。

输入 `.help`后会显示其它命令的帮助文档。

其它信息将参阅SQL语言介绍。

利用工具drwidbsh3查看和更换密码的示例：



前提是要通过Dr.Web服务器配置文件预先停用管理员密码加密参数。详情参见G1. Dr.Web服务器配置文件部分的`passwd-salt`。

1. 使用数据库路径启动工具`drwidbsh3`：
   - 如果是OS Linux内设数据库：

```
/opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite
```

   - 如果是OS Windows内设数据库：

```
"C:\Program Files\DrWeb Server\bin\drwidbsh3" "C:\Program Files\DrWeb
Server\var\database.sqlite"
```

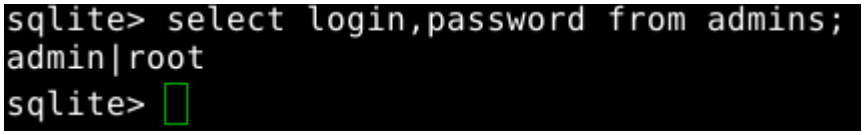
2. 查看`admins`列表中保存的所有数据需执行以下命令：

```
select * from admins;
```

3. 查看所有管理员账户用户名和密码需执行以下命令：

```
select login,password from admins;
```

4. 下图为命令执行结果示例，如只存在一个账户，用户名为admin，密码为root：



5. 更改密码使用的命令为update。以下为将账户admin的密码更改为qwerty的命令示例：

```
update admins set password='qwerty' where login='admin';
```

6. 退出工具使用的命令为：

```
.exit
```

H7.3. Dr.Web服务器远程诊断工具

Dr.Web服务器远程诊断工具可远程连接Dr.Web服务器进行基本管理，并可查看运行统计信息。图形版本只支持Windows操作系统。

工具的可用版本：

- OS Windows下为图形版本。
- UNIX家族操作系统下为控制台版本。

提供以下Dr.Web服务器远程诊断工具版本：

可执行文件	位置	描述
drweb-cntl-*<操作系统>*-*<位数>*	管理中心的管理→工具部分	为工具的独立版本。可从自定义目录启动，可用于相应操作系统的任一计算机。
	Dr.Web服务器目录 webmin/utilities	
drwcntl	Dr.Web服务器目录bin	此工具版本取决于是否具备服务器库。只能从所在目录启动。



工具版本drweb-cntl-*<操作系统>*-*<位数>*和drwcntl功能相同。以下介绍的是为drwcntl版本，但所有示例同样适用于另一版本。



连接Dr.Web服务器远程诊断工具必须启用插件Dr.Web Server FrontDoor。启用操作是在**Dr.Web**服务器配置的模块标签勾选插件**Dr.Web Server FrontDoor**。

连接Dr.Web服务器远程诊断工具要求管理员具备**使用高级功能**权限。否则会禁止管理员通过远程诊断工具访问Dr.Web服务器。

使用TLS连接工具（不论是图形工具还是控制台工具）都必须在指定Dr.Web服务器地址时直接给出协议：`ssl://`*<IP地址或DNS名称>*。

如何设置Dr.Web服务器来连接Dr.Web服务器远程诊断工具参见**管理员手册**的远程访问Dr.Web服务器。

工具的控制台版本

启动命令格式：

`drwcntl [-?|-h|--help] [+`*<日志文件>*`] [`*<服务器>* `[`*<注册用户名>* `[`*<密码>*`]]]`

其中：

- `-? -h --help`——导出工具使用指令帮助文档。
- *<日志文件>*——将工具的所有此写入指定路径的日志文件。
- *<服务器>*——工具连接的Dr.Web服务器地址，格式为：`[(tcp|ssl)://]`*<IP地址或DNS名称>*`[:`*<端口>*`]`。

  使用一种支持的协议进行连接的前提条件：

  a) 按照ssl连接时配置文件frontdoor.conf中应有标签<ssl />。这时只能按照ssl进行连接。

  b) 按照tcp连接时配置文件frontdoor.conf中应停用标签<ssl />。这时只能按照tcp进行连接。

  如未在Dr.Web服务器地址行给出连接参数，则使用：

参数	默认值
连接协议	tcp 使用TCP连接时需在管理中心**管理** → **远程访问Dr.Web服务器**取消对**使用TLS**的勾选。取消勾选后停用配置文件frontdoor.conf中的符号<ssl />。
Dr.Web服务器IP地址或DNS名称	工具要求以相应格式输入Dr.Web服务器地址。
端口	10101 Dr.Web服务器端允许的端口在**远程访问Dr.Web服务器**部分给出并保存在配置文件frontdoor.conf。如这一部分设置为使用其他端口，必须在连接工具时明指此端口。

- *<注册用户名>*——Dr.Web服务器管理员注册用户名。
- *<密码>*——管理员访问Dr.Web服务器的密码。

  如在连接行为给出管理员注册用户名和密码，工具会要求输入相应的账户。

可用指令：

- cache *<操作>*——使用文件缓存。 具体操作使用以下指令：
  - clear——清空文件缓存，
  - list——显示文件缓存的所有内容，
  - matched *<正则表达式>*——显示文件缓存中符合此正则表达式的内容，
  - maxfilesize [*<大小>*]——显示 / 指定预加载文件对象的最大大小。无补充参数是显示当前大小。需指定对象时在指令名称后输入需要的大小（字节）。
  - statistics——显示使用文件缓存的统计信息。
- calculate *<功能>* ——计算指定的顺序。具体顺序使用以下指令：
  - hash [*<标准>*] [*<行>*]——计算指定行哈希。使用以下参数指定具体标准：
    - gost——按照国标计算指定行的哈希，
    - md5——计算指定行的MD5哈希，
    - gost——按照SHA标准计算指定行的哈希，
    - sha1——按照SHA1标准计算指定行的哈希，
    - sha224——按照SHA224标准计算指定行的哈希，
    - sha256——按照SHA256标准计算指定行的哈希，
    - sha384——按照SHA384标准计算指定行的哈希，
    - sha512——按照SHA512.标准计算指定行的哈希，
  - hmac [*<标准>*] [*<行>*]——计算指定行HMAC。使用以下参数指定具体标准：
    - md5——计算指定行HMAC-MD5，
    - sha256——计算指定行HMAC-SHA256。
  - random——生成任意数，
  - uuid——生成任意识别码。
- clients *<操作>*——获取信息并管理连接到Dr.Web服务器的客户端。使用以下参数调出具体功能：
  - addresses [*<正则表达式>*]——显示符合此正则表达式的工作站的网络地址。如未给出正则表达式，则显示所有工作站的地址。
  - caddresses [*<正则表达式>*]——显示符合此正则表达式的工作站的IP地址数量。如未给出正则表达式，则显示所有工作站的数量。
  - chosts [*<正则表达式>*]——显示符合此正则表达式的工作站的计算机名称数量。如未给出正则表达式，则显示所有工作站的数量。
  - cids [*<正则表达式>*]——显示符合此正则表达式的工作站的识别码数量。如未给出正则表达式，则显示所有工作站的数量。
  - cnames [*<正则表达式>*]——显示符合此正则表达式的工作站的名称数量。如未给出正则表达式，则显示所有工作站的数量。

  - `disconnect [<正则表达式>]`——中断识别码符合此正则表达式的工作站的当前连接。如未给出正则表达式，则中断当前所有工作站连接。
  - `enable [<模式>]`——显示 / 指定客户端连接Dr.Web服务器的模式。无补充参数时显示当前模式。指定模式时需使用以下指令：
    - `on`——接受与客户端的所有连接。
    - `off`——拒绝与客户端的所有连接。
  - `hosts <正则表达式>`——显示符合此正则表达式的工作站的计算机名称。
  - `ids <正则表达式>`——显示符合此正则表达式的工作站的识别码。
  - `names <正则表达式>`——显示符合此正则表达式的工作站的名称。
  - `online <正则表达式>`——显示识别码、名称或地址符合此正则表达式的工作站的连接时长。连接时长从工作站最近一次连接Dr.Web服务器开始。
  - `statistics <正则表达式>`——显示符合此正则表达式的客户端数量统计信息。
  - `traffic <正则表达式>`——显示符合此正则表达式的当前在线的客户端资费数据。
- `core`——记录Dr.Web服务器进程转储。
- `cpu <参数>`——显示安装Dr.Web服务器的计算机的CPU使用统计信息。具体指标使用以下指令：
  - `clear`——删除积累的所有统计数据，
  - `day`——显示今日CPU负载图，
  - `disable`——停用CPU负载追踪，
  - `enable`——启用CPU负载追踪，
  - `hour`——显示当前一个小时内CPU负载图，
  - `load`——显示CPU平均负载，
  - `minute`——显示前一分钟CPU负载图，
  - `rawd`——显示一天内CPU负载数值统计信息，
  - `rawh`——显示最近一个小时内CPU负载数值统计信息，
  - `rawl`——显示CPU平均负载数值统计信息，
  - `rawm`——显示最近一分钟内CPU负载数值统计信息，
  - `status`——显示CPU负载统计信息追踪状态。
- `debug <参数>`——调试设置。使用补充指令给出具体参数。可利用指令`? debug`调出帮助，查看补充指令列表。

  指令`debug signal`只可用于UNIX家族操作系统的Dr.Web服务器。

- `die`——停止Dr.Web服务器并记录Dr.Web服务器进程转储。

  指令`die`只可用于UNIX家族操作系统的Dr.Web服务器。

- `dwcp <参数>`——指定/查看Dr.Web Control Protocol设置（包括Dr.Web服务器、代理端和代理端安装程序日志）。可用参数：

  - compression *<模式>*——指定以下一种流量压缩模式：
    - on——启用压缩，
    - off——停用压缩，
    - possible——可能压缩。
  - encryption *<模式>*——指定以下一种流量加密模式：
    - on——启用加密，
    - off——停用加密，
    - possible——可能加密。
  - show——显示Dr.Web Control Protocol当前设置。
- io *<参数>*——显示Dr.Web服务器进程数据只读 / 写入统计信息。具体参数使用以下指令：
  - clear——删除积累的所有统计数据，
  - disable——停用统计信息追踪，
  - disable——启用统计信息追踪，
  - rawdr——显示一天内数据只读数值统计信息，
  - rawdw——显示一天内数据写入数值统计信息，
  - rawh——显示最近一个小时内的数值统计信息，
  - rawm——显示最近一分钟内的数值统计信息，
  - rday——显示一天内数据只读图形统计信息，
  - rhour——显示最近一个小时内数据只读图形统计信息，
  - rminute——显示最近一分钟内数据只读图形统计信息，
  - status——显示统计信息追踪状态，
  - wday——显示一天内数据写入图形统计信息，
  - whour——显示最近一个小时内数据写入图形统计信息，
  - wminute——显示最近一分钟内记录数据的图形统计信息。
- log *<参数>*——将此行写入Dr.Web服务器日志文件或指定 / 查看日志详细等级。取决于具体参数分别执行以下操作：
  - log *<行>*——将此行写入Dr.Web服务器日志文件，详细等级为NOTICE。
  - log \s [*<等级>*]——指定/查看日志详细等级。不指定等级使用\s启动时为当前详细等级。日志详细等级可用值为： ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRIT。
- lua *<脚本>*——执行给出的LUA脚本。
- mallopt *<参数>*——内存分配设置。使用补充指令给出具体设置。可利用指令? mallopt调出帮助，查看补充指令列表。



指令mallopt只可用于Linux家族操作系统的Dr.Web服务器。

要获得此指令参数特点详细介绍，请阅读glibc库中的mallopt()功能描述。可通过指令man mallopt调出此功能的帮助文档。

- memory *<参数>*——显示安装Dr.Web服务器的计算机的内存使用统计信息。具体参数使用以下指令：
  - all——显示所有信息和统计数据，
  - heap——显示动态内存信息，
  - malloc——显示内存分配统计信息，
  - sizes——显示分配分内存大小统计信息，
  - system——显示系统内存信息。



指令memory只可用于OS Windows、Linux家族操作系统和FreeBSD家族操作系统的Dr.Web服务器。 对memory指令补充参数有以下限制：

- system——只可用于OS Windows和Linux家族操作系统的Dr.Web服务器，
- heap——只可用于OS Windows和Linux家族操作系统的Dr.Web服务器，
- malloc——只可用于Linux家族操作系统和FreeBSD家族操作系统的Dr.Web服务器，
- sizes——只可用于Linux家族操作系统和FreeBSD家族操作系统的Dr.Web服务器。

- monitoring *<模式>*——指定/查看CPU资源使用监控模式（cpu *<参数>*）和导入/导出（io *<参数>*）Dr.Web服务器进程。可用指令：
  - disable——停用监控，
  - enable——启用监控，
  - show——显示当前模式。
- printsta——将Dr.Web服务器运行统计信息写入日志。
- reload——重启Dr.Web Server FrontDoor插件。
- repository *<参数>*——管理库。使用以下参数调出具体功能：
  - all——显示库中所有产品和各产品所有文件数量，
  - clear——清空缓存，不取决于缓存中对象的TTL值，
  - fill——将库中所以文件放入缓存，
  - keep——总是保存当前处于缓存的库中所有文件，不取决于对象的TTL值，
  - loaded——显示当前处于缓存的库中所有产品和各产品所有文件数量，
  - reload——从磁盘重启库，
  - statistics——显示库更新的统计信息。
- restart——重启Dr.Web服务器。
- show *<参数>*——显示安装Dr.Web服务器的系统的相关信息。使用补充指令给出具体参数。可利用指令？ show调出帮助，查看补充指令列表。



对show指令补充参数有以下限制：

- memory——只可用于OS Windows和Linux家族操作系统的Dr.Web服务器，
- mapping——只可用于OS Windows和Linux家族操作系统服务器，
- limits——只可用于UNIX家族操作系统的Dr.Web服务器，

- processors——只可用于Linux家族操作系统的Dr.Web服务器。

- sql *<请求>*——执行此SQL请求。
- stop——停止Dr.Web服务器。
- traffic *<参数>*——显示Dr.Web服务器网络流量统计信息。具体参数使用以下指令：
  - all——显示自Dr.Web服务器开始运行起的总流量。
  - incremental——显示最近一次启动指令traffic incremental后新增流量。
  - last——显示从上次固定点后的流量变化。
  - store——为last创建固定点。
- update *<参数>*——获取信息并管理更新。使用以下参数调出具体功能：
  - active——显示当前进行更新的代理端列表。
  - agent [*<模式>*]——显示 / 指定代理端从Dr.Web服务器进行更新的模式。无补充参数时显示当前模式。指定模式时需使用以下指令：
    - on——启用代理端更新。
    - off——停用代理端更新。
  - gus——启动从GUS更新库，不取决于从GUS的更新进程状态。
  - http [*<模式>*]——显示/指定Dr.Web服务器从GUS更新库的模式。无补充参数时显示当前模式。指定模式时需使用以下指令：
    - on——启用从GUS更新库。
    - off——停用从GUS更新库。
  - inactive——显示当前不进行更新的代理端列表。
  - track [*<模式>*]——显示 / 指定代理端更新追踪模式。无补充参数时显示当前模式。指定模式时需使用以下指令：
    - on——启用代理端更新追踪。
    - off——停用代理端更新追踪。这时update active不会调出正在更新的代理端列表。
- version——导出工具版本信息。

H7.4. Dr.Web服务器脚本运行远程诊断工具

Dr.Web服务器远程诊断工具可远程连接Dr.Web服务器进行基本管理，并可查看运行统计信息。与drwcntl不同，工具drwcmd可用于运行脚本。

提供以下Dr.Web服务器脚本运行远程诊断工具控制台版本：

可执行文件	位置	描述
drweb-cmd-*<操作系统>*-*<位数>*	管理中心的管理→工具部分	为工具的独立版本。可从自定义目录启动，可用于相应操作系统的任一计算机。
	Dr.Web服务器目录 webmin/utilities	

可执行文件	位置	描述
drwcmd	Dr.Web服务器目录bin	此工具版本取决于是否具备服务器库。只能从所在目录启动。

工具版本drweb-cmd-*<操作系统>*-*<位数>*和drwcmd功能相同。以下介绍的是为drwcmd版本，但所有示例同样适用于另一版本。

连接Dr.Web服务器远程诊断工具必须启用插件Dr.Web Server FrontDoor。启用操作是在**Dr.Web服务器配置**的**模块**标签勾选插件**Dr.Web Server FrontDoor**。

连接Dr.Web服务器远程诊断工具要求管理员具备**使用高级功能**权限。否则会禁止管理员通过远程诊断工具访问Dr.Web服务器。

如何设置Dr.Web服务器来连接Dr.Web服务器远程诊断工具参见**管理员手册**的远程访问Dr.Web服务器。

启动命令格式：

drwcmd [*<参数>*] [*<文件>*]

可用参数

工具drwcmd参数使用原则遵循附录H. Dr.Web Enterprise Security Suite所含软件命令行参数部分介绍的总体原则。

- --?——显示参数说明文档。
- --help——显示参数说明文档。
- --commands=*<指令>*——执行指定的命令（与执行drwcntl工具指令类似）。可指定多个指令，用;隔开。
- --debug=yes|no——以调试模式记录工具运行日志（输出标准线程stderr）。默认为no。
- --files=yes|no——允许从指定文件执行指令（与执行drwcntl工具指令类似）。默认为yes。

  在文件给出指令应为每行一个指令。空行忽略。注释开始可使用符合#。
- --keep=yes|no——支持在执行最后一个指令后并在工具结束运行前连接Dr.Web服务器。默认为no。
- --output=*<文件>*——用于输出Dr.Web服务器回应的文件。默认如未指定文件，使用标准输出线程stdout。

  如果文件名称以符合(+)开始，则指令执行结果会添加到文件结尾，否则文件将覆盖写入。
- --password=*<密码>*——在Dr.Web服务器进行身份验证的密码。可在文件中参数--resource中给出。

- `--read=yes|no`——允许从资源文件读取Dr.Web服务器连接参数。默认为`yes`。
- `--resource=`*<文件>*——资源文件，包含Dr.Web服务器连接参数：Dr.Web服务器地址和管理员在Dr.Web服务器进行身份验证的注册信息。默认使用文件`.drwcmdrc`，所在目录为：
  - UNIX家族操作系统：`$HOME`
  - OS Windows：`%LOCALAPPDATA%`

  文件中每一行为空格隔开的3个词段：*<Dr.Web服务器> <用户> <密码>*。

  某词段中间的空格利用`%S`给出。百分符号则利用`%P`。

  例如：

```
ssl://127.0.0.1 user1 password1

ssl://127.0.0.1 user2 password2

ssl://127.0.0.1 user pass%Sword
```



使用参数`--resource`是必须指定参数 `--server`。将连接参数 `--server`中指定的Dr.Web服务器，使用的是与此Dr.Web服务器地址对应的资源文件中的注册数据。

- `--server=`*<Dr.Web服务器>*——Dr.Web服务器地址。默认为`ssl://127.0.0.1`。可由参数`--resource`中指定的文件确定。
- `--user=`*<用户>*——在Dr.Web服务器进行身份验证的用户名。可在文件中参数`--resource`中给出。
- `--verbose=yes|no`——输出Dr.Web服务器详细回应（输出标准线程`stdout`）。默认为`no`。
- `--version`——导出工具版本信息。

连接Dr.Web服务器的流程：

1. 启动Dr.Web服务器连接参数时优先的是参数值`--server`、`--user`和`--password`。
2. 如参数`--server`未给出，则使用默认地址——`ssl://127.0.0.1`。
3. 如参数`--user`未给出，则在文件`.drwcmdrc`（可在`--resource`另行指定）搜索所需Dr.Web服务器和字母排序最先的用户名。
4. 如参数`--password`未给出，则在文件`.drwcmdrc`（可在`--resource`另行指定）按照Dr.Web服务器和用户名进行搜索。



将从文件`.drwcmdrc`（可在`--resource`另行指定）读取用户名和密码，如参数`--read`不禁止读取。

5. 如没有通过参数或资源文件给出用户名和密码，工具则要求通过控制台输入登录账户。

执行指令的特点：

- 如指令文件为空值（`-`），则读取从控制台输入的指令。
- 如同时给出`--commands`指令和文件列表，则先执行在`--commands`给出的指令。

- 如没有给出--commands指令和文件列表，则读取从控制台输入的指令。

例如：

如要先执行--command中的指令，然后执行控制台指令，需输入：

```
drwcmd --commands=<指令> -- -
```

运行结束码

- 0——已成功执行。
- 1——已调用参数帮助文档：--help 或--?。
- 2——命令行解析出错：未给出身份认证参数等原因。
- 3——创建Dr.Web服务器回应输出文件时出错。
- 4——在Dr.Web服务器进行身份验证时出错：管理员用户名和/或密码不正确。
- 5——与Dr.Web服务器的连接错误中断。
- 127——未能确定的致命错误。

H7.5. Dr.Web库加载器



库加载器图形版本工具的介绍见管理员手册中的工具的图形版本。

提供以下Dr.Web库加载器工具控制台版本：

可执行文件	位置	描述
drweb-reploader-<*操作系统*>-<*位数*>	管理中心的管理→工具部分	为工具的独立版本。可从自定义目录启动，可用于相应操作系统的任一计算机。
	Dr.Web服务器目录webmin/utilities	
drwreploader	Dr.Web服务器目录bin	此工具版本取决于是否具备服务器库。只能从所在目录启动。



工具版本drweb-reploader-<*操作系统*>-<*位数*>和drwreploader功能相同。以下介绍的是为drwreploader版本，但所有示例同样适用于另一版本。

启动控制台工具需指定参数，可使用库加载器配置文件来简化这一过程。在软件中提供配置文件，所有参数均为下面介绍的默认值，只有--ssh-auth除外：配置文件中参数值为pubkey。

可用参数

- --archive——将库压缩存档。默认为no。

- `--auth` *<参数>*——在更新服务器进行身份验证所使用的注册信息，格式为*<用户>*`[:`*<密码>*`]`。
- `--cert-file` *<路径>*——SSL身份认证根证书库路径。
- `--cert-mode` `[`*<参数>*`]`在——可自动接受的SSL证书类型。此设置只用于支持加密的安全协议。

  *<参数值>*可为：

  - `any`——接受所有证书，
  - `valid`——只接受有效的SSL证书，
  - `drweb`——只接受Dr.Web证书，
  - `custom`——接受自定义证书。

  默认值为`drweb`。
- `--config` *<路径>*—— 库加载器配置文件路径。
- `--cwd` *<路径>*——当前工作目录的路径。
- `--ipc`——将工具运行过程相关数据的传输纳入标准输出线程。默认为`no`。
- `--help`——显示参数说明文档。
- `--license-key` *<路径>*——授权密钥文件路径（应指示密钥或其MD5）。
- `--log` *<路径>*——库加载流程日志文件路径。
- `--mode` *<模式>*——加载更新的模式：
  - `repo`——以Dr.Web服务器库格式加载库。加载的文件可直接利用管理中心导入，用于更新Dr.Web服务器库。默认为使用。
  - `mirror`——以GUS更新区格式加载库。加载的文件可置于本地网络的更新镜像。之后可将Dr.Web服务器设置为直接从此更新镜像获取最新版本的库，而不是从GUS服务器获取。
- `--only-bases`——只加载病毒库。默认为：`no`。
- `--path` *<参数值>*——从GUS将库加载到*<参数值>*所指定的目录。使用`--archive`压缩库时可以指定到目录名称的路径，也可指定到压缩文件文件名的路径。如不指定压缩文件文件名，则使用默认文件名`repository.zip`。
- `--product` *<参数值>*——需更新的产品。默认加载整个库。
- `--prohibit-cdn`——加载更新时禁止使用CDN。默认为`no`，即允许使用CDN。
- `--proto` *<协议>*——加载更新使用的协议：`http | https | ftp | ftps | sftp | scp | filefile | ftp | ftps | http | https | scp | sftp | smb | smbs`。默认为`https`。
- `--proxy-auth` *<参数值>*——代理服务器身份验证信息：注册用户名和密码，格式为*<用户名>*`[:`*<密码>*`]`。
- `--proxy-host` *<参数值>*——代理服务器地址，格式为*<服务器>*`[:`*<端口>*`]`。默认为：`3128`。
- `--rotate` *<N><f>,<M><u>*——库加载器运行日志轮循模式。设置同Dr.Web服务器日志轮循。

  默认值为`10，10m`，即保存10个大小为10MB的文件，使用压缩。
- `--servers` *<参数值>*——GUS服务器地址。建议使用默认值：`esuite.geo.drweb.com`。
- `--show-products`——显示GUS的产品列表。默认为：`no`。

- --ssh-auth *<类型>*——按照SCP/SFTP连接时在更新服务器进行身份验证的类型。*<类型>*可以是以下一个参数值：
  - pwd——使用密码登录。密码在--auth指定。
  - pubkey——按照公钥登录。这时必须在--ssh-prikey给出私钥，以便提取相应的公钥。
- --ssh-prikey *<路径>*——SSH私钥路径。
- --ssh-pubkey *<路径>*——SSH公钥路径。
- --strict——出现错误时停止加载。默认为no。
- --update-key *<路径>*——用于检查从GUS加载的更新签名的公钥路径或公钥目录路径。用于检查更新真实性的公钥update-key-*.upub在Dr.Web服务器的etc目录。
- --update-url *<参数值>*——GUS服务器包含Dr.Web产品更新的目录。建议使用默认值：/update。
- --v——导出工具版本信息。
- --verbosity*<详细等级>*——日志详细等级。默认值为TRACE3。允许值为：ALL、DEBUG3、DEBUG2、DEBUG1、DEBUG、TRACE3、TRACE2、TRACE1、TRACE、INFO、NOTICE、WARNING、ERROR、CRIT。参数值ALL和DEBUG3意义相同。
- --version *<版本>*——需加载更新的Dr.Web服务器版本，格式为*<主版本号>*.*<主版本号>*。例如，服务器端版本13的*<主版本号>*参数为13.00。不同Dr.Web服务器版本可更新的产品列表会有所不同。可在相应版本帮助手册库加载器配置文件参数<products>中查看可更新产品列表。

参数使用特点

启动库加载器工具时请注意以下规则：

必须指定参数。	前提是
--license-key	总是
--update-key	
--path	
--cert-file	如以下参数的参数值为： • --cert-mode valid | drweb | custom， • --proto https | ftps | smbs。
--ssh-prikey	如以下参数的参数值为： • --proto sftp | scp， • --ssh-auth pubkey。

使用举例

1. 创建可导入的所有产品压缩文件：

```
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. 创建可导入的病毒库压缩文件：

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

3. 创建可导入的只包含Dr.Web服务器的压缩文件：

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

H7.6. 用于UNIX操作系统的Dr.Web代理端的远程安装工具

用于UNIX操作系统的Dr.Web代理端的远程安装工具能够将Dr. Web代理端远程安装到反病毒网络中的UNIX家族操作系统工作站。如需还可利用此工具安装Dr.Web for UNIX file servers。

此工具以命令行模式运行，可用版本有：

可执行文件	位置	描述
drweb-unix-install-*<操作系统>*-*<位数>*	管理中心的管理→工具部分	为工具的独立版本。可从自定义目录启动，可用于相应操作系统的任一计算机。随库或Dr.Web服务器更新。
	Dr.Web服务器目录webmin/utilities	
drwunixinstall	Dr.Web服务器目录bin	此工具版本取决于是否具备服务器库。只能从所在目录启动。只随Dr.Web服务器更新。

工具版本drweb-unix-install-*<操作系统>*-*<位数>*与drwunixinstall功能相同。以下介绍的是drwunixinstall版本，但所有参数和格式同样适用于另一版本。

启动命令格式：

```
drwunixinstall [<参数>] <工作站1的IP地址>[:<端口SSH>[^<用户名>[^<密码>]]] <工作站2的IP地址>[:<端口SSH>[^<用户名>[^<密码>]]] ...
```

可用参数

工具drwunixinstall参数使用原则遵循附录H. Dr.Web Enterprise Security Suite所含软件命令行参数部分介绍的总体原则。

- --help——显示参数说明文档。
- --ak <*身份验证参数*>——指定在远程工作站进行身份验证的备用参数，使用加密密钥，格式为：

  ```
  <用户名>^<Dr.Web服务器私钥路径>^<Dr.Web服务器公钥路径>[^<私钥密码>]
  ```

  如生成指令时同时指定常规身份验证参数<*用户名*>^<*密码*>和使用加密密钥的备用参数，则启动工具是首先使用有加密密钥的参数。

- --ap <*用户名*>^<*密码*>——在远程工作站进行身份验证使用多次输入密码模式（keyboard-interactive）。

- --certificate <*路径*>——指定Dr.Web服务器证书文件路径。默认为webmin/install/unix/workstation/drwcsd-certificate.pem。
- --cpus <*数量*>——指定进行远程安装使用的处理器内核数量。默认为4。
- --ctimeout <*时长*> ——指定在远程工作站等待安装包传输结束的最长时限。以秒计，默认为600。
- --debug——以调试模式记录工具运行日志。默认为no。
- --esuite <*服务器地址*> ——输入Dr.Web服务器地址，从这一服务器进行远程安装，安装结束后代理端将连接此服务器。格式为：[udp://]<*IP地址或DNS名称*>[:<*端口*>]
- --ctimeout <*时长*> ——指定在远程工作站等待安装包安装结束的最长时限。以秒计，默认为900。
- --from <*路径*>——指定Dr.Web服务器上安装包目录路径。默认为webmin/install/unix。
- --long——记录工具运行日志时指示时间标志。默认为no。
- --pwd <*密码*> ——使用su和/或sudo指令在远程工作站进行身份验证的密码。
- --remote-temp <*路径*> ——指定远程工作站上的用于保存Dr.Web服务器软件和证书的临时文件夹的路径。默认使用系统给出的文件夹。
- --server——安装Dr.Web for UNIX file servers替代Dr.Web代理端。默认为no。
- --simultaneously <*数量*>——指定能同时安装Dr.Web代理端的工作站最多数量。
- --sshdebug——以调试模式记录工具运行日志，对使用SSH协议的所有操作进行细节记录。默认为no。
- --sshwaitdebug——以调试模式记录工具运行日志，对使用SSH协议的所有操作以及有超时时限的操作进行细节记录。默认为no。
- --stimeout <*时长*> ——使用su和/或sudo指令在远程工作站进行身份验证时等待密码输入的最长时限。以秒计，默认为10。
- --su——安装时使用指令su将权限升为超级用户权限。默认为no。
- --sudo——安装时使用指令sudo将权限升为超级用户权限。默认为no。
- --temp <*路径*> ——指定Dr.Web服务器上用于保存证书的文件夹的路径。默认使用系统给出的文件夹。
- --timeout <*时长*> ——指定在远程工作站等待建立连接和完成验证结束的最长时限。以秒计，默认为30。
- --verbosity<*等级*>——指定工具运行日志详细等级。默认值为info。允许值为：all、debug3、debug2、debug1、debug、 trace3、trace2、trace1、trace、info、notice、warning、error、crit。参数值all和debug3意义相同。
- --version——导出工具版本信息。

H7.7. 用于Windows操作系统的Dr.Web代理端的远程安装工具

用于Windows操作系统的Dr.Web代理端的远程安装工具能够将Dr. Web代理端远程安装到反病毒网络中的Windows族操作系统工作站。

此工具以命令行模式运行，可用版本有：

可执行文件	位置	描述
drweb-windows-install-*<操作系统>*-*<位数>*	管理中心的管理→工具部分	为工具的独立版本。可从自定义目录启动，可用于相应操作系统的任一计算机。随库或Dr.Web服务器更新。
	Dr.Web服务器目录webmin/utilities	
drwwindowsinstall	Dr.Web服务器目录bin	此工具版本取决于是否具备服务器库。只能从所在目录启动。只随Dr.Web服务器更新。

工具版本drweb-windows-install-*<操作系统>*-*<位数>*与drwwindowsinstall功能相同。以下介绍的是drwwindowsinstall版本，但所有参数和格式同样适用于另一版本。

启动命令格式：

drwwindowsinstall *<参数>*

可用参数

工具drwwindowsinstall参数使用原则遵循附录H. Dr.Web Enterprise Security Suite所含软件命令行参数部分介绍的总体原则。

- --help——显示参数说明文档。
- --console=yes|no——以调试模式导出工具运行日志。默认为no。
- --disable-v1=yes|no——工具运行时停用SMB协议版本1（SMBv1）。默认为no。
- --distribution *<文件名称>*——手动给出将在远程工作站启动的代理端安装包文件名称。默认为drwinst.exe。
- --install-address *<工作站IP地址>*——输入将安装代理端的远程工作站地址。同时给出多个工作站时地址用逗号（","）或分号（";"）隔开，中间没有空格。
- --install-certificate *<路径>*——指定Dr.Web服务器证书文件路径。
- --install-clients *<数量>*——指定能同时安装Dr.Web代理端的工作站最多数量。默认为8。
- --install-compression *<模式>*——设置Dr.Web服务器与远程工作站连接时的压缩模式：on——启用压缩，off——停用压缩，possible——可能压缩。最后一个参数表示模式取决于Dr.Web服务器端的设置。默认为possible。
- --install-encryption *<模式>*——设置Dr.Web服务器与远程工作站连接时的加密模式：on——启用加密，off——停用加密，possible——可能加密。最后一个参数表示模式取决于Dr.Web服务器端的设置。默认为possible。
- --install-language *<语言代码>*——指定代理端界面语言，使用ISO 639-1标准的双字母代码。如不指定或代理端不支持指定的语言，使用远程远程工作站的系统语言。

- --install-path *<路径>* ——指定远程工作站上的代理端安装文件夹路径。默认为%ProgramFiles%\DrWeb。
- --install-register=yes|no——安装结束后在已安装程序列表中注册代理端。默认为no。
- --install-server *<服务器地址>* ——输入Dr.Web服务器地址，从这一服务器进行远程安装，安装结束后代理端将连接此服务器。格式为：[udp://]*<IP地址或DNS名称>*[:*<端口>*]
- --install-timeout *<时长>* ——指定在远程工作站等待代理端安装结束的最长时限。以秒计，默认为300。
- --install-user *<用户名>*@*<域名>*:*<密码>* 或 *<域名>**<用户名>*:*<密码>* ——指定登录远程工作站的用户名和密码。
- --log *<路径>* ——指定工具运行日志文件路径。默认为Dr.Web服务器安装目录子目录var中的drwsmb.log。
- --machine *<名称>* ——指定完成代理端安装并连接Dr.Web服务器后远程工作站在Dr.WebEnterprise Security Suite反病毒网络中的名称。默认使用已在操作系统注册的计算机名称。
- --rotate=*<N><f>*,*<M><u>* ——指定工具运行日志轮循模式。格式与用于Dr.Web服务器日志轮循模式的类似参数一样。默认为10,10m。
- --service-id *<注册表中的名称>* ——指定Windows注册表中代理端远程安装服务的名称。默认为DrWebRsvcRunner。
- --service-name *<可显示名称>* ——指定Services表中代理端远程安装服务的名称。默认为Dr.Web Remote Runner Service。
- --target-root *<目录名称>* ——指定在远程工作站管理员分享资源中的目录名称，从Dr.Web服务器复制的代理端安装包将从此目录启动。默认为TEMP。
- --target-volume *<资源名称>* ——指定安置代理端安装文件的管理员分享资源名称。默认为ADMIN$。
- --threads *<数量>* ——指定池中出入线程数量。默认为 2。
- --verbosity*<等级>*——指定工具运行日志详细等级。默认值为trace。允许值为：all、debug3、debug2、debug1、debug、 trace3、trace2、trace1、trace、info、notice、warning、error、crit。参数值all和debug3意义相同。
- --version——导出工具版本信息。

附录I. Dr.Web服务器导出的环境变量

为简化由Dr.Web服务器按日程运行的进程的设置，需要有Dr.Web服务器目录位置信息，为此Dr.Web服务器向启动进程环境导出以下变量：

- DRWCSD_HOME——根目录路径（安装目录）。参数值为-home，如启动Dr.Web服务器时设置了这一参数，反之是启动时的当前目录。
- DRWCSD_BIN——执行文件目录路径。参数值为-bin-root，如启动Dr.Web服务器时设置了这一参数，反之是根目录的bin子目录。
- DRWCSD_VAR——Dr.Web服务器有权写入的目录路径，此目录用于保存可变化文件（如日志以及库文件）。参数值为-var-root，如启动Dr.Web服务器时设置了这一参数，反之是根目录的var子目录。

附录J. Dr.Web Enterprise Security Suite 中正则表达式的使用

Dr.Web Enterprise Security Suite的某些参数使用以下类型的正则表达式：

- Lua语言正则表达式。

  设置反病毒网络工作站的用户组自动组籍时使用。

  Lua语言正则表达式语法详细介绍见http://www.lua.org/manual/5.1/manual.html#5.4.1。
- PCRE软件库正则表达式。

  PCRE库语法详细描述见http://www.pcre.org/。

  本附录仅为PCRE库正则表达式使用基本条件简要说明。

J1. PCRE正则表达式选项

在Dr.Web服务器配置文件或管理中心使用正则表达式指定Dr.Web扫描仪设置中不需要扫描的对象。

正则表达式格式：

```
qr{EXP}options
```

其中EXP——表达式本身，options——选项顺序（字母串），qr{}——元符号。整体示例：

```
qr{pagefile\.sys}i
```

——OS Windows NT交换文件

正则表达式和其选项描述见下。更详细的信息参http://www.pcre.org/pcre.txt。

- 选项'a'，对应PCRE_ANCHORED

  选择此设置后，模板强制“抛锚”，即限制为仅匹配搜索符号串中第一个搜索项（“主题行”）。也可以通过模板中相应结构来进行此设置。
- 选项 'i'，对应PCRE_CASELESS

  选择此设置后，模板匹配大写和小写字母。此功能可通过设置选项(?i)进行修改。
- 选项 'x'，对应 PCRE_EXTENDED

  选择此设置后，模板中忽略符号间空格，但空格在控制符号前或位于符号类内部时不忽略。空格不包括符号VT（代码11）。此外，也忽略符号类以外的符号间符号和不在控制符号或换行符号前的符号#。可在模板通过设置(?x)修改此选项。此设置可在复杂模板内部添加说明。应注意，其仅用于数据符号。空格符号不能位于模板中特殊符号串内部，如不能在导入子模板的符号串(?(内。
- 选项 'm'，对应PCRE_MULTILINE

  默认PCRE认为主题行由一行符号组成（即便是实际上主题行包含换行符号）。元符号"*行开始*”“^”仅在行开始匹配，而元符号"*行结束*”“$”仅在行结束或最后一个换行符前匹配（如未勾选选项PCRE_DOLLAR_ENDONLY）。

  如勾选选项PCRE_MULTILINE，元符号"*行开始*”和"*行结束*”关联至主题行其前或其后的第一个换行符，以及行的开始和结束。可在模板通过设置(?m)修改此选项。如文本中无符号“\n”或模板中无^或$，选项PCRE_MULTILINE无效。
- 选项'u'，对应PCRE_UNGREEDY

此选项取消量词的"匹配优先"，默认为"非匹配优先"，如其后为"?"，则还原"匹配优先"。还可以通过设置模板的(?U)来进行修改。

- 选项'd'，对应PCRE_DOTALL

  选择此设置后，模板点符号与包括新行符号的所有符号相匹配。无此元符号，则排除新行符号。可通过在模板添加新选项(?s)来更改此设置。负级，如，[^a]，无论是否有此设置，始终和新行符号匹配。

- 选项'e'，对应 PCRE_DOLLAR_ENDONLY

  选择此设置后，模板美元符号仅与主题行结尾匹配。如无此设置，美元直接在行末换行符前的位置（但不是任何其它新行符号之前）。选项PCRE_DOLLAR_ENDONLY忽略，如设定了PCRE_MULTILINE。

J2. PCRE正则表达式特点

正则表达式——是从左到右与文本进行对比的模板。模板中大多数符号标志其本身并对应在文本中使用符号。

正则表达式的主要优点是可在模板中启用不同方案和进行重复。正则表达式使用不代表自身的元符号编码，这些元符号以特殊方式解读。

有两组不同的元符号：在方括号中使用的元符号和在方括号外使用的元符号。下面分别加以详细介绍。在方括号以外使用下列元符号：

符号	说明
\	普通控制符号（escape），有几种方案
^	为该行（或多行文本）的开始
$	为该行（或多行文本）的结束
.	匹配除了换行符以外的任意符号（默认）
[	符号类描述开始
]	符号类描述结束
|	备选分支开始
(	子模板开始
)	子模板结束
?	扩展（的意义 以及量词0或1 以及最小化量词
*	0及更高
+	1及更高

符号	说明
	以及“格量词”
{	最小/最大量词开始

模板方括号内部分称为“符号类"。符号类中的元符号是：

符号	说明
\	普通控制符号（escape）
^	否定类，但仅在类开始时
-	确定符号范围
[	POSIX符号类（如其后为POSIX语法）
]	关闭符号类

附录K. 日志文件格式

Dr.Web服务器日志文件（参见**管理员手册**中的Dr.Web服务器运行日志）为文本格式，文件中每一行代表一个通知。

通知行格式如下：

<年><月><日>.<点><分><秒>.<百分之一秒> <通知类型> [*<进程id>*] *<线程名称>* [*<通知来源>*] *<通知>*

其中：

- *<年><月><日>.<点><分><秒>.<百分之一秒>*——日志文件记录此通知的准确时间。
- *<通知类型>*——日志记录等级：
  - **ftl**（fatal error——致命错误）——运行重大错误通知；
  - **err**（error——错误）——运行错误通知；
  - **wrn**（warning——预警）——错误预警；
  - **ntc**（notice——备注）——重要信息通知；
  - **inf**（info——信息）——信息通知；
  - **tr0..3**（trace0..3——跟踪）——以不同详细等级跟踪操作（**跟踪3**为最高详细等级）；
  - **db0..3**（debug0..3 ——调试）——不同详细等级的调试通知（**调试3**为最高详细等级）。

  以**tr0..3**（跟踪）和**db0..3**（调试）记录日志仅供Dr.Web Enterprise Security Suite软件研发人员使用。

- [*<进程id>*]——进程独有识别码，在此进程期间执行了将通知写入日志文件的线程。在某些操作系统下[*<进程id>*]格式可能为[*<进程id> <线程id>*]。
- *<线程名称>*——将通知写入日志文件的线程的符号标志。
- [*<通知来源>*]——将通知写入日志文件的系统名称。并非总是有通知来源。
- *<通知>*——依照日志等级对操作的文字描述。可包括格式化的描述，也可包含某些情况下的重要变量。

例如：

```
1.20081023.171700.74 inf [001316] mth:12 [Sch] Job "Purge unsent IS
  events" said OK
```

其中：

- 20081023——*<年><月><日>*，
- 171700——*<点><分><秒>*，
- 74——*<百分之一秒>*，
- inf——*<通知类型>*——信息性通知，
- [001316]——[*<进程id>*]，
- mth:12——*<线程名称>*，
- [Sch]——[*<通知来源>*]——任务调度器，

- Job "Purge unsent IS events" said OK——*<通知>*成功完成任务清空未发送事件。

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

   其中：

   - 20081028——*<年><月><日>*，
   - 135755——*<点><分><秒>*，
   - 61——*<百分之一秒>*，
   - inf——*<通知类型>*——信息性通知，
   - [001556]——[*<进程id>*]，
   - srv:0——*<线程名称>*，
   - tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193——*<通知>* 已通过指定套接字建立新的连接。

附录L. Web API 和Dr.Web Enterprise Security Suite的整合

Web API介绍 见**Web API for Dr.Web Enterprise Security Suite**手册 。

应用

整合**Web API**与Dr.Web Enterprise Security Suite后可以集成账户操作功能，使用户服务管理过程自动化。可用于建立获取用户申请并向用户分发安装文件的动态网页。

身份验证

与Dr.Web服务器的交互作用使用HTTP(S)协议。**Web API**接收REST请求并返回XML。访问Web API使用Basic HTTP身份验证（按照RFC 2617标准）。不符合RFC 2617标准时，HTTP(S)服务器不会询问客户账户（Dr.Web Enterprise Security Suite管理员注册用户名和密码）。

附录M. 授权

本章节包含Dr.Web Enterprise Security Suite软件使用的第三方软件库列表、授权信息和项目开发地址。

第三方库	授权	项目URL
asio	https://www.boost.org/LICENSE_1_0.txt*	https://think-async.com/Asio/
boost	https://www.boost.org/LICENSE_1_0.txt*	https://www.boost.org/
brotli	MIT License**	https://github.com/google/brotli
bsdiff	Custom	http://www.daemonology.net/bsdiff/
c-ares	https://c-ares.org/license.html*	https://c-ares.org/
cairo	Mozilla Public License** GNU Lesser General Public License**	https://www.cairographics.org/
CodeMirror	MIT License**	https://codemirror.net/
curl	https://curl.se/docs/copyright.html*	https://curl.se/libcurl/
ICU	https://www.unicode.org/copyright.html#License*	https://icu.unicode.org/home
fontconfig	Custom	https://www.freedesktop.org/wiki/Software/fontconfig/
freetype	GNU General Public License** FreeType Project License (BSD like)	https://www.freetype.org/
GCC runtime libraries	GNU General Public License** with exception*	https://gcc.gnu.org/
HTMLayout	Custom	https://terrainformatica.com/a-homepage-section/htmlayout/
jemalloc	*https://github.com/jemalloc/jemalloc/blob/dev/COPYING**	https://github.com/jemalloc/jemalloc
jQuery	MIT License** GNU General Public License**	https://jquery.com/
JSON4Lua	MIT License**	https://github.com/craigmj/json4lua
Leaflet	BSD License https://github.com/Leaflet/Leaflet/blob/master/LICENSE*	https://leafletjs.com

第三方库	授权	项目 URL
libpng	http://libpng.org/pub/png/src/libpng-LICENSE.txt*	http://libpng.org/pub/png/libpng.html
libradius	Juniper Networks, Inc.*	https://www.freebsd.org
libssh2	3-Clause BSD License https://github.com/libssh2/libssh2/blob/master/COPYING*	https://www.libssh2.org/
libxml2	MIT License**	http://www.xmlsoft.org/
Linenoise NG	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://scripts.sil.org/cms/scripts/render_download.php?format=file&media_id=OFL_plaintext&filename=OFL.txt*	https://fonts.google.com/noto/use
OpenLDAP	https://www.openldap.org/software/release/license.html*	https://www.openldap.org
OpenSSL	https://www.openssl.org/source/license.html*	https://www.openssl.org/
Oracle Instant Client	https://www.oracle.com/downloads/licenses/instant-client-lic.html*	https://www.oracle.com/index.html
ParaType Free Font	https://www.paratype.ru/public/pt_openlicense_eng.asp*	https://www.paratype.ru
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/
pixman	MIT License**	http://pixman.org/
Prototype JavaScript	MIT License**	http://prototypejs.org/assets/2009/8/31/prototype.js

第三方库	授权	项目URL
framework		
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 https://www.sqlite.org/copyright.html	https://www.sqlite.org/index.html
wtl	Common Public License** Microsoft Public License**	https://sourceforge.net/projects/wtl/
zlib	https://www.zlib.net/zlib_license.html*	https://www.zlib.net/

*——授权文字内容见下。

**——基础授权文本链接：

授权	地址
Common Public License	https://opensource.org/licenses/cpl1.0.php
GNU General Public License	https://www.gnu.org/licenses/gpl-3.0.html
GNU Lesser General Public License	https://www.gnu.org/licenses/lgpl-3.0.html
Microsoft Public License	https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649456(v=pandp.10)
MIT License	https://opensource.org/licenses/mit-license.php
Mozilla Public License	https://www.mozilla.org/en-US/MPL/2.0/
3-Clause BSD License	https://opensource.org/licenses/BSD-3-Clause

M1. 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.
```

M2. 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.
```

M3. 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.
```

M4. 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.
```

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. 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.

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

M7. 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.
```

M8. 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
```

M9. 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 $
```

M10. Libssh2

```
Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>

Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>

Copyright (c) 2006-2007 The Written Word, Inc.

Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
```

```
Copyright (c) 2009-2014 Daniel Stenberg

Copyright (C) 2008, 2009 Simon Josefsson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

Neither the name of the copyright holder nor the names of any other contributors may
be used to endorse or promote products derived from this software without specific
prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
```

M11. Linenoise NG

linenoise

```
Copyright (c) 2010, Salvatore Sanfilippo <antirez at gmail dot com>

Copyright (c) 2010, Pieter Noordhuis <pcnoordhuis at gmail dot com>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

  * Redistributions of source code must retain the above copyright notice, this list
of conditions and the following disclaimer.

  * Redistributions in binary form must reproduce the above copyright notice, this
list of conditions and the following disclaimer in the documentation and/or other
materials provided with the distribution.

  * Neither the name of Redis nor the names of its contributors may be used to endorse
or promote products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
```

```
SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
```

wcwidth

```
Markus Kuhn -- 2007-05-26 (Unicode 5.0)

Permission to use, copy, modify, and distribute this software for any purpose and
without fee is hereby granted. The author disclaims all warranties with regard to this
software.
```

ConvertUTF

```
Copyright 2001-2004 Unicode, Inc.

 Disclaimer

 This source code is provided as is by Unicode, Inc. No claims are made as to fitness
for any particular purpose. No warranties of any kind are expressed or implied. The
recipient agrees to determine applicability of information provided. If this file has
been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for
any claim will be exchange of defective media within 90 days of receipt.

 Limitations on Rights to Redistribute This Code

 Unicode, Inc. hereby grants the right to freely use the information supplied in this
file in the creation of products supporting the Unicode Standard, and to make copies
of this file in any form for internal or external distribution as long as this notice
remains attached.
```

M12. Net-snmp

```
Various copyrights apply to this package, listed in various separate parts below.
Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

 Copyright 1989, 1991, 1992 by Carnegie Mellon University

      Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

      All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for
any purpose and without fee is hereby granted, provided that the above copyright
notice appears in all copies and that both that copyright notice and this permission
notice appear in supporting documentation, and that the name of CMU and The Regents of
```

the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

```
* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to
endorse or promote products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications,
nor the names of their contributors may be used to endorse or promote products derived
from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:
```

```
* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or
product names may not be used to endorse or promote products derived from this
software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be
used to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.
```

```
* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used
to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
```

M13. 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.

M14. 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.
```

M15. 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.]
```

M16. 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

M17. 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
```

M18. 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.
```

M19. 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.
```

M20. 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
```

第三章、常见问题

将Dr.Web服务器迁至另一台计算机（OS Windows）

将Dr.Web服务器迁至另一台计算机时需注意传输协议的设置，如需请在管理→**Dr.Web**服务器配置的传输标签作必要的修改。

启动和停止Dr.Web服务器的操作（参见管理员手册中的启动和停止Dr.Web服务器）。

Windows操作系统下转移 Dr.Web服务器（安装类似版本的Dr.Web服务器）

1. 停止运行中的Dr.Web服务器。
2. 在命令行使用参数modexecdb database-export启动drwcsd.exe，将数据库内容导出到文件。OS Windows操作系统下完整的导出命令行可为：

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log modexecdb database-export <文件完整名称>
```

3. 保存C:\Program Files\DrWeb Server\etc目录内容。
4. 卸载Dr.Web服务器
5. 在选定的计算机安装新Dr.Web服务器（带新数据库的空服务器）。利用OS Windows服务控制工具或通过管理中心停止 Dr.Web服务器。
6. 将先前保存的etc目录内容拷贝到C:\Program Files\DrWeb Server\etc。
7. 在命令行使用参数modexecdb database-import启动drwcsd.exe，将数据库内容从文件导入。OS Windows操作系统下完整的导入命令行可为：

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log modexecdb database-import <文件完整名称>
```

8. 启动Dr.Web服务器服务。

使用内设数据库时可以不进行数据库的导出和导入，只需保存内设数据库dbinternal.dbs文件，在新安装的Dr.Web服务器上用原Dr.Web服务器数据库文件替代新数据库文件。

Windows操作系统下转移 Dr.Web服务器（安装另一版本的Dr.Web服务器）

1. 停止运行中的Dr.Web服务器。
2. 使用SQL服务器工具保存数据库（如使用的是内设数据库，只需保存database.sqlite文件）。
3. 保存C:\Program Files\DrWeb Server\etc目录内容。
4. 卸载Dr.Web服务器

5. 在选定的计算机安装新Dr.Web服务器（带新数据库的空服务器）。利用OS Windows服务控制工具或通过管理中心停止 Dr.Web服务器。
6. 将先前保存的etc目录内容拷贝到C:\Program Files\DrWeb Server\etc。
7. 在新Dr.Web服务器配置文件drwcsd.conf中指定数据库路径，恢复数据库。
8. 使用参数modexecdb database-upgrade启动drwcsd.exe，更新数据库。OS Windows操作系统下完整命令行可为：

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log modexecdb database-upgrade
```

9. 启动Dr.Web服务器服务。

如转移**Dr.Web**服务器时更改**IP**地址或名称：



如是通过管理中心指定新Dr.Web服务器地址，而不是在工作站代理端本身设置中给出，这时为使代理端转至新服务器，需让新旧两个Dr.Web服务器同处于运行状态，直到结束整个转移过程。

1. 照上述步骤转移Dr.Web服务器。
2. 为所有连接原Dr.Web服务器的代理端按照将Dr.Web代理端连接到另一Dr.Web服务器一节描述的操作指定新Dr.Web服务器地址。

   如是通过管理中心指定新Dr.Web服务器地址，而不是在工作站代理端本身设置中给出，这时为使代理端转至新Dr.Web服务器，新旧两个Dr.Web服务器的代理端设置都应指定新服务器地址。
3. 等待所有代理端转至新Dr.Web服务器。之后可以删除原Dr.Web服务器。

将Dr.Web代理端连接到另一Dr.Web服务器

将代理端连接到另一Dr.Web服务器有两种方式：

1. 利用管理中心。

   不直接访问工作站进行远程设置的前提是工作站还与原Dr.Web服务器保持连接。同时需要原来的和新的Dr.Web服务器管理中心都能访问。

2. 直接在工作中设置。

   直接在工作中设置。要求有这一工作站的管理员权限和在Dr.Web服务器指定的更改代理端设置的权限。不具备上述权限的情况下本地转接到另一Dr.Web服务器只能是删除已安装的代理端后安装指定有新Dr.Web服务器设置的新代理端。如没有本地删除代理端的情绪，可使用工具Dr.Web Remover在工作站删除代理端，或通过管理中心删除代理端。

利用管理中心将Dr.Web代理端转至另一Dr.Web服务器

1. 在新Dr.Web服务器允许登录参数不正确的工作站作为新工作站申请新的登录参数。操作是在管理中心选择主菜单的**管理** → 控制菜单的**Dr.Web服务器配置**→**常规**标签：
   a) 勾选**将未登录的列为新工作站**。
   b) 如**新工作站注册模式**下拉列表选择的是**总是拒绝访问**，需更改为**手动批准访问**或**自动允许访问**。
   c) 应用更改需点击**保存**后重启Dr.Web服务器。

   > 如公司网络政策不允许更改步骤1的设置，则需要直接在工作中更改原先在管理中心创建工作站账户时指定的登录参数。

2. 在代理端连接的原Dr.Web服务器指定新Dr.Web服务器参数。操作是在管理中心选择主菜单的**反病毒网络** → 网络分层列表 选择需要的工作站（或工作站组）→ 在控制菜单选择**连接参数**：
   a) 如新Dr.Web服务器的证书与原Dr.Web服务器证书不符，需在**证书**一栏指示新Dr.Web服务器证书路径。
   b) 在**服务器**一栏输入新Dr.Web服务器地址。
   c) 点击**保存**按钮。

直接在工作站将Dr.Web代理端转至另一Dr.Web服务器

1. 在代理端设置中给出新Dr.Web服务器参数。操作是利用代理端图标菜单打开**安全中心** →点击关闭的锁头，打开锁头后可访问高级设置 → 按钮访问设置 → 选项**服务器** → 按钮**更改设置**：
   a) 如新Dr.Web服务器的证书与原Dr.Web服务器证书不符，需利用**证书列表**按钮指示新Dr.Web服务器证书路径。
   b) 点击**添加**按钮输入新Dr.Web服务器的相应参数。
2. 将工作站列为新工作站（在Dr.Web服务器清空登录参数）。操作是在步骤1的连接参数设置点击：**工作站连接参数**按钮 → **清空参数并作为新工作站连接**按钮 → **清空参数**按钮。

如事先知道连接新Dr.Web服务器的ID和密码，可在**工作站ID**和**密码**两栏输入。这种情况下没有必要将工作站列为新工作站。

更换Dr.Web Enterprise Security Suite DBMS类型

OS Windows下



启动和停止Dr.Web服务器的操作（参见管理员手册中的启动和停止Dr.Web服务器）。

1. 停止运行中的Dr.Web服务器。
2. 在命令行使用参数modexecdb database-export启动drwcsd.exe，将数据库内容导出到文件。OS Windows操作系统下完整的导出命令行可为：

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log modexecdb database-export D:\esbase.es"
```

此例中Dr.Web服务器安装于目录C:\Program Files\DrWeb Server，库导出到D盘根目录的某文件esbase.es。

如果文件路径中有空格和/或本民族文字符号（或者文件名含有空格和/或本民族文字符号），则路径需使用引号：

```
"D:\<路径名>\esbase.es"。
```

3. 启动Dr.Web服务器。连接管理中心后将Dr.Web服务器设置为使用另一DBMS。拒绝重启Dr.Web服务器。
4. 停止运行中的Dr.Web服务器。
5. 请删除数据库文件。
6. 使用命令行参数modexecdb database-init启动drwcsd.exe，进行新数据库初始化。OS Windows操作系统Dr.Web服务器数据库初始化命令行可为：

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log modexecdb database-init D:\Keys\agent.key<
密码>
```

此例中Dr.Web服务器安装于目录 "C:\Program Files\DrWeb Server"，而代理端密钥agent.key在D:\Keys。

如果文件路径中有空格和/或本民族文字符号（或者文件名含有空格和/或本民族文字符号），则路径需使用引号：

```
"D:\<路径名>\agent.key"
```

7. 在命令行使用参数modexecdb database-import启动drwcsd.exe，将数据库内容从文件导入。OS Windows操作系统下完整的导入命令行可为：

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log modexecdb database-import D:\esbase.es"
```

8. 启动Dr.Web服务器服务。

UNIX操作系统下

1. 利用脚本停止Dr.Web服务器：
   - OS **Linux**：

```
/etc/init.d/drwcsd stop
```

   - OS **FreeBSD**：

```
/usr/local/etc/rc.d/drwcsd stop
```

   或者利用管理中心。
2. 使用参数`modexecdb database-export`启动Dr.Web服务器，将数据库内容导出到文件。Dr.Web服务器安装目录完整的命令行可为：
   - OS **Linux**：

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-
export /var/opt/drwcs/esbase.es
```

   - OS **FreeBSD**：

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-
export /var/drwcs/esbase.es
```

   此例中数据库导出到用户根目录的文件`esbase.es`。
3. 利用脚本启动Dr.Web服务器：
   - OS **Linux**：

```
/etc/init.d/drwcsd start
```

   - OS **FreeBSD**：

```
/usr/local/etc/rc.d/drwcsd start
```

   连接管理中心，将Dr.Web服务器设置为使用另一DBMS：在菜单**管理** → **Dr.Web服务器配置** → **数据库**标签。

   还可以通过直接编辑Dr.Web服务器配置文件`drwcsd.conf`将Dr.Web服务器设置为使用另一DBMS。操作是注释/删除当前数据库记录后写入新数据库（详见附录G1. Dr.Web服务器配置文件）。

   出现重启Dr.Web服务器提示，不进行重启。
4. 停止Dr.Web服务器（参见步骤**1**）。
5. 请删除数据库文件。
6. 使用参数`modexecdb database-init`启动`drwcsd`，进行新数据库初始化。初始化命令行可为：
   - OS **Linux**：

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-init
```

- OS **FreeBSD**：

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-init
```

7. 使用参数`modexecdb database-import`启动文件`drwcsd`，将数据库内容从文件导入。导入命令行可为：

- OS **Linux**：

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-
import /var/opt/drwcs/esbase.es
```

- OS **FreeBSD**：

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-
import /var/drwcs/esbase.es
```

8. 启动Dr.Web服务器（参见步骤**3**）。



如启动Dr.Web服务器脚本时要求指定参数（如指定Dr.Web服务器安装目录、更改日志详细等级等等），需在启动脚本进行相应修改：

- OS **FreeBSD**：

```
/usr/local/etc/rc.d/drwcsd
```

- OS **Linux**：

```
/etc/init.d/drwcsd
```

恢复Dr.Web Enterprise Security Suite数据库

Dr.Web服务器运行过程中会定期在以下命令备份重要信息：授权密钥文件、数据库内容、加密私钥、Dr.Web服务器和管理中心的配置文件。

备份保存于以下目录：

- OS **Windows**：*<安装磁盘>*:\DrWeb Backup
- OS **Linux**：/var/opt/drwcs/backup
- OS **FreeBSD**：/var/drwcs/backup

进行定期备份需在Dr.Web服务器日程中启用每日任务。如日志中暂无此任务，建议新建。

备份中所有文件可使用，只有数据库内容除外。数据库备份保存为.gz格式，与gzip和其他存档兼容。可利用指令modexecdb database-import将数据库内容从备份导入到Dr.Web服务器工作数据库来恢复数据。

可使用管理员通过管理中心在**管理** → **管理数据库** → **导出**（仅限**导出整个数据库模式**）手动创建的备份来恢复数据库。

不同版本Dr.Web服务器数据库的恢复

只有当建立备份的Dr.Web服务器和进行数据库恢复的Dr.Web服务器同属一个主版本时，才可恢复数据库。

例如：

- 版本13的Dr.Web服务器建立的数据库备份只能利用版本13的Dr.Web服务器进行恢复。
- 版本10的Dr.Web服务器建立的数据库备份不可利用版本13的Dr.Web服务器恢复。

如果在Dr.Web服务器从较早版本更新到13.0版本时由于某种原因数据库受损，需完成以下操作：

1. 删除Dr.Web服务器版本13.0。这时将自动备份Dr.Web服务器使用的文件。
2. 安装更新前的旧版本Dr.Web服务器，也就是建立数据库备份的版本。

   这时按照正常更新流程使用所有保存的Dr.Web服务器文件，只有数据库除外。

   Dr.Web服务器安装过程中创建新数据库。
3. 按照常规操作从备份恢复数据库（见下）。
4. 在Dr.Web服务器设置中停用代理端、Dr.Web服务器和网络安装程序的协议，操作是在管理中心主菜单选择**管理**一项，在打开的窗口选择控制菜单中的**Dr.Web服务器配置**，进入**模块**标签，取消对相应选项的勾选。
5. 按照常规方式将Dr.Web服务器升级到版本13.0（参见管理员手册中的Dr.Web Enterprise Security Suite及其组件的更新）。
6. 启用在步骤4关闭的代理端、Dr.Web服务器和网络安装程序的协议。

OS Windows下

启动和停止Dr.Web服务器的操作（参见管理员手册中的启动和停止Dr.Web服务器）。

从备份恢复数据库

1. 停止运行中的Dr.Web服务器。
2. 从相应的备份文件导入数据库内容。导入行可为：
   - 对于版本13之前的Dr.Web服务器

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log importdb "<备份文件路径>\database.gz"
```

   - 对于版本13以及之后的Dr.Web服务器

```
C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log modexecdb database-import "<备份文件路径
>\database.gz"
```

   命令行以一行输入。此例中Dr.Web服务器安装于目录 `C:\Program Files\DrWeb Server`。
3. 启动Dr.Web服务器服务。

（在同一主版本范围内）更换Dr.Web服务器版本时或当前版本数据库受损时恢复数据库

1. 停止运行中的Dr.Web服务器。
2. 删除当前数据库内容。操作是：
   2.1. 使用内设数据库时：
   a) 删除数据库文件`database.sqlite`。
   b) 进行新数据库的初始化。OS Windows操作系统下Dr.Web服务器数据库初始化命令行可为：
   - 对于版本13之前的Dr.Web服务器

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log initdb D:\Keys\agent.key - - <密码>
```

   - 对于版本13以及之后的Dr.Web服务器

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log modexecdb database-init D:
\Keys\agent.key<密码>
```

命令行以一行输入（命令行格式参见附录H3.3. 数据库管理指令中带modexecdb database-init参数的drwcsd）。此例中Dr.Web服务器安装于目录C:\Program Files\DrWeb Server，而授权密钥agent.key在目录D:\Keys。

c) 执行此命令后在 Dr.Web服务器安装目录的var文件夹应出现新的数据库文件database.sqlite。

2.2. 使用外设数据库时：利用指令cleandb（如果是版本13之前的Dr.Web服务器）或 modexecdb database-clean （如果是版本13以及之后的Dr.Web服务器）清空数据库（参见附录 H3.3. 数据库管理指令）。

3. 从相应的备份文件导入数据库内容。导入行可为：

- 对于版本13之前的Dr.Web服务器

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log importdb "<备份文件路径>\database.gz"
```

- 对于版本13以及之后的Dr.Web服务器

```
C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log modexecdb database-import "<备份文件路径>\database.gz"
```

命令行以一行输入。此例中Dr.Web服务器安装于目录 C:\Program Files\DrWeb Server。

4. 启动Dr.Web服务器服务。

UNIX操作系统下

1. 停止Dr.Web服务器运行（如为启用状态）：

- OS **Linux**：

```
/etc/init.d/drwcsd stop
```

- OS **FreeBSD**：

```
/usr/local/etc/rc.d/drwcsd stop
```

2. 从Dr.Web服务器安装目录的以下目录删除数据库文件database.sqlite：

- OS **Linux**：/var/opt/drwcs/
- OS **FreeBSD**：/var/drwcs/



使用外设数据库时清空数据库需利用指令cleandb（如果是版本13之前的Dr.Web服务器）或modexecdb database-clean （如果是版本13以及之后的Dr.Web服务器）（参见附录 H3.3. 数据库管理指令）。

3. 进行Dr.Web服务器数据库初始化。使用的命令是：

- OS **Linux**：
  - 对于版本13之前的Dr.Web服务器

```
/etc/init.d/drwcsd -log=drwcsd.log initdb
```

- 对于版本13以及之后的Dr.Web服务器

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-init
```

- OS **FreeBSD**：
  - 对于版本13之前的Dr.Web服务器

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log initdb
```

  - 对于版本13以及之后的Dr.Web服务器

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-init
```

4. 执行此命令后在Dr.Web服务器安装目录的var文件夹应出现新的数据库文件database.sqlite。
5. 从相应的备份文件导入数据库内容。导入行可为：
   - OS **Linux**：
     - 对于版本13之前的Dr.Web服务器

```
/etc/init.d/drwcsd -log=drwcsd.log importdb "<备份文件路径>/database.gz"
```

     - 对于版本13以及之后的Dr.Web服务器

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-import "<备份文件路径>/database.gz"
```

   - OS **FreeBSD**：
     - 对于版本13之前的Dr.Web服务器

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log importdb "<备份文件路径>/database.gz"
```

     - 对于版本13以及之后的Dr.Web服务器

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-import "<备份文件路径>/database.gz"
```

6. 启动Dr.Web服务器。
   - OS **Linux**：

```
/etc/init.d/drwcsd start
```

   - OS **FreeBSD**：

```
/usr/local/etc/rc.d/drwcsd start
```

如启动Dr.Web服务器脚本时要求指定参数（如指定Dr.Web服务器安装目录等等），需在启动脚本进行相应修改：

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

如需要更改Dr.Web服务器日志详细等级，需使用文件`local.conf`：

- OS Linux：`/var/opt/drwcs/etc/local.conf`；
- OS FreeBSD：`/var/drwcs/etc/local.conf`。

如果有代理端是在创建最后一次备份之后安装的，则从此备份恢复数据库后这样的代理端无法连接Dr.Web服务器。可远程将这样的工作站列为新工作站。操作是在**管理** → **Dr.Web服务器配置**的**常规**标签勾选**将未登录工作站列为新工作站**。在**新工作站注册模式**下拉列表选择**自动允许访问**。点击**保存**后重启Dr.Web服务器。

在所有工作站成功连接新Dr.Web服务器后，将Dr.Web服务器设置更改为符合公司安全策略的设置。

恢复数据库后建议通过管理中心连接Dr.Web服务器，在**管理** → **Dr.Web服务器任务计划器**检查是否有**服务器关键数据备份**任务。如没有这一任务，建议创建。

更新局域网服务器上的客户端

更新局域网服务器上安装的代理端时，可能不希望对这样的工作站进行重启或停用网络软件。

为避免执行局域网重要功能的工作站出现运行中断，建议使用以下模式更新代理端和反病毒软件：

1. 在Dr.Web服务器日程中将更新所有组件任务更改为只更新病毒库。
2. 将新的更新所有组件的任务时间设置为对局域网运行影响不大的时间。

   Dr.Web服务器日程任务的创建和编辑见管理员手册中的Dr.Web服务器日程设置。



不建议在执行重要网络功能的服务器（域控制器、授权分发服务器等等）安装组件SpIDer Gate、SpIDer Mail和Dr.Web防火墙，以免网络服务与Dr.Web反病毒软件内部组件可能发生冲突。

使用DFS通过Active Directory安装代理端

通过Active Directory安装Dr.Web代理端时可能需使用分布式文件系统服务（DFS）。

此方式在某些情况下，如局域网中存在几个域控制器时会更为方便。

在带多个域控制器的网络安装Dr.Web代理端

1. 在每个域控制器建立名称相同的目录。
2. 利用DFS将创建的目录合并为一个根目标目录。
3. 进行管理员安装，将软件包`*.msi`安装到建立的目标目录（见 **安装手册**中的使用Active Directory服务安装Dr.Web代理端）。
4. 在组策略对象编辑器中指定软件包时使用此目标目录。
   应使用的网络名称格式： *<domain>**<folder>*
   其中：*<domain>*——域名，*<folder>*——目标目录名称。

Dr.Web服务器出现事故后恢复反病毒网络

如Dr.Web服务器建议执行相应流程恢复反病毒网络的运行能力，不需要在工作站重新安装代理端。

恢复运行指的是在保留原IP地址和DNS名称的计算机安装新的Dr.Web服务器。

具备Dr.Web服务器备份的情况下进行还原

Dr.Web服务器运行过程中会定期在以下命令备份重要信息：授权密钥文件、数据库内容、加密私钥、Dr.Web服务器和管理中心的配置文件。

备份保存于以下目录：

- OS **Windows**：*<安装磁盘>*:\DrWeb Backup
- OS **Linux**：/var/opt/drwcs/backup
- OS **FreeBSD**：/var/drwcs/backup

进行定期备份需在Dr.Web服务器日程中启用每日任务。如日志中暂无此任务，建议新建。

备份中所有文件可使用，只有数据库内容除外。数据库备份保存为.gz格式，与gzip和其他存档兼容。可利用指令modexecdb database-import-and-upgrade将数据库内容从备份导入到Dr.Web服务器工作数据库来恢复数据。

可使用管理员通过管理中心在**管理** → **管理数据库** → **导出**（仅限**导出整个数据库模式**）手动创建的备份来恢复数据库。

建议将备份和其他重要文件同时保存到另一台计算机。这样如果安装Dr.Web服务器的计算机出现故障，可以恢复数据和Dr.Web服务器运行功能。如授权密钥丢失可找回，详见**管理员手册**中的授权。

在Dr.Web服务器出现故障且保存有备份时恢复Dr.Web服务器

1. 选择安装新的Dr.Web服务器的计算机。将此计算机与现运行的代理端隔离：可与安装代理端的网络断开，或临时使用另一IP地址，或采取其他方便的隔离方式。
2. 安装新的Dr.Web服务器。
3. 在**管理** → **授权管理器**添加上次安装Dr.Web服务器的授权密钥并将其分发给相应的组，包括**Everyone**组。如安装Dr.Web服务器时未给出授权密钥，则必须执行此步骤。
4. 从GUS更新Dr.Web服务器库：
   a) 打开管理中心的**管理**→**库状态**。
   b) 点击**检查更新**按钮即可检查GUS是否有产品更新并从GUS服务器下载更新。
5. 如有Dr.Web服务器新版本，则将其更新到最新版本：
   a) 打开管理中心的**管理**→**Dr.Web服务器**。

b) 查看Dr.Web服务器版本列表需点击当前Dr.Web服务器版本或点击**版本列表**。打开**Dr.Web服务器更新**部分，显示可用的Dr.Web服务器更新和备份列表。

c) 更新Dr.Web服务器版本需在**所有版本**列表勾选最新的服务器版本后点击**保存**按钮。

d) 等待Dr.Web服务器完成更新。

6. 停止Dr.Web服务器。

7. 将Dr.Web服务器重要数据替换为从备份获得的数据：

操作系统	配置文件
Windows	etc在Dr.Web服务器安装目录
Linux	/var/opt/drwcs/etc
FreeBSD	/var/drwcs/etc

8. 设置数据库。

a) 外设数据库：

不需要进行其他操作来连接数据库和Dr.Web服务器（前提是保存有Dr.Web服务器配置文件）。

如新安装的Dr.Web服务器版本高于原Dr.Web服务器，需使用指令modexecdb database-upgrade更新外设数据库：

- OS Windows：

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log
modexecdb database-upgrade
```

- OS Linux：

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-upgrade
```

- OS FreeBSD：

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-upgrade
```

b) 外设或内设数据库备份：

使用外设数据库时需事先利用指令modexecdb database-clean清空数据库（参见附录H3.3. 数据库管理指令）。

从相应备份文件导入数据库，并利用指令modexecdb database-import-and-upgrade将数据库格式更新为新安装的Dr.Web服务器版本：

- OS Windows：

```
C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log modexecdb database-import-and-upgrade "<
备份文件路径>\database.gz"
```

- OS Linux：

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-import-and-upgrade "<备份文件路径>/database.gz"
```

- OS FreeBSD：

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-import-and-upgrade "<备份文件路径>/database.gz"
```



所有更换的Dr.Web服务器文件都需设定安装原来的Dr.Web服务器时指定的系统权限。

UNIX家族操作系统：rw用于drwcs:drwcs。

9. 启动Dr.Web服务器。
10. 检查从数据库备份获得的数据是否完整，是否为可用数据：代理端设置、反病毒网络树结构状态等等。
11. 根据步骤1中选择的Dr.Web服务器隔离方式恢复代理端对Dr.Web服务器的访问。



如果有代理端是在创建最后一次备份之后安装的，则从此备份恢复数据库后这样的代理端无法连接Dr.Web服务器。可远程将这样的工作站列为新工作站。操作是在**管理** → **Dr.Web服务器配置**的**常规**标签勾选**将未登录工作站列为新工作站**。在**新工作站注册模式**下拉列表选择**自动允许访问**。点击**保存**后重启Dr.Web服务器。

在所有工作站成功连接新Dr.Web服务器后，将Dr.Web服务器设置更改为符合公司安全策略的设置。

不具备Dr.Web服务器备份的情况下进行还原

在服务器出现故障且没有保存任何备份时恢复服务器

1. 选择安装新的Dr.Web服务器的计算机。将此计算机与现运行的代理端隔离：可与安装代理端的网络断开，或临时使用另一IP地址，或采取其他方便的隔离方式。
2. 安装新的Dr.Web服务器。
3. 在**管理** → **授权管理器**添加上次安装Dr.Web服务器的授权密钥并将其分发给相应的组，包括**Everyone**组。如安装Dr.Web服务器时未给出授权密钥，则必须执行此步骤。
4. 从GUS更新Dr.Web服务器库：
   a) 打开管理中心的**管理**→**库状态**。
   b) 点击**检查更新**按钮即可检查GUS是否有产品更新并从GUS服务器下载更新。
5. 如有Dr.Web服务器新版本，则将其更新到最新版本：
   a) 打开管理中心的**管理**→**Dr.Web服务器**。
   b) 查看Dr.Web服务器版本列表需点击当前Dr.Web服务器版本或点击**版本列表**。打开**Dr.Web服务器更新**部分，显示可用的Dr.Web服务器更新和备份列表。
   c) 更新Dr.Web服务器版本需在**所有版本**列表勾选最新的服务器版本后点击**保存**按钮。
   d) 等待Dr.Web服务器完成更新。

6. 在Dr.Web服务器配置更改工作站连接设置：
   a) 打开**管理** → **Dr.Web服务器配置**。
   b) 在**常规**标签勾选**将未登录的列为新工作站**。
   c) 在**常规**标签**新工作站注册模式**下拉列表选择**自动允许访问**。
   d) 点击**保存**并重启Dr.Web服务器。
7. 在管理中心**反病毒网络**部分按照原版本反病毒网络树结构建立用户组。如需可在创建的用户组指定自动组籍规则。
8. 如需可按照原版本指定代理端设置和Dr.Web服务器设置（第6步的临时设置除外）。
9. 如需可在**管理** → **库详细配置**更改库设置。
10. 根据步骤1中选择的Dr.Web服务器隔离方式恢复代理端对Dr.Web服务器的访问。
11. 更换需连接新Dr.Web服务器的所有工作站上的加密公钥。
    - 如自我保护组件为启用，将安装新Dr.Web服务器时创建的公钥复制到工作站的操作是：

      `es-service.exe -p <密钥>`

      或

      `es-service.exe --addpubkey=<密钥>`

      在*<密钥>*指示复制的加密公钥的路径。

      公钥会复制到代理端安装目录。默认是目录`%ProgramFiles%\DrWeb`（详见附录H2. Windows操作系统Dr.Web代理端）。
    - 如工作站上自我保护组件为停用，可将安装新Dr.Web服务器时创建的公钥复制到上述目录。
12. 在所有工作站都成功连接新Dr.Web服务器后，将在第5步指定的Dr.Web服务器设置更改为符合公司安全策略的设置。

管理Windows操作系统Dr.Web服务器的日志记录等级

可用以下一个方式更改**Windows操作系统Dr.Web服务器日志的详细等级**：

- 利用管理中心的**Dr.Web服务器配置** → **日志**部分。

  建议采取这一方式。在**日志**可以指定任一Dr.Web服务器日志详细等级，还可指定一些其他设置。

  详细信息见**管理员手册**中的设置Dr.Web服务器配置→日志。
- 利用控制台指令：

```
drwcsd [<参数>] install
```

  可利用参数`--verbosity`指定任一Dr.Web服务器日志详细等级。

  利用命令行参数管理Dr.Web服务器的相关详细信息参见H3.8. 参数介绍。

  将日志记录等级设为**详细**的指令示例：

```
drwcsd --daemon "--home=C:\Program Files\DrWeb Server" "--bin-root=C:
\Program Files\DrWeb Server" "--var-root=C:\Program Files\DrWeb
Server\var" --verbosity=ALL --log=drwcsd.log --rotate=10,50m install
```

其他参数为必设，如重新指定了Dr.Web服务器安装目录和其工作目录。

更改日志记录详细等级后必须重新启动Dr.Web服务器：

```
drwcsd restart
```

- 利用OS Windows开始主菜单中的指令。

  这时只有两个日志详细登记：详细或标准：

  a) 软件→服务器管理→详细日志
  或
  软件→服务器管理→标准日志

  b) 软件→服务器管理→重新启动。

自动确定OS Android工作站位置

Dr.Web Enterprise Security Suite可自动向管理员提供受保护的OS Android工作站所在位置。

确定移动设备位置

1. 设置将受保护移动设备位置数据传输给服务器：
   a) 在Dr.Web安全管理中心的反病毒网络树结构选择所需的OS Android工作站。
   b) 选择控制菜单中的**Dr.Web for Android**。
   c) 在常规标签勾选跟踪所在地。在发送坐标的时间间隔下列列表选择更新设备位置信息的时间间隔。
   d) 保存更改。
2. 通过以下一种方式自动确定位置：
   - 如设备上启用的位置供应商（GPS，移动网络）且信号稳定，则利用移动设置本身来确定其位置。
   - 如设备上停用的位置供应商（GPS，移动网络）且没有GPS信号，则Dr.Web Enterprise Security Suite利用Yandex.Locator服务根据移动信号塔坐标（GSM, 3D, LTE）和WiFi ID来确定移动设备的位置。
     设置Yandex.Locator技术需即会被设置插件**Yandex.Locator**：
     a) 在Yandex公司官网https://yandex.ru/dev/locator/keys/get/获取API密钥。
     b) 在Dr.Web安全管理中心的管理 → 模块部分勾选插件**Yandex.Locator**。
     c) 在**API密钥**一栏输入在步骤a)获得的密钥。
     d) 保存更改后重启Dr.Web服务器。

   只有OS Android 5.1或更早版本的移动设备才可使用WiFi ID。

3. 在Dr.Web安全管理中心查看工作站位置：
   a) 在反病毒网络的树结构中选择在步骤1为其指定相应设置的工作站。
   b) 工作站属性的位置部分会自动出现从移动设备获得的地理坐标。
   c) 点击在地图上指示后会在OpenStreetMap看到此坐标对应的移动设备所在地。

访问Dr.Web服务器数据库示例

下面是访问PostgreSQL数据库的SQL请求示例。访问其他数据库所使用的申请可能因数据库本身特点以及具体使用情况而有所区别。



SQL语言无法兼顾组和工作站的级别

直接向数据库发出的请求

1. 打开您的Dr.Web服务器的管理中心。
2. 转至**管理** → **SQL控制台**。
3. 输入相应的SQL请求，请求示例见下。
4. 点击**执行**按钮。

SQL请求示例

1. 搜索安装有OS Windows服务器版本且病毒库早于2019.07.04-00:00:00 UTC (12.0)的工作站。

```
SELECT
  stations.name Station,
  groups_list.name OS,
  station_products.crev Bases
FROM
  stations
  INNER JOIN groups_list ON groups_list.platform =(
    CAST(stations.lastos AS INTEGER) & ~15728640
  )
  AND (
    (
      CAST(stations.lastos AS INTEGER) & 2130706560
    ) = 33554560
  )
  INNER JOIN station_products ON station_products.id = stations.id
  AND station_products.product = '10-drwbases'
  AND station_products.crev < 12020190704000000;
```

2. 搜索其在**反病毒网络**→**统计信息**→**状态**部分的记录严重性为**高**或**最高**的工作站。

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id IN (
    SELECT
      DISTINCT id
    FROM
      station_status
    WHERE
      severity >= 1342177280
  );
```

3. 提取状态符合的工作站以及具备这些状态的工作站的数量。

```
SELECT
  code Code,
  COUNT(code) Num
FROM
  (
    SELECT
      DISTINCT id,
      code
    FROM
      station_status
  ) AS t
GROUP BY
  Code
ORDER BY
  Code;
```

4. 提取2019.06.01至2019.07.01期间识别码为'373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'的组或其所有内嵌组所包含的工作站上发现最多的10个威胁。

```
SELECT
  cat_virus.str Threat,
  COUNT(cat_virus.str) Num
FROM
  station_infection
  INNER JOIN cat_virus ON cat_virus.id = station_infection.virus
WHERE
  station_infection.infectiontime BETWEEN 20190601000000000
  AND 20190701000000000
  AND station_infection.id IN (
    SELECT
      sid
    FROM
      station_groups
    WHERE
      gid = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      OR gid IN (
        SELECT
          child
        FROM
          group_children
        WHERE
          id = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      )
  )
GROUP BY
  cat_virus.str
ORDER BY
  Num DESC
LIMIT
  10;
```

5. 提取10个感染最严重的工作站。

```
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. 如用户组不是其所含工作站的基组，则从这些用户组删除所有工作站。

```
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. 搜索反病毒网络中其域名包含于SpIDer Gate白名单自身设置的对象。

```
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. 从管理员登录管理中心失败审计事件中提取错误登录及其代码。

```
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. 搜索未安装必要安全补丁的OS Windows工作站。

```
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'
          )
      )
  );
```

第四章、问题和解除方法

远程安装问题诊断

安装原则：

1. Dr.Web服务器连接远程计算机上的资源ADMIN$（*<远程机>*\ADMIN$\Temp）并将网络安装程序drwinst.exe（位置在Dr.Web服务器安装目录的webmin\install\windows ）和SSL证书drwcsd-certificate.pem（位置在Dr.Web服务器安装目录的etc）拷贝到目录*<远程机>*\ADMIN$\Temp。
2. Dr.Web服务器使用管理中心设置中对应的参数在远程计算机上启动文件drwinst.exe。

成功安装要求在启动安装的**Dr.Web**服务器：

1. 能够访问远程计算机上的ADMIN$\Temp。

   可用以下方式检查是否可以访问：

   在Windows Explorer地址行输入：

   *<远程计算机>*ADMIN$\Temp

   应出现登录该资源的用户名和密码输入提示。输入安装页面所显示的账户。

   ADMIN$\Tem资源不可访问的可能原因：

   a) 账户不具备管理员权限；
   b) 计算机处于关机状态或网关阻止访问445端口；
   c) 如不在域中，OS Windows Vista或更高版本限制远程访问ADMIN$\Temp。
   d) 不存在目录所有人或用户或组访问目录权限不足。
2. 曾有对文件drwinst.exe和加密公钥*.pub的访问权限。

管理中心显示详细信息（阶段和错误码），根据这一信息可以判断错误原因。

远程安装Dr.Web代理端错误列表

阶段	错误	原因
按照SMB连接工作站 *<host>*	工作站 *<host>*地址错误	要代理端的工作站IP地址不是正确的IPv4/IPv6地址或未能将DNS名称转换为地址：或者是此DNS名称不存在，或者是名称服务器设置有误。
	按照SMB连接工作站 *<host>*出错	未能按照SMB连接到工作站。可能的原因： • 工作站上停用了服务器服务； • 无法访问远程计算机上的445 TCP端口，可能原因： ▫ 计算机处于关机状态； ▫ 网关阻止该端口； ▫ 远程计算机上的OS有别于OS Windows； • 未设置本地账户共享和安全策略模块； • 无法访问身份验证服务器（域控制器）； • 未知用户或错误密码。
	在工作站 *<host>*打开共享资源 *<share>*权限不足	远程计算机上不存在ADMIN$资源。或者打开资源权限不足。
将文件发送到工作站 *<host>*	未能在工作站 *<host>*共享资源 *<share>*中找到路径 *<path>*	不存在目录ADMIN$/TEMP。
	未能在工作站 *<host>*共享资源 *<share>*中创建临时目录 *<path>*	未能在ADMIN$/TEMP创建临时目录，例如，写入权限不足。
	未能在工作站 *<host>*共享资源 *<share>*中删除临时目录 *<path>*	进程结束后未能在ADMIN$/TEMP删除目录。例如，未能等到服务结束进程，或者是有人在此目录打开了文件。
	未能在Dr.Web服务器打开只读文件 *<path>* 未能在Dr.Web服务器读取文件 *<path>*	Dr.Web服务器上不存在安装文件，或对安装文件的权限不足。
	未能在工作站 *<host>*共享资源 *<share>*中打开文件 *<path>*进行写入 未能在工作站 *<host>*共享资源 *<share>*中写入文件 *<path>*	读取/写入相应文件或在相应目录进行操作的权限不足。

阶段	错误	原因
在工作站 *<host>* 创建服务	连接工作站 *<host>*上的服务器服务（srvsvc RPC）时出错	无法远程管理服务。
	连接工作站 *<host>*上的SCM时出错 未能在工作站 *<host>*创建服务 未能在工作站 *<host>*启动服务 未能在工作站 *<host>*停止服务 未能在工作站 *<host>*删除服务	管理服务权限不足。
在工作站 *<host>* 执行服务	未能获取工作站 *<host>*上的服务状态	可能是SCM出现错误。
	工作站 *<host>*上的安装因超时中断	安装器未能在指定时间内安装代理端。可能的原因：工作站与Dr.Web服务器间为慢通道，未能加载必要的数据。
	未能获取工作站 *<host>*共享资源 *<share>*的路径	未能确定工作站上到资源ADMIN$的路径。
	工作站 *<host>*上服务出错而结束执行。结束状态：*<state>*。错误代码：*<rc>*。	代理端安装器错误。

消除安装Windows操作系统Dr.Web代理端时的BFE服务错误

Dr.Web for Windows反病毒软件某些组件需要启用基础过滤模块（BFE）。如不存在此服务或受损，则无法安装Dr.Web for Windows代理端。BFE服务受损或不存在可能是由于工作站上存在安全威胁。

如安装Windows操作系统Dr.Web代理端时BFE服务出错，请执行以下操作：

1. 使用Doctor Web公司提供的清除工具CureNet!对工作站进行扫描。
   可在此申请工具试用版（不包含清除功能）：https://download.drweb.com/curenet/。
   可在此了解使用工具完整版本的条件和价格：https://estore.drweb.com/utilities/。
2. 手动启动或重启BFE服务。如未能启动BFE服务或列表中不存在此服务，请联系 Microsoft公司技术支持部门。
3. 启动Windows操作系统Dr.Web代理端安装，按照**安装手册**的常规流程进行安装。
   如上述操作未能解决问题，请联系Doctor Web公司技术支持。

技术支持

如安装和使用产品过程中出现问题，在联系技术支持部门之前建议先采用以下方式解决：

- 参阅最新版本的说明文档和帮助手册：https://download.drweb.com/doc/；
- 查阅常见问题：https://support.drweb.com/show_faq/；
- 访问Doctor Web公司论坛：https://forum.drweb.com/。

如仍未能解决出现的问题，可采用下面的一种方式联系Doctor Web公司技术支持：

- 在https://support.drweb.com/页面填写问题提交表；
- +86 (022) 5982-3480 工作时间：周一至周五,早9:00至晚5:00。

Doctor Web公司在其他地区和国家分支机构的联系方式见官网：
https://company.drweb.com/contacts/offices/。

索引

D

DBMS设置 15
Dr.Web服务器
  还原 205
  配置文件 76
  启动参数 117
  转移 191

[其它]

备份
  服务器 205
  数据库 198
代理端
  启动参数 116
代理服务器
  配置文件 102
  启动参数 128
反病毒扫描仪 127
  命令行 127
  启动参数 127
管理中心
  配置文件 97
还原
  服务器 205
  数据库 198
环境变量 155
加密
  密钥，生成 134
密钥
  加密，生成 134
配置文件
  Dr.Web服务器 76
  代理服务器 102
  格式 76
  管理中心 97
  库加载器 108
启动参数
  Dr.Web服务器 117
  代理端 116
  代理服务器 128
  反病毒扫描仪 127
  网络安装程序 113
扫描仪
  反病毒 127
数据库
  MySQL 23
  ODBC 17
  Oracle 19
  PostgreSQL 21
  备份 198
  还原 198
  内设 15
通知
  模板参数 38
网络安装程序
  启动参数 113
网络地址 67
  Dr.Web代理端 69
  代理端安装程序 69
  格式 67
系统要求 10
正则表达式 156

© Doctor Web, 2022