Dr.WEB

Enterprise Security Suite

管理员手册



© 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**
管理员手册
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 9
1.1. 文档用途 9
1.2. 标志与缩写 10
第二章、**Dr.Web Enterprise Security Suite** 12
2.1. 关于产品 12
2.2. 系统要求 19
2.3. 供货方案 24
第三章、授权 26
3.1. 授权特点 26
3.2. 通过服务器间连接分发授权 27
3.3. 自动更新授权 29
第四章、开始运行 32
4.1. 反病毒网络的部署 32
4.2. 网络连接设置 32
4.2.1. 直接连接 33
4.2.2. Dr.Web服务器搜索服务 34
4.2.3. 使用SRV协议 34
4.3. 保障安全连接 35
4.3.1. 流量加密和压缩 35
4.3.2. 安全连接保障工具 40
4.3.3. 将客户端连接到Dr.Web服务器 41
4.4. Dr.Web Enterprise Security Suite与**Active Directory**的集成 42
第五章、反病毒网络组件及其接口 45
5.1. Dr.Web服务器 45
5.1.1. Windows操作系统Dr.Web服务器管理 47
5.1.2. UNIX家族操作系统Dr.Web服务器管理 50
5.2. 保护工作站 53
5.3. Dr.Web安全管理中心 54
5.3.1. 管理 57
5.3.2. 反病毒网络 59
5.3.3. 收藏 65
5.3.4. 搜索栏 66
5.3.5. 事件 67

5.3.6. 设置 68
5.3.7. 支持 71
5.4. Dr.Web安全管理中心组件 72
5.4.1. 网络搜索仪 72
5.5. 反病毒网络组件交互作用示意图 75
第六章、反病毒网络管理员 79
6.1. 管理员身份验证 79
6.1.1. Dr.Web服务器数据库管理员身份验证 80
6.1.2. 使用LDAP/AD进行身份验证 80
6.1.3. 使用RADIUS进行身份验证 81
6.1.4. 使用PAM进行身份验证 82
6.1.5. 使用Active Directory进行身份验证 83
6.1.6. 使用LDAP进行身份验证 84
6.2. 管理员和管理员组 85
6.2.1. 管理员级别 86
6.2.2. 管理员权限 87
6.3. 对管理员与管理员组账户的管理 89
6.3.1. 管理记录和组的创建与删除 89
6.3.2. 找回管理员密码 91
6.3.3. 编辑管理员账户和管理员组 92
第七章、工作站的综合管理 95
7.1. 工作站继承配置 95
7.2. 组 98
7.2.1. 系统组和用户组 98
7.2.2. 组管理 101
7.2.3. 将工作站添加到组 104
7.2.4. 对比组和工作站 107
7.2.5. 将设置复制到其它组/工作站 108
7.3. 策略 108
7.3.1. 策略管理 109
7.3.2. 为工作站指定策略 110
7.4. 模式 110
7.4.1. 创建和指定模式 112
7.4.2. 模式设置 113
第八章、工作站的管理 119
8.1. 对工作站账户的管理 119

8.1.1. 工作站连接策略 119
8.1.2. 工作站的删除和恢复 120
8.1.3. 合并工作站 121
8.2. 工作站常规设置 121
8.2.1. 工作站属性 121
8.2.2. 保护组件 125
8.2.3. Windows操作系统工作站的硬软件配置 126
8.3. 设置工作站配置 128
8.3.1. 工作站用户权限 128
8.3.2. 工作站任务日程 129
8.3.3. 可安装的反病毒软件包组件 133
8.3.4. 连接参数 134
8.3.5. 授权密钥 135
8.4. 设置反病毒组件 137
8.5. 工作站反病毒扫描 140
8.5.1. 按类型中断已启动组件的运行 140
8.5.2. 启动工作站扫描 141
8.5.3. 设置扫描仪参数 141
8.6. 查看工作站统计信息 148
8.6.1. 统计信息 148
8.6.2. 图表 155
8.6.3. 隔离区 156
8.7. 分发安装文件 159
8.8. 向工作站发送通知 160
第九章、管理虚拟环境的工作站 163
9.1. 将工作站接通扫描服务器的操作 163
9.2. 与虚拟桌面基础架构集成 167
第十章、Dr.Web服务器设置 170
10.1. 授权管理 170
10.1.1. 授权管理器 170
10.1.2. 授权使用报告 177
10.2. 记录日志 178
10.2.1. 实时日志 178
10.2.2. 审计日志 180
10.2.3. Dr.Web服务器日志 181
10.2.4. 库更新日志 183

10.2.5. 通知日志 184
10.3. 设置Dr.Web服务器配置 185
10.3.1. 常规 186
10.3.2. 流量 187
10.3.3. 网络 189
10.3.4. 统计信息 194
10.3.5. 安全策略 197
10.3.6. 缓存 198
10.3.7. 数据库 199
10.3.8. 模块 201
10.3.9. 位置 201
10.3.10. 授权 202
10.3.11. 日志 203
10.4. 远程访问Dr.Web服务器 203
10.5. Dr.Web的SNMP代理端配置 204
10.6. Dr.Web服务器日程设置 205
10.7. 设置Web服务器配置 214
10.7.1. 常规 215
10.7.2. 高级 217
10.7.3. 传输 217
10.7.4. 安全策略 217
10.7.5. 模块 218
10.7.6. 处理器 219
10.8. 自定义钩子 221
10.9. 通知模板 224
10.10. 通知设置 225
10.10.1. 通知配置 225
10.10.2. Web控制台通知 228
10.10.3. 未发送的通知 230
10.11. 管理Dr.Web服务器库 230
10.11.1. 库状态 234
10.11.2. 推迟的更新 234
10.11.3. 库常规配置 235
10.11.4. 库详细配置 238
10.11.5. 库内容 242
10.12. 应用程序监控 244

10.12.1. 测试模式 246
10.12.2. 可信任的应用程序 248
10.12.3. 应用程序手册 251
10.13. 补充功能 252
10.13.1. 数据库管理 252
10.13.2. Dr.Web服务器统计信息 254
10.13.3. 备份 255
10.13.4. 工具 256
10.13.5. 企业产品 257
10.14. 多台Dr.Web服务器网络特点 259
10.14.1. 部署多台Dr.Web服务器网络 259
10.14.2. 设置Dr.Web服务器间连接 261
10.14.3. 使用多Dr.Web服务器的反病毒网络 266
10.14.4. Dr.Web服务器群集 266
第十一章、更新Dr.Web Enterprise Security Suite组件 270
11.1. 更新Dr.Web服务器和利用备份还原 270
11.2. 手动更新Dr.Web服务器库 271
11.3. 按照日程更新Dr.Web服务器的库 271
11.4. 未接通互联网的Dr.Web Server的库更新 272
11.4.1. 复制另一Dr.Web服务器的库 273
11.4.2. Dr.Web库加载器 273
11.5. 工作站更新限制 276
11.6. 移动模式下Dr.Web代理端的更新 278
第十二章、补充组件设置 279
12.1. Dr.Web代理服务器 279
12.1.1. 远程设置代理服务器 282
12.2. NAP Validator 285
索引 288

第一章、导言

1.1. 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/。

1.2. 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、Dr.Web Enterprise Security Suite

2.1. 关于产品

Dr.Web Enterprise Security Suite用于组织和管理可靠的统一保护系统，为包括移动设备和员工家用电脑在内的公司局域网提供全面的反病毒保护。

安装有能够交互作用的Dr.Web Enterprise Security Suite组件的所有计算机和移动设备构成统一的*反病毒网络*。

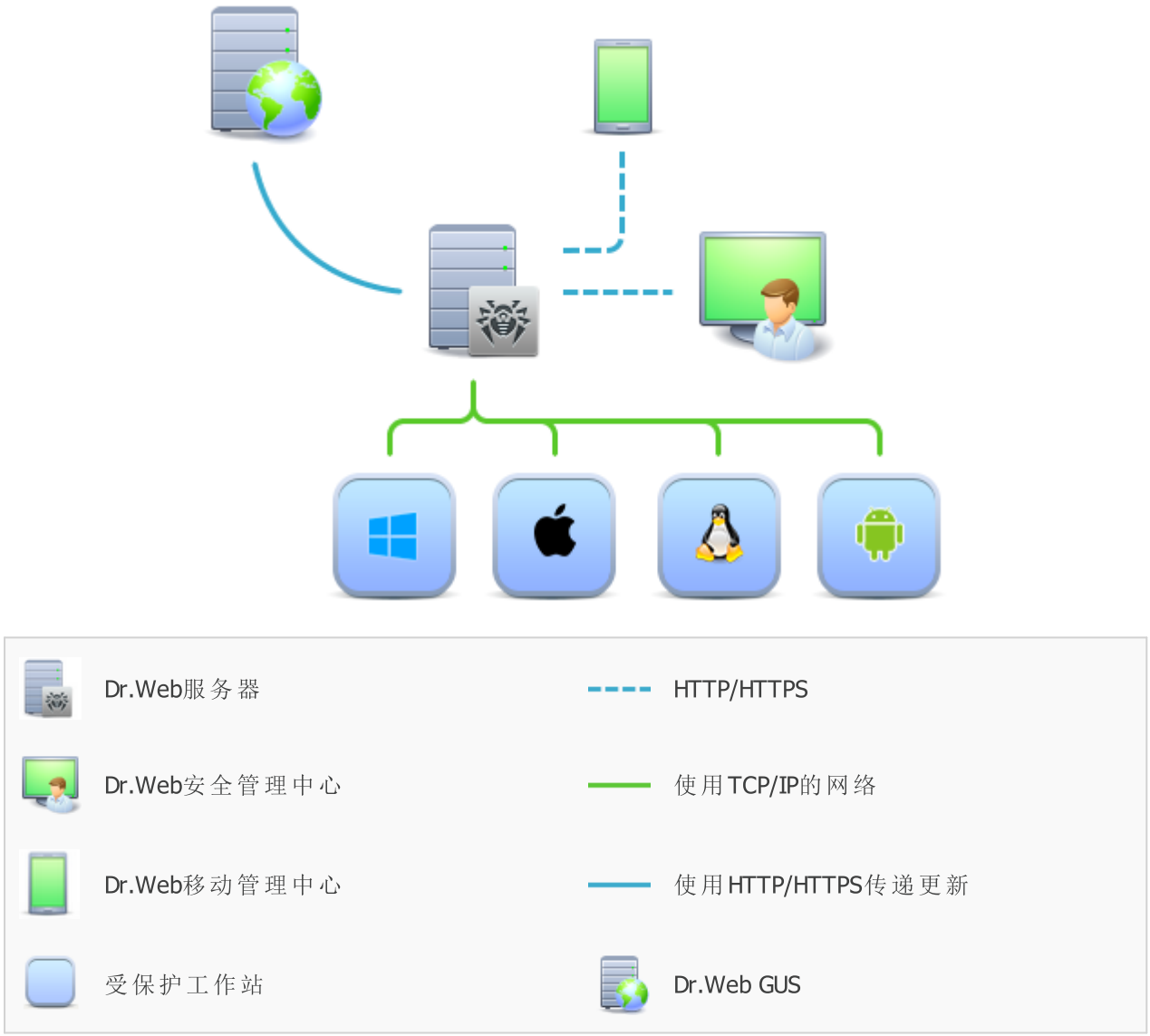


图**1-1.**反病毒网络逻辑结构

Dr.Web Enterprise Security Suite反病毒网络为*服务器-客户端*结构。其组件安装到用户和管理员的电脑和移动设备，以及在局域网执行服务器功能的计算机。反病毒网络组件使用TCP/IP协议相互交换信息。 既可通过局域网，也可通过互联网将反病毒软件包安装到受保护工作站（并在安装后对其进行管理）。

统一保护服务器

统一保护服务器（以下简称Dr.Web服务器）安装于反病毒网络中的任何一台电脑，而且不一定要安装的在局域网执行服务器功能的计算机。对电脑的基本系统要求参见系统要求。

服务器软件支持多平台，可使用以下操作系统的计算机作为统一保护服务器：

- OS Windows，
- UNIX家族操作系统（Linux、FreeBSD）。

统一保护服务器保存用于受保护计算机各种操作系统的反病毒软件包、病毒库、反病毒软件包的更新以及用户密钥和受保护计算机软件包设置。统一保护服务器通过互联网从全球更新系统服务器获取反病毒组件和病毒库更新并将更新分发至受保护工作站。

可使用由多个统一保护服务器组成的集群管理反病毒网络中的受保护工作站。

统一保护服务器支持重要数据（数据库、配置文件等）备份功能。

统一保护服务器记录统一的反病毒网络事件日志。

统一数据库

统一数据库连接统一保护服务器，保存反病毒网络事件统计数据、服务器本身的设置、受保护工作站参数和安装于受保护工作站的反病毒组件的参数。

可使用以下类型的数据库：

内设数据库。是统一管理服务器内置的数据库SQLite3。

外设数据库。 内置驱动程序可理解以下数据库：

- MySQL,
- Oracle,
- PostgreSQL （包括Postgres Pro）、
- ODBC驱动程序：用于连接其它数据库，如Microsoft SQL Server/Microsoft SQL Server Express.

可使用任意一种能够满足需要的数据库。选择时应遵循对数据库的要求，如：可用于相应规模的反病毒网络；数据库软件使用特点；数据库本身的管理功能以及企业具体要求和标准。

统一保护管理中心

统一保护管理中心和统一保护服务器一起自动安装，是Web界面，通过编辑服务器设置以及保存于服务器和受保护计算机上的受保护计算机设置来对统一保护服务器和反病毒网络进行管理。

管理中心可在任何一台能够与统一保护服务器建立网络连接的计算机上打开。几乎所有操作系统下都可使用管理中心，可支持其所有功能的浏览器为：

- Windows Internet Explorer，
- Microsoft Edge，
- Mozilla Firefox，
- Google Chrome。

可能方案参见系统要求。

统一保护管理中心具有以下功能：

- 便于将反病毒软件安装到受保护工作站，包括：预先在网络中搜索计算机后远程安装到工作站；创建带有独有识别码和统一保护服务器连接参数的软件版本，以简化管理员进行反病毒软件的安装或让用户能够将反病毒软件自行安装到工作站。
- 利用组机制简化对反病毒网络工作站的管理 （详见第七章、工作站的综合管理）。
- 对工作站上的反病毒软件包进行统一管理，包括删除OS Windows 工作站上的部分组件或整个反病毒软件；设置反病毒软件包组件运行参数；为工作站用户指定设置和管理受保护工作站的权限 （详见第八章、工作站的管理）。
- 对工作站反病毒扫描进行统一管理，包括：按照日程或管理员从管理中心发出的指令远程启动反病毒扫描； 统一设置反病毒扫描参数，这些参数会发送到工作站并以指定参数启动本地扫描（详见工作站反病毒扫描）。
- 获取受保护工作站状态统计信息、病毒统计信息、已安装的反病毒软件包状态、已启用的反病毒组件状态以及受保护工作站硬软件配置列表（详见查看工作站统计信息）。
- 具备灵活的统一保护服务器和反病毒网络管理系统，可限定不同管理员的权限，且管理员可通过外部身份验证系统Active Directory、LDAP、RADIUS和PAM 登录（详见第六章、反病毒网络管理员）。
- 管理工作站反病毒保护授权，可利用分支系统为工作站、工作站组指定授权，还可在多服务器反病毒网络中的不同统一保护服务器间传递授权（详见授权管理器）。
- 利用设置选项可为统一保护服务器和其组件灵活指定配置，包括：指定维护日程；接入用户进程；灵活设置更新系统，从GUS获取反病毒网络所有组件的更新并将其传播到工作站；设置管理员反病毒网络事件通知系统，可选择不同方式送达通知；设置服务器间连接，管理多服务器反病毒网络的配置（详见第十章、Dr.Web服务器设置）。

将反病毒保护安装至工作站的详细信息参见**安装手册**。

Dr.Web安全管理中心的一个组成部分是与统一保护服务器一同自动安装的Web服务器。Web服务器的主要任务是保证运行管理中心页面和客户端网络连接。

统一保护移动管理中心

用于iOS和Android移动设备的单独组件是移动管理中心（*Dr.Web Mobile Control Center*）。使用此应用程序对设备的基本要求参见系统要求。

移动管理中心利用加密协议连接统一保护服务器，运行需使用反病毒网络管理员账户。移动管理中心具备 管理中心的基本功能：

1. 管理反病毒网络工作站上安装的反病毒组件：
   - 在所选工作站或所选组的所有工作站启动快速扫描或完全扫描；
   - 设置Dr.Web扫描仪侦测到恶意对象时的反应；
   - 查看和管理所选工作站或所选组的所有工作站上隔离区文件。
2. 收集反病毒网络状态信息：
   - 在Dr.Web服务器注册的工作站数量，其当前状态（在线/离线）；
   - 受保护工作站感染统计信息。
3. 管理工作站和工作站组：
   - 查看设置；
   - 查看和管理反病毒软件包组件；

- 删除工作站和组；
- 向工作站发送自定义内容的通知；
- 重启OS Windows工作站；
- 将工作站和组添加至快速访问收藏项。

4. 通过Push及时对话系统查看并管理反病毒网络重要事件通知：
   - 在Dr.Web服务器显示所有通知；
   - 指定对通知事件的反应；
   - 按照指定的过滤参数搜索通知；
   - 删除通知；
   - 排除因自动删除丢失通知。
5. 管理等待与Dr.Web服务器连接的新工作站：
   - 批准访问；
   - 拒绝工作站。
6. 管理反病毒软件包更新出错的工作站：
   - 显示出错的工作站；
   - 在出错的工作站更新组件。
7. 管理Dr.Web服务器库：
   - 查看库中产品状态；
   - 启动从Dr.Web全球更新系统进行库更新。
8. 按名称、地址和ID在反病毒网络查找工作站和工作站组。

可从管理中心下载Dr.Web Mobile Control或直接在应用商店App Store和Google Play下载。

保护网络中的工作站

在网络中的受保护工作站和移动设备安装管理模块 （客户端）和用于相应操作系统的反病毒软件包。

软件支持多平台，可对以下操作系统的计算机和移动设备进行反病毒保护：

- OS Windows，
- UNIX家族操作系统，
- macOS，
- OS Android。

受保护工作站可以是用户电脑，也可以是局域网中的服务器，支持对Microsoft Outlook邮件系统的反病毒保护。

管理模块定期从统一保护服务器下载反病毒组件和病毒库更新，并向统一保护服务器发送受保护计算机上的病毒事件信息。

如统一保护服务器无法访问，可直接通过互联网从全球更新系统更新受保护工作站上的病毒库。

分别为不同操作系统的工作站提供的保护功能见下。

OS Windows工作站

反病毒扫描

按照用户调用或日程对计算机进行扫描。还可从管理中心远程启动工作站扫描，包括检查是否存在Rootkit。

文件监视器

实时模式下对文件系统进行不间断检查，检查所有启动的进程，以及在硬盘创建的文件和在移动设备打开的文件。

邮件监视器

使用邮件客户端时检查所有进出邮件。

还可进行垃圾邮件过滤（如授权允许使用这一功能）。

Web 监视器

检查所有使用HTTP协议对网站的访问。消除HTTP流量存在的威胁（如获取和发送的文件中存在的威胁），限制访问可疑的资源和错误资源 。

办公控制

控制对本地资源和网络资源的访问，包括控制对网站的访问。可监控重要文件的完整性，防止无意更改或病毒感染，禁止员工访问不需要的信息。

防火墙

保护计算机免于未经授权的外部访问，防止重要信息通过互联网泄露。控制互联网连接和数据传输，在数据包和应用程序层面阻止可疑的连接。

隔离区

将恶意对象和可疑对象隔离到专门的文件夹。

自我保护

保护Dr.Web Enterprise Security Suite文件和目录，防止未经授权进行删除、被用户无意间删除修改或被恶意软件修改。启用自我保护时只允许Dr.Web进程访问Dr.Web Enterprise Security Suite的文件和目录。

预防性保护

预防潜在危险。监控对操作系统重要对象的访问，监控驱动程序的加载以及自启动软件和系统服务的运行，并跟踪已启动进程，如发现病毒活动则阻断进程。

应用程序监控

对工作站所有进程的活动进行监控，可让反病毒网络管理员调整受保护工作站上的应用是否允许使用或禁止使用。

UNIX家族操作系统工作站

反病毒扫描

扫描引擎。执行数据（文件内容、磁盘设备启动记录、来自Dr.Web for UNIX其他组件的数据）的反病毒扫描。安排扫描次序。对可清除的威胁进行清除。

反病毒扫描、管理隔离区

文件系统对象扫描组件和隔离区管理器。接受来自Dr.Web for UNIX其他组件的文件扫描任务。按照日程巡视文件系统目录，将文件提交给扫描引擎进行扫描。删除已感染文件，隔离文件或从隔离区还原文件、管理隔离区目录。保证缓存保存的是已检查文件和已侦测到的威胁注册表的最新信息。

供所有检查文件需对象的组件使用，如SpIDer Guard（for Linux、SMB、NSS）。

扫描Web流量

ICAP服务器，对申请和经代理服务器的HTTP流量进行分析。阻断已感染文件的传输，阻止访问不良Web资源和系统管理员列入黑名单的网络节点。

用于GNU/Linux系统的文件监视器

Linux文件系统监视器。以背景模式运行，监控GNU/Linux文件系统中执行的文件操作（如创建文件，打开、关闭和启动文件）。向文件扫描组件申请对新创建文件和内容更改的文件以及软件启动时的执行文件进行扫描。

用于Samba目录的文件监视器

Samba共享文件监视器。以背景模式运行，监控文件系统中对划分给SMB服务器文件库Samba的目录的操作（如创建文，打开、关闭文件，只读和写入操作）。向文件扫描组件申请对新创建文件和内容更改的文件进行扫描。

NSS文件监视器

NSS卷（Novell Storage Services）监视器。以背景模式运行，监控文件系统指定节点的NSS卷中的操作（如创建文件，打开、关闭文件以及写入操作）。将新创建文件和内容更改的文件发送给文件扫描组件进行扫描。

检查网络连接

对网络流量和URL进行检查的组件。负责检查从网络加载到本地节点和从本地节点上传到外网的数据是否存在威胁，阻止访问不良Web资源和系统管理员列入黑名单的网络节点。

邮件监视器

对邮件进行检查的组件。分析邮件协议通知、解析电子邮件以备检查是否含有威胁。有两种运行模式：

1. 邮件服务器（Sendmail, Postfix等等）过滤器，利用Milter、Spamd或Rspamd接口接入。
2. 透明代理邮件协议（SMTP, POP3, IMAP）。这种模式下使用SpIDer Gate。

macOS工作站

反病毒扫描

按照用户调用或日程对计算机进行扫描。还可从管理中心远程启动工作站扫描。

文件监视器

实时模式下对文件系统进行不间断检查，检查所有启动的进程，以及在硬盘创建的文件和在移动设备打开的文件。

Web 监视器

检查所有使用http协议对网站的访问。消除http流量存在的威胁（如获取和发送的文件中存在的威胁），阻止访问可疑的资源和错误资源。

隔离区

将恶意对象和可疑对象隔离到专门的文件夹。

OS Android 移动设备

反病毒扫描

按照用户调用或日程对移动设备进行扫描。还可从管理中心远程启动工作站扫描。

文件监视器

实时模式下对文件系统进行不间断检查。在试图将文件保存到移动设备时对其进行检查。

来电和短信过滤

过滤SMS短信和电话可阻止不需要接听的电话和接收的短信，如广告短信和来自未知号码的电话和短信。

防盗器

在移动设备丢失或被窃时确定其所在地或及时上锁。

限制访问互联网资源

URL过滤器使移动设备用户远离不良网路资源。

防火墙

保护移动设备免于未经授权的外部访问，防止重要信息通过互联网泄露。控制互联网连接和数据传输，在数据包和应用程序层面阻止可疑的连接。

帮助解决安全问题

对移动设备安全状态进行诊断和发现，消除发现的问题和漏洞。

控制应用程序的启动

禁止在移动设备启动管理员允许启动列表中不包含的应用程序。

保证反病毒网络各组件间的连接

可利用以下功能保证反病毒网络各组件间的连接稳定、安全：

Dr.Web代理服务器

代理服务器可选择性加入反病毒网络。代理服务器的主要任务是在无法建立直接连接的情况下保证Dr.Web服务器与受保护工作站的连接。

通过代理服务器可将反病毒网络中的任意一台计算机作为：

- 更新转发中心，这样可以降低Dr.Web服务器的网络负载和Dr.Web服务器与代理服务器的连接负载，利用缓存功能还可缩短受保护工作站获取更新的时间。

- 将受保护工作站病毒事件转发给Dr.Web服务器的转发中心，这样也可以降低网络负载，并在Dr.Web服务器和受保护工作站处于不同的网络的情况下保证数据的传输。

流量压缩

可使用专门算法压缩反病毒网络组件间传输数据，以便将网络流量降至最低。

流量加密

可反病毒网络组件间传输数据时进行加密，已提高保护等级。

补充功能

NAP Validator

NAP Validator是补充组件，用于使用Microsoft Network Access Protection（NAP）技术检查受保护工作站软件运行能力。通过执行对网络工作站运行能力的要求达到提高安全级别的目的。

库加载器

Dr.Web库加载器是补充工具，用于从全球更新系统加载Dr.Web Enterprise Security Suite产品。可用于加载Dr.Web Enterprise Security Suite产品更新，并在获取更新后将其转至没有接通互联网的Dr.Web服务器。

Dr.Web扫描服务器

Dr.Web扫描服务器为单独组件，用于在虚拟环境运行。扫描服务器安装于一个虚拟机，处理来自其他虚拟机的反病毒扫描申请。

2.2. 系统要求

Dr.Web Enterprise Security Suite的安装和正常运行要求：

- 反病毒网络计算机应能够访问Dr.Web服务器或Dr.Web代理服务器。
- 为保证反病毒组件间的互动，计算机上应打开以下端口：

端口号	协议	连接	用途
2193	TCP	• Dr.Web服务器和代理服务器进出流量 • 代理端出港流量	用于连接反病毒组件与Dr.Web服务器和服务器间连接。 包括使用代理服务器与客户端建立连接。
	UDP	进港，出港	用于运行网络搜索仪。
139, 445	TCP	• Dr.Web服务器出港流量 • 代理端进港流量	用于远程安装Dr.Web代理端
	UDP	进港，出港	

端口号	协议	连接	用途
9080	HTTP	• Dr.Web服务器进港流量 • 管理中心所在服务器出港流量	用于运行Dr.Web安全管理中心。
9081	HTTPS		
10101	TCP		用于运行Dr.Web服务器远程诊断工具。
80	HTTP	出港	用于从GUS获取更新。
443	HTTPS		

Dr.Web服务器

组件	系统要求
处理器	CPU支持SSE2，频率1.3 GHz或更高。
内存	• 最低要求：1GB。 • 建议使用：2GB以上。
硬盘空间	• Dr.Web服务器软件需要至少50GB设置以及补充空间用于保存临时文件，如在Dr.Web服务器安装目录子目录 `var\installers-cache`保存代理端个人安装包（每个约17MB）。 • 数据库占用不高于5GB。 • 不论Dr.Web服务器安装于何处，OS Windows系统盘或UNIX家族操作系统的`/var/tmp`（如临时文件区有改动，则为另一临时文件区）： ▫ Dr.Web服务器安装要求空间不小于4.3GB用于启动安装程序和解压临时文件； ▫ Dr.Web服务器运行需要系统盘有可用空间用于保存临时文件和运行文件，这与数据库大小和库设置无关。
操作系统	• Windows。 • Linux，需具备`glibc` 2.13或更高版本。 • FreeBSD11.3或更高版本。 支持的操作系统的完整列表见附录中的附录A。
支持虚拟环境和云环境	支持在符合上述系统要求的操作系统于虚拟环境和云环境下运行，包括： • VMware； • Hyper-V； • Xen； • KVM。
其它	使用数据库Oracle要求具备库`Linux kernel AIO access library`（`libaio`）。

Dr.Web服务器不可安装到文件系统不支持符号链接的逻辑盘，比如FAT文件系统。

可在管理中心的**管理→工具**部分加载的管理工具应在符合Dr.Web服务器系统要求的计算机启动。

Dr.Web代理服务器

组件	系统要求
处理器	CPU支持SSE2，频率1.3 GHz或更高。
内存	不少于1GB。
硬盘空间	不少于1GB。
操作系统	• Windows。 • Linux，需具备glibc 2.13或更高版本。 • FreeBSD11.3或更高版本。 支持的操作系统的完整列表与**附录**中的附录A中Dr.Web服务器支持的操作系统列表相同。

Dr.Web安全管理中心

a) 网络浏览器：

- Internet Explorer 11；
- Microsoft Edge 0.10或更高版本；
- Mozilla Firefox 44或更高版本；
- Google Chrome 49或更高版本；
- Opera最新版本；
- Safar最新版本。

使用网络浏览器Windows Internet Explorer时许注意：

- 在启用**Enhanced Security Configuration for Windows Internet Explorer**模式的网络浏览器Windows Internet Explorer不能保证管理中心完全正常运行。
- 如安装Dr.Web服务器的计算机名称中含有符号"_"（下划线），则不可在浏览器中利用管理中心操作Dr.Web服务器。这种情况下必须使用另一种网络浏览器。
- 正常运行管理中心需要在打开管理中心的浏览器的可信任网址中添加安装有Dr.Web服务器的计算机的IP地址和/或DNS名称。
- 在带有平铺界面的OS Windows 8和OS Windows Server 2012通过**开始**菜单正常打开管理中心需对网络浏览器进行以下设置：**浏览器属性→所有程序→打开Internet Explorer**勾选**总是以经典视窗在Internet Explorer**。
- 在浏览器Windows Internet Explorer使用加密协议https正常运行管理中心必须安装浏览器的所有最新更新。
- 浏览器Windows Internet Explorer使用兼容模式无法正常运行管理中心。

b) 运行管理中心建议使用的屏幕分辨率为1280x1024 px。

Dr.Web移动管理中心

安装应用的操作系统不同，系统要求也有所区别：

操作系统	系统要求	
	操作系统版本	设备
iOS	iOS 9及更高版本	Apple iPhone Apple iPad
Android	Android 4.1–11.0	–

NAP Validator

服务器端：

- OS Windows Server 2008。

代理端：

- OS Windows XP SP3、OS Windows Vista SP2、OS Windows Server 2008 SP2。



NAP Validator的系统要求与Dr.Web代理端系统要求相同。具体要求取决于反病毒解决方案安装于何种操作系统（支持的操作系统完整列表见文件附录中的附录A. 支持的操作系统版本完整列表）：

Dr.Web代理端和反病毒软件包

系统要求取决于反病毒解决方案安装于何种操作系统（支持的操作系统完整列表见附录中的附录A. 支持的操作系统版本完整列表）：

- OS Windows：

组件	系统要求
处理器	CPU频率1GHz或更高。
可用内存	不少于512MB。
硬盘可用空间	不少于1.5GB用于执行文件以及用于运行日志和临时文件的补充空间。
其它	1. 正常显示**Windows**操作系统**Dr.Web**代理端帮助需使用Windows Internet Explorer 6.0或更高版本。 2. 插件Dr.Web for Microsoft Outlook要求具备从Microsoft Office安装的Microsoft Outlook客户端： • Outlook 2000； • Outlook 2002；

组件	系统要求
	• Outlook 2003； • Outlook 2007； • Outlook 2010 SP2； • Outlook 2013； • Outlook 2016； • Outlook 2019。

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。

- Linux家族操作系统：

组件	系统要求
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）； • ARM64； • E2K (Elbrus)
可用内存	不少于512MB（推荐为1GB或更多）。
硬盘可用空间	所按照产品目录所在卷可用磁盘空间不少于2GB。

- macOS、OS Android：配置要求与操作系统要求相符。

支持Dr.Web代理端在符合上述系统要求的操作系统于虚拟环境和云环境下运行，包括：

- VMware；
- Hyper-V；
- Xen；
- KVM。

在Dr.Web Enterprise Security Suite管理的反病毒网络工作站不应使用其他反病毒软件（包括其他版本的Dr.Web反病毒软件产品）。

Dr.Web扫描服务器

组件	系统要求
管理程序	VMware、Hyper-V、Xen、KVM

组件	系统要求
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(RAM)	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。

2.3. 供货方案

软件**Dr.Web Enterprise Security Suite**根据所选**Dr.Web**服务器操作系统供货：

1. UNIX家族操作系统：
   - `drweb-13.00.0-<编号>-esuite-server-<操作系统版本>.tar.gz.run`
     Dr.Web服务器软件
   - `drweb-reploader-<操作系统>-<位数>`
     Dr.Web库加载器控制台版本。

2. OS Windows：
   - `drweb-13.00.0-<编号>-esuite-server-<操作系统版本>.exe`
     Dr.Web服务器软件
   - `drweb-13.0.0-<编号>-esuite-agent-full-windows.exe`
     Dr.Web代理端完整安装程序。
   - `drweb-reploader-windows-<位数>.exe`
     Dr.Web库加载器控制台版本。
   - `drweb-reploader-gui-windows-<位数>.exe`
     Dr.Web库加载器图形版本。

Dr.Web服务器软件包含以下组件：

- 支持相应操作系统的Dr.Web服务器软件；
- Dr.Web服务器安全数据；
- Dr.Web安全管理中心软件；
- 用于Windows操作系统工作站的Dr.Web代理端软件和反病毒软件包；

- 用于Windows操作系统的Dr.Web代理端更新模块；
- 用于Windows操作系统的Dr.Web反垃圾邮件；
- 用于Windows操作系统的Dr.Web病毒库、反病毒专家内置过滤器数据库和反垃圾邮件数据库；
- 帮助文档；
- Doctor Web公司新闻。

除软件外还提供序列号，注册序列号后您会获得授权密钥文件。

安装Dr.Web服务器后可从全球更新系统将以下Dr.Web企业产品加载到库中：

- 安装到OS UNIX（包括局域网服务器）、Android、macOS受保护工作站的产品；
- Dr.Web扫描服务器；
- Dr.Web for IBM Lotus Domino；
- Dr.Web for Microsoft Exchange Server；
- Dr.Web代理服务器；
- 用于Windows操作系统的Dr.Web代理端完整安装程序；
- 用于Active Directory的Dr.Web代理端；
- Active Directory架构更改工具；
- Active Directory对象参数更改工具；
- NAP Validator。

第三章、授权

使用反病毒解决方案Dr.Web Enterprise Security Suite需要具备授权。

Dr.Web Enterprise Security Suite反病毒解决方案使用授权的组成和价格取决于受保护工作站的数量，包括在Dr.Web Enterprise Security Suite网络中作为受保护工作站的服务器数量。

在购买Dr.Web Enterprise Security Suite解决方案时一定要告知授权销售商这一信息。所使用的Dr.Web服务器数量不影响授权价格。

授权密钥文件

Dr.Web Enterprise Security Suite使用权通过授权密钥文件来控制。

授权密钥文件格式使用电子签名防止文件被修改。编辑文件会使密钥文件失效。为防止密钥文件意外受损，请不要对其进行修改和/或在文件编辑器查看文件后进行保存。

授权密钥文件以zip压缩文档形式提供，包含一个或几个用于受保护工作站的密钥文件。

用户可利用以下一种方式获取授权密钥文件：

- 授权密钥文件有可能包含于购买的Dr.Web Enterprise Security Suite反病毒软件中，如果制作软件包时纳入了授权密钥文件。但一般产品随附的只是序列号。
- 用户在Doctor Web公司地址为https://products.drweb.com/register/v4/网页（如产品所附注册卡中未标明其它地址）注册序列号后，授权密钥文件通过电子邮箱发送给用户。 请登录指定网页，填写客户信息表并输入序列号（序列号印于注册卡）。密钥文件压缩文档会发送至您所指定是邮箱。也可从此网站直接加载密钥文件。
- 授权密钥文件可通过单独载体提供。

建议在授权密钥文件到期前将其保存，以便在重新安装或恢复软件组件时使用。如丢失密钥文件可在指定网址重复注册操作，重新获取授权密钥文件；重新注册时需输入与第一次注册相同的序列号和相同的客户信息；只可更改邮箱地址。更改邮箱地址后授权密钥文件会发送至新地址。

可使用试用密钥文件了解反病毒软件功能。试用密钥可保证主要反病毒组件的所有功能的运行，但使用期有限。获取试用密钥文件需在网页https://download.drweb.com/demoreq/biz/填写申请表。我公司会对申请进行审核。批准后授权密钥文件压缩文档会发送到用户指定的邮箱。

如何在安装过程中使用授权密钥文件详见**安装手册**中的安装Dr.Web服务器。

如何在已部署的反病毒网络使用授权密钥文件详见授权管理器。

3.1. 授权特点

1. Dr.Web服务器不需要授权。

Dr.Web服务器UUID在之前的Dr.Web Enterprise Security Suite版本中保存在Dr.Web服务器密钥，现在保存于Dr.Web服务器配置文件（自版本10起）。

- 安装新Dr.Web服务器时生成新的UUID。
- 升级较早版本的Dr.Web服务器时，UUID会自动从上一版本的配置文件中提取并写入新安装的Dr.Web服务器的配置文件。

升级Dr.Web服务器群集时，负责更新数据库的Dr.Web服务器获得授权密钥，其他Dr.Web服务器需手动添加密钥。

2. 授权密钥只用于受保护工作站。可为工作站指定密钥，也可为工作站组指定密钥：密钥将适用于所有从这一工作站组继承密钥的工作站。为反病毒网络的所有没有密钥自身设置的工作站指定密钥文件的方法是将密钥设为**Everyone**组的密钥。
3. 授权密钥文件在安装Dr.Web服务器时指定（参见**安装手册**的安装Dr.Web服务器）。

   安装Dr.Web服务器可以在没有授权密钥的情况下进行。可在安装后本地添加密钥，或利用服务器间连接添加。
4. 利用服务器间连接可将保存于此Dr.Web服务器的密钥中的可选量授权分发给Dr.Web邻居服务器在指定的时间段内使用。
5. 可使用多个不同的密钥，如有效期不同或受保护工作站反病毒组件不同。每一授权密钥可同时指定给多个授权对象（组或工作站）。可为同一授权对象同时指定多个授权密钥。
6. 为同一对象指定多个密钥时需注意：
   a) 如同一对象的多个密钥中允许使用的反病毒组件有所区别，则只允许使用不同密钥都允许的组件。例如，如果为某工作站指定的一个密钥支持反垃圾邮件，而另一个密钥不支持反垃圾邮件，则组中工作站不能安装反垃圾邮件。
   b) 对象授权设置取决于为此对象指定的所有密钥。如果密钥有效期不同，则在有效期最短的密钥到期后需要手动替换或删除到期的密钥。如果到期的密钥对可安装的反病毒组件有限制，则必须在**可安装组件**部分调整对象的设置。
   c) 对象授权数量根据为此对象指定的所有密钥来计算。还需考虑可通过服务器间连接将授权转发给Dr.Web邻居服务器（参见第4节）。这时需要从总授权量中减去已转发给Dr.Web邻居服务器的授权数量。

管理授权密钥需使用授权管理器。

在授权管理器指定授权密钥时该密钥的所有信息会保存在数据库。

3.2. 通过服务器间连接分发授权

多Dr.Web服务器反病毒网络可在Dr.Web服务器间分配一定数量、一定期限的授权。

在Dr.Web服务器间传递授权需按照设置Dr.Web服务器间连接设置服务器间连接。

分发授权适用以下连接方案：

- Dr.Web主服务器给出授权，Dr.Web子服务器接收，按照分发授权连接设置（不可更改）。

- 在同级Dr.Web服务器间传递授权。这时给出授权的Dr.Web服务器的连接设置的**授权**中应勾选**发送**，而接收授权的Dr.Web服务器应勾选**接收**。

设置给出授权的**Dr.Web**服务器的操作

1. 打开将向Dr.Web邻居服务器分发授权的反病毒网络Dr.Web服务器的管理中心。
2. 在管理中心主菜单选择**管理**一项，在控制菜单选择**授权管理器**。
3. 如授权密钥尚未添加，需按照授权管理器部分的介绍添加密钥。密钥中的授权数量应符合此Dr.Web服务器和所有将接收授权的Dr.Web服务器下属的工作站总数。

   一般只需要一个授权密钥，其包含的授权在所有Dr.Web服务器间分配。
4. 计算从此密钥要分发给Dr.Web邻居服务器多少授权。需要注意，Dr.Web邻居服务器也可能将部分授权分发给其他Dr.Web服务器。这时从Dr.Web主服务器给出的是授权总量，之后依次分发。还要注意在分发期结束前和分发出去的授权返还之前Dr.Web主服务器无法使用这些授权。
5. 按照授权管理器部分的介绍设置将授权分发到Dr.Web邻居服务器。

   在**授权结束日期**指定分发出去的授权的有效期。此期限可与本授权相同或短于本授权期限。到期后所有授权将从Dr.Web邻居服务器撤回，重新归入本授权密钥可用授权列表。必要时可随时按照授权管理器部分的介绍编辑这一期限。
6. 如需可更改授权分发设置。操作是打开**Dr.Web服务器配置**。
7. 在**授权**标签给出以下针对给出授权的Dr.Web服务器的设置：
   - **给出的密钥自动延期期限**——从此Dr.Web服务器密钥给出的密钥的有效期。到期后对给出的密钥进行相同期限的自动延期。授权管理器第5步给出的授权分发期内会重复自动延期。
     此机制用于保证如Dr.Web子服务器关闭而无法返还密钥时授权会返还给Dr.Web主服务器。
   - **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。授权同步用于确认Dr.Web主服务器给出的授权于Dr.Web子服务器接收的授权数量相符。此机制用于查找错误和偷换分发授权的情况。
   - **创建报告的周期**——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。此设置在Dr.Web主服务器给出，但Dr.Web子服务器同样按照此设置发送报告。
   - **计算活跃工作站的周期**——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。此设置在Dr.Web主服务器给出，但Dr.Web子服务器同样按照此设置发送报告。
8. 保存更改后重启Dr.Web服务器。

设置接收授权的**Dr.Web**服务器的操作

1. 打开从Dr.Web邻居服务器接收授权的反病毒网络Dr.Web服务器的管理中心：
2. 如需可更改授权分发设置。操作是打开**Dr.Web服务器配置**。
3. 在**接收授权预延期时间**指定**接收授权预延期时间**——从Dr.Web邻居服务器接收的授权自动延期期限剩余时间，从这一时间开始此Dr.Web服务器申请对这些授权进行自动预延期。

   这一设置的使用取决于配置Dr.Web服务器间连接时在**连接参数**选择的连接类型（见设置Dr.Web服务器间连接）：

- 周期性连接类型：如连接设置中指定的连接周期大于在分发授权的Dr.Web服务器指定的**给出的密钥自动延期期限**，则在**给出的密钥自动延期期限**到期前进行这些授权的自动延期。
- 不间断连接类型：不应用此设置。

4. 保存更改后重启Dr.Web服务器。

3.3. 自动更新授权

Dr.Web Enterprise Security Suite授权可自动更新。

自动更新授权意味着：

- 授权密钥到期时软件会自动将其更换为事先购买的授权。
- 自动更新针对为其购买了延期的授权密钥。
- 用于自动更新的授权密钥在需延期的授权密钥到期前保存在Doctor Web公司服务器。

自动更新授权流程

以下情况启动自动更新授权流程：

- 管理员在管理中心授权管理器任务面板点击**检查是否有更新并替换授权密钥**。
- 执行Dr.Web服务器日程中的**库更新**任务。任务设置中应勾选了**更新授权密钥**。

> 自动更新授权密钥的前提是更新的授权属于此Dr.Web服务器：最初通过手动添加或自动更新获取。从Dr.Web邻居服务器利用服务器间连接获取的授权无法执行自动更新授权密钥。

自动更新授权流程分以下步骤：

1. 检查Doctor Web服务器（GUS）上是否有授权密钥。
2. 从GUS将授权密钥加载到Dr.Web服务器，之后添加到数据库和授权管理器。
3. 将心授权密钥分发搭配前一密钥的对象。

解决于各步骤结果流程可在任一步骤正常结束。

执行自动更新后可能出现的结果：

1. *GUS上不存在授权没有可用于自动更新。*

   不进行任何操作。
2. *GUS上有授权密钥可用于自动更新。当前授权组件有别于新授权（新授权中缺少当前授权中的某些组件）和/或新授权数量少于当前授权。*

   从Doctor Web公司服务器加载新授权并添加到授权管理器和Dr.Web服务器数据库，但不向授权对象分发。这种情况下必须手动进行分发。

   向管理员发送**无法自动更新授权密钥**的通知。通知中包含无法自动分发密钥的具体原因。
3. *GUS上有授权密钥可用于自动更新。当前授权组件与新授权相符或新授权组件多于当前授权所有组件，新密钥授权数量等于或多于当前密钥中的授权。*

从Doctor Web公司服务器加载新授权并添加到授权管理器和Dr.Web服务器数据库，分发到分发原授权的对象，包括Dr.Web邻居服务器。

当所有Dr.Web子服务器都不再使用原授权后原授权会被删除。如果自动更新时Dr.Web子服务器处于关机状态，则原授权会一直保留到Dr.Web子服务器连线。

以下情况下原授权将保留到手动删除：

- 如果无法向Dr.Web子服务器分发自动更新时获取的授权（Dr.Web服务器永久离线）。
- 如果Dr.Web子服务器使用的协议版本不支持自动更新功能。这种情况下授权将转给Dr.Web子服务器，但不会分发。

向管理员发送**已自动更新授权密钥**的通知。更新通知将从每一个分发到新授权的Dr.Web服务器发出。

所有向管理员发送的通知可在 **管理→通知配置** 进行设置。

发送每个通知后执行用户钩子**自动更新授权密钥**。

手动更新授权

如果购买授权密钥是用于自动更新当前密钥，则不需要手动将新密钥添加到授权管理器。根据情况（上述第二种情况）则需要手动将授权分发到授权对象。

但如果在执行自动更新授权密钥流程之前通过授权管理器添加了按照第三种情况可以自动更新的新授权（见上），则执行任务时只分发新授权密钥。这时可能出现的情况：

a) 新授权密钥已手动分发到所有分发有原密钥（被更新的密钥）的对象。这时执行更新任务时不会进行任何更改。

b) 新授权密钥没有手动分发到所有分发有原密钥（被更新的密钥）的对象。这时执行更新任务时新密钥会分发到还没有接到更新的所有剩余对象。

   如果新授权密钥分发到了原密钥不包含的对象，则执行更新任务时薪密钥也会分发到这些对象。这时可能出现的情况：

   - 授权数量满足所有授权对象：包括原授权包含的对象和手动指定新授权的对象。出现这种情况是条件是新密钥授权数量超出原密钥授权数量。这种情况下执行更新任务时不会进行任何更改。
   - 授权数量不能满足所有原授权包含的对象，因为授权已手动指定给了其他对象。对于剩余的对象不进行更新，但原授权仍会被删除，对象没有授权。出现可用授权这些对象会获得新的授权密钥。这时的操作取决于被授权对象的类型：
     - 如果新密钥中授权数量没有满足本Dr.Web服务器下属工作站，则在工作站每次连接Dr.Web服务器时都会检查是否有可用授权。如工作站连接时发现有可用授权，则会提供给这一工作站。
     - 如果新密钥中授权数量没有满足Dr.Web邻居服务器的需求，则每分钟自动检查一次是否有可用授权。如发现有可用授权，则会提供给Dr.Web邻居服务器。

授权密钥文件

自动更新过程中需注意授权密钥文件的以下特点：

- 执行自动更新时需新授权从Doctor Web公司服务器加载，新授权信息保存在Dr.Web服务器数据库并体现在授权管理器。这时并不创建授权密钥文件。
- 获取授权密钥文件需使用**管理→授权管理器→导出密钥**选项。授权密钥文件也可以在执行用户钩子**自动更新密钥文件**时获得。
- 删除授权时信息从授权管理器和Dr.Web服务器数据库删除，但授权密钥文件会保留在Dr.Web服务器目录。

第四章、开始运行

4.1. 反病毒网络的部署

部署反病毒网络简要说明：

1. 规划反病毒网络结构，使所有应受保护的计算机和移动设备纳入网络。

   选择将作为Dr.Web服务器的计算机。反病毒网络中可以设置几个Dr.Web服务器。这种网络的部署特点详见多台Dr.Web服务器网络的特点。

   Dr.Web服务器可以安装于任何一台计算机，而不只是执行局域网服务器功能的计算机。对计算机的基本要求见系统要求一节。

   在所有受保护计算机，包括局域网服务器，安装同一版本的Dr.Web代理端。区别在于Dr.Web服务器设置中指定有不同的可安装反病毒组件列表。

   安装Dr.Web服务器要求对相应计算机进行一次性访问（实机操作或使用程序远程管理和启用工具）。反病毒工作站的软件一般是由用户自行本地安装，但也可以通过局域网利用Dr.Web安全管理中心进行远程安装。安装完成以后，所有操作都可以由反病毒网络管理员从其计算机进行，不需要访问Dr.Web服务器或工作站。

   在进行反病毒网络规划时建议列出所有有权访问管理中心的责任人，并根据其可以执行的功能设定不同的角色。必须为每一角色创建管理员组。将具体管理员的账户移至相应管理员组就可以实现管理员与角色的对接。如需可以将管理员组（角色）分出级别，设置为多级别体系，可以为每一级别分别设置管理员访问权限。

   Dr.Web代理端在Windows Server 2016以及更高版本的Windows服务器操作系统上正常运行必须利用组策略手动停用Windows Defender。

4.2. 网络连接设置

概述

连接Dr.Web服务器的客户端有：

- Dr.Web代理端。
- Dr.Web代理端安装程序。
- Dr.Web邻居服务器。
- Dr.Web代理服务器。

连接总是由客户端主动建立。

客户端连接Dr.Web服务器可以通过以下方式：

1. 通过直接连接。

   这种方式有很多优点，但并不是在任何情况下都是最佳方式（还有些情况下这种方式不可取）。

2. 通过Dr.Web服务器发现服务。

   默认情况下（如果未直接指定其他方式）客户端使用的正是这一服务。

   如果有可能会需要重新设置整个系统，例如需要将 Dr.Web服务器转至另一台计算机或者有必要改变安装有Dr.Web服务器的计算机的IP地址时，需要使用这种连接方式。

3. 使用SRV协议。

   利用这种方式可以按照计算机名称搜索Dr.Web服务器和 / 或基于DNS服务器SRV记录的Dr.Web服务器服务。

设置反病毒网络Dr.Web Enterprise Security Suite使用直接连接时可以关闭Dr.Web服务器发现服务。关闭服务时传输描述（**管理** → **Dr.Web服务器配置** → **网络** → 传输）中的Multicast组一栏应为空。

防火墙设置

反病毒网络各组件正常互动要求在所有反病毒网络中的计算机上打开反病毒网络组件所使用的所有端口和接口。

安装Dr.Web服务器时安装程序会自动将Dr.Web服务器的端口和接口添加到OS Windows防火墙排除项。

如除了OS Windows操作系统内设防火墙外还使用其它防火墙，网络管理员应手动进行相应设置。

4.2.1. 直接连接

Dr.Web服务器设置

在Dr.Web服务器设置中应指定接收TCP连接所应监听的地址（参见**附录**中的附录E. 网络地址特点）。

此参数需在Dr.Web服务器设置中的**管理** → **Dr.Web服务器配置** → **网络** → 传输 → 地址一栏指定。

默认情况下Dr.Web服务器设定"监听"的是：

- **地址**：为空表示使用安装Dr.Web服务器的计算机的*所有网络接口*。
- **端口**：2193——使用端口2193。



端口2193为Dr.Web Enterprise Management Service在IANA注册的端口。

Dr.Web服务器只要"监听"一个所有客户端已知的TCP端口即可保证 Dr.Web Enterprise Security Suite整个系统的正常运行。

Dr.Web代理端设置

安装代理端可以在以下参数明确指明Dr.Web服务器地址（启动Dr.Web服务器的计算机的IP地址或DNS名称）：

```
drwinst /server <Dr.Web服务器地址>
```

安装代理端时建议使用事先已在DNS注册的Dr.Web服务器名称。这样做如果将来Dr.Web服务器安装到另一台计算机，可以简化反病毒网络设置过程。

默认情况下没有给出参数的`drwinst`命令会扫描网络搜索Dr.Web服务器并尝试将代理端与在网络中搜索到的第一个Dr.Web服务器建立连接（使用Dr.Web服务器发现服务的*Multicasting*模式）。

这样代理端将在安装过程中得知Dr.Web服务器地址。

之后可在代理端设置中手动更改Dr.Web服务器地址。

4.2.2. Dr.Web服务器搜索服务

使用这一连接方式时客户端事先不知道Dr.Web服务器地址。在每次建立连接前都在网络中搜索Dr.Web服务器。进行搜索时客户端向网络发送广播申请，等待Dr.Web服务器回应其地址。接到回应后与Dr.Web服务器建立连接。

这时Dr.Web服务器应对网络进行*监听*，以便获取客户端的连接申请。

设置这种连接方式有几种途径。重要的是为客户端指定的Dr.Web服务器搜索方式要与Dr.Web服务器回应部分的设置相符。

Dr.Web Enterprise Security Suite默认情况下使用的是*Multicast over UDP*模式：

1. Dr.Web服务器在组播组中使用Dr.Web服务器设置中的地址注册。
2. 代理端在搜索Dr.Web服务器时第1中指定的组播地址向网络发出组播请求。

默认情况下为Dr.Web服务器进行的监听的地址为设定`udp/231.0.0.1:2193`（与直接连接相似）。

此参数需在管理中心设置指定：**管理** → **Dr.Web服务器配置** →**网络**→ **传输** → **TCP/IP**。不给出设置则使用默认地址。

4.2.3. 使用SRV协议

OS Windows客户端支持客户端网络协议*SRV*（网络格式列于**附录**中的附录E. 网络地址特点）。

实现通过**SRV**记录连接**Dr.Web**服务器的方式：

1. 安装Dr.Web服务器时在Active Directory域名注册，安装程序将相应的SRV记录载入DNS服务器。

   SRV记录按照RFC2782载入DNS服务器（见 https://datatracker.ietf.org/doc/html/rfc2782）。

2. 申请连接Dr.Web服务器时用户通过`srv`提交申请。

   例如：启动代理端安装程序：

   - 明指服务名称`myservice`：
     ```
     drwinst /server "srv/myservice"
     ```
   - 不明指服务名称。这时将在SRV记录搜索默认名称`drwcs`：
     ```
     drwinst /server "srv/"
     ```

3. 客户端使用SRV协议功能连接Dr.Web服务器。

   如Dr.Web服务器未指明，默认使用的服务名称为`drwcs`。

4.3. 保障安全连接

4.3.1. 流量加密和压缩

加密模式用于保证非安全通道传输的数据的安全，避免重要信息泄露以及加载到受保护工作站的软件被替换。

Dr.Web Enterprise Security Suite反病毒网络使用以下加密手段：

- 电子数字签名（国标 R 34.10-2001）。
- 非对称加密（VKO GOST R 34.10-2001 — RFC 4357）。
- 对称加密（国标28147-89）。
- 哈希加密功能（国标 R 34.11-94）。

Dr.Web Enterprise Security Suite反病毒网络可加密Dr.Web服务器与客户端之间的流量，包括：

- Dr.Web代理端。
- Dr.Web代理端安装程序。
- Dr.Web邻居服务器。
- Dr.Web代理服务器。

由于组件间特别是Dr.Web服务器之间可能会出现很大的流量，反病毒网络可设置对此流量进行压缩。设置压缩策略和不同客户端间的设置兼容性与加密设置相同。

设置兼容策略

加密和压缩使用策略在反病毒网络每一组件分别设置，同时其它组件的设置应与Dr.Web服务器的设置相符。

在设置Dr.Web服务器和客户端加密和压缩策略时应注意有些设置会产生冲突，导致Dr.Web服务器和客户端失去连接。

表 4-1 中何种设置下Dr.Web服务器与客户端间的连接为加密/压缩（**+**），何种设置下为不加密/不压缩（**–**），哪些设置会产生冲突（**错误**）。

表4-1. 加密和压缩策略设置兼容

	Dr.Web服务器设置		
客户端设置	是	可能	否
是	+	+	错误
可能	+	+	–
否	错误	–	–



如果计算机性能接近所安装组件的最低要求，流量加密会显著增加其计算负荷。如果没有额外安全保证的需求，可以不使用加密模式。

取消加密时应依次将Dr.Web服务器和组件转为**可能**模式，以免客户端-服务器间发生冲突。

使用压缩会减小流量，但相比加密，要占用更多内存，会更大程度地增加计算机的计算负荷。

通过Dr.Web代理服务器连接

客户端通过Dr.Web代理服务器连接Dr.Web服务器时必须考虑所有三个节点的加密和压缩设置。这时：

- Dr.Web服务器和代理服务器（这时作为客户端）的设置一个按照表4-1匹配。
- 客户端和代理服务器（这时作为Dr.Web服务器）的设置一个按照表4-1匹配。

是否可以通过代理服务器取决于Dr.Web服务器和客户端相应版本所支持的加密技术：

- 如果Dr.Web服务器和客户端支持13.0版本中使用的TLS加密，则只需执行上面描述的条件就可以建立连接。
- 如果有一个组件不支持TLS加密：在Dr.Web服务器和/或客户端安装的是使用国标加密的版本10或更早版本，则需要按照表4-2进行补充检查。

表4-2. 使用代理服务器时加密和压缩策略设置兼容

与客户端的连接设置	与Dr.Web服务器的连接设置			
	无	压缩	加密	全部
无	一般模式	一般模式	错误	错误
压缩	一般模式	一般模式	错误	错误
加密	错误	错误	透明模式	错误
全部	错误	错误	错误	透明模式

标志说明

与Dr.Web服务器和客户端的连接设置	
无	压缩和加密都不支持。
压缩	只支持压缩。
加密	只支持加密。
全部	压缩和加密都支持。
连接结果	
一般模式	已建立的连接意味着以一般模式运行，处理指令并进行缓存。
透明模式	已建立的连接意味着以透明模式运行，不处理指令，不进行缓存。选择最低的加密协议版本：如果有一个客户端（Dr.Web服务器或代理端）为版本13，而另一个是版本10，则建立版本10中使用的加密。
错误	代理服务器与Dr.Web服务器和客户端的连接将中断

这样，如果Dr.Web服务器和代理端版本不同：一个是版本13，另一个是版本10和更早，则通过代理服务器建立连接应用以下限制：

- 在代理服务器进行缓存只能是在与Dr.Web服务器和客户端的连接都不使用加密的情况下。
- 使用加密只能是与Dr.Web服务器和客户端的连接都使用加密且压缩参数相同（两个连接都有压缩或都没有压缩）。

在Dr.Web服务器设置加密和压缩

设置Dr.Web服务器压缩和加密的操作

1. 在管理中心主菜单选择**管理**。
2. 在打开的窗口选择控制菜单中的**Dr.Web服务器配置**。

3. 在**网络** → **传输**标签的**加密**和**压缩**下拉列表中选择以下一种方案：
   - **是**——同所有客户端间的流量都必须加密（或压缩）（如安装Dr.Web服务器时未另行设置，此方案为加密默认设置）。
   - **可能**——如客户端的设置不禁止加密（或压缩），则与这些组件间的流量将进行加密（或压缩）。
   - **否** ——不支持加密（或压缩）（如安装Dr.Web服务器时未另行设置，此方案为压缩默认设置）。



在Dr.Web服务器端设置加密和压缩时许注意将和此Dr.Web服务器连接的客户端的特点。并非所有客户端都支持流量加和压缩。

在Dr.Web代理服务器设置加密和压缩

统一为代理服务器设置加密和压缩



如果代理服务器未连接Dr.Web服务器，因而不能远程进行设置管理。需按照**安装手册**中的将代理服务器连接到Dr.Web服务器的描述设置连接。

1. 为代理服务器的Dr.Web控制服务器打开管理中心。
2. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击需编辑其设置的代理服务器的名称，如果代理服务器从基组继承设置，则点击基组名称。
3. 在打开的控制菜单选择**Dr.Web代理服务器**。打开设置选项。
4. 打开**监听**标签。
5. 在**与客户端的连接参数**的**加密**和**压缩**下拉列表中选择代理服务器和其所服务的客户端间流量的加密和压缩模式，包括代理端和代理端安装程序。
6. 在**在与Dr.Web服务器的连接参数**指定向其重定向流量的Dr.Web服务器列表。在表中选择需要的Dr.Web服务器后点击这一部分工具面板的按钮，编辑与所选Dr.Web服务器的连接参数。在打开的窗口的**加密**和**压缩**下拉列表选择代理服务器与所选服务器间流量的加密和压缩模式。
7. 点击**保存**按钮保存指定的设置。

为代理服务器本地设置加密和压缩



如果代理服务器连接Dr.Web控制服务器，可进行远程设置，则将按照从Dr.Web服务器获取的设置重写代理服务器的配置文件。这种情况下必须从Dr.Web服务器远程指定设置或停用从这一Dr.Web服务器接收配置。

配置文件`drwcsd-proxy.conf`描述见**附录**的附录G4。

1. 在安装代理服务器的电脑端口配置文件`drwcsd-proxy.conf`。
2. 编辑与客户端和Dr.Web服务器连接的压缩和加密设置。
3. 重启代理服务器：

- OS Windows：
  - 如果代理服务器是作为OS Windows服务启动，则利用系统工具重启服务。
  - 如果代理服务器是在控制台启动，重启需点击CTRL+BREAK。
- UNIX家族操作系统：
  - 将信号SIGHUP发送给代理服务器守护进程。
  - 需执行以下命令：

  OS Linux：

  ```
  /etc/init.d/dwcp_proxy restart
  ```

  OS FreeBSD：

  ```
  /usr/local/etc/rc.d/dwcp_proxy restart
  ```

为工作站设置加密和压缩

统一为工作站设置加密和压缩

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。
2. 在打开的控制菜单选择**连接参数**。
3. 在**常规**标签**压缩模式**和**加密模式**下拉列表中选择以下一种方案：
   - **是**——一定加密（或压缩）与Dr.Web服务器间的流量。
   - **可能**——如Dr.Web服务器的设置不禁止加密（或压缩），则与Dr.Web服务器的流量将进行加密（或压缩）。
   - **否**——不支持加密（或压缩）。
4. 点击**保存**。
5. 设置传至工作站后立即生效。如更改设置时工作站离线，则更改会在工作站再次连接Dr.Web服务器时立即传至工作站。

可在安装代理端时设置加密和压缩：

- 从管理中心进行远程安装时直接在**网络安装**的设置中指定加密和压缩模式。
- 进行本地安装时图形安装程序不可更改加密和压缩模式，但可在启动安装程序时利用命令行参数进行设置（参见**附录**中的H1. 网络安装程序）。

完成代理端安装后不可在工作站本地更改加密和压缩模式。默认模式设置为**可能**（如安装过程中未另行指定），也就是说是否加密和压缩取决于Dr.Web服务器端的设置。但可以通过管理中心更改代理端的设置（见上）。

用于Android操作系统的Dr.Web反病毒软件

反病毒软件Dr.Web for Android不支持加密，也不支持压缩。如果Dr.Web服务器端或代理服务器端（如通过代理服务器建立连接）压缩和/或加密的设置为**是**，将无法连接服务器。

用于Linux操作系统的Dr.Web反病毒软件

安装反病毒软件是不可更改加密和压缩模式。默认模式为**可能**。

完成反病毒软件安装后只可通过控制台模式更改工作站的加密和压缩设置。控制台模式介绍和相应的命令行参数见**Dr.Web for Linux用户手册**。

也可通过管理中心更改工作站设置（见上）。

用于macOS的Dr.Web反病毒软件

完成代理端安装后不可再工作站本地更改加密和压缩模式。默认模式设置为**可能**，也就是说是否加密和压缩取决于Dr.Web服务器端的设置。

也可通过管理中心更改工作站设置（见上）。

4.3.2. 安全连接保障工具

安装Dr.Web服务器时创建以下保障反病毒网络各组件间安全连接的工具：

1. **Dr.Web服务器加密私钥**`drwcsd.pri`。

   保存在Dr.Web服务器，不分发给反病毒网络其他组件。

   如丢失私钥需手动恢复反病毒网络各组件间的连接（创建所有密钥和证书并将其分发到网络所有组件）。

   以下情况使用私钥：

   a) 创建公钥和证书。

   加密公钥和证书在安装Dr.Web服务器过程中自动从私钥创建。私钥可以是新创建的，也可以为已有私钥（如安装上一Dr.Web服务器的私钥）可随时使用服务器工具`drwsign`创建加密密钥和证书（参见 **附录** 中的 H7.1.数字密钥和证书生成工具）。

   公钥和证书介绍见下。

   b) Dr.Web服务器验证。

   远程客户端进行Dr.Web服务器验证使用的是电子数字签名（每次连接进行一次）。

   Dr.Web服务器使用私钥为通知进行数字签名后将通知发送给客户端。客户端利用证书检查通知签名。

   c) 数据解密。

   Dr.Web服务器和客户端间流量加密时客户端发送给Dr.Web服务器的数据利用私钥在服务器解密。

2. **Dr.Web服务器加密公钥**`*.pub`。

   反病毒网络所有组件均可访问。公钥从私钥创建（见上）。从同一私钥每次生成的公钥相同。

   从Dr.Web服务器版本11开始公钥用于连接老版本的客户端。其他功能由证书取代，证书中包含加密公钥。

3. **Dr.Web服务器证书**`drwcsd-certificate.pem`。

   反病毒网络所有组件均可访问。证书中包含加密公钥。证书从私钥创建（见上）。从同一私钥每次生成的新的证书。

   连接Dr.Web服务器的客户端与具体证书对应，因此如某客户端丢失证书，则只有当网络中还有另一组件也使用同一证书的情况下才有可能找回证书：可从Dr.Web服务器或另一客户端将证书复制到丢失证书的客户端。

   以下情况使用证书：

   a) Dr.Web服务器验证。

   远程客户端进行Dr.Web服务器验证使用的是电子数字签名（每次连接进行一次）。

   Dr.Web服务器使用私钥为通知进行数字签名后将通知发送给客户端。客户端利用证书检查通知签名（具体是利用证书中包含的公钥）。之前的Dr.Web服务器版本是直接利用公钥。

   要求客户端具备来自其要连接的Dr.Web服务器的一个或几个可信任证书。

   b) 数据解密。

   Dr.Web服务器和客户端间流量加密时由客户端利用公钥对数据进行加密。

   c) 实现Dr.Web服务器与远程客户端之间的TLS对话。

   d) 代理服务器验证。

   远程客户端进行代理服务器验证使用的是电子数字签名（每次连接进行一次）。

   代理服务器使用Dr.Web服务器私钥和证书为自己的证书签名。信任Dr.Web服务器证书的客户端会自动信任使用这一证书签名的证书。

4. **Web服务器私钥。**

   保存在Dr.Web服务器，不分发给反病毒网络其他组件。详细介绍见下。

5. **Web服务器证书。**

   反病毒网络所有组件均可访问。

   用于实现Web服务器与浏览器之间的TLS对话（按照HTTPS）。

   以Web服务器私钥为基础安装Dr.Web服务器时生成自签名证书，由于此证书不是知名证书中心发布，因此浏览器不会接受。

   要使用受保护的连接（HTTPS），需执行以下一种操作：

   - 将自签名证书添加到所有工作站和打开管理中心的浏览器的可信任证书或排除项。
   - 获取由知名证书中心发布的证书。

4.3.3. 将客户端连接到Dr.Web服务器

客户端连接到Dr.Web服务器要求客户端必须具备Dr.Web服务器证书，不论Dr.Web服务器和客户端直接的流量是否加密。

可连接Dr.Web服务器的客户端有：

- **Dr.Web代理端。**

  连接Dr.Web服务器以便在统一管理模式下运行代理端要求工作站具备来自代理端连接的Dr.Web服务器的一个或几个可信任证书。

  安装时使用的证书以及通过统一设置从Dr.Web服务器获得的证书处于注册表，但不使用证书文件本身。

  可以利用命令行参数将唯一一份证书文件添加到代理端安装目录（而非注册表）和证书总表。使用这一证书在统一设置出现错误时也可连接到Dr.Web服务器。

  没有证书或证书无效时代理端无法连接到Dr.Web服务器，但会继续运行，并可以移动模式更新，如允许工作站在此模式下运行。

- **Dr.Web代理端安装程序。**

  在工作站安装代理端时所选安装文件应同时具备Dr.Web服务器证书。

  启动在管理中心创建的安装包时，安装包包含证书，不需要另行指定证书文件。

  安装代理端时证书数据记录到注册表，之后不再使用证书文件本身。

  没有证书或证书无效时安装程序不能安装代理端（包括所有类型代理端安装文件）。

- **Dr.Web邻居服务器。**

  设置版本11 或更高版本的Dr.Web邻居服务器间连接时必须在每一Dr.Web服务器指定其连接的Dr.Web服务器的证书（参见中的设置Dr.Web服务器间连接）。

  任何一个证书不存在或无效都会导致无法建立服务器间连接。

- **Dr.Web代理服务器。**

  代理服务器连接Dr.Web服务器并可通过管理中心进行远程配置要求安装代理服务器的工作站上有证书。这时代理服务器还支持加密。

  没有证书的情况下代理服务器会继续运行，但无法进行远程管理，也不支持加密和缓存。



原来使用公钥的老版本反病毒网络正常更新为使用证书的新版本不需要进行任何其他操作。

不建议将版本11的Dr.Web服务器的代理端连接版本10的Dr.Web服务器，反之亦然。

4.4. Dr.Web Enterprise Security Suite与Active Directory的集成

如果受保护的局域网中使用Active Directory，可此服务与Dr.Web Enterprise Security Suite集成。



下面介绍的所有方法各自独立，可单独使用，也可结合使用。

Dr.Web Enterprise Security Suite与Active Directory的集成基于以下方法：

1. 在Active Directory域名注册Dr.Web服务器，以便使用SRV协议访问Dr.Web服务器

安装Dr.Web服务器时可以利用安装器在Active Directory域中注册Dr.Web服务器。在DNS服务器注册过程中会创建对应Dr.Web服务器的SRV记录。之后客户端可通过此SRV记录连接Dr.Web服务器。

详见安装手册OS Windows下Dr.Web服务器的安装和使用SRV协议。

2. 将反病毒网络结构与Active Directory域同步

可设置反病毒网络结构与Active Directory域中工作站自动同步。此时Active Directory计算机容器转变为反病毒网络工作站组。

操作是在Dr.Web服务器日程启用任务与**Active Directory**同步。管理员可利用Dr.Web服务器任务计划器自行创建此任务。

详见Dr.Web服务器日程设置。

3. Active Directory用户作为管理员在Dr.Web服务器进行身份验证

可以使用Active Directory账户在Dr.Web服务器进行身份验证后管理反病毒网络。可使用以下一种方式：

- LDAP/AD身份验证。适用于所有支持的操作系统的Dr.Web服务器。通过管理中心按照相应Active Directory属性为用户设置Dr.Web服务器访问权限。不需直接访问域控制器和Active Directory设备，不需在Active Directory端进行设置。
- Microsoft Active Directory。仅适用于纳入目的域的Windows操作系统Dr.Web服务器。直接在Active Directory设备设置有Dr.Web服务器访问权限的用户和用户组。需利用补充工具进行初始设置。供货软件包含数据包`drweb-13.00.0-<编号>-esuite-modify-ad-schema-<操作系统版本>.exe` 和 `drweb-13.00.0-<编号>-esuite-aduac-<操作系统版本>.msi`，还包含于**Dr.Web**企业产品Dr.Web服务器库。

选择哪种方式取决于Dr.Web服务器操作系统和有访问权限的用户的设置方法。

详见管理员身份验证。

4. 在Active Directory域工作站远程安装Dr.Web代理端

可在Active Directory域工作站远程安装Dr.Web代理端。操作是：

a) 借助用于Active Directory的专门代理端安装器在目标共享资源进行管理员安装。数据包`drweb-13.00.0-<编号>-esuite-agent-activedirectory.msi`包含于**Dr.Web**企业产品Dr.Web服务器库。

b) 设置Active Directory相应策略，以便将数据包自动安装到域内工作站。

详见安装手册中的使用Active Directory服务安装Dr.Web代理端。

5. 在Active Directory域搜索工作站

可利用网络搜索已在Active Directory域中搜索工作站。搜索是可以确认找到的工作站是否已安装有Dr.Web，如未安装，则通过管理中心远程安装代理端。

可将此方法与第4部分介绍的利用Active Directory策略自动安装数据包的方法一同使用。

详见的网络搜索仪。

6. 在**Active Directory**域搜索用户

可在Active Directory搜索用户并为其创建用户模式，提供办公控制和应用程序监控的更多设置。

详见**Windows**工作站管理手册。

第五章、反病毒网络组件及其接口

5.1. Dr.Web服务器

以Dr.Web Enterprise Security Suite为基础部署的反病毒网络中应至少设有一个Dr.Web服务器。

为提高反病毒网络的可靠性和高效性，也为均衡负载起见，Dr.Web Enterprise Security Suite可以部署在使用多台Dr.Web服务器的反病毒网络。在这种情况下服务器软件同时安装到几台计算机。

Dr.Web服务器是常驻内存的服务。Dr.Web服务器软件支持多种操作系统（支持的操作系统的完整列表见附录中的附录A）。

主要功能

Dr.Web服务器具备以下功能：

- 在所选计算机或计算机组进行反病毒软件包安装初始化，
- 查询每一受保护计算机上安装的反病毒软件包版本号，以及病毒库创建日期和版本号，
- 更新统一安装目录内容和更新目录，
- 更新受保护计算机上的病毒库和反病毒软件包执行文件，以及反病毒网络组件的执行文件。

收集反病毒网络状态信息

Dr.Web服务器收集受保护计算机上安装的软件（Dr.Web代理端，详细介绍见下）发送来的反病毒软件包运行信息并建立日志。在常规事件日志（数据库）中进行记录。小规模网络（不超过200–300台计算机）记录常规事件日志可使用内置数据库。大网络建议使用外设数据库。

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

一般事件日志记录的信息包括：

- 受保护计算机上反病毒软件包的版本，
- 工作站反病毒软件的安装和更新日期，以及软件版本，

- 病毒库更新日期，以及病毒库版本，
- 受保护计算机上操作系统的版本、处理器类型、操作系统系统目录的位置等信息，
- 反病毒软件包配置和运行模式，
- 病毒事件信息，包括侦测出的计算机病毒名称、侦测日期、采取的操作和清除结果等信息。

Dr.Web服务器在发生与反病毒网络运行相关的事件时会通知反病毒网络管理员。通知反病毒网络管理员使用电子邮件或Windows操作系统的常规多播工具。如何设置需发出通知的事件以及通知其他设置参见通知设置。

Web服务器

Web服务器是Dr.Web安全管理中心的组成部分，执行以下功能：

- 在管理中心进行管理员身份验证和登录；
- 管理中心页面运行自动化；
- 支持管理中心生成的动态页面；
- 支持与客户端的加密HTTPS连接。

5.1.1. Windows操作系统Dr.Web服务器管理

界面和Dr.Web服务器的管理

通常利用Dr.Web服务器外设界面管理中心来管理Dr.Web服务器。

对Dr.Web服务器进行设置和基本管理的元素，位置在安装Dr.Web服务器时Windows操作系统主菜单程序出现的文件夹**Dr.Web Server**：

- 目录**服务器管理**包含以下指令：
  - **详细日志**——将Dr.Web服务器运行日志详细等级设为**全部**。
  - **开始**——启动Dr.Web服务器服务。
  - **停止**——停止Dr.Web服务器服务。
  - **重启库**——从磁盘重新加载Dr.Web服务器库。
  - **重新加载模板**——重新读取管理员通知模板。
  - **重启**——重启Dr.Web服务器服务。
  - **检查数据库**——开始检查内设数据库。
  - **标准日志**——将Dr.Web服务器运行日志详细等级设为**信息**。



执行指令**详细日志**和**标准日志**后必须重新启动Dr.Web服务器才能应用更改。操作是执行**重新启动**指令。



日志记录的高级设置见管理中心的 日志。

相应的控制台指令参见**附录**中的H3. Dr.Web服务器。

- **Web界面**选项——用于打开管理中心并连接安装于本机的Dr.Web服务器（使用地址 http://localhost:9080）。
- **帮助文档**选项——用于打开HTML格式的管理员手册文档。

Dr.Web服务器目录结构如下：

默认安装目录（安装时刻更改）：`C:\Program Files\DrWeb Server`

- `bin`——Dr.Web服务器执行文件。
- `ds-modules`——已解压的脚本模块。
- `etc`——反病毒网络组件主要配置文件。
- `fonts`——PDF文件字体。
- `var`——此目录包含下列子目录：
  - `backup`——数据库和其它重要数据的备份。
  - `extensions`——用于自动执行指定任务的自定义钩子。
  - `file-cache`——文件缓存。

  - installers-cache——在管理中心创建工作站时缓存代理端个人安装包和组安装包。生成安装包时创建。
  - plugins——插件临时对象。
  - object——管理中心对象缓存。
  - reports——用于生成和保存报告的临时目录。必要时创建。
  - repository——库目录，病毒库、反病毒软件包文件和反病毒网络组件的当前更新都置于此目录。目录中分软件各功能组件子目录，而子目录中再按操作系统区分子目录。以其用户名启动Dr.Web服务器的用户（一般情况下是用户**LocalSystem**）应能够写入这一目录。
  - sessions——管理中心对话。
  - tmp——临时文件。
  - twin-cache——解压后的病毒库，用于兼容更早版本的Dr.Web代理端。还可包含库中其他解压文件，如代理端安装程序。
  - upload——加载由管理中心指定的临时文件的目录。加载大文件时创建。
- vfs——将脚本模块和语言包打包。
- webmin——管理中心元素。
- websockets——用于运行网络套接字的脚本。

备份目录（可更改或删除）：*<安装磁盘>*:\Drweb Backup。



更新文件夹 \var\repository中的内容按照HTTP\HTTPS协议根据为Dr.Web服务器指定的日程自动从更新服务器下载，反病毒网络管理员也可以手动将更新放到此文件夹。

主要配置文件

文件	描述	默认文件夹
agent.key（文件名称可能有区别）	代理端授权密钥	etc
certificate.pem	SSL证书	
database.conf	数据库默认参数设置模板	
download.conf	形成代理端安装包的网络设置	
drwcsd.conf（文件名称可能有区别）	Dr.Web服务器配置文件	
drwcsd.conf.distr	Dr.Web服务器默认参数配置文件模板	
drwcsd.pri	加密私钥	
enterprise.key（文件名称可能有区别）	Dr.Web服务器授权密钥。从较早版本升级时如存在则保存此密钥。安装新的Dr.Web服务器13.0时没有	

文件	描述	默认文件夹
frontdoor.conf	用于Dr.Web服务器远程诊断工具的配置文件	
http-alerter-certs.pem	发送push通知时用于验证主机apple-notify.drweb.com的证书	
private-key.pem	RSA私钥	
yalocator.apikey	插件Yandex.Locator的API密钥	
webmin.conf	管理中心配置文件	
auth-ads.conf	通过Active Directory进行管理员外部身份验证的配置文件	
auth-ldap.conf	通过LDAP进行管理员外部身份验证的配置文件	
auth-ldap-rfc4515.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。	
auth-radius.conf	通过RADIUS进行管理员外部身份验证的配置文件	
database.sqlite	内设数据库	var
*.pub	加密公钥	管理中心的**管理**→**加密密钥**部分

启动和停止Dr.Web服务器

默认情况下Dr.Web服务器在安装后自动启动，之后每次重启操作系统时自动启动。

还可以通过以下方式启动、重启或停止Dr.Web服务器：

- 一般情况：
  - 利用菜单**开始** → **所有程序** → **Dr.Web Server**中的相应命令。
  - 利用OS Windows**控制面板**中**管理**部分的管理工具。
- 通过管理中心停止和重启：
  - 在**管理**部分：重启利用按钮，停止利用按钮。
- 利用从Dr.Web服务器安装目录bin子目录执行的控制台命令（另参见**附录**中的H3. Dr.Web服务器）：
  - `drwcsd start`——启动Dr.Web服务器。
  - `drwcsd restart`——完全重启Dr.Web服务器服务。
  - `drwcsd stop`——正常结束Dr.Web服务器运行。

> 注意！ Dr.Web服务器识别环境变量必须利用服务管理方式或控制台指令重启服务。

5.1.2. UNIX家族操作系统Dr.Web服务器管理

界面和Dr.Web服务器的管理

Dr.Web服务器无内设界面。通常利用Dr.Web服务器外设界面管理中心来管理Dr.Web服务器。

Dr.Web服务器安装目录结构如下：

/opt/drwcs/用于Linux操作系统，/usr/local/drwcs用于FreeBSD操作系统：

- bin——Dr.Web服务器执行文件。
- doc——许可协议。
- ds-modules——已解压的脚本模块。
- fonts——PDF文件字体。
- lib——Dr.Web服务器运行使用的库。
- vfs——将脚本模块和语言包打包。
- webmin——管理中心元素。
- websockets——用于运行网络套接字的脚本。

/var/opt/drwcs/用于Linux操作系统，/var/drwcs用于FreeBSD操作系统：

- backup——数据库和其它重要数据的备份。
- coredump——Dr.Web服务器崩溃转储。出现转储时创建。
- etc——反病毒网络组件主要配置文件。
- extensions——用于自动执行指定任务的自定义钩子。
- installers-cache——在管理中心创建工作站时缓存代理端个人安装包和组安装包。生成安装包时创建。
- file-cache——文件缓存。
- log——Dr.Web服务器日志文件。
- plugins——插件临时对象。
- object——管理中心对象缓存。
- reports——用于生成和保存报告的临时目录。必要时创建。
- repository——更新目录，病毒库、反病毒软件包文件和反病毒网络组件的当前更新都置于此目录。目录中分软件各功能组件子目录，而子目录中再按操作系统区分子目录。以其用户名启动Dr.Web服务器的用户（一般情况下是用户**drwcs**）应能够写入这一目录。
- run——Dr.Web服务器进程ID。
- sessions——管理中心对话。
- tmp——临时文件。
- twin-cache——解压后的病毒库，用于兼容更早版本的Dr.Web代理端。还可包含库中其他解压文件，如代理端安装程序。
- upload——加载由管理中心指定的临时文件的目录。加载大文件时创建。

/etc/opt/drweb.com/用于OS Linux，/usr/local/etc/drweb.com用于OS FreeBSD：

- software/drweb-esuite.remove——用于删除Dr.Web服务器的脚本。
- 可能有补充文件和目录。

/usr/local/etc/rc.d/用于FreeBSD操作系统：

- drwcsd——用于启动和停止Dr.Web服务器的脚本。

/var/tmp/drwcs——删除Dr.Web服务器后的备份。

主要配置文件

文件	描述	默认文件夹
agent.key（文件名称可能有差异）	代理端授权密钥	• OS Linux：/var/opt/drwcs/etc • OS FreeBSD：/var/drwcs/etc
certificate.pem	SSL证书	
common.conf	配置文件（用于某些UNIX家族操作系统）	
database.conf	数据库默认参数设置模板	
download.conf	形成代理端安装包的网络设置	
drwcsd.conf（文件名称可能有区别）	Dr.Web服务器配置文件	
drwcsd.conf.distr	Dr.Web服务器默认参数配置文件模板	
drwcsd.pri	加密私钥	
enterprise.key（文件名称可能有区别）	Dr.Web服务器授权密钥。从较早版本升级时如存在则保存此密钥。安装新的Dr.Web服务器13.0时没有	
frontdoor.conf	用于Dr.Web服务器远程诊断工具的配置文件	
http-alerter-certs.pem	发送push通知时用于验证主机apple-notify.drweb.com的证书	
private-key.pem	RSA私钥	
yalocator.apikey	插件Yandex.Locator的API密钥	
webmin.conf	管理中心配置文件	
auth-ldap.conf	通过LDAP进行管理员外部身份验证的配置文件	
auth-ldap-rfc4515.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。	

文件	描述	默认文件夹
auth-pam.conf	通过PAM进行管理员外部身份验证的配置文件	
auth-radius.conf	通过RADIUS进行管理员外部身份验证的配置文件	
database.sqlite	内设数据库	• OS Linux: /var/opt/drwcs • OS FreeBSD: /var/drwcs
*.pub	加密公钥	管理中心的管理→加密密钥部分

启动和停止Dr.Web服务器

默认情况下Dr.Web服务器在安装后自动启动，之后每次重启操作系统时自动启动。

还可以通过以下方式启动、重启或停止Dr.Web服务器：

- 通过管理中心停止和重启：
  - 在管理部分：重启利用按钮，停止利用按钮。
- 利用相应的控制台指令（另参见附录H3. Dr.Web服务器）：
  - 启动：
    - OS FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd start
      ```
    - OS Linux:
      ```
      # /etc/init.d/drwcsd start
      ```
  - 重新启动：
    - OS FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd restart
      ```
    - OS Linux:
      ```
      # /etc/init.d/drwcsd restart
      ```
  - 停止：
    - OS FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd stop
      ```
    - OS Linux:
      ```
      # /etc/init.d/drwcsd stop
      ```

注意！Dr.Web服务器识别环境变量必须利用控制台指令重启服务。

5.2. 保护工作站

可通过管理中心设置的反病毒组件设置详细说明见**管理员手册**对相应操作系统工作站的管理。

安装有反病毒软件包的受保护计算机，依照其在反病毒网络中的功能，被叫做反病毒网络*工作站*。必须注意的是，就其在局域网中的功能而言，这样的计算机既可能是局域网的工作站，也可能是局域网的服务器。

工作站的反病毒保护是利用支持相应操作系统的Dr.Web反病毒软件包。

反病毒软件包安装到受保护工作站并与Dr.Web服务器连接，每一工作站都列于Dr.Web服务器注册的一个或几个组中（详见系统组和用户组）。工作站和Dr.Web服务器间的信息传输使用局域网协议（TCP/IP版本4或6）。

安装

可利用下列一种方式将反病毒软件包安装到工作站：

1. 本地安装，用户直接在用户计算机或移动设备上进行本地安装，用户和管理员均可执行。
2. 远程安装。远程安装通过管理中心在局域网进行。由反病毒网络管理员执行。不需要用户的参与。

如何将反病毒保护安装至工作站的详细信息参见**安装手册**。

管理

与Dr.Web服务器连接的情况下管理员可管理工作站反病毒软件包的以下功能：

- 利用管理中心对工作站反病毒软件进行统一设置。

  这时管理员可以禁止，也可以允许用户更改工作站反病毒软件设置。
- 设置反病毒扫描和其他在工作站执行的任务日程。
- 获取扫描统计信息以及反病毒专家运行和工作站状态的其他信息。
- 启动和停止反病毒扫描等操作

更新

Dr.Web服务器加载更新并发送至与其连接的代理端。这样就可以自动设置、保持或调整最佳反病毒保护策略，而不受工作站用户计算机熟练程度的影响。

在工作站临时与反病毒网络断开时，工作站反病毒软件会使用本地备份的设置，依然能够对工作站进行反病毒保护（在用户授权有效期内），但不能进行病毒库和软件更新。如允许工作站以*移动模式*运行，在与Dr.Web服务器断开后可直接从GUS服务器获得更新。

工作站移动模式介绍见Dr.Web移动代理端的更新。

5.3. Dr.Web安全管理中心

Dr.Web安全管理中心的功用是对反病毒网络进行整体管理（包括改变网络的组成和结构），对管理反病毒网络的所有组件以及 Dr.Web服务器进行设置。

为了使管理中心能够在网络浏览器Windows Internet Explorer下正常运行，必须在浏览器设置中将管理中心地址添加到可信任区域：**服务 → 浏览属性 → 安全 → 信任的网站**。

为了使管理中心能够在网络浏览器Chrome下正常运行，必须在浏览器设置中开启cookies。

连接Dr.Web服务器

从任何一台与Dr.Web服务器有网络连接的计算机可以使用以下地址登录管理中心：

`http://`*<Dr.Web服务器地址本>*`:9080`

或

`https://`*<Dr.Web服务器地址>*`:9081`

其中*<Dr.Web服务器地址>*为安装有Dr.Web服务器的计算机的IP地址或域名。

使用http连接时端口号为9080，使用https加密连接时端口号为9081。

在身份验证对话窗口输入管理员注册信息。超级管理员默认为：

- 用户名——**admin**。
- 密码：
  - OS Windows下为安装Dr.Web服务器时指定的密码。
  - UNIX家族操作系统下密码是Dr.Web服务器安装过程中自动生成的密码（参见**安装手册**中的OS UNIX下Dr.Web服务器的安装）。

可以找回密码，详见找回管理员密码。

通过https（应用SSL的加密连接）登录时，浏览器会要求确认Dr.Web服务器所使用的证书。要求确认时可能会伴有对证书不信任以及怀疑证书有错误的信息。出现这一信息是由于对浏览器而言为未知证书。加载管理中心需接受此证书。否则将无法加载。

在某些版本的浏览器，如**FireFox 3**或更高版本，通过HTTPS加载时将出现错误，不能加载管理中心。这种情况下需在显示错误的页面选择**将此网站添加到例外列表**一项（在错误通知下方）。添加后就会允许访问管理中心。

Dr.Web安全管理中心

管理中心窗口分为（见图5-1）*标题区*和*工作区*。

主菜单

管理中心主菜单包括以下选项：

- 管理，
- 反病毒网络，
- 搜索栏，
- 登录管理中心所使用的管理员账户名称。还包含于服务器间连接菜单，
- 事件，
- 设置，
- 帮助，
- **退出**按钮用于结束与管理中心的本次对话。

工作区

*工作区为*管理中心的基本功能区。按照执行的操作由两或三面板组成。这时功能面板为自左向右依次排列：

- 控制菜单总是在窗口的左侧，
- 取决于控制菜单选项，会显示一个或两个补充面板。出现两个补充面板时右侧面板显示中间面板元素的属性或设置栏。

界面语言为每一管理员账户单独设定（参见管理员账户管理一节）。

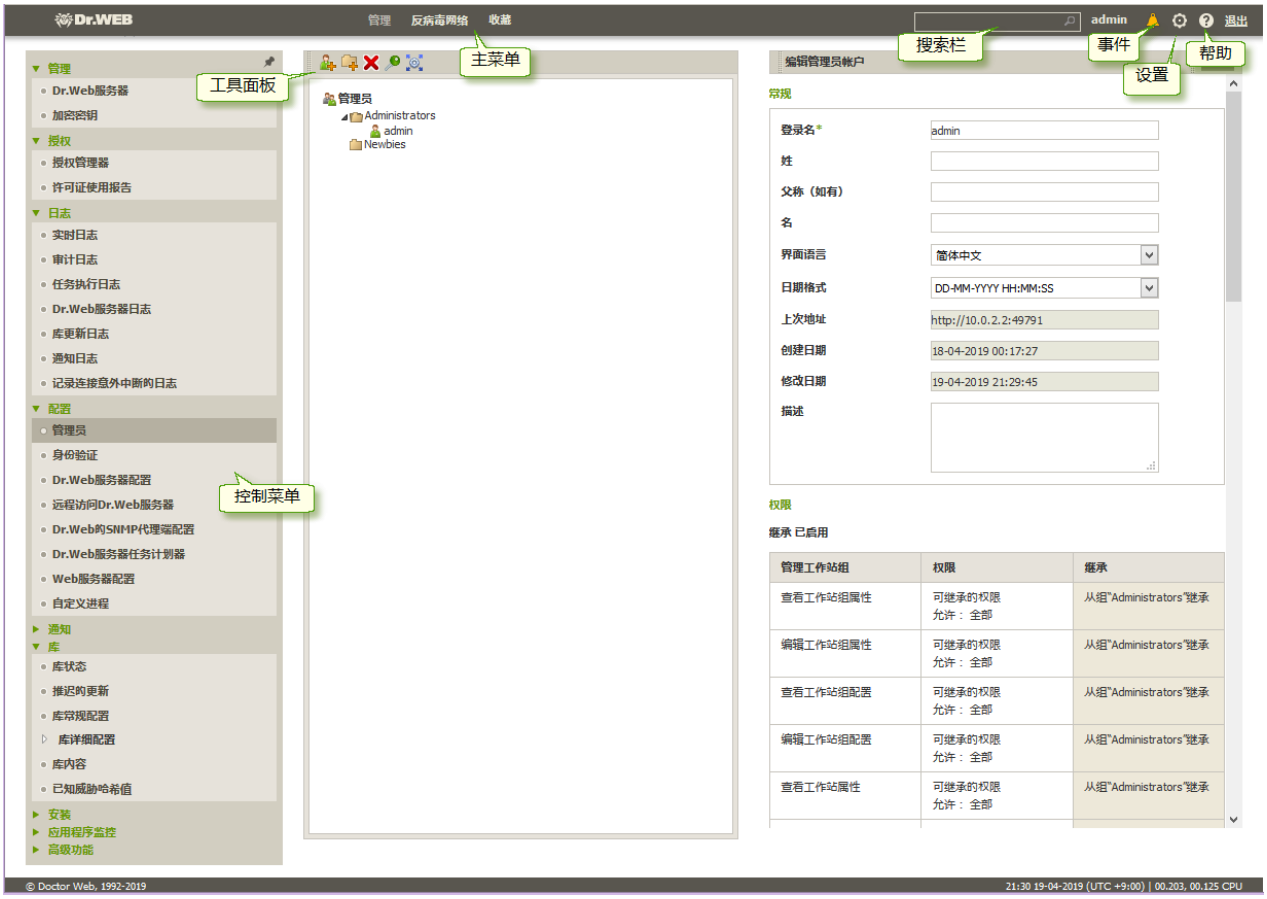


图**5-1. Dr.Web**安全管理中心窗口。点击绿框中的元素转至相应部分

控制菜单

窗口左侧为控制菜单，使用控制菜单可查看、编辑信息。

控制菜单可以收起。这时至显示菜单各部分名称。鼠标移至相应部分时会显示该部分的菜单选项。

管理控制菜单显示需使用右上角的图标：

- **取消菜单固定**——取消菜单固定并以收起模式显示。
- **固定菜单**——固定展开的菜单。

服务器间连接菜单

多服务器反病毒网络部署及服务器间连接设置相关信息见[多台Dr.Web服务器网络特点](#)。

存在与其他Dr.Web服务器的服务器间连接时主菜单添加以下功能用于注册管理员用户名：

- 管理员用户名旁边显示当前Dr.Web服务器名称。
- 点击管理员名称时打开Dr.Web邻居服务器下拉列表。如未指定邻居名称，则显示其识别码。点击邻居后可进行以下两种操作：

- 如邻居设置中指定了管理中心IP地址，则打开Dr.Web邻居服务器管理中心。操作类同工具面板管理邻居的按钮 → 。
- 如未指定Dr.Web邻居服务器的管理中心地址，则打开邻居设置，以便指定IP地址。

5.3.1. 管理

在管理中心主菜单选择**管理**。

控制菜单

窗口左侧为控制菜单，使用控制菜单可查看、编辑本窗口显示的信息。

控制菜单包括以下选项：

1. 管理

- **Dr.Web服务器**——利用此项打开的面板可以查看Dr.Web服务器的基本信息，使用位于面板右上方的按钮 可以重新启动服务器，按钮 停止服务器。如已加载Dr.Web服务器更新，这一部分会出现Dr.Web服务器更新和Dr.Web服务器版本列表，用于更新和备份。
- **加密密钥**——用于导出（本地保存）加密公钥和私钥，以及Dr.Web服务器证书。

2. 授权

- 授权管理器——利用此项可管理授权密钥文件。
- 授权使用报告——包含授权使用信息，包括Dr.Web邻居服务器对授权的使用情况。

3. 日志

- 实时日志——可实时（事件出现时）查看与Dr.Web服务器运行相关的事件和更改。
- 审计日志——用于查看Dr.Web Enterprise Security Suite管理子系统实施的事件和更改。
- **任务执行日志**——Dr.Web服务器上设置的任务列表，标有任务完成情况和说明。
- Dr.Web服务器日志——是Dr.Web服务器运行相关日志列表。
- 库更新日志——为从全球更新系统加载的更新列表，包含更新的产品校检详细信息。
- 通知日志——为管理员发送到反病毒网络工作站的所有文本通知。
- **连接非正常中断日志**——记录Dr.Web服务器与客户端的所有非正常连接中断，包括工作站、代理端安装程序、Dr.Web邻居服务器、代理服务器。

4. 配置

- 管理员——打开反病毒网络管理员账户控制面板。
- 身份验证——打开管理中心管理员认证控制面板。
- Dr.Web服务器配置——打开Dr.Web服务器主要设置面板。
- 远程访问Dr.Web服务器——包含Dr.Web服务器远程诊断工具的连接设置。
- Dr.Web的SNMP代理端配置——打开Dr.Web的SNMP代理端插件连接参数的设置面板。

- Dr.Web 服务器任务计划器——打开Dr.Web服务器任务日程设置面板。
- Web服务器配置——打开Web服务器主要设置面板。
- 自定义钩子——打开自定义钩子设置面板。

5. 通知

- Web控制台通知——用于查看和管理利用**Web控制台**获取的管理员通知。
- 未发送的通知——用于跟踪和管理未能按照**通知配置**发送的管理员通知。
- 通知配置——用于设置关于反病毒网络事件的管理员通知。
- 通知模板——管理员可向工作站发送的自定义文本通知模板列表。

6. 库

- 库状态——用于检查库的状态：库中组件最近一次更新的日期和组件的当前状态。并从GUS更新库。
- 推迟的更新——包含在**库详细配置**中设置为暂时禁止更新的产品列表。
- 库常规配置——打开全球更新系统连接设置和所有产品库更新窗口。
- 库详细配置——用于为库中每一产品分别设置校检更新配置。
- 库内容——用于查看和管理库中文件和文件夹。
- **已知威胁哈希值**——用于按照已知按照已知威胁哈希值公报进行搜索。按哈希值列搜索需点击。
  此选项可以使用的前提是已授权使用已知威胁哈希值公报。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**（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）。

7. 安装

- 网络搜索仪——可以指定网络列表，既可以进行网络扫描以便通过确定计算机状态判断工作站是否安装有反病毒软件，也可以进行最新反病毒软件的安装。
- **网络安装**——可以很方便地将代理端软件安装到具体的工作站（参见**安装手册**中的利用Dr.Web安全管理中心安装Dr.Web代理端）。

8. 应用程序监控

- 可信任的应用程序——安装有应用程序监控的工作站上总是允许启动的应用程序列表（在为工作站指定的模式的设置可选择允许启动的应用列表）。
- 应用程序目录——已安装到工作站的所有应用程序列表。

9. 补充功能

- 数据库管理——用于直接维护Dr.Web服务器使用的数据库。
- Dr.Web服务器统计信息——为当前Dr.Web服务器运行统计信息。
- **SQL控制台**——可执行对Dr.Web服务器使用的数据库的SQL申请。
- **Lua控制台**——可执行Lua脚本，包括直接在控制台输入的脚本，也包括从我家加载的脚本。



有Lua控制台访问权限的管理员可访问Dr.Web服务器目录内的整个文件系统以及安装Dr.Web服务器的计算机的某些系统指令。

禁止对Lua控制台的访问需为相应管理员取消**高级**权限（参见管理员和管理员组）。

- 备份——用于查看和保存Dr.Web服务器重要数据备份。
- 工具——打开运行Dr.Web Enterprise Security Suite所需补充工具加载页面：

5.3.2. 反病毒网络

在管理中心主菜单选择**反病毒网络**一项。

控制菜单

窗口左侧为控制菜单，使用控制菜单可查看、编辑本窗口显示的信息。

控制菜单包括以下选项：

1. 常规
   - 图表
   - 安全识别码
   - 保护组件
   - 隔离区
   - 硬件和软件
   - 已发现的设备
   - 用户对话
   - 处于不活跃状态的工作站
   - 属性
   - 组成员规则（如选择了一个用户组）
   - Dr.Web代理服务器（选择代理服务器或代理服务器组时）
2. 统计信息
3. 配置
   - Dr.Web代理服务器（选择代理服务器或组**Proxies**或其子组时）
   - 权限
   - 任务计划器
   - 可安装组件
   - 连接参数
   - 更新限制
   - 用于**UNIX**操作系统的**Dr.Web**代理端——可设置UNIX家族操作系统工作站威胁侦测统计信息发送周期。

- 用于所选工作站操作系统的反病毒保护组件列表或用于所选组操作系统的反病毒保护组件列表。

> 可通过管理中心设置的反病毒组件设置详细说明见**管理员手册**对相应操作系统工作站的管理。

反病毒网络分层列表

在窗口中央显示的是反病毒网络的分层列表。反病毒网络分层列表显示反病毒网络元素树结构。此结构的节点为组和组中所包含的工作站。

可以对列表中的元素进行以下操作：

- 鼠标左键点击组或工作站的名称可以显示（在窗口左侧）相应元素的控制菜单，在属性面板（在窗口右侧）显示工作站简短信息。
- 鼠标左键点击组的图标可以显示或收起组的内容。
- 鼠标左键点击组的图标可以转至工作站属性。

> 同时选择分层列表中的多个工作站和组请按住CTRL键或SHIFT键使用鼠标选择。

列表中元素的图标取决于元素的类型或状态（见表5-1）。

表5-1. 分层列表元素图标

图标	描述
	组：基本图标
	总是在分层列表中显示的组。
	分层列表不显示组的情况： • 对组应用了**设置组的显示** → **如为空则隐藏**且当前组中没有工作站， • 对组应用了**设置组的显示** → **隐藏**且当前在**树设置**中取消了对**显示隐藏组**一项的勾选。
	如为组设置了工作站自动归属规则，用户组基本图标旁会显示组籍规则图标。 需要显示标志时请在工具面板中选择**树设置** → **显示组籍规则图标**。
	工作站：基本图标
	工作站已安装有反病毒软件，且可以访问。
	工作站已安装有反病毒软件，且可以访问。工作站状态严重性为**中等**。需打开状态查看此工作站具体情况后确定需要管理员采取的操作。

图标	描述
	需要显示标志时请在工具面板中选择 **树设置 → 显示工作站状态重要性**。
	工作站已安装有反病毒软件，且可以访问。工作站状态严重性为**最高**或**高**。需打开状态查看此工作站具体情况后确定需要管理员采取的操作。 需要显示标志时请在工具面板中选择 **树设置 → 显示工作站状态重要性**。
	工作站无法访问。
	工作站上的反病毒软件已卸载。
	通过网络远程安装代理端时工作站的状态。从代理端成功安装到工作站到第一次连接Dr.Web服务器这段时间工作站处于这一状态。
代理服务器：基本图标	
	为连接您的Dr.Web服务器的代理服务器。
	代理服务器已连接到您的Dr.Web服务器，但没有使用为其指定的设置。
	代理服务器已连接到您的Dr.Web服务器，并在使用为其指定的设置。
组、工作站和代理服务器的高级图标	
	如工作站、工作站组和代理服务器有自身设置，在基本图标上可显示自身设置图标。 需要显示标志时请在工具面板中选择 **树设置 → 显示自身设置标志**。 例如，如果是一个已安装有反病毒软件且可以访问的工作站有自身设置，则会显示为：。
策略	
	工作站反病毒组件设置策略或策略版本。
模式	
	用于保存应用程序监控组件设置的模式，活跃状态。
	用于保存应用程序监控组件设置的模式，测试状态。
	停用的用于保存应用程序监控组件设置的模式。
	模式用于保存为其指定的可信任应用程序组不包含于Dr.Web服务器库中的应用程序监控组件的设置。

利用分层列表的工具面板可以对反病毒网络目录中的各元素进行管理。

工具面板

分层列表的工具面板包括以下元素：

常规——用于管理分层列表的常规参数。可在下拉列表中选择相应的选项：

删除所选对象——用于删除分层列表中的对象。操作是在列表中选择一个或多个对象后点击**删除所选对象**。

删除组籍规则——用于删除自动归属工作站的规则。

将此组设为基组——将在分层列表中选出的组设置为该组所有工作站的基组。

为工作站设定基组——将在分层列表中选出的工作站指定基组。这时如在分层列表中选出的是一个组，则该组就成为该组所有工作站的基组。

合并工作站——将工作站合并为分层列表中的同一个账户。可在同一工作站使用不同账户注册时使用这一功能。

删除自身设置——用于删除在分层列表中选出的对象的自身设置。这时该对象将继承其基组的设置。如在分层列表中选出的是一个组，则该组中所有工作站的设置将被删除。

向工作站发送通知——用于向用户发送通知，通知内容自定。

重置密码——删除所选工作站访问反病毒组件设置的用户密码，此选项只可用于Windows操作系统工作站。

重启工作站——远程重启工作站。可在此工作站的 状态查看是否确实需要重启，如因反病毒组件更新/更改而需要重启。

删除Dr.Web代理端——从选定的工作站或工作站组删除代理端和反病毒软件。

安装Dr.Web代理端——打开网络搜索仪，以便把代理端安装到所选工作站。只有选出已批准的新工作站或所选工作站上已卸载代理端时此项才可使用。

恢复已删除的工作站——恢复已删除的工作站。只有选择组**Status**中的子组**Deleted**所含工作站时此项才可使用。

分发安装文件——将所选工作站的安装文件分发到此项设置中指定的电子邮箱。

取消为对象指定模式——将某模式从未所选对象指定的模式列表中删除。如所选对象指定有模式，则此项可用（对象在树结构中显示为此模式的子元素）。

添加网络对象——创建新的网络元素。请在下拉列表中选择相应选项：

创建工作站——创建新工作站（见**安装手册**中的创建新账户）。

创建组——创建新的工作站组。

创建连接——与Dr.Web邻居服务器建立连接。

创建策略——为工作站设置创建新策略。

创建代理服务器——为连接代理服务器创建新账户（见**安装手册**中的 创建代理服务器账户）。

创建模式——创建新模式，用于保存工作站反病毒组件设置。

导出数据：

保存为**CSV**文件——将所选反病毒网络工作站的常规数据写入CSV格式的文件。

保存为**HTML**文件——将所选反病毒网络工作站的常规数据写入HTML格式的文件。

保存为**XML**文件——将所选反病毒网络工作站的常规数据写入XML格式的文件。

保存为PDF文件——将所选反病毒网络工作站的常规数据写入PDF格式的文件。

> 选择上述**导出数据**中的选项时将只导出所选组中所选工作站的相关信息。

导出配置——将反病毒网络所选对象的配置保存到文件。选择此项时会提示选择需要保存的配置项。

导入配置——从文件加载反病毒网络所选对象的配置。选择此项时会提示选择加载配置的文件和需要加载的配置项。

导出统计信息——将反病毒网络所选对象的反病毒组件运行统计信息保存到文件。选择此项时会提示选择需要保存的统计信息项和导出格式。

分发配置——将所选对象的配置分发到反病毒网络其他对象。选择此项时会提示需要分发配置的对象和需要分发的配置项。

指定策略——将所选策略指定给组和个别工作站。此项需选择策略适用的对象。

指定模式——将在反病毒网络树结构中选出的设置模式指定给对象：工作站、用户和组。此选项会提示您选择指定此模式的对象。

设置组显示。用于更改组显示参数。更改时需在分层列表中选出一个组，然后在下拉列表中选择以下一种方式（这时组的标志会发生改变，参见表5-1）：

隐藏——该组在分层列表中的显示将一直处于关闭状态。

若为空则隐藏——如果该组为空组（不含有工作站），该组在分层列表中的显示将处于关闭状态。

显示——该组将一直在分层列表中显示。

管理组件——用于管理工作站上的反病毒组件。需在下拉列表中选择以下一个操作：

还原失败组件——强制还原运行出错组件的状态。还原为工作站当前安装的产品校检状态。

中断已启用的组件——中断工作站上已启动的反病毒组件。可在保护组件中断或启动个别组件的运行。

扫描——用于扫描工作站，可在下拉列表中选择扫描模式：

Dr.Web Agent扫描仪：快速扫描。此模式下利用Dr.Web Agent扫描仪扫描以下对象：

- 内存，
- 所有磁盘引导区，
- 自启动对象，
- 启动盘根目录，
- Windows安装盘根目录，
- Windows系统文件夹，
- 文件夹我的文档，
- 系统临时目录，
- 用户临时目录。

Dr.Web Agent扫描仪：完全扫描。这种模式下利用Dr.Web Agent扫描仪扫描所有硬盘和移动设备（包括启动引导区）。

Dr.Web Agent扫描仪：自定义扫描。这种模式下可利用Dr.Web Agent扫描仪扫描任意文件夹和文件。

未批准的工作站——用于管理新工作站列表，新工作站即还未批准注册的工作站（详见工作站连接策略）。只有选择组**Status**中的子组**Newbies**所含工作站时此项才可使用。Dr.Web服务器批准注册或拒绝访问后工作站会自动从预设子组**Newbies**中删除。可在下拉列表中选择以下一种方式来管理工作站的注册：

允许所选工作站访问并指定基组——批准工作站访问Dr.Web服务器，并从列表中为工作站指定基组。

取消应在连接时执行的操作——为未获得批准的工作站取消之前指定的在工作站连接Dr.Web服务器时应执行的操作。

拒绝所选工作站访问——禁止工作站访问Dr.Web服务器。

阻止参数。用于改变工作站登录Dr.Web服务器的参数。可在下拉列表中选择下列参数：

。

阻止期——指定工作站不可登录Dr.Web服务器的起止日期。

树设置——更改分层列表的显示。启用参数需勾选下拉菜单的选项：

- 对于组：
  - **所有组籍**——重复显示同时是几个组（只指标志为白色文件夹的组，参见表5-1）成员的工作站。勾选此项后会显示组中所有工作站，如取消勾选，则同一工作站只显示一次。
  - **显示隐藏组**——显示反病毒网络中的所有组。取消对此项的勾选后空组（不含有工作站的组）将隐藏。这样在某些情况下，如空组数量较多时可减少多余的信息，方便列表的使用。
- 对于Dr.Web服务器的客户端（工作站、代理服务器和Dr.Web邻居服务器）：
  - **显示客户端识别码**——显示Dr.Web服务器客户端的独有识别码。
  - **显示客户端名称**——如有，则显示Dr.Web服务器客户端名称。

> 不可同时关闭显示客户端识别码和名称。**显示客户端识别码**和**显示客户端名称**两个参数中至少要有一个启用。

  - **显示客户端地址**——显示Dr.Web服务器客户端的IP地址。
  - **显示工作站的服务器**——显示工作站所连接的Dr.Web反病毒服务器的名称或者IP地址。适用于纳入Dr.Web服务器群集的工作站。
  - **显示策略图标**——在指定有策略的工作站图标旁显示策略图标。
  - **显示工作站状态重要性**——显示在线工作站状态重要性。此时会添加状态颜色标卡（参见表5-1）。如停用此项，则状态对应和的工作站会显示为相同图标。
- 对于所有元素：
  - **显示自身设置标志**——在Dr.Web服务器客户端和组的图标上标志是否存在自身设置，包括工作站、代理服务器和Dr.Web邻居服务器。
  - **显示描述**——显示Dr.Web服务器客户端和组的描述，包括工作站、代理服务器和Dr.Web邻居服务器（描述可在属性中给出）。
  - **显示客户端数量**——显示Dr.Web服务器客户端数量：包括客户端所在反病毒网络所有组的工作站、代理服务器和Dr.Web邻居服务器。

- **显示组籍规则图标**——在按照组籍规则自动添加到组的工作站图标上做相应标志、在有自动添加的工作站的组的图标上做相应标志。

客户端排序设置——更改Dr.Web服务器客户端排序参数和在反病毒网络树结构中的排列顺序，包括工作站、代理服务器和Dr.Web邻居服务器。

- 选择排序采用的参数需勾选下列一个选项（只可选择一个参数）：
  - **识别码**——按照客户端特有识别码排序。
  - **名称**——按照客户端名称排序。
  - **地址**——按照客户端网络地址排序。没有网络地址的客户端则自由排序。
  - **创建日期**——按照在Dr.Web服务器创建客户端账户的日期排序。
  - **上次连接日期**——按照上次连接Dr.Web服务器的日期排序。
- 选择排序顺序需勾选下列一个选项：
  - **递增排序**。
  - **递减排序**。

树设置和**客户端排序设置**互相关联：

- 如在**客户端排序设置**部分选择了一个排序参数，此参数会自动在**树设置**部分启用（如原为停用）。
- 如果在**树设置**部分停用在**客户端排序设置**部分选择的参数，则排序参数会自动更改为按照客户端名称排序。如果客户端名称显示为停用状态，则改为按照客户端识别码排序（名称和识别码显示不可同时停用）。

属性面板

属性面板用于显示工作站和组的属性及设置。

显示属性面板

1. 在分层列表中点击工作站或组的名称。
2. 在管理中心窗口右侧打开所选组或工作站的属性面板。设置详情参见编辑组和工作站属性。

5.3.3. 收藏

管理中心可以将界面标签保存到收藏，以方便操作。比如可以快速打开经常用到的管理中心页面。

收藏列表管理

1. 在管理中心主菜单选择**收藏**。
2. 打开收藏的管理中心页面列表。
3. 利用收藏页面列表可以：
   - 打开相应页面。操作是点击列表中的标签。
   - 删除收藏的所有标签。操作是选择**清空收藏**。

添加到收藏

1. 打开需要添加到收藏的管理中心页面。
2. 点击控制菜单上方页面名称旁的图标☆。
3. 打开**添加标签**窗口。在**名称**一栏自动添加页面名称，格式为*<主菜单选项>* > *<控制菜单选项>*。如需可更改标签名称。
4. 可进行的操作：
   - 在收藏保存页面需点击**添加**。页面名称旁的图标会更换为★。
   - 不更改收藏列表并关闭窗口需点击**取消**。

编辑和删除收藏中的标签

1. 打开收藏中需要编辑或删除的管理中心页面。
2. 点击控制菜单上方页面名称旁的图标★。
3. 打开**编辑标签**窗口。可进行的操作：
   - 可更改**名称**一栏。应用更改需点击**更新**按钮。
   - 删除收藏的页面需点击**删除**。页面名称旁的图标会更换为☆。

5.3.4. 搜索栏

*搜索面板*位于管理中心主菜单最右侧，用于快速搜索需要的对象。既可以按照指定参数搜索组，也可以搜索个别工作站。

搜索工作站或工作站组：

1. 在搜索面板下拉列表中选择搜索标准：
   - **工作站**——用于按照名称搜索工作站，
   - **单位**——用于搜索归属某单位的用户组，
   - **工作站ID**——用于按照识别码搜索工作站，
   - **组ID**——用于按照识别码搜索组，
   - **用户ID**——用于按照用户识别码搜索工作站，
   - **用户名**——用于按照工作站用户名搜索工作站，
   - **IP地址**——用于按照IP地址搜索工作站，
   - **MAC地址**——用于按照MAC地址搜索工作站，
   - **设备**——用于按照工作站安装的硬件名称或等级搜索工作站，
   - **软件**——用于按照工作站安装的软件名称搜索工作站。
   - **配置**——用于按照工作站上反病毒组件的参数值搜索工作站。选择此项时打开具备以下设置的搜索面板：
     - **组件**——在下拉列表选择一个反病毒组件的名称，将在此组件的设置中进行搜索。可使用搜索栏方便查找组件：开始输入名称后系统会自动显示与输入字符相符的组件名称。

- **参数**——在下拉列表选择一个可按照其参数值进行搜索的参数的名称。如参数的参数值结构复杂，则无法利用这样的参数进行搜索。
- **值**——指定上面所选参数的参数值。取决于不同参数，可能是下拉列表，或是一个输入栏。

点击**搜索**按钮后开始按照组件参数搜索工作站。

2. 除**配置**（见上）外，其他搜索项需输入搜索内容。可输入：
   - 与搜索项完全相符的具体行；
   - 使用通配符：允许使用的通配符为*和?。
3. 按ENTER键开始搜索。打开高级搜索面板和反病毒网络树结构。
4. 在分层列表中显示所有符合搜索参数的对象，这时：
   - 如果搜索的是工作站，则将显示工作站所属所有组，
   - 如果没有找到任何对象，则会显示空白的分层列表和**未找到任何对象**。

5.3.5. 事件

主菜单显示为**事件**的部分是管理员需要处理的事件。

图标可为以下状态：

——没有网络新事件通知。

——有非重要事件通知。

——有需要管理员处理的重要事件通知。

对事件列表可采取以下操作：

1. 点击图标后打开反病毒网络事件下拉列表。这时图标会自动变为。
2. 点击事件通知行后转至管理中心负责相应功能的页面。
3. 事件列表中的每个通知标签颜色代表事件的重要性（与图标类似）。转至负责相应功能的页面后通知被确定为已读，标签变为灰色。

表5-2. 反病毒网络事件通知列表

事件	重要性	管理中心部分	描述
通知有新工作站	非重要事件	反病毒网络 打开反病毒网络树结构中的**Newbies**组	新工作站已连接到Dr.Web服务器，等待管理员批准访问。出现这一特征的前提是Dr.Web服务器配置文件新工作站注册模式设为手动批准访问。
未读新闻	非重要事件	支持 → 新闻	有Doctor Web公司未读新闻。
新通知	非重要事件	管理 → **Web**控制台通知	有使用**Web**控制台获得的管理员新通知。
紧要通知	重要事件		

事件	重要性	管理中心部分	描述
有服务器更新	重要事件	管理 → **Dr.Web**服务器	Dr.Web服务器更新已加载到库，可进行安装。
服务器配置发生更改。需重新启动服务器。	重要事件	管理 → **Dr.Web**服务器配置	Dr.Web服务器配置文件设置在启动Dr.Web服务器后发生了变化。应用新设置需要重启Dr.Web服务器。
Web服务器配置发生更改。需重新启动服务器。	重要事件	管理 → **Web**服务器配置	Web服务器配置文件设置在启动Dr.Web服务器后发生了变化。应用新设置需要重启Dr.Web服务器。

5.3.6. 设置

转至管理中心设置页面需在主菜单点击**设置**按钮。

本节的所有设置只在管理员当前账户下有效。

窗口左侧的控制菜单包含以下各项：

- 我的账户；
- 界面；
- 订阅。

我的账户

利用此项可以对反病毒网络管理员的当前账户进行管理（另参见管理员和管理员组）。

常规

有*标志的输入栏必须填写。

必要时可以编辑以下参数：

- **登录名**——管理员登录管理中心的用户名；
- 管理员姓名；
- 与账户绑定的**电子邮箱地址**。
- **界面语言**，该管理员使用的界面语言。

如果您所选择的语言目前没有界面更新，会提示您启用此语言的更新。操作是打开**管理** → **库常规配置** → **Dr.Web服务器** → **Dr.Web安全管理中心语言**。勾选需要的语言后点击**保存**。库进行更新时就会为所选语言更新界面。还可在**库状态**手动启动更新。

- **日期格式**，该管理员在编辑含有日期的设置时所使用的日期格式。可选用的格式有：
  - 欧洲格式：`DD-MM-YYYY HH:MM:SS`
  - 美国格式：`MM/DD/YYYY HH:MM:SS`
- 账户**描述**。
- 更换密码时点击工具面板的**更换密码**按钮。

以下参数为只读：

- 账户创建日期和其参数上次更改日期；
- **上一地址**——显示该账户上次连接的网络地址。

权限

管理员权限介绍和编辑操作见编辑管理员。

更改参数后点击**保存**。

接口

树设置

此项的参数用于改变分层列表的外观，与 **反病毒网络**主菜单的 工具面板**树结构外观设置**类似：

- 对于组：
  - **所有组籍**——重复显示同时是几个组（只指标志为白色文件夹的组，参见表5-1）成员的工作站。勾选此项后会显示工作站所有组籍，如取消勾选，则同一工作站只显示一次。
  - **显示隐藏组**——显示反病毒网络中的所有组。取消对此项的勾选后空组（不含有工作站的组）将隐藏。这样在某些情况下，如空组数量较多时可减少多余的信息，方便列表的使用。
- 对于Dr.Web服务器的客户端（工作站、代理服务器和Dr.Web邻居服务器）：
  - **显示客户端识别码**——显示Dr.Web服务器客户端的独有识别码。
  - **显示客户端名称**——显示Dr.Web服务器客户端名称。

不可同时关闭显示客户端识别码和名称。**显示客户端识别码**和**显示客户端名称**两个参数中至少要有一个启用。

  - **显示客户端地址**——显示Dr.Web服务器客户端的IP地址。

- **显示工作站的服务器**——显示工作站所连接的Dr.Web反病毒服务器的名称或者IP地址。适用于纳入Dr.Web服务器群集的工作站。
- **显示工作站状态重要性**——显示在线工作站状态重要性。此时会添加状态颜色标卡（参见表 5-1）。如停用此项，则状态对应和的工作站会显示为相同图标。

- 对于所有元素：
  - **显示自身设置标志**——在Dr.Web服务器客户端和组的图标上标志是否存在自身设置，包括工作站、代理服务器和Dr.Web邻居服务器。
  - **显示描述**——显示Dr.Web服务器客户端和组的描述，包括工作站、代理服务器和Dr.Web邻居服务器（描述可在属性中给出）。
  - **显示客户端数量**——显示Dr.Web服务器客户端数量：包括客户端所在反病毒网络所有组的工作站、代理服务器和Dr.Web邻居服务器。
  - **显示组籍规则图标**——在按照组籍规则自动添加到组的工作站图标上做相应标志、在有自动添加的工作站的组的图标上做相应标志。

客户端排序设置

利用这部分设置可以更改Dr.Web服务器客户端排序参数和其在反病毒网络树结构中的排列顺序，包括工作站、代理服务器和Dr.Web邻居服务器。这部分的设置与**反病毒网络**主菜单工具面板上的**客户端排序设置**类似：

- 选择排序采用的参数需勾选下列一个选项（只可选择一个参数）：
  - **识别码**——按照客户端特有识别码排序。
  - **名称**——按照客户端名称排序。
  - **地址**——按照客户端网络地址排序。没有网络地址的客户端则自由排序。
  - **创建日期**——按照在Dr.Web服务器创建客户端账户的日期排序。
  - **上次连接日期**——按照上次连接Dr.Web服务器的日期排序。
- 选择排序顺序需勾选下列一个选项：
  - **递增排序**。
  - **递减排序**。

时间间隔

这一项用于设定显示统计数据的时间间隔（参见查看工作站统计信息）：

- 在**查看统计信息的默认时间间隔**下拉列表中指定的时间间隔默认将适用于所有统计数据。

  第一次打开统计信息页时显示的将是该段时间的统计数据。必要时可在统计信息各部分更改时间段。
- 如需保存在各部分统计信息上一次指定的时间段，请勾选**保存上次查看统计信息的时间间隔**。

  如勾选此项，则第一次打开统计信息页时显示的将是在浏览器中最近一次选择的时间段。

  如取消勾选，则第一次打开统计信息页时显示的将是在**查看统计信息的默认时间间隔**一项指定的时间段。

登录

在**无操作期**下拉列表选择的时长确定到时后浏览器会自动中断与管理中心对话的时长。

导出为PDF

此项用于设置将统计数据导出为PDF格式时的文本：

- 在**报表字体**下拉列表可选择导出为PDF格式时使用的字体。
- 在**报表字体大小**一栏可指定导出为PDF格式时使用的字体大小。

报表

此项用于设置在管理中心**报表**部分如何显示统计信息：

- 在**页面行数**指定分页显示统计数据时报表每页最多行数。
- 勾选**显示图表**后会显示统计报告中的图形。取消勾选则不显示图形。

订阅

此项应用设置Doctor Web公司新闻订阅。

勾选**自动订阅新栏目**后管理中心的**新闻**页面会自动添加新出现的新闻栏目。

5.3.7. 支持

运行Dr.Web Enterprise Security Suite产品过程中获取帮助的操作是点击**支持**按钮。打开的菜单包含以下选项：

- **帮助**——打开管理员帮助文档中介绍当前所在管理中心页面的章节。如管理员帮助文档中没有介绍当前所在管理中心页面的相应章节，**帮助**按钮不会出现在图标菜单。
- **支持**——打开管理中心**支持**部分（见下）。

支持

支持部分包含以下元素：

1. 补充资源链接
   - **论坛**——转至Doctor Web公司论坛。
   - **新闻**——转至Doctor Web公司新闻页面。
   - **联系技术支持**——打开Doctor Web公司技术支持网页。
   - **提交可疑文件**——打开病毒提交格式，将病毒提交到Doctor Web病毒研究室。
   - **Doctor Web wiki**——转至介绍Doctor Web公司产品的百科知识库网页。
   - **通知办公控制**出现的误报——打开通知格式，用于提交办公控制模块的误报或未能阻止有害链接。

2. **帮助文档**部分。每个文件都有HTML和 PDF两种格式，但存在PDF格式前提的是在管理中心为所选界面语言进行了相应勾选，并在**库常规配置** → **Dr.Web服务器** → 帮助文档部分设定更新PDF格式的文档。点击相应文档的名称就可以打开HTML格式文件。打开PDF格式需在**下载**栏点击图标。为方便查阅，帮助文档分为几个部分：
   - **Dr.Web Enterprise Security Suite的安装和使用（管理员手册）**

     这部分文档是对Dr.Web Enterprise Security Suite如何运行的全面介绍。可以在相应章节了解反病毒保护的部署和设置步骤、其组件与他方软件的交互作用以及您所安装的 Dr.Web Enterprise Security Suite版本发生的最新更改。
   - **Dr.Web Enterprise Security Suite保护下的工作站管理（管理员手册）**

     这部分文档介绍的是对Dr.Web Enterprise Security Suite反病毒网络包含的Doctor Web公司各产品的设置和统一管理。
   - 用户手册

     这部分文档是对Doctor Web公司各产品安装及设置的详细介绍，以及用户使用建议和常见问题解答。



利用Dr.Web移动管理中心将帮助文档下载到Android设备时文件会自动保存到下载文件夹。

如Dr.Web服务器使用自签名HTTPS协议，在将帮助文档下载到Android设备前请检查您的设备是否已安装这一Dr.Web服务器证书。

5.4. Dr.Web安全管理中心组件

5.4.1. 网络搜索仪

网络搜索仪功能

- 浏览网络，发现工作站。
- 启动工作站上是否有Dr.Web代理端。
- 按照管理员指令将Dr.Web代理端安装到找到的工作站。Dr.Web代理端安装详情见**安装手册**中的利用Dr.Web安全管理中心安装Dr.Web代理端。

网络搜索仪运行原则

网络搜索仪支持以下搜索模式：

1. 在Active Directory进行搜索。
2. 按照NetBIOS搜索。
3. 按照ICMP搜索。
4. 按照TCP搜索。
5. 高级模式：确定是否有代理端。

启用所有模式时的运行原则：

1. 前三个模式平行启动。不重复查询已查询过的工作站。
2. 按照TCP搜索后开始按照ICMP搜索未回应的地址。如按照ICMP搜索为停用，则按照TCP搜索与头两种模式平行启动。

> ICMP搜索基于ping查询，可能因网络策略而被阻止（如被防火墙设置阻止）。
>
> 例如：
>
> 如果Windows操作系统（Vista以及更高版本）的操作系统中如网络设置中指定了公共网络，则操作系统将阻止所有ping命令。

3. 查询利用头四种模式搜索到的工作站是否安装有代理端。

> 网络搜索仪能够确定工作站是否安装4.44或更高版本的代理端，不能与更早版本的代理端进行交互作用。

已安装到受保护工作站的代理端处理网络搜索仪发送至一定端口的请求。默认使用端口udp/2193。相应地，网络搜索仪中默认查询的也是上述端口。根据是否可通过上述端口交换信息（访问-相应）网络搜索仪判断是否安装有代理端。

> 如果工作站上的设置（如利用防火墙）禁止udp/2193接收软件包，则代理端无法被发现，网络搜索仪就会认为工作站上没有安装代理端。

启动网络搜索仪

扫描网络

1. 打开网络搜索仪窗口。打开窗口需要在管理中心主菜单中选择**管理**一项，在打开的窗口选择**网络搜索仪**。打开网络搜索仪窗口。
2. 勾选**启用按照ICMP搜索**后将在给出的IP地址范围内通过ICMP协议搜索工作站。
3. 勾选**启用按照TCP搜索**后将在给出的IP地址范围内通过TCP协议搜索工作站。

   设置本模式：

   - **快速搜索**。快速搜索网络时只问询工作站基本端口： 445、139、22、80。
   - **扩展搜索**。扩展搜索网络时问询多个常用端口。严格按照顺序扫描以下端口：445、139、135、1025、1027、3389、22、80、443、25、21、7、19、53、110、115、123、220、464、465、515、873、990、993、995、1194、1433、1434、2049、3306、3690、4899、5222、5269、5432、6000、6001、6002、6003、6004、6005、6006、6007、6446、9101、9102、9103、10050、10051、8080、8081、98、2193、8090、8091、24554、60177、60179。
   - **IPv4地址**——IPv4地址列表：
     - 单个地址：10.4.0.10
     - 地址段：172.16.0.1-172.16.0.123

- 使用网络前缀：192.168.0.0/24

多个地址时使用“;”或“,”隔开。

- **IPv6地址**——IPv6地址列表：
  - 单个地址：fe80::9109:1808:8e44:735b%3
  - 地址段：[FC00::0001]-[FC00::ffff]
  - 使用网络前缀：[::ffff:10.0.0.1]/7

多个地址时使用“;”或“,”隔开。

4. 勾选**启用按照NetBIOS搜索**后将通过NetBIOS协议搜索工作站。

设置本模式：

- **域**——搜索工作站使用的域列表。使用逗号分开不同的域。
- 勾选**扩展搜索**后将利用从网络浏览器获得的信息进行扩展搜索。

5. 勾选**启用在Active Directory进行搜索**后将在Active Directory域名搜索工作站。



使用网络搜索仪在Active Directory域名搜索工作站时，打开管理中心的浏览器必须使用具备Active Directory域名对象搜索权限的用户域名启动。

在Active Directory域搜索工作站只使用加密协议ldaps。

设置本模式：

- **Active Directory控制器**——Active Directory控制器，如dc.example.com。
- **注册用户名**——Active Directory用户的注册用户名。
- **密码**——Active Directory用户的密码。



Windows操作系统的Dr.Web服务器没有必要一定进行Active Directory搜索设置。注册信息默认采用启动Dr.Web服务器进程的用户的注册信息（一般为LocalSystem）。

UNIX家族操作系统的Dr.Web服务器必须进行设置。

- 在**保护连接**下拉列表选择交换数据时使用的加密类型：
  - **STARTTLS**——通过指令STARTTLS转为受保护的连接。默认连接使用的端口为25。
  - **SSL/TLS**——开通单独的受保护连接。默认连接使用的端口为465。
  - **无**——不使用加密。将使用未受保护的连接交换数据。

6. 在**常规参数**部分指定所有搜索模式都使用的参数：

- **超时时限（秒）**——等待工作站响应的时限，以秒计。
- **一个工作站的问询次数**——等待响应时对同一个工作站的问询次数上限。
- **同时问询数量**——同时对其发出问询的工作站数量上限。
- 勾选**显示工作站名称**后搜索到网络中计算机时会不仅显示其IP地址，而且会显示其域名。如工作站没在DNS服务器注册，则只显示其IP地址。
- 勾选**确定是否安装代理端**后将确定工作站是否已安装了代理端。

如**确定是否安装代理端**为停用，则所有搜索到的工作站的状态都显示为，即工作站反病毒软件包状态未知。

- **端口**——按照UDP协议搜索代理端使用的端口。端口号范围为1-65535。默认使用端口2193。

7. 点击**搜索**。开始搜索网络。
8. 搜索过程中窗口将加载计算机列表，标注安装有Dr.Web代理端。

   展开目录各项，每项各对应工作站组（域）。所有目录元素对应工作站组合工作站，均注有图标，各图标含义见下：

图标	描述
工作站组	
	组中有的计算机可以安装Dr.Web Enterprise Security Suite反病毒软件。
	组中工作站已安装有反病毒软件或者工作站无法从网络访问。
工作站	
	工作站已安装有反病毒软件，处于活跃状态。
	工作站处于活跃状态，反病毒软件状态不确定：工作站未安装反病毒软件，或未检查是否安装有反病毒软件。

   对应标志有的工作站的目录项可继续展开，查看已安装的组件。

5.5. 反病毒网络组件交互作用示意图

图5-2为反病毒网络组成总体示意图。

此示意图所表示的反病毒网络只包含一个Dr.Web服务器。在规模较大的企业应部署带有几个Dr.Web服务器的反病毒网络，以便分配负载。

下面的例子中反病毒网络部署于一个局域网内，实际上Dr.Web Enterprise Security Suite和反病毒软件包的安装和运行并不要求计算机处于一个局域网，只需要能连接互联网就可以了。

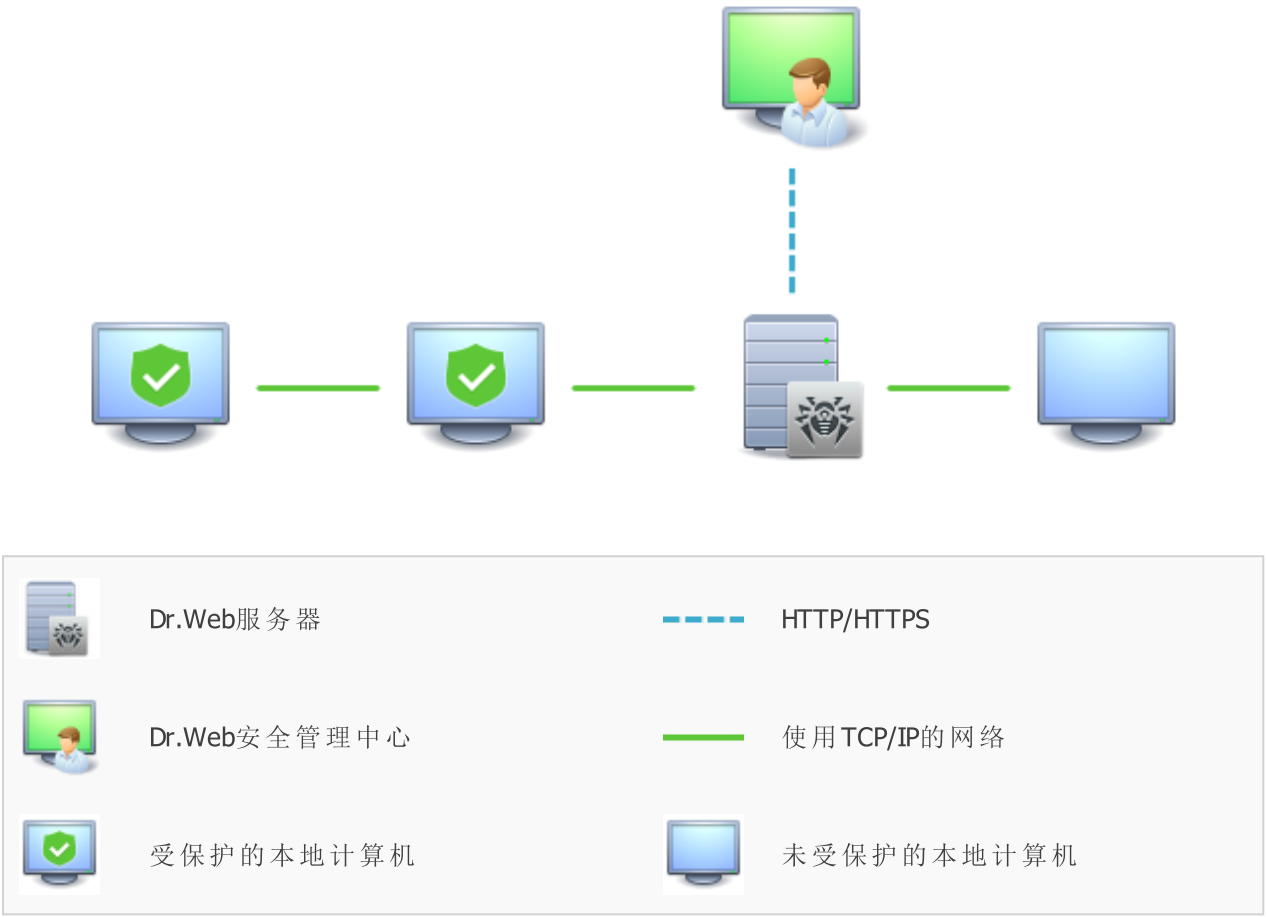


图**5-2.**反病毒网络结构

启动**Dr.Web** 服务器时顺序执行以下操作：

1. 从bin目录加载Dr.Web服务器文件。
2. 加载Dr.Web服务器任务管理器。
3. 加载统一安装目录和更新目录，进行信息系统（通知系统）初始化。
4. 检查Dr.Web服务器数据库的完整性。
5. 执行Dr.Web服务器任务管理器的任务。
6. 等待Dr.Web代理端信息和管理中心命令。

所有命令、数据和统计信息流都必须经过Dr.Web服务器。管理中心也只与Dr.Web服务器进行信息交换；按照管理中心的命令由服务器将命令传递给Dr.Web代理端，由Dr.Web服务器进行工作站配置的更改。

这样，反病毒网络的逻辑结构会是图5-3所示。

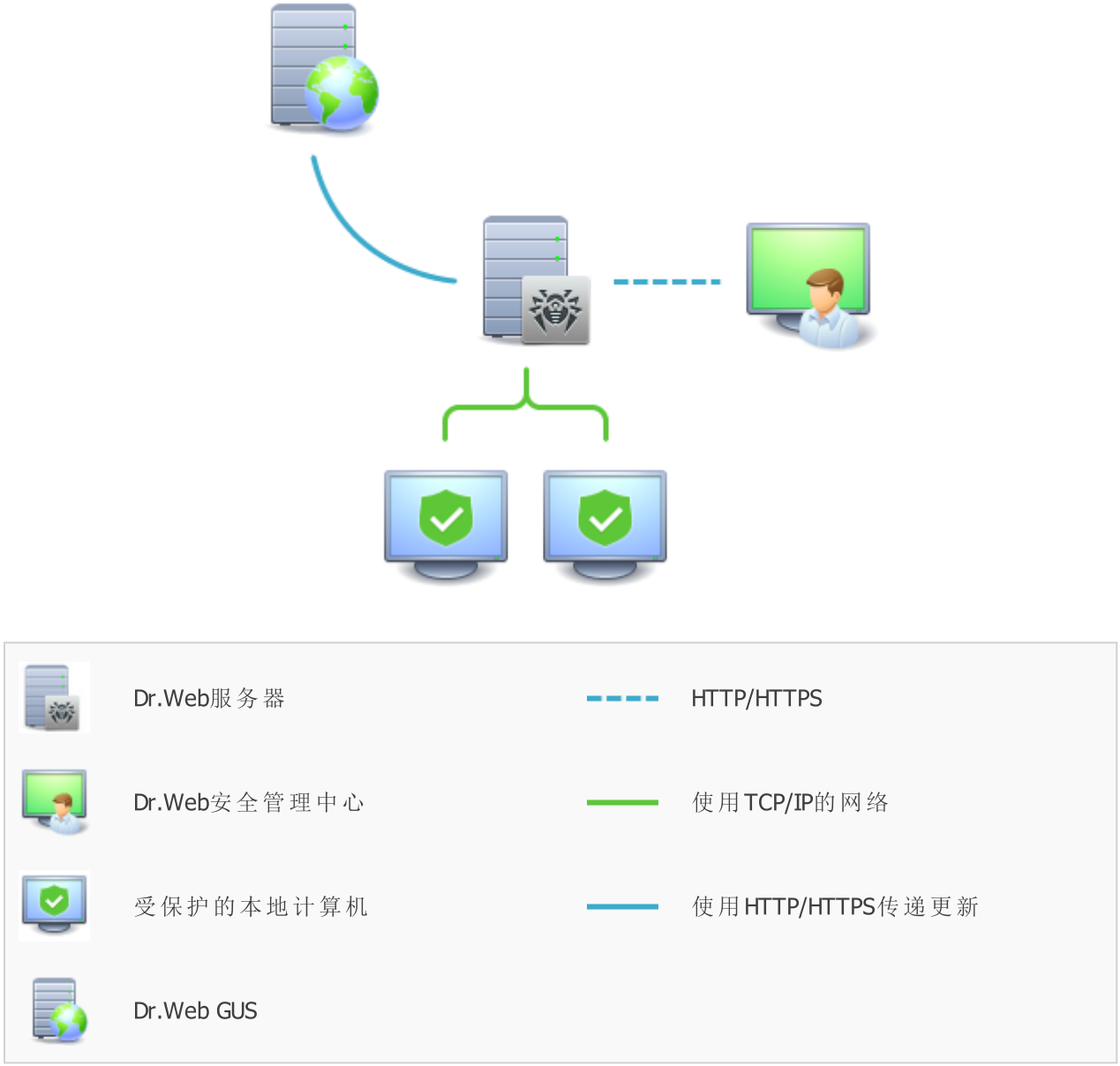


图5-3.反病毒网络逻辑结构

在Dr.Web服务器和工作站组件间（图 5-3中用细实线表示）传递：

- 代理端获取统一日程和本工作站统一日程的申请；
- 代理端和反病毒软件包设置；
- 例行任务（扫描、病毒库更新等等）执行申请，
- 反病毒软件包文件——在代理端接收到安装任务时传递，
- 软件和病毒库更新——在执行更新任务时传递，
- 代理端有关工作站配置的通知；
- 代理端和反病毒软件包运行统计信息，以便纳入统一日志；
- 病毒事件及其他记录事件通知。

工作站和Dr.Web服务器间的流量取决于工作站的设置和数量，可能达到很高的流量。因此Dr.Web Enterprise Security Suite反病毒网络可进行流量压缩。这一可选模式介绍见使用流量加密和压缩。

可以对工作站和Dr.Web服务器间的流量进行加密，以防止泄露利用此通道传递的信息，并可避免应加载到工作站的软件被替换。默认情况下此功能为启用。使用这一模式的介绍参见 使用流量加密和压缩。

从网络更新服务器向Dr.Web服务器（图5-3中用粗实线表示）传递信息使用的是HTTP协议，所传递的是复制统一安装目录和更新目录所需文件以及这一过程的技术信息。使用校检和检验机制来保证所传递信息（Dr.Web Enterprise Security Suite软件文件和反病毒软件包）的完整性：传递中受损或被替换的文件将不会被Dr.Web服务器接收。

Dr.Web服务器和管理中心间（图5-3中用虚线表示）所传递的信息是Dr.Web服务器配置（包括网络拓扑信息）和工作站设置。这一信息会直观体现在管理中心，如果用户（反病毒网络管理员）对设置进行了更改，更改会传递给Dr.Web服务器。

管理中心与所选Dr.Web服务器的连接建立前必须进行反病毒网络管理员身份验证，方式是在该Dr.Web服务器输入管理员注册用户名和密码。

第六章、反病毒网络管理员

反病毒网络管理员应当是具备局域网管理员工作经验和反病毒保护知识的可靠的、业务水平较高的人员。管理员有访问Dr.Web服务器安装目录的所有权限。根据企业内部安全策略及人员状况，可以让反病毒管理员拥有局域网管理员权限，或者是与局域网管理员紧密合作。

对反病毒网络进行日常管理不要求反病毒网络管理员具备反病毒网络中计算机上的管理员权限。但代理端软件的远程安装和卸载只能在局域网中进行，要求具备此网的管理员权限，而进行Dr.Web服务器调试要求有服务器安装目录的完全访问权限。

在进行反病毒网络规划时建议列出所有有权访问管理中心的责任人，并根据其可以执行的功能设定不同的角色。必须为每一角色创建管理员组。将具体管理员的账户移至相应管理员组就可以实现管理员与角色的对接。如需可以将管理员组（角色）分出级别，设置为多级别体系，可以为每一级别分别设置管理员访问权限。

6.1. 管理员身份验证

登录Dr.Web服务器可通过以下方式进行管理员身份验证：

- 将管理员信息保存于Dr.Web服务器数据库。
- 利用设置LDAP/AD连接LDAP和Active Directory服务器。
- 使用RADIUS协议。
- 使用PAM（仅限UNIX家族操作系统）。

从上一版本更新Dr.Web服务器时还可使用以下身份认证类型（如上一版本启用了这些类型）：

停用这些身份认证方式后将会去掉管理中心设置中的相关选项。

首次安装Dr.Web服务器不提供这些选项。

- 利用Active Directory（适用于OS Windows下的Dr.Web服务器版本）。
- 使用LDAP协议。

认证方式依次按以下原则进行：

1. 首先尝试认证Dr.Web服务器数据库管理员。
2. 身份验证方式的使用次序取决于管理中心设置中这些方式的排列顺序。
3. 默认情况下，通过外部系统进行身份验证的方式为停用。

更改身份验证方式使用次序

1. 在管理中心主菜单选择**管理**。
2. 在控制菜单选择**身份验证**。

3. 打开的窗口为身份验证类型列表，按使用次序排列。可移动（drag'n'drop）更改次序。
4. 应用更改需重启Dr.Web服务器。



管理员注册用户名不应重复。

管理员将无法通过外部系统登录，如果Dr.Web服务器已有用户名相同的管理员。

每一次保存**身份验证**部分的更改时会自动备份包含管理员身份验证参数的上一版本配置文件。共保存10个不同版本的备份。

备份与配置文件在同一目录，目录名称格式为：

<文件名称>_<创建时间>

其中*<文件名称>*取决于身份验证系统：`auth-ads.conf`、`auth-ldap.conf`、`auth-radius.conf`、`auth-pam.conf`。

可使用备份在无法访问管理中心界面时恢复配置文件。

6.1.1. Dr.Web服务器数据库管理员身份验证

默认使用将管理员信息保存于Dr.Web服务器数据库的验证方式。

打开管理员账户管理页面

1. 在管理中心主菜单选择**管理**。
2. 在控制菜单选择**管理员**。打开Dr.Web服务器所有管理员的列表。
   详见管理员和管理员组一节。

6.1.2. 使用LDAP/AD进行身份验证

启用**LDAP/AD**身份验证

1. 在管理中心主菜单选择**管理**。
2. 在控制菜单选择**身份验证**。
3. 在打开的窗口进入**LDAP/AD**身份验证。
4. 勾选**使用LDAP/AD身份验证**。
5. 点击**保存**按钮。
6. 应用更改需重启Dr.Web服务器。

可在任一LDAP服务器设置使用LDAP协议的身份验证。使用这一机制还可以设置UNIX家族操作系统下的Dr.Web服务器，以便登录域控制器的Active Directory。

为方便用户在此选项可切换LDAP/AD身份验证的简易设置和高级设置。

LDAP/AD身份验证身份验证设置保存于配置文件auth-ldap-rfc4515.conf。

还提供包含标准设置的配置文件：auth-ldap-rfc4515-check-group.conf、auth-ldap-rfc4515-check-group-novar.conf、auth-ldap-rfc4515-simple-login.conf。

身份验证运行算法原则和各参数见附录的附录C3。

6.1.3. 使用RADIUS进行身份验证

使用RADIUS身份验证协议需要安装实施此协议的服务器，如freeradius（详情参见https://freeradius.org/）。

在开始设置通过ADIUS进行身份认证之前请确认已将处于Dr.Web服务器 目录etc的字典dictionary.drweb已拷贝到目录 /usr/share/freeradius。此字典保存Doctor Web公司RADIUS参数值（VSA——Vendor-Specific Attributes）。

请利用命令行指定对目录/usr/share/freeradius中的文件dictionary.drweb的访问权限。命令示例见下：

```
chmod 644 /usr/share/freeradius/dictionary.drweb
```

在文件/etc/raddb/dictionary的结尾添加下面一行：

```
$INCLUDE/usr/share/freeradius/dictionary.drweb
```

在文件 /etc/raddb 的开始添加以下几行：

```
<注册名> Cleartext-Password := "<密码>"

DrWeb-ES-Adm-Flag = 1
```

在执行玩上述操作后利用管理中心启用RADIUS身份认证。

启用RADIUS身份验证

1. 在管理中心主菜单选择管理。
2. 在控制菜单选择身份验证。
3. 在打开的窗口进入RADIUS身份验证。
4. 勾选使用RADIUS身份验证。
5. 点击保存按钮。
6. 应用更改需重启Dr.Web服务器。

在管理中心设置以下RADIUS服务器运行参数：

- 服务器、端口、密码——连接RADIUS服务器的参数：IP地址/DNS名称、端口号、密码。
- 超时时限——等待RADIUS服务器响应的时限，以秒计。

- **重复尝试次数**——再次尝试连接RADIUS服务器的次数。

还可以使用配置文件auth-radius.conf来设置RADIUS高级参数，从配置文件位于服务器的etc目录。

除了提供管理中心设置的参数，还可利用配置文件设置识别码NAS值。依据RFC2865此识别码可替代IP地址/DNS名称作为客户端连接RADIUS服务器的识别码。在配置文件中保存为以下格式：

```
<!-- NAS identifier, optional, default - hostname -->
<nas-id value="drwcs"/>
```

6.1.4. 使用PAM进行身份验证

启用PAM身份验证

1. 在管理中心主菜单选择**管理**。
2. 在控制菜单选择**身份验证**。
3. 在打开的窗口进入**PAM身份验证**。
4. 勾选**使用PAM身份验证**。
5. 点击**保存**按钮。
6. 应用更改需重启Dr.Web服务器。

UNIX家族操作系统PAM身份验证利用的是身份验证插件。

可通过以下犯上设置PAM身份验证参数：

- 利用管理中心设置身份验证方式：在**管理**→**身份验证**→**PAM身份验证**。
- 配置文件auth-radius.xml，位于Dr.Web服务器的etc目录。配置文件示例：

```
...
<!-- Enable this authorization module -->
  <enabled value="no" />
<!-- This authorization module number in the stack -->
  <order value="50" />
<!-- PAM service name>" -->
  <service name="drwcs" />
<!-- PAM data to be queried: PAM stack must return INT zero/non-zero -->
  <admin-flag mandatory="no" name="DrWeb_Esuite_Admin" />
...
```

在Dr.Web Enterprise Security Suite端设置的PAM身份验证参数描述

管理中心元素	auth-pam.xml文件元素			描述
	标签	属性	有效值	
复选框**使用PAM身份验证**	<enabled>	value	yes | no	此选项用于确定是否使用PAM身份验证。
请*拖移*：	<order>	value	整数值，应与其他方法参数	使用多种身份验证方式时PAM身份验证的排号。

管理中心元素	auth-pam.xml文件元素			描述
	标签	属性	有效值	
			值相符	
输入栏服务名称	<service>	name	-	用于创建PAM内容的服务的名称。PAM可从/etc/pam.d/<*服务名称*>读取服务政策，如文件不存在，则从 /etc/pam.conf读取。 如未给出参数（配置文件没有符号<service>），则默认使用名称drwcs。
复选框控制项必须勾选	<admin-flag>	mandatory	yes | no	此参数用于确定将用户验证为管理员是否必需控制项。 默认为yes。
输入栏控制项名称	<admin-flag>	name	-	参数行，使用此行PAM模块读取选项。 默认为：DrWeb_Esuite_Admin。

设置PAM身份验证模块时请使用Dr.Web Enterprise Security Suite端指定的参数，参数没有指定时，需使用其默认值。

6.1.5. 使用Active Directory进行身份验证

在启用Active Directory身份认证之前请确认您要为其启用认证的账户不在**受保护用户**组。由于Dr.Web服务器是服务，对**受保护用户**组的账户进行身份认证会出错。关于受保护用户安全组详细信息可参阅Microsoft公司官网。

启用**Active Directory**身份验证

1. 在管理中心主菜单选择**管理**。
2. 在控制菜单选择**身份验证**。
3. 在打开的窗口进入 **Microsoft Active Directory**。
4. 勾选使用 **Microsoft Active Directory**身份验证。
5. 点击**保存**按钮。
6. 应用更改需重启Dr.Web服务器。

从Active Directory进行管理员认证是在管理中心只是设置允许使用这一认证方式。

编辑Active Directory管理员属性需要在Active Directory服务器手动进行。

编辑**Active Directory**管理员



以下操作要求计算机上必须具有Active Directory管理员工具。

1. 编辑管理员参数需执行以下操作：
   a) 启动工具`drweb-13.00.0-<编号>-esuite-modify-ad-schema-<操作系统版本>.exe`对Active Directory架构进行修改（此工具包含于Dr.Web服务器软件）。
   修改Active Directory架构会占用一些时间。对于不同配置的域，同步和应用修改后的构架会占用5分钟或更长时间.



如之前已利用Dr.Web服务器版本6的工具修改了Active Directory架构，不需要使用Dr.Web服务器版本13的工具再次进行修改。

   b) 注册工具Active Directory Schema （Active Directory构架），操作是以相应管理员权限执行命令`regsvr32 schmmgmt.dll`，然后运行`mmc`并添加工具**Active Directory Schema**。
   c) 利用添加的工具Active Directory Schema在**User**一项和（如需）**Group**一项添加辅助项**DrWebEnterpriseUser**和高级属性**DrWebAdmin**。



如尚未完成修改后构架的应用，会找不到**DrWebEnterpriseUser**一项。这种情况下请稍后按照**c)** 重试。

   d) 以管理员权限运行文件`drweb-13.00.0-<编号>-esuite-aduac-<操作系统版本>.msi`（包含于Dr.Web Enterprise Security Suite 13.0软件），等待安装结束。
2. 属性编辑图形界面可通过控制面板打开：**Active Directory Users and Computers** → **Users** 部分 → 选定用户**Administrator Properties**属性编辑窗口 → **Dr.Web Authentication**标签。
3. 编辑时可使用以下参数（每一属性值可以为**yes**、**no**或**not set**）：
   User is administrator——指示用户为全权管理员。



身份验证运行算法原则和各参数见附录的附录C1。

6.1.6. 使用LDAP进行身份验证



只有在从上一版本更新Dr.Web服务器时刻通过管理中心设置此选项。停用此身份认证方式后将会去掉管理中心设置中的相关选项。

首次安装Dr.Web服务器不能访问这些选项。

启用**LDAP**身份验证

1. 在管理中心主菜单选择**管理**。
2. 在控制菜单选择**身份验证**。
3. 在打开的窗口进入**LDAP**身份验证。
4. 勾选**使用LDAP身份验证**。
5. 点击**保存**按钮。
6. 应用更改需重启Dr.Web服务器。

可在任一LDAP服务器设置使用LDAP协议的身份验证。使用这一机制还可以设置UNIX家族操作系统下的Dr.Web服务器，以便登录域控制器的Active Directory。



LDAP身份验证设置保存于配置文件`auth-ldap.conf`。

身份验证运行算法原则和各参数见**附录**的附录C2。

与Active Directory不同，可在任一LDAP架构下设置登录机制。默认情况下尝试使用为Active Directory确定的Dr.Web Enterprise Security Suite属性。

LDAP身份验证流程：

1. 从管理中心或在xml-配置文件中给出LDAP服务器地址。
2. 指定用户名需完成以下操作：
   - 如设置有规则，使用DOS类通配符（带符号*）将用户名转换为DN（Distinguished Name）。
   - 如设置有规则，使用正则表达式将用户名转换为DN。
   - 如设置中有脚本，使用用户脚本将用户名转换为DN。
   - 如所有转换规则都不能使用，按原样使用已给出的用户名。



用户名给出格式没有固定的规则，可以是企业内认同的格式，即不要求强制更改LDAP架构。此架构下转换使用的是将用户名转换为LDAP DN。

3. 转换后与Active Directory相同，利用得到DN的和输入密码尝试在LDAP服务器注册此用户。
4. 接下来与Active Directory相同，为得到的DN读取LDAP对象属性。可能的属性值将记录到配置文件。
5. 如还有未确定的管理员属性值，则有继承设置时（在配置文件）会在用户所属组搜索需要的属性，搜索与使用Active Directory时相同。

6.2. 管理员和管理员组

打开管理员账户管理页面

1. 在管理中心主菜单选择**管理**。
2. 在控制菜单选择**管理员**。打开Dr.Web服务器所有管理员的列表。

管理中心的管理员都可以访问**管理员**一项。但只有**Administrators**组中具有**查看管理员组属性和配置**权限的管理员可以访问整个管理员级别树结构。其他管理员只能访问其所在组和其子组中的账户。

在工具面板的**管理员**部分可使用以下选项：

 创建帐户

 创建组

 删除所选对象

 更改密码

 分发管理员权限

6.2.1. 管理员级别

管理员级别列表为管理员组和管理员账户的树结构。树结构的节点是管理员组和管理员组中包含的账号。每一管理员只能列入一个组。组的子组嵌套深度不限。

预设组

安装Dr.Web服务器后自动创建两个组：

- **Administrators**。此组一开始只有一个全权管理员**admin**，在安装Dr.Web服务器时自动创建（见下）。
- **Newbies**。此组一开始为空。通过LDAP、Active Directory和RADIUS进行外部身份验证的管理员会自动添加到这个组中。

  Newbies组中的管理员默认只具备只读权限。

预设管理员

安装Dr.Web服务器后自动创建一个管理员账户：

参数	说明
注册用户名	**admin**
密码	在安装Dr.Web服务器时指定（安装进程第9步）。
权限	全权
编辑账户	不得编辑此管理员权限，此管理员也无法删除。

分层列表的显示

- 在反病毒网络分层列表中：管理员只能看到在**查看工作站组属性**权限中允许的用户组。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。

- 在管理员分层列表中：**Newbies**组管理员看到的树结构根组为其所在组，也就是只能看到本组和其子组的管理员。**Administrators**组的管理员能够看到所有组的所有管理员。

6.2.2. 管理员权限

管理员在管理中心能够进行的操作取决于其权限，可为单独的账户指定权限，也可为工作站组指定权限。

管理员权限系统可进行以下权限控制操作：

- 指定权限

  创建管理员或管理员组时为其指定权限。权限从管理员和管理员组创建时进入的父组继承。创建时不可更改权限。

- 继承设置

  默认情况下管理员和管理员组从其父组继承权限，但可以停用继承。
  - 如停用继承，则管理员使用直接为其账户指定的个人权限。此时不计父组权限。
  - 管理员或管理员组继承权限时不是重新指定父组权限，而是将父组所有权限按照树结构向上重计。根据所指定权限和父组权限计算最终权限的计算表见权限合计。

- 编辑权限

  创建管理员或管理员组时不可编辑权限。只可为已创建的对象通过账户或组设置来编辑权限。编辑个人权限时只可减少权限。预设管理员**admin**以及预设组**Administrators**和**Newbies**的权限不可编辑。

  编辑权限的操作见编辑权限一节。

编辑权限

编辑管理员或管理员组权限

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**管理员**一项。
2. 在管理员列表选择需要编辑的账户。打开属性编辑窗口。
3. 在**权限**部分可编辑允许所选管理员或管理员组进行的操作。
4. 可使用开关来控制所选对象是否继承父组权限：

   启用继承

   停用继承
5. 基本设置在权限列表中给出：

   a) 第一列为权限名称。列头取决于按照类型合并权限的具体项目。

   管理员权限和具体权限负责的管理中心各组成部分简介见**附录**中的附录C4. 权限对应项。

b) **权限**一列为第一列中相应权限的设置。

管理的对象	权限一列的设置列表	指定权限的原则
权限为所有对象指定		
权限不可按照所管理的对象分组。	可设定以下一种类型的权限： • **自身权限**——此对象指定有自己的设置。 • **继承权限**——设置从父组继承。	在相应权限所在行勾选**提供**或取消勾选。
权限为对象（工作站、管理员或组）列表指定		
• *全部提供*——权限提供给所有管理对象。 • *全部禁止*——权限不提供给任何管理对象。 • *提供给某些对象*。这种情况下需指定提供此权限的对象列表。对应所有其他对象此权限为禁止。 • *不提供给某些对象*。这种情况下需指定不提供此权限的对象列表。对于所有其他对象此权限为允许。	合并设置时同时显示以下类型的权限： • **自身权限**——为此对象指定的设置。 • **最终取消**——对象的自身权限与父组权限的合并结果。 继承设置时只显示**可继承权限**。	点击对象列表（包括指定**全部**时）。取决于需编辑的是何种权限打开的窗口会显示反病毒网络树结构、管理员组树结构或资费标准树结构。在树结构中选择需要的对象。多选使用CTRL和SHIFT。如需可勾选**适用于本节所有权限**，这样设置会应用于被编辑的权限所在部分的所有权限。 点击： • **提供**用于允许所选对象权限。 • **禁止**用于禁止所选对象权限。

对于同一权限不可同时指定禁止对象和允许对象列表。允许和禁止相互排斥。

c) **继承**一列为此权限相对于父组的状态：
- **从组继承**——已启用从指定父组继承权限，未指定自身权限。
- **自身权限**——未启用从指定父组继承权限，指定有自身权限。
- **与组合并**——已启用从指定父组继承权限，指定有自身权限。将父组权限与自身权限合并获得最终权限（参见合并权限）。
  这种情况下可删除对象自身权限。操作是在**继承**一列点击。删除自身权限后将设为**从组继承**。

合并权限

继承权限时最终权限（管理员或管理员组）的计算取决于父组权限和为对象本身指定的权限。下表为最终权限规则：

父组权限	继承者的权限	最终权限
全部提供	为个别对象提供	为继承者对象提供

父组权限	继承者的权限	最终权限
为个别对象提供	为个别对象提供	合并允许对象列表
为个别对象提供	全部提供	全部提供
父组与继承者权限为禁止，且其中一个为全部禁止		全部禁止
对于个别对象为禁止	对于个别对象为禁止	合并禁止对象列表
全部禁止	全部提供	全部提供
对于个别对象为禁止	全部提供	对于父对象为禁止
对于个别对象为禁止	为个别对象提供	从禁止对象中排除允许的对象。如排除后禁止列表不为空，则结果为禁止剩余的对象，否则结果则为允许所有继承者对象
为个别对象提供	全部禁止	全部禁止
全部提供	对于个别对象为禁止	对于继承者对象为禁止
为个别对象提供	对于个别对象为禁止	从允许对象中排除禁止的对象。如排除后允许列表为空，则结果为全部禁止，否则结果则为禁止剩余对象。

6.3. 对管理员与管理员组账户的管理

6.3.1. 管理记录和组的创建与删除



管理员注册用户名不应重复。

管理员将无法通过外部系统登录，如果Dr.Web服务器已有用户名相同的管理员。

添加管理员



创建管理员账户需要具备**创建管理员和管理员组**的权限。

添加新的管理员账户

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**管理员**一项。
2. 在工具面板点击**创建账户**。打开账户设置窗口。
3. 在**常规**部分设定以下参数：

- 在**注册用户名**一栏指定该管理员访问管理中心所使用的用户名。允许使用小写字母（a-z）、大写字母（A-Z）、数字（0-9）、符号"_"和"."。
- 在**密码**和**确认密码**指定访问Dr.Web服务器的密码，也就是访问管理中心的密码。



设置管理员密码时不得使用本民族语言符号。



只有当管理员采用内部身份验证时才可设置密码一栏。

在管理中心为采用外部身份验证的管理员指定的上述输入栏参数无效。

- 可在**姓**、**名**和**父称**输入管理员个人信息。
- 请输入**电子邮箱地址**。如不输入，则无法在需要时重置密码。
- 在**界面语言**下拉列表选择此管理员使用的管理中心界面语言（默认为Web浏览器语言或英语）。



如果您所选择的语言目前没有界面更新，会提示您启用此语言的更新。操作是打开**管理** → **库常规配置** → **Dr.Web服务器** → **Dr.Web安全管理中心语言**。勾选需要的语言后点击**保存**。库进行更新时就会为所选语言更新界面。还可在**库状态**手动启动更新。

- 在**日期格式**下拉列表选择该管理员在编辑含有日期的设置时所使用的日期格式。可选择的格式有：
  - 欧洲格式：`DD-MM-YYYY HH:MM:SS`
  - 美国格式：`MM/DD/YYYY HH:MM:SS`
- 在**描述**一栏可输入对账户的描述，内容自定。



有*标志的输入栏必须填写。

4. 在**组**部分指定管理员父组。表中所列是可以为管理员指定的组。为所创建的管理员指定的组为勾选。默认新创建的管理员列入当前管理员父组。更改方式是勾选需要指定的组。

   每一管理员只能列入一个组。

   管理员从父组继承权限（参见管理员权限）。
5. 设置所有参数后点击**保存**按钮建立管理员账户。



建议在创建新管理员账户后按照通知配置部分的说明设置通知，这样新增管理员就可以及时获取反病毒网络事件的相关信息。如需按日程生成统计信息报表则需启用**统计信息报表**通知。

添加管理员组



创建管理员组需要具备**创建管理员和管理员组**的权限。

添加新的管理员组账户

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**管理员**一项。
2. 在工具面板点击**创建组**。打开组设置窗口。
3. 在**常规**部分设定以下参数：
   - 在**组**一栏指定该管理员组名称。允许使用小写字母（a-z）、大写字母（A-Z）、数字（0-9）、符号"_"和"."。
   - 在**描述**一栏可输入对组的描述，内容自定。
4. 在**组**部分指定管理员组的父组。表中所列是可指定的父组。为所创建的组指定的组为勾选。默认新创建的管理员族列入当前管理员父组。更改方式是勾选需要指定的组。

   只可指定一个父组。

   管理员从父组继承权限（参见管理员权限）。
5. 设置所有参数后点击**保存**按钮建立管理员组。

删除管理员和管理员组



删除管理员账户和管理员组账户需要分别具备**删除管理员账户**和**编辑管理员组属性和配置**权限。

删除管理员或管理员组账户

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**管理员**一项。
2. 在管理员分层列表中选出需要删除的管理员账户或管理员组账户。
3. 在工具面板点击**删除所选对象**按钮。

6.3.2. 找回管理员密码

可利用下面这些方式找回管理员密码：

1. 在登录Dr.Web安全管理中心时重置密码。
2. 启动Dr.Web服务器时在命令行指定新密码。
3. 可直接在Dr.Web服务器数据库查看或更改密码，如果是内设数据库需使用工具drwidbsh3，如果是外设数据库需使用第三方SQL代理端—前提是停用了密码的加盐加密（不建议）。工具详情和使用示例请参见**附录**中的附录H7.2. 内设数据库管理工具。

在登录**Dr.Web**安全管理中心时清空密码的操作

1.打开登录页面（http://*<Dr.Web服务器地址>*:9080或https://*<Dr.Web服务器地址>*:9081）。

2.点击**重置密码**。

3. 在打开的窗口填写需找回密码的管理员账户的**登录名**和**电子邮箱地址**。

输入的电子邮箱地址应与管理员账户设置中指定的电子邮箱地址相符。

4.点击**发送链接**。指定的电子邮箱地址会收到重置密码链接。

发送此邮件的前提是对SMTP服务器预先进行了设置（见电子邮箱）。

5.点击此链接后在打开的页面指定新密码。

在启动**Dr.Web**服务器时利用命令行更换密码的操作：

从命令行启动Dr.Web服务器，启动时指定更换密码的相应参数、管理员注册名和新密码：

```
drwcsd modexecdb set-admin-password <注册名> <新密码>
```

6.3.3. 编辑管理员账户和管理员组

编辑管理员账户和管理员组账户需要具备**编辑管理员账户**和**编辑管理员组属性和配置**权限。

编辑自身账户要具备**编辑自身设置**权限。

有*标志的输入栏必须填写。

编辑管理员帐户

1. 在管理员列表选择需要编辑的账户。打开属性编辑窗口。
2. 在**常规**部分可编辑创建时指定的参数，这时：
   a) 更换管理员账户密码时请在工具面板点击**更换密码**。

有相应权限的管理员可以编辑所有其他管理员的密码管理员密码不可编辑。

设置管理员注册名时不得使用本民族语言符号。

b) 以下管理员参数为只读：
   - 账户创建日期和其参数上次更改日期；
   - **状态**——显示该账户上次连接的网络地址。

3. 在**组**部分可更改管理员组。表中所列是可以为管理员指定的组。为所创建的管理员指定的组为勾选。更改方式是勾选需要指定的组。

   必须为管理员指定父组。每一管理员只能列入一个组。从指定的父组继承权限。

   另参见编辑组籍。
4. 在**权限**部分可编辑允许所选管理员进行的操作。

   编辑权限的操作见编辑权限一节。
5. 应用更改需点击**保存**。

编辑管理员组

1. 在管理员列表选择需要编辑的组。打开属性编辑窗口。
2. 在**常规**部分可编辑创建时指定的参数。
3. 在**组**部分可更改父组。表中所列是可指定为父组的组。当前父组为勾选。更改方式是勾选需要指定的组。

   必须为管理员组指定父组。从指定的父组继承权限。

   另参见编辑组籍。
4. 在**权限**部分可编辑允许所选管理员组进行的操作。

   编辑权限的操作见编辑权限一节。
5. 应用更改需点击**保存**。

可采用以下一种方式管理员和管理员组指定父组：

- 按照以上描述的方式更改管理员和管理员组设置。
- 将管理员账户或管理员组移动（drag-and-drop）分层列表中需要指定为父组的组中户。

将管理员权限或管理员组权限分发给另一管理员或管理员组

1. 在管理员列表选择需要分发器权限的对象。可以选择一个管理员或一个管理员组。
2. 在工具面板点击**分发管理员权限**按钮。
3. 在打开的窗口选择需要为其指定权限的对象。请注意以下事项：
   - 可以选择一个或多个需要为其指定权限的对象。可以是管理员，也可以是管理员组。
   - 这些权限将成为所选对象的自身权限。中断从父组继承权限。
   - 不可为默认对象（**Administrators**、**Newbies**、 管理员**admin**）指定权限。
   - 只可为允许**编辑管理员账户**和**编辑管理员组属性和配置**的对象分发权限。
   - 如果分发的权限超过执行分发操作的管理员的自身权限，则不会进行权限分发，返回执行操作权限不足的通知。

4. 点击保存按钮。

第七章、工作站的综合管理

可利用以下工具对工作站进行综合管理：

- 组

  一个工作站可列入的组数量不限。根据工作站状态列入预设组，选择列入用户组。但只有一个组为工作站基组。

- 策略

  为一个工作站只可指定一个策略或不指定任何策略。

- 模式

  模式用于为组件应用程序监控指定设置。模式可以指定给工作站、工作站组，也可指定给个别用户。

  监控工作站应用启用需要为工作站或工作站用户至少指定一个可用模式。

工作站设置类型

- **可继承设置**

  创建工作站时从策略或从基组继承设置。详细信息参见工作站继承配置。

- **自身设置**

  工作站运行过程中可中断继承并指定自身设置。

  为工作站指定自身设置的方式是编辑相应设置。

  工作站指定有自身设置时，策略或基组的设置及其发生的更改都不会再对工作站设置产生影响。

  可以恢复从策略或基组进行继承。操作是点击管理中心相应设置项或工作站属性部分工具面板上的**删除自身设置**。

> 工作站配置元素设置各项都会显示是自身设置还是从相应对象继承的设置。
>
> 可将部分设置项指定为自身设置，部分设置项指定为从策略继承，而在没有策略时从基组继承。

可以为不同的组和工作站指定不同的设置。

7.1. 工作站继承配置

创建工作站或组时总是继承设置：

- 新组从其父组继承设置。如没有父组（所建组为分层列表中的根组），则从组**Everyone**继承设置。
- 创建新工作站时工作站从指定的策略继承设置。如没有指定策略，工作站从其所属的一个组继承设置。这个组称为*基组*。

工作站运行过程中可中断继承并指定自身设置。

应用程序监控组件的设置继承原则有别于标准原则。详见应用程序监控组件的设置继承。

工作站设置应用优先级

1. 如工作站设有自身设置，则应用自身设置。这时可为工作站指定策略。指定有自身设置时中断部分设置的继承。
2. 如没有自身设置，则应用为其指定的策略。
3. 如没有自身设置，也没有指定策略，则使用基组设置。

设有自身设置	指定有策略	使用的设置
+	+	自身设置
+	–	自身设置
–	+	策略中的设置
–	–	基组的设置

可以不给工作站指定任何策略，但工作站必须有基组。

工作站从策略继承设置

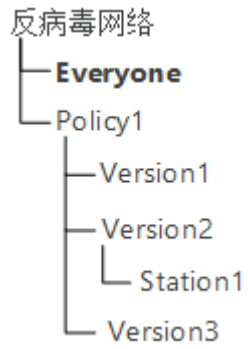
如工作站指定有策略，则工作站从策略继承设置。

策略的设置发生改变时工作站将继承改变，工作站设有自身设置时例外。创建工作站时可为其指定策略。可随时更换策略。如没有指定任何策略，则从基组继承设置。

策略没有分层继承构架。创建策略时其设置复制为相应对象的自身设置（默认为策略**Default policy**）。只有一个版本为策略的当前版本，也只有当前版本的设置为策略的设置。只可为工作站指定当前版本。

例如：

分层列表为以下树结构：



为工作站Station1指定有策略Policy1。版本Version2为策略Policy1的当前版本。版本Version2的设置即为策略Policy1的设置，为工作站自身设置。

工作站从组继承设置

如没有为工作站指定策略，则工作站从其基组继承设置。

基组设置发生改变时这些改变也将由此组中的工作站继承，工作站设有自身设置时例外。创建工作站时可为其指定基组。默认基组为**Everyone**。可随时更换基组。

如果基组不是**Everyone**组，而所指定的基组是反病毒网络分层列表的根组，且没有自身设置，则从**Everyone**组继承设置。

可建立内嵌组。

有内嵌组时如工作站没有自身设置，则配置项按照内嵌组的结构顺序继承。按分层列表自下而上搜索设置，从工作站基组开始到其父组，直到树结构根部。如未发现自身设置，在继承**Everyone**组的配置元素。

例如：

分层列表为以下树结构：



组Group4是工作站Station1的基组。工作站Station1继承设置时将按照以下顺序搜索设置：Station1 → Group4 → Group3 → Group2 → Group1 → Everyone。

默认情况下网络结构显示工作站所属的所有组。如在网络目录中仅显示工作站所属基组，需在管理中心工具面板的**树结构类型设置**取消对**所有组成员**的勾选。

应用程序监控组件的设置继承

应用程序监控模式设置可能不仅指定给了工作站和工作站组，还可能指定给了个别用户或用户组。

设置应用优先级：

1. 存在自定义设置时自定义优先级最高。
2. 无自定义设置时用户组设置为最高优先级。
3. 如没有给用户和用户组指定设置，工作站按工作站设置应用优先级继承设置。

7.2. 组

分组机制用于简化对反病毒网络工作站的管理。

将工作站合并为组可以：

- 在组中所有工作站执行组操作。

  单独选择一个或几个组后可以在组中工作站启动、查看和中断扫描。还可以查看统计信息（包括感染、病毒、启动/结束、扫描和安装错误等等）以及一个组或几个组中所有工作站的汇总数据。
- 通过组为组中工作站进行统一设置（参见第七章、工作站的综合管理）。
- 组织（构架）工作站列表。

还可建立内嵌组。

7.2.1. 系统组和用户组

系统组

Dr.Web Enterprise Security Suite包含几个预设系统组。这些组在安装Dr.Web服务器时创建，且不可删除。但管理员根据需要可以选择不显示预设组。

每一个系统组（**Everyone**组除外）含有一系列具备一定共同特征的子组。

从安装Dr.Web服务器到工作站连接会只显示一个系统组**Everyone**。显示所有系统组需要使用工具面板**树结构设置**部分的**显示隐藏组**一项。

Everyone

此组中包含所有Dr.Web服务器已知的工作站。**Everyone**组包含所有工作站和组的默认设置。

Active Directory

组中为在Active Directory域注册的用户和用户组。执行Dr.Web服务器日程的与**Active Directory同步**任务后此组会出现于反病毒网络树结构中。

Configured

组中为指定有自身设置的工作站。

Neighbors

组**Neighbors**包含所有和本Dr.Web服务器连接的Dr.Web服务器，此组用于管理多Dr.Web服务器反病毒网络中各服务器间的关联（参见多台Dr.Web服务器网络特点）。

如何建立新的服务器间关联详见设置Dr.Web服务器间连接。

组**Neighbors**包含内嵌组，显示与本Dr.Web服务器连接的Dr.Web邻居服务器状态：

- 组**All neighbors**包含所有与本Dr.Web服务器连接的Dr.Web邻居服务器。
- 组**Children**包含Dr.Web子服务器。
- 组**Offline**含有当前不在线的Dr.Web服务器。
- 组**Online**含有当前在线的Dr.Web服务器。
- 组**Parents**包含Dr.Web主服务器。
- 组**Peers**包含同级Dr.Web服务器。

Operating system

此类子组体现的是工作站当前使用的操作系统。这些组不止用于显示，可含有工作站设置，也可以作为基组。

- **Android**家族子组。此家族中每一组对应的是移动设备Android操作系统的具体版本。
- **macOS**家族子组。此家族包括一系列组，每组对应macOS操作系统的具体版本。
- **UNIX**家族子组。此家族包括一系列组，每组对应UNIX家族操作系统，如Linux、FreeBSD等等。
- **Windows**家族子组。此家族包括一系列组，每组对应Windows操作系统的具体版本。
- **Unknown OS**类。这里显示的工作站的操作系统属于Dr.Web服务器未知的操作系统。

Policies

组，内含策略，用于设置工作站。

> 组**Policies**在反病毒网络树结构中显示的前提是Dr.Web服务器配置中允许使用策略。

Profiles

内为OS Windows工作站应用程序监控组件设置模式的组。参见模式。

Proxies

组，内含Dr.Web代理服务器，用于连接代理端和Dr.Web邻居服务器。

Status

Status组含几个内嵌组，这些内嵌组反应的是工作站的当前状态：工作站是否连接Dr.Web服务器，以及反病毒软件的状态：软件是否已删除或者到期。这些状态组只用于显示状态，不能含有任何设置，也不能作为基组。

- **Deinstalled**组。工作站上的Dr.Web代理端软件一被删除，工作站就会移动到**Deinstalled**组。
- 组**Deleted**包含之前由管理员从Dr.Web服务器删除的组。可以恢复此组中的工作站（参见工作站的删除和恢复）。
- **New**组中为管理员通过管理中心创建的工作站，但这些工作站尚未安装代理端。
- **Newbies**组。包含所有当前未被批准在Dr.Web服务器注册的工作站。批准注册或拒绝访问Dr.Web服务器后工作站会自动从此预设组中删除。（详见工作站连接策略）。
- **Offline**组中含有当前所有不在线的工作站。
- **Online**组中含有当前所有在线的工作站（对Dr.Web服务器的请求做出反应）。
- **Update Errors**组中包含反病毒软件的更新出错的工作站。

Transport

此类子组体现的是工作站当前使用哪一协议连接Dr.Web服务器。这些状态组只用于显示状态，不能含有任何设置，也不能作为基组。

- **TCP/IP**组中所含工作站当前使用TCP/IP协议版本4进行连接。
- **TCP/IP Version 6**组中所含工作站当前使用TCP/IP协议版本6进行连接。

Ungrouped

此组所含工作站不包含于任何用户组。

用户组

是反病毒网络管理员为方便管理而创建的组。管理员可以建立自己的组以及内嵌组，并将相应的工作站列入其中。Dr.Web Enterprise Security Suite对用户组的组成、名称没有任何限制。

为便于使用，7-1中归纳了所有组和组的类型，以及特征参数，支持某参数则为（+），不支持则为（–）。

特征参数包括：

- **自动组籍**。此参数说明工作站是否会自动成为该组的成员（即该组是否支持自动组籍），以及在Dr.Web服务器运行过程中该组的组成是否会自动发生变化。
- **管理组籍**。此参数说明管理员是否可以对该组的成员进行管理，即向组中添加新工作站或者将工作站从该组中删除。
- **基组**。此参数说明该组是否可以作为工作站的基组。
- **设置**。此参数说明该组是否可以含有反病毒组件设置（即组中工作站可以继承组的设置）。

表7-1. 组及其支持的参数

组/组类型	参数			
	自动组籍	组籍管理	基组	设置内容
Everyone	+	–	+	+
Configured	+	–	–	–
Operating System	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
Ungrouped	+	–	–	–
用户组	–	+	+	+



在*组管理员*账户下该账户管理的用户组将显示为树结构根组，即便是该组实际上有父组。这时可以访问此组的所有子组。

7.2.2. 组管理

7.2.2.1. 组的创建与删除

创建新组

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在工具面板选择**添加网络对象**，然后在子菜单中选择**创建组**。

打开组创建窗口。

3. **识别码**一栏为自动填写。必要时在创建过程中可以对识别码进行编辑。识别码中不应有空格。组创建后将不可再更改其识别码。
4. 在**名称**一栏输入组的名称。
5. 如果是内嵌组则应在**父组**一栏从下拉列表中选择新建组的父组。新组若没有自身设置，则从父组继承设置。根组（没有父组）此栏为空，根组会添加到分层列表根部，并从**Everyone**继承设置。
6. 可在**描述**一栏输入需要的说明。
7. 点击**保存**按钮。

您所创建的组一开始为空组。向组中添加工作站参见将工作站添加到组。

删除现有组

1. 在管理中心分层列表中选择需要删除的用户组。
2. 在工具面板点击**常规** → **删除所选对象**。

> 预设组不可删除。

7.2.2.2. 编辑组

编辑组设置

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中选择组。
2. 用以下方式打开组属性页面：
   a) 点击反病毒网络分层列表中的组名称。早管理中心窗口右侧会自动打开组属性。
   b) 选择控制菜单的**属性**一项。打开组属性窗口。
3. 组属性窗口包含**常规**和**配置**。其内容和设置见下。

> 在管理中心右侧窗口打开组属性（参见**2.a)**）后可以访问**工作站信息**，查看该组成员的总体信息。

4. 点击**保存**按钮保存修改。

常规

常规部分包括以下信息：

- **识别码**——组的独有识别码。不可编辑。
- **名称**——组的名称。必要时可以更改用户组的名称。预设组的**名称**一栏不可编辑。
- **父组**——该组所属父组。若该组没有自身设置，则从父组继承设置。如没有父组，该组将从**Everyone**组继承设置。
- **描述**——组描述，非必填项。

工作站信息

工作站信息部分包括以下信息：

- **工作站**——该组中包含的工作站总数。
- **为基组**——所选组为基组的工作站数量。
- **在线工作站**——所选组中当前在网络的工作站的数量（online）。

单位

如创建组时将其设为单位或公司，则可编辑**单位**部分。在这一部分可编辑此组所代表的单位的相关信息。单位所在国家不同，相关信息也会有所不同。



只可在创建组时将其指定为某单位。创建后不可取消。

配置



工作站如何从基组继承设置详见第七章、工作站的综合管理。

在**配置**部分可以更改此组的配置，包括：

图标	设置	描述部分
	此组为基组的工作站从此组继承的工作站用户权限。设置组权限与设置工作站权限相同。	工作站用户权限
	此组为基组的工作站从此组继承的工作站任务统一启动日程。设置组日程与设置工作站日程相同。	工作站任务日程
	以此组为基组的工作站的授权密钥。	授权密钥
	此组为基组的工作站从此组继承的工作站反病毒软件更新限制。	工作站更新限制
	此组为基组的工作站从此组继承的工作站可安装组件列表。 编辑组的组件列表与编辑工作站的组件列表相同。	可安装的反病毒软件包组件
	自动将工作站添加至此组的规则。只适用于用户组。	自动组籍设置
	反病毒软件包组件设置。设置组的反病毒软件包组件与设置工作站组件相同。	设置反病毒组件

对设有自身设置的组，在**配置**部分显示中断继承和有自身设置的内嵌组数量。点击此选项后会打开组列表，显示组名称和识别码。

7.2.3. 将工作站添加到组

指定基组

为工作站或工作站组指定基组有几种方式：

为工作站设置基组

1. 在主菜单中选择**反病毒网络**一项，在打开窗口的分层列表中点击工作站名称。
2. 打开工作站属性面板。也可通过在控制菜单选择**属性**一项打开工作站属性。在打开的窗口进入**组**一项。
3. 更改基组的操作是在**组籍**部分点击相应组的图标。这时组图标上会出现**1**。
4. 点击**保存**按钮。

为几个工作站设置基组

1. 在主菜单中选择**反病毒网络**一项，在打开窗口的分层列表中点击工作站名称（也可以选择组，这时操作将适用于这些组中的所有工作站）。选择几个工作站或组可以按住CTRL或SHIFT键用鼠标选择。
2. 在工具面板点击**常规** → **为工作站指定基组**。打开的窗口是可以设置为所选对象基组的所有组的列表。
3. 点击要设为基组的组的名称。

可以把一个组设为其所属所有工作站的基组。操作是在目录中选出需要设为基组的组，然后在管理中心工具面板点击**常规** → **将此组设为基组**。

添加到用户组

Dr.Web Enterprise Security Suite中设有以下两种将工作站添加到用户组的方式：

1. 将工作站手动添加到组。
2. 利用组籍规则自动添加。

7.2.3.1. 将工作站手动添加到组

有几种方式可将工作站添加到用户组中：

1. 更改工作站设置。
2. 在分层列表中移动工作站 （drag-and-drop）。

通过工作站设置来编辑其所属组

1. 在主菜单中选择**反病毒网络**一项，在打开窗口的分层列表中点击工作站名称。
2. 打开工作站属性面板。也可通过在控制菜单选择**属性**一项打开工作站属性。
3. 在打开的**工作站属性**面板转至**组**标签。

   组籍中列出的是此工作站目前所属的工作站组和可以归属的工作站组。

4. 向用户组添加工作站时需在**组籍**中勾选此组。
5. 从用户组删除工作站时需在**组籍**中取消对此组的勾选。

> 不可从预设组中删除工作站。

6. 点击**保存**按钮保存修改。

在工作站**属性**页面还可以为工作站指定基组（详见工作站继承配置元素，基组）。

通过分层列表来编辑工作站所属组

1. 在主菜单选择**反病毒网络**，展开组和工作站分层列表。
2. 添加工作站时需按下CTRL键，利用鼠标将工作站移动至需要将其添加为成员的组（drag-and-drop）。
3. 如果需要将工作站从一个用户组移至另一个用户组，需利用鼠标将工作站从原所在组移动至需要将其添加为成员的组（drag-and-drop），这时工作站从原所在组删除。

> 上述2、3两种方式移动预设组中的工作站时，工作站都只会添加到用户组，而不会从预设组删除。

7.2.3.2. 自动组籍设置

Dr.Web Enterprise Security Suite可以设置自动将工作站添加到用户组的规则。

指定自动将工作站添加到用户组的规则

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在反病毒网络分层列表选择需要为其创建组籍规则的用户组。
3. 打开组籍规则编辑页面，打开的方式有：
   - 在窗口右侧的组属性面板的**配置**部分点击**组籍规则**。
   - 在控制菜单的**常规**部分选择**组籍规则**。
   - 在控制菜单的**常规**部分选择**属性**，进入**配置**标签后点击**组籍规则**。
4. 在打开的查看设置工作站列入本组的条件：
   a) 如之前未曾为该组指定成员规则，点击**添加规则**。
   b) 勾选**指定此组为基组**后，为其创建规则的组会自动成为按照所指定的规则列入该组的所有工作站的基组。
   c) 为每个规则需指定以下设置：
      - 选择作用于一个规则阵列的原则：**符合所有条件**、**符合任一条件**、**不符合任何条件**。
      - 在下拉条件列表选择：要检查是否符合条件的工作站参数；符合此条件的原则，如指工作站参数，请输入条件。
        工作站可按以下条件归组：
        工作站IP地址（IP地址的字符串、所在子网或正则表达式）；
        - **工作站描述** （描述中所含字符串或正则表达式）；

- **工作站ID** （ID中所含字符串或正则表达式）；
- **新工作站** （工作站按照是否为新工作站添加到组）；
- **Active Directory中的LDAP DN** （LDAP DN中所含字符串或正则表达式）；

指定参数**Active Directory的LDAP DN**时必须：

1. 在Dr.Web服务器日志启用任务与**Active Directory**同步（在管理→**Dr.Web**服务器任务计划器部分）。
2. 在组籍规则将**Active Directory的LDAP DN**的条件行指定为所需DN值，例如：
   `OU=OrgUnit,DC=Department,DC=domain,DC=com`

只可在**符合正则表达式**时给出正则表达式。其他类型值按照完全符合输入行内容进行搜索。

正则表达式使用方法简介见**附录**中的附录J. Dr.Web Enterprise Security Suite中正则表达式的使用。

- **操作系统**，安装于工作站（Windows、UNIX、macOS、Android等，还有一个参数是"未知"）；
- **操作系统版本序号** （编号所含编码或正则表达式）；
- **工作站平台** （安装于工作站的操作系统版本；仅限Android、Windows和macOS）；
- **连接协议** （TCP IP、TCP IPv6、UNIX）；
- **Dr.Web服务器ID** （ID中所含字符串或正则表达式）；
- **工作站名称** （字符串，包含于名称或正则表达式）；
- **工作站类型** （全代理端、虚拟代理端和扫描服务器）。

▫ 在本阵列添加新条件需点击条件行右侧的。

d) 添加新阵列需点击阵列右侧的。这时需制定此阵列与其他阵列的合并原则：

▫ **和**——应同时满足所有阵列的条件。

▫ **或**——需满足至少一个阵列的条件。

5. 保存并应用规则需点击以下一个按钮：
   - **现在应用**——保存组籍规则并立即应用于本Dr.Web服务器注册的所有工作站。如连接Dr.Web服务器的工作站较多，执行这一指令会占用一定时间。重组工作站的规则会立即应用于所有已注册的工作站，并将在工作站连接时应用于所有工作站，包括首次在Dr.Web服务器注册的工作站。
   - **在工作站连接时应用**——保存组籍规则并在工作中连接Dr.Web服务器时应用。重组工作站的规则会在所有已注册的工作站下次连接Dr.Web服务器时应用，并将在Dr.Web服务器新注册的工作站进行第一次连接时应用。
6. 为用户组指定了自动组籍规则后反病毒网络分层列表中该组图标旁会出现图标，前提是在工具面板 **树结构设置**勾选了**显示组籍图标**。

如工作站是按照组籍规则自动添加到用户组的，则进行手动删除没有任何意义，因为下一次连接Dr.Web服务器时工作站还会自动添加到这一工作组。

删除自动将工作站添加到用户组的规则

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在反病毒网络分层列表选择需要为其删除组籍规则的用户组。
3. 执行以下一种操作：
   - 在工具面板点击**删除组籍规则**。
   - 在窗口右侧的组属性面板的**配置**部分点击**删除组籍规则**。
   - 在控制菜单的**常规**部分选择**属性**，进入**配置**标签后点击**删除组籍规则**。
4. 删除组籍规则后所有按照规则列入用户组的工作站会从组中删除。如果管理员曾将此用户组指定为某些工作站的基组，则从组中删除工作站时会将其基组指定为**Everyone**。

7.2.4. 对比组和工作站

可以进行组和工作站基本参数对比。

对比反病毒网络中的一些对象

1. 选择主菜单中的**反病毒网络**一项，在打开的分层列表中选择需要进行对比的对象。选择使用CTRL和SHIFT按键。有几种方式：
   - 选择几个工作站——用于对比所选工作站；
   - 选择几个组——用于对比所选组和其所有内嵌组；
   - 选择几个工作站和组——用于对比所有工作站：既包括直接在分层列表中选出的工作站，也包括所有选出的组及其内嵌组中所包含的工作站。
2. 在控制菜单点击**对比**。
3. 打开所选对象的对比表。
   - 组对比参数：
     - **工作站**——该组中包含的工作站总数。
     - **在线工作站**——当前处于活动状态的工作站数量。
     - **为基组**——所选组为基组的工作站数量。
     - **自身设置**——指定有自身设置（不是从父组继承的设置）的组件列表。
   - 工作站对比参数：
     - **工作站**创建日期。
     - **工作站的基组**。
     - **自身设置**——指定有自身设置（不是从父组继承的设置）的组件列表。
     - **已安装组件**——已安装于此工作站的反病毒组件列表。

7.2.5. 将设置复制到其它组/工作站

病毒工具设置、日程设置、用户权限以及组或工作站的其它设置都可以复制到（传播）到其它组或工作站。

复制设置

1. 点击**将设置适用于另一对象**按钮：
   在反病毒组件配置编辑窗口；
   在日程编辑窗口；
   在更新限制设置窗口；
   在可安装的组件窗口；
   在工作站用户权限设置窗口。
   打开反病毒网络分层列表。
2. 在列表中选择组和工作站，以便将设置复制到所选对象。
3. 点击**保存**按钮，以便更改所选对象的设置。

7.3. 策略

*策略*为工作站存在的所有设置总和：权限、任务日程、授权密钥、更新限制、可安装组件列表、反病毒组件配置。



策略只可指定给工作站。

允许使用策略来设置工作站

1. 在管理中心主菜单选择**管理**，在打开的窗口选择控制菜单中的**Dr.Web服务器配置**一项。
2. 在**常规**标签：
   a) 勾选**使用策略**。
   b) 在**策略版本数量**一栏指定可为每一策略建立的最多版本数量。如创建策略新版本时已超过次数量，则会删除最早的策略版本。
3. 应用更改需点击**保存**按钮后重新启动Dr.Web服务器。
4. 允许使用策略后创建预设策略**Default policy**。此策略不可删除，但可以编辑并指定给工作站。



预设策略**Default policy**位于系统组**Policies**，默认改组为隐藏。在反病毒网络分层列表中显示此组需在工具面板勾选**树设置 → 设置 → 显示隐藏组**。



管理策略及其设置要求管理员具备**查看策略属性和配置**和**编辑策略属性和配置**权限。

如没有指定相应权限，则反病毒网络树结构和授权管理器将显示策略，但无法查看策略内容，也不可对策略进行管理。

7.3.1. 策略管理

创建策略

创建新策略

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在工具面板选择**添加网络对象**，然后在子菜单中选择**创建策略**。

   打开策略创建窗口。
3. **识别码**一栏为自动填写。必要时在创建过程中可以对识别码进行编辑。识别码中不应有空格。策略创建后将不可再更改其识别码。
4. 在**名称**一栏输入策略名称。
5. 创建策略时从**Default policy**复制默认设置。更改复制设置的来源对象需点击**选择另一对象**。在打开的窗口选择列表中的一个对象。可以是组、工作站、另一策略或策略另一版本。只可选择一个对象。点击**点击**。策略创建窗口显示所选对象。
6. 点击**保存**按钮后按指定参数创建策略。
7. 创建策略时自动创建策略版本，对应策略添加时间。

策略版本

策略可有多个版本，但数量不会超过Dr.Web服务器配置中指定的数量。版本名称对应创建时间。

创建策略新版本

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 利用反病毒网络分层列表可访问策略设置。可编辑策略配置创建新版本。可手动编辑或导入/分发反病毒网络另一对象（工作站、组、策略）的配置。
3. 保存更改时会以指定的策略设置自动创建策略新版本。创建的版本会被指定为当前版本。



只有一个策略版本为当前版本，可指定给工作站。

策略版本设置为只读。

更改当前策略版本

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在分层列表选择需更改当前版本的策略。
3. 在打开的策略属性面板的**常规**部分的**当前版本**下拉列表选择所需版本。

4. 点击**保存**按钮。

删除策略

可整体删除策略，也可删除其版本。

删除策略或策略版本

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在分层列表选择一个策略或策略版本。
3. 在工具面板点击**常规** → **删除所选对象**。

删除策略时需注意以下事项：

- 删除策略的最后一个版本时策略也随之删除。
- 删除当前版本时，上一版本（日期最近）成为当前版本。
- 策略版本被删除的所有工作站将使用此策略的当前版本。

7.3.2. 为工作站指定策略

为一个工作站只可指定一个策略。

只可为工作站指定指定有授权密钥的那一策略。

为工作站指定或更改策略

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在分层列表选择需为其指定或更改策略的工作站。
3. 在打开的工作站属性面板**组**标签的**策略**列表勾选需要指定的策略。
   这时自动取消对之前为工作站指定的策略的勾选，因为一个工作站只可指定一个策略。
   可取消所有勾选。这时工作站恢复指定策略前的设置。
4. 点击**保存**按钮。

7.4. 模式

*模式*决定组件应用程序监控的设置，将根据这些设置在工作中阻止或允许应用程序、模块、脚本编译器、驱动程序和MSI包。

模式由管理员创建并指定给策略、工作站或用户，包括工作站组和用户组。模式决定应用程序监控的运行模式。

设置模式需利用反病毒网络的树结构：

- 所有模式列于预设组**Profiles**。
- 为其指定了具体模式的对象在反病毒网络树结构中成为此模式的子元素。

设置应用程序监控

1. 创建新模式。
2. 指定模式设置。
3. 请将模式指定给相应对象。



建议在测试模式下设置模式。

有以下几种模式运行方式：

- 停用——不使用模式设置。
- 活跃——模式设置应用于为其指定了此模式的对象。
- 全面*测试*——模式处于全面测试状态。测试状态下模拟应用程序监控运行，全面记录事件日志（参见应用程序监控事件），但实际上并不阻止应用。
- 测试*规则*——模式处于活跃状态，但只将功能分析和规则设置运用到对象。但测试模式下的规则不会影响应用的使用。规则模拟运行的结果记录到事件日志（参见应用程序监控事件）。可在允许性和禁止性规则设置部分启用或停用规则测试状态。

下表为某些设置会指定各模式运行状态

方式 设置	已停用	活跃状态	测试*全面*	测试*规则*
常规 → 启用模式	–	+	+	+
常规 → 将模式转为全面测试状态	不活跃	–	+	–
<方式> → *<规则>* → 启用规则	不活跃	+/–	+/–	+
<方式> → *<规则>* → 将规则转为测试状态	不活跃	–	+/–	+

标志说明

+	设置应为启用
–	设置应为停用
+/–	设置无效
不活跃	设置不可编辑

7.4.1. 创建和指定模式

创建新模式

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在打开窗口的工具面板选择**添加网络对象**→**创建模式**。
3. 在打开的面板指定**模式名称**。之后如需可在常规设置部分更改名称。
4. 点击**保存**按钮。
5. 新模式创建后移至**Profiles**。

将模式指定给对象

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在打开窗口的分层列表选择需要指定的模式。
3. 在工具面板点击**导出数据**→**指定模式**。

   在打开的窗口选择需为其指定模式的对象：

   - **Active Directory**标签的列表与反病毒网络树结构中按照Dr.Web服务器日程的与**Active Directory同步**任务进行更新的列表类似。这两种列表包含相同对象，但将为其指定模式的对象的类型有所区别。
     - 在**Active Directory工作站**列表可以选择在Active Directory域注册的工作站组或个别工作站。
     - 在**Active Directory用户**列表可以选择在Active Directory域注册的用户组或个别用户。

   不可再不同列表选择相同的对象。

   - 在**反病毒网络**标签可选择以下对象：
     - 工作站组。这时设置将应用到所选组的所有工作站的所有用户的账户。
     - 工作站组的个别工作站。这时设置将应用到所选工作站的所有用户的账户。
     - 组**Policies**中策略。这时设置将应用到被指定所选策略的工作站的所有用户账户。
   - 在**本地用户**标签可选择组用户或工作站的个别用户。这时设置将只应用到相应工作站的所选用户账户。

   指定模式时的优先级详情请参阅 应用程序监控组件的设置继承。
4. 点击**保存**按钮。所有所选对象将添加到将应用此模式的对象列表（在树结构中显示为此模式的内含对象）。

停止将模式设置应用到对象

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在打开窗口的分层列表打开模式内含对象列表，选择需要取消应用模式的对象。
3. 在工具面板点击**常规**→**取消为对象指定模式**。

7.4.2. 模式设置

编辑模式设置

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 用以下方式打开模式属性页面：
   a) 点击反病毒网络分层列表中的模式名称。在管理中心窗口右侧会自动打开模式属性面板。
   b) 点击反病毒网络树结构中的模式按钮或选择模式，然后选择控制菜单的**属性**一项。打开模式属性窗口。
3. 在**常规**部分指定模式运行原则：
   - 在**模式名称**可更改模式名称。
   - 勾选**启用模式**后开始使用此模式。
     - 勾选**将模式转为全面测试状态**后将只记录活动日志。日志记录会和启用设置时一样，可利用此项来调试模式的运行情况。
   - 在功能分析标准指定预设规则集，满足此规则集经允许或禁止应用启动。
4. 执行在**常规**部分给出的设置需在模式设置点击**保存**。
5. 在**允许性方式**部分列出的是模式设置总表：已创建允许性规则数量和为此模式指定的可信任的应用程序组数量。启用或停用此方式或设置规则和可信任的应用程序需点击允许性方式链接进入相应的部分。
6. 在**禁止性方式**部分列出的是模式设置总表：已创建禁止性规则数量。启用或停用此方式或设置规则和可信任的应用程序需点击禁止性方式链接进入相应的窗口。

需注意应用程序监控模式的以下特点：

- 如**功能分析依据的标准**没有启用任何标准，则模式本身也会停用。
- 如设置模式时**功能分析依据的标准**中没有为任何标准指定高级设置并停用了禁止和允许，则设置无法保存。
- 如未指定允许性规则，也没有指定可信任的应用程序，则会停用允许性方式。
- 如未给出禁止性规则，会停用禁止性方式。

7.4.2.1. 功能分析

在*功能分析*指定预设规则集，根据规则允许或禁止应用启动执行相应功能。

可在模式属性的**常规 → 功能分析依据的标准**。



如**功能分析依据的标准**没有启用任何标准，则模式本身也会停用。

如**功能分析依据的标准**没有为任何标准指定高级设置并停用了禁止和允许，则模式本身也会停用。

设置应用功能分析的操作

1. 在**功能分析依据的标准**勾选需要使用的标准：
   - **启动应用程序**，
   - **加载和执行模块**，
   - **启动脚本解释器**，
   - **加载驱动程序**，
   - **安装MSI数据包**，
   - **可执行程序完整性**。

   如果是第一次设置模式，勾选每一标准时其高级设置中会自动启用其允许性方式。

   自动启用是为了增强安全性，防止使用允许性或禁止性方式后工作站运行所必需的操作系统对象被阻止。

   如需之后可在高级设置中会停用这些允许性方式。

2. 为所选标准指定高级设置需点击相应标准旁的**编辑**。打开设置列表。

   功能分析的设置可以用于允许启动应用，也可以用于禁止启动应用。

   勾选需要的设置。

3. 无启用了某标准，但没有指定高级设置，则会使用这一标准按照相应的允许性或禁止性方式设置监控所有对象。

   例如：

   - 如指定的标准是**启动脚本解释器**，但没有给出高级设置，则会按照相应的允许性或禁止性方式设置监控所有脚本解释器的启动。
   - 如指定的标准是**启动脚本解释器**，且高级设置为**禁止从移动载体启动场景**，则只禁止从移动载体启动脚本。

4. 如果给出了高级设置，但没有启用标准，则高级设置以及标准本身都不会得到执行。
5. 保存高级设置需在高级设置列表窗口点击**保存**。
6. 保存功能分析设置需在模式设置窗口点击**保存**。

7.4.2.2. 允许性方式

*允许性方式*意味着在所有受监控的工作站只允许启动**可信任的应用程序**列表中的应用和符合允许规则的应用。其他应用都会被禁止。

只使用允许性规则时也可启用允许性模式。在这种情况下只是作为功能分析的补充，允许启用禁止列表中的某些应用。例如，如果在功能分析中指定禁止从网络和共享资源启用应用，但在允许性规则中指定允许某一应用，则可以在禁止其他应用的同时允许此应用运行。

可在模式属性部分的**允许性方式**标签编辑允许性规则和可信任的应用。

使用允许性方式

1. 在**允许性方式**标签勾选**使用允许性方式**。
2. 至少要在以下一个部分给出设置：
   - 允许性规则。
   - 可信任的应用程序。
3. 点击**保存**。

如未指定允许性规则，也没有指定可信任的应用程序，则会停用允许性方式。

允许性规则

可在模式属性部分的**允许性方式 → 允许性规则**编辑允许性规则。

创建新的允许性规则

1. 在**允许性规则**点击工具面板的➕**创建规则**。
2. 早**添加规则**窗口给出**规则名称**后点击**保存**。
3. 在规则列表选择新建的规则，在打开的属性面板给出设置：
   a) 勾选**启用规则**后开始使用此规则。
   b) 如需检查规则的运行情况，需勾选**将规则设为测试状态**状态。此状态下不会在工作站监控应用，但会和启用规则一样记录事件日志。规则测试模式下对应用的启动和阻止结果会体现于应用程序监控事件。
   取消对**将规则转为测试状态**的勾选后，规则为活跃状态，按照其设置在工作站启用应用（参见模式运行模式）。
   c) 在**按以下标准允许应用启动**部分选择允许在工作中启动应用依据的选项。

请在**文件名称**一栏输入文件或文件夹的名称。支持变量和掩码。如未指示路径，则此参数为处于任意位置的此名称文件。

还可在应用程序监控事件和应用程序手册在从工作站获取的数据的基础创建允许性规则。这种情况下规则中的应用参数会自动填写。

4. 点击**保存**。

创建允许性规则副本

1. 在**允许性规则**的规则列表选择需建立副本的规则。
2. 在工具面板点击**规则副本**。
3. 规则列表出现新工作，其设置从步骤1所选规则复制。规则名称中添加数字**1**。

删除允许性规则

1. 在**允许性规则**的规则列表选择需删除的规则。
2. 在工具面板点击**删除规则**。

可信任的应用程序

如使用可信任的应用程序，需执行以下一种操作：

- 如将在您的Dr.Web服务器收集可信任的应用程序（参见可信任应用程序库），需在管理中心的**管理** → **应用程序监控** → **可信任的应用程序**激活对可信任应用的信息收集。
- 如可信任的应用程序是按照服务器间连接从Dr.Web邻居服务器发送至此Dr.Web服务器，需在发送和接收**可信任的应用程序**的Dr.Web服务器库中给出相应设置。

可在模式属性部分的**允许性方式** → **可信任的应用程序**编辑此模式的可信任应用程序。

打开列表是为此模式指定的所有可信任的应用程序组。

可信任的应用程序组（或应用程序白名单）是按照指定标准从所选工作站或工作站组收集的应用程序列表。为其将此模式知道为允许模式的反病毒网络工作站上可以启动这些应用。



如您的Dr.Web服务器是按照服务器间协议从Dr.Web邻居服务器获得可信任的应用程序（参见可信任应用程序库），则组列表会出现带有图标 ! 的记录**服务器库中不存在此可信任应用程序组**。有这样记录的是从产品**可信任的应用程序**上一校检添加的组，而添加后获得的新校检中不包含这些组。应用程序在相应工作站上的运行可能并不受影响，但为防止模式运行出现问题起见，建议从模式设置中删除这样的组。

向模式添加可信任的应用程序组

1. 在**可信任的应用程序**部分的工具面板点击**向模式添加可信任的应用程序组**。
2. 打开的窗口为所有可选的可信任的应用程序组。



设置允许性方式时从库中对于产品**可信任的应用程序**可选的组列表中选择可信任应用程序组。

3. 勾选需要添加到模式的应用程序组。
4. 点击**保存**。

从模式删除可信任的应用程序组

1. 在**可信任的应用程序**列表勾选需要从此模式删除的应用程序组。
2. 在工具面板点击**删除可信任的应用程序组**。
3. 此组应用会从为其指定此模式的工作站允许启动的应用列表中删除。

从模式删除后可信任的应用程序组本身并不会被删除，仍保留在库中，并可以重新添加到此模式或其他模式。

7.4.2.3. 禁止性方式

*禁止性方式*意味着在所有受监控的工作站只禁止启动符合禁止规则的应用。其他应用都允许使用。

可在模式属性部分的**禁止性方式**标签编辑禁止性规则。

使用禁止性方式

1. 在**禁止性方式**标签勾选**使用禁止性方式**。
2. 按照下面介绍的步骤创建禁止性规则。
3. 点击**保存**。

如未给出禁止性规则，会停用禁止性方式。

创建新的禁止性规则

1. 在**禁止性规则**点击工具面板的➕**创建规则**。
2. 早**添加规则**窗口给出**规则名称**后点击**保存**。
3. 在规则列表选择新建的规则，在打开的属性面板给出设置：
   a) 勾选**启用规则**后开始使用此规则。
   b) 如需检查规则的运行情况，需勾选**将规则设为测试状态**状态。此状态下不会在工作站监控应用，但会和启用规则一样记录事件日志。规则测试模式下对应用的启动和阻止结果会体现于应用程序监控事件。
   取消对**将规则转为测试状态**的勾选后，规则为活跃状态，按照其设置在工作站禁止应用（参见模式运行状态）。
   c) 在**按以下标准禁止应用启动**部分选择允许在工作中禁止应用依据的选项。

请在**文件名称**一栏输入文件或文件夹的名称。支持变量和掩码。如未指示路径，则此参数为处于任意位置的此名称文件。

还可在应用程序监控事件和应用程序手册在从工作站获取的数据的基础创建禁止性规则。这种情况下规则中的应用参数会自动填写。

4. 点击**保存**。

创建禁止性规则副本

1. 在**禁止性规则**的规则列表选择需建立副本的规则。

2. 在工具面板点击**规则副本**。
3. 规则列表出现新工作，其设置从步骤1所选规则复制。规则名称中添加数字**1**。

删除禁止性规则

1. 在**禁止性规则**的规则列表选择需删除的规则。
2. 在工具面板点击**删除规则**。

第八章、工作站的管理

在Dr.Web Enterprise Security Suite控制下的反病毒网络可以对工作站上的反病毒软件包进行统一设置。Dr.Web Enterprise Security Suite可以：

- 设置反病毒组件参数配置；
- 设置扫描日程；
- 在工作站启动日程设置以外的任务；
- 启动工作站更新进程，包括更新发生错误后取消错误状态重新更新。

同时反病毒网络管理员既可以允许工作站用户自行进行设置和启动任务，也可以禁止用户的参与或者在很大程度上加以限制。

在Dr.Web服务器暂时无法访问工作站时，也可以更改工作站组配置。这些更改在工作站恢复与Dr.Web服务器的连接后即会生效。

8.1. 对工作站账户的管理

8.1.1. 工作站连接策略

通过管理中心创建工作站的操作见**安装手册**中的创建新账户。

管理工作站登录Dr.Web服务器取决于以下一些参数：

1. 如果在工作站安装代理端时取消了对在**Dr.Web服务器手动登录**的勾选，则工作站登录Dr.Web服务器的模式将遵照在服务器上给出的相应设置 （为默认设置），见下。
2. 如果在工作站安装代理端时选择的登录方式为**在服务器手动登录**，且设有**识别码**和**密码**，则在连接Dr.Web服务器时工作站都会自动进行登录，而不取决于Dr.Web服务器的设置 （使用`drweb_ess_<OS>_<工作站>.exe`安装包安装代理端时的默认设置。参见**安装手册**的安装文件）。

如何在安装代理端时指定其登录方式参见**用户手册**。

更改工作站登录**Dr.Web** 服务器的模式

1. 打开Dr.Web服务器配置。操作是在主窗口选择**管理**，在打开的窗口选择控制菜单中的**Dr.Web服务器配置**。
2. 在**常规**标签**新工作站注册模式**下拉列表选择一个模式：
   - **手动批准访问**（如在安装Dr.Web服务器时未作更改，此模式为默认模式），
   - **总是拒绝访问**，
   - **自动允许访问**。

手动批准访问

在**手动批准访问**模式下新工作站移至组**Status**的系统子组**Newbies**，需管理员直接处理。

更改工作站登录**Dr.Web**服务器的模式

1. 在管理中心主菜单选择**反病毒网络**。在反病毒网络树结构中选择**Status** → **Newbies**中的工作站。

   可在反病毒网络访问组**Status** → **Newbies**需满足以下条件：

   1. 在**管理** → **Dr.Web**服务器配置 → **常规**部分的**新工作站注册模式**设置为**手动批准访问**。
   2. 管理员具备**批准新工作站**的权限。

2. 设置对Dr.Web服务器的访问需在工具面板**未批准的工作站**选择对所选工作站的操作：

   允许所选工作站访问并指定基组——批准工作站访问Dr.Web服务器，并从列表中为工作站指定基组。

   取消应在连接时执行的操作——为未获得批准的工作站取消之前指定的在工作站连接Dr.Web服务器时应执行的操作。

   拒绝所选工作站访问——禁止工作站访问Dr.Web服务器。

拒绝访问

在**总是拒绝访问**模式下Dr.Web服务器会拒绝新工作站的访问请求。管理员需手动创建工作站记录并为其设置访问密码。

自动允许访问

在**自动允许访问**模式下所有申请访问Dr.Web服务器的工作站都自动进行连接，不需管理员批准。这时将**Dr.Web服务器配置常规**标签**基组**下拉列表中的组指定为工作站基组。

8.1.2. 工作站的删除和恢复

删除工作站

删除工作站记录

1. 在主菜单选择**反病毒网络**。
2. 在打开窗口的分层列表选择需要删除的一个或几个工作站。
3. 在工具面板点击**常规** → **删除所选对象**。
4. 打开确认删除工作站窗口。点击**确定**按钮。

工作站从分层列表中删除后已知已删除工作站列表，通过管理中心可恢复此列表中的工作站。

恢复工作站

恢复工作站记录

1. 在主菜单选择**反病毒网络**，在打开窗口选择需要恢复的一个或几个工作站。

> 所有已删除的工作站处于**Status**组中的子组**Deleted**。

2. 点击工具面板的**常规** → **恢复已删除的工作站**。
3. 打开工作站恢复页面.可以在恢复工作站时设置以下参数：
   - **基组**——选择工作站恢复后所属的基组。默认值是删除前工作站的基组。

> 同时恢复几个工作站时默认情况下选择的是**原基组**，即每一工作站都将添加到其删除前所在基组。选择某个组时，所有要恢复的工作站都指定为此组。

   - 在**组籍**部分可以更改工作站所属组列表。默认为删除前工作站所属组。在**组籍**中所列是工作站可以归属的组，通过勾选确认工作站组籍。
4. 点击**恢复**按钮后以设定的参数恢复工作站。

8.1.3. 合并工作站

在对数据库进行操作或反病毒工作站上重新安装软件时在分层列表中可能会出现几个有相同名称的工作站（其中只有一个对应相应的工作站）。

去除重复出现的工作站名称

1. 利用CTRL按键选出同一工作站的所有名称。
2. 在工具面板中选择 **常规** → **合并工作站**。
3. 在列中选出认为是主要工作站的一项。其他工作站将被删除，其描述将归于所选工作站。
4. 在列中选择其设置将归于所选主工作站的一个工作站。
5. 点击**保存**按钮。

8.2. 工作站常规设置

8.2.1. 工作站属性

查看、编辑工作站属性

1. 在管理中心主菜单选择**反病毒网络**，在打开的窗口分层列表中选择工作站。
2. 用以下方式打开工作站属性页面：
   a) 点击反病毒网络分层列表中的工作站名称。在管理中心窗口右侧会自动打开工作站属性。

b) 选择控制菜单的**属性**一项。打开工作站属性窗口。

3. 工作站属性窗口包含几组参数，分别是：**常规**、**配置**、**组**、**安全策略**、**位置**。其内容和设置见下。
4. 点击**保存**按钮保存修改。

删除工作站自身设置

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中选择工作站，然后点击工具面板上的**常规** → **删除自身设置**。打开此工作站设置列表，自身设置有旗标。
2. 保留需要删除的自身设置的旗标。留作自身设置的需取消其旗标。点击**删除**按钮。保留旗标的设置将恢复为从基组继承设置。

8.2.1.1. 常规

常规部分以下栏目为只读：

- **工作站识别码**——工作站独有代码。在创建工作站账户时给出，之后无法更改。
- **名称**——工作站名称。在创建工作站账户时给出。代理端连接后会自动替换为计算机名称。
- **创建日期**——在Dr.Web服务器创建工作站账户的日期。
- **安全识别码**——OS Windows用户账户独有安全代码（SID——security identifier）。OS Windows工作站连接Dr.Web服务器后自动给出。
- **LDAP DN**——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。工作站连接Dr.Web服务器后自动给出。
- **MAC地址**——工作站MAC地址。工作站连接Dr.Web服务器后自动给出。
- **上次连接日期**——工作站上次连接Dr.Web服务器的日期。

可以指定或更改以下输入栏：

- 在**密码**一栏指定工作站登录Dr.Web服务器的密码（必须在**确认密码**一栏重复输入此密码）。更换密码时，为连接代理端起见，需在工作站的代理端连接设置中重复此操作。
- 在**描述**一栏输入工作站补充信息。



有*标志的输入栏必须填写。

此部分还包含以下链接：

- 在**安装文件**一项是此工作站代理端安装程序下载链接。

  创建新工作站后和未指定工作站操作系统之前在软件下载部分分别列出Dr.Web Enterprise Security Suite支持的操作系统的相应链接。
- 在**配置文件**一项是OS Android、macOS和OS Linux下工作站连接Dr.Web服务器设置文件下载链接。

8.2.1.2. 配置

在**配置**部分可以更改工作站的配置，包括：

图标	设置	描述部分
	工作站用户权限	工作站用户权限
	工作站任务统一启动日程	工作站任务日程
	工作站授权密钥	授权密钥
	反病毒软件更新限制	工作站更新限制
	可安装组件列表	可安装的反病毒软件包组件
	此工作站的反病毒软件包组件设置	设置反病毒组件

管理中心还有用于删除自身设置的按钮。这些按钮位于其所对应的设置按钮右侧。删除自身设置后工作站将重新获得从基组继承的配置。

更改SpIDer Gate和/或办公控制设置时需注意，这两个组件互相关联，如利用**删除自身设置**按钮删除了其中一个组件的自身设置，另一组件的自身设置也将被删除（删除后从父组继承设置）。

8.2.1.3. 组

在**组**部分可设置此工作站所属组列表。**组籍**中列出的是此工作站目前所属的工作站和可以归属的工作站。

设置工作站组籍

1. 向用户组添加工作站时需在**组籍**中勾选此组。
2. 从用户组删除工作站时需在**组籍**中取消对此组的勾选。

不可从预设组中删除工作站。

3. 更改基组的操作是在组籍部分点击相应组的图标。这时组图标上会出现**1**。

8.2.1.4. 安全策略

在**安全策略**部分限定安装在此工作站的代理端连接Dr.Web服务器所使用的网络地址。

设置访问权限限制

1. 勾选**使用此访问权限列表**后可设置允许地址列表或禁止地址列表。取消则允许所有连接。
2. 允许从一定TCP地址的访问，此地址应添加到**TCP：允许**或**TCPv6：允许**名单。
3. 禁止一个TCP地址的访问，此地址应添加到**TCP：禁止**或**TCPv6：禁止**名单。
4. 所有名单中都不包含的地址可以是都允许或都禁止，这取决于是否勾选**禁止优先**：如勾选了此项，**禁止**列表具有比**允许**列表更高的优先级。所有名单中都不包含的地址或两个名单都包含的地址将为禁止。只允许包含于**允许**列表且不包含于**禁止**列表的地址。

编辑地址列表的操作：

1. 在相应输入栏输入网络地址，格式为：*<IP地址>*/[*<前缀>*]。
2. 添加新地址栏需点击相应项的按钮。
3. 删除地址栏需点击相应地址栏旁边的按钮。
4. 应用更改需点击**保存**按钮。

只有计算机安装有IPv6界面才可显示TCPv6地址输入列表。

前缀使用举例：

1. 前缀24代表网络掩码为：`255.255.255.0`
   包含254个地址。
   这些网络的主机地址为：`195.136.12.*`
2. 前缀8代表网络掩码为`255.0.0.0`
   包含的地址达16777214个（256*256*256-2）
   这些网络的主机地址为：`125.*.*.*`

8.2.1.5. 代理服务器

在**代理服务器**给出与此工作站安装的Dr.Web代理服务器的设置。

安装代理服务器并设置与Dr.Web服务器的连接详见**安装手册**中的安装代理服务器。

如代理服务器安装在工作站：

1. 在**识别码**一栏出现管理中心创建的代理服务器账户识别码。创建账户后不可编辑识别码。
2. 在**名称**一栏可更改管理中心创建的代理服务器账户的名称。
3. 在**密码**和**确认密码**两栏可更改管理中心创建的代理服务器账户的密码。密码用于代理服务器连接Dr.Web服务器。在管理中心更改密码时需确认代理服务器连接设置中的密码与管理中心更改的密码相符。密码不符会造成代理服务器无法连接Dr.Web服务器，无法通过管理中心远程管理配置。

4. 在**组籍**指定所建代理服务器归属的组。更改方式是勾选列表中所需组。
   每一代理服务器只能列入一个组。
   可选择组**Proxies**或其子组。
5. 可删除与所编辑工作站相邻的代理服务器。操作是点击 **删除代理服务器**。
   点击**保存**后代理服务器从工作站卸载。代理服务器账户从Dr.Web服务器删除。

如代理服务器未安装在工作站：

1. 如要在所选工作站安装代理服务器，需勾选此项**创建邻居代理服务器**并给出所创建的代理服务器参数。参数与创建代理服务器的参数相同。
2. 点击**保存**后在管理中心创建代理服务器账户。设置传送到工作站后在此工作站以背景模式安装代理服务器。代理端将只通过安装的代理服务器连接Dr.Web服务器。对用户而言，代理服务器为透明使用。

8.2.1.6. 位置

在**位置**标签指定工作站地理位置的补充信息。

还可在此标签查看工作站在地图上的位置。

查看工作站在地图上的位置

1. 在**纬度**和**经度**以十进制度（Decimal Degrees）输入工作站地理坐标。
2. 点击**保存**按钮保存输入的数据。
3. 在**位置**标签显示的OpenStreetMap地图预览图出现对应坐标的标记。
   如无法打开预览图，会显示文字**在地图上标出**。
4. 查看全图需点击预览图或**在地图上标出**。

> 可为OS Android工作站设置自动确定位置。
>
> 如何使用和设置这一功能的详细信息参见**附录**中的自动确定OS Android工作站位置。

8.2.2. 保护组件

组件

查看工作站上已安装的反病毒软件包组件，并可启用或停止组件运行

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。
2. 在打开的控制菜单选择**常规**中的子项**保护组件**。
3. 打开所选工作站已安装组件相关信息。

可安装组件列表取决于：

- 授权密钥允许使用的组件；
- 工作站操作系统；
- 管理员在反病毒网络服务器上进行的设置。管理员可以在安装代理端前，也可在安装后更改工作站反病毒软件包组件组成（参见可安装的反病毒软件包组件）。

4. 如需可直接从管理中心更改组件运行状态。操作是勾选需改变其状态的组件，点击工具面板的相应图标：
   - ——停止工作站上所选组件的运行。
   - ——启动工作站上的所选组件。

停止组件运行时当前扫描进程将中断、扫描仪停止运行，监视器暂停运行。

还可按照启动类型来停止组件运行，参见按类型中断已启动组件的运行。

5. 如需可将工作站组件运行状态数据导出到文件。操作是在工具面板点击下面的一个按钮：
   将数据保存到**CSV**文件，
   将数据保存到**HTML**文件，
   将数据保存到**XML**文件，
   将数据保存到**PDF**文件。

病毒库

查看工作站上已安装的病毒库

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站的名称。
2. 在打开的控制菜单选择**统计信息**中的子项**病毒库**。
3. 打开已安装病毒库信息窗口：具体病毒库文件名称；病毒库版本；病毒记录数量；病毒库创建时间。

如**病毒库**一项不显示，可在主菜单选择**管理**，在打开的窗口选择控制菜单中的**Dr.Web服务器配置**一项，在**统计信息**标签勾选**病毒库监控**和**工作站状态监控**，之后重新启动Dr.Web服务器。

只有选择单个工作站时**病毒库**一项才可选用。

8.2.3. Windows操作系统工作站的硬软件配置

Dr.Web Enterprise Security Suite可以收集查看Windows操作系统工作站硬软件配置相关信息。

收集工作站硬软件配置信息

1. 在Dr.Web服务器启用统计信息收集功能：
   a) 在管理中心主菜单选择**管理**一项。
   b) 选择控制菜单中的**Dr.Web服务器配置**。
   c) 在Dr.Web服务器设置打开 **统计信息**标签后勾选**设备和软件组成**。
   d) 应用更改需点击**保存**按钮后重新启动Dr.Web服务器。
2. 在工作站允许息收集统计信息：
   a) 在管理中心主菜单选择**反病毒网络**一项。
   b) 在反病毒网络分层列表选择需要允许收集统计信息的工作站或工作站组。选择工作站组时许注意设置的继承规则：如所选组工作站设有自身设置，则更改组设置后，工作站设置不会发生相应改变。
   c) 在控制菜单的**配置→ Windows**选择**Dr.Web**代理端。
   d) 在代理端设置**常规**标签勾选**收集工作站信息**。如之前Dr.Web服务器设置中没有设置允许收集统计信息，此项不可使用。如需可更改**工作站信息收集周期（分钟）**参数值。
   e) 应用更改需点击**保存**按钮。设置将发送到工作站。

查看一个或多个作站硬软件配置信息

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在反病毒网络分层列表选择工作站或组。
3. 在控制菜单的**常规**部分选择**设备和软件组成**。
4. 报表中包含所选工作站硬软件配置信息，分以下标签：
   - **硬件**——工作站安装的硬件列表。
   - **软件**——工作站安装的软件产品列表。
   - **Windows更新**——工作站上安装的Windows操作系统更新包。
5. **工作站**一列每一标签包含显示器信息的工作站的名称。
6. 编辑列表中的数据显示：
   - 利用⚙选择报表中显示的列。
   - 利用▼指定搜索内容，在整个报表进行搜索。
7. 如需可将硬软件配置数据导出到文件。操作是在工具面板点击下面的一个按钮：
   将数据保存到**CSV**文件，
   将数据保存到**HTML**文件，
   将数据保存到**XML**文件，
   将数据保存到**PDF**文件。

8.3. 设置工作站配置

8.3.1. 工作站用户权限

通过**Dr.Web**安全管理中心设置工作站用户权限

1. 在主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站名称。在控制菜单选择**权限**。打开权限设置窗口。
2. 在对应工作站操作系统的标签编辑权限。改变权限设置时通过勾选相应项或取消勾选。
3. 在以下标签编辑OS Windows、macOS、Linux和Android工作站权限：
   - **组件**——设置反病毒组件管理权限。默认情况下用户可以启用每个组件，但不可编辑组件配置，也不可停用。
   - **常规**——设置Dr.Web代理端及其功能的管理权限：

权限部分选项	选项作用	如取消勾选，工作站发生的变化
OS Windows工作站		
更改**Dr.Web**代理端配置	勾选后允许用户在工作站更改Dr.Web代理端设置。	代理端设置中的**基本**部分无法进行以下设置： • **通知**：不可进行任何设置。 • **服务器**：不可访问与Dr.Web服务器的连接设置、**将系统时间与服务器时间同步**和**如无法连接服务器，使用移动模式**两个选项。 • **自我保护**：不可设置**禁止更改系统日期和时间**、**禁止用户操作仿真**。 • **高级**：在**日志**部分不可设置**Dr.Web**更新、**Dr.Web**服务和**扫描出错时创建内存转储**。
停用自我保护	勾选后允许用户在工作站停用自我保护。	代理端设置中的**基本** → **自我保护**部分无法更改**启用自我保护**和**启用对虚拟机的支持**。
卸载**Dr.Web**代理端	勾选后允许用户在工作站卸载Dr.Web代理端。	禁止从工作站上删除代理端，不论是利用安装程序还是使用Windows操作系统的常规工具。这时删除代理端只能通过在管理中心工具面板选择**常规** → **卸载Dr.Web代理端**。
macOS工作站		
在移动模式下启动	勾选后，如无法连接Dr.Web服务器，允许用户转为移动模式，以便直接从Dr.Web全球更新系统获取更新。	应用程序主窗口**更新**一项不可更改。

权限部分选项	选项作用	如取消勾选，工作站发生的变化
Linux家族操作系统工作站		
在移动模式下启动	勾选后，如无法连接Dr.Web服务器，允许用户转为移动模式，以便直接从Dr.Web全球更新系统获取更新。	以控制台模式运行时：无法使用指令`drweb-ctl update`从GUS更新病毒库。
OS Android工作站		
在移动模式下启动	勾选后，如无法连接Dr.Web服务器，允许用户转为移动模式，以便直接从Dr.Web全球更新系统获取更新。	移动设备上启动的应用程序主窗口更新一项不可更改。

关闭代理端某项设置的更改时将使用关闭前的最后设置。

菜单相应选项功能描述见相应操作系统Dr.Web保护产品的用户手册。

4. 可点击**将设置适用于另一对象**按钮将这些设置复制到另一对象。
5. 可通过点击**将本部分设置导出到文件**将这些设置导出到文件。
6. 可通过点击**将设置从文件导入到这一部分**从文件导入设置。
7. 点击**保存**按钮接受所进行的权限更改。

如果在更改工作站设置时工作站没有连接Dr.Web服务器，则新设置在代理端恢复与Dr.Web服务器的连接后生效。

8.3.2. 工作站任务日程

Dr.Web Enterprise Security Suite具有设置*统一任务日程*的功能，统一日程由反病毒网络管理员指定，按照配置中的继承原则继承。

任务日程——是在指定时间自动执行的任务列表。日程的主要应用时在用户最方便的时间对工作站进行反病毒扫描，且不需要手动启用扫描仪。此外，Dr.Web代理端可以执行下面介绍的其他操作。

通过Dr.Web安全管理中心可对工作站（或组）定期执行的任务统一日程进行编辑。

用户不可在工作站查看和编辑任务统一日程。

统一日程任务执行结果不记录到代理端的统计数据，而是发送到Dr.Web服务器并保存到Dr.Web服务器的统计数据。

编辑统一日程

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。在控制菜单选择**任务计划器**一项。打开工作站任务列表。



如所选工作站和组是从父组继承设置，则本节的大部分工具都不可访问。必要时了利用工具面板的以下元素来更改任务日程中的继承设置：

继承策略或父组设置——删除任务日程自身设置，设为继承父组本部分的设置。

复制策略或父组设置并将其指定为自身设置——复制父组任务日程的设置并将其指定给所选工作站。这时会中断继承，所有任务日程之后方式的更改都将被认为是自身设置。

2. 利用工具面板的相应元素管理日程：

a) 工具面板常规元素用于创建新任务和管理整个日程。

创建任务——添加新任务。此操作详见编辑任务。

将设置适用于另一对象——将任务复制到其它组和工作站。详见将设置复制到其它组/工作站。

将本部分设置导出到文件——将日程保存到专门格式的文件。

从文件将设置导入到本部分——从专门式格的文件导入日程。



不可将Dr.Web服务器任务列表导入到工作站任务计划器，也不可进行反向操作。

b) 管理现有任务可勾选个别任务或利用表头全选。如所选工作站或组不是从父组继承任务日程设置，在工具面板会出现管理所选任务的元素：

设置		操作
状态	允许执行	如果所选任务之前为禁止，则按照为其指定的日程激活。
	禁止执行	禁止执行所选任务。任务会保存在日程表，但不会执行。
 在常规标签利用**允许执行**选项可进行相同操作。		
重要性	设为重要	如未按照日程执行任务，则在下次启动Dr.Web代理端时再次执行。
	设为不重要	只在日程指定时间执行，不论是否有未能执行的情况。

设置	操作
在常规标签利用重要任务选项可进行相同操作。	
复制设置	复制在当前日程中选出的任务。指定复制设置操作时会创建与所选任务设置相同的新任务。
二次执行	对于一次性任务：按照为其指定的时间再次执行（更改任务执行次数见编辑任务）。
删除所选任务	从日程中删除所选任务。
执行任务	立即执行列表中所选任务。这时即便是按照日程禁止执行的任务也会启动执行。

3. 更改任务参数需在列表中选择需要任务，这时或打开**编辑任务**窗口，介绍见下。
4. 编辑结束后需点击**保存**按钮接受更改。

如编辑后日程为空（不包含任何任务），管理中心会建议您或者使用从组继承的日程，或者使用空日程。如需要拒绝使用从组继承的日程，则可设置空日程。

编辑任务

利用编辑任务可：

1. 创建新任务。
   操作是在工具面板点击**创建任务**。
2. 编辑现有任务。
   操作是在任务列表中点击相应任务的名称。

打开任务参数编辑窗口。编辑现有任务时的设置与创建新任务相同。

界面有*标志的输入栏必须填写。

编辑任务参数

1. 在**常规**标签设定以下参数：
   - 在**名称**一栏输入任务名称，任务在日程中将以这一名称显示。
   - 如要激活任务的执行，需勾选**允许执行**。如取消勾选，任务会保存在日程表，但不会执行。

可在任务计划器利用工具面板的**状态**进行相同的设置。

- 勾选**重要任务**后如未按照日程时间执行任务（应执行任务时Dr.Web代理端为停用状态）则在下次启动Dr.Web代理端时再次执行。如某时段多次未执行任务，则启动Dr.Web代理端时只执行1次。

可在任务计划器利用工具面板的**重要性**进行相同的设置。

如果工作站启动时有几项扫描任务，则只执行排在列队第一位的任务。

例如：任务**Daily scan**为允许状态，同时重要任务"利用Agent扫描仪进行扫描"在设定时间未能执行，则在工作站启动时将执行**Daily scan**，而不会执行逾期的重要任务。

- 如取消对**异步启动任务**的勾选，任务将列入任务计划器的任务顺序执行队列。如勾选此项，则启动此任务不需等待执行次序。

2. 在**操作**标签的**操作**下拉列表选择任务类型并设置执行参数：

任务类型	参数描述
写入日志文件	行——写入日志文件的通知内容。
运行程序	给出以下参数： • 在**路径**输入需启动的执行文件全称（带路径）。 • 在**参数**一栏输入启动程序命令行参数。 • 勾选**等待程序结束运行**同步执行后将等待此任务启动的程序结束运行。这时服务器会记录程序启动、返回码和程序结束运行时间。如取消对**等待程序结束运行**同步执行的勾选，则认为启动程序后任务就已完成，代理端只记录程序启动。
Dr.Web Agent扫描仪。快速扫描	扫描设置参数见设置扫描仪参数。
Dr.Web Agent扫描仪。自定义扫描	
Dr.Web Agent扫描仪。完全扫描	

只可在OS Windows、UNIX家族操作系统和macOS工作站远程启动扫描仪。

3. 在**时间**标签：
   - 在**周期**下拉列表选择任务启动模式并根据所选周期相应设置时间：

启动模式	参数描述
启动时	任务将在代理端开始运行时启动执行。 启动无高级参数设置。

启动模式	参数描述
在执行初始任务N分钟后	需在**初始任务**下拉列表选择此任务执行时间相对应的任务。 在**分钟**栏指定或从列表中选择执行初始任务后过多少分钟开始执行此任务。
每天	需输入几点几分，任务将每天在指定时间启动执行。
每月	需选择日期（几号），输入几点几分，任务将每月在指定日期指定时间启动执行。
每周	需选择星期几，输入几点几分，任务将每周在指定日期指定时间启动执行。
每小时	需输入从0到59的数字（分钟数）——任务将每小时在指定分钟启动执行。
每N分钟	需输入**N**值，确定执行任务的时间间隔。 如**N**等于或大于60，则任务每过**N**分钟启动执行一次。如**N**小于60，任务将在每小时内**N**的整倍分钟启动执行。

- 勾选**在第一次执行后禁止**后任务只在指定时间执行一次。如取消勾选，将按照指定周期多次执行。
  可利用日程部分工具面板的**二次执行**按钮重复已经执行过的一次性任务。
- 勾选**按照UTC启动任务**后会以世界时间（时区UTC+0）为准启动任务。如取消勾选，则按照工作站本地时间启动任务。

4. 结束编辑后点击**保存**按钮保存对原有参数的更改或新建任务的参数。

8.3.3. 可安装的反病毒软件包组件



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。

设置反病毒软件包可安装组件列表

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。在打开的控制菜单选择**可安装的组件**一项。
2. 在下拉列表为必要组件选择以下一种方式：
   - **必须安装**——指定工作站上必须安装此组件。创建新工作站时此组件列入反病毒软件包。为已有工作站设定**必须安装**后组件会添加到现有的反病毒软件包。
   - **可安装**——可以安装此反病毒组件。是否安装由用户在安装代理端时决定。
   - **不可安装**——禁止在工作站上安装此组件。创建新工作站时此组件不会列入反病毒软件包。为已有工作站设定**不可安装**后组件会从现有的反病毒软件包删除。

   表8-1所示为在何种用户设定参数和管理员在Dr.Web服务器的设定下组件会安装到工作站（+）。

表8-1.

由用户设定	在Dr.Web服务器设定		
	必须	可以	不可以
安装	+	+	
不安装	+		

3. 点击**保存**按钮保存设置和工作站反病毒软件包组成的相应改变。

8.3.4. 连接参数

在**连接参数**标签的参数用于设置与Dr.Web服务器的交互作用：

- 在**证书**一栏给出Dr.Web服务器SSL证书（`drwcsd-certificate.pem`）。点击按钮选择证书文件。

  工作站可同时保持多个证书，如更换加密密钥时或从一个Dr.Web服务器转至另一服务器时。这种情况下不得指定两个一样的证书。

  增添证书需点击后选择证书文件。

  删除现有证书需点击要删除的证书旁的按钮。

  必须指定证书。

- 在**服务器**一栏指定Dr.Web服务器或Dr.Web代理服务器地址（详见Dr.Web代理服务器）。此栏可为空，这时代理端将使用用户本地计算机设置中的Dr.Web服务器地址（安装所使用的Dr.Web服务器的地址）。

  可指定一个Dr.Web服务器地址，也可指定几个不同Dr.Web服务器的地址。添加Dr.Web服务器地址需点击后再新增输入栏输入地址。Dr.Web服务器网络地址格式见**附录**中的附录E.网络地址特点。

  Dr.Web服务器地址示例：

  tcp/10.4.0.18:2193

  tcp/10.4.0.19

  10.4.0.20

  如果输入的**服务器**参数值不正确，则代理端会与Dr.Web服务器断开并无法再与之连接。这种情况下必须直接在工作站设定Dr.Web服务器地址。

- 在**搜索次数**指定使用*Multicasting*模式连接时重复搜索Dr.Web服务器的次数。
- 在**搜索超时时限（秒）**指定使用*Multicasting*模式连接时重复 Dr.Web服务器搜索尝试的次数时间间隔。
- **压缩模式**和**加密模式**确定网络流量的加密和压缩设置。

- 在**网络监听参数**一栏指定管理中心搜索运行中的Dr.Web代理端时使用的UDP端口。禁止监听端口需输入**NONE**。

  此参数以网络格式输入，网络格式列于**附录**中的附录E. 网络地址特点。

  默认值为**udp/:2193**，即"所有接口、端口2193"。

8.3.5. 授权密钥

可采用以下方式查看和编辑工作站或工作站组的授权密钥列表：

1. 利用授权管理器。
2. 利用反病毒网络中授权对象（工作站或工作站组）的配置。

利用授权对象配置编辑授权密钥列表

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 打开需编辑器授权密钥的对象的工作站属性或组属性。
3. 在配置部分点击 **编辑**图标或**授权密钥**链接。
4. 打开的**授权密钥**显示对象的授权密钥列表，其当前状态（为继承密钥或自身指定密钥），以及本Dr.Web服务器可以使用的所有密钥。如需可直接进入授权管理器。
5. 对密钥列表采取的操作取决于对象授权密钥的当前状态：

操作	当前密钥为继承的密钥	当前密钥为自身指定的密钥	未指定任何密钥
添加授权密钥	将中断继承。新密钥添加到指定密钥列表，密钥列表转为自身指定的列表。	新密钥添加到指定密钥列表。	密钥作为自身指定密钥添加到对象的授权密钥列表。
删除授权密钥	不可进行此操作。	密钥将从对象的密钥列表中删除。	不可进行此操作。
设为继承	不可进行此操作。	当前密钥将从对象的密钥列表中删除，指定为从基组/父组继承密钥。	不可进行此操作。
中断继承	将中断继承。密钥列表不变，但转为自身指定的密钥列表。	不可进行此操作。	不可进行此操作。

当前密钥为继承的密钥

添加授权密钥

1. 在**授权密钥**窗口的**所有密钥**列表选择一个或几个需要添加的密钥。
2. 点击。
3. 如工作站可安装组件列表与添加的密钥不符，会出现相应通知并建议编辑最终组件列表。

4. 进行更改后点击**保存**。
5. 将中断继承。新密钥添加到指定密钥列表，密钥列表转为自身指定的列表。

中断继承且保留授权密钥列表

1. 在**授权密钥**窗口点击**从基组复制设置并将其设为自身设置.**
2. 将中断继承。从基组/父组复制密钥列表并将其指定为对象的自身指定列表。
3. 点击**保存**。

当前密钥为自身指定的密钥

添加授权密钥

1. 在**授权密钥**窗口的**所有密钥**列表选择一个或几个需要添加的密钥。
2. 点击。
3. 如工作站可安装组件列表与添加的密钥不符，会出现相应通知并建议编辑最终组件列表。
4. 进行更改后点击**保存**。
5. 新密钥添加到指定密钥列表。

删除授权密钥

1. 在**授权密钥**窗口的**对象密钥**列表点击需要删除的密钥旁的。

> 如删除了所有密钥，则设为从基组/父组继承授权密钥（另见设为继承）。

2. 点击**保存**。
3. 如工作站可安装组件列表与保留的密钥不符，会出现相应通知并建议编辑最终组件列表。

设为继承

1. 可用以下一个方式设为继承：
   - 打开需设为继承的对象的工作站属性或组属性。在配置部分点击**删除密钥**。
   - 在**授权密钥**窗口的**所有密钥**点击所有指定的密钥的旁边的。点击**保存**。
2. 当前密钥将从对象的密钥列表中删除，指定为从基组/父组继承密钥。
3. 如工作站可安装组件列表与继承的密钥不符，会出现相应通知并建议编辑组件列表。

未指定任何密钥

> Dr.Web服务器未添加任何密钥或Dr.Web服务器添加了密钥但没有分发到包括**Everyone**组在内的任何对象时才会出现这种情况。

添加授权密钥

1. 在**授权密钥**窗口的**所有密钥**列表选择一个或几个需要添加的密钥。
2. 点击。
3. 点击**保存**。
4. 密钥作为自身指定密钥添加到对象的授权密钥列表。

8.4. 设置反病毒组件

可通过管理中心设置的反病毒组件设置详细说明见**管理员手册**对相应操作系统工作站的管理。

组件

分别为不同操作系统的工作站提供的保护功能见下。

OS Windows工作站

Dr.Web扫描仪、Dr.Web Agent 扫描仪

按照用户调用或日程对计算机进行扫描。还可从管理中心远程启动工作站扫描，包括检查是否存在Rootkit。

SpIDer Guard

实时模式下对文件系统进行不间断检查，检查所有启动的进程，以及在硬盘创建的文件和在移动设备打开的文件。

SpIDer Mail

使用邮件客户端时检查所有进出邮件。

还可进行垃圾邮件过滤（如授权允许使用这一功能）。

SpIDer Gate

检查所有使用http协议对网站的访问。消除http流量存在的威胁（如获取和发送的文件中存在的威胁），阻止访问可疑的资源和错误资源 。

办公控制

控制对本地资源和网络资源的访问，包括控制对网站的访问。可监控重要文件的完整性，防止无意更改或病毒感染，禁止员工访问不需要的信息。

防火墙

保护计算机免于未经授权的外部访问，防止重要信息通过互联网泄露。控制互联网连接和数据传输，在数据包和应用程序层面阻止可疑的连接。

隔离区

将恶意对象和可疑对象隔离到专门的文件夹。

自我保护

保护Dr.Web Enterprise Security Suite文件和目录，防止未经授权进行删除、被用户无意间删除修改或被恶意软件修改。启用自我保护时只允许Dr.Web进程访问Dr.Web Enterprise Security Suite的文件和目录。

预防性保护

预防潜在危险。监控对操作系统重要对象的访问，监控驱动程序的加载以及自启动软件和系统服务的运行，并跟踪已启动进程，如发现病毒活动则阻断进程。

应用程序监控

对工作站所有进程的活动进行监控，可让反病毒网络管理员调整受保护工作站上的应用是否允许使用或禁止使用。

UNIX家族操作系统工作站

Dr.Web Scanning Engine

扫描引擎。执行数据（文件内容、磁盘设备启动记录、来自Dr.Web for UNIX其他组件的数据）的反病毒扫描。安排扫描次序。对可清除的威胁进行清除。

Dr.Web File Checker

文件系统对象扫描组件和隔离区管理器。接受来自Dr.Web for UNIX其他组件的文件扫描任务。按照日程巡视文件系统目录，将文件提交给扫描引擎进行扫描。删除已感染文件，隔离文件或从隔离区还原文件、管理隔离区目录。保证缓存保存的是已检查文件和已侦测到的威胁注册表的最新信息。

供所有检查文件需对象的组件使用，如SpIDer Guard（for Linux、SMB、NSS）。

Dr.Web ICAPD

ICAP服务器，对申请和经代理服务器的HTTP流量进行分析。阻断已感染文件的传输，阻止访问不良Web资源和系统管理员列入黑名单的网络节点。

SpIDer Guard for Linux（仅包含于用于GNU/Linux家族操作系统的软件包）

Linux文件系统监视器。以背景模式运行，监控GNU/Linux文件系统中执行的文件操作（如创建文件，打开、关闭和启动文件）。向文件扫描组件申请对新创建文件和内容更改的文件以及软件启动时的执行文件进行扫描。

SpIDer Guard for SMB

Samba共享文件监视器。以背景模式运行，监控文件系统中对划分给SMB服务器文件库Samba的目录的操作（如创建文，打开、关闭文件，只读和写入操作）。向文件扫描组件申请对新创建文件和内容更改的文件进行扫描。

SpIDer Guard for NSS （仅包含于用于GNU/Linux家族操作系统的软件包）

NSS卷（Novell Storage Services）监视器。以背景模式运行，监控文件系统指定节点的NSS卷中的操作（如创建文件，打开、关闭文件以及写入操作）。将新创建文件和内容更改的文件发送给文件扫描组件进行扫描。

SpIDer Gate（仅包含于用于GNU/Linux家族操作系统的软件包）

对网络流量和URL进行检查的组件。负责检查从网络加载到本地节点和从本地节点上传到外网的数据是否存在威胁，阻止访问不良Web资源和系统管理员列入黑名单的网络节点。

Dr.Web MailD

对邮件进行检查的组件。分析邮件协议通知、解析电子邮件以备检查是否含有威胁。有两种运行模式：

1. 邮件服务器（Sendmail, Postfix等等）过滤器，利用Milter、Spamd或Rspamd接口接入。
2. 透明代理邮件协议（SMTP, POP3, IMAP）。这种模式下使用SpIDer Gate。



用于UNIX家族操作系统工作站的其他组件为补充组件，用于反病毒软件运行的内部设置。

macOS工作站

Dr.Web扫描仪、Dr.Web Agent 扫描仪

按照用户调用或日程对计算机进行扫描。还可从管理中心远程启动工作站扫描。

SpIDer Guard

实时模式下对文件系统进行不间断检查，检查所有启动的进程，以及在硬盘创建的文件和在移动设备打开的文件。

SpIDer Gate

检查所有使用http协议对网站的访问。消除http流量存在的威胁（如获取和发送的文件中存在的威胁），阻止访问可疑的资源和错误资源 。

隔离区

将恶意对象和可疑对象隔离到专门的文件夹。

OS Android 移动设备

Dr.Web扫描仪、Dr.Web Agent 扫描仪

按照用户调用或日程对移动设备进行扫描。还可从管理中心远程启动工作站扫描。

SpIDer Guard

实时模式下对文件系统进行不间断检查。在试图将文件保存到移动设备时对其进行检查。

来电和短信过滤

过滤SMS短信和电话可阻止不需要接听的电话和接收的短信，如广告短信和来自未知号码的电话和短信。

防盗器

在移动设备丢失或被窃时确定其所在地或及时上锁。

Cloud Checker

URL过滤器使移动设备用户远离不良网路资源。

防火墙（仅可在移动设备进行设置）

保护移动设备免于未经授权的外部访问，防止重要信息通过互联网泄露。控制互联网连接和数据传输，在数据包和应用程序层面阻止可疑的连接。

安全审计（仅可在移动设备进行设置）

对移动设备安全状态进行诊断和发现，消除发现的问题和漏洞。

应用程序过滤器

禁止在移动设备启动管理员允许启动列表中不包含的应用程序。

8.5. 工作站反病毒扫描

工作站用户可利用Dr.Web扫描仪自行对工作站进行反病毒扫描。

代理端不能运行也可以正常启用扫描仪，包括以安全模式启动 系统时。

利用管理中心可：

- 查看所有当前启用的反病毒组件列表。
- 按类型中断已启用的反病毒组件。
- 设置扫描参数，启动反病毒扫描任务。

8.5.1. 按类型中断已启动组件的运行

使用此选项时当前扫描中断，扫描仪停止运行，已启动的监视器中断运行。

注意！无法从管理中心启动监视器SpIDer Guard、SpIDer Mail和SpIDer Gate。

中断工作站上某类型的所有组件的运行

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中选择所需组或个别反病毒工作站。
2. 在反病毒网络目录工具面板点击**组件管理**。在下拉列表中选择**中断已启动的组件**。
3. 在打开的面板勾选需立即中断的组件类型：
   - **中断任务计划器启动的Dr.Web Agent扫描仪**——中断按照统一任务日程启动的Dr.Web Agent扫描仪的扫描进程。
   - **中断管理员启动的Dr.Web Agent扫描仪**——中断由管理员从管理中心手动启动的Dr.Web Agent扫描仪的扫描进程。
   - **中断用户启动的Dr.Web Agent扫描仪**——中断由用户在工作站启动的Dr.Web Agent扫描仪的扫描进程。
   - **中断SpIDer Guard、SpIDer Mail、SpIDer Gate、办公控制、防火墙、自我保护和预防性保护**——中断相应组件的运行。

选择所有类型的操作是勾选**中断已启动的组件**面板标头。

4. 点击**中断**按钮。

8.5.2. 启动工作站扫描

启动工作站反病毒扫描

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在打开窗口的分层列表中点击工作站或组的名称。
3. 在工具面板点击**扫描**。在工具面板打开的列表中选择一种扫描模式：

   Dr.Web Agent扫描仪。快速扫描。此模式下扫描以下对象：

   - 内存，
   - 所有磁盘引导区，
   - 自启动对象，
   - 启动盘根目录，
   - Windows安装盘根目录，
   - Windows系统文件夹，
   - 文件夹我的文档，
   - 系统临时目录，
   - 用户临时目录。

   Dr.Web Agent扫描仪。完全扫描。这种模式下扫描所有硬盘和移动载体（包括启动引导区）。

   Dr.Web扫描仪。自定义扫描。此模式下可任意选择需要扫描的目录和文件，并可设置扫描高级参数。
4. 选择扫描类型后打开扫描仪设置窗口。必要时可更改扫描参数（参见设置扫描仪参数）。
5. 点击**扫描**按钮在所选工作站启动扫描进程。

> 远程启动的Dr.Web Agent扫描仪以背景模式进行扫描，不向用户显示通知。

8.5.3. 设置扫描仪参数

利用管理中心可进行以下反病毒扫描设置：

- Dr.Web扫描仪设置。这一扫描仪由用户在工作中启动，不可从管理中心远程启动。但管理员可统一更改设置，更改后的设置分发并保存到工作站。
- Dr.Web Agent扫描仪设置。此扫描仪从管理中心远程启动，对工作站的扫描与Dr.Web扫描仪进行的扫描类似。Dr.Web Agent扫描仪设置相当于Dr.Web扫描仪的高级设置，在启动工作站反病毒扫描时指定。

设置Dr.Web扫描仪参数

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在打开窗口的分层列表中点击工作站或组的名称。
3. 在打开的控制菜单的**配置**部分的相应操作系统选择**扫描仪**。打开扫描仪设置窗口。
4. 指定必要的参数。Dr.Web扫描仪参数介绍见相应操作系统的**用户手册**。
5. 点击**保存**按钮。设置将保存于管理中心并分发到相应工作站。

设置Dr.Web Agent扫描仪参数

Dr.Web Agent扫描仪在启动工作站反病毒扫描时指定，见启动工作站扫描。

扫描仪设置部分列表中可用（+）或不可用（–）设置取决于启动工作站扫描的方式，详见下表。

表8-2. 不同启动方式下的扫描仪设置

启动工作站扫描的方式	设置			
	常规	操作	限制	排除项
Dr.Web Agent扫描仪。自定义扫描	+	+	+	+
Dr.Web Agent扫描仪。快速扫描	–	+	+	–
Dr.Web Agent扫描仪。完全扫描	–	+	+	–

按照启动远程扫描的工作站的操作系统，扫描仪设置部分只可使用操作系统支持的选项。

8.5.3.1. 常规



扫描UNIX家族操作系统和macOS工作站时不支持的设置使用方括号**[ ]**。

扫描Android操作系统工作站时不支持的设置使用圆括号**( )**。

在**常规**部分可进行以下反病毒扫描设置：

- 在下拉列表中选择一种扫描模式：
  - **扫描所有磁盘**——对所有可访问的本地盘进行反病毒扫描。
    这时可以进行的高级设置有：
    - 勾选**扫描启动扇区**后扫描仪会检查启动扇区，既包括本地磁盘的引导扇区，也包括物理磁盘的主引导扇区。
    - 勾选**[扫描自启动程序]**后检查操作系统开始运行时自动启动的程序。
    - 勾选**[(扫描加载中的程序和模块)]**后检查在内存中启动的进程。
    - 勾选**[(侦测rootkit)]**后侦测具有在系统隐藏其踪迹功能的恶意软件。
    - 勾选**扫描固定磁盘**后检查固定盘（硬盘等等）。

  - 勾选**扫描移动磁盘对象**后检查所有移动信息载体，如软盘驱动器、CD/DVD-盘、闪存盘等等。
- **检查指定路径**——只对指定的路径进行反病毒扫描。
  在**需扫描的路径**指定需要检查的路径列表（建立此列表的操作见下）。
  - 向列表添加新行是需点击 按钮，然后在打开的输入行输入路径。
  - 删除列表中现有项时点击需删除行前的 按钮。
- 勾选**使用启发式分析**后扫描仪启用启发式分析侦测未知病毒。在此模式下有可能出现扫描仪误报。
- 勾选**检查符号链接**后扫描时会检查符号链接。
- 勾选**[(转用电池时中断扫描)]**后如用户电脑转为使用电池供电则会中断反病毒扫描。
- 勾选**[扫描过程中关闭网络]**一项用于在扫描时关闭计算机和局域网、互联网的连接。
- 勾选**压缩文件**一项后会检查压缩包内文件是否感染。
- 勾选（**邮件文件**）一项后会检查邮箱。
- 勾选**[(安装包)]**一项后会检查程序安装包。
- **[(扫描优先级)]**下拉列表用于确定扫描进程相对于操作系统现有资源的优先级。
- 勾选**[(计算机资源负载等级)]**后会限制扫描进程对计算机资源的使用，需在下拉列表选择扫描仪产生的最大负载。在没有其他任务的情况下将最大限度地占用资源。

> 在单引擎单处理器系统选项**计算机资源负载等级**不会对扫描仪产生的实际负载产生明显的影响。

- 在**[(使用的内核数量)]**一栏指定扫描仪最多可使用的内核数量。有效值为0至32。0值表示可以使用所有可用内核。

  设置工作站组是需注意，此参数为绝对值，而非可用内核数量比例。因此指定同一数值会使内核数量不同的工作站产生不同的负载。
- **(扫描结束后的操作)**下拉列表指定在完成扫描后自动执行操作：
  - **不进行操作**——结束扫描后不对用户计算机进行任何操作。
  - **[关机]**——结束扫描后关闭用户计算机。在关机前扫描仪会对侦测到的威胁执行设定的操作。
  - **[重启工作站]**——结束扫描后重启用户计算机。在重启前扫描仪会对侦测到的威胁执行设定的操作。
  - **[转入待机模式]**。
  - **转入睡眠模式**。

8.5.3.2. 排除项

在**排除项**可指定不需要进行反病毒扫描的目录和文件名单。

编辑不需扫描的路径和文件列表

1. 在**不需扫描的路径和文件**输入行输入相应文件和目录的路径。
2. 向列表添加新行是需点击 按钮，然后在打开的输入行输入路径。

3. 删除列表中现有项时点击需删除行前的 按钮。

不需扫描的对象列表中可包含以下类型的列表项：

1. 不需扫描的对象的直接路径.这时：
   - 符号 \ 或 / —— 排除对操作系统安装目录所在磁盘的扫描，
   - 以符号\结束的路径——排除对此目录的扫描；
   - 不以符号\结束的路径——排除对以此行开始的所有子目录的扫描。

   OS Windows示例： C:\Windows——不检查C:\Windows目录文件和其所有子目录。

   UNIX家族操作系统示例： /etc——不检查/etc目录文件和其所有子目录。
2. 不需检查的对象的掩码。设定掩码可使用通配符?和*。

   OS Windows示例: C:\Windows**.dll——不检查所有处于 C:\Windows目录所有子目录中扩展名为dll的文件。

   UNIX家族操作系统示例： /etc/*/*.pub——不检查所有处于/etc目录所有子目录中扩展名为pub的文件。
3. 不需扫描的对象路径中操作系统指定的环境变量。

   OS Windows示例： %WINDIR%\SysWOW64\——不检查C:\Windows目录的SysWOW64子目录中的文件。

   UNIX家族操作系统示例： /home/*/network——不检查/home目录的network子目录中的文件。
4. 正则表达式。可使用正则表达式来设定路径。任何一个全名（带路径）与正则表达式相符的文件都不进行扫描。

在启动病毒扫描前请阅读OS Windows计算机反病毒软件使用建议。相关介绍的链接：https://support.microsoft.com/en-us/topic/virus-scanning-recommendations-for-enterprise-computers-that-are-running-currently-supported-versions-of-windows-c067a732-f24a-9079-d240-3733e39b40bc。此介绍有助于优化系统性能。

用于设定不需扫描的路径的正则表达式语法为：

qr{表达式}符号

最常见的符号为i，表示"不区分字母大小写"。

不需扫描的路径和文件正则表达式范例

正则表达式	说明
qr{\\pagefile\.sys$}i	不检查OS Windows页面文件
qr{\\notepad\.exe$}i	不检查文件notepad.exe
qr{^C:}i	不检查磁盘C
qr{^.:\\WINNT\\}i	不检查所有磁盘上的目录WINNT

正则表达式	说明
qr{(^C:)|(^.:\\WINNT\\)}i	合并上述两种情况
qr{^C:\\dir1\\dir2\\file\.ext$}i	不检查文件c:\dir1\dir2\file.ext
qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i	不检查文件file.ext，如果文件处于c:\dir1\dir2和其子目录
qr{^C:\\dir1\\dir2\\}i	不检查目录c:\dir1\dir2和其子目录
qr{dir\\[^\\]+}i	不检查处于任何目录的子目录dir，但检查子目录
qr{dir\\}i	不检查处于任何目录中的子目录dir，也不检查其子目录

正则表达式使用方法简介见**附录**中的附录J. Dr.Web Enterprise Security Suite中正则表达式的使用。

在**检查以下文件内容**部分可以排除对复合对象的扫描，操作是取消勾选：

- 勾选**压缩文件**一项后扫描仪检查压缩包内文件是否感染。
- **邮件文件**一项要求检查邮箱。
- **安装包**一项要求扫描仪检查程序安装包。

8.5.3.3. 操作

扫描UNIX家族操作系统和macOS工作站时不支持的设置使用方括号**[ ]**。

在**操作**标签可指定扫描仪侦测到已感染或可疑文件、恶意软件以及已感染压缩文件时的反应。

Dr.Web Agent扫描仪自动应用对侦测到的恶意对象应采取的操作。

对发现的威胁可以采取以下操作：

- **清除**——将被感染的对象恢复到感染前的状态。如对象无法清除或未能成功清除，将执行为无法清除的对象设置的操作。

  这一操作只适用于被已知的可清除病毒感染的对象，不包括木马程序和复合对象（压缩文件、邮件文件或者容器格式文件）中的被感染文件。
- **删除**——删除已被感染的对象。
- **隔离**——将被感染对象移动到工作站隔离区文件夹。
- **通知**——只是向管理中心发送侦测出了病毒的通知（报告模式设置见通知设置一节）。
- **忽略**——不执行任何操作，也不在扫描统计信息发送通知。

表 8-3. 扫描仪侦测到恶意对象时采取的操作

对象	操作				
	清除	删除	隔离	通知	忽略
已感染	+/*	+	+		
可疑文件		+	+/*		+
无法清除		+	+/*		
安装包		+	+/*		
压缩文件		+	+/*		
邮件文件			+/*		+
引导扇区	+/*			+	
广告程序		+	+/*		+
拨号器		+	+/*		+
恶作剧程序		+	+/*		+
风险程序		+	+/*		+
黑客工具		+	+/*		+

标志说明

+	对这一类型的对象可以采取该操作
+/*	该操作是对这一类型对象的默认操作

可使用以下设置指定对发现的威胁采取的操作

- **已感染**下拉列表指定扫描仪发现被已知病毒感染的文件时采取的操作。
- **可疑**下拉列表指定扫描仪发现疑是感染病毒的文件时（启发式分析仪作出反应）采取的操作。



扫描包括操作系统安装目录时建议为可疑文件设置**通知**操作。

- **无法清除**下拉列表指定扫描仪发现被已知的无法清除的病毒感染的文件时以及在尝试清除但未能成功的情况下采取的操作。
- **已感染的安装包**下拉列表指定扫描仪在软件安装包发现已感染文件或可疑文件时采取的操作。
- **已感染的压缩文件**下拉列表指定扫描仪在压缩文件发现已感染文件或可疑文件时采取的操作。

- **已感染的邮件文件**下拉列表指定扫描仪在发现已感染的邮件格式文件时采取的操作。

> 在复合对象（压缩文件、邮件文件或文件容器）内侦测到病毒或可疑代码时对威胁采取的操作涉及整个对象，而非只涉及其被感染的部分。默认在这些情况下采取的操作是报告。

- **已感染的引导扇区**下拉列表指定扫描仪在引导扇区发现病毒或可疑代码时采取的操作。
- 以下下拉列表指定扫描仪侦测到相应不良软件时采取的操作：
  - 广告程序；
  - 拨号器；
  - 恶作剧程序；
  - 风险程序；
  - 黑客工具。

> 如将操作设置为**忽略**，则不会执行任何操作：不会向管理中心发送设置为**报告**时发送的发现病毒通知。

勾选**[自动重启计算机]**后如侦测到清除要求重启的对象时会在扫描结束后自动重启。如取消勾选，则不会重启。管理中心收到的工作站扫描统计信息中会记录需重启工作站以完成清除。需要重启的状态相关信息在状态一列显示。如需管理员可从管理中心重启工作站（参见反病毒网络）。

勾选**显示扫描进程**后管理中心会显示指示器和工作站扫描进程状态行。

8.5.3.4. 限制

> 扫描UNIX家族操作系统和macOS工作站时不支持的设置使用方括号**[ ]**。

在**限制**部分可进行以下反病毒扫描设置：

- **扫描最长用时（毫秒）**——用于扫描一个对象的最长用时，以毫秒计。超过此时限会终止扫描这一对象。
- **压缩文件最大嵌套深度**——压缩文件内最多嵌套数量。如压缩文件中嵌套层数超过此值，扫描将只进行到指定深度。
- **[压缩文件最大大小（KB）]**——进行扫描的压缩文件最大大小。如压缩文件大小超过此值，则不会进行解压和扫描。
- **压缩文件最大压缩比**——如扫描仪确定压缩文件的压缩级别超过此值，则不会进行解压和扫描。
- **[解压文件最大大小（KB）]**——文件解压后最大大小。如扫描仪确定压缩文件解压后大小会超过此值，则不会进行解压和扫描。
- **[压缩率扫描限制（KB）]**——压缩文件中开始检查压缩率的最小文件的大小。

8.6. 查看工作站统计信息

利用**反病毒网络**控制菜单可以查看以下信息：

- 统计信息——工作站反病毒组件运行统计信息、工作站和反病毒软件状态信息，用于查看并保存所有统计信息或类型报表的汇总报告。
- 图表——工作站上侦测出的感染图表信息。
- 隔离区——远程访问工作站上隔离区的内容。

8.6.1. 统计信息

可设置自动创建包含所需统计报表的统计报告。这样的自选内容统计报告不仅可保存于Dr.Web服务器，还可发送到邮箱。

操作是在Dr.Web服务器的日程设置**创建统计报告**。

查看报表

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。
2. 在打开的控制菜单选择**统计信息**中的子项。

统计信息菜单选项：

- **威胁**——用于查看受保护工作站安全威胁侦测统计：感染对象名单、分布、威胁名称、反病毒软件采取的操作等等。
- **错误**——用于查看在一定时期内所选工作站上发生的扫描错误。
- 汇总数据——用于查看、保存所有统计信息或所选类型报表的汇总报告。如**统计信息**中其它项均为隐藏，此项不显示。
- 扫描统计信息——用于获取工作站反病毒软件运行统计数据。
- **开始/结束**——用于查看工作站上曾启用的组件列表。
- **威胁统计信息**——用于查看工作站上侦测到的安全威胁统计，按威胁类型和数量分组。
- 状态——用于查看工作站可能需要干预的特殊状态。
- **任务**——用于查看在指定时段内工作站任务列表。
- **已阻止的设备**——用于查看工作站上被组件办公控制阻止的设备列表。
- **产品**——用于查看所选工作站上已安装的产品的信息。产品指的是Dr.Web服务器库产品。
- **病毒库**——用于查看已安装的病毒库相关信息：具体病毒库文件的名称；病毒库版本；病毒记录数量；病毒库创建日期。只有选择工作站后才可使用此项。
- **模块**——用于查看 Dr.Web反病毒软件所有模块的详细信息：模块介绍，包括其功能名称；产品各模块文件；模块版本等等。只有选择工作站后才可使用此项。
- **预防性保护事件**——用于查看预防性保护组件在工作站发现的事件的统计信息。
- 应用程序监控事件——用于查看应用程序监控组件在工作站发现的事件的统计信息。
- **代理端网络安装**——用于查看工作站或工作站组代理端安装列表。

- **代理端卸载**——用于查看删除了Dr.Web反病毒软件的工作站列表。

> 显示**统计信息**中隐藏选项需在主菜单选择**管理**，在打开的窗口选择控制菜单的**Dr.Web服务器配置**。在**统计信息**标签勾选相应选项（见下），然后点击**保存**并重新启动Dr.Web服务器。

表**8-4**。统计信息选项与**Dr.Web**服务器配置文件统计信息部分复选框的对应关系

统计信息选项	**Dr.Web**服务器配置统计信息部分的选项
威胁	侦测到的安全威胁
错误	扫描错误
扫描统计信息	扫描统计信息
启动/完成	组件启动/结束
威胁统计信息	侦测到的安全威胁
状态	工作站状态
任务	工作站任务执行日志
已阻止的设备	已阻止的设备
病毒库	工作站状态 病毒库状态
模块	工作站模块列表
预防性保护事件	侦测到的安全威胁
应用程序监控事件	应用程序监控按照进程活动性的统计信息 应用程序监控按照被阻止进程的统计信息
代理端安装	代理端安装

查看不同组件运行结果和工作站总计信息使用的是同一界面，细化信息的操作相同。

以下是通过管理中心查看总计信息的举例。

8.6.1.1. 汇总数据

查看汇总数据

1. 在分层列表选择工作站或组。
2. 在控制菜单选择**统计信息**中的**汇总数据**选项。
3. 打开的窗口中显示当前数据列表。

如果需要在报表中体现一定的统计信息，请点击工具面板上的，在下拉列表选择需要的类型：**扫描统计信息**、**威胁**、**任务**、**启动/完成**、**错误**。此报告各部分的统计数据对应**报表**部分各项的统计数据。查看所选报表数据需点击**更新**。

4. 如果报告中包含侦测到的威胁报表，可在控制面板选用以下选项：

选项	描述
排除对文件的扫描	用于将所选对象添加到保护组件扫描排除项列表： a) 在**威胁**报表勾选一个或多个侦测到的对象。 b) 点击。 c) 在打开的窗口给出以下设置： • **设为扫描排除项并指定SpIDer Guard自身设置**——将所选对象添加到组件SpIDer Guard扫描排除项列表。此时如果排除项列表发生更改的网络节点之前是从其基组继承了SpIDer Guard组件设置，则会中断继承并出现自身设置。 • **设为扫描排除项并指定Dr.Web扫描仪自身设置**——将所选对象添加到组件Dr.Web扫描仪扫描排除项列表。此时如果排除项列表发生更改的网络节点之前是从其基组继承了Dr.Web扫描仪组件设置，则会中断继承并出现自身设置。 • **在为下列对象设置排除项**列表选择所选对象将列入其排除项列表的网络节点：可以是发现此对象的工作站，或是列表中的工作站和用户组。 d) 点击**排除**按钮。
扫描	二次扫描所选对象。在下拉列表选择扫描类型。

5. 显示某一时段的数据可以：在下拉列表选择相对于今日的时段，或者在工具面板自行设定时段。自行设定时段时可输入日期或点击日期栏旁边的日历图标。加载数据需点击**更新**。
6. 如需可利用以下按钮保存统计信息报表以便打印或进行后续处理：
   - 将数据保存到**CSV**文件，
   - 将数据保存到**HTML**文件，
   - 将数据保存到**XML**文件，
   - 将数据保存到**PDF**文件。

8.6.1.2. 扫描统计信息

获取工作站反病毒软件运行统计数据

1. 在分层列表选择工作站或组。

> 如需查看几个工作站或组的统计信息，可以使用SHIFT或CTRL按键同时选择多个对象。

2. 在控制菜单选择**统计信息**中的**扫描统计信息**选项。
3. 打开统计信息窗口。默认设置是显示最近24小时的统计数据。

4. 显示某一时段的数据可以：在下拉列表选择相对于今日的时段，或者在工具面板自行设定时段。自行设定时段时可输入日期或点击日期栏旁边的日历图标。加载数据需点击**更新**。打开统计信息列表。
5. 查看具体反病毒工具运行详细信息需点击工作站名称。打开统计数据详细信息列表窗口（或当前窗口的子窗口）。
6. 点击相应列标题中的箭头（递增顺序或递减顺序）可以进行数据排序。
7. 如需可利用以下按钮保存统计信息报表以便打印或进行后续处理：

   将数据保存到**CSV**文件，

   将数据保存到**HTML**文件，

   将数据保存到**XML**文件，

   将数据保存到**PDF**文件。
8. 查看病毒事件的图形统计需点击控制菜单选择**图表**一项。打开统计图信息窗口（详细介绍见下）。

8.6.1.3. 状态

查看工作站状态信息

1. 在分层列表选择工作站或组。
2. 在控制菜单选择**统计信息**中的**状态**选项。
3. 工作站状态信息按照过滤器设置显示。点击表头的可更改过滤器以下参数：
   - 在**搜索**栏输入搜索内容，在整个报表进行搜索。
   - 在**重要性**列表勾选通知的重要性：状态调整列表只包含具备所选重要性的通知。
   - 在**来源**列表勾选将在列表中显示的事件的来源：
     - **代理端**——显示来自连接本Dr.Web服务器的代理端的事件。
     - **服务器**——显示来自本Dr.Web服务器的事件。
   - 在**工作站**列表勾选将在列表中显示的工作站的状态类型：
     - **在线**——显示连接本Dr.Web服务器且当前在线（online）的工作站的事件。
     - **离线**——显示连接本Dr.Web服务器且当前离线（offline）的工作站的事件。
     - **已删除**——显示删除Dr.Web反病毒软件的工作站的最后一个事件。

   可使用过滤器列表的下列按钮管理过滤器设置：
   - **默认**——将过滤器所有设置设定为默认值。
   - **更新**——应用所选过滤器设置。
4. 获取此报表更详细的信息和进行数据排序的操作同扫描统计信息列表。

   还可查看多个工作组的运行结果个统计信息，只需在分层列表中选出需要查看的工作站。
5. 如需可利用以下按钮保存报表以便打印或进行后续处理：

   将数据保存到**CSV**文件，

- 将数据保存到**HTML**文件，
- 将数据保存到**XML**文件，
- 将数据保存到**PDF**文件。

8.6.1.4. 应用程序监控事件

设置获取统计信息

激活从工作站向应用程序监控事件发送信息

1. 在**反病毒网络**树结构选择安装有应用程序监控并需要收集其应用程序启动信息的工作站或工作站组。
2. 在控制菜单选择**Windows → Dr.Web代理端**一项。
3. 在**常规**标签勾选**追踪应用程序监控事件**，勾选后追踪应用程序监控组件在工作站记录到的进程活动，并将事件信息发送至Dr.Web服务器。未与Dr.Web服务器连接时会积累事件记录并在建立连接后发送。如取消勾选则忽略进程活动。
4. 点击**保存**。

激活Dr.Web服务器为应用程序监控事件收集信息的操作

1. 在**管理 → Dr.Web服务器配置**打开**统计信息**标签。
2. 选择下面一个选项：
   - **应用程序监控按照进程活动性的统计信息**，此项用于获取和记录所有进程的任何活动：既包括应用程序监控允许的进程，也包括禁止的基础。选择此项后手册会记录应用程序，前提是创建和指定了至少一个模式，包含功能分析依据的标准的一个或几个类型。在创建模式并将其指定给反病毒网络工作站前，允许启动所有应用程序。
   - **应用程序监控按照被阻止进程的统计信息**，此项用于获取和记录应用程序监控禁止启动所有进程的活动。选择此项后手册只在创建阻止应用启动的模式并将其指定给反病毒网络工作站后开始记录应用程序。

   > 应用程序监控按照进程活动性的统计信息会大大增加整个反病毒网络信息收集的总量。

3. 点击**保存**按钮。
4. 请重启Dr.Web服务器。
5. 重启Dr.Web服务器后开始按照指定的设置记录从所有安装有应用程序监控的工作站发送来的所有统计信息。

查看统计信息

查看应用程序监控组件在工作站发现的事件

1. 在分层列表选择工作站或组。
2. 在控制菜单选择**统计信息**中的**应用程序监控事件**选项。

3. 打开的窗口为所选工作站被禁止或允许的应用列表。
4. 默认显示最近一日的统计信息。显示某一时段的数据可以：在下拉列表选择相对于今日的时段，或者在工具面板自行设定时段。自行设定时段时可输入日期或点击日期栏旁边的日历图标。加载数据需点击**更新**。将加载统计信息列表。这一列表各列内容的相关介绍见下表。

表8-5. 应用程序监控事件列表各列内容的相关介绍

列名称	描述
识别码	工作站识别码
工作站	工作站名称
工作站地址	工作站地址
安全识别码	用户账户安全识别码
用户	工作站用户
事件类型	工作站上已启动事件的类型
应用的操作	针对工作站上已启动应用的操作
功能分析依据的标准	允许或禁止应用所依据的标准
功能分析的隐码	功能分析所依据标准的参数，用于确定是否允许应用在工作站启动
模式ID	模式识别码
模式名称	模式名称
规则ID	规则识别码
规则名称	规则名称
运行模式	规则开始使用的模式
进程文件路径	进程文件的位置
进程	被允许或禁止在工作站启动的进程
进程哈希公报	内含已启动进程文件哈希值的公报
脚本文件路径	脚本文件的位置
脚本	脚本文件
脚本哈希公报	内含已启动脚本文件哈希值的公报
事件的出现	事件出现的日期和时间，
事件通知	发出事件通知的日期和时间

列名称	描述
文件哈希值（**SHA-256**）	按照SHA-256算法的哈希值
文件描述	文件描述
出品人	文件出品人
证书出品人	发布证书的验证中心
证书哈希值（**SHA-1**）	按照SHA-1算法的证书哈希值
证书生效日	证书生效日
证书失效日	证书失效日

5. 如需可利用以下按钮保存统计信息报表以便打印或进行后续处理：
   将数据保存到**CSV**文件，
   将数据保存到**HTML**文件，
   将数据保存到**XML**文件，
   将数据保存到**PDF**文件。

有模式或规则处于测试模式时自始自终按照应用程序监控运行模式对工作站启动的应用进行检查。统计信息中记录应用与所有可能类型出现的相符情况：功能分析设置、规则和可信任应用组。因此，同一个应用可能在**所采取的操作**一栏出现多个记录，也就是按照某类型允许使用和/或按照另一类型被阻止。

创建规则

根据应用程序监控事件统计信息创建新规则

1. 在**统计信息** → **应用程序监控事件**选择为其创建启动监控规则的试图启用应用事件行：
2. 点击信息行就会打开所选事件信息窗口。
3. 点击**创建规则**。
4. 打开新规则创建窗口。给出以下设置：
   a) 在**模式名称**下拉列表选择为其创建新规则的应用程序监控模式。
   b) 在**规则名称**指定所创建的规则的名称。
   c) 在**规则类型**选择所创建规则的类型：禁止性或允许性。
   d) 在**运行状态**选择所创建规则的运行状态（与从模式创建规则时**将规则转为测试状态**选项相符）。
   如需检查规则的运行情况，需选择**测试**状态。此状态下不会在工作站阻止应用，但会和启用规则一样记录事件日志。规则测试模式下对应用的启动和阻止结果会体现于**应用程序监控事件**。
   在**活跃**模式下按照规则在工作中阻止应用（参见模式运行模式）。

e) 在**按下列标准禁止应用程序启动/按下列标准允许应用程序启动**（取决于在4c一步选择的规则类型）部分会自动填写应用程序信息。如需可编辑设置。

5. 点击**保存**。新规则会添加到指定的应用程序监控模式。

8.6.2. 图表

感染图表

查看侦测到的感染图表信息

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。在打开的控制菜单选择**常规**部分的**图表**一项。
2. 打开的窗口含以下图形和数据：
   - **病毒活动**——图表显示每一时段在所有所选工作站和组侦测到的恶意对象总数。
   - **最流行的威胁**——十种感染文件数量最多的威胁。图表中显示具体威胁对应的被感染对象数量信息。
   - **威胁类型**——根据恶意对象分类给出威胁列表。圆周图显示所有威胁所占比例。
   - **已采取的操作**——对侦测到的恶意对象已采取的操作列表。圆周图显示所有操作所占比例。
   - **受攻击最严重的工作站**——发现安全威胁的工作站列表。表中显示每一工作站上侦测到的威胁总数。
3. 查看预设时间段内的图形数据需在任务面板下拉列表选择某一日或某一月。或指定任意时段，可输入日期或在下拉日历选择日期。查看数据需点击**更新**按钮。

汇总图表

常规部分**图表**一项和控制菜单**统计信息**的部分选项可显示图形和数据。下表为所有可能收集的图表和相应的控制菜单选项。

表**8-6**控制菜单各项图表对应关系

图表	菜单选项
病毒活动	图表
最流行的威胁	图表 威胁 威胁统计信息
感染类型	图表 威胁统计信息
受攻击最严重的工作站	图表
已采取的操作	图表

图表	菜单选项
	威胁
按工作站分列错误数量	错误
按组件分列错误数量	错误
按组件分列威胁	启动/完成
按组件分列错误	启动/完成

- **工作站错误数量**——反病毒组件功能出现错误的工作站列表。图表显示每一工作站上出现的错误总数。
- **组件错误数量**——显示工作站上运行发生错误的组件。圆周图显示所有组件错误所占比例。
- **组件威胁侦测**——侦测到安全威胁的反病毒组件列表。图表显示每一组件侦测到的威胁总数。
- **组件错误**——显示运行发生错误的反病毒组件列表。图表每一组件错误总数。

8.6.3. 隔离区

隔离区内容

反病毒软件的某个组件可隔离文件，如扫描仪。

用户可自己对隔离区中的文件进行二次扫描，方式可以是利用管理中心或通过工作站上的隔离区管理器。

在管理中心查看和编辑隔离区内容的操作

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。在控制菜单选择**常规**部分的**隔离区**一项。
2. 打开的窗口中显示隔离区当前状态数据列表。

   如选择的是一个工作站，则显示的是该工作站隔离区中的对象列表。

   如选择的是几个工作站、一个组或几个组，则显示的是一系列列表。每一列表为每一工作站的隔离区对象。



隔离区对象二次扫描统计信息显示于**信息**一列，只记录通过管理中心启动的二次扫描。

如隔离的不止一个威胁，在下拉列表查看所有威胁列表需点击**信息**一列的隔离对象数量。

如隔离区对象出现状态**未感染**，说明对一开始被判断为威胁在隔离后进行了二次扫描，二次扫描结果为对象是安全的对象。

只可手动从隔离区还原对象。

3. 查看某一时段被隔离的文件可指定相对于今日的时段，或者在工具面板自行设定时段。自行设定时段时可输入日期或点击日期栏旁边的日历图标。查看数据需点击**更新**。
4. 更改数据显示请在表头点击图标。
   - 设置行的显示（适用于长字符行）。
   - 选择要在报表中显示的列。
5. 筛选隔离区文件需点击表头的按钮，设置以下筛选参数：
   - **搜索**——指定搜索内容，在整个报表进行搜索。表中将只显示与搜索行相符的搜索结果。
   - **执行隔离操作的组件**——选择隔离文件的Dr.Web保护组件。
   - **威胁**——选择根据Doctor Web公司分类标准确定的威胁名称。
   - **原名**——请输入对象被隔离前的名称。
   - **文件大小，B**——利用滑块指定侦测到的对象的大小区间，以字节计。

   点击**应用**以便显示隔离区文件筛选结果。

   点击**按照默认设置**以便将所有筛选参数恢复为初始值。
6. 处理隔离区文件需先勾选相应的一个或多个文件，或者全选打开的隔离区页面的文件（在表头勾选），在工具面板选择以下一种操作：

选项	描述
删除文件	
删除所选文件	将所选文件从隔离区以及从系统中删除。
删除所有文件	删除符合所选参数的所有文件，也就是隔离区窗口显示d所有文件。
导出	扶着并保存所选文件。 可疑文件移至用户计算机本地隔离区文件夹后，可以通过管理中心复制并保存这些文件。这个功能可用于将文件发送给Doctor Web公司病毒实验室进行分析。 导出时文件会保存在压缩包内，压缩包的名称是所导出的文件的哈希值。压缩包中除了导出的对象，还有一个CSV文件，是有关对象的常规选项。默认情况下压缩包有密码保护，密码是virus。

选项	描述
还原文件	
	只有确认隔离区文件是安全对象时才可使用还原功能。
还原所选文件	将所选文件恢复到该文件在计算机上的初始位置，即将文件返回到移动至隔离区前在工作站的所处文件夹。
按照参数还原文件	在打开的窗口给出以下设置： • 如果只选择了一个对象： ▫ **将文件还原为**——将所选文件以指定名称还原至指定文件夹。在**将文件还原至这一路径**指定工作站上用于还原文件的完整路径。必须包含文件名称。默认为隔离前所在路径和隔离前的文件名。如需可更改此参数。 ▫ **按照威胁类型还原文件**——还原隔离区属某威胁类型的所有文件。威胁类型在**还原包含这一威胁的文件**一栏指定。 ▫ **按路径还原文件**——还原从某目录隔离的所有文件。在**还原从以下目录隔离的所有文件**指定工作站目录路径。从此目录隔离的所有文件将被还原。按照默认设置是所选文件所在目录的路径。如需可更改此参数。 • 选择多个对象时： ▫ **还原文件**——将文件恢复到该文件在计算机上的初始位置，即将文件返回到移动至隔离区前原来所在的文件夹。 ▫ **按照威胁类型还原文件**——还原隔离区与所选文件属同一威胁类型的所有文件。 • 在**在以下对象还原**选择将还原所选对象的网络节点：可以是发现此对象的工作站，或是列表中的用户组。 • **设为扫描排除项并指定SpIDer Guard自身设置**——将所选对象添加到组件SpIDer Guard扫描排除项列表。此时如果排除项列表发生更改的网络节点之前是从其基组继承了SpIDer Guard组件设置，则会中断继承并出现自身设置。 • **设为扫描排除项并指定Dr.Web扫描仪自身设置**——将所选对象添加到组件Dr.Web扫描仪扫描排除项列表。此时如果排除项列表发生更改的网络节点之前是从其基组继承了Dr.Web扫描仪组件设置，则会中断继承并出现自身设置。
还原所有文件	将隔离区窗口所有文件恢复到该文件的初始位置，即将文件返回到移动至隔离区前在工作站的所处文件夹。

选项	描述
扫描文件	
扫描所选文件	对所选隔离区文件进行二次扫描。
扫描所有文件	对隔离区所有文件进行二次扫描。

离线工作站再次连接Dr.Web服务器后即会向其发送还原要求和二次扫描要求。

7. 可用以下一种格式导出隔离区状态数据：
   - 将数据保存到**CSV**文件，
   - 将数据保存到**HTML**文件，
   - 将数据保存到**XML**文件，
   - 将数据保存到**PDF**文件。

8.7. 分发安装文件

在工作站创建新的用户账户时管理中心就会生成一个用于安装Dr.Web代理端的安装包。安装包包含Dr.Web代理端安装程序、Dr.Web服务器连接参数及工作站登录Dr.Web服务器参数（安装包以及利用安装包进行代理端安装的相关介绍参见**安装手册**中的Dr.Web代理端本地安装）。

创建安装包后可将安装包分发到用户邮箱。

分发安装包时邮件内容：

1. 在设置中禁止附件（勾选**只发送链接**，见下）：邮件只包含软件包下载链接。
2. 工作站操作系统为已知（允许附件）：
   a) OS Windows：邮件附件为用于Windows操作系统的Dr.Web代理端。
   b) OS Linux、macOS、OS Android：邮件附件为相应操作系统的Dr.Web代理端安装文件和包含Dr.Web服务器连接设置配置文件。
3. 工作站操作系统未知——新的工作站账户，代理端尚未安装（允许附件）：
   a) 如Dr.Web服务器上没有OS Linux、macOS、OS Android工作站安装包（如Dr.Web服务器未加载**Dr.Web企业产品**）：邮件附件为用于Windows操作系统Dr.Web代理端安装文件和用于OS Linux、macOS、OS Android工作站的Dr.Web服务器连接设置配置文件。
   b) 如Dr.Web服务器上除了OS Windows安装包，还至少有一个其他操作系统的安装包：邮件附件为用于Windows的Dr.Web代理端安装文件和用于OS Linux、macOS、OS Android工作

站的Dr.Web服务器连接设置配置文件，以及下载OS Linux、macOS、OS Android工作站安装文件的链接。

利用电子邮箱群发安装包

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中选择以下对象：
   - 选择为其生成了安装包的工作站。
   - 选择为其生成了安装包的工作站组。

   同时选择多个对象使用CTRL或SHIFT按键。
2. 在工具面板点击**常规**→**分发安装文件**。
3. 在打开的**分发安装文件**窗口给出以下参数：
   - 在**常规**部分：
     - 勾选**打包为zip压缩文件**。将安装包打包为压缩文件可以避免因用户邮件系统禁止邮件附件为执行文件而无法发送安装包。
     - 勾选**只发送链接**后邮件中只发送下载安装包的链接，而不发送安装包文件附件。此选项适用于客户邮件服务器自动删除邮件附件的情况。
   - 在**收件人电子邮箱**指定发送安装包的电子邮箱地址。如选择了多个工作组或工作站组，需分别在工作站名称旁指定相应的电子邮箱地址。

   设置发送电子邮件的参数在**管理**菜单的**Dr.Web服务器配置**中的**网络**标签的子标签 电子邮件。
4. 点击**发送**按钮。

8.8. 向工作站发送通知

系统管理员可以向用户发送通知，通知内容可自行编辑，包括：

- 消息正文；
- 网络资源超链接；
- 公司标志（或其他图形）；
- 窗口标题中显示接收通知的确切日期。

通知在用户端以弹出窗口方式显示（见 图8-1）。

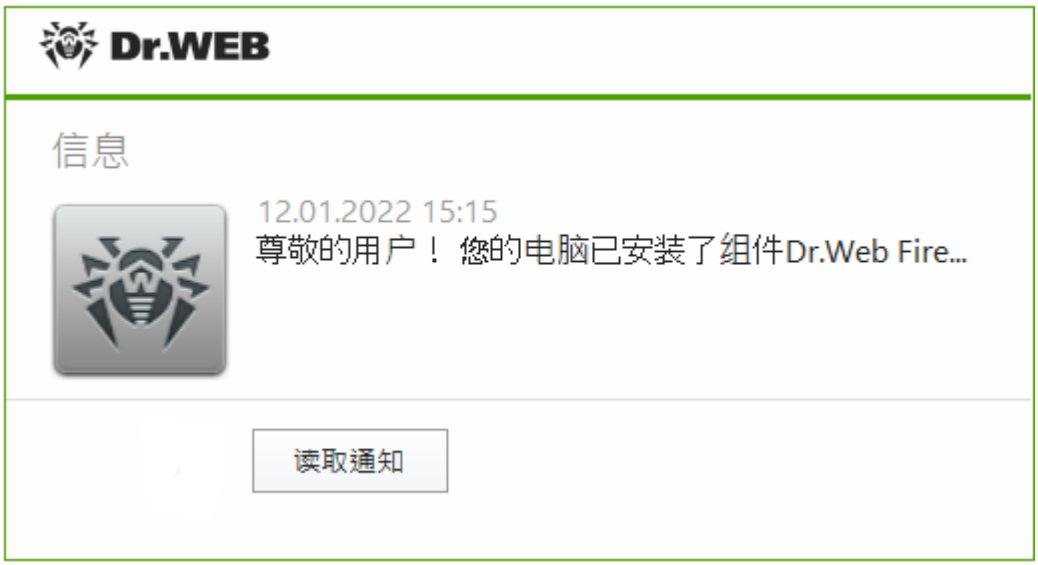


图 **8-1. OS Windows**工作站通知窗口

向用户发送通知

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在打开窗口的分层列表中点击工作站或组的名称，然后点击工具面板的**常规**→ **向工作站发送通知**。
3. 在打开的窗口填写以下栏目：
   - 在**通知标题**指定通知的标题，例如可在此输入公司名称。此内容将在通知标题中徽标右侧显示。如此栏为空，则通知窗口标题为通知相关信息。
   - **消息正文**——必填项。
   - 勾选**在通知中显示徽标**后可在通知窗口标题显示图标。需给出图标的以下参数：
     - 点击**徽标文件**右侧的按钮可本地计算机加载图形文件，需在打开的文件系统浏览器中选择需要的对象（参见徽标文件格式）。
   - 勾选**在通知中显示链接**后可在通知中加入网路资源超链接。

   添加链接需要：

   a) 在**链接名称**一栏输入链接的文字名称，这一文字将在通知中包含的链接位置显示。

   b) 在**链接URL地址**一栏给出点击链接打开的网页的URL地址。

   c) 在**通知内容**添加`{link}`，加入标记的地方都会出现指定的链接。通知中`{link}`标记的数量不限，但所有的链接都有同样的参数（由**链接URL地址**和**链接名称**两栏设定）。存在一个或多个`{link}`标记时，链接将只置于标记所在处。

   d) 如**{link}**未在通知内容中给出，链接将出现在通知结尾，单列一行。
   - 勾选**只向在线工作站发送通知**后，通知只发送给在网络中的工作站（online）。勾选此项后不会向离线工作站发送通知。如取消勾选，则会在离线工作站连接后发送通知。
   - 勾选**显示发送状态**后会显示通知发送状态。
4. 点击**发送**按钮。

徽标文件格式

通知中加入的图形文件（徽标）应符合以下条件：

1. 图形文件格式：BMP、JPG、PNG、GIF、SVG。
2. 图形文件大小不应超过512KB。
3. 图形大小为72x72像素。不是此大小的图形在发送时会调整为默认大小。
4. 颜色深度（位深）为任意（8–24位）。



如需在通知中显示透明底色的标志，需使用PNG或GIF格式的文件。

在发送用户通知，特别是在群发前建议先发送到一台安装有代理端的计算机，以便检查是否得当。

通知发送示例

发送图8-1这个通知时，指定的参数是：

通知内容：

```
尊敬的用户！


您的电脑已安装了组件Dr.Web Firewall，此组件为防火墙。

查看此组件功能的详细信息请点击{link}。


此致

敬礼！

网络管理员
```

链接URL地址： http://drweb.com/

链接名称： 这里

第九章、管理虚拟环境的工作站

Dr.Web Enterprise Security Suite可保护虚拟环境，也就是为客户端提供服务是虚拟机群集（以下简称*客户虚拟机*）：虚拟主机、远程办公系统、企业云盘等等。

群集中的一个或几个虚拟机获得*服务器*角色；在这些虚拟机安装专门的软件（Dr.Web扫描服务器），利用这一软件处理来自客户虚拟机的反病毒扫描请求。

扫描服务器包括：

- 扫描引擎，功能的对数据进行威胁侦测；
- 病毒库以及办公控制的内置过滤器数据库。

在客户虚拟机安装Dr.Web虚拟代理端，由统一保护服务器的管理，向服务虚拟机传递扫描申请以及需要扫描的文件。这种保护方式可以大大减少客户虚拟机的负载，原因是：

- 扫描在客户虚拟机外进行；
- 没有必要保证每个客户虚拟机有最新的病毒库和内置过滤器数据库；
- 使用虚拟网络（而非物理网络）来在同一服务器（管理程序）下的虚拟机之间传递数据，这样可以保证数据交换的数据和扫描速度。

扫描服务器可以是任何一个组的成员。也可将所有扫描服务器归为一个组，包括可以按照设定的组籍规则自动归组。

> 将扫描服务器添加到组以及组籍规则的设置于其他工作站无异。组管理详细信息参见将工作站添加到组。

工作站利用在虚拟环境运行的代理端与扫描服务器进行交互作用。虚拟代理端在统一保护服务器的控制下运行，向扫描服务器传递检查文件和URL的申请。

9.1. 将工作站接通扫描服务器的操作

扫描服务器——是一个虚拟机，具备特殊身份，安装有专用软件，用于处理其他虚拟机的扫描申请。

扫描服务器安装步骤和设置相关介绍详见**Dr.Web Enterprise Security Suite**安装手册中的Dr.Web扫描服务器的安装。

> 只有您的授权允许的情况下才可将工作站接通扫描服务器。

将工作站接通扫描服务器的操作

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在反病毒网络树结构选择需接通扫描服务器的工作站或组。
3. 在**配置**部分选择**虚拟代理端**。

4. 勾选**使用扫描服务器**后在**扫描服务器的网络地址**一栏输入扫描服务器地址。

> 一个虚拟代理端只可指定一个扫描服务器的地址。
>
> 如不需指定具体的地址，请使用默认设置udp://:18008 ——这时会自动确认扫描服务器，不取决于为其指定的是IPv4还是IPv6。

可使用以下一种格式指定地址：

- tcp://<IP地址>:<端口> （可以指定为IPv4地址或IPv6地址；指定IPv6地址使用方括号，如tcp://[fd15:4ba5:5a2b:1008:edc8:733e:1dd7:789c]:7777）；
- udp://:<端口> （这种格式只指定工作站搜索扫描服务器使用的协议和端口）；
- srv://service@<domain>（通过搜索DNS域名<domain>的SRV记录确定服务所在服务器的地址和端口； 如未给出域名，会从DNS设置文件的search栏或domain栏提取，取决于哪一栏在设置文件中排在最后）。

5. 点击**保存**按钮。

高级设置

使用扫描服务器要求用户具备相应的权限等级。

默认所有工作站用户都具备启动扫描服务器的权限，但没有暂停和更改配置的权限。如需可为反病毒网络管理员提供高级权限。管理员可以完全禁止个别工作站或组使用扫描服务器。

权限相关详细信息参见工作站用户权限。

在扫描服务器以及连接扫描服务器的UNIX操作系统工作站都可以指定高级设置，使用的是配置文件drweb.ini （[MeshD]部分）。可利用管理中心更改drweb.ini文件（在工作站设置中选择**UNIX →Dr.Web代理端 → 配置**）。

这些设置的详细描述见下表。

> 在Windows操作系统工作站只可指定扫描服务器地址。下表中其他设置都不支持。

参数	描述
LogLevel *{详细等级}*	记录日志的详细等级。可选择以下一个数值： • DEBUG——最详细的等级（调试等级）。输出所有通知以及调试详细。 • INFO——输出所有通知。 • NOTICE ——输出有关错误的通知、预警和通知。 • WARNING ——输出有关错误的通知和预警。 • ERROR ——只输出有关错误的通知。 **默认值：** Notice

参数	描述
Log *{日志类型}*	记录日志的方式。可选择以下一个数值： • Stderr[:ShowTimestamp] —— 通知将以标准错误流stderr输出。 • Auto —— 需记录的通知传输到工作站上的配置管理Dr.Web ConfigD的守护进程，由其将记录根据相应设置统一保存至一处。 • Syslog[:*<facility>*] — 通知将由系统日志服务组件 **syslog** 传输。. • 补充标记 *<facility>*用于指定syslog用于保存通知的日志类型。可用参数值： ▫ DAEMON——守护进程通知； ▫ USER——用户进程通知； ▫ MAIL ——邮箱程序通知； ▫ LOCAL0 ——本地进程0通知； … ▫ LOCAL7——本地进程7通知； ▫ *<路径>* ——通知将直接保存到工作站的指定文件。 **默认值：** Auto
IdleTimeLimit *{时间间隔}*	虚拟代理端或扫描服务器无操作最长时限，超时则结束运行。 扫描服务器和虚拟代理端都将设置此参数。 如设置为 None，虚拟代理端/扫描服务器会始终运行；在无操作时不会向其发送信号 SIGTERM。 最小值—— 10s。 **默认值：** 30s
DebugSsh *{逻辑}*	指定在已将日志详细等级设定为LogLevel = Debug的情况下是否需要在工作站进行SSH协议通知日志记录。 **默认为：** no
ListenAddress *{<IP地址>:<端口>}*	客户端连接套接字（地址和端口），扫描服务器在此套接字等待客户端工作站连接。 只在扫描服务器设置此参数。 必需给出此参数，以便扫描服务器能够监听IPv6接口并通过IPv6为虚拟代理端提供服务。 IPv6地址使用方括号。 如此参数为空行，扫描服务器会结束运行。

参数	描述
	将此参数设置为''（也就是空行），必须同时具备停用和更改扫描服务器配置的权限。.
DnsResolverConfPath *{路径}*	域名允许子系统（DNS resolver）设置文件的路径。 如扫描服务器地址使用的是SRV记录，需为虚拟代理端设置此参数。 **默认值：** /etc/resolv.conf
DiscoveryResponderPort *{端口}*	扫描服务器按照UDP协议响应客户端申请的端口。 **默认值：** 18008
EngineChannel *{On / Off}*	启用或停用服务器提供扫描引擎服务。 只在扫描服务器设置此参数。 **默认值：** On 将此参数更改为Off必须同时具备停用扫描服务器和更改其配置的权限。
EngineUplink *{地址}*	扫描服务器地址（与利用管理中心设置时格式相同）。 只在虚拟代理端设置此参数。 **默认值：***未指定*
EngineDebugIpc *{逻辑}*	指定在已将日志详细等级设定为 LogLevel = Debug的情况下是否需要记录扫描服务调试信息。 **默认为：** no
UrlChannel *{On / Off}*	启用或停用服务器提供URL扫描服务。 **默认值：** On 将此参数更改为Off必须同时具备停用扫描服务器和更改其配置的权限。
UrlUplink *{地址}*	用于扫描URL的上级节点的地址。 只在虚拟代理端设置此参数。 **默认值：***未指定*
UrlDebugIpc *{逻辑}*	指定在已将日志详细等级设定为 LogLevel = Debug的情况下是否需要记录URL扫描服务调试信息。 **默认为：** no

9.2. 与虚拟桌面基础架构集成

Dr.Web Enterprise Security Suite支持与与虚拟桌面基础架构（VDI）的集成。在与支持RDP协议终端模式的*瘦客户端*运行时会用到这一功能。

这时反病毒网络的运行方式是：

1. 反病毒网络管理员创建预装软件和Dr.Web代理端的*虚拟工作组标准镜像*，之后将其连接到Dr.Web服务器。
2. 利用创建的镜像克隆需要的虚拟工作站。
3. 指定时间段过后虚拟工作站会被删除。需要时会重新利用创建的镜像克隆虚拟工作站。

与VDI运行前对反病毒网络进行的设置

1. 在管理中心主菜单选择**反病毒网络**一项，创建将作为标准镜像的工作站。。
2. 将Dr.Web代理端和所有必要的软件安装到创建的工作站。将工作站连接至Dr.Web服务器。
3. 将一个工作站指定为扫描服务器并安装相应软件。
4. 在所创建的工作站的设置中指定使用扫描服务器。指定工作站需连接的扫描服务器地址。
5. 在同一位置创建新组，虚拟工作站将在此组中。
6. 设置虚拟工作站注册次序。操作是在管理中心进入**管理** → 自定义钩子。以事件**新工作站连接Dr.Web服务器**为基础添加新钩子。在**钩子文字**一栏输入：

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

if args.id == '<标准工作站识别码>' then

  return { "id", dwcore.get_uuid(), "pgroup", "<基组识别码>" }

end
```

在*<标准工作站识别码>*必须输入在第1步创建的标准工作站的ID。在*<基组识别码>*输入在第5步创建的组的ID。这些信息科随时在 **反病毒网络**树结构的对象属性中查看。

克隆是每个新的虚拟工作站会获得与标准工作站识别码相同的识别码。按照钩子工作站在连接Dr.Web服务器是会为其生成新的UUID，之后工作站以识别码在基组注册。

编写钩子时建议与内置的**新工作站连接Dr.Web服务器**钩子模板进行比对。在管理中心钩子树结构选择**Examples of the hooks** → **新工作站** → **新工作站连接Dr.Web钩子服务器**后可确认信息，包括可能的供选参数和返回值。

按时删除不使用的虚拟工作站

为合理分配授权一级避免数据库积存虚拟工作站删除信息起见，需要设置任务，用于自动删除不使用的工作站。不使用的工作站值的是在指定的时间段未连接过Dr.Web服务器的工作站。

指定自动删除不使用的工作站这一任务的操作

1. 在管理中心进入**管理** → **Dr.Web服务器任务计划器**。

2. 在工具面板点击**创建任务**后创建新任务。
3. 在**操作**标签下拉列表选择**执行脚本**，之后从单独文件导入，或手动在下面的输入栏输入以下Lua脚本：

```
local adminName = 'admin'
-- 输入组ID
local gid       = '<基组识别码>'
-- 指定非活跃状态时段（以秒计）
localinterval=86400


require('st-db-state')
require('core/datetime')
require('core/admins/admins')
local lastseen = Datetime.timeUnixstampToDBFormat(Datetime.nowTimestamp()
- interval)
local stations = {}
-- 执行向数据库发出请求
local res, err1 = DBuilder()
    :select('id, lastseenat')
    :from('stations')
    :where('gid', gid)
    :where('lastseenat '..dwcore.base64_decode('PA=='), lastseen)
    :where('state !=', st_db_state.st_db_state_logged_in)
    :get()
if res and next(res) then
  for i = 1, #res do
    table.insert(stations, res[i][1])
  end
end
-- 删除不活跃的工作站
local function delete_stations(ids)
  local admin, err    = Admin:initWithLogin(adminName)
  require 'core/admins/admins'
  require('core/stations/stations')
  local status, results_stations = Stations:delete(ids, admin)
  return ''
end
return delete_stations(stations)
```

在*<基组识别码>*输入在与VDI集成的准备阶段的第5步创建的组的ID。

此脚本会从数据库获得在最近24小时（86400秒）未连接过Dr.Web服务器的工作站的ID，并从相应ID的组中删除这些工作站。

建议每次有要求重启操作系统的反病毒组件更新后都要更新标准镜像。更新后检查一下标准工作站识别码，如需在钩子文字中进行复制。

第十章、Dr.Web服务器设置

本章介绍的是对反病毒网络和Dr.Web服务器运行参数的下述管理功能：

- 授权管理——授权参数；
- 记录日志——查看并管理Dr.Web服务器运行日志，查看Dr.Web服务器运行详细统计信息；
- 设置Dr.Web服务器配置——设置Dr.Web服务器运行参数；
- Dr.Web服务器日程设置——设置Dr.Web服务器维护任务日程；
- 设置Web服务器配置——设置Web服务器运行参数；
- 自定义钩子——连接和设置用户进程；
- 通知设置——设置反病毒网络事件管理员通知系统以及通知发送方式；
- 管理Dr.Web服务器库——设置用于从GUS更新所有反病毒网络组件的库以及向工作站分发更新；
- 数据库管理——对Dr.Web服务器数据库的直接维护；
- 多台Dr.Web服务器网络特点——多服务器反病毒网络配置及服务器间连接设置；
- 与虚拟桌面基础架构集成——Dr.Web服务器设置，用于使用虚拟桌面的基础架构（VDI）。

10.1. 授权管理

10.1.1. 授权管理器

Dr.Web Enterprise Security Suite授权原则和特点详见授权。

授权管理器界面

授权管理器包含于管理中心。这一组件用于管理反病毒网络对象的授权。

打开授权管理器窗口需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**授权管理器**。

密钥分层列表

授权管理器主窗口是密钥树结构——分层列表，其节点为授权密钥，和指定了授权密钥的工作站、组和策略。

工具面板包括以下元素：

选项	描述	密钥树结构中的对象从属性
添加授权密钥	添加密钥文件新纪录。	此选项无条件可选。 功能取决于是否在密钥树结构选择了一个对象（参见添加新的授权密钥）。
删除所选对象	删除密钥与授权对象的关联。	在密钥树结构选择了一个对象（工作站、组或策略）或授权密钥后可使用此选项。
将密钥分发到组和工作站	将所选密钥替换或添加给授权对象。	在密钥树结构选择了一个授权密钥后可使用此选项。
导出密钥	保存书签密钥文件的本地备份。	
检查是否有更新并替换授权密钥	为所有密钥检查GUS是否有更新。有更新时会下载密钥并进行替换（见自动更新授权）。	此选项无条件可选。 操作适用到树结构中的所有授权密钥。
将密钥分发至Dr.Web邻居服务器	将所选密钥中的授权分发给Dr.Web邻居服务器。	在密钥树结构选择了一个授权密钥后可使用此选项。

通过设置树结构可以改变分层列表的显示：

- 复选框**显示授权数量**用于启用/停用在密钥树结构显示授权密钥文件可提供的授权总数。
- 可使用以下选项更改树结构：
  - **密钥**这一选项的功能是将反病毒网络所有授权密钥显示为分层树结构的根节点。具备相应授权密钥的组、工作站和策略成为内含元素。这是树结构的基本显示方式，用于管理授权对象和授权密钥。
  - **组**这一选项的功能是将包含直接为其指定了授权密钥的对象的组显示为分层树结构的根节点。组内工作站和策略以及为这些对象指定的授权密钥成为内含元素。这种树结构用于直观显示授权信息，不能对树结构对象进行管理。
- 可使用以下选项更改树结构：
  - **显示客户端识别码**——启用 / 停用显示工作站特有识别码。
  - **显示客户端名称**——启用 / 停用工作站名称的显示工作站。
  - **显示客户端地址**——启用 / 停用显示工作站IP地址。
  - **显示描述**——启用 / 停用显示工作站和工作站组描述。

使用授权

利用授权管理器可以对授权密钥进行以下操作：

1. 查看授权相关信息。
2. 添加新的授权密钥。
3. 更新授权密钥。
4. 更换授权密钥。
5. 扩展授权密钥列表。
6. 删除授权密钥、删除授权列表中的对象。
7. 将授权分发到Dr.Web邻居服务器。
8. 编辑分发到Dr.Web邻居服务器的授权。

查看授权相关信息

查看授权信息时需在授权管理器主窗口选择要查看的密钥账户（点击密钥账户名称）。在打开的窗口会显示：

- 从此授权密钥文件可提供的和使用中的授权数量。
- 授权用户。
- 授权销售商。
- 授权识别码和序列号。
- 授权到期日期。
- 此授权是否支持反垃圾邮件模块。
- 授权密钥的MD5哈希值
- 允许的哈希公报列表，用于报告侦测到的威胁的所属。如没有此功能授权，则没有这一参数。

> 不具备哈希公报授权不影响反病毒保护的等级。具备此授权时可以通知管理员侦测到的威胁一包含于威胁已知哈希公报。

- 此授权允许使用的反病毒组件。

添加新的授权密钥

添加新的授权密钥

1. 在授权管理器主窗口的工具面板点击**添加授权密钥**按钮。
2. 在打开的面板点击后选择含有授权密钥的文件。
3. 勾选此项：
   - 为**Everyone**组指定授权密钥，如果这是反病毒网络中的第一个密钥。添加的密钥会自动指定给**Everyone**组。

- **替换Everyone组授权密钥**，如果这不是反病毒网络中的第一个密钥。**Everyone**组的当前密钥将被替换为添加的授权密钥。

> 如**Everyone**组指定有多个密钥，则替换列表中的第一个。
>
> 如需替换**Everyone**组中特定的某一密钥，请利用更新授权密钥来进行替换。

4. 点击**保存**按钮。
5. 授权密钥将添加到密钥树结构。

   如果在第3步没有勾选替换Everyone组授权密钥，则添加的授权密钥不会和任何对象捆绑。这时指定授权对象需执行下面介绍的替换授权密钥或扩展授权密钥列表。

更新授权密钥

更新授权密钥时新的授权密钥会指定给被更新密钥相对应的对象。

可使用更新操作来替换到期的密钥或允许组件列表有所区别的密钥，这时密钥树结构不会发生改变。

更新授权密钥

1. 在授权管理器主窗口密钥树结构选择需更新的密钥。
2. 在打开的密钥属性面板点击后选择含授权密钥的文件。
3. 点击**保存**按钮。打开可安装组件设置窗口，参见更换授权密钥时的设置操作部分的介绍。
4. 点击**保存**按钮后更新授权密钥。

更换授权密钥

更换授权密钥时删除授权对象的所有当前授权密钥后添加新密钥。

将当前密钥更换为新密钥

1. 在授权管理器主窗口密钥树结构选择需指定给授权对象的密钥：组、工作站和策略。
2. 在工具面板点击**将密钥分发到组和工作站**。打开反病毒网络分层列表。
3. 在列表中选择授权对象。多选使用CTRL和SHIFT。

> 为策略制定密钥需选择此策略或此策略的当前版本（选择策略当前版本时密钥会自动指定给策略，反之亦然）。
>
> 也可将密钥指定给非策略当前版本的任一版本。这时密钥将指定给这一版本，而不会指定给策略。在为其指定了密钥的版本替代当前版本之前，指定的密钥不会应用于工作站。
>
> 需将授权密钥直接指定给策略或其版本。

4. 点击**更换授权密钥**按钮。打开可安装组件设置窗口，参见更换授权密钥时的设置操作部分的介绍。

5. 点击**保存**按钮后更换授权密钥。

扩展授权密钥列表

添加授权密钥时保留授权对象的所有当前授权密钥，并添加新密钥。

向现有授权密钥列表添加新的授权密钥

1. 在授权管理器主窗口密钥树结构选择需添加到对象授权列表的密钥：组、工作站或策略。
2. 在工具面板点击**将密钥分发到组和工作站**。打开反病毒网络分层列表。
3. 在列表中选择授权对象。多选使用CTRL和SHIFT。

> 为策略制定密钥需选择此策略或此策略的当前版本（选择策略当前版本时密钥会自动指定给策略，反之亦然）。
>
> 也可将密钥指定给非策略当前版本的任一版本。这时密钥将指定给这一版本，而不会指定给策略。在为其指定了密钥的版本替代当前版本之前，指定的密钥不会应用于工作站。
>
> 需将授权密钥直接指定给策略或其版本。

4. 点击**添加授权密钥**按钮。打开可安装组件设置窗口，参见更换授权密钥时的设置操作部分的介绍。
5. 点击**保存**按钮后添加授权密钥。

删除授权密钥、删除授权列表中的对象

> 不可删除**Everyone**组密钥的最后一个账户。
>
> 为授权密钥无自身设置的工作站指定的策略本身应指定有授权密钥。

删除授权密钥或授权对象

1. 在授权管理器主窗口选择要删除的授权密钥，或者此密钥对应的对象（工作站、组或策略），然后在工具面板点击**删除所选对象**按钮。这时：
   - 如果选择的是组或工作站，则这一对象从密钥对应对象列表中删除。删除个人授权密钥的组和工作站设为继承授权密钥。
   - 如果选择的是策略，则从授权密钥对应对象列表中删除此策略的当前版本。如选择的是策略当前版本，则删除策略本身。但在删除非当前版本的策略版本时不会删除策略本身及其当前版本。
   - 如果选择的是授权密钥，则这一密钥账户从反病毒网络中删除。此密钥对应的组和工作站设为继承授权密钥。
2. 打开可安装组件设置窗口，参见更换授权密钥时的设置操作。
3. 点击**保存**按钮后删除所选密钥。

将授权分发到Dr.Web邻居服务器。

将此Dr.Web服务器未使用的部分授权分发给Dr.Web邻居服务器时，在分发有效期内此Dr.Web服务器将无法使用已分发的授权。

将授权分发到Dr.Web邻居服务器的操作

1. 在授权管理器主窗口密钥树结构选择需分发到Dr.Web邻居服务器的未使用的授权。
2. 在工具面板点击**将密钥分发到Dr.Web邻居服务器**。打开Dr.Web邻居服务器分层列表。
3. 在Dr.Web服务器列表选择相应的服务器。
4. 在每一Dr.Web服务器前给出以下参数：
   - **授权数量**——需要从本密钥分发给Dr.Web邻居服务器的可用授权数量。
   - **授权结束日期**——分发出去的授权的有效期。到期后所有授权将从Dr.Web邻居服务器撤回，重新归入本授权密钥可用授权列表。
5. 点击其中一个按钮：
   - **添加授权密钥**——用于将授权添加到Dr.Web邻居服务器现有授权列表。打开可安装组件设置窗口，参见添加授权密钥时的设置操作部分的介绍。
   - **更换授权密钥**——用于删除Dr.Web邻居服务器现有授权，只指定当前分发的授权。打开可安装组件设置窗口，参见更换授权密钥时的设置操作部分的介绍。

编辑分发到Dr.Web邻居服务器的授权。

编辑分发到Dr.Web邻居服务器的授权的操作

1. 在授权管理器主窗口密钥树结构选择相应的Dr.Web邻居服务器。
2. 在打开的属性面板编辑以下参数：
   - **授权数量**——从此Dr.Web服务器分发给Dr.Web居服务器的可用授权数量。
   - **授权结束日期**——分发出去的授权的有效期。到期后所有授权将从Dr.Web邻居服务器撤回，重新归入相应授权密钥可用授权列表。
3. 点击**保存**按钮后更新可分发授权信息。

更改可安装组件列表

更换授权密钥时的设置操作

本节介绍的是完成以下任务时如何设置可安装组件：

- 更新授权密钥；
- 更换授权密钥；
- 删除授权密钥；
- 将授权分发到Dr.Web邻居服务器时更换密钥。

执行上述任务时设置可安装组件

1. 可安装组件设置窗口的对象列表中列有：
   - 工作站、组和策略及其可安装组件列表。
   - 在**当前密钥**一列是对象的密钥列表以及当前的可安装组件的设置。
   - 在**要指定的密钥**一列是需要为对象指定的密钥以及此密钥中包含的可安装组件的设置。
   - 如需可勾选**只显示区别**，以便只显示其当前所在和要指定的密钥的设置有区别的组件。
2. 设置安装组件列表的操作：
   a) 在**要指定的密钥**可设置可安装组件的最终列表。
      - 在**要指定的密钥**一列可安装组件按照当前设置及新密钥允许使用（+）或不允许使用（–）来确定是否可以使用的规则是：

当前设置	要指定的密钥的设置	最终设置
+	+	+
–	+	+
+	–	–
–	–	–

      - 只有当**要指定的密钥**一列设置中为允许使用此组件时，才可以更改组件设置（降低安装权限）。
   b) 勾选需要中断继承的对象（工作站、组和策略），这些对象将接受**要指定的密钥**一列的可安装组件设置作为其个人自身设置。其他对象（不进行勾选的对象）将继承**要指定的密钥**一列的最初设置。

将授权密钥时添加到密钥列表时的设置

本节介绍的是完成以下任务时如何设置可安装组件：

- 扩展授权密钥列表。
- 将授权分发到Dr.Web邻居服务器时添加密钥。

执行上述任务时设置可安装组件

1. 可安装组件设置窗口的对象列表中列有：
   - 工作站、组和策略及其可安装组件列表。
   - 在**当前密钥**一列是对象的密钥列表以及当前的可安装组件的设置。
   - 在**要指定的密钥**一列是需要为对象添加的密钥以及此密钥中包含的可安装组件的设置。
2. 如需可勾选**只显示区别**，以便只显示其当前所在和要指定的密钥的设置有区别的组件。请注意，在**要指定的密钥**一列给出的不是这一密钥本身的组件设置，而是添加后的最终设置。
3. 设置安装组件列表的操作：
   a) 在**要指定的密钥**可设置可安装组件的最终列表。

- 在**要指定的密钥**一列可安装组件按照当前设置及新密钥允许使用（+）或不允许使用（–）来确定是否可以使用的规则是：

当前设置	要指定的密钥的设置	最终设置
+	+	+
–	+	–
+	–	–
–	–	–

- 只有当**要指定的密钥**一列设置中为允许使用此组件时，才可以更改组件设置（降低安装权限）。

b) 勾选需要中断继承的对象（工作站、组和策略），这些对象将接受**要指定的密钥**一列的可安装组件设置作为其个人自身设置。其他对象（不进行勾选的对象）将继承**要指定的密钥**一列的最初设置。

10.1.2. 授权使用报告

授权使用报告包含此Dr.Web服务器和Dr.Web邻居服务器当前使用的所有授权相关信息，包括利用服务器间连接传递的授权。



报告按照**Dr.Web服务器配置** → **授权**部分**授权使用情况报告的设置**给出的设置创建（由Dr.Web邻居服务器发送）。

查看报告需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**授权使用报告**。

这一部分显示以下信息：

- 关于此Dr.Web服务器可以支配的所有授权的报告。Dr.Web服务器未与Dr.Web邻居服务器建立任何连接时也会显示此报告。
- 关于此Dr.Web服务器下属Dr.Web邻居服务器可以支配的授权的报告，包括从此服务器利用服务器间连接获取的授权。显示服务器间连接树结构依次向下所有Dr.Web邻居服务器发送的报告。

每一报告均为一个表格，只显示一个Dr.Web服务器（生成报告的服务器）的授权使用情况。

表头显示以下信息：

- **Dr.Web服务器**——Dr.Web服务器（生成报告的服务器）的名称。
- **从邻居获取的授权共计**——此Dr.Web服务器通过服务器间连接获取的授权总数。

表中数据为：

- **用户**——表行所列授权密钥的用户。
- **授权共计**——此Dr.Web服务器此授权密钥所提供的授权总数。
- **可用**——此密钥中尚未使用的授权数量。

- **使用中共计**——生成报告时已使用的授权的总数（包括分发给工作站和Dr.Web邻居服务器的授权）。
- **供工作站使用**——连接Dr.Web服务器（生成报告的服务器）的工作站使用的授权。
- **正在等候**——生成报告的服务器等候获取的授权的数量。包括Dr.Web服务器已使用一定数量授权（或者是指定给了自己的工作站，或者是利用服务器间连接传递给其他服务器）而失去了部分授权。例如，授权密钥被替换为另一授权数量减少的密钥，或者从Dr.Web父服务器获取的授权数量减少。
- **预备**——已利用服务器间连接给出的授权数量，但应接收授权的尚未获取这些授权：Dr.Web邻居服务器尚未连接，因此尚未获取授权。这些授权已在密钥中作了预备，不可指定给其他工作站或Dr.Web服务器。
- **已按服务器间连接给出**——生成报告的Dr.Web服务器利用服务器间连接发给自己的Dr.Web邻居服务器的授权数量。
- **已按服务器间连接接收**——生成报告的Dr.Web服务器利用服务器间连接从自己的Dr.Web邻居服务器接收的授权数量。
- **报告日期**——生成报告的日期。

对于生成报告的Dr.Web服务器自身工作站使用的授权可查看补充信息。操作是点击**供工作站使用**一列的授权数量（不应为零止）。打开的**组使用的授权**一列显示以下信息：

- **组名称**——接收授权的工作站组的名称。
- **已分发授权**——已分发给工作站组的授权总数。
- **活跃的工作站**——组中活跃的工作站的数量。活跃的工作站是密钥所归属的Dr.Web服务器上报告生成设置中所指定的期限内连接过服务器的工作站。

10.2. 记录日志

10.2.1. 实时日志

实时日志可在事件出现时实时查看与Dr.Web服务器运行相关的事件和更改。



实时日志只在管理中心显示，不记录到文件。Dr.Web服务器日志文件按照其设置进行记录，与实时日志和实时日志的设置无关。

打开另一页面时实时日志所有信息都将删除。

日志表含有以下数据：

- **No.**——记录编号。按照来自Dr.Web服务器的通知的顺序继续编号。
- **日志格式时间**——事件出现时间，采用Dr.Web服务器日志的时间格式。可以按照这一事件在Dr.Web服务器日志查找事件。
- **时间**——事件出现时间，采用用户方便的格式。
- **等级**——所发生事件符合的日志记录等级。
- **PID**——发生事件的进程的识别码。
- **TID**——发生事件的线程的识别码。

- **线程**——发生事件的线程的名称。
- **子系统**——发生事件的子系统的名称。
- **通知**——事件通知内容。点击列表中的通知即可打开全部内容。如通知文本采用HTML码，正常显示需勾选**HTML文本格式化**。注意，如果通知包含JavaScript，会执行脚本。

更改列表中的数据显示

- 使用图标：
  - 设置行的显示（适用于长字符行）。
  - 选择要在报表中显示的列。
- 使用图标：
  - 指定搜索内容，在整个报表进行搜索。表中将只显示与搜索行相符的搜索结果。
  - 勾选相应等级后则只显示具体等级。
  - 勾选相应子系统后则只显示具体子系统。

  如需要日志只记录具体子系统的具体等级的通知，需设置日志记录。

工具面板包括以下管理日志的元素：

设置数据的显示——打开设置日志记录窗口。

清空报表——删除表中显示的所有数据，此操作不可逆。

停止数据收集——停止将事件信息记录到报表。正在记录数据的情况下可使用此按钮。点击后按钮改变为**启动数据收集**。

启动数据收集——开始将事件信息记录到报表。停止记录数据的情况下可使用此按钮。点击后按钮改变为**停止数据收集**。

设置实时日志记录

1. 在控制面板点击**设置数据的显示**。打开**设置数据的显示**窗口。
2. 在**记录最多数量**一栏限制日志报表记录数量。达到此限制后记录新数据时会删除最老的记录。
3. 在**更新频率，秒**一栏指定日志写入新纪录的时间间隔，以秒计。
4. 利用**按照子系统搜索**一栏可按照下列子系统名称进行搜索。子系统数量较多时可用于设置具体子系统的日志记录详细等级。
5. 子系统列表用于设置要显示的数据和其详细等级。
   a) 勾选需在表中显示其通知的子系统。
   b) 为所选子系统选择日志记录的详细等级。
   c) 勾选所有子系统的操作是勾选列表表头。
   d) 为所有子系统指定相同的日志记录详细等级的操作是在下列列表选择勾选子系统旁的**all**。表中将只显示所选子系统的通知。
6. 点击**应用**按钮后按照新设置显示数据。
7. 点击**关闭**则关闭窗口，不更改日志显示。

10.2.2. 审计日志

审计日志用于查看Dr.Web Enterprise Security Suite管理子系统实施的事件和更改。

查看审计日志

1. 在管理中心主菜单选择**管理**。
2. 在打开的窗口选择控制菜单中的**审计日志**。
3. 打开注册事件表窗口。可在工具明白指定要查看的操作执行日期。可在下拉列表选择时段或点击日期输入栏打开日历选择任一时段。点击**更新**后会显示所选日期的日志。
4. 进行报表格式设置需点击表头右角的图标。可在下拉列表设置以下选项：
   - 启用或停用长句子的换行。
   - 选择将在表中显示的列（名称旁有旗标）。点击列名称行可设置显示 / 不显示此列。
   - 选择表中各列排列次序。更改的方式是将相应列拖至相应位置。
5. 日志表含有以下数据：
   - **时间**——执行操作的日期和时间。
   - **结果**——操作执行结果简短记录：
     - **OK**——操作成功执行。
     - **失败**——执行操作时出现错误。操作未能执行。
     - **开始**——操作已开始。其结果只有在操作结束后才能得知。
     - **无权限**——启动操作的管理员没有执行此操作的权限。
     - **推迟**——操作推迟到某时间或某事件发生时执行。
     - **无法执行**——此操作为禁止执行的操作。例如，删除系统组。

     出现错误而结束的操作（**状态**一列为**失败**）所在行标为红色。

   - **通知 / 错误**——对操作和出现的错误的详细描述。
   - **注册用户名**——Dr.Web服务器管理员的注册用户名。如操作直接由管理员执行或是在以此管理员账户连接Dr.Web服务器执行时记录注册用户名。
   - **地址**——执行此操作的IP地址。只在从外部连接Dr.Web服务器时记录，包括通过管理中心或Web API进行的连接。
   - **子系统**——由其发起或通过其发起操作的子系统的名称。审计记录适用于下列子系统：
     - **管理中心**——操作是由管理员通过Dr.Web安全管理中心进行的。
     - **Web API**——操作是通过Web API执行的，如从按照管理员账户连接的外部应用（参见：**附录**中的附录L. Web API和Dr.Web Enterprise Security Suite的整合）。
     - **服务器**——操作是由Dr.Web服务器执行的，如按照服务器日程。
     - **工具**——操作是通过外部工具发起的，如通过Dr.Web服务器远程诊断工具。
6. 如需可将所选时段的数据导出到文件。操作是在工具面板点击下面的一个按钮：

   将数据保存到**CSV**文件，

   将数据保存到**HTML**文件，

将数据保存到**XML**文件，

将数据保存到**PDF**文件。

10.2.3. Dr.Web服务器日志

Dr.Web服务器记录其运行日志。

Dr.Web服务器日志用于调试以及在反病毒网络组件运行出现异常时解除故障。

默认日志文件名称为drwcsd.log，位置在：

- OS **UNIX**：
  - OS Linux：/var/opt/drwcs/log/drwcsd.log；
  - OS FreeBSD：/var/drwcs/log/drwcsd.log。
- OS **Windows**：在Dr.Web服务器安装目录var子目录。

文件为普通文本格式（参见**附录**中的附录K. 日志文件格式）。

利用管理中心查看Dr.Web服务器运行日志

1. 在管理中心主菜单选择**管理**。
2. 在打开的窗口选择控制菜单中的**Dr.Web服务器日志**。
3. 打开Dr.Web服务器运行日志列表窗口。根据轮循模式设置使用的Dr.Web服务器日志文件名称格式为：*<file_name>*.*<N>*.log或*<file_name>*.*<N>*.log.gz，其中*<N>*——排序编号：1、2等等。如：文件名称为drwcsd时运行日志文件列表为：
   - drwcsd.log——当前文件（进行写入的文件）；
   - drwcsd.1.log.gz——上一文件；
   - drwcsd.2.log.gz等等——数字越大，日志文件越陈旧。
4. 管理日志文件需勾选一个或几个文件。勾选表头可全选。在工具面板有以下操作按钮：

   导出所选日志文件——保存所选日志文件本地备份。如需从远程计算机查看日志文件内容可采用保存备份的方式。

   删除所选日志文件——删除所选日志文件，删除后不可恢复。

利用管理中心的日志部分可更改Dr.Web服务器日志记录模式。

管理日志详细等级

取决于指定的设置，Dr.Web服务器日志记录的信息详细等级不同。在进行调试或需要解决运行出现的问题时可以提高某些信息源或所有信息源的通知的详细程度，在联系Dr.Web技术支持时也会有可能需要提供详细日志。设置此参数有几种方式：

- 利用管理中心的**管理** → **Dr.Web服务器配置** → **日志**。这种方式可以指定所有信息源的通知的详细程度。
- 启动Dr.Web服务器时在命令行利用`-verbosity`来进行设置。这种方式更为灵活，如需可以指定个别一个或几个信息源的通知的详细程度。此参数的格式见**附录**的H3.8. 参数介绍。
- 利用单独的配置文件`logging.conf`。需在Dr.Web服务器安装目录的子目录`etc`创建此名称的配置文件，之后在文件中指定通知源和详细等级，格式为*<通知源>*:*<等级>*。通过`logging.conf`设置的详细等级优先于通过其他方式设置的详细等级。

`logging.conf`文件内容示例：

```
Alert:all, Server:err, SqLite3:inf
```

除逗号外，任意其他空格字符都可以作为隔离符，包括普通的空格、制表符、回车等等。可直接在Dr.Web服务器日志文件查看通知源列表，或者通过管理中心，在**管理** → **Lua控制台**执行指令`drwcs.log_subsystems()`。可以使用的详细等级见**附录**的附录K. 日志文件格式。

> 以这种方式指定的详细登记会由子系统继承。也就是说，比如文件中同时指定参数`Socket/Client:inf`和`Socket:all`，子系统`Socket/Client`，遵循父级的设置，会在日志记录所有相关事件信息，而不只是信息性的通知。

- 对于UNIX家族操作系统的Dr.Web服务器需在配置文件`local.conf`利用专门从事来指导。如何使用此文件的介绍见下。

设置UNIX运行日志

UNIX家族操作系统的Dr.Web服务器设有通过单独的配置文件设置Dr.Web服务器运行日志记录的功能：

- OS Linux：`/var/opt/drwcs/etc/local.conf`；
- OS FreeBSD：`/var/drwcs/etc/local.conf`。

`local.conf`文件内容：

```
# Log level.

DRWCS_LEV=info

# Log rotation.

DRWCS_ROT=10z,10m
```

参数值对应启动Dr.Web服务器命令行参数值：

- `-verbosity=`*<详细等级>*——记录Dr.Web服务器运行日志的详细等级。
- `-rotate=`*<N><f>*, *<M><u>*——Dr.Web服务器运行日志轮循模式。

参数详细描述参见**附录**中的H3.8. 参数介绍。

如在Dr.Web服务器运行过程中对文件local.conf进行了编辑，应用更改需重启Dr.Web服务器。应使用操作系统工具来进行重启。

更新或删除Dr.Web服务器时会对文件local.conf进行备份，以便在进行Dr.Web服务器软件包更新时管理日志记录等级。

10.2.4. 库更新日志

库更新日志为从全球更新系统加载的更新列表，包含更新的产品校订详细信息。

查看库更新日志

1. 在管理中心主菜单选择**管理**。
2. 在打开的窗口选择控制菜单中的**库更新日志**。
3. 打开注册事件表窗口。可在工具明白指定要查看的操作执行日期。可在下拉列表选择时段或点击日期输入栏打开日历选择任一时段。点击**更新**后会显示所选日期的日志。
4. 如需在表中显示某类型事件，请点击工具面板上的图标。在下拉列表选择筛选参数：
   - **产品名称**——日志报告中将显示与表中所选产品相关的所有事件。
   - **更新结果**——日志报告中将显示所有更新进程和更新机构。可依据更新结果来筛选进程：
     - **未能在GUS服务器找到这一产品**；
     - **未能在GUS服务器找到授权密钥**；
     - **更新已停用**；
     - **已成功完成更新**。
   - **发起者**——日志报告中将显示由下列系统发起的更新进程：
     - **从命令行启动**——更新由管理员使用相应的控制台指令发起。
     - **由任务计划器启动**——更新是按照Dr.Web服务器日程任务启动的。
     - **服务器间更新**——更新是从Dr.Web主服务器按照服务器间连接获得。只有在多服务器反病毒网络按照服务器间连接传播更新是才存在此类更新发起对象。
     - **从管理中心启动**——更新是管理员从Dr.Web安全管理中心的库状态部分启动的。
     - **导入库**——更新是管理员从Dr.Web安全管理中心的库内容部分加载的。
5. 日志表含有以下数据：
   - **管理员**——Dr.Web服务器管理员的注册用户名。如操作直接由管理员执行时显示。
   - **网络地址**——执行此操作的IP地址。只在从外部连接Dr.Web服务器时记录，包括通过管理中心或Web API进行的连接。
   - **发起者**——发起更新进程的系统。
   - **库目录**——更新过程中发生变化的Dr.Web服务器库目录名称。
   - **产品名称**——已加载或要求加载的库产品名称。
   - **开始**——从全球更新系统开始加载具体产品更新的日期和时间。
   - **结束**——从全球更新系统结束加载具体产品更新的日期和时间。
   - **更新结果**——库更新结果。成功完成更新简短信息或更新出错原因。

出现错误而结束的操作**更新结果**一栏标为红色。

- **初始校订**——更新进程开始前本产品最后一次校订编号（校订按照其日期编号）。
- **获取的校订**——更新进程中加载的本产品的校订的编号（校订按照其日期编号）。
- **已更新文件**——发生改变的文件汇总。格式为：*<文件数量>* – *<对文件进行的操作>*。

6. 如需可将所选时段的数据导出到文件。操作是在工具面板点击下面的一个按钮：

 将数据保存到**CSV**文件，

 将数据保存到**HTML**文件，

 将数据保存到**XML**文件，

 将数据保存到**PDF**文件。

10.2.5. 通知日志

在通知日志显示管理员发送到反病毒网络工作站的所有文本通知（见向工作站发送通知）。

已发送通知日志包含以下信息：

- **发送日期**。
- **发件人**——发送通知时登录管理中心的管理员的注册名。
- **状态**——管理员发送的通知数量和成功发送至工作站的通知数量。如发出和送达通知数量相符，则信息为灰色。
- **通知**——已发送的通知的内容。分项显示发送时指定的其他设置的相关信息。

点击表中具体通知后打开送达详细信息：所有收件人列表和成功送达日期，如未成功送达，显示**未能送达**。

管理通知日志可使用工具面板的下列选项：

**再次发送所选通知**——在日志中选出一个或几个通知后此选项可用（见下）。

**将所选通知保存为模板**——将已发送的帖子设为模板。在日志中选出一个或几个通知后此选项可用。管理已保存的模板使用的是通知模板。

在下拉列表选择需显示的通知的发送时间段。可通过下拉日历选择日期。应用这一时段需点击**更新**。

重新发送一个通知

1. 勾选一个需要发送的通知。
2. 点击**再次发送所选通知**。
3. 打开**发送通知**窗口。给出以下设置：
   a) 在**反病毒网络**树结构已选择出之前接收通知的工作站或工作站组。可保留之前的接收对象或在给出的列表中选择新的接收对象：可以是工作站，也可以是工作站组。
   b) 通知设置同 向工作站发送通知的设置。

4. 点击**发送**按钮。

重新发送多个通知

1. 勾选多个通知：
2. 点击**再次发送所选通知**。
3. 打开**发送多个通知**窗口。在**通知列表**出现所选的需再次发送的通知。通知名称与上次发送到工作站的日期相符。
4. 点击**全部发送**，发送列表中所有通知。
5. 如需编辑某通知，需在**通知列表**选择后在**通知设置**指定以下参数：
   a) 在**反病毒网络**树结构已选择出之前接收通知的工作站或工作站组。可保留之前的接收对象或在给出的列表中选择新的接收对象：可以是工作站，也可以是工作站组。
   b) 通知设置同 向工作站发送通知的设置。
   c) 取消发送某通知需点击**删除**按钮。

10.3. 设置Dr.Web服务器配置



每一次保存**Dr.Web服务器配置**部分的更改时会自动备份上一版本的Dr.Web服务器配置文件。共保存10个不同版本的备份。

备份与配置文件在同一目录，目录名称格式为：

`drwcsd.conf_<创建时间>`

可使用备份在无法访问管理中心界面时恢复配置文件。

设置Dr.Web服务器配置参数

1. 在管理中心主菜单选择**管理**。
2. 在打开窗口的控制菜单选择**Dr.Web服务器配置**。打开Dr.Web服务器设置窗口。



有*标志的输入栏必须填写。

3. 在工具面板可使用以下选项：

   **重启Dr.Web服务器**——重新启动Dr.Web服务器，以便应用对本部分的修改。修改设置并点击**保存**按钮后出现此选项。

   **从备份恢复配置**——下拉列表包含保存的设置备份，可利用备份取消当前的修改。修改设置并点击**保存**按钮后出现此选项。

   **将所有参数设为初始值**——还原这一部分所有参数此次编辑前的参数值（上次保存的参数值）。

   **将所有参数设定为默认值**——将这一部分所有参数设为默认值。
4. 应用对设置的效果需点击**保存**按钮，之后要求重启Dr.Web服务器。需点击工具面板的**重启Dr.Web服务器**按钮。

10.3.1. 常规

在**常规**标签指定运行Dr.Web服务器的以下设置：

- **服务器名称**——此Dr.Web服务器的名称。如未指定，使用安装Dr.Web服务器的计算机的名称。
- **Dr.Web服务器语言**——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。

> 如果您所选择的语言目前没有界面更新，会提示您启用此语言的更新。操作是打开**管理** → **库常规配置** → **Dr.Web服务器** → **Dr.Web安全管理中心语言**。勾选需要的语言后点击**保存**。库进行更新时就会为所选语言更新界面。还可在**库状态**手动启动更新。

- **平行申请数量**——用于处理客户端发出的数据的线程数量，包括代理端、代理端安装程序、Dr.Web邻居服务器。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。

> 从版本10开始，不可从管理中心修改参数**登录等候列队**。
>
> 默认情况下安装新Dr.Web服务器时此参数为50。从老版本升级保存原配置文件时，从原配置文件提取参数值。
>
> 如需更改登录等候列队参数，需更改Dr.Web服务器配置文件以下参数值：
>
> ```
> <!-- Maximum authorization queue length -->
> <maximum-authorization-queue size='50'/>
> ```

- 在**新工作站注册模式**下拉列表指定新工作站连接策略（参见工作站连接策略）。
  - **默认基组**下拉列表确定自动确认工作站登录Dr.Web服务器时工作站的基组。
- 勾选**将未登录的工作站列为新工作站**后清空未能登录的工作站访问Dr.Web服务器的参数。在更改Dr.Web服务器设置（如加密公钥）或更换数据库时这一功能会很有帮助：在这些情况下工作站不能进行连接，需要重新获得访问Dr.Web服务器的新参数。
- 勾选**自动创建账户**后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。如取消勾选只可按照启动安装包的组中已创建的账户数量进行安装。
- 在**允许的Dr.Web服务器与代理端系统时间差**一栏指定Dr.Web服务器系统时间与Dr.Web代理端系统时间之间允许的差别，以分钟计。如超出此允许值，则在Dr.Web服务器的工作站状态作出标记。默认为3分钟。值为0表示不进行系统时间比照。
- 勾选**替换IP地址**后，在Dr.Web服务器日志文件将计算机IP地址更换为DNS名称。
- 在**工作站名称**下拉列表给出的是工作站在管理中心反病毒网络目录中工作站名称的显示格式。
- 利用**替换工作站名称**下拉列表可以指定将显示的工作站名称替换为DNS全名或确定的部分DNS名称（无法确定DNS名称时显示IP地址）。

> **替换IP地址**默认为不勾选。如DNS服务设置不当，启用这两项功能会大大减慢Dr.Web服务器的运行速度。启用两项中的任何一种功能时都建议允许在DNS服务器

缓存域名。

如**替换工作站名称**下拉列表中选择了一种替换方式，而在反病毒网络中使用代理服务器，则所有通过代理服务器连接Dr.Web服务器的所有工作站在管理中心的显示都将是安装有代理服务器的计算机的名称。

- 勾选**同步工作站描述**后将管理中心上的工作站描述与用户计算机描述同步（System properties页面的Computer description）。如在管理中心没有工作站的描述，此栏将记录用户端的计算机描述。如描述相异，则管理中心的描述将被用户端的描述代替。
- 勾选**同步地理位置**后会在多服务器反病毒网络的Dr.Web服务器间同步工作站地理位置。勾选后可指定以下参数：
  - **起始同步**——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。
- 勾选**使用策略**则允许使用策略设置受保护工作站参（参见策略）。
  - **策略版本数量**——可为每一策略建立的最多版本数量。
- 在**Dr.Web服务器版本备份数量**一栏指定通过管理中心转为Dr.Web服务器新校检时创建的备份可保存的最多数量（参见更新Dr.Web服务器和利用备份还原）。值为0表示保存所有校检备份。
- 勾选**允许使用代理端协议传输文件数据**后允许按SFTP协议从代理端向Dr.Web服务器发送文件数据。取消勾选后不传输数据。
- 在**Lua虚拟机数量**一栏指定预备Web服务器使用的Lua虚拟机的最多数量。
- 在**Lua虚拟机创建脚本**输入背景模式下创建Web服务器使用的Lua虚拟机时执行的脚本。

10.3.2. 流量

10.3.2.1. 更新

在**更新**标签限制Dr.Web服务器和代理端间传递更新时的网络流量。

详见更新流量限制。

限制代理端更新流量

1. 在**更新同时进程数量**一栏指定从本Dr.Web服务器同时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。设置为**0**时取消对同时进程数量的限制。
2. 勾选**限制更新流量**后会限制Dr.Web服务器和代理端间传递更新时的网络流量。

   如取消勾选，则不限制传递代理端更新占用的带宽。
3. 勾选后在**最大传递速度（KB/s）**一栏指定传递更新的最大限速。限定后更新会在指定带宽内传递所有代理端更新产生的总流量。

   可指定五种代理端更新数据传输速度限制。添加速度限制输入行需点击。删除限制需点击相应行旁边的删除按钮。
4. 日程表中更新限制模式时段划分为每星期每天的每30分钟。

更改数据传输速度限制模式需点击表格中相应区间。可按照drag-and-drop同时选择多个时段。

表格颜色按照表格下方颜色变化方式而周期变化，从流量无限制的方案开始至禁止传输数据结束。

5. 结束编辑后点击**保存**按钮保存更改。

10.3.2.2. 安装

在**安装**标签限制在工作站安装Dr.Web代理端过程中数据传输网络流量。

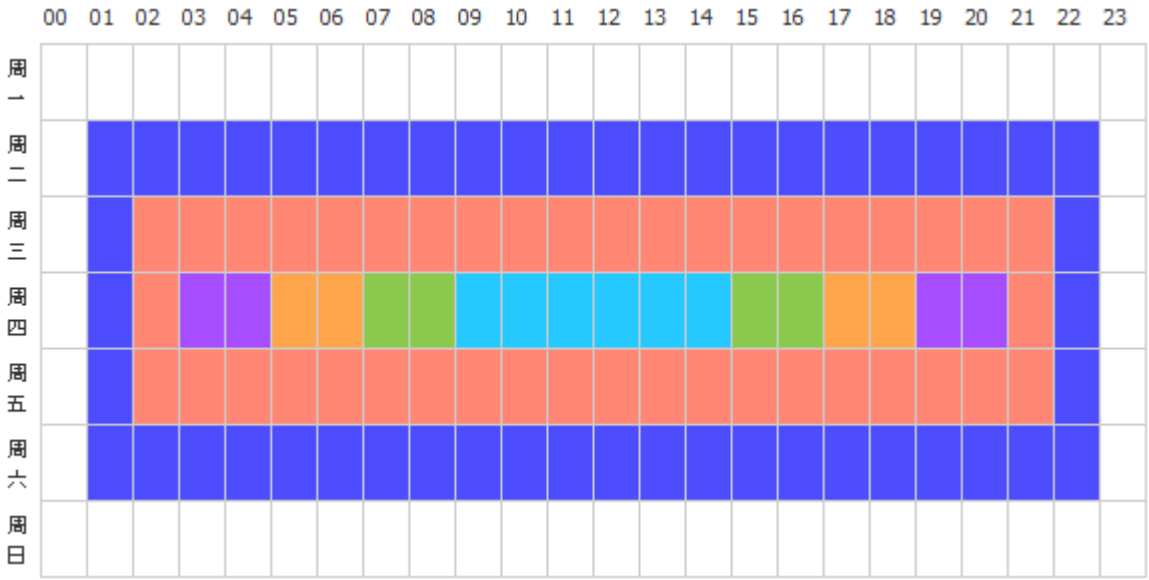
详见限制工作站流量。

限制代理端安装流量

1. 在**安装同时进程数量**一栏指定从本Dr.Web服务器同时启动的安装分发对话最大数量。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。设置为**0**时取消对同时进程数量的限制。
2. 勾选**限制代理端安装流量**后会限制在安装Dr.Web代理端时从Dr.Web服务器传递数据产生的网络流量。

   如取消勾选，则安装代理端时不限制传递数据占用的带宽。
3. 勾选后在**最大传递速度（KB/s）**一栏指定传递数据的最大限速。限定后更新会在指定带宽内传递所有安装代理端产生的总流量。

   可指定五种代理端安装数据传输速度限制。添加速度限制输入行需点击。删除限制需点击相应行旁边的删除按钮。
4. 日程表中数据传输速度限制模式时段划分为每星期每天的每30分钟。



更改数据传输速度限制模式需点击表格中相应区间。可按照drag-and-drop同时选择多个时段。

表格颜色按照表格下方颜色变化方式而周期变化，从流量无限制的方案开始至禁止传输数据结束。

5. 结束编辑后点击**保存**按钮保存更改。

10.3.2.3. 限制工作站流量

Dr.Web Enterprise Security Suite反病毒网络中可限制Dr.Web服务器与代理端将的数据传输。区分为更新传输限制和安装代理端时的数据传输限制。

有以下流量限制方案：

1. 限制向所有工作站传输数据的总速。

   在Dr.Web服务器配置部分进行设置：管理中心主菜单的**管理**→控制菜单的**Dr.Web服务器配置**→**流量**标签→**更新**或**安装**子标签→参数**限制更新流量**或**安装代理端时限制流量**。
2. 更新工作站或工作站组时限制向个别工作站或组传输数据的速度。

   在工作站配置部分进行设置：管理中心主菜单的**反病毒网络**→在分层列表选择组或工作站→控制菜单的**限制更新**→参数**限制更新流量**。

流量限制原则：

1. 如Dr.Web服务器设置中启用的是限制数据传输总速，则从Dr.Web服务器向所有工作站传输数据的总速不可超过指定数值。这时：
   a) 不论不同Dr.Web服务器与工作站间连接带宽有无区别，数据传输速度平摊到所有工作站。
   b) 如Dr.Web服务器和工作站间带宽低于a)中每一工作站平均带宽，则此工作站数据传输限定为其带宽。剩余的总带宽按照a)原则平摊到其他工作站。
2. 如果为工作站组或个别工作站启用了数据传输速度限制，则向这些工作站或组传输数据的速度不会超过限值。其他工作站则不受限制，以最高速度传输数据。
3. 如Dr.Web服务器设置中启用的是限制数据传输总速和对组或工作站进行了个别限制，则：
   a) 向受限组或工作站传输数据的速度不会超过这些组合工作站设置中指定的限值。
   b) 总限速减去a)中工作站限值后平摊到所有其他工作站。
   c) 如Dr.Web服务器和未受个别限制的工作站间带宽低于b)中每一工作站平均带宽，则这样的工作站数据传输限定为其带宽。剩余的总带宽按照b)原则平摊到其他未受个别限制的工作站。

10.3.3. 网络

10.3.3.1. DNS

在**DNS**标签指定访问DNS服务器的参数：

- **DNS请求超时时限（秒）**——允许正向/反向DNS请求的超时时限（以秒计）。为0时不限定等待允许DNS请求的时间。
- **重复DNS请求的次数**——未能成功允许DNS请求时重复DNS请求的最多次数。
- 勾选**指定DNS服务器回应保存时间**后指定缓存DNS服务器回应的时长（TTL）。
  - **对应肯定回应（分钟）**——（TTL）缓存DNS服务器肯定回应的时长，以分钟计。
  - **对应否定回应（分钟）**——（TTL）缓存DNS服务器否定回应的时长，以分钟计。
- **DNS-over-HTTPS服务器地址**——兼容的DNS-over-HTTPS服务器地址。

DNS-over-HTTPS——执行HTTPS协议DNS解析的协议。此方式可阻止拦截和操纵DNS数据，从而提高用户的私密性和安全性。DNS-over-HTTPS协议运行原理是加密发给DNS服务器的申请和服务器做出的响应，会隐藏用户使用DoH联系的远程服务器名称。

正常运行必须在**Dr.Web GUS**标签可用证书下拉列表指定任意。

- **DNS服务器**——替代默认系统列表的DNS服务器列表。
- **DNS服域名**——替代默认系统列表的DNS域名列表。

10.3.3.2. 代理服务器

在**代理服务器**标签指定代理服务器参数。

勾选**使用代理服务器**，指定通过代理服务器连接Dr.Web服务器。勾选后可进行以下设置：

- **代理服务器**——代理服务器IP地址或DNS名称。如需可在地址行指定端口，格式为<*地址*>:<*端口*>。默认使用端口3128。
- 如登录代理服务器需按照指定方式进行身份验证，需勾选**使用身份验证**后给出以下参数：
  - 填写**代理服务器用户**和**代理服务器用户密码**。
  - 需选择一种身份验证方式：

选项		描述
任一方式		使用代理服务器支持的一种身份验证方式。如代理服务器支持多种方式，将使用最可靠的一种。
任一安全方式		使用代理服务器支持的一种安全身份验证方式。这种模式下不使用Basic身份验证。如代理服务器支持多种方式，将使用最可靠的一种。
以下方式：	Basic身份验证	使用Basic身份验证。不建议使用这一方式，因为传输账户时不加密。
	Digest身份验证	使用Digest身份验证。加密登录方式。
	支持IE的Digest验证	使用Digest验证。加密的身份验证方式。可支持浏览器Internet Explorer版本6和更早版本。
	NTLM身份验证	使用NTLM身份验证。加密登录方式。使用Microsoft公司的NTLM协议。
	通过winbind的NTLM验证	使用通过外部应用winbind进行的NTLM验证。加密的身份验证方式。
	GSS-Negotiate身份验证	使用GSS-Negotiate身份验证。加密登录方式。

10.3.3.3. 传输

在**传输**标签设置Dr.Web服务器连接客户端所使用的传输协议参数。

- 在**加密**下拉列表选择Dr.Web服务器和与其连接的代理端、Dr.Web邻居服务器、网络安装程序之间的流量加密策略。
- 在**压缩**下拉列表选择Dr.Web服务器和与其连接的代理端、Dr.Web邻居服务器、网络安装程序之间的流量加密策略。

  参数介绍详见流量加密和压缩。
  - 勾选**是**和**可能**后出现**压缩等级**下拉列表。压缩等级为1到9，1为最低，9为最高。

> 详细信息参见流量加密和压缩。

- 在**TLS对话方加密密钥**一栏指定TLS对话方加密密钥文件路径。用于已对话方（session tickets）为基础恢复TLS对话，对话方使用指定的密钥加密。

在**TCP/IP**部分是在按照TCP/IP协议与Dr.Web服务器的连接参数：

- **地址**和**端口**——对应与此协议捆绑的网络接口的IP地址和端口号。Dr.Web服务器监听有上述设置的接口，以便与安装在工作站上的代理端进行交互作用。
- 勾选**发现**后启用Dr.Web服务器发现服务。
- 勾选**Multicasting**后搜索Dr.Web服务器时使用*Multicast over UDP*模式。
- **Multicast组**——注册Dr.Web服务器的multicast组IP地址。用于在搜索在线Dr.Web服务器时与代理端和网络安装程序交互作用。如不指定，默认使用组`231.0.0.1`。
- **名称**——Dr.Web服务器名称。如不指定，则使用在**常规**标签所指定的名称（见上，如未指定任何名称，则使用计算机的名称）。如在此栏指定的名称有别于在**常规**标签所指定的名称，则使用为协议指定的名称。此名称用于代理端按照发现服务搜索Dr.Web服务器等操作。
- 仅在UNIX家族操作系统下：在**路径**一栏指定连接套接字路径，如连接代理端的套接字路径。

> 详细信息参见网络连接设置。

这些参数以网络格式输入，网络格式列于**附录**中的附录E. 网络地址特点。

10.3.3.4. 电子邮箱

在**电子邮箱**标签设置从管理中心发送邮件的参数，如发送管理员通知、群发工作站安装包或找回管理员密码：

- **发件人电子邮箱**——邮件发件人电子邮箱地址。
- **服务器地址**——用于发送邮件的SMTP服务器的地址。
- **端口**——用于连接SMTP服务器的端口。默认情况下如打开单独的TLS受保护连接则使用端口465，否则使用端口25。
- **用户**、**密码**——SMTP服务器用户的用户名和密码，如SMTP服务器要求身份验证。

- **连接SMTP服务器的超时时限**——与SMTP服务器连接的超时时限，以秒计。数值应为等于或大于1的整数。
- 在**保护连接**下拉列表选择交换数据时使用的加密类型：
  - **STARTTLS**——通过指令STARTTLS转为受保护的连接。默认连接使用的端口为25。
  - **SSL/TLS**——开通单独的受保护连接。默认连接使用的端口为465。
  - **无**——不使用加密。将使用未受保护的连接交换数据。
- 勾选**使用CRAM-MD5身份验证**后在邮件服务器使用*CRAM-MD5*身份验证。
- 勾选**使用DIGEST-MD5身份验证**后在邮件服务器使用*DIGEST-MD5*身份验证。
- 勾选**使用LOGIN身份验证**后在邮件服务器使用*LOGIN*身份验证。
- 勾选**使用AUTH-NTLM身份验证**后在邮件服务器使用*AUTH-NTLM*身份验证。
- 勾选**使用普通身份认证**后在邮件服务器使用*plain text*身份验证。
- 勾选**检查服务器证书**后会检查邮件服务器的TLS证书。在**Dr.Web服务器证书**一栏指定Dr.Web服务器TLS根证书路径。
- 勾选**调试模式**用于获得SMTP对话过程详细日志。
- 在**收件人E-mail地址**可指定电子邮箱地址，以便测试发送邮件。点击**发送测试性通知**后按照指定设置发送测试邮件（类同Dr.Web服务器通知）。

10.3.3.5. 群集

在**群集**标签设置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。

使用群集需给出以下参数：

- **Multicast组**——Dr.Web服务器交换信息使用的multicast组的IP地址。
- **端口**——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。
- **生命期**——在Dr.Web服务器群集内传输数据的数据报生命期。
- **接口**——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。



创建Dr.Web服务器群集应注意的事项见Dr.Web服务器群集。

10.3.3.6. 加载

在**加载**标签指定Dr.Web服务器参数，这些参数在生成反病毒网络工作站代理端安装文件时使用。代理端安装程序在连接Dr.Web服务器时会使用这些参数：

- **Dr.Web服务器地址**——Dr.Web服务器IP地址或DNS名称。

  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。
- **端口**——代理端安装程序连接Dr.Web服务器使用的端口。

  如果中未指定端口，则使用端口2193（设置于管理中心**管理**→**Dr.Web服务器配置**→网络→的传输）。

加载部分的设置保存在配置文件download.conf（参见**附录**中的G3.配置文件download.conf）。

10.3.3.7. 组更新

在**组更新**标签设置使用multicast协议向工作站发送组更新。

启用multicast协议向工作站发送更新，需勾选**启用组更新**。

组更新基本原则：

1. 如组更新为启用，则所有连接此Dr.Web服务器的工作站的更新分两步进行：
   a) 工作站监听指定的Dr.Web服务器所在Multicast组。出现组更新时工作站通过*multicast over UDP*加载更新。
   b) 传递组更新后Dr.Web服务器向工作站发出存在更新的标准通知。未能通过组更新加载的内容将使用TCP协议按照一般更新加载到工作站。
2. 如组更新为停用，则所有工作站的更新只以常规方式按照TCP协议进行。

设置组更新使用的参数：

- **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）。
- **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。
- **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。
- **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。
- **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。
- **"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。
- **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。

指定可使用组更新的multicast组列表，需在**multicast组**部分指定以下参数：

- **Multicast组**——工作站获得组更新使用的multicast组的IP地址。
- **端口**——发送更新multicast传输协议捆绑Dr.Web服务器网络接口的端口号。

> 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。

- **生命期**——在组更新过程中传输数据的数据报生命期。

- **接口**——发送更新multicast传输协议捆绑的Dr.Web服务器网络接口的IP 地址。

  每一行给出一个multicast组的设置，添加multicast组需点击。

指定多个multicast组时，请注意：

- 为不同Dr.Web服务器应指定分发组更新使用的不同的multicast组。
- 为分发组更新的不同Dr.Web服务器应指定不同的**接口**和**端口**。
- 使用多个multicast组时，组中工作站不应有重复。也就是说反病毒网络的每个工作站只能包含于一个multicast组。

在**访问控制列表**指定对获得组更新的工作站的网络地址的限制：

- 允许获取组更新的工作站将监听指定的multicast组，以一般流程获取更新（见 钩子1）。
- 禁止获取组更新工作站不监听指定的multicast组是否有更新，使用TCP加载所有更新（见 钩子2）。

列表设置同安全策略部分的列表设置。

10.3.4. 统计信息

在**统计信息**设定标签需要在日志文件和Dr.Web服务器数据库进行记录的统计信息，之后可在管理中心统计信息查看。

通过勾选以下各项可向数据库添加相应类型的信息：

- **隔离区状态**——允许监控工作站上的隔离区状态，并将信息记录到数据库。
- **设备和软件组成**——允许监控工作站的硬软件配置，并将信息记录到数据库。
- **工作站模块列表状态**——允许监控工作站上反病毒软件的模块列表，并将信息记录到数据库。
- **已安装组件列表**——允许监控工作站已安装的反病毒软件组件（扫描仪、监视器等等），并将信息记录到数据库。
- **工作站用户对话**允许监控工作站用户对话，将在安装有代理端的计算机登录系统用户的用户名记录到数据库。
- **组件开始/结束信息**——允许监控工作站上反病毒软件组件（扫描仪、监视器等等）的启动和结束运行，并将信息记录到数据库。
- **侦测到的安全威胁**——允许监控工作站威胁侦测，并将信息记录到数据库。

  如勾选**侦测到的安全威胁**，可设置威胁统计的高级参数。
  - 勾选**追踪病毒流行**后启用向管理员通知病毒流行的模式。如取消勾选，则以常规模式通知发现病毒感染。勾选此项后还可以指定以下追踪病毒流行的参数：
    - **禁止发送通知的时段**——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。
    - **计算已感染工作站数量的周期**——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。
    - **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（**网络病毒流行**通知）。
    - **最常见威胁的数量**——病毒流行报告必须记录的最常见的威胁的数量。

- 勾选**将预防性保护报告汇总**后会发生统一的预防性保护多事件报告。取消勾选，则收到的是预防性保护事件单独通知。勾选时刻指定以下汇总参数：
  - **禁止发送通知的时段**——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。
  - **计算事件数量的周期**——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。
  - **事件数量**——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（**预防性保护汇总报告**通知）。
  - **最活跃进程的数量**——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。
- 勾选向**Doctor Web公司发送统计信息**后允许将工作站安全威胁侦测统计信息发送给Doctor Web公司。勾选后出现以下输入栏：
  - **间隔时间**——发送统计信息的时间间隔，以分钟计；
  - **识别码**——MD5密钥（在Dr.Web服务器配置文件）。

只有发送统计信息**时间间隔**一项为必填项。

- **连接非正常结束**——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。

  指定以下连接非正常结束设置：
  - **禁止发送通知的时段**——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。
  - **计算已结束连接数量的周期**——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。
  - **个别连接结束通知的连接数量**——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（**连接非正常结束**通知）。
  - **多起连接结束通知的连接数量**——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（**记录到多起连接非正常结束**通知）。
  - **短连接时长**——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**）。
- **扫描错误**——允许监控工作站扫描出错，并将信息记录到数据库。
- **扫描统计信息**——允许监控工作站扫描结果，并将信息记录到数据库。
- **代理端安装**——允许监控工作站代理端安装信息，并将信息记录到数据库。
- **已阻止的设备**——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服务器数据库。
- **应用程序监控对进程活动情况的统计信息**——允许跟踪工作站应用程序监控阻止的进程的活动，并将信息记录到服务器数据库。
- **应用程序监控对进程阻止情况的统计信息**——允许跟踪工作站应用程序监控阻止的进程，并将信息记录到服务器数据库。
- **应用程序监控多起阻止**——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。

  指定以下事件设置：
  - **禁止发送通知的时段**——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。

- **计算被阻止进程数量的周期**——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。
- **阻止数量**——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（**记录到应用程序监控大量阻止进程**通知）。
- **最常用模式数量**——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。

- **工作站任务执行日志**——允许监控工作站任务执行结果，并将信息记录到数据库。
- **工作站状态**——允许监控工作站状态，并将信息记录到数据库。
  - **病毒库状态**——允许监控工作站病毒库状态（组成、更改），并将信息记录到数据库。勾选**工作站状态**后才可勾选此项。
- **位置信息**——允许获取工作站位置信息并将信息写入数据库。

查看统计信息

1. 在主菜单选择**反病毒网络**。
2. 在分层列表选择工作站或组。
3. 打开控制菜单的相应选项（参见下表）。



统计数据的详细描述见查看工作站统计信息一节。

下表为Dr.Web服务器设置中**统计信息**勾选项所对应的**反病毒网络**页面控制菜单选项。取消对某一**统计信息**勾选项的勾选后将隐藏相应的控制菜单选项。

表10-1. Dr.Web服务器设置与控制菜单选项对应表

Dr.Web服务器设置	**菜单选项**
隔离区状态	常规→隔离区 配置→Windows→Dr.Web代理端→允许远程管理隔离区
设备和软件组成	常规→设备和软件组成 常规→已发现的设备
工作站模块列表	报表→模块
已安装组件列表	常规→已安装组件
用户对话	常规→用户对话
组件启动/结束	报表→启动/结束
侦测到的安全威胁	统计信息→威胁 统计信息→威胁统计信息 统计信息→预防性保护事件

Dr.Web服务器设置	菜单选项
扫描错误	统计信息→错误
扫描统计信息	统计信息→扫描统计信息
代理端安装	统计信息→代理端安装
已阻止的设备	统计信息→已阻止的设备
应用程序监控按照进程活动性的统计信息	统计信息→应用程序监控事件 管理 → 应用程序监控 → 应用程序手册
应用程序监控按照被阻止进程的统计信息	
工作站任务执行日志	统计信息→任务
工作站状态	统计信息→状态 统计信息→病毒库
病毒库状态	统计信息→病毒库

10.3.5. 安全策略

在**安全策略**标签对代理端、网络安装程序和其它（邻居）Dr.Web服务器访问此Dr.Web服务器使用的网络地址进行限制。

以下两个勾选项用于管理Dr.Web服务器审计日志：

- **管理员操作审计**允许记录管理员从管理中心所进行操作的审计日志，并将日志保存到数据库。
- **服务器内部操作审计**允许记录Dr.Web服务器内部操作的审计日志，并将日志保存到数据库。
- **Web API操作审计**允许记录从XML API进行的操作的审计日志，并将日志保存到数据库。

> 在主菜单选择**管理**中的**审计日志**一项即可查看审计日志。

安全策略标签还有三个补充标签，在这些标签可对相应类型的连接进行选择：

- **代理端**——Dr.Web代理端连接本Dr.Web服务器使用的IP地址限制列表。
- **安装程序**——Dr.Web代理端安装程序连接本Dr.Web服务器使用的IP地址限制列表。
- **邻居**——Dr.Web邻居服务器连接本Dr.Web服务器使用的IP地址限制列表。
- **发现服务**——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。

限制访问（为代理端、安装程序、Dr.Web邻居服务器或发现服务指定）的操作：

1. 勾选**使用此访问权限列表**后可设置允许地址列表或禁止地址列表。取消则允许所有连接。

2. 允许从一定TCP地址的访问，此地址应添加到**TCP：允许**或**TCPv6：允许**名单。
3. 禁止一个TCP地址的访问，此地址应添加到**TCP：禁止**或**TCPv6：禁止**名单。
4. 所有名单中都不包含的地址可以是都允许或都禁止，这取决于是否勾选**禁止优先**：如勾选了此项，**禁止**列表具有比**允许**列表更高的优先级。所有名单中都不包含的地址或两个名单都包含的地址将为禁止。只允许包含于**允许**列表且不包含于**禁止**列表的地址。

编辑地址列表的操作：

1. 在相应输入栏输入网络地址，格式为：*<IP地址>*/[*<前缀>*]。
2. 添加新地址栏需点击相应项的按钮。
3. 删除地址栏需点击相应地址栏旁边的按钮。
4. 应用更改需点击**保存**按钮。

只有计算机安装有IPv6界面才可显示TCPv6地址输入列表。

前缀使用举例：

1. 前缀24代表网络掩码为：255.255.255.0
   包含254个地址。
   这些网络的主机地址为：195.136.12.*
2. 前缀8代表网络掩码为255.0.0.0
   包含的地址达16777214个（256*256*256-2）
   这些网络的主机地址为：125.*.*.*

10.3.6. 缓存

在**缓存**标签指定清空服务器缓存的参数：

- **缓存完全清空周期**——全部清空缓存的周期。
- **隔离区文件**——删除Dr.Web服务器端隔离区文件的周期。
- **库文件**——删除库文件的周期。
- **缓存文件**——清空缓存文件的周期。
- **安装包**——删除个人和组安装包的周期。

  点击按钮 **现在删除所有安装包**后会删除先前创建的位于var目录的installers-cache子目录的所有个人安装包和组安装包。需要注意的是：删除后再次下载这些安装包时会重新创建，这会占用一定的时间。

指定数值时请注意下拉列表中的计量单位。

10.3.7. 数据库

在**数据库**标签指定Dr.Web服务器运行所必需的DBMS。

> **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。

指定数据库运行参数

1. 在**连接数量**一栏给出的是Dr.Web服务器与数据库的最大连接数量。如需改变默认设置，建议在更改前征得技术支持部门的同意。
2. 勾选**结束维护后自动清理数据库**后在初始化、更新和导入后后自动执行推迟的数据库清理。取消勾选则不执行清理。这时建议在Dr.Web服务器日程设置**清空数据库**任务或利用数据库管理手动执行清理。

   执行自动清理是在Dr.Web服务器日志创建隐藏任务。此任务在结束维护进程的当夜执行，时间是Dr.Web服务器当地时间 01:17。执行此任务的前提是维护进程结束后一天内Dr.Web服务器日程中没有指定执行任务**清空数据库**。
3. 在**数据库**下拉列表中选择数据库类型：
   - **MySQL**——外设数据库，
   - **ODBC**——用于通过ODBC连接使用外设数据库，

     > 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。

   - **Oracle**——外设数据库，不支持FreeBSD，

     > 使用外设DBMS Oracle必须安装和此DBMS一起供应的最新的ODBC驱动程序，不可以使用由Microsoft提供的Oracle ODBC驱动程序。

   - **PostgreSQL**——外设数据库，
   - **SQLite3**——内设数据库（Dr.Web服务器组件）。
4. 指定运行数据库所需参数：
   - 如选择的是内设数据库，如需可在****一栏输入数据库文件的完整路径，设置缓存大小和数据记录模式。
   - 外设数据库参数见**附录**中的附录B. DBMS使用设置。DBMS驱动程序参数一节。
5. 应用设置需点击**保存**按钮。

> Dr.Web服务器软件包含支持的DBMS的内设客户，因此：

- 如计划使用与Dr.Web服务器一起供应的ODBC内设客户端，在安装（更新）Dr.Web服务器时在安装程序设置中需选择自定义安装，在下一窗口确认**数据库支持**部分允许安装相应的DBMS内设客户端。
- 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使用数据库。

Dr.Web服务器安装程序支持产品更改模式。启动Dr.Web服务器安装程序并选择**更改选项**可添加或删除个别组件，如数据库管理驱动程序。

默认设置为使用内设DBMS。选择这一模式会大大增加Dr.Web服务器的计算负荷。如反病毒网络规模较大建议使用外设DBMS。更换DBM的操作见**附录**中的更换Dr.Web Enterprise Security Suite DBMS类型。

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

可以对Dr.Web服务器使用的数据库进行清理，即：删除事件记录以及在一段时间内未访问Dr.Web服务器的工作站的相关信息。清理数据库需进入Dr.Web服务器日程，然后设置相应的任务。

10.3.7.1. 恢复数据库

内设数据库**SQLite3.**出现错误时可使用常规工具恢复受损数据库。

数据库受损后需按以下流程进行操作：

1. 数据库受损时不能启动和运行Dr.Web服务器：
   a) 在Dr.Web服务器运行过程中：如在与数据库进行常规交互作用时出错，Dr.Web服务器会自动停止。
   b) 在Dr.Web服务器启动过程中：如数据库**SQLite3**设置中的**检查镜像完整性**下拉列表选择了**快速检查**或**完全检查**，则会自动检测数据库镜像的完整性。如发现错误则不会启动Dr.Web服务器。
2. 启动Dr.Web服务器必须先恢复受损数据库：
   a) 如数据库**SQLite3**设置中勾选了**自动恢复受损镜像**，则启动服务器会自动恢复数据库镜像。

b) 如未启用自动恢复数据库镜像，可在从命令行启动Dr.Web服务器时使用参数repairdb（参见附录中的H3.3. 数据库管理命令）。

10.3.8. 模块

在**模块**标签指定Dr.Web服务器与其它Dr.Web Enterprise Security Suite组件交互作用的模式：

- 勾选**Dr.Web代理端协议**后启用Dr.Web服务器与Dr.Web代理端的交互作用协议。
- 勾选**Microsoft NAP Health Validator**协议后启用Dr.Web服务器与Microsoft系统运行能力检测组件NAP Validator的交互作用协议。
- 勾选**Dr.Web代理端安装程序协议**后启用Dr.Web服务器与Dr.Web代理端安装程序的交互作用协议。
- 勾选**Dr.Web服务器群集协议**后启用群集系统中Dr.Web服务器间的交互作用协议。
- 勾选**Dr.Web服务器协议**后启用Dr.Web服务器与其他Dr.Web服务器的交互作用协议。默认为停用。设置多服务器网络时（参见. 多台Dr.Web服务器网络特点）需勾选**Dr.Web服务器协议**。
- 勾选**Dr.Web代理服务器协议**后启用Dr.Web服务器与Dr.Web代理服务器的交互作用协议。
- 勾选**Dr.Web安全管理中心插件**后可使用Dr.Web管理中心管理Dr.Web服务器和反病毒网络。



取消对**Dr.Web安全管理中心插件**勾选后，Dr.Web服务器重启后Dr.Web安全管理中心将无法对其进行访问。这时只能通过远程诊断工具管理Dr.Web服务器和反病毒网络，前提是插件**Dr.Web Server FrontDoor**一项为勾选。

- 勾选插件**Dr.Web Server FrontDoor**后可使用插件Dr.Web Server FrontDoor连接Dr.Web服务器远程诊断工具（参见远程访问Dr.Web服务器）。
- 勾选**Dr.Web的SNMP代理端插件**后允许Dr.Web服务器使用SNMP协议与网络控制系统交换信息（参见Dr.Web的SNMP代理端配置一节）。
- 勾选插件**Yandex.Locator**后允许使用插件Yandex.Locator确定连接到Dr.Web服务器的移动设备的位置。
  - 在**API密钥**输入利用Yandex公司相应服务获取的API密钥。



如启用了插件Yandex.Locator，但未指定API密钥，将无法激活插件。



如何使用和设置插件Yandex.Locator的详细信息参见附录中的自动确定OS Android工作站位置。

10.3.9. 位置

在**位置**标签指定安装Dr.Web服务器计算机地理位置的补充信息。

还可在此标签查看Dr.Web服务器在地图上的位置。

查看**Dr.Web**服务器在地图上的位置

1. 在**纬度**和**经度**以十进制度（Decimal Degrees）输入Dr.Web服务器地理坐标。
2. 点击**保存**按钮将输入的数据保存到Dr.Web服务器配置文件。
   显示地图不需要重启Dr.Web服务器。但应用修改后的地理坐标必须重启Dr.Web服务器。
3. 在**位置**标签显示的OpenStreetMap地图预览图出现对应坐标的标记。
   如无法打开预览图，会显示文字**在地图上标出**。
4. 查看全图需点击预览图或**在地图上标出**。

10.3.10. 授权

在**授权**标签指定Dr.Web服务器间分发授权的设置，以及授权使用情况报告设置。

设置已超过授权数量限制的通知

- **剩余授权数量**——剩余授权数量降至此值时会发送**授权密钥中的授权数量限制**通知。
- **剩余授权数量**——剩余授权数量降至此比例时会发送**授权密钥中的授权数量限制**通知。

授权使用情况报告的设置

在Dr.Web服务器间发送报告时只在Dr.Web主服务器指定设置，Dr.Web子服务器也会同样使用。

如未设置与Dr.Web邻居服务器的连接，这些选项只供当前Dr.Web服务器创建自身报告使用。

- **创建报告的周期**——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。
- **计算活跃工作站的周期**——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。

给出授权的Dr.Web服务器的设置

- **给出的密钥自动延期期限**——从此Dr.Web服务器密钥给出的密钥的有效期。到期后对给出的密钥进行相同期限的自动延期。授权管理器第5步给出的授权分发期内会重复自动延期。
  此机制用于保证如Dr.Web子服务器关闭而无法返还密钥时授权会返还给Dr.Web主服务器。
- **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。授权同步用于确认Dr.Web主服务器给出的授权于Dr.Web子服务器接收的授权数量相符。此机制用于查找错误和偷换分发授权的情况。

接受授权的Dr.Web服务器的设置

- **接收授权预延期时间**——从Dr.Web邻居服务器接收的授权自动延期期限剩余时间，从这一时间开始此Dr.Web服务器申请对这些授权进行自动预延期。

  这一设置的使用取决于配置Dr.Web服务器间连接时在**连接参数**选择的连接类型（见[设置Dr.Web服务器间连接]）：

  - 周期性连接类型：如连接设置中指定的连接周期大于在分发授权的Dr.Web服务器指定的**给出的密钥自动延期期限**，则在**给出的密钥自动延期期限**到期前进行这些授权的自动延期。
  - 不间断连接类型：不应用此设置。

Dr.Web服务器间分发授权详细信息见[通过服务器间连接分发授权]。

10.3.11. 日志

在**日志**标签设置Dr.Web服务器运行日志：

- 在**Dr.Web服务器日志详细等级**下列列表选择记录Dr.Web服务器运行日志的详细等级。
- **最多文件数量**——将保存的日志文件最多数量（包括当前文件和归档文件）。
- **Dr.Web服务器日志轮循模式**——Dr.Web服务器运行日志轮循模式。需选择以下一项：
  - **按照大小轮循**指定对每一日志文件大小的上限。

    每一文件最大大小——每一日志文件的大小上限。当前文件达到此上限后归档，并相应更改文件名称，同时创建新的日志文件。
  - **按照时间轮循**指定每一日志文件进行记录的时长。

    每一文件记录最长时限——每一日志文件进行记录的时间上限。当前文件达到此上限后归档，并相应更改文件名称，同时创建新的日志文件。
- 勾选**日志文件存档**后轮循过程中会将陈旧的日志压缩存档。

应用更改必须重启Dr.Web服务器。

可以利用管理中心，也可利用相应的控制台指令来执行重启。

Dr.Web服务器日志相关详细信息参见[Dr.Web服务器日志]。

10.4. 远程访问Dr.Web服务器

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。

设置**Dr.Web**服务器远程诊断工具连接参数

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**远程访问Dr.Web服务器**一项。
2. 指定连接协议设置：
   - 勾选**使用TLS**一项则允许远程诊断工具按照TLS协议连接Dr.Web服务器。如取消勾选则只可按照TCP协议连接。
     按照TLS协议连接需给出以下设置：
     - **证书**——连接时将检查的证书文件。下拉列表中是Dr.Web服务器目录中可选证书。
     - **SSL私钥**——连接时将检查的SSL私钥文件。下拉列表中是Dr.Web服务器目录中可选SSL私钥。
     - 在**TLS对话方加密密钥**一栏指定TLS对话方加密密钥文件路径。用于已对话方（session tickets）为基础恢复TLS对话，对话方使用指定的密钥加密。
     - **允许的密码列表**——此行用于确定允许用于与客户端连接的OpenSSL包密码列表。如留此行为空，将使用`DEFAULT`，表示`ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`。
3. 请指定连接接口设置：
   - **地址**——远程诊断工具连接时Dr.Web服务器端监听的IP地址。
   - **端口**——远程诊断工具连接时Dr.Web服务器端监听的端口。默认使用端口10101。

   添加连接接口需点击后填写补充输入栏。

   禁止使用之前指定的接口连接的方式是点击相应接口旁的按钮，将该接口从列表中删除。
4. 点击**保存**按钮。

Dr.Web服务器远程诊断工具的控制台版本使用介绍见**附录**中的H7.3. Dr.Web服务器远程诊断工具。

10.5. Dr.Web的SNMP代理端配置

Dr.Web的SNMP代理端使用SNMP协议将Dr.Web Enterprise Security Suite与网络控制系统进行整合。整合后可监控Dr.Web组件运行状态，并收集侦测和解除威胁的相关统计信息。

监控系统金额任一SNMP管理器都可访问Dr.Web服务器，服务器将通过Dr.Web的SNMP代理端提供信息。

可使用与Dr.Web服务器一起提供的MIB了解Dr.Web的SNMP代理端所能提供的信息。文件`DRWEB-ESUITE-STAT-MIB.txt`在服务器安装目录的子目录`etc`。

允许Dr.Web服务器使用SNMP协议与网络控制系统交换信息必须启用Dr.Web的SNMP代理端插件，操作是在**Dr.Web服务器配置**的模块标签勾选**Dr.Web的SNMP代理端插件**。

设置**Dr.Web的SNMP代理端插件连接参数**

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**Dr.Web的SNMP代理端插件配置**一项。
2. 在**社区**一栏给出SNMPv2c社区名称。默认为**public**。
3. 指定连接网络控制系统的接口设置：
   - **接口**——Dr.Web服务器端监听来自网络控制系统的连接使用的IP地址。
   - **端口**——Dr.Web服务器端监听来自网络控制系统的连接使用的端口。

   添加连接接口需点击后填写补充输入栏。

   禁止使用之前指定的接口连接的方式是点击相应接口旁的按钮，将该接口从列表中删除。
4. 勾选**只允许本地网络连接**后只允许从本地网络连接Dr.Web的SNMP代理端。

   勾选后需填写**本地地址列表**，网络控制系统可从这些地址连接Dr.Web的SNMP代理端。
5. 点击**保存**按钮。

10.6. Dr.Web服务器日程设置

设置**Dr.Web服务器任务执行日程**

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**Dr.Web服务器任务计划器**一项。打开Dr.Web服务器任务列表。
2. 利用工具面板的相应元素管理日程：

   a) 工具面板常规元素用于创建新任务和管理整个日程。可随时选择使用这些工具。

   添加默认日程中的任务——将默认日程中的所有任务添加到当前日程。这时会保留所有当前日程并添加所有默认日程。即便是当前日程已包含默认任务（完全相同或经更改），包括执行时间完全相同的情况下，也会添加默认任务。

   设置为默认日程——删除当前日程的所有任务，启用默认任务日程。

默认日程——初次安装Dr.Web服务器时创建的任务列表。此日程不可更改。

创建任务——添加新任务。此操作详见编辑任务。

将本部分设置导出到文件——将日程保存到专门格式的文件。

从文件将设置导入到本部分——从专门式格的文件导入日程。

不可将Dr.Web服务器任务列表导入到工作站任务计划器，也不可进行反向操作。

b) 管理现有任务可勾选个别任务或利用表头全选。之后在工具面板会出现管理所选任务的元素：

设置		操作
状态	允许执行	如果所选任务之前为禁止，则按照为其指定的日程激活。
	禁止执行	禁止执行所选任务。任务会保存在日程表，但不会执行。
 在常规标签利用**允许执行**选项可进行相同操作。		
重要性	设为重要	如未按照日程执行任务，进行非例行任务启动。
	设为不重要	只在日程指定时间执行，不论是否有未能执行的情况。
 在常规标签利用**重要任务**选项可进行相同操作。		
 复制设置		复制在当前日程中选出的任务。指定**复制设置**操作时会创建与所选任务设置相同的新任务。
 二次执行		对于一次性任务：按照为其指定的时间再次执行（更改任务执行次数见编辑任务）。
 删除所选任务		从日程中删除所选任务。
执行任务		立即执行列表中所选任务。这时即便是按照日程禁止执行的任务也会启动执行。

3. 更改任务参数需在列表中选择需要任务，这时或打开**编辑任务**窗口，介绍见下。
4. 编辑结束后需点击**保存**按钮接受更改。

编辑任务

利用编辑任务可：

1. 创建新任务。
   操作是在工具面板点击**创建任务**。
2. 编辑现有任务。
   操作是在任务列表中点击相应任务的名称。

打开任务参数编辑窗口。编辑现有任务时的设置与创建新任务相同。

 有*标志的输入栏必须填写。

编辑任务参数

1. 在**常规**标签设定以下参数：
   - 在**名称**一栏输入任务名称，新任务在日程中将以这一名称显示。
   - 如要激活任务的执行，需勾选**允许执行**。如取消勾选，任务会保存在日程表，但不会执行。

     可在任务计划器利用工具面板的**状态**进行相同的设置。

   - 勾选**重要任务**后如因某种原因未能在指定时间执行此任务，则会进行非例行任务启动。任务计划器每分钟查看一次任务列表，发现有重要任务未执行，就会启动执行。如启动时任务已未执行多次，则只非例行启动一次。

     可在任务计划器利用工具面板的**重要性**进行相同的设置。

   - 如取消对**异步启动任务**的勾选，任务将列入任务计划器的任务顺序执行队列。如勾选此项，则启动此任务不需等待执行次序。
2. 在**操作**标签的**操作**下拉列表选择任务类型并设置执行参数：

任务类型	参数描述
与**Active Directory**同步	此任务用于同步网络结构：Active Directory计算机容器转变为反病毒网络工作站组。 需指定以下参数： • **Active Directory**控制器——Active Directory控制器，如dc.example.com。 • 注册用户名——Active Directory用户的注册用户名。 • 密码——Active Directory用户的密码。 Windows操作系统的Dr.Web服务器没有必要一定进行设置。注册信息默认采用启动Dr.Web服务器进程的用户的注册信息（一般为LocalSystem）。 UNIX家族操作系统的Dr.Web服务器必须进行设置。 • 在**保护连接**下拉列表选择交换数据时使用的加密类型： ▫ **STARTTLS**——通过指令STARTTLS转为受保护的连接。默认连接使用的端口为25。 ▫ **SSL/TLS**——开通单独的受保护连接。默认连接使用的端口为465。 ▫ 无——不使用加密。将使用未受保护的连接交换数据。

任务类型	参数描述
	默认此任务为停用。激活需在任务设置或工具面板选择**允许执行**。
停止**Dr.Web**服务器	此任务用于结束Dr.Web服务器运行。 启动无高级参数设置。
写入日志文件	此任务是将指定行写入Dr.Web服务器日志文件。 **行**——写入日志文件的通知内容。
创建统计报告	此任务用于创建反病毒网络统计数据报告。 创建报告需启用**统计报告**（参见通知配置）。创建的报告将保存在安装Dr.Web服务器的计算机。获取报告的方式取决于通知类型： • 如通知发送方式为**电子邮箱**：向通知设置中指定的电子邮箱发送邮件，邮件包含报告位置链接，附件为报告本身。 • 所有其他通知发送方式：发送包含报告位置链接的通知。 创建任务需指定以下参数： • **通知模式**——通知组名称，按照通知组设置创建报告。标题名称在创建新的通知组时指定。 • **报告语言**——报告数据使用的语言。 • **日期格式**——包含日期的统计信息的显示格式。可选格式为： ▫ 欧洲格式：`DD-MM-YYYY HH:MM:SS` ▫ 美国格式：`MM/DD/YYYY HH:MM:SS` • **报告格式**——保存统计报告的文件格式。 • **报告期**——报告所含统计信息所属时间段。 • **组**——报告所含统计信息所属工作站组列表。同时选择多个工作站组使用CTRL或SHIFT按键。 • **报表**——报告所含统计信息所属报表。同时选择多个报表使用CTRL或SHIFT按键。 • **报告保存期**——在安装Dr.Web服务器的计算机保存报告的时间，从创建报告起计时。
叫醒工作站	

任务类型	参数描述
	此任务用于为工作站开机，例如：在执行扫描任务前。 开机参数： • **唤醒所有工作站**——是将所有连接此Dr.Web服务器的工作站开机。 • **按指定参数唤醒工作站**——是只唤醒符合以下参数的工作站： ▫ **IP地址**——需开机的工作站IP地址列表。格式为：10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30。设置列表时用逗号或换行将不同地址分开。也可将IP地址更换为计算机DNS名称。 ▫ **MAC地址**——需开机的工作站MAC地址列表。MAC地址位组使用符号 ':'隔开。设置列表时用逗号或换行将不同地址分开。 ▫ **组**——需开启其所属工作站的组列表。更改组列表需点击**编辑**（或组识别码，如组已指定）后在打开的查看选择需要的组。同时选择多个工作站组使用CTRL或SHIFT按键。 ⚠ 执行此任务需要工作站安装有支持Wake-on-LAN的网卡。 是否支持Wake-on-LAN可查看网卡说明或网卡属性（**控制面板** → **网络和Internet** → **网络连接** → **更改适配器设置** → **配置** → **高级**，为属性利用**Magic Packet唤醒指定值** → **启用**）。
可用授权所剩不多	此任务用于在为所选工作站组指定的所有密钥的授权剩余不多时发送通知**组中工作站数量已接近授权上限**。 ⓘ 为所选组指定是授权密钥有可能同时指定给其他授权对象。 需指定以下参数： • **可用授权数量**——为所选组指定的授权密钥剩余授权数量降至此值时会向管理员发送相应通知。 • **可用授权所占比例**——为所选组指定的授权密钥剩余授权数量降至此值时会向管理员发送相应通知。 • **组**——需检查其授权剩余数量的工作站组列表。同时选择多个工作站组使用CTRL和SHIFT按键。
向工作站发送通知	此任务是向工作站或工作站组发送自定义内容的通知。 通知设置详细信息参见向工作站发送通知。
工作站久未连接	

任务类型	参数描述
	此任务用于通知工作站很长时间未连接本Dr.Web服务器。 设置通知的操作是在通知配置使用**工作站久未连接服务器**选项。 在**天**指定认为工作站久未连接的时段。
库备份	此任务是定期进行库备份： 需指定以下参数： • **路径**——指定保存备份的目录的完整路径。 • **备份最多数量**——指定此目录保存的库备份的最多数量。达到数量限制后保存新备份时会删除现有备份中最陈旧的一个。 • **库区**确定保存反病毒组件的什么信息块： ▫ **整个库**——为在下表选出的组件保存库中所有校检。 ▫ **只限重要校检**——只为在下表选出的组件保存库中标为重要的校检。 ▫ **只限配置文件**——只为在下表选出的组件保存配置文件。 • 勾选需保存其信息的组件。 ⚠ 用于保存备份的目录应为空。否则在进行备份时会删除此目录内容。
执行脚本	此任务是执行在**脚本**一行指定的Lua脚本。 ⚠ 在使用同一数据库的多个Dr.Web服务器同时执行**执行脚本**类任务会导致任务执行出错。 执行Lua脚本时管理员可访问Dr.Web服务器目录内的整个文件系统以及安装Dr.Web服务器的计算机的某些系统指令。 禁止对日程的访问需为相应管理员取消**编辑Dr.Web服务器日程**的权限（参见管理员和管理员组）。
授权密钥到期	此任务用于显示Dr.Web产品授权即将到期的通知。 需指定离到期多长时间开始显示提示。

任务类型	参数描述
更换加密密钥	此任务是定期更换以下保证组件间加密的工具： • Dr.Web服务器上的私钥drwcsd.pri， • 工作站上的公钥*.pub， • 工作站上的证书drwcsd-certificate.pem。 由于某些工作站在更换密钥时可能处于离线状态，更换分两步执行。必须为每一步设置两个任务，且第二步需在第一步执行后过一段时间再执行，以保证在这段时间内工作站肯定会连接Dr.Web服务器。 创建任务时许需从下拉列表选择相应的步骤： • **添加新密钥**——是第一步，在这一步创建未激活的一对加密密钥和证书。工作站连接Dr.Web服务器后获得新的公钥和证书。 • **删除原密钥并转用新密钥**——是第二步，在这一步通知工作站转用新的加密密钥和证书，之后将现有工具更换为新工具：更换工作站上的公钥、证书和Dr.Web服务器上的私钥。 因某种原因没有获得新公钥和证书的工作站将无法连接Dr.Web服务器。解决的方式是手动将新公钥和证书置于工作站（在工作站更换密钥的操作参见**附录**中的将Dr.Web代理端连接到另一Dr.Web服务器）。
更新库	此任务用于启动从GUS更新库产品。 需指定以下参数： • 在**产品**列表勾选需按照此任务更新的库产品。 • 勾选**更新授权密钥**，激活库更新时自动更新授权密钥。详细信息见自动更新授权。
服务器关键数据备份	此任务用于为Dr.Web服务器以下重要数据建立备份： • 数据库， • 授权密钥文件， • 加密私钥。 需指定以下参数： • **路径**——指定保存数据的目录（如不指定，则使用默认目录）。 • **备份最多数量**——指定最多备份数量（数值0表示取消数量限制）。 详见**附录**中的附录 H3.5。

任务类型	参数描述
	用于保存备份的目录应为空。否则在进行备份时会删除此目录内容。
清空数据库	此任务是通过执行指令vacuum收集Dr.Web服务器数据库不使用的记录并将其删除。 启动无高级参数设置。
清空旧工作站	此任务是删除陈旧的工作站。 需指定一个时间段（默认为90天），如在此时段内工作站未曾访问Dr.Web服务器，则被确认为陈旧工作站并移至反病毒网络的**Deleted**组。这样的工作站会在执行**清空过时记录**任务时从Dr.Web服务器数据库彻底删除（从**Deleted**组删除工作站的期限在**清空过时记录**任务参数中为**已删除工作站**类型指定，自移至**Deleted**组时开始计时）。 旧数据自动从数据库删除是为了节约磁盘空间。默认情况下任务**清空过时记录**和**清空旧工作站**是时限是90天。减少天数会降低积累的反病毒网络各组件运行统计数据的代表性。增加天数会加大Dr.Web服务器的资源占用。
清空旧记录	此任务是从数据库删除陈旧信息。要删除的记录类型列于任务参数。 必须指定天数，超过此时段后数据库记录将被确认为旧记录，并且从Dr.Web服务器删除。 需为每一类型的记录分别指定数据删除期。
清空未发送事件	此任务是从数据库删除未发送的事件。 必须指定一个时段，超过此时段未发送的事件将被删除。 这里指的是Dr.Web子服务器向Dr.Web主服务器发送的事件。事件未能成功发送时会被列入未发送列表。Dr.Web子服务器按照设置的周期重新尝试发送。执行**清空未发送事件**任务时会删除保存期达到或超过指定时段的所有事件。
清空过时通知	

任务类型	参数描述
	此任务是从数据库删除以下通知： • 代理端通知 • Web控制台通知 • 按日程创建的报告 删除的是标记为过时的通知，即保存期一到期的通知，可自行设置保存期： • 对于通知：在为相应发送方式创建新通知时指定保存期（参见通知配置）。 • 对于报告：在创建报告任务重指定保存期。 启动无高级参数设置
运行程序	此任务用于启动任意程序。 由此任务启动的软件为背景模式。 需指定以下参数： • 在**路径**输入需启动的执行文件全称（带路径）。 • 在**参数**一栏输入启动程序命令行参数。 • 勾选**等待程序结束运行**同步执行后将等待此任务启动的程序结束运行。这时Dr.Web服务器会记录程序启动、返回码和程序结束运行时间。如取消对**等待程序结束运行**同步执行的勾选，则认为启动程序后任务就已完成，Dr.Web服务器 只记录程序启动。
Dr.Web邻居服务器久未连接	此任务用于通知Dr.Web邻居服务器很长时间未连接本Dr.Web服务器。 设置通知需在通知配置使用**邻居服务器久未连接**选项。 在**小时**和**分钟**指定认为Dr.Web邻居服务器久未连接的时段。
重启**Dr.Web**服务器	此任务用于重新启动Dr.Web服务器。 启动无高级参数设置。

3. 在**时间**标签设定以下参数：
   - 在**周期**下拉列表选择任务启动模式并根据所选周期相应设置时间：

启动模式	参数描述
结束时	任务将在Dr.Web服务器结束运行后启动执行。 启动无高级参数设置。
启动时	任务将在Dr.Web服务器开始运行时启动执行。 启动无高级参数设置。
在执行初始任务N分钟后	需在**初始任务**下拉列表选择此任务执行时间相对应的任务。 在**分钟**栏指定或从列表中选择执行初始任务后过多少分钟开始执行此任务。
每天	需输入几点几分，任务将每天在指定时间启动执行。
每月	需选择日期（几号），输入几点几分，任务将每月在指定日期指定时间启动执行。
每周	需选择星期几，输入几点几分，任务将每周在指定日期指定时间启动执行。
每小时	需输入从0到59的数字（分钟数）——任务将每小时在指定分钟启动执行。
每N分钟	需输入**N**值，确定执行任务的时间间隔。 如**N**等于或大于60，则任务每过**N**分钟启动执行一次。如**N**小于60，任务将在每小时内**N**的整倍分钟启动执行。

- 勾选**在第一次执行后禁止**后任务只在指定时间执行一次。如取消勾选，将按照指定周期多次执行。

可利用日程部分工具面板的**二次执行**按钮重复已经执行过的一次性任务。

4. 结束编辑后点击**保存**按钮保存对原有参数的更改或新建任务的参数。

10.7. 设置Web服务器配置

每一次保存**Web服务器配置**部分的更改时会自动备份上一版本的Web服务器配置文件。共保存10个不同版本的备份。

备份与配置文件在同一目录，目录名称格式为：

`webmin.conf_<创建时间>`

可使用备份在无法访问管理中心界面时恢复配置文件。

设置Web服务器配置参数的操作

1. 在管理中心主菜单选择**管理**。
2. 在打开窗口的控制菜单选择**Web服务器配置**。打开Web服务器设置窗口。

有*标志的输入栏必须填写。

3. 在工具面板可使用以下选项：

   重启Dr.Web服务器——重新启动Dr.Web服务器，以便应用对本部分的修改。修改设置并点击**保存**按钮后出现此选项。

   从备份恢复配置——下拉列表包含保存的设置备份，可利用备份取消当前的修改。修改设置并点击**保存**按钮后出现此选项。

   将所有参数设为初始值——还原这一部分所有参数此次编辑前的参数值（上次保存的参数值）。

   将所有参数设定为默认值——将这一部分所有参数设为默认值。

4. 应用对设置的效果需点击**保存**按钮，之后要求重启Dr.Web服务器。需点击工具面板的**重启Dr.Web服务器**按钮。

10.7.1. 常规

在**常规**标签指定运行Web服务器的以下设置：

- **Dr.Web服务器地址**——Dr.Web服务器IP地址或DNS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。
- **客户端平行申请数量**——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。
- **输入/输出线程数量**——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。
- **HTTP/1协议对话超时时限（秒）**——HTTP协议版本1对话超时时限。应用不间断连接时如客户端在指定时限内未发出请求，Dr.Web服务器会中断连接。此超时时限在本次对话过程中开始交换数据前有效。
- **按照HTTP/1协议发送最低速度（B/s）**——使用HTTP协议版本1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。
- **按照HTTP/1协议接收最低速度（B/s）**——使用HTTP协议版本1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。
- **HTTP/1发送超时时限（秒）**——在HTTP协议版本1协议一次对话内发送数据的超时时限。如在此时限内未能发送数据，则关闭对话。
- **HTTP/1接收超时时限（秒）**——在使用HTTP协议版本1协议进行的一次对话内接收数据的超时时限。如在此时限内未收到代理端发出的申请，则关闭对话。此超时时限在本次对话过程中开始交换数据后有效。
- **发送缓存大小（KB）**——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。

- **接收缓存大小（KB）**——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。
- **请求长度上限（KB）**——HTTP请求大小上限。
- **启用flood进攻防御**——勾选此项后将采取防御措施，阻止flood进攻。请指定以下进攻侦测参数：
  - **时长（秒）**——以秒记时段，如在此时段收到一定数量的申请，则会判定出现来自客户端的flood攻击。
  - **申请数量**——判定出现来自客户端的flood攻击所依据的一定时段内收到的申请数量下限。
  - **阻断时间（秒）**——在此期间内将阻止与客户端连接。

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

- **可压缩的响应最大大小（KB）**——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。
- **可压缩的响应最小大小（B）**——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。
- **压缩类型使用次序：**
  - **由客户端定义**——压缩类型使用次序由客户端按照允许的压缩类型定义。
  - **由服务器定义**——压缩类型使用次序由服务器按照允许的压缩类型定义。这时需要在下表指定压缩类型次序。更改次序需进行相应移动。

  可启用或停用以下压缩类型，并可指定次序（如次序由Dr.Web服务器确定）：
  - **使用GZIP压缩**——勾选此项则启用此压缩类型。在**GZIP压缩等级**指定0-9的一个数值。0值表示停用压缩。
  - **使用Deflate压缩**——勾选此项则启用此压缩类型。在**Deflate压缩等级**指定0-9的一个数值。0值表示停用压缩。
  - **使用Brotli压缩**——勾选此项则启用此压缩类型。在**Brotli压缩等级**指定0-11的一个数值。0值表示停用压缩。
- **替换IP地址**——勾选后在Dr.Web服务器日志文件将计算机IP地址更换为DNS名称。
- **启用HTTP/2支持**——勾选此项则支持按照HTTP协议版本2连接Web服务器。
  - **HTTP/2协议对话超时时限（秒）**——HTTP协议版本2对话超时时限。应用不间断连接时如客户端在指定时限内未发出请求，服务器会中断连接。
- **保持TLS对话持续**——勾选此项后使用TLS不间断连接。老版本的浏览器可能不支持不间断的TLS连接。如按照TLS协议运行出现问题，请停用此参数。
- **证书**——TLS证书文件路径。下拉列表中是Dr.Web服务器目录中可选证书。
- **TLS私钥**——TLS私钥文件路径。下拉列表中是Dr.Web服务器目录中可选TLS私钥。
- **TLS对话方加密密钥**——TLS对话方加密密钥文件路径。用于已对话方（session tickets）为基础恢复TLS对话，对话方使用指定的密钥加密。
- **允许的密码列表**——此行用于确定允许用于与客户端连接的OpenSSL包密码列表。如留此行为空，将使用`DEFAULT`，表示`ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`。

10.7.2. 高级

在**高级**部分指定运行Web服务器的以下设置：

- 勾选**显示脚本错误**后在浏览器显示脚本错误。此参数供Doctor Web公司技术支持和研发人员使用。如无特殊需要，不建议更改。
- 勾选**追踪脚本运行**后启动脚本运行追踪。此参数供Doctor Web公司技术支持和研发人员使用。如无特殊需要，不建议更改。
- 勾选**允许结束脚本运行**后允许中断脚本运行。此参数供Doctor Web公司技术支持和研发人员使用。如无特殊需要，不建议更改。
- 利用**自定义HTTP信头**的输入栏可以添加自定义发Web服务器回应HTTP信头。默认Web服务器使用三个预设安全信头：`X-XSS-Protection`、`X-Content-Type-Options`和`X-Frame-Options`。可利用Dr.Web服务器安装目录的子目录中的配置文件`webmin.conf`查看信头并进行编辑。

10.7.3. 传输

在**传输**标签设置监听Web服务器接入连接使用的网络地址，如连接管理中心或执行Web API请求使用的网络地址。

在**监听的地址**部分设置应监听的接收HTTP协议连接的接口列表：

- **地址**——允许接收其连接的网络接口的IP地址。
- **HTTP端口**——允许接收HTTP协议连接的网络接口的端口号。
- **HTTPS端口**——允许接收HTTPS协议连接的网络接口的端口号。

  默认情况下Web服务器"监听"的是：
  - **地址**：`0.0.0.0`——使用安装Web服务器的计算机的"所有网络接口"。
  - **端口**：`9080`——使用HTTP协议的标准端口`9080`。
  - **端口**：`9081`——使用HTTPS协议的标准端口`9081`。

添加新地址栏需点击按钮。删除具体地址行需点击旁边的按钮。

10.7.4. 安全策略

在**安全策略**标签限定Web服务器接收其发出的HTTP和HTTPS请求的网络地址。

常规

- 勾选**转至受保护连接**后自动将所有HTTP连接转至HTTPS。
- 勾选**返回详细信头**后Web服务器会在"Server"信头返回环境详细信息。
- 勾选**将URI转换为小写**后所有对Web服务器申请中的URI将转换为小写。转换只涉及URI中包含路径的部分。
- 勾选**启用对客户应用程序访问的监控**后将禁止机器人软件和下表中的其他客户应用程序访问管理中心界面。

确定需禁止的客户应用程序列表：

- 在**客户应用程序名称**一栏给出禁止其访问管理中心接口的客户应用程序名称。区分大小写。如未指定，则使用应用的URI。
- 在**定义用正则表达式**一栏给出确定禁止其访问管理中心接口的应用程序的正则表达式。

访问限制

限制某类型连接访问的操作

1. 允许利用HTTP或HTTPS访问需将相应地址分别列入**HTTP：允许**或**HTTPS：允许**。
2. 禁止利用HTTP或HTTPS访问需将相应地址分别列入**HTTP：禁止**或**HTTPS：禁止**。
3. 所有名单中都不包含的地址可以是都允许或都禁止，这取决于是否勾选**HTTP禁止优先**或**HTTPS禁止优先**：如勾选了此项，则禁止所有名单中都不包含的地址（或两个名单都包含的地址）；如不勾选，则允许这样的地址。

编辑地址列表的操作

1. 在相应输入栏输入网络地址，然后点击**保存**按钮。
2. 网络地址输入格式：*<IP地址>*/[*<前缀>*]。

> 只有计算机安装有IPv6界面才可显示TCPv6地址输入列表。

3. 添加新地址栏需点击相应项的按钮。
4. 删除地址栏需点击按钮。

前缀使用举例：

1. 前缀24代表网络掩码为：255.255.255.0
   包含254个地址。
   这些网络的主机地址为：195.136.12.*
2. 前缀8代表网络掩码为255.0.0.0
   包含的地址达16387064个（256*256*256）
   这些网络的主机地址为：125.*.*.*

10.7.5. 模块

> 未经技术支持建议，不要更改这一部分的设置。

在**模块**部分设置Lua脚本，随执行Web界面其他脚本进行加载。

- **搜索路径中的脚本目录**的下拉列表确定在**路径**部分列表的什么位置添加当前目录（当前执行的脚本所在目录）：

- 第一个——在列表开始处添加，
- 最后一个——在列表末尾处添加，
- 不使用——不添加。

- **掩码**部分给出不同掩码，用于按照**路径**部分给出的路径搜索Lua模块。
- **路径**部分给出路径，用于搜索**路径**部分的Lua模块。路径是相对于Web服务器根目录的路径。

例如：

如在**模块**部分没有给出高级设置，就无法找到位于`var-root/webmin/esuite/include/head.ds`的脚本。

即使在**模块**部分没有给出设置，也可以找到目录`ds-modules`或`webmin/vfs`中的模块，因为这是全球模块，而非Web界面模块。

10.7.6. 处理器



除了访问权限和身份验证，未经技术支持建议，不要更改这一部分的设置。

在**处理器**部分设置处理来自Web客户端的请求的方式和环境。

常规

不同类型的处理器有不同的设置。

对于Web套接字是根据**协议**属性来选择相应的处理器。

对于其他类型是根据**前缀**属性来选择相应的处理器。

在**类型**下拉列表选择可使用的处理器类型：

- **处理器**

  执行指定的脚本，其参数为URL中路径。如无路径，参数为**目录**一栏的路径。
  - **前缀**——HTTP请求的URL中路径的前缀。
  - **目录**——Web服务器根目录，发出的文件的路径从此目录开始。
  - **脚本**——脚本处理器。

- **混合处理器**

  取决于请求对应的文件类型，可以是**静态文件**类型，或者是**脚本**类型。
  - **前缀**——HTTP请求的URL中路径的前缀。
  - 索引文件列表。当Web客户端要求目录索引时此列表确定以什么顺序加载哪些文件。
  - **脚本**——应被确定为Lua脚本的文件扩展名列表。

- 脚本

  请求对应的任何文件都作为Lua脚本执行。
  - 前缀——HTTP请求的URL中路径的前缀。
  - 目录——Web服务器根目录，发出的文件的路径从此目录开始。

- 静态文件

  文件内容不变。
  - 前缀——HTTP请求的URL中路径的前缀。
  - 目录——Web服务器根目录，发出的文件的路径从此目录开始。
  - 索引文件列表。当Web客户端要求目录索引时此列表确定以什么顺序加载哪些文件。

- 虚拟文件系统

  与**静态文件**类型类似，但文件是从**目录**一栏指定的dar格式压缩文件加载。
  - 前缀——HTTP请求的URL中路径的前缀。
  - 目录——Web服务器根目录，发出的文件的路径从此目录开始。

- 预设的**Web**套接字

  Websocket应用，通过可分库实现，带服务器（dll或elf shared object）。库文件名称与Web套接字协议相符，文件位于lib-root/websockets。
  - 身份验证脚本——用于进行用户登录的Lua脚本文件名称。
  - 协议——WebSocket-Protocol的栏值，在连接Web套接字的HTTP请求中传输。

- **Web**套接字用户

  Websocket应用，通过Lua脚本实现。脚本文件名称与Web套接字协议相符，文件位于home-root/websockets。
  - 身份验证脚本——用于进行用户登录的Lua脚本文件名称。
  - 协议——WebSocket-Protocol的栏值，在连接Web套接字的HTTP请求中传输。

访问权限

访问限制列表（ACL），用于限制客户端访问Web服务器使用的网络地址。

设置与Dr.Web服务器安全设置类似。

如未给出设置，则认为允许所有地址。

登录

可用于所有类型的处理器，只有Web套接字除外。

这一部分的设置确定的是资源列表，访问这些资源时要求在Web客户端进行 basic http身份验证。

- **作用域**——Web服务器发给客户端的参数`WWW-Authenticate: Basic realm="ADMIN"`。实际上是身份验证者的简单描述，与用户名无关。

限制某类型连接访问的操作

1. 允许客户端按照HTTP或HTTPS连接时自由访问某些路径，需将这些路径添加到相应的**HTTP：自由访问**或**HTTPS：自由访问**。
2. 要求客户端按照HTTP或HTTPS连接时在访问某些路径时进行身份验证，需将这些路径添加到相应的**HTTP：要求身份认证**或**HTTPS：要求身份认证**。
3. 所有名单中都不包含的路径可以是要求进行身份认证或是不要求，这取决于是否勾选**身份验证申请优先**：如勾选了此项，则访问所有名单中都不包含的路径（或两个名单都包含的路径）要求身份验证；如不勾选，则允许自由访问这样的地址。

编辑地址列表的操作

1. 在输入栏输入正则表达式，用于启动相对于**目录**一栏所指定目录的路径。
2. 添加新地址栏需点击相应项的按钮。
3. 删除地址栏需点击按钮。

10.8. 自定义钩子

执行Lua脚本时管理员可访问Dr.Web服务器目录内的整个文件系统以及安装Dr.Web服务器的计算机的某些系统指令。

禁止对自定义钩子的访问需为相应管理员取消**编辑Dr.Web服务器配置和库配置**权限（参见管理员和管理员组）。

为简化并自动执行Dr.Web服务器的某些任务，可以使用Lua脚本格式的自定义钩子。

自定义钩子在Dr.Web服务器安装目录的以下子目录：

- OS Windows：`var\extensions`
- OS FreeBSD：`/var/drwcs/extensions`
- OS Linux：`/var/opt/drwcs/extensions`

安装Dr.Web服务器后子目录中出现预设自定义钩子。

编辑自定义钩子建议使用管理中心。

设置执行自定义钩子

1. 在管理中心主菜单选择**管理**。
2. 在打开窗口的控制菜单选择**自定义钩子**。 打开自定义钩子设置窗口。

钩子树结构

钩子分层列表以树结构显示，节点为钩子组和组中包含的自定义钩子。

初始树结构包含以下预设组：

- **Examples of the hooks**——包含所有可用自定义钩子模板。利用这些模板可创建自己的自定义钩子。不可编辑和执行钩子模板。
- **IBM Syslog**——包含用于与IBM Tivoli系统整合的自定义钩子。符合钩子的事件记录为*Syslog*。

  所有事件记录到一个文件，路径为：
  - OS Windows：
    `var\export\tivoli\syslog\drwcs_syslog.log`
  - OS FreeBSD：
    `/var/drwcs/export/tivoli/syslog/drwcs_syslog.log`
  - OS Linux：
    `/var/opt/drwcs/export/tivoli/syslog/drwcs_syslog.log`
- **IBM W7Log**——包含用于与IBM Tivoli系统整合的自定义钩子。符合钩子的事件记录为*W7Log XML*。

  为每一事件创建一个文件，路径为：
  - OS Windows：
    `var\export\tivoli\w7log\`*<事件名称>_<unix_timestamp>*
  - OS FreeBSD：
    `/var/drwcs/export/tivoli/w7log/`*<事件名称>_<unix_timestamp>*
  - OS Linux：
    `/var/opt/drwcs/export/tivoli/w7log/`*<事件名称>_<unix_timestamp>*

树结构中元素的图标取决于元素的类型或状态（见表10-7）。

表 10-7. 钩子树结构元素图标

图标	描述
钩子组	
	允许执行钩子的钩子组。
	禁止执行钩子的钩子组。
钩子	
	允许执行的钩子。
	禁止执行的钩子。

管理钩子树结构

管理钩子树结构使用工具面板的以下元素：

添加——用于添加钩子树结构元素的下拉列表：

添加钩子——添加新的自定义钩子。

添加钩子组——创建新的钩子组。

删除所选对象——删除再树结构中选出的自定义钩子或钩子组。

允许执行钩子——与勾选钩子编辑器的**允许执行钩子**选项进行的操作相同。参见激活钩子。

禁止执行钩子——与利用钩子编辑器取消对**允许执行钩子**的勾选进行的操作相同。参见激活钩子。

管理钩子组

创建新组

1. 在工具面板选择**添加** → **添加钩子组**。
2. 在打开的窗口给出以下参数：
   - 勾选**允许执行钩子**后激活此组中的钩子。参见激活钩子。
   - 在**组名称**指定所创建的组的自定义名称。
3. 点击**保存**按钮。

更改组使用次序

1. 通过在树结构上下移动（drag and drop）钩子组调整次序。
2. 更改此次序后自动更改执行次序：首先执行位于树结构上端的组中的钩子。

将钩子列入另一个组

1. 在树结构中选择需要移动的钩子。
2. 在打开的属性面板的**父组**下拉列表选择目标组。
3. 点击**保存**按钮。

钩子管理

添加新钩子

1. 在工具面板选择**添加** → **添加钩子**。
2. 在打开的窗口给出以下参数：
   - 勾选**允许执行钩子**后激活创建的钩子。参见激活钩子。
   - 在**父组**下拉列表选择此钩子所属的组。之后可以更改父组，另见上。
   - 在**钩子**下拉列表选择钩子类型。钩子类型决定调用此钩子的操作。

- 在**钩子文字**输入调用此钩子时执行的lua脚本。
  在**钩子信息**部分输入调用此钩子的事件；此钩子是否可以访问Dr.Web服务器数据库；以及此类钩子进港参数和反馈值列表。

3. 点击**保存**按钮。

编辑钩子

1. 在树结构中选择需要编辑的钩子。
2. 窗口右侧自动打开此钩子的属性面板。可编辑创建钩子时指定的所有参数，只有**钩子**参数除外。此参数确定调用钩子的事件，创建钩子后不可再进行更改。
3. 点击**保存**按钮。

激活钩子

是否激活钩子和钩子组决定在相应事件出现时是否执行钩子。

激活钩子或钩子组

1. 在树结构中选择需要激活的钩子或钩子组。
2. 执行以下一种操作：
   - 在工具面板点击**允许执行钩子**按钮。
   - 在右侧窗口所选对象属性面板勾选**允许执行钩子**。点击**保存**。

激活钩子时的注意事项：

如需钩子在与钩子对应的事件发生时执行，需：

a) 钩子本身已激活；
b) 钩子所在组已激活。

> 如果钩子所在组未激活，即便是钩子本身为激活状态，也不会执行。
>
> 钩子所在组激活后，只执行本身为激活状态的钩子。

10.9. 通知模板

在**通知模板**部分列出的是管理员可向工作站发送的自定义文本通知模板列表（见向工作站发送通知）。

可利用以下一种方式将通知添加到模板列表：

1. 可以之前管理员已发送的通知为基础创建模板。创建此类模板在通知日志。
2. 可创建全新模板。操作是点击工具面板**通知模板**部分的**创建模板**按钮。设置同向工作站发送通知部分的设置。

管理通知模板可使用工具面板的下列按钮：

删除——删除所选通知模板。

创建模板——创建新的通知模板（见上）。

编辑——编辑已存在的模板的设置。在列表选择一个模板后才可选用此项。

向工作站发送通知——利用所选模板向工作站发送一个或几个通知（见下）。

发送一个通知

1. 勾选一个通知模板。
2. 点击**向工作站发送通知**。
3. 打开**发送通知**窗口。给出以下设置：
   a) 在**反病毒网络**树结构选择接收通知的工作站或工作站组。
   b) 通知设置同 向工作站发送通知的设置。
4. 点击**发送**按钮。

发送多个通知

1. 勾选多个通知模板：
2. 点击**向工作站发送通知**。
3. 打开**发送多个通知**窗口。在**通知列表**出现所选通知。通知名称为其模板名称。
4. 点击**全部发送**，发送列表中所有通知。
5. 如需编辑某通知，需在**通知列表**选择后在**通知设置**指定以下参数：
   a) 在**反病毒网络**树结构选择接收通知的工作站或工作站组。
   b) 通知设置同 向工作站发送通知的设置。
   c) 取消发送某通知需点击**删除**按钮。

10.10. 通知设置

Dr.Web Enterprise Security Suite可向Dr.Web Enterprise Security Suite反病毒网络管理员发送有关病毒攻击、反病毒网络组件状态及其他事件的通知。

10.10.1. 通知配置

设置反病毒网络事件通知

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**通知配置**一项。
2. 要单独为管理中心的每一位管理员设置通知配置。为其指定设置的管理员的名称在**接收通知的管理员**一栏显示。为另一管理员设置通知需点击后在打开的窗口选择管理员。
3. 首次设置时默认为主管理员**admin**添加一个通知单元。如管理员通知列表为空需在**通知列表**点击**添加通知**。
4. 启用通知发送需将各通知单元表头左侧的开关置于相应位置：

——发送本单元通知。

——不发送本单元通知。

5. 可设置多个通知单元（模式），如用于区分发送方式。添加新单元需点击通知单元设置右侧的。表下方会出现新的通知单元。不同单元的设置，同通知模板文本设置一样，为分别独立进行。
6. 在**标头**输入通知单元名称。在Dr.Web服务器日程设置任务**创建统计报告**时会使用此名称。之后如需要编辑名称，需鼠标左键点击后进行修改。如存在多个单元，则点击标头后出现各单元标头列表。
7. 选择群发方式需在**通知发送方式**下拉列表选择一种类型：
   - Dr.Web代理端——使用代理端日志发送通知。
   - Web控制台——将通知发送到Web控制台查看。
   - 电子邮件——利用电子邮箱发送通知。
   - Push通知——将Push通知发送到Dr.Web移动安全管理中心。只有当Dr.Web移动安全管理中心连接本Dr.Web服务器后在**通知发送方式**下拉列表中才会出现此项。
   - SNMP——使用SNMP日志发送通知。

   每一发送方式具体设置见下。
8. 在通知列表勾选需按照当前通知单元发送方式发送的通知。
9. Dr.Web服务器通知预设有一组标准通知文本。

> 预设通知及其参数介绍见**附录**，附录D2. 通知模板参数。

设置具体通知的操作：

a) 点击标题部分的**转换为通知编辑模式**。

b) 更改通知设置时点击许编辑的通知。打开通知模板。如需可编辑通知内容。通知文本中可使用变量（花括号）。可使用通知标头下拉列表添加变量。在生成通知时系统会按照当前设置将变量转为具体内容。可选变量见**附录**中的附录D2. 通知系统模板参数。

c) 使用邮箱通知可在每个帖子模板编辑器的**信头**部分添加自定义栏（见**a)**）。信头格式应符合标准RFC 822、RFC 2822，不与邮箱通知标准确定的输入栏交叉。RFC 822标准可保证以X-开始的信头不在信头规格内，因此建议名称使用格式X-*<信头名称>*。如：`X-Template-Language: Chinese`。

d) 可为**工作站**部分指定将通知其事件的工作站列表。在模板编辑窗口**跟踪的工作站组**树结构中选择将跟踪其事件并发送相应通知的工作站组。多选利用CTRL或SHIFT。

e) 进行更改后点击标题中的**退出通知编辑模式**。

> 对于**SNMP**发送方式通知模板文本在客户端（RFC 1067名称为*控制工作站*）指定。在管理中心的**工作站**部分只可指定将通知其事件的工作站列表。

10. 点击**保存**按钮应用所有更改。

使用代理端日志发送通知

使用代理端协议只可将通知发送到Windows操作系统Dr.Web代理端。

使用代理端日志发送通知需指定以下参数：

- 在**Dr.Web服务器重新发送**指定如Dr.Web服务器在下述情况下重复发送通知的设置：
  - **数量**——Dr.Web服务器未能成功发送通知时重复发送的尝试次数。默认为10。
  - **超时时限**——Dr.Web服务器尝试重新发送的时限，以秒计。默认为300秒钟。
- **工作站**——接收通知的工作站的识别码。可在工作站属性查看识别码。
- **发送测试性通知**——按照通知系统设置发送测试性通知。

在Web控制台显示的通知

在Web控制台显示的通知需设置以下参数：

- 在**Dr.Web服务器重新发送**指定如Dr.Web服务器在下述情况下重复发送通知的设置：
  - **数量**——Dr.Web服务器未能成功发送通知时重复发送的尝试次数。默认为10。
  - **超时时限**——Dr.Web服务器尝试重新发送的时限，以秒计。默认为300秒钟。
- **通知保存时间**——收到通知后进行保存的时长。默认为1天。超出此时长后按照Dr.Web服务器日程中的**删除陈旧通知**任务设置删除通知。

  使用此方式发送的通知可在Web控制台通知设置无限期保存。
- **发送测试性通知**——按照通知系统设置发送测试性通知。

利用电子邮箱发送通知

利用电子邮箱发送通知时需指定以下参数：

- 在**Dr.Web服务器重新发送**指定如Dr.Web服务器在下述情况下重复发送通知的设置：
  - **数量**——Dr.Web服务器未能成功发送通知时重复发送的尝试次数。默认为10。
  - **超时时限**——Dr.Web服务器尝试重新发送的时限，以秒计。默认为300秒钟。
- **收件人电子邮箱**——通知收件人的电子邮箱地址。每一栏只可输入一个电子邮箱地址。添加收件人点击。删除输入栏点击。

  设置发送电子邮件的参数在**管理**菜单的**Dr.Web服务器配置**中的**网络**标签的子标签 电子邮件。
- **发送测试性通知**——按照通知系统设置发送测试性通知。

Push通知

向移动管理中心发送push通知需给出以下参数：

- 在**Dr.Web服务器重新发送**指定如Dr.Web服务器在下述情况下重复发送通知的设置：
  - **数量**——Dr.Web服务器未能成功发送通知时重复发送的尝试次数。默认为10。
  - **超时时限**——Dr.Web服务器尝试重新发送的时限，以秒计。默认为300秒钟。
- **发送测试性通知**——按照通知系统设置发送测试性通知。

使用SNMP协议发送通知

使用SNMP发送通知需指定以下参数：

- 在**Dr.Web服务器重新发送**指定如Dr.Web服务器发送失败后尝试重复发送通知的设置：
  - **数量**——Dr.Web服务器未能成功发送通知时重复发送的尝试次数。默认为10。
  - **超时时限**——Dr.Web服务器尝试重新发送通知的时限，以秒计。默认为300秒钟。
- 在**SNMP子系统重新发送**指定如SNMP子系统发送失败后尝试重复发送通知的设置：
  - **数量**——SNMP子系统未能成功发送通知时重复发送的尝试次数。默认为5。
  - **超时时限**——SNMP子系统进行一次重新发送通知尝试的时限，以秒计。默认为5秒钟。
- **收件人**——接收SNMP请求的实体。如计算机IP地址或DNS名称。每一栏只可输入一个收件人。添加收件人点击。删除输入栏点击。
- **发件人**——发送SNMP请求的实体。如计算机IP地址或DNS名称（应当能够被DNS服务器识别）。默认使用空白值。
- **社区**——SNMP社区或上下文。默认为`public`。
- **发送测试性通知**——按照指定的设置发送测试性通知。



您可使用与SNMP子系统服务器一起提供的MIB在解析SNMP trap时获取OID描述。文件`DRWEB-ESUITE-NOTIFICATIONS-MIB.txt`和`DRWEB-MIB.txt`在Dr.Web服务器安装目录的子目录`etc`。

10.10.2. Web控制台通知

利用管理中心可跟踪和管理使用**Web控制台**方式收到的管理员通知（管理员通知发送介绍见通知配置）。

查看和管理Web控制台通知

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**Web控制台通知**一项。打开Web控制台发送的通知列表。
2. 查看通知需点击表中对应的行。打开通知内容窗口。这时通知会自动标为已读。
3. 使用工具面板上是选项对通知列表进行管理：
   a) 如需显示一定时间段内收到的通知，可采用以下一种方式：
      - 在工具面板下拉列表选择一个预设时段。

- 在下拉日历选择任意开始和截止日期。

更改设置值后点击**更新**按钮，显示符合设置条件的通知。

b) 管理具体通知可勾选个别通知或利用表头全选。之后在工具面板会出现以下元素：

删除——删除所有所选通知，删除后无法恢复。

将通知标为已读——将所有所选通知标为已读。

c) 管理具体类型的通知可勾选相应类型通知。之后在工具面板会出现以下元素：

未批准的工作站——只有选择**工作站在等待确认**类通知后才可使用此项。可在下拉列表批准工作站或拒绝工作站访问Dr.Web服务器。

扫描——只有选择**网络病毒流行**、**扫描进程出错**和**发现安全威胁**类通知后才可使用此项。可在下拉列表指定在工作站启动Dr.Web扫描仪的参数。

组件管理——只有选择**工作站更新出现重大错误**类通知后才可使用此项。可在下拉列表指定在工作站启动反病毒软件更新的参数。

重启工作站——只有选择**应用更新必须重启工作站**类通知后才可使用此项。此项会启动工作站重启。

d) 如需可将通知导出到文件。导出的是当前表格中符合时间段和列过滤设置的通知。

导出通知需点击工具面板的一个按钮：

将数据保存到**CSV**文件，

将数据保存到**HTML**文件，

将数据保存到**XML**文件，

将数据保存到**PDF**文件。

4. 使用通知表格中的选项对通知进行管理：

a) 如通知在保存期到期后也不应删除，需勾选通知旁的图标**保存通知，不自动删除**（通知保存期在**Web控制台发送方式设置的**通知配置部分给出）。勾选后这些通知将一直保存，删除方式只能是在**Web控制台通知**部分将其手动删除或取消这些通知旁边的图标。

b) 如要只显示特定的通知，需点击需筛选的表列的标题。在打开的菜单勾选需显示的通知的参数。

筛选可使用的选项：

列	参数	操作
重要性	重大错误	只显示具备相应重要级别的通知。勾选所有选项则显示所有通知。
	高	
	中等	
	低	
	最低	
来源	代理端	显示有关工作站事件的通知
	Dr.Web服务器	显示有关Dr.Web服务器事件的通知

c) 进行报表格式设置需点击表头右角的图标。可在下拉列表设置以下选项：

- 启用或停用长句子的换行。
- 选择将在表中显示的列（名称旁有旗标）。点击列名称行可设置显示 / 不显示此列。
- 选择表中各列排列次序。更改的方式是将相应列拖至相应位置。

10.10.3. 未发送的通知

利用管理中心可跟踪和管理未能按照通知配置发送的管理员通知。

查看和管理未发送的通知

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**未发送的通知**一项。打开此Dr.Web服务器未发送的通知列表。
2. 未发送通知列表中包含的通知是未能发送给收件人的通知，但尚未达到这一通知设置中指定的重新发送尝试次数。
3. 未发送通知列表包含以下信息：
   - **通知**——预设通知列表中的通知名称。
   - **信头**——通知组名称，此通知是按照此组设置发送的。
   - **剩余发送次数**——未能成功发送时重新发送尝试的剩余次数。重新发送尝试次数在通知配置中指定。通知发送后不能再更改此通知的重新发送尝试次数。
   - **下次发送时间**——下次重新发送尝试的时间。重新发送尝试的时间间隔在通知配置中指定。通知发送后不能再更改此通知的重新发送尝试时间间隔。
   - **收件人**——通知收件人地址。
   - **错误**——导致通知未能发送的错误。
4. 管理未发送通知的操作：
   a) 勾选具体通知或通过勾选表头全选表中所有通知。
   b) 使用工具面板的下列按钮：
   重发——立即发送所选通知。这是非例行重发。如失败剩余重发次数将减少一次，下次重发时间将按照通知配置指定的时间间隔从此次非例行重发时间顺延。
   删除——删除所有所选未发送的通知，删除后无法恢复。
5. 下述情况对未发送的通知采取删除操作：
   a) 通知已发送给收件人。
   b) 通知已被管理员手动或通过工具面板的**删除**按钮删除。
   c) 重发尝试次数达到限定值，而通知还是未能成功发送。
   d) 在通知配置已删除了此通知按照其设置发送的通知组。

10.11. 管理Dr.Web服务器库

Dr.Web服务器*库*用于保存软件标样，并从GUS服务器对其进行更新。

库中为一系列*产品*文件。每一产品保存于Dr.Web服务器目录`var/repository`下单独的子目录。库管理功能可针对每一产品单独使用。

库更新管理使用产品*校检*这一概念。校检代表当前时间产品文件的正确状态（包括文件名称和校检和），并具有独有代码加以区分。

更新库产品

更新库产品可以是：

a) 从**Dr.Web**全球更新系统将更新加载到**Dr.Web**服务器。

按照Dr.Web服务器日程自动从GUS更新Dr.Web服务器库。

- 查看库更新任务是在库常规配置的**任务计划器**标签。
- 更改GUS更新日程需打开Dr.Web服务器日程设置。
- 检查是否有扫更新并手动加载更新，需在库状态点击**检查更新**。

另参见未接通互联网的Dr.Web Server的库更新。

b) 多服务器网络中的各**Dr.Web**服务器之间分发更新。

如反病毒网络中安装有多个Dr.Web服务器，可设置服务器间连接来传递库更新。

- Dr.Web主－子服务器间从GUS接收更新的是主服务器，Dr.Web子服务器会自动从Dr.Web主服务器获取所有更新。
- 同级服务器间客将任何一个Dr.Web服务器指定为从GUS接收更新的服务器。其他Dr.Web服务器会自动从此服务器获取所有更新。

服务器间连接设置见多台Dr.Web服务器网络特点。

如网络中设置了服务器间连接，且其他Dr.Web邻居服务器从您的Dr.Web服务器获取更新，需要在您的Dr.Web服务器同时启用这些Dr.Web邻居服务器的系统更新和界面语言更新。

c) 从**Dr.Web**服务器向工作站分发更新。

代理端每次连接Dr.Web服务器都会检查更新，如发现更新会从Dr.Web服务器加载并安装到工作站，代理端运行过程中隔一段时间也会检查、加载和安装更新（不需设置，对管理员为透明操作）。

如需可以在工作站更新限制限制代理端进行更新是时间和流量。

设置库参数

反病毒网络管理员可以对库进行以下参数设置：

- 执行**a)**类型操作时更新网站列表。

  可在库常规配置设置连接GUS的参数。

- **限制需要进行a)类型同步的产品种类。**

  从GUS加载的产品可在库常规配置和 库详细配置加以限制。
  这样管理员可以只监控部分产品的变化情况。

- **限制需要进行c)类型同步的产品组成。**

  Dr.Web服务器管理员可以选择具体需要安装到工作站的组件。选择组件在可安装的反病毒软件包组件。

- **监控转用新校检。**

  为库中每一产品分别设置校检更新配置在库详细配置。
  这时可在使用前自行测试产品。

- **管理库中文件和文件夹。**

  库内容 部分用于查看和管理库中文件和目录：可导入和导出个别产品，也可导入导出整个裤及其设置。

库中产品组成

目前提供以下产品：

- **Dr.Web管理员工具**

  用于所有支持的操作系统的工具：
  - Dr.Web库加载器（图形版本和控制台版本），
  - Dr.Web移动管理中心（App Store和Google Play链接），
  - Dr.Web系统信息收集工具，
  - 数字密钥和证书生成工具，
  - Dr.Web服务器远程诊断工具，
  - Dr.Web服务器脚本运行远程诊断工具，
  - Dr.Web for Windows删除工具，
  - 用于UNIX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代理端远程安装工具。

  所有工具都可从管理中心的**管理→工具**下载。

- **Dr.Web Agent for UNIX**

  用于UNIX操作系统的内置过滤器数据库和反垃圾邮件数据库，以及反垃圾邮件引擎。

- **Windows操作系统Dr.Web代理端**

  用于OS Windows工作站反病毒组件软件。

- 用于**Android**操作系统的**Dr.Web**数据库

  OS Android工作站病毒库。

- **SpIDer Gate**数据库

  用于Windows操作系统的反病毒组件内置过滤器数据库。

- **Dr.Web**反垃圾邮件数据库

  用于Windows操作系统的Dr.Web反垃圾邮件数据库。

- **Dr.Web**病毒库

  用于OS Windows和UNIX家族操作系统工作站的病毒库和反病毒引擎。

- **Dr.Web**服务器安全数据

  包括密钥、脚本和证书，用于保证反病毒网络组件更新和Dr.Web服务器与代理端间数据传输的安全性。

- 可信任的应用程序

  OS Windows工作站应用程序监控组件的可信任的应用程序组。

  产品**可信任的应用程序**不能从GUS进行更新。此产品只能使用服务器间连接在Dr.Web邻居服务器间分发。

  产品**可信任的应用程序**的库设置的详细信息见可信任的应用程序。

- 帮助文档

  手册和帮助，可在管理中心**支持**部分打开。

- 已知威胁哈希值

  已知威胁哈希列表

- **Dr.Web**企业产品

  以下产品的安装包：

  - 安装到OS UNIX（包括局域网服务器）、Android、macOS受保护工作站的产品，
  - Dr.Web for IBM Lotus Domino，
  - Dr.Web for Microsoft Exchange Server，
  - Dr.Web代理服务器——不与与Windows操作系统Dr.Web代理端一起安装，而是单独安装代理服务器的安装包，
  - 用于Windows操作系统的Dr.Web代理端完整安装程序，
  - 用于Active Directory的Dr.Web代理端，
  - Active Directory架构更改工具，
  - Active Directory对象参数更改工具，
  - NAP Validator。

10.11.1. 库状态

检查库的当前状态或者更新反病毒网络组件

1. 在管理中心主窗口选择**管理**，在打开的窗口选择控制菜单中的**库状态**一项。
2. 打开的窗口显示库产品列表、当前使用的校检的日期、上次加载校检的日期和产品状态。

> 状态一列为上次更新时Dr.Web服务器库中产品的状态。

3. 使用工具面板的下列按钮管理库内容：
   - 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。如查看的组件已过时，则会自动进行更新。
   - 下载库更新日志需点击工具面板的以下一个按钮：
     - 将数据保存到**CSV**文件，
     - 将数据保存到**HTML**文件，
     - 将数据保存到**XML**文件，
     - 将数据保存到**PDF**文件。
   - 点击**从磁盘重启库**后从磁盘重新启动库的当前版本。

   启动Dr.Web服务器时将库内容加载到内存。如在Dr.Web服务器运行过程中管理员没有利用管理中心而更改了库内容，如使用外设工具或手动更新了库内容，则使用加载于磁盘的库版本需要进行重启。

10.11.2. 推迟的更新

在**推迟的更新**部分是**库详细配置**→ *<产品>* → 推迟的更新中设置为暂时禁止更新的产品列表。推迟的校检为*冻结*。

冻结的产品列表包含以下信息：

- **库中目录**——库中冻结产品目录的名称：
  - 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。

- **校检**——被冻结的校检的代号。
- **推迟至**——本产品更新推迟开始的时间。

点击冻结产品表行打开此产品被冻结校检的详细信息。

如需暂时取消将最新校检分发给反病毒网络所有工作站时可使用冻结更新的功能，例如需在个别工作站首先测试此校检时。

使用推迟更新功能的操作详见**库详细配置**→ 推迟的更新。

管理推迟的更新

1. 更新所有需要编辑推迟更新操作的产品。可勾选冻结产品表表头全选。
2. 在工具面板中选择操作：

   立即执行——取消冻结，将此校检列入按常规流程分发到工作站的校检列表。

   取消更新——取消冻结并禁用词校检。恢复从GUS获取更新。取消冻结的校检从产品列表删除，接收到下一校检时此校检会从磁盘删除。

   更改更新延迟时间——指定此产品校检有错误的时间。冻结开始时间为从GUS获得此校检的时间。
3. 如对冻结产品未进行解冻操作，则**更新延迟时间**一到，校检会自动解冻并列入按常规流程分发到工作站的校检列表。

10.11.3. 库常规配置

库常规配置部分用于指定全球更新系统连接参数和库更新所有产品的参数。

编辑库配置

1. 在管理中心主菜单选择**管理**。
2. 在打开的窗口选择控制菜单中的**库常规配置**。
3. 设置从GUS进行更新的所有必需参数，参数具体介绍见下。
4. 如在编辑过程中需要取消所有修改，需使用工具面板的下列按钮：

   将所有参数设为初始值——将这一部分所有参数还原为此次编辑前的参数值（上次保存的参数值）。将个别参数还原为初始值使用每个参数旁边的按钮。

   将所有参数设为默认值——将这一部分所有参数还原为Dr.Web服务器配置文件保存的默认值。将个别参数还原为默认值使用每个参数旁边的按钮。
5. 点击**保存**后保存库配置的所有更改。这时会从磁盘重启库当前版本。

> 应用新的库配置需要一定时间。更改配置后立即从GUS更新库时使用的可能是之前的设置。

10.11.3.1. Dr.Web GUS

在**Dr.Web GUS**标签对Dr.Web全球更新系统连接参数进行设置。加载更新所使用的协议遵照**获取更新使用的协议**下拉列表中的协议：

协议类型	描述
HTTP/HTTPS	用于从Web服务器获取更新的协议
FTP/FTPS	用于从FTP服务器获取更新的协议
FILE	用于从到安装有Dr.Web服务器的计算机的本地目录获取更新的协议
CIFS/SMB	用于从统一文件系统获取更新的协议
SCP/SFTP	用于使用加密连接获取更新的协议

编辑与**GUS**建立连接

- 在**获取更新使用的协议**下拉列表选择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**Dr.Web全球更新系统服务器列表**设置。
- **基本URI**——更新服务器上包含Dr.Web产品更新的目录。如从Dr.Web GUS服务器获取更新，没有特殊需要不应更改此参数。
- 如在**获取更新使用的协议**选择的是支持加密的协议，需在**可用证书**下拉列表选择建立连接时自动接受的TLS证书类型。
- 如在**可用证书**列表选择的是**自定义**，则必须在**证书**输入栏指定TLS证书文件路径。
- **注册用户名**——如需要进行身份验证，登录更新服务器的用户名。
- **密码**——如需要进行身份验证，登录更新服务器的密码。
- 在**登录方式**下拉列表选择更新服务器登录方式。
- **临时保存校检数量**一栏临时保存于磁盘的每一产品的校检数量，不包括**库详细配置**中**校检列表**标签已作出标志的校检。

  如需可在同步分别为每一产品指定此设置，但在保存了对常规配置的更改后，设置会变为常规值。
- 勾选**使用CDN**，允许加载库时使用Content Delivery Network。
- 如需可在**Dr.Web全球更新系统服务器列表**部分编辑GUS服务器列表：
  - 将GUS服务器添加到此列表需点击后再新添输入栏输入GUS服务器地址。
  - 从此列表删除GUS服务器需点击需要删除的服务器旁边的按钮。
  - 表中GUS服务器顺序确定加载库时访问Dr.Web服务器的次序。可使用服务器所在行左侧小柄上移下移更改GUS服务器顺序。

  安装Dr.Web服务器时列表中只包含Doctor Web公司更新服务器。如需可设置自己的更新区并将其添加到更新服务器列表。

10.11.3.2. 任务计划器

任务管理器标签是Dr.We服务器日程中的所有库更新任务。

可在Dr.Web服务器任务管理器创建、删除和编辑库更新任务。

10.11.3.3. Dr.Web代理端

- **Dr.Web for UNIX代理端**标签选择哪些UNIX操作系统需要更新工作站上可安装的组件。

  完全禁止从GUS获取UNIX代理端更新的操作是打开库详细配置的**Dr.Web for UNIX代理端**，在同步标签勾选**停用产品更新**。

- 在**Windows操作系统Dr.Web代理端**标签选择是否需要更新OS Windows下工作站上可安装的所组件，还是只更新病毒库。
- 在**Windows操作系统Dr.Web代理端**标签指定从GUS下载的OS Windows代理端和反病毒软件包界面语言。

10.11.3.4. Dr.Web服务器

- 在**Dr.Web服务器**标签指定哪些操作系统需要更新Dr.Web服务器文件：
  - 获取所有支持的操作系统的Dr.Web服务器更新需勾选**更新可从GUS更新的所有平台**。
  - 获取个别操作系统Dr.Web服务器更新需勾选相应的操作系统。

  完全禁止从GUS获取Dr.Web服务器更新的操作是打开库详细配置的**Dr.Web服务器**，在同步标签勾选**停用产品更新**。

- 在**Dr.Web安全管理中心语言**标签指定从GUS下载的管理中心界面语言。
  - **使用的语言**部分是设置中为管理员指定的语言列表。
  - **未使用的语言**部分是设置中没有为任何管理员指定的语言列表。
- 在**帮助文档**标签选择语言，所选语言的帮助文档会出现在**帮助** → 支持。
  - 帮助文档分为**使用的/不使用的语言**的原则与**Dr.Web安全管理中心语言**区分原则相同。
  - 访问PDF格式的手册需在**PDF格式文档**部分勾选语言选择下方的**更新文档**。

10.11.3.5. Doctor Web公司新闻

在**Doctor Web公司新闻**标签指定下载新闻的语言列表。

订阅新闻的设置是在设置 → **订阅**。

还可在管理中心主菜单**支持** → **新闻**阅读已下载的Doctor Web公司新闻。

10.11.3.6. Dr.Web安装包

- 在**Dr.Web企业产品**标签下拉列表勾选需要从GUS更新的产品：
  - **更新所有产品**——从GUS更新库时会更新所有可以更新的企业产品。
  - **只更新所选产品**——从GUS更新库时会只更新下表勾选的产品。

  从GUS加载后企业产品出现在**管理** → **高级功能** → 企业产品部分，安装页面也会出现相应链接：

  `https://<Dr.Web服务器地址>:<端口号>/install/`

  其中*<Dr.Web服务器地址>*为安装有Dr.Web服务器的计算机的IP地址或域名。在*<端口号>*需输入端口号`9080`（如果是http则为`9081`）。
- 在**Dr.Web管理工具**标签下拉列表勾选需要从GUS更新的工具：
  - **更新所有产品**——从GUS更新库时会更新所有可以更新的管理员工具。
  - **只更新所选产品**——从GUS更新库时会只更新下表勾选的工具。

  从GUS加载后管理工具会出现在**管理**→**高级功能**→ 工具。

10.11.4. 库详细配置

库详细配置部分用于为库中每一产品分别设置校检配置。

编辑库配置

1. 在管理中心主菜单选择**管理**。
2. 在打开窗口控制菜单**库详细配置**选择需要编辑的产品。
3. 设置所选产品库的所有必需参数，参数具体介绍见下。
4. 在工具面板可使用以下选项对产品整体校检进行管理：
   - **删除库中产品**——将产品从库中彻底删除。执行这一操作时会删除产品的所有校检，且会停用从GUS进行产品更新。产品未从库中删除时此项可选，删除后按钮名称更换为**恢复库中产品**。

     从库中删除产品后**校检列表**为空，其他标签保留原样，但因产品不在库中而不能应用这些标签的设置。

   - **恢复库中产品**——将之前利用**删除库中产品**按钮删除的产品恢复到库中。执行这一操作时会启用从GUS进行产品更新。将GUS上产品最新校检加载到库中。请注意加载数据的大小。可在库常规配置对加载更新进行设置。恢复产品后按钮名称更换为**删除库中产品**。
   - **保存并从磁盘重启**——保存所有更改。这时会从磁盘重启库当前版本（参见库状态）。

10.11.4.1. 校检列表

在**校检列表**标签是在此Dr.Web服务器可访问的此产品所有校检相关信息。

删除某些校检时需进行勾选，然后点击工具面板的**删除所选校检**按钮。

不可删除所有校检。每一产品应至少包含一个校检。

将库中某产品整体删除使用**删除库中产品**按钮。

删除校检——此操作不可逆。

校检列表包含以下项目：

列名称	内容描述
可分发校检	此列使用自动标志表示产品校检状态。有两种标志： ——*可分发校检*。此类校检用于更新工作站上的代理端和反病毒软件。 采用以下方式选择可分发校检： 1. 分发在**当前**列带有标志的校检。只可标志出一个校检。 2. 如在**当前**列未标出，则分发在**保存**列带有标志的上一校检。 3. 如在**当前**和**保存**两列均未标出，则分发最新校检。 自动标志总是对应可分发校检。 ——*被冻结的校检*。此校检不分发给工作站，不从Dr.Web服务器加载新校检。校检被冻结时的操作参见推迟的更新。 存在被冻结的校检时，采用以下方式选择可分发校检： 1. 如在**当前**列有标志，则向工作站分发当前校检。 2. 如在**当前**列无标志，则向工作站分发被冻结校检之前的校检。
当前	使用标志指定用于更新工作站上的代理端和反病毒软件的产品校检。 只可标志一个当前校检。 可不标志当前校检。 另见将产品校检退回到上一版本。
应保存	使用标志指定自动清理库时应保存的校检（参见同步）。 可同时标志多个校检。 也可不为任何校检进行标志。 如产品某校检运行稳定，需将其标志为应保存。如从GUS下载的新校检不稳定时，可以返回到前一校检。
应保持校检	自动标记确定此校检中的组件安装于工作站，且限制更新（在更新限制勾选了**只更新库**或**禁止所有更新**）。 此校检在自动清理库时不会被删除，可用于重新安装工作站出错组件或安装补充组件。

列名称	内容描述
校检	获取产品校检的日期。 如校检被冻结，则此列出现阻止状态。

将产品校检退回到上一版本

是否可以将工作站上安装的产品退回到之前的版本分以下情况：

- 带组件库（病毒库、SpIDer Gate库、反垃圾邮件库、Dr.Web Agent for Android库）的产品都可以退回到上一版本。
- 将Windows操作系统的Dr.Web代理端退回到早期版本必须在更新限制部分允许**允许过渡到早期版本**。

> 将Windows代理端版本退回到上一校检（用于安装到代理端版本更早的工作站），将强制重启工作站，时间间隔为5分钟，无法更改时间间隔或取消重启。工作站会出现弹出窗口通知用户会重启。

- 其它产品（如应用程序监控组件的可信任的应用程序）退回到上一版本需要在更新限制部分勾选**获取最新更新**，因为会返回到库详细配置中标志位**当前**的校检。其他情况下不会退回到上一版本，Dr.Web服务器会等待更新的校检。

10.11.4.2. 同步

在**同步**标签设置从GUS更新Dr.Web服务器库的参数。

- 在**临时保存的校检数量**一栏指定临时保存在磁盘的产品校检数量，此数量不计在**校检列表**标签有标志的校检。如接收新校检时，而临时保存校检数量已达到此限值，则删除最陈旧的校检。被标志为**当前**、**保存**、**可分发校检**和**应保持校检**的校检不会被删除。

  编辑Dr.Web GUS部分时所有产品此设置都会改为统一值。
- 勾选**停用产品更新**后禁止从GUS获取此产品更新。这种情况下代理端会更新到Dr.Web服务器上的当前校检（或根据选择方式选出的可分发校检）。
- 勾选**只在接到申请时更新**后只在收到工作站更新此产品的申请时从GUS更新产品。其他情况下不从GUS加载产品更新。

  如果您使用的Dr.Web服务器接通互联网可自动从GUS获取更新，则使用此选项是不需要管理员进行其他操作：只要有工作站申请从Dr.Web服务器更新某产品后就会自动下载更新。

  如果您使用的Dr.Web服务器未接通互联网，而是手动从另一Dr.Web服务器或利用库加载器加载更新，则在安装或更新为其启用了**只在接到申请时更新**选项的产品前必须手动将这些产品加载到库中。

> 安装Dr.Web服务器版本13时或Dr.Web服务器更新至版本13后库产品用于**Android**操作系统的**Dr.Web**库、用于**UNIX**操作系统的**Dr.Web**代理端和**Dr.Web**代理服务器默认情况下只在工作站申请更新这些产品后才会更新。

- 在**使用服务器间连接分发**部分设置以下参数：

- 勾选**禁止向Dr.Web邻居服务器分发更新**后禁止使用服务器间连接传输产品。此选项不影响从GUS更新产品的设置。
- 勾选**禁止从Dr.Web邻居服务器获取更新**后禁止使用服务器间连接获取产品更新。此选项不影响从GUS更新产品的设置。

某些产品还可使用以下设置：

- 勾选**只更新以下文件**后，只从GUS获取指定文件的更新。
- 勾选**不更新以下文件**后，不从GUS获取指定文件的更新。

  指定文件需使用正则表达式。

如两个选项都已勾选，则文件筛选方式为：

1. 从产品全部文件列表筛选出**只更新以下文件**一项指定的文件。
2. 从步骤1获取的列表中删除**不更新以下文件**一项指定的文件。
3. 只从GUS更新步骤2筛选出的文件。

10.11.4.3. 通知

在**通知**标签设置库更新通知：

- 勾选**只不通知以下文件**后，只对此项下表指定文件的相关事件不发送通知。
- 勾选**通知以下文件**后，只是此项下表指定的文件更新后才发送通知。

  指定文件需使用正则表达式。

如未做限制，则发送通知配置页面启用的所有通知。

库更新通知参数设置在通知配置页面的**库**部分。

10.11.4.4. 推迟的更新

在**推迟的更新**标签可推迟一段时间再向工作站分发更新。推迟的校检为冻结的校检。

如需暂时取消将最新校检分发给反病毒网络所有工作站时可使用冻结更新的功能，例如需在个别工作站首先测试此校检时。



切换版本时不建议启用冻结校检的功能。取消冻结后工作站反病毒软件包更新可能会出现问题。

使用推迟更新功能

1. 为需要冻结的产品按照以下介绍的方式设置推迟的更新。
2. 取消分发最新更新，需在校检列表将一个之前的校检标志位当前校检。
3. 为应获得最新校检的工作站组在**反病毒网络** → 工作站更新限制勾选**获取最新更新**。其他工作站将只获取在第二步标志的当前校检。
4. 下一次符合**只推迟以下文件的更新**一项的从GUS加载的校检将会被冻结，推迟到在**更新延迟时间**列表设定的时间。

设置推迟更新

1. 勾选**推迟更新**，暂时取消从GUS获取此产品的更新。
2. 在**更新延迟时间**下拉列表选择推迟加载更新的时间，以从GUS服务器获取更新的时间为起始时间。
3. 如需可勾选**只推迟以下文件的更新**，推迟符合下表所列通配符的文件的更新。指定通配符需使用正则表达式。

   如不更新此项，则冻结所有从GUS接收的更新。

取消冻结

- 在**校检列表**点击**立即执行**，取消冻结，将此校检列入按常规流程分发到工作站的校检列表。
- 在**校检列表**点击**取消更新**，取消冻结并禁用此校检。恢复从GUS获取更新。取消冻结的校检从产品列表删除，接收到下一校检时此校检会从磁盘删除。
- 如对冻结产品未进行解冻操作，则**更新延迟时间**一到，校检会自动解冻并列入按常规流程分发到工作站的校检列表。

在推迟的更新部分可对所有产品被冻结的校检进行管理。

10.11.5. 库内容

库内容部分用于查看和管理库中文件和文件夹的当前内容。

库内容主窗口为库内容树结构，包含当前版本库的所有目录和文件，以及每一产品所有校检列表。

查看库信息

查看库对象，需在库内容树结构选择相应对象。打开的属性面板包含以下信息：

- 在**所选对象**列出的是树结构所选对象详细信息：**类型**、**大小**（只限文件）、**创建日期**和**更改日期**。
- 在**库状态**列出的是库中所有对象整体信息：对象当前列表和上次更新日期。

库的管理

使用工具面板的下列按钮管理库内容：

将库文件导出存档，

导入库存档文件，

删除所选对象——删除库树结构中所选对象，删除后不可恢复。

> 更改库内容，如删除或导入库对象后，需重启库，以便Dr.Web服务器能够使用更改后的数据。

参见库状态。

导出库

将库文件保存为zip存档

- 将库整体存档需在工具面板点击**将库文件导出存档 → 库中所有内容**。点击后会将库整个导出，不论树结构中选择的是哪一对象。
- 只将所有产品最新校检存档需在工具面板点击**将库文件导出存档 → 所有产品的最近一次校检**。
- 只将库中所有配置文件存档需在工具面板点击**将库文件导出存档 → 配置文件**。点击后会导出位于库和所有产品根目录的所有文件。
- 只将库中个别对象存档需先利用CTRL或SHIFT键在树结构选择相应对象，然后在工具面板点击**将库文件导出存档 → 已选对象**。

数据较大时导出用时可能会超过一个对话期。如对话到期前未能完成导出，则会自动终止进程，并不会生成所要导出数据的压缩文件。

导出库对象是需注意其基本类型：

a) 库从Zip压缩文件。此类压缩文件含以下一种类型的库对象：
   - 整个库。
   - 整个一个产品。
   - 一个产品的一个完整校检。

   导出对象获得的压缩文件可利用**库内容**导入。此类压缩文件名称包含前缀`repository_`。

b) 库单独文件的Zip压缩文件。

   导出树结构低于**a)**对象的文件和目录而获得的压缩文件不能利用**库内容**导入。此类压缩文件包含前缀`files_`。

   此类压缩文件可作为文件备份，用于手动更换。但不建议不通过**库内容**而进行手动更换。

导入库

从zip存档加载库文件

1. 点击工具面板的**导入库存档文件**。
2. 在打开窗口的**选择文件**部分使用按钮指定库文件的zip存档。

   只可导出以下一种类型的库对象时获得的zip存档：
   - 整个库。
   - 整个一个产品。
   - 一个产品的一个完整校检。

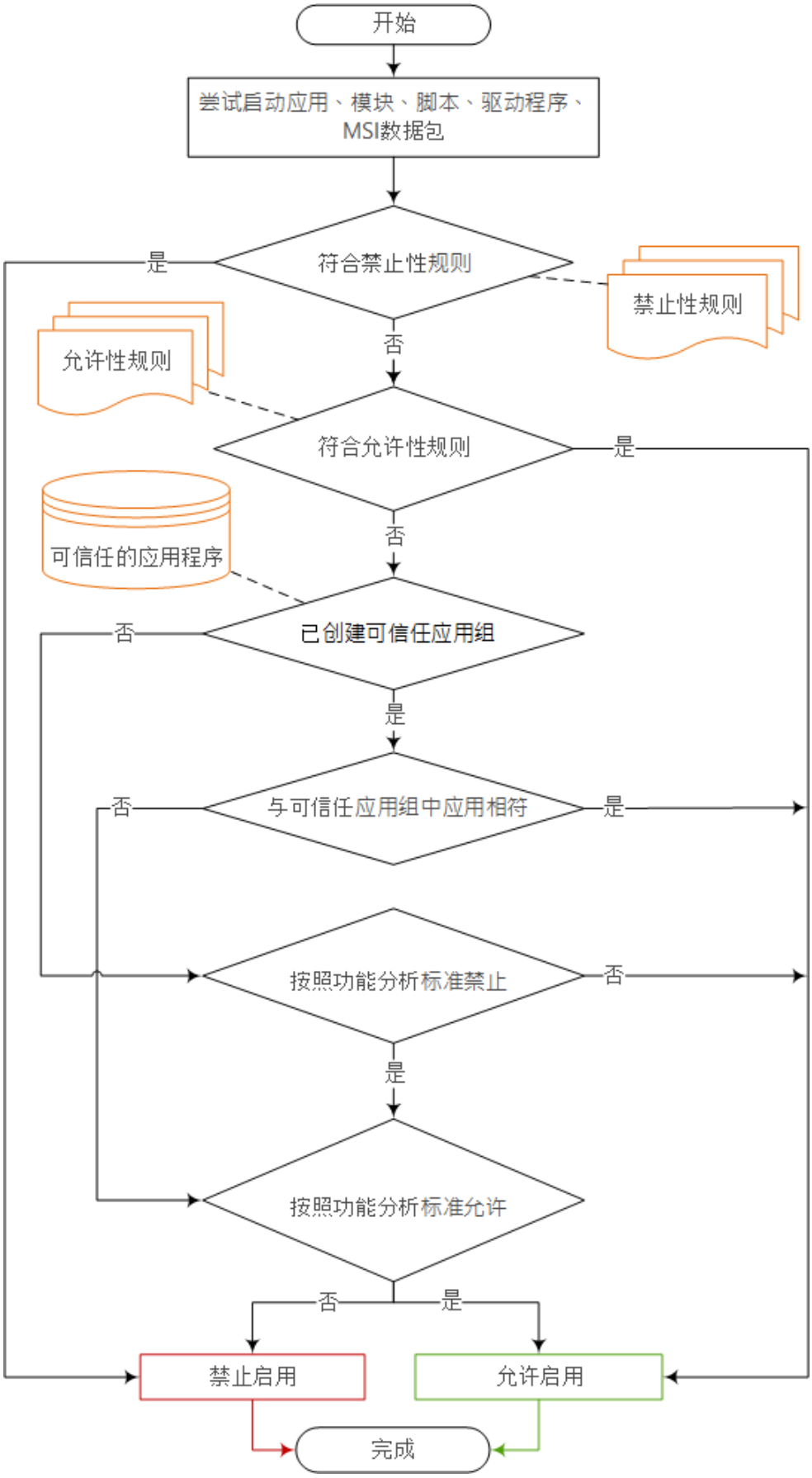
   此类压缩文件导出时名称包含前缀`repository_`。

3. 在**导入设置**部分设定以下参数：
   - **只添加空缺的校检**——此导入模式下只加载当前版本空缺的库校检。其他不做更改。
   - **更换整个库**——此导入模式下将当前库整个替换为导入的库。
   - 勾选**导入配置文件**后将在导入库时同时导入配置文件。
4. 点击**导入**开始导入过程。

10.12. 应用程序监控

利用应用程序监控可设置反病毒网络中安装有Dr.Web for Windows代理端的受保护工作站上允许使用和禁止使用的应用、模块、脚本编译器、驱动程序和MSI数据包。

应用程序监控运行方式见下。



应用程序监控的主要工具：

- 模式——规则列表，确定工作站上允许使用和禁止使用的应用。模式由管理员创建并指定给策略、工作站或用户，包括工作站组和用户组。模式决定应用程序监控的运行模式。

  设置模式需利用**反病毒网络**的网络树结构。
- 应用程序列表：
  - 可信任的应用程序——应用程序列表，根据指定规则列出并按管理员允许从工作站收集。在允许模式下此列表的应用均可使用。每一模式设置中可选择列表中不同的应用组。
  - 应用程序手册——已安装到受保护工作站的所有应用程序列表。在背景模式下自动生成，管理员无法更改。

  可通过**管理**部分设置应用列表。
- 应用程序监控事件——为应用程序监控组件在工作站发现的事件的统计信息。

  可在**反病毒网络→统计信息**部分查看应用程序监控事件。

应用程序监控基本运行模式：

- *功能分析*——预设规则集，根据规则允许或禁止应用启动执行相应功能。
- *允许性方式*——意味着在所有受监控的工作站只允许启动**可信任的应用程序**列表中的应用和符合允许规则的应用。其他应用都会被禁止。
- *禁止性方式*——意味着在所有受监控的工作站只禁止启动符合禁止规则的应用。其他应用都允许使用。



可同时启用或停用允许性方式和禁止性方式，也可单独启用或停用。

功能分析应一直处于启用状态。如停用功能分析的所有规则，将停止对应用程序的监控。

设置应用程序监控

1. 创建新模式。
2. 指定工作站、用户和组，新创建的模式的设置将应用到这些对象。
3. 指定模式设置。



建议在测试模式下设置模式。

10.12.1. 测试模式

可利用*测试模式*来确认一下设置的模式或规则的运行能力，在这种模式下会模拟应用程序监控的运行。不会实际阻止应用，但会模拟模式或规则实际使用情况并记录日志（见应用程序监控事件）。

启用模式测试的操作

1. 在模式属性的**常规**部分勾选**启用模式**后开始使用此模式。
2. 勾选**将模式设为全面测试**。
3. 点击**保存**。

测试状态下反病毒网络树结构**Profiles**组中相应的模式的图标会是。在指定了此模式的工作站不会按照模式中的功能分析标准、允许性和禁止性规则阻止应用的启动，但会在**反病毒网络 → 统计信息 → 应用程序监控事件**收集统计信息。这一日志中会显示每一启动的应用的详细信息，进行分析后可以对模式进行修改。

确信测试的模式符合要求后需将测试状态改为实际使用状态。活跃状态下反病毒网络树结构**Profiles**组中相应的模式的图标会是。

停用模式测试的操作

1. 在模式属性的**常规**部分取消对**将模式设为全面测试**的勾选。
2. 点击**保存**。

测试模式也可以用于检验模式中单独的允许性和禁止性规则，而且不需要将模式全部转为测试状态。

启用对模式中单独的允许性和禁止性规则的测试的操作

1. 在模式属性的**允许性规则**或**禁止性规则**选择需要测试的规则。
2. 在打开的规则设置勾选**启用规则**和**将规则设为测试状态**。
3. 点击**保存**。

这时工作站应用将会*被阻止*，但知识按照模式中的功能分析标准以及没有设为测试状态的允许性和禁止性规则来进行阻止。而设为测试状态的允许性和禁止性规则与模式为测试状态时一样，运行结果会记录到**应用程序监控事件**部分的运行日志。



与整个模式为测试状态时不同，有个别规则处于测试状态不会影响模式在反病毒网络树结构的图标显示。有个别规则处于测试状态的活跃模式的图标为。

确信测试的规则符合要求后需将测试状态改为实际使用状态。

停用对模式中单独的允许性和禁止性规则的测试的操作

1. 在模式属性的**允许性规则**或**禁止性规则**选择测试中的规则。
2. 在打开的规则设置取消对**将规则设为测试状态**的勾选。
3. 点击**保存**。

10.12.2. 可信任的应用程序

管理可信任应用程序

可信任的应用程序组（或应用程序白名单）是按照指定标准从所选工作站或工作站组收集的应用程序列表。此应用程序监控模式指定为允许方式的反病毒网络工作站上可以启动这些应用。

为形成可信任应用程序组收集信息是一个占用资源较大的过程，受标准设置的影响，可能会造成计算机运行缓慢。为减少反病毒网络工作站负载进行信息收集可以只选择一个或几个*标准工作站*——也就是专门为此目的选择工作站。最好选择的是刚安装完操作系统、最新更新和所有必要软件的工作站。

管理可信任的应用程序需在负责收集信息的Dr.Web服务器打开**管理** → **应用程序监控** → **可信任的应用程序**。

打开列表是所有可信任的应用程序组。

在工具面板可使用以下按钮：

➕创建可信任的应用程序组

重新创建可信任的应用程序组

删除可信任的应用程序组

创建新的可信任的应用程序组

1. 在**可信任的应用程序**部分的工具面板点击➕**创建可信任的应用程序组**。
2. 在**常规**窗口指定以下设置：
   - **组名称**——新创建的可信任的应用程序组的名称。
   - **描述**——新创建的组的自定义描述，非必填项。

   点击**下一步**。
3. 在**添加将应用添加到可信任列表的参数**给出设置，工作站应用将根据这些设置添加到新创建的可信任的应用程序组（每一标准一个至少选择一个设置）。

   如可信任应用程序组的信息收集需要在系统资源不能完全被此任务占用的计算机进行，需勾选**为信息收集进程设置低优先级**。

   > 启用此参数可以节省信息收集对计算机资源的消耗，但会大大增加完成信息收集需占用的时间。

   - **搜索区域**——勾选收集应用信息依据的区域。

     > 在**按指定路径搜索**一项可指定多个路径用于搜索应用。不同路径用";"隔开。

   - **可添加哈希值类型**——勾选其哈希值将添加到新创建的可信任的应用程序组的对象。
   - **文件种类**——勾选搜索时需考虑的文件。

点击下一步。

4. 在网络树结构选择收集应用信息并添加到可信任列表的工作站或工作站组。多选使用CTRL和SHIFT。

   勾选**不计内置组**后只收集所选组中工作站信息。取消勾选则收集所选组及其子组所有工作站的信息。

5. 点击**保存**按钮。
6. 开始安装指定设置在工作站收集应用信息。收集过程可能占用很长时间。

   查看可信任的应用程序组的状态和更新：

   - 在**可信任的应用程序**部分的主信息表，
   - 在**可信任的应用程序**部分的主信息表点击组对应的行后打开的组补充信息。



应用程序信息收集实在相应工作站的当前对话期间进行。如在完成信息收集前工作站关闭或重启，则再次启动后会重新开始，不会保存之前收集的部分信息。

更新可信任的应用程序组

1. 在**可信任的应用程序**列表勾选需要更新的应用程序组。
2. 在工具面板点击**重新创建可信任的应用程序组**。

删除可信任的应用程序组

1. 在**可信任的应用程序**列表勾选需要删除的应用程序组。
2. 在工具面板点击**删除可信任的应用程序组**。
3. 此组应用会从工作站允许启动的应用列表中删除，并停止安装此组设置收集可信任的应用程序。



不可删除指定为应用程序监控模式的可信任应用程序组。

删除可信任的应用程序组时库中会创建产品**可信任的应用程序**的新校检并分发给Dr.Web邻居服务器。这可能可能导致这些Dr.Web邻居服务器上应用程序监控设置中包含此组的模式的运行出现问题。

从可信任应用程序组删除某个工作站的应用的相关信息

1. 在**可信任的应用程序**列表点击需要删除的工作站应用信息行。
2. 在打开窗口的工作站列表勾选需删除其应用信息的工作站。
3. 在工具面板点击**删除所选工作站**。



删除所有工作站后可信任应用程序组将一并删除。

可信任应用程序库

为应用程序监控模式设置允许性方式时从库中对于产品**可信任的应用程序**可选的组列表中选择可信任应用程序组。

如在反病毒网络中使用多个使用服务器间连接的Dr.Web服务器，可以通过以下方式在Dr.Web服务器间分配负载来简化信息收集：

- 管理员在一个Dr.Web服务器上收集来自受保护工作站的信息。信息自动记录到Dr.Web服务器库中的产品**可信任的应用程序**，并按照指定的设置使用服务器间连接进行分发。

  可在网中多个Dr.Web服务器上收集可信任应用程序的信息，但这些Dr.Web服务器负责的网络段应相互隔绝。
- 其他Dr.Web服务器按照指定的设置使用服务器间连接获取产品**可信任的应用程序**的更新。无需在这些Dr.Web服务器设置收集可信任的应用程序信息，从邻居服务器获得的产品校检会写入库中。

产品**可信任的应用程序**不能从GUS进行更新。此产品只能使用服务器间连接在Dr.Web邻居服务器间分发。

在收集可信任的应用程序前需确定哪些Dr.Web服务器负责收集信息并分发给Dr.Web邻居服务器，哪些服务器使用服务器间连接获取信息。确定后需对每台Dr.Web服务器分别进行设置。

设置负责收集信息并分发可信任应用程序信息的**Dr.Web**服务器

1. 打开**管理**部分。
2. 打开**库详细配置** → **可信任的应用程序**。
3. 在**同步**标签取消对 **禁止向Dr.Web邻居服务器发送更新**的勾选，勾选**禁止从Dr.Web邻居服务器获取更新**。
4. 点击**保存**。
5. 打开**管理** → **应用程序监控** → **可信任的应用程序**后按照以下介绍设置收集可信任的应用程序。
6. 在从收集可信任的应用程序组设置中指定的所有工作站获取信息后库中写入产品**可信任的应用程序**的新校检。写入后使用服务器间连接分发给Dr.Web邻居服务器。

设置接收可信任应用程序信息的**Dr.Web**服务器

1. 打开**管理**部分。
2. 打开**库详细配置** → **可信任的应用程序**。
3. 在**同步**标签取消对 **禁止从Dr.Web邻居服务器获取更新**的勾选。

   如果Dr.Web服务器须使用服务器间连接产品**可信任的应用程序**分发给其他Dr.Web邻居服务器，还需取消对 **禁止向Dr.Web邻居服务器发送更新**的勾选。
4. 点击**保存**。

10.12.3. 应用程序手册

查看应用程序手册需打开**管理** → **应用程序监控** → **应用程序手册**。

应用程序手册包含连接Dr.Web服务器的OS Windows受保护工作站上安装的所有应用程序的信息。

应用程序手册在背景模式下自动生成，管理员无法更改。应用程序首次使用时代理端会将其信息发送到Dr.Web服务器。

以下情况使用手册：

- 获取网络中工作站已安装应用信息。
- 用于创建禁止性和允许性规则。使用手册可简化规则创建过程，所有已知应用的相关信息都会自动填写。

填写应用程序手册

激活从工作站向应用程序手册发送信息

1. 在**反病毒网络**树结构选择安装有应用程序监控并需要收集其应用程序信息的工作站或工作站组。
2. 在控制菜单选择**Windows** → **Dr.Web代理端**一项。
3. 在**常规**标签勾选**追踪应用程序监控事件**，勾选后追踪应用程序监控组件在工作站记录到的所有进程活动，并将事件信息发送至Dr.Web服务器。未与服务器连接时会积累事件记录并在建立连接后发送。如取消勾选，则可能只发送阻止事件（取决于服务器配置中的设置）。
4. 点击**保存**。

激活Dr.Web服务器为应用程序手册收集信息

1. 打开**管理** → **Dr.Web服务器配置**。
2. 打开**统计信息**，选择下面一个选项：
   - **应用程序监控按照进程活动性的统计信息**，此项用于获取和记录所有进程的任何活动：既包括应用程序监控允许的进程，也包括禁止的基础。选择此项后手册会记录应用程序，前提是创建和指定了至少一个模式，包含功能分析依据的标准的一个或几个类型。在创建模式并将其指定给反病毒网络工作站前，允许启动所有应用程序。
   - **应用程序监控按照被阻止进程的统计信息**，此项用于获取和记录应用程序监控禁止启动所有进程的活动。选择此项后手册只在创建阻止应用启动的模式并将其指定给反病毒网络工作站后开始记录应用程序。

   > **应用程序监控按照进程活动性的统计信息**会大大增加整个反病毒网络信息收集的总量。

3. 点击**保存**按钮。
4. 请重启Dr.Web服务器。

5. 重启Dr.Web服务器后开始按照指定的设置记录从安装有应用程序监控的工作站发送来的应用程序启动统计信息。

利用应用程序手册创建规则

根据应用程序手册中的数据创建新规则

1. 在**应用程序手册**选择为其创建启动监控规则的应用的信息行：
2. 点击信息行就会打开所选应用信息窗口。
3. 点击**创建规则**。
4. 打开新规则创建窗口。给出以下设置：
   a) 在**模式名称**下拉列表选择为其创建新规则的应用程序监控模式。
   b) 在**规则名称**指定所创建的规则的名称。
   c) 在**规则类型**选择所创建规则的类型：禁止性或允许性。
   d) 在**运行状态**选择所创建规则的运行状态（与从模式创建规则时**将规则转为测试状态**选项相符）。
   如需检查规则的运行情况，需选择**测试**状态。此状态下不会在工作站监控应用，但会和启用规则一样记录事件日志。规则测试模式下对应用的启动和阻止结果会体现于应用程序监控事件。
   在**活跃**模式下按照规则在工作中阻止应用（参见模式运行模式）。
   e) 在**按下列标准禁止应用程序启动/按下列标准允许应用程序启动**（取决于在4c一步选择的规则类型）部分会自动填写应用程序信息。如需可编辑设置。
5. 点击**保存**。新规则会添加到指定的应用程序监控模式。

10.13. 补充功能

10.13.1. 数据库管理

数据库管理部分用于直接维护Dr.Web服务器使用的数据库。

常规包含以下参数：

- **上次数据库维护**——利用此选项上次启动维护数据库指令的日期。
- 数据库维护指令列表，包含：
  - 指令与Dr.Web服务器日程的任务相同。指令名称对应Dr.Web服务器日程**操作**部分任务的名称（相应任务介绍见表任务类型及其参数）。
  - 指令**数据库分析**。通过执行指令`analyze`优化Dr.Web服务器数据库。
  - 指令**清空未激活的工作站**。此指令用于删除在反病毒网络创建但从未连接Dr.Web服务器的工作站。需指定期限，期限到后会删除未使用的账户。
  可在反病毒网络分层列表的**Status → New**查看未使用的工作站账户列表。

执行服务器维护指令

1. 在指令列表勾选需执行的指令。

如需可更改清空数据库指令的时间间隔，指定时间到期后之前保存的信息会从Dr.Web服务器删除。

2. 点击**现在应用**。会立即执行所选指令。

   可使用Dr.Web服务器任务计划器推迟和/或定期自动执行指令（指令**数据库分析**除外）。

管理数据库可使用工具面板的下列按钮：

 导入，

 导出。

导出数据库

从数据库保存信息

1. 在工具面板点击 **导出**。
2. 在导出设置窗口请选择一种方式：
   - **导出整个数据库**是将数据库的所有信息保存为gz存档。导出获得的XML文件与从命令行使用`modexecdb database-export-xml`启动Dr.Web服务器执行文件时获得的数据库导出文件相同。 此文件可在从命令行使用`modexecdb database-import`启动Dr.Web服务器执行文件时导入。
     指令详细介绍参见**附录**中的H3.3.数据库管理命令。
   - **导出工作站和组信息**是将反病毒网络对象信息保存为zip存档。执行此操作后专门格式文件中将保存此Dr.Web服务器所服务的反病毒网络中工作站组和工作站账户的所有信息。导出的文件包含工作站以下信息：属性、组件配置、权限、更新限制设置、日程、可安装组件列表、统计信息、已删除工作站信息；包含组以下信息：属性、组件配置、权限、更新限制设置、日程、可安装组件列表、父组识别码。
     之后导出的文件可通过**数据库管理**导入。
     - 可在**反病毒网络**树结构选择一个或几个用户组。这时只导出所选组以及所选组为基组的工作站的信息。如未选择任何组，则导出反病毒网络所有用户组和所有工作站的信息。
3. 点击**导出**按钮。
4. 根据打开管理中心的浏览器设置指定数据库压缩文件保存路径。



数据较大时导出用时可能会超过一个对话期。如对话到期前未能完成导出，则会自动终止进程，并不会生成所要导出数据的文件。

导入数据库

包含反病毒网络对象信息的数据库文件可导入新Dr.Web服务器，也可导入已在反病毒网络运行的Dr.Web服务器，例如用于合并两个Dr.Web服务器的下属工作站。



工作站在其信息导入后均可连接到Dr.Web服务器。在进行导入时需注意授权允许的数量。如需可在授权管理器添加原Dr.Web服务器的授权密钥。

从文件加载数据库

1. 在工具面板点击导入。
2. 在打开的导入窗口指定数据库zip存档文件。选择文件可使用按钮。
   只可导入执行**导出工作站和组信息**时获得的zip存档。
3. 点击**导入**开始导入过程。
4. 导入时如发现有的工作站或组的识别码和当前Dr.Web服务器数据库记录的识别码相同，会打开**冲突**窗口，需指定对重复对象的操作。
   组和工作站各为一个列表。
   在相应列表的**组导入模式**或**工作站导入模式**下拉报表选择解决冲突的方式：
   - **全部保存导入数据**——从当前Dr.Web服务器数据库删除所有重复信息，写入导入的数据库的信息。此操作应用于相应列表的所有重复对象。
   - **全部保存当前数据**——保存当前Dr.Web服务器数据库所有重复信息，忽略导入的数据库中重复的信息。
   - **手动选择**——为每一个重复对象手动指定操作。在此模式下重复对象列表转为可编辑状态，可勾选需保存的对象。

   点击**保存**按钮。

10.13.2. Dr.Web服务器统计信息

利用管理中心可查看Dr.Web服务器运行统计信息，包括对安装Dr.Web服务器的计算机系统资源的占用，以及与反病毒网络组件和外部资源，如GUS的网络交互作用。

查看**Dr.Web**服务器运行统计信息

1. 在管理中心主菜单选择**管理**。
2. 在打开的窗口选择控制菜单中的**Dr.Web服务器统计信息**。
3. 打开的查看显示以下统计信息选项：
   - **客户端活动**——连接此Dr.Web服务器的客户端数量信息：Dr.Web代理端、Dr.Web邻居服务器和Dr.Web代理端安装程序。
   - **网络流量**——与Dr.Web服务器交换数据时进出港流量。
   - **使用系统资源**——对安装Dr.Web服务器的计算机系统资源的占用情况。
   - **Microsoft NAP**——Dr.Web NAP Validator运行参数。
   - **使用数据库**——访问Dr.Web服务器数据库的参数。
   - **使用文件缓存**——访问安装Dr.Web服务器的计算机缓存文件的参数。
   - **使用DNS缓存**——访问安装Dr.Web服务器的计算机保存DNS服务器请求缓存的参数。
   - **通知**——管理员通知子系统运行参数。
   - **库**——Dr.Web服务器库与GUS服务器数据交换参数。
   - **WEB统计信息**——向Doctor Web公司服务器发送感染统计信息的参数。
   - **Web服务器统计信息**——访问Web服务器的参数。

- **群集**——多服务器网络中使用Dr.Web服务器群集时按照服务器间同步协议进行访问的访问参数。
- 在**传递组更新**——使用multicast协议向工作站发送组更新时的数据交换参数。

4. 查看相应选项的详细信息需点击选项名称。
5. 打开的表格为数值动态显示器。
6. 打开统计信息的同时开始显示每一参数变化图形。这时：
   - 点击相应名称可以停用图形显示。停用图形显示后参数值会保持动态更新。
   - 再次点击相应名称可重新启用图形显示。
   - 能够轻易图形显示模式的选项和参数值为黑体。
7. 更改数据更新周期的操作是在工具面板**更新频率**下拉列表选择相应的时间间隔。新的时间间隔会自动应用于数字数据和图形数据。
8. 鼠标移至图形数据时出现所选点的数值，格式为：
   - **Abs**——参数绝对值。
   - **Delta**——按照更新频率相对于更新前数值的增量。
9. 点击选项左侧箭头后隐藏选项参数。隐藏参数后图形数据清空，再次打开时重新计量。

10.13.3. 备份

备份部分用于查看目录和文件，保存Dr.Web服务器重要数据本地备份。

备份时保持以下对象：库设置、配置文件、加密密钥、证书、内设数据库备份。

以下情况保存Dr.Web服务器重要数据备份：

- 按照Dr.Web服务器日程执行任务**服务器关键数据备份**。
- 从命令行使用backup启动Dr.Web服务器执行文件时进行备份。此命令介绍参见**附录**中的H3.5. Dr.Web服务器关键数据备份。

查看备份信息

查看备份信息需在分层树结构选择与所要查看的备份对应的对象。备份按照其所在目录置于树结构：默认目录（UNIX家族操作系统的Dr.Web服务器为`var/opt/drwcs/backup`，Windows操作系统的Dr.Web服务器为`C:\DrWeb Backup`）以及Dr.Web服务器日程任务重指定的保存备份的所有路径。Windows操作系统下的Dr.Web服务器如果任务中路径为空，默认将使用目录`C:\Program Files\DrWeb Server\var\backup`。

只可查看Dr.Web服务器目录内保存的备份所含信息。

选择备份目录和文件时打开属性面板，显示所选对象信息：**类型**、**大小**（只限文件）、**创建日期**和**修改日期**。

管理备份

管理备份可使用工具面板的下列按钮：

备份——建立Dr.Web服务器重要数据备份。

导出——在打开管理中心的计算机保存所选对象的备份。

删除所选对象——删除树结构中所选对象，删除后不可恢复。

导出备份

本地保存备份

1. 在树结构选择部分（选择相应目录进行全选）或备份中的个别文件。多选利用CTRL或SHIFT。

   导出库对象是需注意其基本类型：

   a) 以下对象备份为Zip压缩文件：
      - 一个或多个全部备份（如选择的是对应备份的目录）。
      - 备份中的多个文件。

   b) 备份中的多个文件。如果只选择了一个文件，则保存为原格式，不进行存档。
2. 在工具面板点击导出。
3. 根据打开管理中心的浏览器设置指定所选对象保存路径。

备份

创建Dr.Web服务器重要数据备份需点击工具面板的备份按钮。数据保存为gz存档。获得的文件与从命令行使用backup启动Dr.Web服务器执行文件时获得的文件相同。

此命令介绍参见附录中的H3.5. Dr.Web服务器关键数据备份。

10.13.4. 工具



可用工具取决于Dr.Web服务器库设置。启用或停用从GUS获取工具更新需打开管理→库常规配置→Dr.Web安装包→Dr.Web管理员工具。

工具——可加载运行Dr.Web Enterprise Security Suite所需的补充工具：

- Dr.Web库加载器

  用于从全球更新系统下载Dr.Web Enterprise Security Suite产品。Dr.Web库加载器图形版本只支持Windows操作系统。

- **Dr.Web系统信息收集工具**

  此工具用于生成系统及所有已安装软件状态报告，包括受保护工作站Dr.Web解决方案和Dr.Web服务器软件的状态。此报告供反病毒网络管理员进行诊断，或提交给Doctor Web公司技术支持。

- 数字密钥和证书生成工具

  可生成加密密钥和数字证书，还可以进行文件数字签名或检查数字签名。此工具是保证反病毒网络各组件间连接安全的重要工具。

- **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。另参阅远程访问Dr.Web服务器。

- **Dr.Web服务器脚本运行远程诊断工具**

  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。此工具版本用于作为脚本使用。另参阅远程访问Dr.Web服务器。

- **Dr.Web for Windows删除工具**

  用于无法使用常规工具删除非正常安装 / 受损的Dr.Web for Windows代理端时进行删除。不适用于一般情况下正常卸载Dr.Web软件。

- 用于**UNIX**操作系统的**Dr.Web**代理端的远程安装工具

  此工具的功能是将Dr.Web代理端远程安装到UNIX家族操作系统的工作站。

- 用于**Windows**操作系统的**Dr.Web**代理端远程安装工具

  此工具的功能是将Dr.Web代理端远程安装到Windows操作系统的工作站。

- **Dr.Web移动管理中心**

  用于管理使用Dr.Web Enterprise Security Suite构建的反病毒网络。可在iOS和安卓移动设备安装运行。

> 了解运行工具是命令行参数相关信息请查阅附录的**H7.** 工具。

10.13.5. 企业产品

> 可用产品取决于Dr.Web服务器库设置。启用或停用从GUS获取产品更新需打开管理→库常规配置→**Dr.Web**安装包→ Dr.Web企业产品。

在企业产品部分可以加载Dr.WebEnterprise Security Suite反病毒网络所使用的一系列软件的安装包：

- **Dr.Web for Android**

  用于将Dr.Web Agent for Android安装到受保护工作站的数据包。

- **Dr.Web for IBM Lotus Domino**

  用于将Dr.Web для IBM Lotus Domino安装到公司邮件服务器的数据包。

- **Dr.Web for Linux**

  用于将Dr.Web for Linux代理端安装到受保护工作站的数据包。

- **Dr.Web for macOS**

  用于将Dr.Web для macOS安装到受保护工作站的数据包。

- **Dr.Web for Microsoft Exchange Server**

  用于将Dr.Web for Microsoft Exchange Server安装到公司邮件服务器的数据包。

- **Dr.Web for UNIX Internet gateways**

  用于将Dr.Web for UNIX Internet gateways安装到公司网关或代理服务器的数据包。

- **Dr.Web for UNIX mail servers**

  用于将Dr.Web for UNIX mail servers安装到公司邮件服务器的数据包。

- **Dr.Web for UNIX file servers**

  用于将Dr.Web for UNIX file servers安装到公司邮件服务器的数据包。

- **Dr.Web代理服务器**

  用于将Dr.Web代理服务器安装到公司反病毒网络作为代理服务器的计算机的数据包。

- **Dr.Web扫描服务器**

  Dr.Web扫描服务器安装包，此组件用于处理虚拟环境下虚拟机的扫描申请。

- **Dr.Web NAP Validator**

  用于将Dr.Web NAP Validator安装到公司反病毒网络作为网络访问保护服务器的计算机的数据包。

- 用于**Active Directory**的**Dr.Web**代理端

  使用Active Directory服务时的Dr.Web代理端安装工具。

- **Dr.Web**代理端完整安装程序

  用于将Dr.Web for Windows代理端和反病毒保护软件包安装到受保护工作站的数据包。

- **Active Directory对象参数更改工具**

  使用Active Directory服务登录时用于编辑对象属性的工具。

- **Active Directory架构更改工具**

  使用Active Directory服务登录时用于创建新的对象等级并描述其属性的工具。

10.14. 多台Dr.Web服务器网络特点

Dr.Web Enterprise Security Suite允许部署有多台Dr.Web服务器的反病毒网络。在多服务器网络每个工作站只连接一个Dr.Web服务器，所以可分配服务器负载。

Dr.Web服务器间的连接可以为分层结构，从而达到Dr.Web服务器负载的最优分配。

Dr.Web服务器间的信息交换使用专门的*跨服务器同步协议*。

使用跨服务器同步协议可以：

- 在反病毒网络内的Dr.Web服务器间传播更新。
- 从Dr.Web GUS获取更新后可及时进行传递。
- 在Dr.Web邻居服务器间传递受保护工作站状态统计信息。
- 在Dr.Web邻居服务器间传递受保护工作站授权。

10.14.1. 部署多台Dr.Web服务器网络

在反病毒网络可安装多台Dr.Web服务器。这时每个Dr.Web代理端只连接其中一个Dr.Web服务器。每个Dr.Web服务器同与其相连接的工作站构成一个小的反病毒网络（相关描述见前面的章节）。

Dr.Web Enterprise Security Suite可以进行Dr.Web服务器间的信息传递，从而将这些小反病毒网络连成一体。

Dr.Web服务器可向另一 Dr.Web服务器传递：

- 软件和病毒库更新。只有一个服务器从Dr.Web GUS服务器获取更新。
- 病毒事件信息、运行统计信息等等。
- 受保护工作站授权（在Dr.Web服务器间的授权传递在授权管理器设置）。

Dr.Web Enterprise Security Suite分两种Dr.Web服务器间连接类型：

- *主服务器-子服务器连接类型*，主服务器向子服务器传递更新，从子服务器获得事件信息；
- *同级服务器连接类型*，这时信息传递方向和类型都单独设置。

图10-1为多Dr.Web服务器网络结构示例。

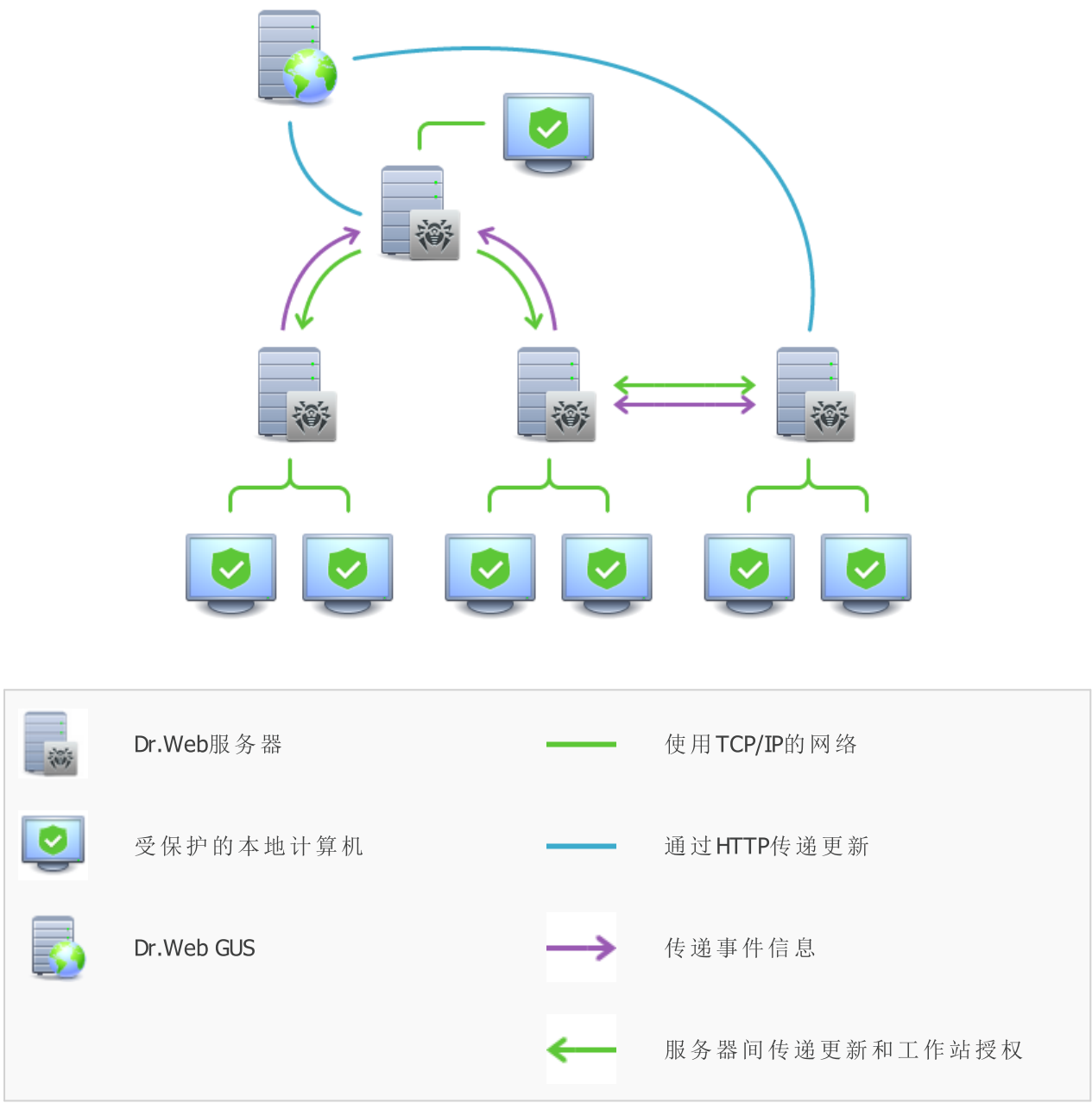


图**10-1.** 多**Dr.Web**服务器网络

多**Dr.Web**服务器反病毒网络的优势包括：

1. 利用一个Dr.Web服务器从Dr.Web GUS服务器获取更新，然后将更新直接或通过中间环节传递给其它Dr.Web服务器。

   Dr.Web服务器如从上一级Dr.Web服务器接收更新，则不从GUS进行更新，即便是日程中设有此任务。

   建议在Dr.Web子服务器日程中添加从GUS服务器获取更新的任务，这样可以保证如Dr.Web主服务器暂时无法访问，连接Dr.Web子服务器的代理端可以获得病毒库和软件模块更新（参见库常规配置）。

在分发更新的Dr.Web主服务器设置从GUS进行更新时必须指定获取针对从此Dr.Web主服务器更新的所有Dr.Web子服务器的操作系统的服务器端软件（参见库常规配置）。

2. 可将工作站分配给几个Dr.Web服务器，从而减小每个服务器的负载。
3. 将从几个Dr.Web服务器收集的信息集中到一个服务器上，可通过管理中心在一次对话过程中获取这台Dr.Web服务器上的综合信息。

Dr.Web Enterprise Security Suite自行监控信息传递，不会出现信息循环传递的问题。

4. 可将未使用的工作站保护授权分发给Dr.Web邻居服务器。这时授权密钥仍归分发授权的Dr.Web服务器支配，分发给Dr.Web邻居服务器的授权有一定使用期限，到期后将被调回。

10.14.2. 设置Dr.Web服务器间连接

使用多个Dr.Web服务器必须对这些服务器间的连接进行设置。

建议预先进行反病毒网络规划，做好结构图，在图中标明计划信息流向，确定同级服务器间应采取的连接类型和"主-子"服务器间应采取的连接类型。之后必须为网络中的每一台Dr.Web服务器设置与Dr.Web"邻居"服务器的连接（只要有信息流相连就是Dr.Web"邻居"服务器）。

存在与其他Dr.Web服务器的服务器间连接时注册管理员用户名主菜单会增加新功能。

Dr.Web主服务器与下属服务器连接设置举例：

有*标志的输入栏必须填写。

1. 首先确认两台Dr.Web服务器都正常运行。
2. 为每一个Dr.Web服务器指定容易区分的名称，以避免设置Dr.Web服务器连接时和今后进行管理时出错。操作是在管理中心菜单的**管理** → **Dr.Web服务器配置** **常规**标签的**名称**一项。此示例中Dr.Web主服务器名称为MAIN，子服务器名称为AUXILIARY。

设置时给出的名称在Dr.Web服务器按照设置建立连接后会自动更换为计算机名称。

3. 在两个Dr.Web服务器都启用服务器协议。操作是进入管理中心 菜单**管理** → **Dr.Web服务器配置**的**模块**标签，勾选**Dr.Web服务器协议**（参见模块）。
4. 重启两个Dr.Web服务器。
5. 利用Dr.Web子服务器管理中心（AUXILIARY）将Dr.Web主服务器（MAIN）添加到Dr.Web邻居服务器列表。

   操作是在主菜单选择**反病毒网络**。打开反病毒网络分层列表。添加Dr.Web邻居服务器需点击工具面板的**添加网络对象**→**创建邻居**。

   打开当前和要添加的Dr.Web服务器连接设置窗口。需给出以下参数：

- 要建立的连接**类型**——**主**。
- **名称**——Dr.Web主服务器名称（MAIN）。
- **密码***——登录Dr.Web主服务器的自定义密码。
- **Dr.Web服务器自身证书**——需设置的Dr.Web服务器的SSL证书列表。点击后选择与当前Dr.Web服务器对应的证书drwcsd-certificate.pem。添加证书需点击后将证书填入新栏。
- **Dr.Web邻居服务器证书***——需连接的Dr.Web主服务器的SSL证书列表。点击后选择与Dr.Web主服务器对应的证书drwcsd-certificate.pem。添加证书需点击后将证书填入新栏。
- **地址***——Dr.Web主服务器网络地址和连接端口。格式为*<Dr.Web服务器地址>*:*<端口>*。

可搜索网络中可访问的Dr.Web服务器列表，操作是：

a) 点击**地址**栏右侧的箭头。

b) 在打开的出口指定网络名单，格式为：使用连字符（如10.4.0.1-10.4.0.10），使用逗号和空格（如10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90），使用网络前缀（如10.4.0.0/24）。

c) 点击按钮。开始浏览网络搜索可访问的Dr.Web服务器。

d) 在可访问Dr.Web服务器列表选择一个Dr.Web服务器。此服务器的地址将写入**地址**栏，用于创建连接。

- **Dr.Web安全管理中心地址**——可指定为Dr.Web主服务器管理中心的首页地址（参见Dr.Web安全管理中心）。
- 在**连接参数**下拉列表指定Dr.Web服务器连接原则。
- 在**加密**和**压缩**下拉列表选择要连接的Dr.Web服务器间流量的加密和压缩模式（参数使用流量的加密和压缩）。
- **给出的密钥自动延期期限**——从此Dr.Web服务器密钥给出的密钥的有效期。到期后对给出的密钥进行相同期限的自动延期。给出的授权分发期内会重复自动延期。使用此设置的前提是由Dr.Web主服务器向当前Dr.Web服务器分发授权。
- **接收的授权延期期限间隔**——设置与Dr.Web主服务器的连接前不使用此设置。
- **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。
- **授权**、**更新**和**事件**中的勾选按照*主-子*连接原则设定，不可进行更改：
  - Dr.Web主服务器发送授权给Dr.Web子服务器；
  - Dr.Web主服务器发送更新给Dr.Web子服务器；
  - Dr.Web主服务器从Dr.Web子服务器接收事件信息。
- 设置管理员接收通知：
  - 勾选**发送Dr.Web邻居服务器事件通知**后会向管理员发送从所设置的Dr.Web邻居服务器接收的事件的通知。如取消勾选，管理员将只会收到自己的Dr.Web服务器的事件通知。可在通知配置设置发送具体类型的通知。
  - 勾选**根据已知威胁哈希值侦测到威胁时发送Dr.Web邻居服务器事件通知**后会在根据已知威胁哈希值侦测到威胁时向管理员发送从所设置的Dr.Web邻居服务器接收的事件的通知。如取消勾选，管理员将只会收到自己的Dr.Web服务器的事件通知。可在通知配置设置发送具体类型的通知。
    此选项可以使用的前提是已授权使用已知威胁哈希值公报。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**（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）。

- 勾选**利用服务器间连接同步工作站硬软件信息**后在接通的工作站收集的硬软件信息以及安装的OS Windows补丁的相关信息会发送给要设置的Dr.Web子服务器。创建邻居连接并接通Dr.Web主服务器后即会发送，并在工作站硬软件发生变化时进行更新。
  此统计信息只从安装有用于Windows操作系统的Dr.Web代理端的工作站收集，前提是按照Windows操作系统工作站的硬软件配置部分的描述在Dr.Web服务器和代理端配置中启用了相应选项。

启用这些选项后可能会大大增加通知的数量。

设置同级Dr.Web服务器时可访问这些选项的前提是在**事件**部分勾选了**接收**。

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**。

根据已知威胁哈希值发现安全威胁时Dr.Web邻居服务器事件通知区分为：**根据已知威胁哈希值发现安全威胁**、**根据已知威胁哈希值侦测威胁时扫描出错**、**预防性保护根据已知威胁哈希值侦测威胁报告**。

- 在**更新限制→事件**可设定从当前Dr.Web服务器向主服务器发送事件的日程（编辑**更新限制**列表与编辑工作站更新限制部分的日程列表相同）。

点击**保存**按钮。

Dr.Web主服务器（MAIN）移至文件夹**Parents**和**Offline**（见图.10-2）。

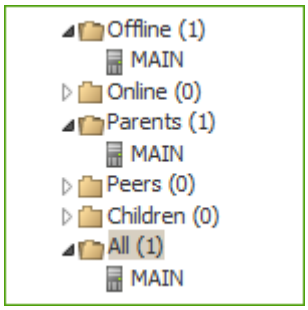


图 **10-2.**

6. 打开Dr.Web主服务器管理中心（MAIN）后将Dr.Web子服务器（AUXILIARY）添加到Dr.Web邻居服务器列表。

   操作是在主菜单选择**反病毒网络**。打开反病毒网络分层列表。添加Dr.Web邻居服务器需点击工具面板的**添加网络对象→** **创建邻居**。

   打开当前和要添加的Dr.Web服务器连接设置窗口。需给出以下参数：

   - 要建立的连接**类型**——**子**。
   - **名称**——Dr.Web子服务器名称（AUXILIARY）。
   - **密码***——输入步骤**5**指定的密码。
   - **Dr.Web服务器自身证书**——需设置的Dr.Web服务器的SSL证书列表。点击后选择与当前Dr.Web服务器对应的证书drwcsd-certificate.pem。添加证书需点击后将证书填入新栏。

- **Dr.Web邻居服务器证书***——需连接的Dr.Web子服务器的SSL证书列表。点击后选择与Dr.Web子服务器对应的证书drwcsd-certificate.pem。添加证书需点击后将证书填入新栏。
- **Dr.Web安全管理中心地址**——Dr.Web子服务器管理中心的首页地址（参见Dr.Web安全管理中心）。
- 在**连接参数**下拉列表指定Dr.Web服务器连接原则。
- 在**加密**和**压缩**下拉列表选择要连接的Dr.Web服务器间流量的加密和压缩模式（参数使用流量的加密和压缩）。
- **分发的授权自动延期期限**——设置与Dr.Web子服务器的连接不时使用此设置。
- **接收的授权预延期时间间隔**——从邻居服务器接收的授权自动延期期限剩余时间，从这一时间开始此Dr.Web子服务器申请对这些授权进行自动预延期。使用此设置的前提是由Dr.Web子服务器将从当前Dr.Web服务器获取授权。
- **授权同步期限**——设置与Dr.Web子服务器的连接时不使用此设置。
- **授权**、**更新**和**事件**中的勾选按照*主-子*连接原则设定，不可进行更改：
  - Dr.Web子服务器从Dr.Web主服务器接收授权；
  - Dr.Web子服务器从Dr.Web主服务器接收更新；
  - Dr.Web子服务器发送事件信息给Dr.Web主服务器。
- 选项发送**Dr.Web邻居服务器事件通知**、**按照已知哈希侦测到威胁时发送Dr.Web邻居服务器事件通知**和**利用服务器间连接同步工作站硬软件信息**已停用且不可更改，原因是Dr.Web子服务器不接收来自Dr.Web主服务器的事件。
- 在**更新限制**→**更新**可设定从当前Dr.Web服务器向子服务器发送更新的日程（编辑**更新限制**列表与编辑工作站更新限制部分的日程列表相同）。

点击**保存**按钮。

Dr.Web子服务器（AUXILIARY）移至文件夹**Children**和**Offline**（见图.10-3）。

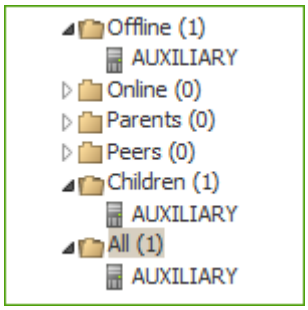


图 **10-3.**

7. 等待Dr.Web服务器间建立连接（一般用时不到一分钟）。检查连接可利用F5键更新Dr.Web服务器列表。连接建立后Dr.Web子服务器（AUXILIARY）从文件夹**Offline**移至文件夹**Online**（见图.10-4）。

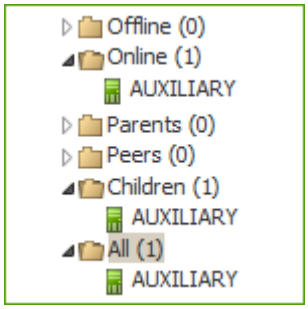


图 **10-4.**

8. 打开Dr.Web子服务器（AUXILIARY）管理中心，确认Dr.Web主服务器（MAIN）已连接子服务器（AUXILIARY）（见图.10-5）。

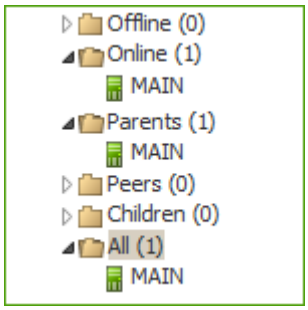


图 **10-5.**

如几个Dr.Web服务器的密码和SSL证书这一对参数相同，则无法建立连接。

建立Dr.Web服务器间平等连接时建议只在其中一个Dr.Web服务器的设置中指定要连接的服务器的地址。这不会影响Dr.Web服务器间的交互作用，但可以避免Dr.Web服务器运行日志中出现**Link with the same key id is already activated**这类记录。

但必须在一端指定要连接的Dr.Web服务器的地址。

下述情况下不可建立 **Dr.Web**服务器间连接：

- 网络连接出现问题。
- 设置连接时给出的Dr.Web主服务器地址有误。
- 其中一台Dr.Web服务器的证书有误。
- 其中一台Dr.Web服务器的密码有误（在Dr.Web邻居服务器给出的密码不符）。

如需在版本**10**和版本**13**的**Dr.Web**服务器间建立服务器间连接，还需执行以下操作：

1. 创建连接时在版本10的Dr.Web服务器指定版本13的Dr.Web服务器的公钥。
2. 使用Dr.Web服务器版本13的工具drwsign（指令gencert）从版本10的Dr.Web服务器私钥生成证书（参见 附录中的 H7.1.数字密钥和证书生成工具）。建立连接时在版本13的Dr.Web服务器指示此证书。

10.14.3. 使用多Dr.Web服务器的反病毒网络

多Dr.Web服务器网络的特点是利用部分Dr.Web服务器（一般是一个或几个Dr.Web主服务器）从Dr.Web GUS服务器获取更新。这时只需要在这些Dr.Web服务器上设置更新任务日程（参见Dr.Web服务器日程设置）。任何一台从Dr.Web GUS 服务器或是从另一台Dr.Web服务器获取更新的Dr.Web服务器，都会立即将更新传给按照设置应传递更新的其它Dr.Web服务器（即所有子服务器，或者设置有从此服务器获取更新的其它同级服务器）。

Dr.Web Enterprise Security Suite 实施自动监控，在由于网络拓扑和Dr.Web服务器设置不完善出现向同一台已接收到更新的Dr.Web服务器从另一节点重复传递此更新时，不会进行重复更新。

管理员可以通过跨服务器连接获取从属某Dr.Web服务器的某部分网络的重要病毒事件总体信息。

查看与此服务器连接的所有Dr.Web服务器病毒事件

1. 在管理中心主菜单选择**反病毒网络**。在打开的反病毒网络树结构的**Neighbors**组中选择需要查看的Dr.Web邻居服务器。
2. 在控制菜单选择**常规→设备和软件组成**后可查看连接到所选Dr.Web邻居服务器的受保护工作站的硬件和软件统计信息。

   这一部分显示的信息与连接您的Dr.Web服务器的工作站相应部分显示的信息类似（参见Windows操作系统工作站的硬软件配置）。
3. 查看连接所选Dr.Web邻居服务器的受保护工作站的反病毒组件运行统计信息需在控制菜单的**统计信息**部分选择相应选项。

   这一部分显示的信息与连接您的Dr.Web服务器的工作站相应部分显示的信息类似（参见统计信息）。

10.14.4. Dr.Web服务器群集

在群集内应只通过安装包更新Dr.Web服务器。更新时需停止所有Dr.Web服务器后按照顺序进行更新。不能利用管理中心进行更新（转至新校检），因为在使用共享数据库的情况下第一个Dr.Web服务器完成更新后，其他Dr.Web服务器将无法继续运行和更新。

在反病毒网络创建Dr.Web服务器群集时必须：

1. 配置文件相同

所有Dr.Web服务器上都应有相同的加密公钥（`*.pub`）和加密私钥（`drwcsd.pri`），以及Dr.Web服务器证书`drwcsd-certificate.pem`。

如之前未生成加密密钥和证书，在安装第一个Dr.Web服务器时会自动生成。

可通过管理中心获得安装群集中其他Dr.Web服务器所需的加密密钥和证书：菜单**管理 → 加密密钥**。可能既要求私钥，也要求证书：安装Dr.Web服务器时指定私钥 `drwcsd.pri`时，

自动生成公钥*.pub证书drwcsd-certificate.pem。生成证书时会创建其新版本，因此群集的所有Dr.Web服务器都要更换为同一版本的证书（见 安全连接保障工具）。

配置文件位置介绍参见Dr.Web服务器部分。

2. Dr.Web服务器统一名称

需为所有Dr.Web服务器指定相同的Dr.Web服务器IP地址和DNS名称，这一地址和名称在生成反病毒网络工作站代理端安装文件时使用。

利用管理中心指定名称：**管理** → **Dr.Web服务器配置**→ 网络→ 加载 → **Dr.Web服务器地址**。这些设置保存在配置文件download.conf（配置文件介绍见附录中的G3. 配置文件download.conf）。

3. 群集使用设置

在网络DNS服务器为每一Dr.Web服务器注册群集共有名称，并设置平衡负载的方式。

在Dr.Web服务器群集指定应用设置必须使用专门的群集协议。

设置群集协议必须为每一Dr.Web服务器在管理中心打开菜单**管理** → **Dr.Web服务器配置**，给出以下设置：

a) 启用群集协议需在模块标签勾选**Dr.Web服务器群集协议**。

b) 设置群集中Dr.Web服务器间交互作用参数需在群集标签指定相应参数。

c) 在输入所有必要参数后点击**保存**并重启Dr.Web服务器。

例如

- multicast组：232.0.0.1
- 端口：11111
- 接口：0.0.0.0

在此例中为群集所有Dr.Web服务器设置所有接口的传输。其他情况下，如有一个网络对群集而言是外网，代理端通过此外网连接，而第二个网络是群集内网，则应只为内网接口打开群集协议。这种情况下接口地址应指定为192.168.1.1, ..., 192.168.1.N。

4. 统一数据库

使用同一个数据库要求所有Dr.Web服务器版本相同。

同一群集中的所有Dr.Web服务器应使用同一个外设数据库。

与非群集情况相同，群集中的每一Dr.Web服务器各自对数据库进行访问，而Dr.Web服务器所有数据都分别保存。各服务器都有自己独有ID，如需，Dr.Web服务器可只从数据库提取与其ID捆绑的记录。使用同一数据库，Dr.Web服务器可以与在群集所有Dr.Web服务器注册的代理端建立连接。

创建使用同一数据库的Dr.Web服务器群集时需注意以下事项：

- 数据库可以另行安装，与所有Dr.Web服务器分开，也可以安装到群集中安装某Dr.Web服务器的计算机。

- 应在安装群集的第一台Dr.Web服务器前或在第一台Dr.Web服务器连接数据库之前创建数据库。
- 在向群集添加新节点的过程中（第一台Dr.Web服务器除外），安装Dr.Web服务器时不建议立即指定群集的统一数据库。否则可能导致保存在数据库的信息被删除。建议首先为Dr.Web服务器指定使用内设数据库，安装完成后将其转换为统一的外设数据库。
可利用管理中心将Dr.Web服务器转换为使用外设数据库：使用**管理** → **Dr.Web服务器配置** → 数据库标签，或通过Dr.Web服务器配置文件`drwcsd.conf`。
- 除了群集中的第一台Dr.Web服务器，不建议将已在反病毒网络运行的使用另一外设或内设数据库的Dr.Web服务器添加到群集。添加会造成数据丢失，包括工作站信息、统计信息、设置（处理保存于配置文件的设置）因为执行导入时数据库数据会全部被删除。这种情况下只能进行某些设置的导入。
- 默认情况下安装或升级更早版本Dr.Web服务器时配置文件`drwcsd.conf`会随机生成加密加盐，用于加密数据库中的管理员密码。为避免登录出现问题需在群集的所有Dr.Web服务器手动给出同一盐值。必要的参数 见文档**附录**中的附录G1. Dr.Web服务器配置文件。

5. 库版本相同

群集中所有Dr.Web服务器的库中更新版本应相同。

可通过以下方式实现：

- 同时从GUS更新群集的所有Dr.Web服务器。这时所有Dr.Web服务器都将获得最新版本的更新。也可从本地更新区设置更新所有Dr.Web服务器的库，从本地更新时将分发被确认的同一版本的产品更新，如创建GUS镜像则分发最新版本。
- 可建立复合结构，综合Dr.Web服务器群集和建立于服务器间连接的分层结构。这时其中一个Dr.Web服务器（可以是，也可以不是群集中的Dr.Web服务器）应设为主服务器，从GUS获得更新。群集的其他Dr.Web服务器成为子服务器，通过服务器间连接从Dr.Web主服务器获取更新。

从本地更新区（GUS镜像）或从Dr.Web主服务器更新群集Dr.Web服务器时必须监控更新区和Dr.Web主服务器的运行状况。如发布更新的节点出现异常，必须将另一Dr.Web服务器设为Dr.Web主服务器或建立新的更新区，从GUS获取更新。

6. 向工作站分发授权的特点

可采用以下方式在群集Dr.Web服务器间分发授权：

a) 在群集内不设置Dr.Web服务器的分层结构。只需将授权密钥（一个或多个）添加到群集中的一个Dr.Web服务器。此授权密钥信息会自动写入同一数据库。这样群集中的Dr.Web服务器可同时使用授权密钥。统一数据库保存的授权总数应与群集Dr.Web服务器下属工作站总和相符。



要让授权没有能够在群集中所有Dr.Web服务器使用，而不是只能在添加密钥的服务器使用，必须在添加密钥后重新启动群集中的其他Dr.Web服务器。

b) 可建立复合结构，综合Dr.Web服务器群集和建立于服务器间连接的分层结构。如果管理代理端的有群集中的Dr.Web服务器，也非群集服务器，则采用这种结构会更为便利。这时在运行过程中直接通过服务器间连接分发授权密钥中的授权数量：
   - 从不在群集的一个Dr.Web服务器向群集中的一个Dr.Web服务器分发。分发的授权供群集中的所有Dr.Web服务器使用，见a)。

- 从在群集的一个Dr.Web服务器（也就是从群集所有Dr.Web服务器共用的密钥）向不在群集的一个Dr.Web服务器分发。

分发授权数量和期限由反病毒网络管理员手动设置（详见通过服务器间连接分发授权）。

例如，需要设置Dr.Web服务器分层结构并确定一个Dr.Web主服务器（可以是，也可以不是群集中的Dr.Web服务器），主服务器将向群集节点分发库更新和授权文件中的授权。

7. Dr.Web服务器日程任务

为了避免重复向数据库发出请求，建议只在其中一个Dr.Web服务器执行Dr.Web服务器日程的以下任务： **Purge Old Data**、**Backup sensitive data**、**Purge old stations**、**Purge expired stations**、**Purge unsent IS events**.。如在统一外设数据库所在计算机上安装的Dr.Web服务器上执行。或选择群集中性能最好的计算机，如果Dr.Web服务器配置有区别，且数据库单独安装在一台计算机上。

第十一章、更新Dr.Web Enterprise Security Suite组件

本章介绍在产品运行过程中对Dr.Web Enterprise Security Suite组件进行更新，不适用于升级到新版本。

如何将产品及其组件升级到新版本见**安装手册**中的第七章、更新Dr.Web Enterprise Security Suite组件。



在更新Dr.Web Enterprise Security Suite和其个别组件之前请一定检查访问互联网的TCP/IP协议设置是否正确，特别需要注意DNS服务是否开启，其设置是否正确。

在更新软件前建议设置库配置，包括设置对Dr.Web GUS的访问（参见库常规配置）。

11.1. 更新Dr.Web服务器和利用备份还原

管理中心具备以下管理Dr.Web服务器软件的功能：

- 将Dr.Web服务器软件更新为从GUS下载的保存于Dr.Web服务器库的一个版本。如何设置从GUS更新库见管理Dr.Web服务器库。
- 将Dr.Web服务器软件还原至保存的备份。Dr.Web服务器转至新版本时**Dr.Web服务器更新**部分会自动创建备份（见下步骤4）。



还可以利用Dr.Web服务器软件来更新Dr.Web服务器。操作描述见**安装手册**的更新OS Windows Dr.Web服务器或更新OS UNIX Dr.Web服务器。

并非所有的Dr.Web服务器更新含有软件文件。某些文件只能通过管理中心安装。

利用管理中心更新UNIX家族操作系统的Dr.Web服务器时，操作系统数据包管理器中显示的Dr.Web服务器版本不发生变化。

管理Dr.Web服务器软件的操作：

1. 在管理中心主菜单选择**管理**，在打开的窗口选择控制菜单中的**Dr.Web服务器**一项。
2. 打开Dr.Web服务器版本列表需执行以下一种操作：
   - 点击主窗口的Dr.Web服务器当前版本。
   - 点击**版本列表**按钮。
3. 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。这时：
   - 在**当前版本**列表显示是现在正在使用的Dr.Web服务器版本。在**更改列表**显示的是与上一版本相比此版本出现的新功能和纠正的错误。
   - 在**所有版本**列表显示的是从GUS下载的此Dr.Web服务器更新列表。在**更改列表**显示的是与每一更新前相比出现的新功能和纠正的错误。
     对应从安装包初始安装的Dr.Web服务器版本的**更改列表**为空。

- 备份列表是为此Dr.Web服务器保存的备份列表。日期显示的是备份时间信息。

4. 更新Dr.Web服务器软件需在所有版本列表勾选相应的Dr.Web服务器版本后点击保存按钮。



只能更新至晚于当前使用版本的Dr.Web服务器版本。

Dr.Web服务器更新过程中当前版本会保存为备份（移至备份部分），而更新后的版本从所有版本移至当前版本部分。

备份保存于以下目录：

`var → update → backup → <老版本>-<新版本>`

更新过程至创建或添加日志文件记录`var → dwupdater.log`。

5. 还原Dr.Web服务器软件需在备份列表勾选相应的Dr.Web服务器版本后点击保存按钮。

还原Dr.Web服务器软件过程中被还原的备份移至当前版本部分。

11.2. 手动更新Dr.Web服务器库

检查库的当前状态或者更新反病毒网络组件

1. 在管理中心主窗口选择管理，在打开的窗口选择控制菜单中的库状态一项。
2. 打开的窗口显示库产品列表、当前使用的校检的日期、上次加载校检的日期和产品状态。



状态一列为上次更新时Dr.Web服务器库中产品的状态。

3. 使用工具面板的下列按钮管理库内容：
   - 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。如查看的组件已过时，则会自动进行更新。
   - 下载库更新日志需点击工具面板的以下一个按钮：
     - 将数据保存到**CSV**文件，
     - 将数据保存到**HTML**文件，
     - 将数据保存到**XML**文件，
     - 将数据保存到**PDF**文件。
   - 点击从磁盘重启库后从磁盘重新启动库的当前版本。

   启动Dr.Web服务器时将库内容加载到内存。如在Dr.Web服务器运行过程中管理员没有利用管理中心而更改了库内容，如使用外设工具或手动更新了库内容，则使用加载于磁盘的库版本需要进行重启。

11.3. 按照日程更新Dr.Web服务器的库

可在Dr.Web服务器设置任务日程，以便定期进行软件更新（详见Dr.Web服务器日程设置）。

设置更新Dr.Web服务器库的日程

1. 在管理中心主菜单选择**管理**，在打开的窗口选择控制菜单中的**Dr.Web服务器任务计划器**一项。打开Dr.Web服务器当前任务列表。
2. 添加新任务时需在工具面板点击**创建任务**按钮。打开任务编辑窗口。
3. 在**常规**标签设定以下参数：
   - 在**名称**一栏输入任务名称，新任务在日程中将以这一名称显示。
   - 如要激活任务的执行，需勾选**允许执行**。如取消勾选，任务会保存在日程表，但不会执行。
   - 勾选**重要任务**后如因某种原因未能在指定时间执行此任务，则会进行非例行任务启动。任务计划器每分钟查看一次任务列表，发现有重要任务未执行，就会启动执行。如启动时任务已未执行多次，则只非例行启动一次。
   - 如取消对**异步启动任务**的勾选，任务将列入任务计划器的任务顺序执行队列。如勾选此项，则启动此任务不需等待执行次序。
4. 在**操作**标签设定以下参数：
   - 进入**操作**标签，在下拉列表中选择任务类型**更新库**。
   - 在**产品**列表勾选需按照此任务更新的库产品。
   - 勾选**更新授权密钥**，激活库更新时自动更新授权密钥。详细信息见自动更新授权。
5. 在**时间**标签设定以下参数：
   - 在**周期**下拉列表选择任务启动模式并根据所选周期相应设置时间。
   - 勾选**在第一次执行后禁止**后任务只在指定时间执行一次。如取消勾选，将按照指定周期多次执行。
6. 点击**保存**按钮后按指定参数创建任务。

11.4. 未接通互联网的Dr.Web Server的库更新

如Dr.Web服务器未接通互联网，无法从GUS服务器获取库更新的Dr.Web Server的库更新，可使用以下更新设置：

- 如网络中有一台Dr.Web服务器可连接互联网获取更新，需设置与此服务器的同级服务器连接或主子服务器连接，Dr.Web子服务器是无法连接互联网的服务器。这样不连接互联网的Dr.Web服务器会从主Dr.Web服务器获取更新。

  服务器间连接设置见多台Dr.Web服务器网络特点。
- 如无法通过设置服务器间连接来从另一Dr.Web服务器自动获取更新，可手动更新未连网Dr.Web服务器的库：
  - 如网络中有一台Dr.Web服务器可连接互联网获取更新，可按照 复制另一Dr.Web服务器的库 部分描述的操作将可更新Dr.Web服务器库的内容复制到未连网服务器。
  - 如果没有可连接互联网的Dr.Web服务器，可以不利用Dr.Web服务器软件从GUS下载库，而是利用Dr.Web库加载器这一工具来下载。

11.4.1. 复制另一Dr.Web服务器的库

如果Dr.Web服务器未接通互联网，则可以通过复制另一已更新的Dr.Web服务器的库来进行手动库更新。



不可以使用此方式将Dr.Web服务器升级为新版本。

从另一**Dr.Web**服务器获取库更新

1. 利用管理中心的**管理** → 库状态更新连接互联网的Dr.Web服务器的库。
2. 利用管理中心的库内容导出库或库的一部分（您所需要的产品）。导出时需注意导出的应是支持导入的对象。
3. 将库压缩文档复制到安装有需更新的Dr.Web服务器的计算机。
   利用管理中心的**管理** → 库内容将库导入到Dr.Web服务器。



如您使用库特殊设置，例如冻结校检或限定只从指定（非最后一个）校检更新代理端，则导入库时需启用**只添加空缺校检**选项，并停用**导入配置文件**选项。

11.4.2. Dr.Web库加载器

如果没有可连接互联网的Dr.Web服务器，从GUS下载库可以不利用Dr.Web服务器软件，而是利用Dr.Web库加载器这一工具来下载。

使用特点

- 从GUS加载库需要Dr.Web Enterprise Security Suite授权密钥，或密钥的MD5哈希，可在管理中心的**管理**→ **授权管理器**查看此值。
- Dr.Web库加载器有以下版本：
  - 图形版本（只限OS Windows），
  - 控制台版本。
- 从GUS加载库可使用代理服务器。



库产品组成信息见管理Dr.Web服务器库。

使用方式

手动替换库

1. 通过Dr.Web库加载器从GUS加载Dr.Web服务器库。

加载时请创建库压缩文档：

a) 使用图形工具时：选择模式**加载库**，并在工具主窗口勾选**压缩库**。

b) 使用控制台工具时：使用参数`--archive`。

2. 将库压缩文档复制到需更新Dr.Web服务器的计算机。

   利用管理中心的**管理** → 库内容将库导入到Dr.Web服务器。



如您使用库特殊设置，例如冻结校检或限定只从指定（非最后一个）校检更新代理端，则导入库时需启用**只添加空缺校检**选项，并停用**导入配置文件**选项。

在局域网服务器创建库镜像

1. 通过Dr.Web库加载器图形工具从GUS加载Dr.Web服务器库。

   加载时在工具主窗口选择模式**同步更新镜像**。

2. 将加载的库移至局域网用于分发库更新的Web服务器。

3. 在**管理** → 库常规配置设置Dr.Web服务器从本地镜像获取更新，而不是从Dr.Web GUS获取更新。更新加载协议的选择取决于第 2步中的服务器类型：Web服务器选HTTP/HTTPS，FTP服务器选择FTP/FTPS等等。例外的是FILE，不可在网络中使用此协议（参见在Dr.Web服务器创建库镜像）。

在Dr.Web服务器创建库镜像

1. 通过Dr.Web库加载器从GUS加载Dr.Web服务器库。

   加载时在工具主窗口选择模式**同步更新镜像**。

2. 将加载的镜像放到安装有Dr.Web服务器的计算机的任一目录。

3. 在**管理**→ 库常规配置设置使用FILE协议获取更新。

   必须在**基本URI**一栏输入镜像所在目录的完整本地路径。这时不使用**Dr.Web全球更新系统服务器列表**。



请确认镜像所在目录的名称是`13.00`。而且**基本URI**指定的是到这一目录的路径，但不包含此目录本身。

11.4.2.1. 工具的图形版本

可通过管理中心的**管理** → **工具**下载只适用于OS Windows的Dr.Web库加载器图形版本。可在任意一台接通互联网的Windows操作系统计算机启动这一版本。

工具位置在Dr.Web服务器安装目录的`webmin/utilities`目录。执行文件`drweb-reploader-gui-windows-<位数>.exe`。

利用Dr.Web库加载器图形版本下载库的操作

1. 启动Dr.Web库加载器图形版本。

2. 在工具主窗口给出以下参数：

a) **授权密钥或MD5密钥**——指定Dr.Web授权密钥文件。操作是点击**浏览**后选择有效的授权密钥文件。也可指定密钥的MD5哈希，可在管理中心的**管理→授权管理器**查看。

b) **加载目录**——指定加载库的目录。

c) 在**模式**列表选择一种更新加载模式：

- **加载库**——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。
- **同步更新镜像**——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。

d) 勾选**压缩**后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。

3. 如需更改连接GUS和加载更新的高级设置，需点击**高级参数**。在打开的窗口可设置以下标签：

a) 在**产品**标签可更改加载的产品列表。设置窗口显示的是可从GUS加载的库所有产品的列表：

- 更新当前GUS产品列表，需点击**更新**按钮。
- 勾选需从GUS加载的具体产品或通过勾选表头全选表中所有产品。

b) 在**Dr.Web GUS**可设置更新服务器参数：

- 表中GUS服务器顺序确定加载库时加载器的访问次序。可使用**上移**和**下移**按钮更改GUS服务器顺序。
- 将GUS服务器添加到此列表需在服务器列表上方的输入栏输入GUS服务器地址，然后点击**添加**按钮。
- 从此列表删除GUS服务器需勾选需要删除的服务器后点击**删除**按钮。
- 在**基本URI**指定GUS服务器包含Dr.Web产品更新的目录。
- 在**协议**下拉列表选择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。
- 在**可用证书**下拉列表选择自动接受的SSL证书类型。此设置只用于支持加密的安全协议。
- **注册用户名**和**密码**——如需要进行身份验证，登录更新服务器的用户注册信息。
- 勾选**使用CDN**，允许加载库时使用Content Delivery Network。

c) 在**代理服务器**标签可设置通过代理服务器连接GUS的连接参数：

- **代理服务器地址**和**端口**——所使用的代理服务器的地址和端口。
- **注册用户名**和**密码**——如需要进行身份验证，登录代理服务器的用户注册信息。

d) 在**任务计划器**标签可设置定期更新日程。执行日程使用OS Windows任务计划器。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。

e) 在**日志**标签可设置更新加载日志的参数。

点击**确定**按钮接受更改并返回Dr.Web库加载器主窗口。

4. 完成所有设置后点击Dr.Web库加载器主窗口的**加载**按钮，以便开始连接GUS并加载库。

11.4.2.2. 工具的控制台版本

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。

用于库加载器工具控制台版本的命令行参数介绍见**附录**的 H7.5. Dr.Web库加载器。

11.5. 工作站更新限制

利用可管理中心可限制Dr.Web服务器和受保护工作站上代理端某一时段内的网络流量。

详见限制工作站流量。

补充安装新组件以及管理员利用控制面板**更新失败组件**启动更新是不限制更新速度。

设置流量限制模式

1. 在主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。在控制菜单选择**更新限制**。
2. 在**更新限制**下拉列表选择限制模式：
   - **更新所有产品**——不限制向工作站传递更新。
   - **禁止所有更新**——在指定时间段禁止向工作站传递任何更新，时间段在下面的**工作站更新日程**列表中指定。
   - **只更新病毒库**——在指定时间段只禁止向工作站传递软件组件更新，时间段在下面的**工作站更新日程**列表中指定。病毒库更新将照常进行。
3. 勾选**降低病毒库久未更新的严重性**后降低病毒库未更新的工作站的状态的重要性。勾选此项后病毒库未更新的工作站在反病毒网络显示为常规图标，工作站**状态**部分重要性显示为**低**。如取消勾选，病毒库未更新的工作站在反病毒网络显示为（如工具面板的**设置树结构**→**显示工作站状态重要性**为启用），在工作站**状态**部分重要性为**最高**或**高**。
4. 在**校检有效期**一栏指定Dr.Web服务器库出现新校检时，工作站已安装的产品校检认为是有效校检的时间段。
5. 勾选**获取最新更新**后工作站会接收所有组件更新，不取决于库详细配置中指定的限制。

如取消勾选，工作站将只获得标志为当前应传播的更新。

6. 勾选**允许转用较早校检**，则允许按照分发设置使用Dr.Web服务器库中的较早校检来替换工作站上的反病毒组件新版本。

   另见将产品校检退回到上一版本。

7. 勾选**限制更新流量**后会限制Dr.Web服务器和代理端间传递更新时的网络流量。

   如取消勾选，则不限制传递代理端更新占用的带宽。

   如勾选，需指定：

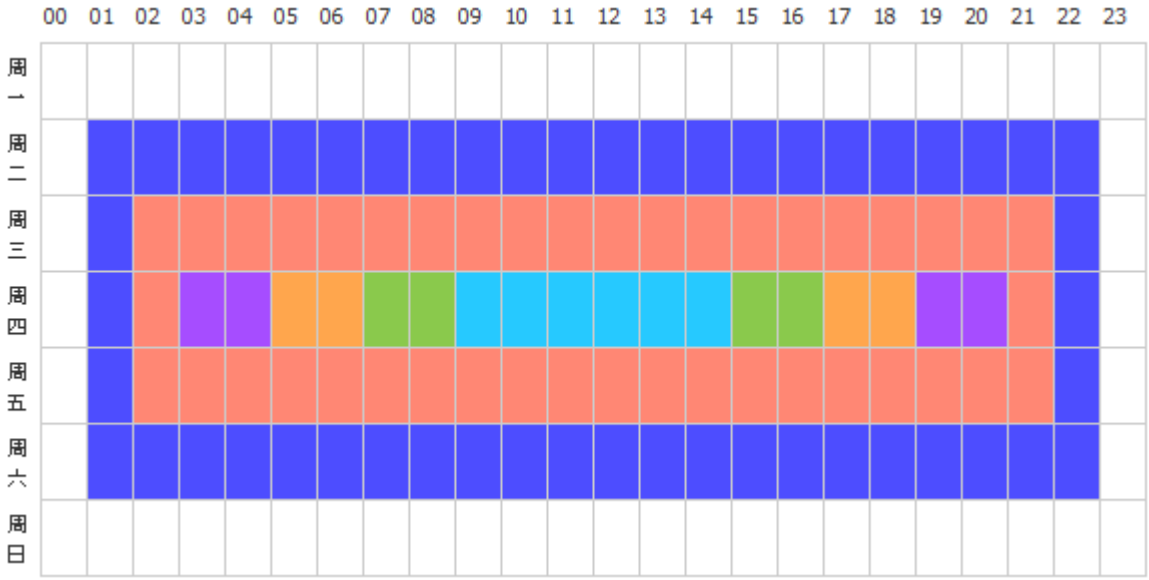
   - 在**默认速度**指定默认情况下更新传递最大限速，也就是未指定其他限制时（日程中空白）的限速。当某时段禁止传递数据，但更新进程已启动时应用此限速（见下）。
   - 勾选后在**最大传递速度（KB/s）**一栏指定传递更新的最大限速。限定后更新会在指定带宽内传递所有代理端更新产生的总流量。

     可指定五种代理端更新数据传输速度限制。添加速度限制输入行需点击。删除限制需点击相应行旁边的删除按钮。

   对**默认速度**和**最大传递速度（KB/s）**两栏指定的数值存在以下限制：

   - 禁止指定0。最小限定值为1KB/s。
   - 输入栏为空（为填写）表示相应时间段没有更新流量限制。

   日程表中数据传输速度限制模式时段划分为每星期每天的每30分钟。



   更改数据传输速度限制模式需点击表格中相应区间。可按照drag-and-drop同时选择多个时段。

   表格颜色以下颜色变化方式而周期变化：

   在设定为**禁止传输数据**的时间段禁止开始传递更新。如此时段开始时更新进程已启动，不会中断进程，而最大传输速度依据**默认速度**的限定值。

8. 结束编辑后点击**保存**按钮保存更改。

在工具面板可使用以下选项：

**将所有参数设为初始值**——还原这一部分所有参数此次编辑前的参数值（上次保存的参数值）。

**将所有参数设定为默认值**——将这一部分所有参数设为默认值。

**将设置适用于另一对象**——将本部分的设置复制到另一工作站、另一工作站组或多个工作组、多个工作站组。

**继承策略或基组设置**——删除工作站自身设置，继承基组本部分的设置。

**复制策略或基组设置并将其指定为自身设置**——复制基组本部分的设置并将其中的给所选工作站。这时不是继承设置，工作站获得的是自身设置。

**将本部分设置导出到文件**——将本部分所有设置保存到专门格式的文件。

**从文件将设置导入到本部分**——从专门式格的文件导入设置，替代本部分所有设置。

11.6. 移动模式下Dr.Web代理端的更新

如果用户的计算机（或笔记本电脑）将长时间不能连接Dr.Web服务器，建议将Dr.Web代理端设置为*移动模式*以便及时从Dr.Web GUS服务器获得更新。



可在代理端设置启用移动模式的前提是管理中心的**反病毒网络** → **权限** → *<操作系统>* → **常规** → 更改**Dr.Web代理端配置**（对于OS Windows）或**以移动模式启动**（对于其他操作系统）部分允许使用移动模式。

移动模式下代理端将试图连接Dr.Web服务器，三次尝试失败后将执行从GUS进行HTTP更新。搜索Dr.Web服务器的时间间隔大约为一分钟。

代理端以移动模式运行时代理端与Dr.Web服务器的连接中断。所有在Dr.Web服务器上对此工作站设置的更改将在代理端关闭移动模式且代理端和Dr.Web服务器重新建立连接后立即生效。



在移动模式下只进行病毒库更新。

代理端在移动模式下运行没有时限，但只在工作站授权密钥有效期内可从GUS加载病毒库更新。最后一次连接Dr.Web服务器时代理端保留授权有效期相关信息（授权密钥本身保存于Dr.Web服务器）。

在代理端设置移动模式参见**用户手册**。

第十二章、补充组件设置

12.1. Dr.Web代理服务器

反病毒网络可以包括一个或几个Dr.Web代理服务器。

代理服务器的主要任务——在无法构架直接访问时保证Dr.Web服务器和Dr.Web代理端之间的连接，例如当Dr.Web服务器和Dr.Web代理端 处于不同网络，而网络间没有路由包交换。

通过代理服务器可将反病毒网络中的任意一台计算机作为：

- 更新转发中心，这样可以降低Dr.Web服务器的网络负载和Dr.Web服务器与代理服务器的连接负载，利用缓存功能还可缩短受保护工作站获取更新的时间。
- 将受保护工作站病毒事件转发给Dr.Web服务器的转发中心，这样也可以降低网络负载，并在Dr.Web服务器和受保护工作站处于不同的网络的情况下保证数据的传输。

主要功能

代理服务器具备以下功能：

1. 进行网络监听，按照指定的协议和端口接收连接。
2. 广播协议（支持TCP/IP）。
3. 按照代理服务器的设置在Dr.Web服务器和Dr.Web代理端之间传递数据。
4. 缓存从Dr.Web服务器接收的代理端和反病毒软件包更新。从代理服务器的缓存下传更新可以保证：
   - 减少网络流量；
   - 减少代理端接收更新的时间。
5. 保证Dr.Web服务器与代理端之间的流量加密。



可建立代理服务器分层结构集群。

使用代理服务器的的反病毒网络总体示意图见图11-1。

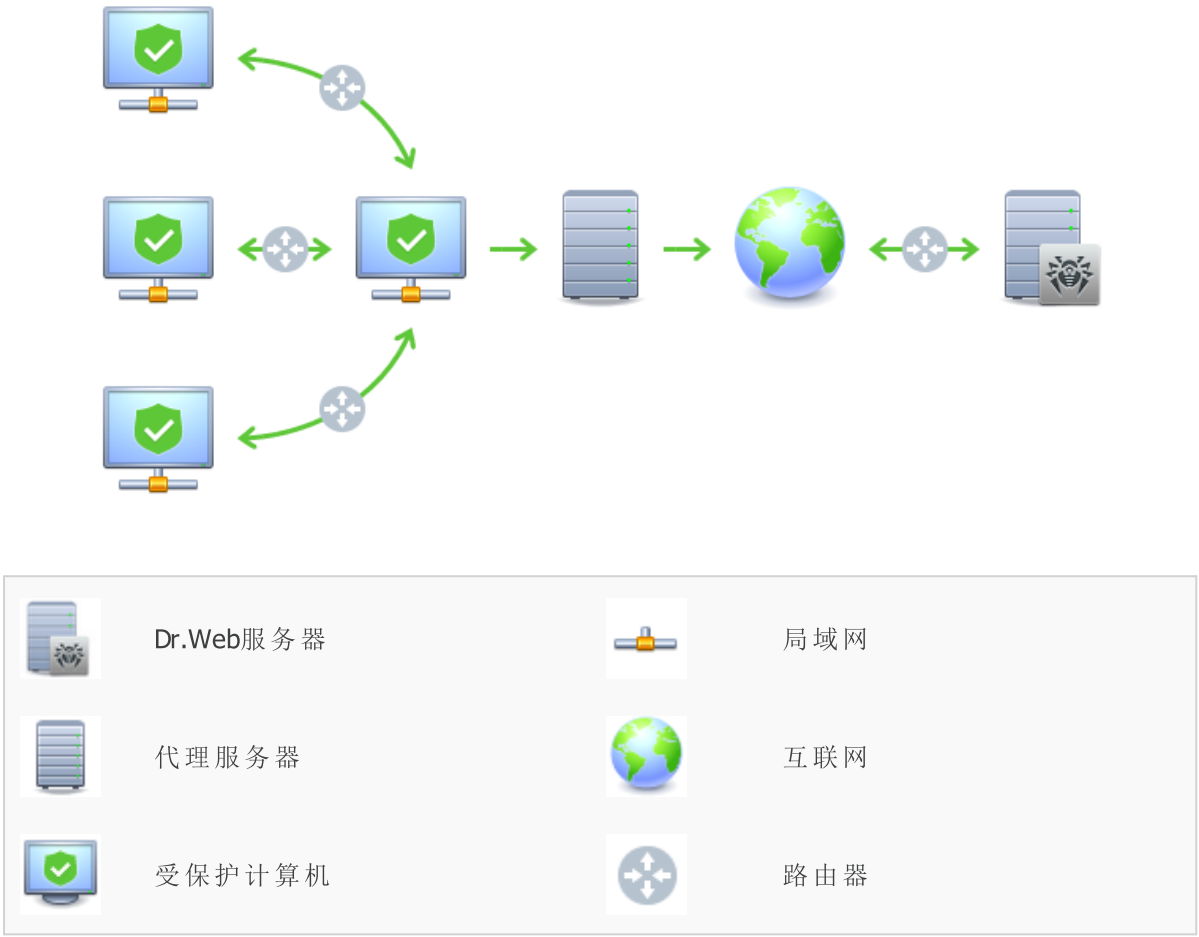


图**11-1**. 使用代理服务器的反病毒网络示意图

运行原理

使用代理服务器需按以下流程进行操作：

1. 如果代理端上没有指定Dr.Web服务器地址，代理端会按照其所在网络的协议发出组播请求。
2. 如代理服务器设置为广播协议（参数`discovery="yes"`），则向代理端发出存在运行中的代理服务器的通知。
3. 代理端将获取的代理服务器参数设置为Dr.Web服务器参数。以后对代理端而言交互作用为透明模式。
4. 按照配置文件参数代理服务器监听指定的端口指定协议的传入连接。
5. 从代理端收到传入连接时代理服务器与Dr.Web服务器建立连接。

存在**Dr.Web**服务器名单时的地址重定向方式：

1. 代理服务器从配置文件`drwcsd-proxy.conf`（参见**附录**的附录G4）将Dr.Web服务器名单加载到内存。
2. Dr.Web代理端连接到代理服务器。

3. 代理服务器将来自Dr.Web代理端的流量转给内存名单中的第一个Dr.Web服务器。
4. 代理服务器滚动内存中的名单，将Dr.Web服务器从名单中的第一位移至名单末尾。

> 代理服务器的配置文件中不保存更改后的Dr.Web服务器次序。重启代理服务器时重新加载配置文件中保存的Dr.Web服务器初始名单。

5. 下一个代理端连接到代理服务器后，重复步骤2之后的操作。
6. 如Dr.Web服务器与反病毒网络断开（如关机或拒绝服务），代理端再次连接到代理服务器，重复步骤2之后的操作。

> 从处于相对代理端而言是外网的计算机启动的网络搜索仪不能发现已安装的代理端。

> 如Dr.Web服务器设置中勾选了**替换NetBIOS名称**，而在反病毒网络中使用代理服务器，则所有通过代理服务器连接Dr.Web服务器的所有工作站在管理中心的显示都将是安装有代理服务器的计算机的名称，而非这些工作站的名称。

流量加密和压缩

代理服务器支持流量压缩.对所传递信息的处理不取决于流量是否压缩。

代理服务器支持流量加密。支持加密需要代Dr.Web理服务器与服务器建立连接（参见**安装手册**中的将代理服务器连接到Dr.Web服务器），并使用Dr.Web服务器证书和私钥为自己的证书签名。代理服务器与Dr.Web服务器间的流量加密依据Dr.Web服务器证书；代理端与代理服务器间的流量加密依据使用Dr.Web服务器证书和私钥签名的代理服务器证书。

缓存

代理服务器支持流量缓存。

产品缓存按校订进行。每一校订保存于单独的目录。每个下一次校订目录中包含旧校订文件的*硬链接（hard links）*和发生更改的文件原件。这样，每一版本的文件在硬盘上只保存一个，所有后续校订目录中是对未更改文件的链接。

配置文件中的参数用于设置以下缓存操作：

- 定期清空过时校订，默认为每小时进行一次。
- 至保留最新校订。所有之前的校订都认为是过时校订而被删除。默认保留最近的3个校订。
- 定期卸载未使用的*memory mapped*文件，默认为每10分钟进行一次卸载。

设置

代理服务器没有图形界面。利用以下一种方式进行设置：

1. 利用管理中心进行远程设置，前提是代理服务器与Dr.Web服务器建立了连接（见 远程设置代理服务器）。

2. 利用配置文件进行设置。代理服务器配置文件格式件见**附录**的附录G4。

只有具备本机管理员权限的用户才可管理代理服务器设置（编辑配置文件）。

Linux家族操作系统的代理服务器正常运行需要重启电脑后进行网络系统设置，且设置不使用网络管理器。

启动和停止

Windows操作系统下使用系统工具启动、停止代理服务器：**控制面板** → **管理工具** → **服务** → 在服务列表中双击**drwcsd-proxy**后在打开的窗口选择需要的操作。

UNIX家族操作系统下通过对代理服务器安装过程中建立的脚本应用`start`命令和`stop`命令启动、停止代理服务器（参见**安装手册**，代理服务器安装）。

OS Windows和OS UNIX下都可以通过启动设置有相应参数的执行文件`drwcsd-proxy`来启动代理服务器（参见附录H5. 代理服务器）。

12.1.1. 远程设置代理服务器

Dr.Web代理服务器连接Dr.Web服务器后可通过管理中心远程设置代理服务器。

连接设置详细信息见**安装手册**中的将代理服务器连接到Dr.Web服务器。

代理服务器只从标志为控制服务器的Dr.Web服务器获得设置。如没有标为控制服务器的Dr.Web服务器，则依次连接所有Dr.Web服务器，直至第一次获取非空白配置。

设置代理服务器

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击代理服务器的名称或组**Proxies**和其子组。
2. 在打开的控制菜单选择**Dr.Web代理服务器**。打开设置选项。
3. 在**证书**标签指定Dr.Web服务器证书列表。必须包括代理服务器连接并向其重定向客户端流量的所有Dr.Web服务器的证书。
   - Dr.Web服务器证书用于连接Dr.Web服务器，以便远程管理设置，并支持Dr.Web服务器与代理服务器之间的流量加密。
   - 使用Dr.Web服务器证书和私钥签名的代理服务器证书（签名在与Dr.Web服务器建立连接后自动进行，不需要管理员参与），用于连接代理端，并支持代理端与代理服务器之间的流量加密。
4. 在**监听**标签设置代理服务器进行流量接收和重定向的参数。

   统一网络监听设置可为所有客户端连接指定统一设置或为每一Dr.Web服务器单独指定设置。

添加新参数集需点击。

删除参数块需点击相应参数集旁的。

每一参数集客单独设置以下代理服务器运行参数：

a) 监听设置部分：

- 在**监听地址**一栏给出代理服务器"监听"的IP地址。值0.0.0.0表示"监听"所有接口。



地址以网络格式输入，网络格式列于**附录**中的附录E. 网络地址特点。

- 在**端口**一栏给出代理服务器将监听的端口号。默认情况下为端口2193。
- 勾选**发现**后启用Dr.Web服务器仿真模式。此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。
- 勾选**Multicasting**一项允许代理服务器响应发给Dr.Web服务器的广播请求。
- 在**Multicast组**一栏给出代理服务器所属多播组的IP地址。代理服务器将监听给出的接口，以便在搜索处于活动状态的网络Dr.Web服务器时与客户端交互作用。如此栏为空，则代理服务器不被纳入任何一个多播组。默认服务器所在多播组是231.0.0.1。

b) 在**与客户端的连接参数**部分：

- 在**加密**下拉列表中选择代理服务器和其所服务的客户端间流量的加密模式，包括代理端和代理端安装程序。
- 在**压缩**下拉列表中选择代理服务器和其所服务的客户端间流量的压缩模式，包括代理端和代理端安装程序。在**压缩等级**一栏指定压缩等级（从1到9）。

c) 在与**Dr.Web服务器的连接参数**指定向其重定向流量的Dr.Web服务器列表。

列表中Dr.Web服务器的次序决定流量重定向次序和代理服务器连接Dr.Web服务器获取设置的次序。更改Dr.Web服务器次序的操作是利用鼠标将相应行拉到需要的位置。

管理Dr.Web服务器可使用Dr.Web服务器列表工具面板的下列按钮：

编辑与所选Dr.Web服务器的连接参数。

添加与Dr.Web服务器的连接参数。

删除与所选Dr.Web服务器的连接参数。

编辑和创建与Dr.Web服务器的连接参数时打开设置窗口，包含以下选项：

- 在**可从此Dr.Web服务器管理代理服务器的设置**选择一种将Dr.Web服务器指定为控制服务器的方式：
  是——Dr.Web服务器将无条件作为控制服务器。可将任意数量的Dr.Web服务器指定如何为服务器，按照代理服务器设置依次连接所有控制Dr.Web服务器，直至第一次获取非空白配置。
  否——Dr.Web服务器任何情况下都不会是控制服务器。可以不指定任何Dr.Web控制服务器。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）（参见**附录**的G4. 代理服务器配置文件）。
  可能——只有没有无条件控制服务器（此设置值为**是**）时此Dr.Web服务器才作为控制服务器。
- 在**重定向地址**部分指定代理服务器将建立的连接重定向使用的 Dr.Web服务器地址。

如**重定向地址**一栏未指定地址或指定为udp/，则代理服务器会利用发现服务，即发出多播请求来搜索Dr.Web服务器（参见步骤9）。

地址以网络格式输入，网络格式列于**附录**中的附录E. 网络地址特点。

- 在**加密**下拉列表中选择代理代理服务器和指定的Dr.Web服务器间连接通道的流量加密模式。
- 在**压缩**下拉列表中代理服务器和指定的Dr.Web服务器间连接通道的流量压缩模式。在**压缩等级**下拉列表选择压缩等级（从1到9）。

利用表格可指定对流量重定向的限制，与Dr.Web服务器设置中的更新和安装部分的设置方式相同。

5. 在**缓存**给出以下代理服务器缓存参数：

   勾选**启用缓存**，缓存代理服务器传输的数据并设置以下参数：

   - 在**校检删除周期（分钟）**指定缓存中校检数量超过最大允许值时对过时校检进行删除的时间间隔，以分钟计。默认为60分钟。
     - 在**应保存校检数量**指定清空后保留在缓存的每一产品校检最多数量。默认保留最新的3个校检，其他删除。
   - 在**卸载未使用文件的周期（以分钟计）**一栏指定从内存卸载未使用文件的时间间隔（单位为分钟）。默认值为10分钟。
   - 在**完整性检查模式**下拉列表选择缓存中数据完整性的检查模式：
     - **启动时**——启动代理服务器时（可能占用较长时间）。
     - **无操作时**——在代理服务器停工时。
   - 勾选**使用预缓存**将按照下面的日程将所选产品新校检从Dr.Web服务器加载到代理服务器。在此期间Dr.Web服务器从GUS获取校检后后立即加载到代理服务器。如取消勾选，则只在代理端向Dr.Web服务器申请校检时新校检才会加载到代理服务器。
     - 在路边中勾选需进行同步的产品。
     - 在**库同步日程**指定为所选产品加载更新的日程。
       更改数据传输速度限制模式需点击表格中相应区间。可按照drag-and-drop同时选择多个时段。
       表格颜色按照表格下方颜色变化方式而周期变化，流量无限制或完全禁止传输数据。
6. 在**事件**给出以下参数：
   - 勾选**缓存事件**后缓存从代理端接收的事件，并将按照下面的日程中允许发送事件的时间段每15分钟向Dr.Web服务器发送一次事件。如果停用缓存，则代理服务器接收到事件后会立即发送到Dr.Web服务器。
   - 在**事件发送日程**指定从代理端接收的事件的传递日程。
     更改数据传输速度限制模式需点击表格中相应区间。可按照drag-and-drop同时选择多个时段。
     表格颜色按照表格下方颜色变化方式而周期变化，传递事件时流量无限制或完全禁止传递事件。
7. 在**转储**给出以下参数：
   - 勾选**此建立内存转储**则在代理服务器运行出现重大错误时建立内存转储。
   - 在**最多转储数量**指定内存转储的最多数量。达到指定值后建立新转储时会删除保存时间最长的转储。设置进行内存转储仅限Windows操作系统。

8. 在**DNS**标签指定访问DNS服务器的参数。设置与Dr.Web服务器的DNS设置方式相同。
9. 在**发现**标签设置为重定向客户端搜索Dr.Web服务器时广播请求回应的保存参数（参看步骤4c）。
   - **成功响应，秒**——保存搜索Dr.Web服务器时对广播请求作出回应的Dr.Web服务器的列表的期限（以秒计）。超过次期限后会重新发出请求。
   - **失败响应，秒**——保存搜索Dr.Web服务器时没有服务器对广播请求作出回应的的信息的期限（以秒计）。超过次期限后会重新发出请求。
10. 在**更新**标签设置从Dr.Web服务器自动更新代理服务器软件的参数：
    - 勾选**启用自动更新**后会自动从Dr.Web服务器加载代理服务器新校检并进行安装。更新日程取决于代理服务器预缓存的设置（参见步骤5）：
      a) 如果代理服务器未列入预缓存列表（包括不启用缓存的情况），则会按照自动更新日程加载和安装代理服务器更新。
      b) 如果代理服务器已列入预缓存列表，则会按照预缓存日程日程加载代理服务器更新。获得代理服务器新校检后会按照自动更新日程转至新校检。
    - 在**更新日程**指定进行自动更新的日程。
      更改数据传输速度限制模式需点击表格中相应区间。可按照drag-and-drop同时选择多个时段。
      表格颜色按照表格下方颜色变化方式而周期变化，更新时流量无限制或完全禁止传输更新。
11. 结束编辑需点击**保存**按钮。

12.2. NAP Validator

概述

*Microsoft Network Access Protection（NAP）*是Windows操作系统内置的策略平台，通过执行对未来系统运行的要求来保证网络安全。

使用NAP技术时可创建用户运行策略来判断电脑状态。以下情况会对得出的判断加以分析：

- 在允许访问或交互作用前，
- 自动更新相应要求以保证其兼容，
- 调整电脑以保证符合指定的要求。

NAP技术详细介绍见Microsoft Docs官网。

NAP技术在Dr.Web Enterprise Security Suite中的使用

Dr.Web Enterprise Security Suite使用NAP技术检查受保护工作站上反病毒软件的运行能力。执行这一功能的组件是Dr.Web NAP Validator。

检查运行能力使用以下工具：

- 安装并设置好的NAP运行能力检查服务器。

- Dr.Web NAP Validator是使用Dr.Web用户策略判断受保护系统反病毒软件运行能力的工具（System Health Validator - SHV）。安装在设为NAP服务器的电脑。
- 系统运行能力客户端（System Health Agent - SHA）。和Dr.Web代理端软件一同自动安装到工作站。
- Dr.Web服务器作为更正服务器，用以保证工作站反病毒软件正常运行。



图**12-2.** 使用**NAP**的反病毒网络示意图

检查流程如下：

1. 代理端有相应设置时自动激活检查进程。
2. 工作站上的SHA与安装在NAP服务器的组件Dr.Web NAP Validator建立连接。
3. Dr.Web NAP Validator对运行策略进行检测（见下）。检查过程是NAP Validator根据对设置规则的执行情况评价反病毒软件运行情况并确定系统当前状态等级：
   - 通过检查的工作站符合设定的策略元素，被认为是正常运行的工作站并允许在网络中运行。

- 只要不符合策略中的一个元素，工作站就被判断为非正常运行状态。这样的工作站只允许访问Dr.Web服务器，并与网络其他部分隔离。Dr.Web服务器恢复工作站运行能力后再次对其进行检查。

运行能力要求：

1. 代理端处于运行状态（已启动运行）。
2. 病毒库已更新（病毒库与服务器上的病毒库相符）。

NAP Validator的设置

Dr.WebNAP Validator （见 安装手册的NAP Validator的安装） 安装到设有NAP服务器的电脑后，需执行以下操作：

1. 打开NAP服务器设置组件（命令为`nps.msc`）。
2. 在**Policies**部分选择子项**Health Policies**。
3. 在打开的窗口打开元素属性：
   - **NAP DHCP Compliant**。在设置窗口勾选**Dr.Web System Health Validator**，指定使用组件Dr.Web NAP Validator的策略。在下拉列表选择**Client passed all SHV checks**，承认符合指定策略所有要素的工作站为正常运行的工作站。
   - **NAP DHCP Compliant**。在设置窗口勾选**Dr.Web System Health Validator**，指定使用组件Dr.Web NAP Validator的策略。在下拉列表选择**Client fail one or more SHV checks**，承认有一项指定策略要素不符的工作站为非正常运行。

索引

A

Active Directory
- 概述 42
- 管理员身份验证 83

D

Dr.Web服务器
- 功能 45
- 界面，OS Windows 47
- 界面，UNIX 50
- 连接类型 259
- 连接设置 261
- 目录组成，UNIX 50
- 目录组成，Windows 47
- 启动，UNIX 52
- 启动，Windows 49
- 日程 205
- 日志 181
- 设置 185
- 实时日志 178

Dr.Web服务器发现服务 34

G

GUS
- 手动更新 271

N

NAP Validator 285
- 设置 287

S

SRV协议 34

V

VDI 167

W

Web服务器 214
- 设置 214

[其它]

备份
- 服务器，创建 255
- 服务器，还原 270

策略
- 工作站连接 119
- 工作站设置 108

产品 24

创建
- 组 101

代理端
- 更新 278
- 功能 53
- 移动模式 278

代理端移动模式 278

代理服务器
- 高级设置 282
- 功能 279
- 启动、停止 282

登录
- Active Directory 83
- LDAP 84
- LDAP/AD 80
- PAM 82
- RADIUS 81
- 内部验证 80
- 外部验证 79
- 自动 71

反病毒扫描 140

反病毒扫描仪
- 启动 141

反病毒网络 259
- 病毒事件 266
- 创建 32
- 结构 75, 259
- 连接设置 261
- 组件 75

反病毒组件 137

服务器目录、组成，UNIX 50

服务器目录、组成，Windows 47

服务器日志 181

服务器实时日志 178

隔离区 156

更新
- Dr.Web Enterprise Security Suite 270
- 按日程 271
- 代理端 278
- 库 271
- 强制 271
- 手动 271
- 移动模式 278

索引

工作站 129
从组中删除 104
管理 119
还原 120
日程 129
扫描 129, 140
设置，复制 108
设置，继承 95
添加到组 104
统计信息 148
未批准的 119
卸载 120
新工作站 119
正在连接 119
组籍 105
工作站连接 119
公钥 40
功能
代理端 53
服务器 45
管理员
管理 85
权限 87
身份验证 79
组 86
管理中心
分层列表 60
工具面板 62
描述 54
属性面板 65
主菜单 55
管理中心语言 68, 90
还原
工作站 120
基组 95
加密
概述 35
界面
服务器，UNIX 50
服务器，Windows 47
管理中心 54
库
常规配置 235
更新 271
内容 242
详细配置 238
状态 234, 271
库加载器 273
连接，服务器间连接
类型 259
设置 261
流量
加密 35
压缩 35
组成 77
流量压缩 35
密钥
加密 40
试用 26
授权密钥 26
配置
Web服务器 214
服务器 185
启动
Dr.Web服务器，UNIX 52
Dr.Web服务器，Windows 49
强制更新 271
权限，管理员 87
任务计划器
服务器 205
工作站 129
日程
服务器 205
更新 271
工作站 129
扫描
手动 140
自动 129
扫描仪
反病毒 140
网络 72
设置
Web服务器 214
服务器 185
设置，复制 108
身份验证
Active Directory 83
LDAP 84
LDAP/AD 80
PAM 82
RADIUS 81
内部验证 80

索引

身份验证
  外部验证 79
试用密钥 26
手动更新库 271
授权 26
  扫描选项 26
授权管理器 170
授权密钥
  管理 135, 170
  获取 26
  在邻居服务器间分发 27
  自动更新 29
私钥 40
通知
  Web控制台 228
  模板 224
  日志 184
  设置 225
  向用户发送 160
统计信息
  服务器 254
  工作站 148
图标
  反病毒网络 60
  自定义钩子 222
未批准的工作站 119
系统要求 19
系统组 98
卸载
  工作站 120
  工作站，从组中 104
  组 102
新工作站 119
应用程序监控 244
  标准工作站 248
  测试模式 246
  功能分析 113
  禁止性方式 117
  禁止性规则 117
  可信任的应用程序 114, 248
  模式 110
  应用程序手册 251
  允许性方式 114
  允许性规则 114
预设组 98
找回
  管理员密码 91
证书 40
注册
  Dr.Web产品 26
  工作站于服务器 119
自动登录 71
组 98
  基 95
  删除工作站 104
  设置，复制 108
  设置，继承 95
  添加工作站 104
组件
  反病毒 137
  网络 75

© Doctor Web, 2022