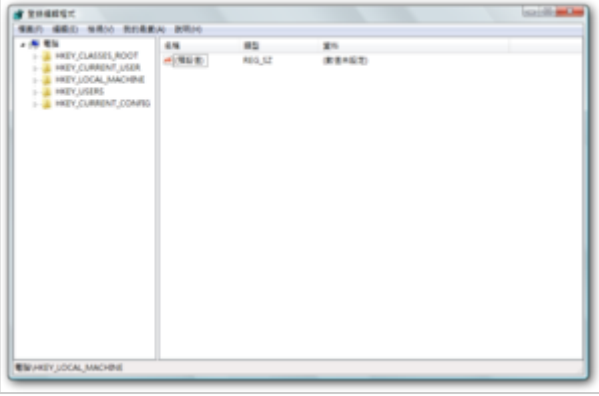
注册表

维基百科，自由的百科全书

中国大陆	注册表
台湾	登录档
港澳	登录档

注册表（Registry，台湾、港澳译作登录档，中国大陆译作注册表）是Microsoft Windows中的一个重要的数据库，用于存储系统和应用程序的设置信息。早在Windows 3.0推出OLE技术的时候，注册表就已经出现。随后推出的Windows NT是第一个从系统级别广泛使用注册表的操作系统。但是，从Windows 95开始，注册表才真正成为Windows用户经常接触的内容，并在其后的操作系统中继续沿用至今。



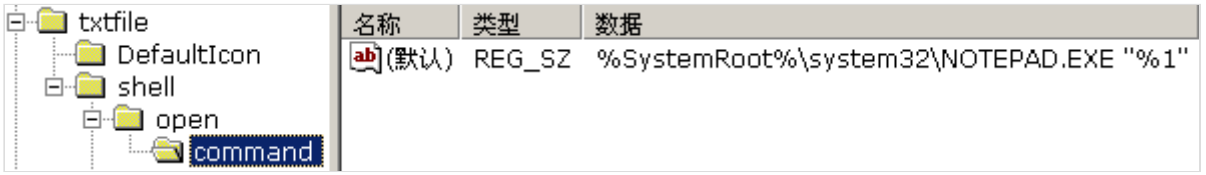
Windows Vista中的注册表编辑程序

目录

数据结构

注册表由键（key，或称“项”）、子键（subkey，子项）和值项（value）构成。一个键就是树状数据结构中的一个节点，而子键就是这个节点的子节点，子键也是键。一个值项则是一个键的一条属性，由名称（name）、数据类型（datatype）以及数据（data）组成。一个键可以有一个或多个值，每个值的名称各不相同，如果一个值的名称为空，则该值为该键的默认值。

在注册表编辑器（Regedit.exe）中，数据结构显示如下，其中，command键是open键的子键，(默认)表示该值是默认值，值名称为空，其数据类型为REG_SZ，数据值为%systemroot%\system32\NOTEPAD.EXE "%1



以上信息的意义是：txt类型的文件在右键菜单里的“打开”一项使用的程序是“NOTEPAD.EXE”，即用记事本打开文件。

数据类型

注册表的数据类型主要有以下五种：

显示类型（在编辑器中）	数据类型	说明
REG_SZ	字符串	文本字符串
REG_BINARY	二进制数	不定长度的二进制值，以十六进制显示
REG_DWORD	双字	一个 32 位的二进制值，显示为 8 位的十六进制值
REG_MULTI_SZ	多字符串	含有多个文本值的字符串，此名来源于字符串间用 nul 分隔、结尾两个 nul
REG_EXPAND_SZ	可扩充字符串	含有环境变量的字符串

此外，注册表还有其他的数据类型，但是均不常用：

- REG_DWORD_BIG_ENDIAN - DWORD 的大头版本，下面同理
- REG_DWORD_LITTLE_ENDIAN
- REG_FULL_RESOURCE_DESCRIPTOR
- REG_QWORD - DWORD 的四字（64 位）版本
- REG_FILE_NAME

注册表的分支结构

注册表有五个一级分支，下面是这五个分支的名称及作用：

名称	作用
HKEY_CLASSES_ROOT	存储Windows可识别的文件类型的详细列表，以及相关联的程序。
HKEY_CURRENT_USER	存储当前用户设置的信息。
HKEY_LOCAL_MACHINE	包括安装在计算机上的硬件和软件的信息。
HKEY_USERS	包含使用计算机的用户的信息。
HKEY_CURRENT_CONFIG	这个分支包含计算机当前的硬件配置信息。

注册表的存储方式

注册表的存储位置随着Windows的版本变化而不同。尤其是Windows NT系列操作系统和Windows 95系列的存储方式有很大区别。注册表被分成多个文件存储，称为Registry Hives，每一个文件被称为一个配置单元。

在早期的Windows 3.x系列中，注册表仅包含一个reg.dat文件，所存放的内容后来演变为HKEY_CLASSES_ROOT分支。

Windows NT家族的配置单元文件：

名称	注册表分支	作用
SYSTEM	HKEY_LOCAL_MACHINE\SYSTEM	存储计算机硬件和系统的信息
NTUSER.DAT	HKEY_CURRENT_USER	存储用户参数选择的信息（此文件放置于用户个人目录，和其他注册表文件是分开的）
SAM	HKEY_LOCAL_MACHINE\SAM	用户及密码的数据库
SECURITY	HKEY_LOCAL_MACHINE\SECURITY	安全性设置信息
SOFTWARE	HKEY_LOCAL_MACHINE\SOFTWARE	安装的软件信息
DEFAULT	HKEY_USERS\DEFAULT	缺省启动用户的信息
USERDIFF	HKEY_USERS	管理员对用户强行进行的设置

- 假设Windows安装于C盘，则在Windows XP以前，文件存放于C:\WINNT\SYSTEM32\CONFIG，而XP及以后则存放于C:\WINDOWS\SYSTEM32\CONFIG

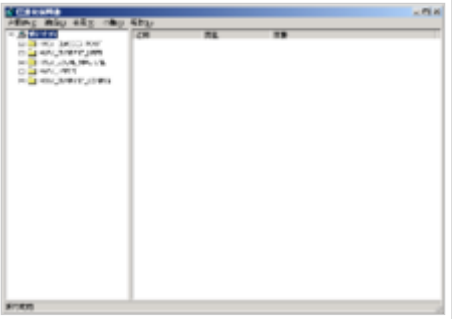
Windos95家族的配置文件

名称	注册表分支	作用
CLASSES	HKEY_CLASSES_ROOT	存储软件组件库有关信息
USER.DAT	HKEY_USERS	存储用户参数选择的信息
SYSTEM.DAT	HKEY_LOCAL_MACHINE	系统信息

编辑注册表

使用注册表编辑器

Microsoft公司不建议用户自行更改注册表，因为如果对注册表进行了不当修改，就有可能造成Windows系统的某些功能失效，甚至导致系统崩溃。但是，Microsoft公司仍然在Windows中提供了注册表编辑器，它位于%systemroot%\regedit.exe。在Windows NT中使用的则是界面有所不同的REGEDT32.exe。而在Windows 2000中，两个程序同时存在于系统中。部分的原因是Windows 2000版本的regedit.exe尚不支持对注册表数据设置安全性。但在Windows XP及以后的操作系统中，regedit.exe已经能够支持注册表安全设置了，因此REGEDT32.exe失去了存在的必要。不过它仍被保留，只是该程序执行时仅仅会自动调用regedit.exe[1]。



在Windows 2000下的注册表编辑器截图

除了编辑本台计算机上注册表数据之外，注册表编辑器亦可以通过文件菜单下的“加载配置单元”菜单项编辑直接编辑文件系统上的注册表数据文件。该功能可以允许用户打开文件系统中的RegHive文件，并将其中的数据映射到HKEY_USERS或者HKEY_LOCAL_MACHINE项下的一个子项之中。[2]

使用脚本

在Windows 98以后的操作系统中，增加了一个脚本语言解释器，可以用来执行一些系统任务。它可以支持VBScript和JavaScript两种脚本语言，都提供了访问注册表的功能。某些病毒就利用这一点通过修改注册表进行传播。

使用第三方或自行编写的软件

访问注册表的系统功能对编程人员是开放的，因此有许多软件都有读写注册表的功能。事实上，Windows平台下开发的软件几乎都在不同程度上修改注册表，以便保存一些在程序多次运行之间需要保留的信息，以及让软件可以通过某种特定方式（例如，右键菜单）启动。也有一些软件是专门开发出来对注册表进行优化和设置的。

使用reg文件

reg文件也是一种修改注册表的方式。在注册表编辑器中，用户可以通过“文件”菜单中的“导出”菜单项来备份注册表中的某些项目到一个reg文件之中；之后用户可以再次通过“导入”菜单项将这些项目还原。reg文件本身也在系统中被关联到regedit.exe，因此直接双击打开reg文件也会起到将其中的项目导入到注册表中的效果。

而事实上，reg文件是根据一定格式编写的纯文本文件。因此，熟练的用户可以直接使用文本编辑器（比如记事本）来创建自己的reg文件，这样做无需在注册表中根据路径一级一级地访问，而且可以直接对大量项目进行批量修改。这些文件还可以被分发给非专业的用户，帮助他们快速地完成注册表的编辑，以减少出错的可能。

Registry APIs

Windows SDK提供了访问注册表的接口。创建或打开的键，必须作为当前已经打开的键的子键。HKEY_LOCAL_MACHINE, HKEY_CLASSES_ROOT, HKEY_USERS, HKEY_CURRENT_USER等预定义的键总是已经打开。使用RegOpenKeyEx打开键；使用RegCreateKeyEx创建键。注册表允许最大512层子键深度。通过一个注册表API调用允许一次打开或创建32层深度的注册表的子键。 RegCloseKey关闭已经打开的键，把数据写回注册表。RegFlushKey把内存中缓存的注册表已修改数据写回到硬盘上，因此代价高昂，要慎重调用。

RegSetValueEx把一个值项与其数据关联到一个键上。RegDeleteVaule从键上删除一个值项。RegDeleteKey删除一个键，但直到关闭相应的注册表句柄（handle）才真正完成删除操作。

RegEnumKeyEx枚举一个键下的所有子键。RegEnumValue枚举一个键下的所有值项。RegQueryValueEx获取一个值项的数据。

RegSaveKeyEx可以把一个键及所有子键保存到一个文件中。RegLoadKey把一个注册表文件装入到系统的注册表，RegUnLoadKey把系统注册表恢复到原状态。

历史

前身

最初，Windows系统及应用程序的信息被存储在后缀名为ini的文本文件中，这就是注册表的前身。但是这么做有着致命弱点：因为每一个程序都会新安装一个或多个ini文件，来存储程序信息，导致信息的分布极为零乱；而且在16位系统下，ini文件的大小必须在64KB之内。所以ini文件被认为不便于使用和管理。

发布与发展

在最早出现于Windows 3.0的OLE技术出现后，微软为了存放系统中大量的软件组件信息，组织了一个reg.dat的数据库来存放这些信息。当时的注册表编辑器为16位版本的regedit.exe，功能较弱。

后来开发的Windows NT则更进一步使用相同的文件格式来存放系统的配置信息，以替换原有的ini文件。该系统为每一个用户在用户目录下创建了一个自身的注册表空间，而系统的设置被存放在系统文件夹中。由于Windows NT是一个32位操作系统，regedit.exe被升级为regedt32.exe，并增加了对权限的设置功能。

在Windows 95中，注册表首次得到广泛应用，逐渐淘汰了原有的ini文件。程序在安装时，不再将数据写入ini文件，而直接写入注册表。为了最大限度兼容旧程序，部分原来用于读写ini文件的专门API函数仍然可用，但现在是访问注册表(写入或读取）。Windows 95为了保持和Windows 3.x系列的兼容性，注册表的架构与Windows NT不同，为此专门开发了另一个32位版本的regedit.exe，它没有设置权限的功能。

在Windows 2000中，由于Windows 95家族已经深入人心，regedit.exe也得到广泛应用，相反regedt32.exe的界面相对比较丑陋，因此微软将windows 95系列的regedit.exe拿过来用。但由于移植过来的regedit.exe仍没有权限设置的功能，regedt32.exe仍然保留在系统中用作权限设置。

到Windows XP和Windows Server 2003中，regedit.exe已经增加了权限的功能，regedt32.exe由于失去作用而被剔除。同时，这个版本的注册表是64位的，这导致了一些兼容性问题，少数可以运行在旧版本Windows的程序在Windows XP中无法运作。

64位Windows的注册表

64位Windows中的注册表结构大致与32位版本相同，但32位程序的信息被放在HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node而不是HKEY_LOCAL_MACHINE\SOFTWARE（64位程序的信息放于此处）。

分散与集中之争

关于分散的文本文件和集中的注册表两种软件配置方式的优劣，目前仍有争论。主流操作系统中，Linux操作系统一直使用单独的文本文件来存放配置信息。而Windows平台下基于.NET框架的软件对注册表的依赖性也大大减弱。事实上，.NET软件通常使用纯文本的XML（称为app.config）文件而不是注册表进行配置，这在某种意义上是向当初的ini文本配置方式的一种回归。部分绿色软件支持者认为，集中式的注册表要求软件需要进行专门的安装步骤才可以正常运行，而单独的文本配置文件则可以不需要安装，只要将软件的文件目录拷贝

过来就可以使用；当不再需要软件的时候，除删除相关文件外对于注册表也需要进行卸载步骤，才有可能不在系统中留下痕迹（很多软件即使提供了卸载步骤，仍然会留下痕迹），如果使用文本配置文件，则能做得更干净。但是，文本配置方式导致某些系统软件的配置较为困难且缺乏统一的界面（如Linux中的情况），也是不争的事实，尽管现在已经有很多软件可以方便进行系统配置，但仍存在标准不够统一的问题。

著名开源软件Fetchmail的作者Eric S. Raymond在《UNIX编程艺术》一书中有如下叙述[3]：

> 对比terminfo数据库和Windows注册表，我们发现注册表出名地容易受到错误代码的破坏。这可能会使整个系统都无法使用。即使系统没有瘫痪，但如果破坏本身干扰了专用的注册表编辑工具，恢复工作就会很困难。

从2000年以来部分恶性病毒如熊猫烧香等的破坏情形看，的确存在“破坏本身干扰注册表编辑器”的问题。在某些情况下，病毒程序会监视系统进程列表，并强行关闭名为regedit的任何程序。这使得受损用户难以直接通过编辑注册表进行恢复。

注册表是Windows操作系统的核心，越来越多的黑客程序将攻击对象转向了注册表。一些程序（尤其是恶意程序），为了达到随系统自动启动的目的，会在注册表创建启动项，因此监控注册表能够有效地预防该类恶意程序的攻击。[4]

风险

不当使用“注册表编辑器”可能会造成严重的问题，甚至可能需要重新安装操作系统。无法保证能够顺利解决因不当使用“注册表编辑器”所造成的问题。您必须自行承担使用“注册表编辑器”的风险。建议您在编辑登录前，先行备份。

注释

1. ^ Regedit.exe 和 Regedt32.exe 的区别. Microsoft Knowledge Database. Microsoft Corporation. [2015-12-03].
2. ^ 将配置单元加载到注册表. Microsoft TechNet库. Microsoft Corporation. 2005-01 [2013-01-08].
3. ^ 此段文字来自该书简体中文版，繁体版的具体译文可能不同于此。
4. ^ 注册表监控 (http://bingoworks.net/article/10052/the-monitoring-program-source-code-of-registry-based-on-the-dot-net)

参考资料

- Windows XP专业版从入门到精通（中文版），Mark Minasi著，王珺、屈马珑等译，ISBN 7-5053-7569-5
- Unix编程艺术（简体中文版），Eric S. Raymond著，姜宏 何源 蔡晓俊 译，电子工业出版社 ISBN 7-121-02116-1

参见

- Microsoft Windows

取自“https://zh.wikipedia.org/w/index.php?title=注册表&oldid=41771622”
