第 3 章

Windows 系统安全

本章导读

Windows 系统管理员应依据业务需要对 Windows 系统安全进行配置与管理。首先，系统管理员应精通 Windows 日志分类以及筛选方法，并能够根据日志信息筛选出安全隐患，及时防护以确保系统数据安全。其次，注册表在 Windows 系统中是很重要的，特别是 reg 命令的应用，应该根据业务需求进行注册表的管理。最后，Windows 防火墙是 Windows 操作系统的重要防护工具，Windows 系统管理员应该妥善掌握防火墙功能，修改入站和出站规则，以达到防护目的。

学习目标

知识目标	• 了解 Windows 日志的分类和作用，并能够说出日志事件状态分类； • 掌握日志安全设置和筛选方法； • 熟悉注册表作用，并能够说出注册表的结构以及根键分类； • 熟悉防火墙的作用，能够说出高级安全防火墙工作过程。
技能目标	• 掌握对 Windows 日志的安全设置和筛选方法； • 掌握注册表管理方法，能够对注册表进行导入、导出以及备份操作； • 掌握防火墙的入站与出站规则的设置方法。

3.1 Windows 日志

Windows 日志简介

3.1.1 Windows 日志简介

Windows 系统日志是记录系统中硬件、软件和系统问题的信息，同时还可以监视系统中发生的事件。在处理应急事件时，客户需要为其提供溯源，这些日志信息在取证和溯源

中都扮演着重要角色，用户可以通过日志来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹。Windows Server 2016 系统主要提供了三类日志来记录系统事件。

（1）系统日志。记录由 Windows 系统组件生成的事件，这些事件通常由系统文件或设备驱动程序生成，包含了启动、关机、服务启动和硬件故障等信息。默认位置为 %SystemRoot%、System32、Winevt、Logs、System.evtx。

（2）应用程序日志。记录应用程序或系统程序生成的事件。例如，数据库应用程序可以在应用程序日志中记录文件错误，程序开发人员可以自行决定监视哪些事件。如果某个应用程序崩溃，那么可以从应用程序日志中找到相应的记录。默认位置为 %SystemRoot%、System32、Winevt、Logs、Application.evtx。

（3）安全日志。记录与系统安全相关的事件，包含各种类型的登录日志、对象访问日志、进程追踪日志、特权使用、账号管理、策略变更、系统事件。安全日志也是调查取证中常用的日志。默认设置下，安全日志是关闭的，管理员可以使用组策略启动安全日志，或者在注册表中设置审核策略，以便当安全日志满后使系统停止响应。默认位置为 %SystemRoot%、System32、Winevt、Logs、Security.evtx。

Windows 日志将记录事件的 5 种状态。

（1）信息（Information），表明应用程序、驱动程序或服务成功操作。

（2）警告（Warning），表明事件可能会导致问题，一般是潜在或需注意的情况，通常不会立即导致系统故障。例如，当磁盘空间不足或未找到相应程序时，都会记录一个警告事件。

（3）错误（Error），错误事件指用户应该知道的重要问题，通常指功能和数据的丢失。例如，一个服务不能作为系统引导被加载，那么它会产生一个错误事件。

（4）成功审核（Success Audit），与失败审核同是安全日志中的特别事件状态，表明成功审核安全访问尝试，如用户成功登录 / 注销、对象成功访问、特权成功使用、账户成功管理、策略成功更改等。例如，所有成功登录系统的事件都会被记录为成功审核事件。

（5）失败审核（Failure Audit），失败审核事件会记录失败的操作。例如，用户试图访问网络驱动器失败，则该尝试会被记录为失败审核事件。

Windows 日志中记录的信息中，主要包含事件的级别、记录时间、来源、事件 ID、关键字、用户、计算机、操作代码及任务类别等，如图 3-1 所示。

图 3-1　事件日志信息

事件 ID 作为 Windows 日志分析的要素之一，每一个独特的标识都承载了特定的含义。在繁杂的事件中，事件 ID 发挥着举足轻重的筛选作用，日志筛选过程均以其为基准。常见事件 ID 如表 3-1 所示。

表 3-1　常见事件 ID

事　件　ID	事 件 类 型	描　　述
4608，4609，4610，4611，4612，4614，4615，4616	系统事件	本地系统进程，如系统启动、关闭和系统时间的改变
4612	清除的审核日志	所有的审核日志清除事件
4624	用户成功登录	所有的用户登录事件
4625	登录失败	所有的用户登录失败事件
4634	用户成功退出	所有的用户退出事件
4656，4658，4659，4660，4661，4662，4663，4664	对象访问	当访问一给定的对象（文件、目录等）访问的类型（例如读、写、删除），访问是否成功或失败，谁实施了这一行为
4719	审核策略改变	审核策略的改变
4720，4722，4723，4724，4725，4726，4738，4740	用户账户改变	用户账户的改变，如账户创建、删除、修变密码等
4727~4737，4739~4762	用户组改变	对一个用户组所做的所有改变，例如添加或移除一个全局组或本地组，从全局组或本地组添加或移除成员等
4768，4776	验证用户账户成功	当一个域用户账户在域控制器成功认证时，生成用户账户成功验证事件
4771，4777	验证用户账户失败	当一个域用户账户在域控制器尝试认证但失败时，生成用户账户验证失败事件
4778，4779	主机会话状态	会话重新连接或断开

表 3-1 中事件 ID 是 4624 对应的事件就是用户成功登录，属于所有用户登录事件。登录事件还包括登录的类型，根据登录类型可以判断黑客登录计算机的具体方式，部分登录事件类型如表 3-2 所示。

表 3-2　部分登录事件类型

登录类型	类 型 名 称	描　　述
2	Interactive	交互式登录（用户从控制台登录）
3	Network	用户或计算机从网络登录到本机。例如，使用 net use 访问网络共享，使用 net view 查看网络共享等
4	Batch	批处理登录类型，无需用户的干预
5	Service	服务控制管理器登录
7	Unlock	用户解锁主机
8	NetworkCleartext	用户从网络登录到此计算机，用户密码用非哈希的形式传递
10	RemoteInteractive	远程交互，使用终端服务或远程桌面连接登录

3.1.2 Windows 日志管理

在 Windows Server 2016 系统中，审核策略默认处于未启用状态。然而，出于系统安全性和故障排查的考虑，强烈建议启用审核策略。通过启用审核策略，可以在系统出现故障或安全事故时，利用系统日志文件进行详细分析，迅速排除故障并追查入侵者的相关信息。这样不仅能够增强系统的安全性，还能提高故障处理的效率。

1. 开启审核策略

可以通过以下操作步骤开启审核策略。

第一步，在服务器管理器的仪表板中选择“工具”选项卡，在下拉列表中选择“本地安全策略”管理工具。打开“本地安全策略”窗口后，在左侧选择“安全设置”下的“本地策略”，接着单击“审核策略”，在右侧选择具体策略双击进行设置。

第二步，打开“审核策略更改属性”窗口，在审核这些操作中选择“成功”“失败”或者两者都选，然后单击“应用”和“确定”按钮。打开“事件查看器”窗口，选择“Windows 日志”，右击“应用程序”，选择“属性”，设置合理的日志属性，即日志最大大小、事件覆盖阈值等，如图 3-2 所示。

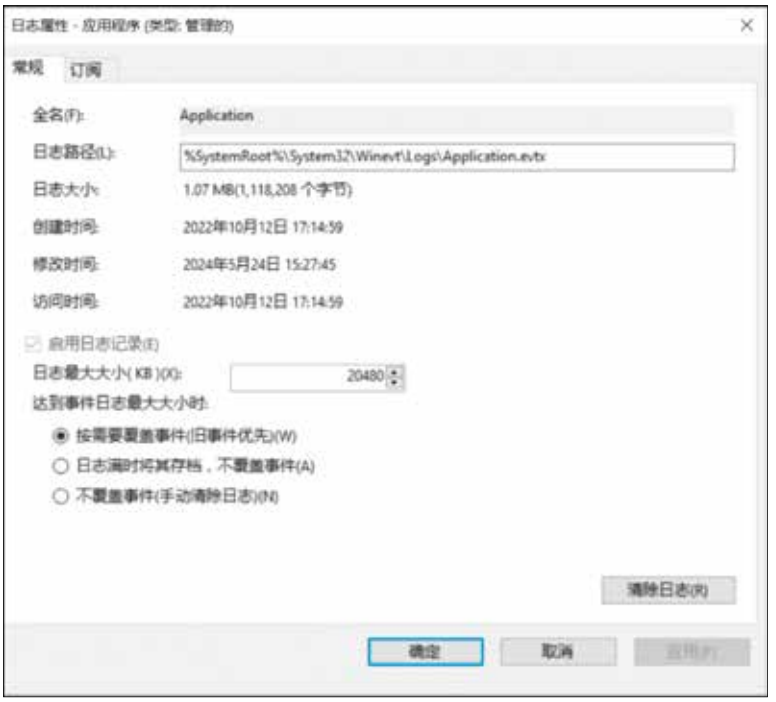

图 3-2　设置日志大小

系统内置的三个核心日志文件（System.evtx、Security.evtx 和 Application.evtx）默认大小均为 20480KB（20MB）。当记录的事件数据超过 20MB 时，默认系统将优先覆盖过期的日志记录。其他应用程序及服务日志默认最大为 1024KB，超过最大限制时也会优先覆盖过期的日志记录。

2. 查看系统日志

通过“事件查看器”窗口可打开一个列表，该列表记录了 Windows 的所有日志条目，每个条目包括关键字、日期和时间、来源、事件 ID、任务类别。

筛选登录失败事件。在事件查看器窗口中单击“安全”选择“筛选当前日志”，或者右击“安全”选择“筛选当前日志”，如图 3-3 所示。

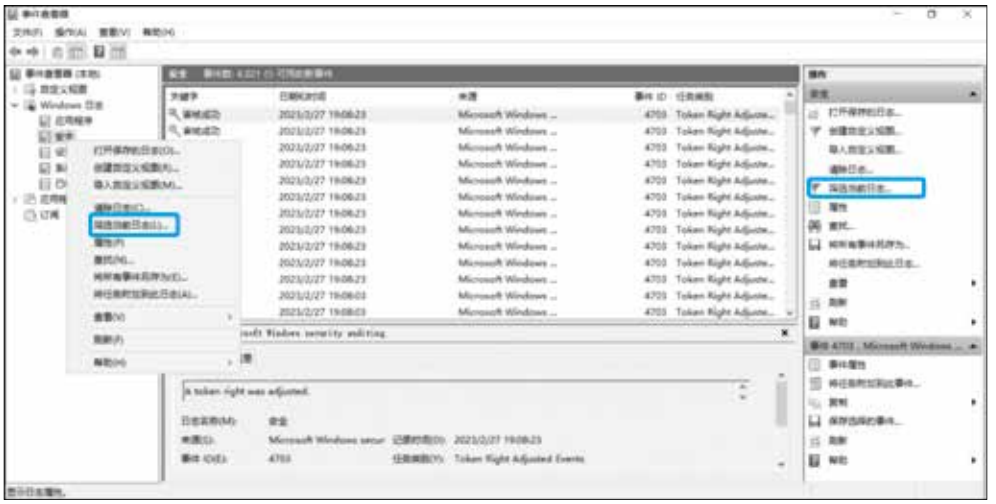

图 3-3　筛选当前日志

在打开“筛选当前日志”窗口后，在输入事件 ID 文本框中输入 4625，单击“确定”按钮，筛选出登录失败事件，如图 3-4 所示。

图 3-4　输入事件 ID

从筛选结果中可以发现，在 18:28 连续两次存在登录失败的情况，该事件有可能是入侵者在渗透 Windows 系统账户密码，需对该事件进行详细查看，如图 3-5 所示。

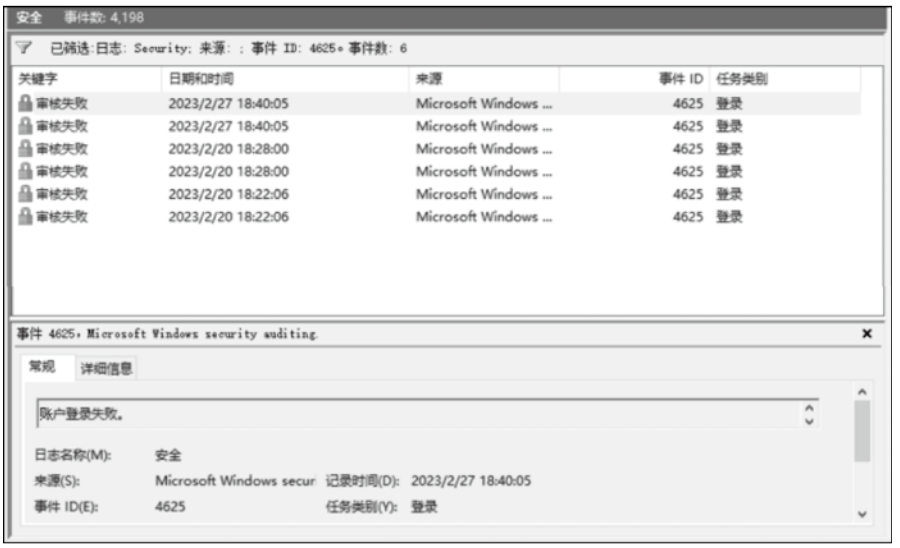

图 3-5　筛选结果

双击该事件，查看详细信息，可以发现该事件类型号为 5，属于服务控制管理器登录，说明是用户直接登录该主机。还可以通过详细信息查看 IP 地址，主机名等信息，如图 3-6 所示。可以通过在高级防火墙进站策略中添加白名单方式，禁止异常信息中的 IP 地址连接主机。

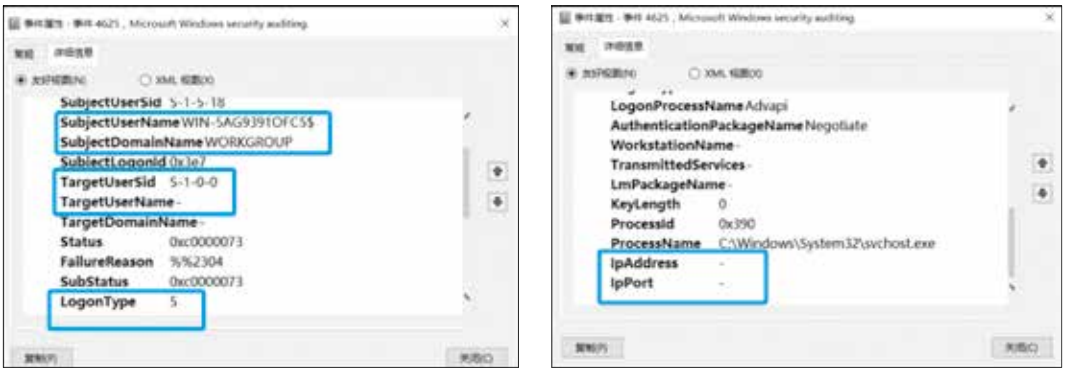

图 3-6　登录失败事件

3.2 注册表安全

注册表安全

3.2.1 注册表简介

Windows 操作系统中注册表是一个经过细致规划与良好组织的数据库，包括操作系统、硬件、应用程序以及用户有关的各类配置信息。注册表中的内容随时都在与系统、硬件、应用程序以及用户进行着交互。当以下几种情况发生时，系统会自动访问注册表内容。

（1）在系统引导过程中，引导加载器读取配置数据和引导设备驱动程序的列表，以便在初始化内核以前将它们加载到内存中。由于配置数据存储在注册表的配置单元中，因此在系统引导过程中需要通过访问注册表来读取配置数据。

（2）在内核引导过程中，内核会从注册表中读取以下信息：需要加载哪些设备驱动程序、各个系统部件如何进行配置，以及如何调整系统的行为。

（3）在用户登录过程中，系统会从注册表中读取每个用户的账户配置信息，包括桌面背景和主题、屏幕保护程序、菜单行为和图标位置、随系统自启动的程序列表、用户最近访问过的程序和文件，以及网络驱动器映射等。

（4）在应用程序启动过程中，应用程序会从注册表中读取系统全局设置，还会读取针对每个用户的个人配置信息，以及最近打开过的程序文件列表。

除了以上列出的注册表被系统或程序自动访问的几种情况外，系统和程序还可能在任何时间访问注册表。例如，有些应用程序可能会持续监视并获取注册表中有关程序配置信息的更新，以便随时将程序的最新配置信息作用于该程序。

除了从注册表中获取系统、程序或用户的配置信息外，注册表中的内容也会在特定情况下自动被系统修改，包括但不限于以下三种情况。

（1）在安装设备驱动程序时，系统会在注册表中创建与硬件配置有关的数据。当系统将资源分配给不同设备以后，系统可以通过访问注册表中的相关内容来确定在系统中安装了哪些设备以及这些设备的资源分配情况。

（2）安装与设置应用程序时，系统会将应用程序的安装信息以及程序本身的选项设置保存到注册表中。

（3）在使用控制面板中的选项更改系统设置时，系统会将相应的配置参数保存到注册表中。

无论用户是否主动编辑注册表，Windows 系统中的许多操作与注册表关系密切。如有必要，用户可以随时编辑注册表。

Windows 系统提供了多种用于编辑注册表的工具，可分为图形界面和命令行两种类型。图形界面的注册表编辑工具主要包括控制面板、组策略以及注册表编辑器。命令行工具指的是命令提示符窗口。

用户在控制面板中对系统进行的各种设置，实际上是在修改注册表中的特定内容。使用控制面板设置系统选项，既可以简化用户的设置过程，也可以避免由用户对注册表直接进行编辑而可能导致的错误，但通过这种方式访问的注册表内容非常有限。

另一个可以编辑注册表内容的图形化工具是组策略，组策略没有控制面板直观，但能访问数量更多的系统选项，而且还可以针对特定计算机或用户进行设置。总体而言，组策略可以对系统实施更强大且灵活的控制。

Windows 注册表基本架构是带有多个配置层面的分层结构。这些层面是通过根键、子键、键值和数据组成。

在 Windows 注册表中，根键位于结构的顶层，根键下包含多个子键。子键可以分为多个不同的层级，这意味着子键下还可以包含子键。每个子键可以包含一个或多个键值，也可以没有键值。键值作为子键的参数，为其提供实际的功能。为了发挥键值的作用，每个键值必须包含由系统或用户指定的数据。数据分为多种不同的类型，从而可以根据需要

存储不同类型的内容，如图 3-7 所示。

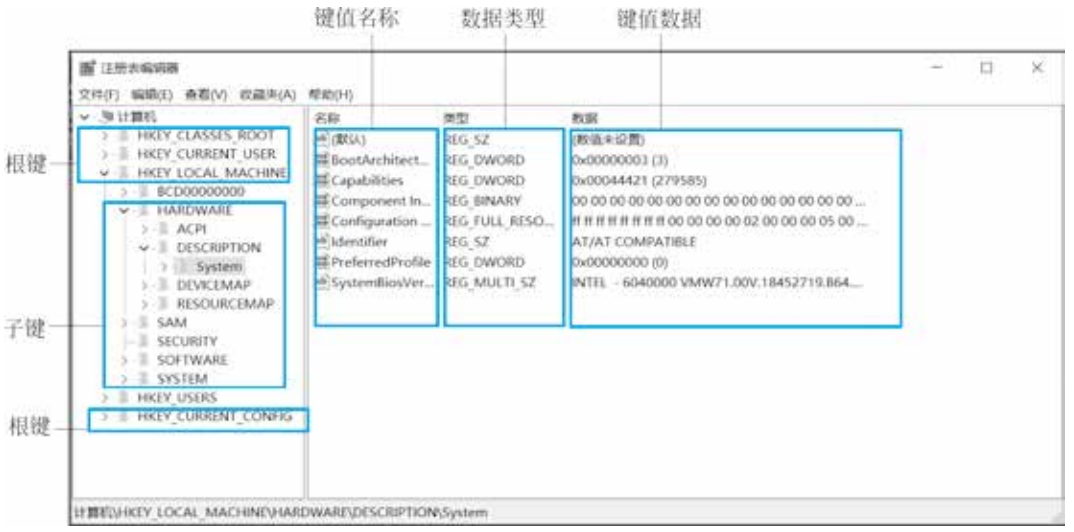

图 3-7　注册表结构

Windows 注册表包含 5 个根键，位于注册表的最顶层，这 5 个根键的名称和功能如表 3-3 所示。用户不能添加新的根键，也不能删除这 5 个根键或修改它们的名称。

表 3-3　根键名称及功能

根 键 名 称	功　　能
HKEY_CLASSES_ROOT	存储文件关联和组件对象模型的相关信息，如文件扩展名与应用程序之间的关联
HKEY_CURRENT_USER	存储当前登录系统的用户账户的相关信息
HKEY_LOCAL_MACHINE	存储 Windows 系统的相关信息，如系统中安装的硬件、应用程序以及系统配置等内容
HKEY_USERS	存储系统中所有用户账户的相关信息
HKEY_CURRENT_CONFIG	存储当前硬件配置的相关信息

子键位于根键下方，每个根键可以包含一个或多个子键，子键中也可以包含子键，这种组织方式类似于文件夹和子文件夹的嵌套关系。很多子键是 Windows 系统自动创建的，用户也可以根据需要手动创建新的子键。

注册表中的每个根键或子键都可以包含键值。当在注册表编辑器中选择一个根键或子键后，会在右侧窗口显示一个或多个项目，这些项目就是所选根键或子键包含的键值。无论是系统还是用户创建的子键，都会包含一个名为“(默认)”的键值。键值由名称、类型和数据三部分组成，总是按“名称”“类型”“数据”这种固定顺序显示。键值数据是指键值中包含的数据，键值数据分为多种不同的数据类型，比如字符串（REG_SZ）、二进制（REG_BINARY）、Dword 值（REG_QWORD）。

无论在注册表编辑器中选择根键还是子键，都会在注册表编辑器底部的状态栏中显示当前选中的根键或子键的完整路径，其格式类似于文件资源管理器中文件夹的完整路径的

表示方法，如图 3-8 所示。

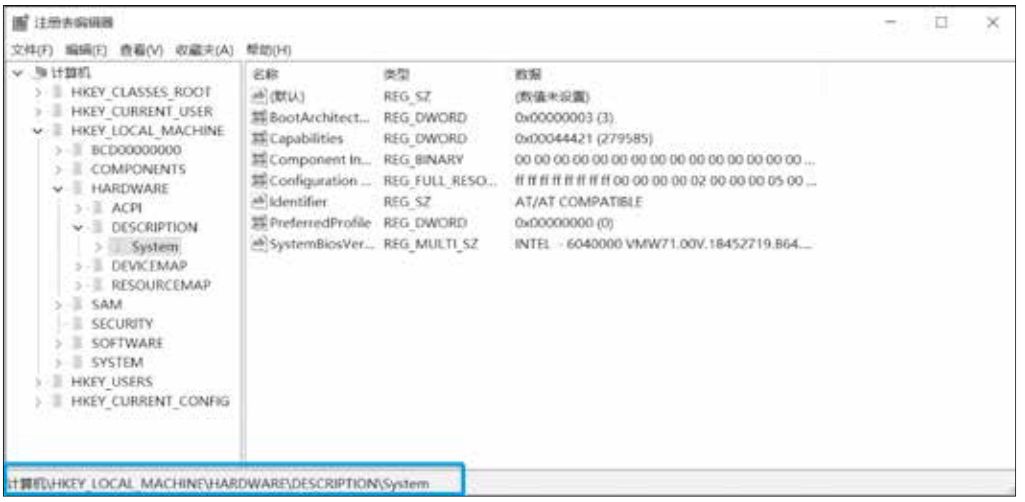

图 3-8　根键 / 子键完整路径

3.2.2 注册表管理

1. 使用图形界面工具管理注册表

在计算机中，注册表是一个重要的数据仓库，用于存储 Windows 操作系统的配置信息、硬件设置、用户偏好以及其他重要数据。由于其关键性和复杂性，注册表的管理显得尤为关键。使用图形界面工具来管理注册表不仅方便、直观，而且实用，普通用户也能轻松地对注册表进行管理和维护，从而提高系统的稳定性和性能。当然，在使用过程中仍需保持谨慎和警惕，确保操作的正确性和安全性。

1）启动注册表编辑器

注册表编辑器提供了专门用于查看、编辑与管理注册表的工具，可以使用以下两种方法启动注册表编辑器。

第一种方法是通过按下 Win+R 组合键打开“运行”对话框，输入 regedit 命令然后按 Enter 键。第二种方法是通过在服务器管理器的仪表板中选择“工具”下拉框，在下拉框中选择“系统配置”，打开“系统配置”窗口后，选择“工具”选项卡，单击“注册表编辑器”，然后单击“启动”按钮即可。

2）备份注册表

启动注册表编辑器后，如果需要对注册表进行备份，可以在注册表编辑器中单击“文件”，然后选择“导出”命令，如图 3-9 所示。在打开的“导出注册表文件”窗口中，选择注册表的保存位置并设置好保存的文件名，然后单击“保存”按钮即可。

为了保证导出的注册表的安全以及方便以后恢复，需要把注册表放在一个安全的目录下，并以保存时的日期对注册表进行编号保存。

使用上面的方法可以导出整个注册表文件，但保存过程耗时较长，文件占用空间也较大。如果只想单独保存注册表的某个分支，可以右击该分支，单击“导出”按钮。

图 3-9　将注册表全部导出

3）还原注册表

在打开的注册表编辑器窗口中，选择“文件”菜单中的“导入”命令，选择以前备份过，本次要还原的注册表文件，单击“打开”按钮即可，如图 3-10 所示。

⚠ **注意：** 注册表还原后一般需要重新启动计算机，注册表的配置信息才能生效。

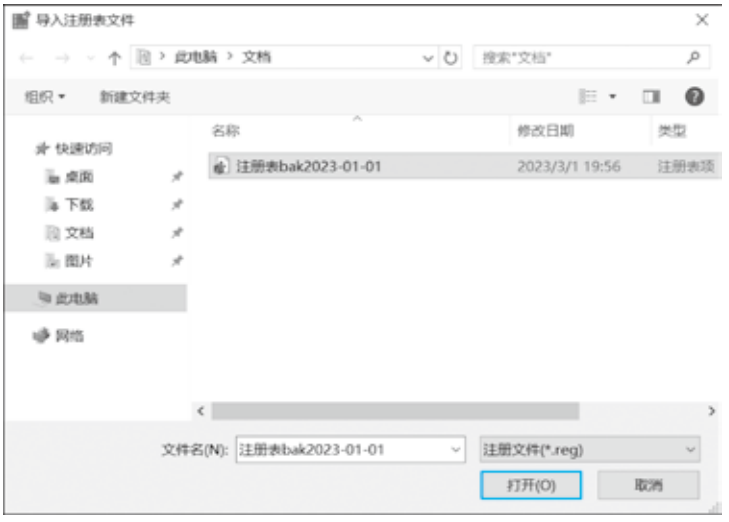

图 3-10　图形界面导入注册表

2. 使用命令行工具管理注册表

除了可以通过图形界面工具管理注册表外，利用 reg 命令同样可以实现对注册表的增加、删除以及修改等操作。reg 命令也被称为控制台注册表编辑器，其默认文件路径位于 C:\Windows\System32\reg.exe。

1）创建注册表

在 DOS 界面输入 reg add 命令创建注册表，具体操作如下：

```
reg add hkcu\ceshireg /v test /t reg_sz /d "这是一个测试注册表键值!" /f
```