Windows实验 - 了解进程、线程、句柄和 Windows 注册表

1. 目标

在本实验中，同学们将使用 SysInternals Suite 中的进程资源管理器了解进程、线程和句柄。同学们还将使用 Windows 注册表更改设置。

第 1 部分：了解进程

第 2 部分：了解线程和句柄

第 3 部分：了解 Windows 注册表

1. 所需资源

* 1 台接入互联网的 Windows PC

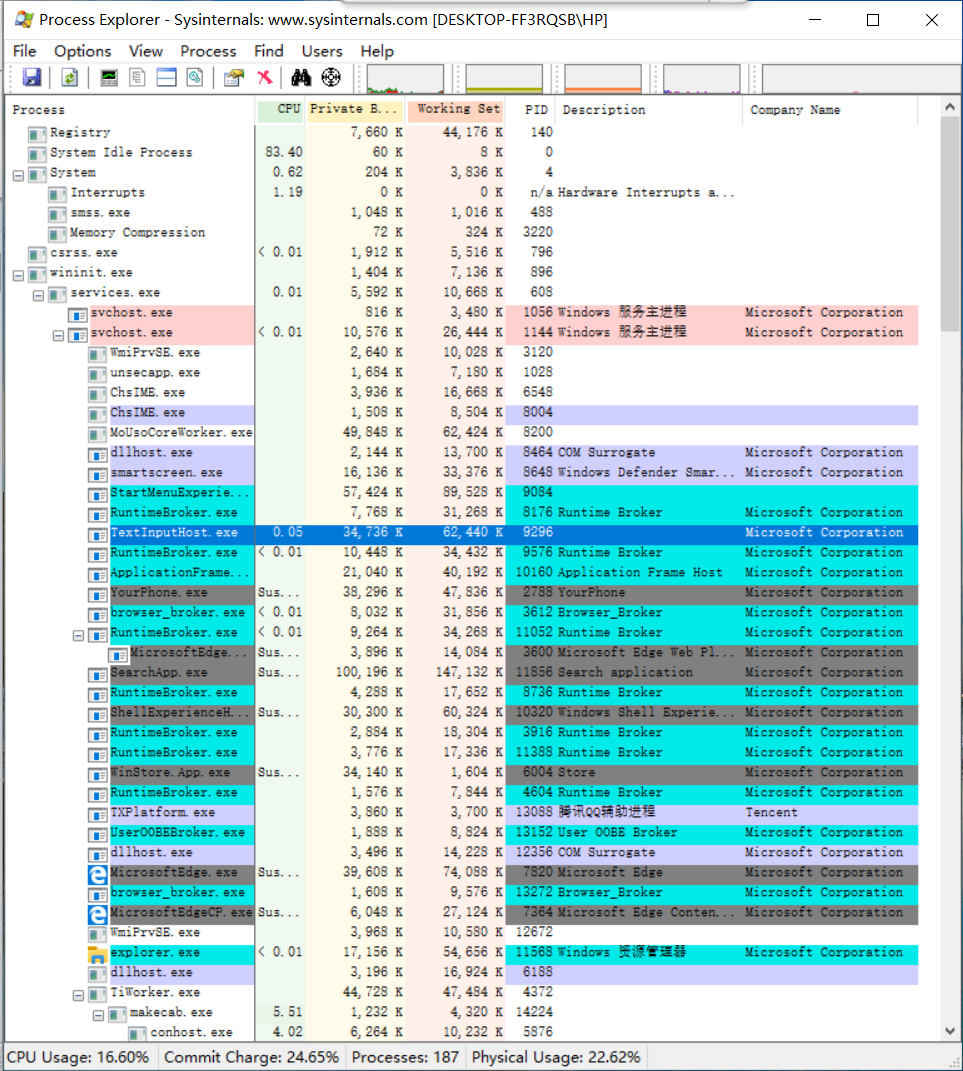
1. 了解进程

在这一部分，同学们将了解进程的相关知识。进程是指正在执行的程序或应用。同学们将使用 Windows SysInternals Suite 中的进程资源管理器了解进程。同学们还将启动和观察新进程。

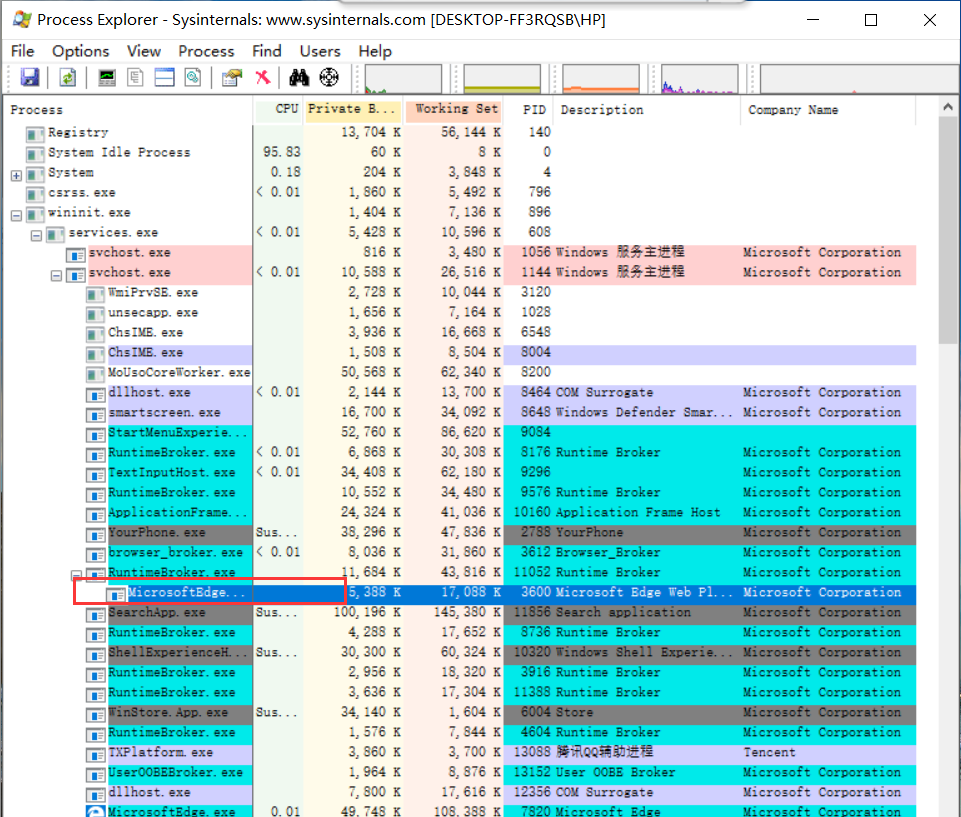
* 1. 下载 Windows SysInternals Suite。
     1. 导航到下面的链接，下载 Windows SysInternals Suite：

<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

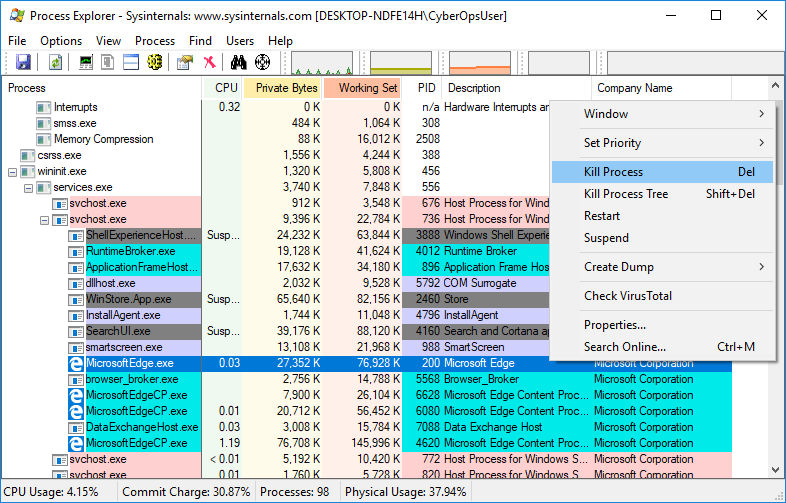
* + 1. 完成下载后，从文件夹提取文件。
    2. 在 Web 浏览器保持打开的情况下，执行下面的步骤。
  1. 了解活动的进程。
     1. 导航到包含所有解压文件的 SysinternalsSuite 文件夹。
     2. 打开 **procexp.exe**。系统提示时，接受《进程资源管理器许可协议》。
     3. 进程资源管理器显示当前活动进程的列表。



* + 1. 要找到 Web 浏览器进程，请将“查找 Window 的进程”图标 () 拖动到已打开的 Web 浏览器窗口中。此示例中使用的是 Microsoft Edge。



* + 1. 同学们可以在 Process Explorer 中终止 Microsoft Edge 进程。右键点击选定的进程，然后选择**终止进程**。

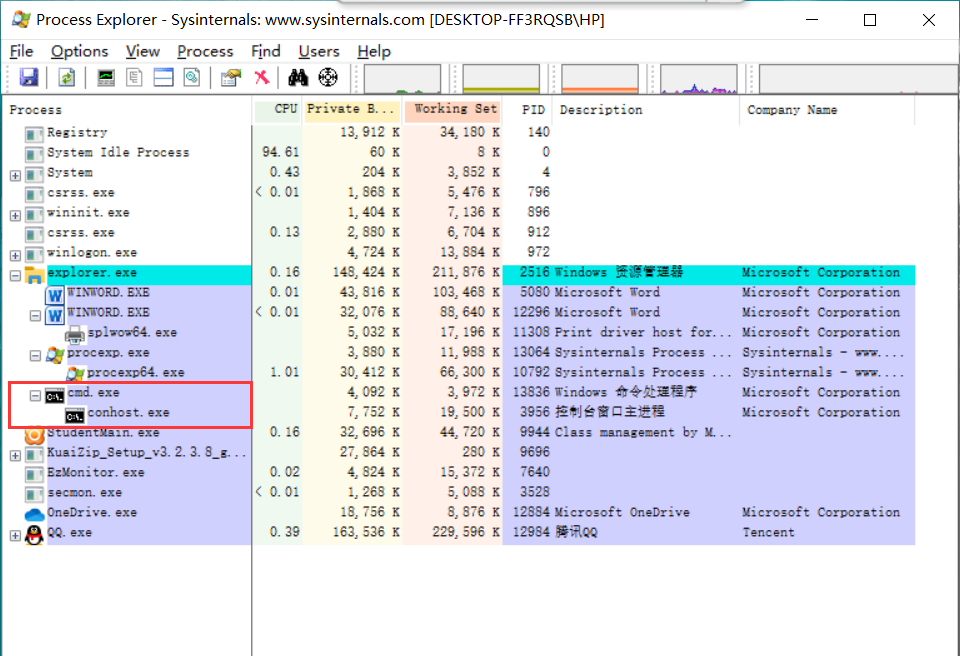


终止进程后，Web 浏览器窗口会发生什么情况？

答：web浏览器窗口被关闭。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. 启动另一个进程。
     1. 打开命令提示符。（依次点击**开始** > 搜索**命令提示符** > 选择**命令提示符**）
     2. 将“查找 Window 的进程”图标 () 拖动到“命令提示符”窗口，在进程资源管理器中找到突出显示的命令提示符进程。
     3. 命令提示符进程为 cmd.exe。它的父进程是 explorer.exe 进程。cmd.exe 有一个子进程，即 conhost.exe。



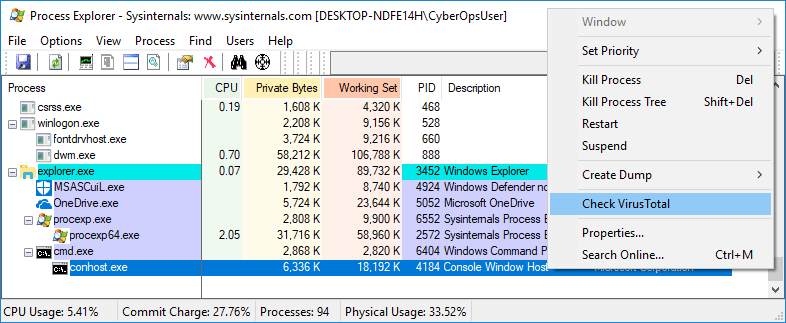
* + 1. 导航到“命令提示符”窗口。在提示符后启动 ping，观察 cmd.exe 进程下的变化。

在 ping 进程中发生了什么？

答：会多出一个PING.EXE子进程。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 查看活动进程列表时，同学们会发现子进程 conhost.exe 表现可疑。要查找恶意内容，请右键点击 **conhost.exe**，然后选择**检查 VirusTotal**。系统提示时，点击**是**，同意《VirusTotal 服务条款》。然后，对系统显示的下一项提示点击**确定**。



* + 1. 展开“进程资源管理器”窗口，或者滚动到右侧，直到看到 VirusTotal 列。点击 VirusTotal 列下的链接。默认 Web 浏览器打开，显示与 conhost.exe 的恶意内容相关的结果。
    2. 右键点击 cmd.exe 进程，选择**终止进程**。子进程 conhost.exe 发生了什么？

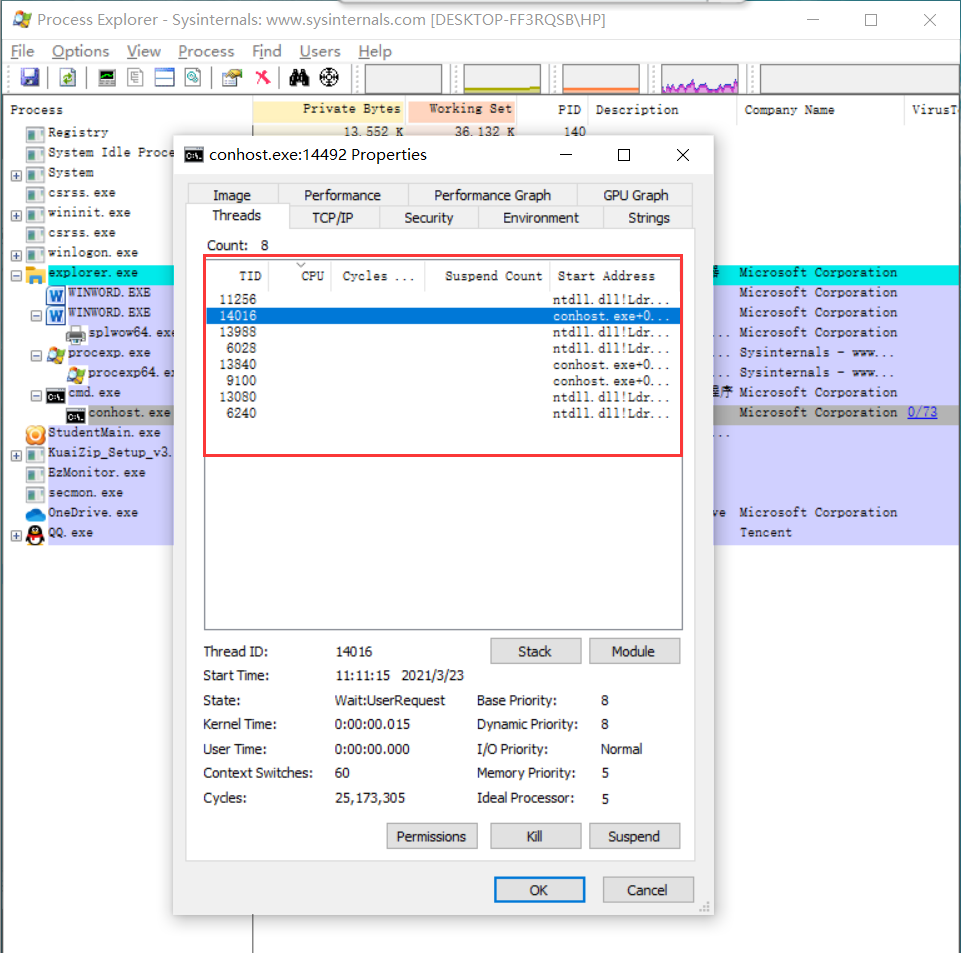
答：和父进程cmd.exe一起终止。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 了解线程和句柄

在这一部分，同学们将了解线程和句柄的相关知识。进程包含一个或多个线程。线程是进程中的一个执行单元。句柄是操作系统管理的内存块或对象的抽象引用。同学们将使用 Windows SysInternals Suite 中的进程资源管理器 (procexp.exe) 了解进程和句柄。

* 1. 了解线程。
     1. 打开命令提示符。
     2. 在进程资源管理器窗口中，右键点击 conhost.exe，然后选择**属性…**。点击**线程**选项卡，查看 conhost.exe 进程的活动线程。



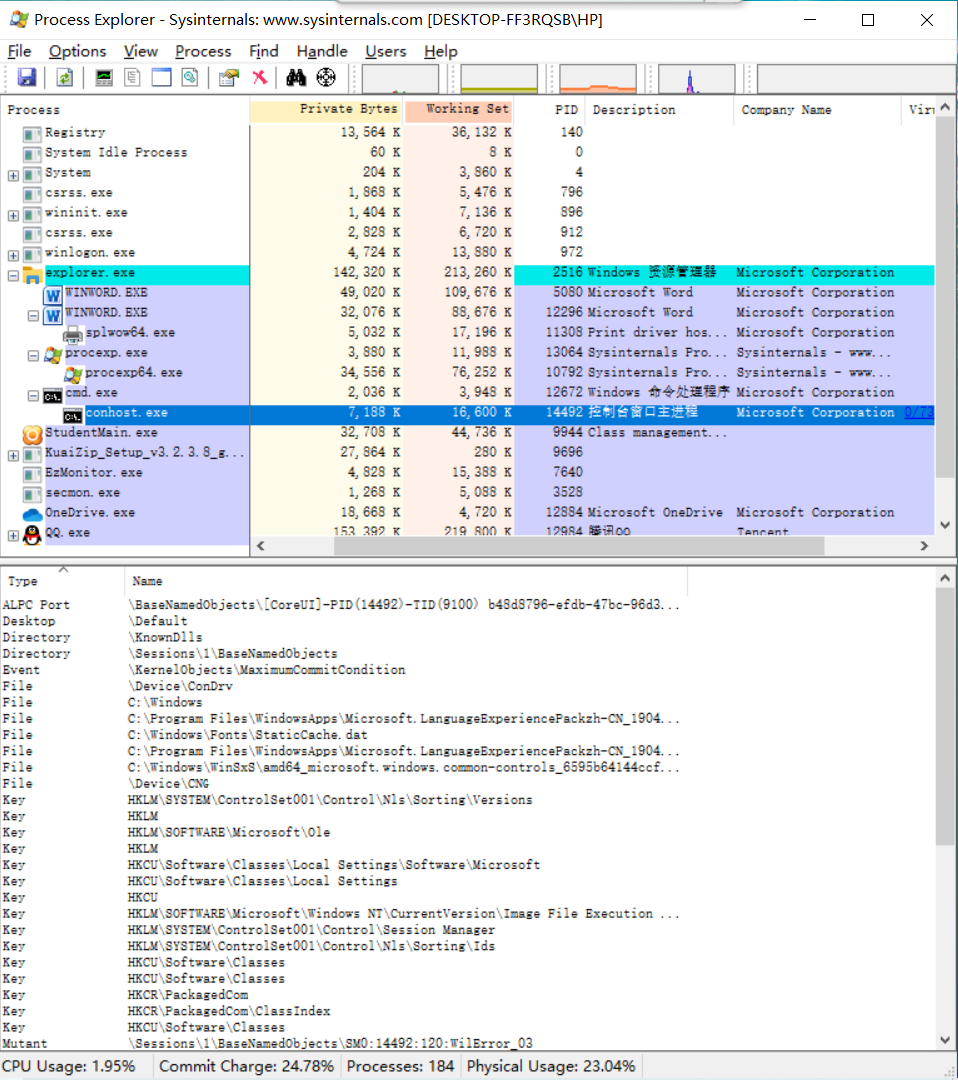
* + 1. 检查该线程的详细信息。“属性”窗口中提供了哪些类型的信息？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. 了解句柄。

在进程资源管理器中，点击**查看** > 选择**显示下面的窗格** > **句柄**，查看与 conhost.exe 进程相关联的句柄。



检查句柄。句柄指向什么？

答：指向指向目标内核对象。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

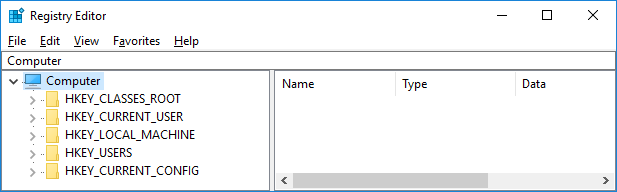
1. 了解 Windows 注册表

Windows 注册表是一个分层数据库，其中存储了大多数操作系统和桌面环境配置设置。在这一部分，同学们将了解注册表的相关知识。

* + 1. 要访问 Windows 注册表，请点击**开始** > 搜索 **regedit**，然后选择**注册表编辑器**。当系统询问时，点击**是**以允许此应用作出更改。

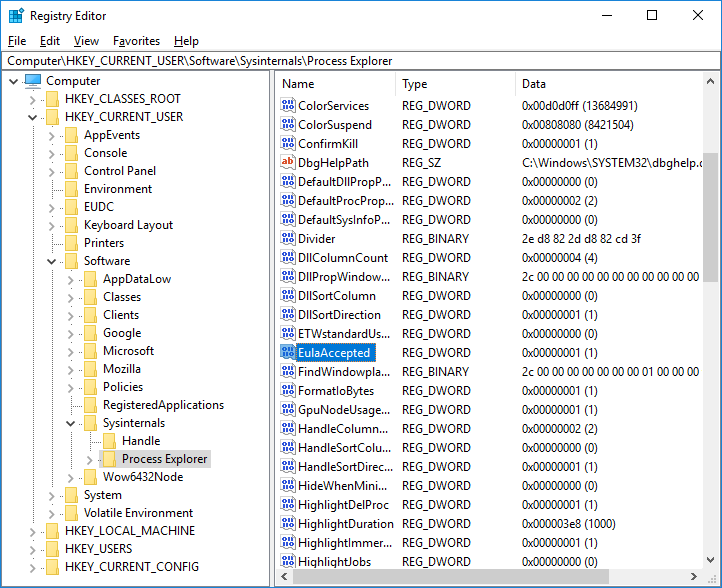
注册表编辑器有五个配置单元。这些配置单元位于注册表的顶层。

* HKEY\_CLASSES\_ROOT 实际上是 HKEY\_LOCAL\_MACHINE\Software\ 的类子项。它存储已注册应用所使用的信息，例如文件扩展名关联，以及编程标识符 (ProgID)、类 ID (CLSID) 和接口 ID (IID) 数据。
* HKEY\_CURRENT\_USER 包含当前登录用户的设置和配置。
* HKEY\_LOCAL\_MACHINE 存储特定于本地计算机的配置信息。
* HKEY\_USERS 包含本地计算机上所有用户的设置和配置。HKEY\_CURRENT\_USER 是 HKEY\_USERS 的子项。
* HKEY\_CURRENT\_CONFIG 存储本地计算机在启动时使用的硬件信息。

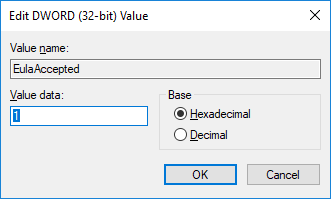


* + 1. 在上一步中，同学们接受了进程资源管理器的 EULA。导航到进程资源管理器的 EulaAccepted 注册表项。

在 **HKEY\_CURRENT\_USER** > **软件** > **Sysinternals** > **进程资源管理器**中点击选择进程资源管理器。向下滚动至项 **EulaAccepted**。注册表项 EulaAccepted 的当前值为 0x00000001(1)。



* + 1. 双击 **EulaAccepted** 注册表项。该值数据当前设置为 1。值 1 表示用户接受了 EULA。



* + 1. 将值数据从 **1** 更改为 **0**。值 0 表示未接受 EULA。点击**确定**继续。

该注册表项在“数据”列中的值是什么？0x00000000(0)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 打开**进程资源管理器**。导航到同学们已下载 SysInternals 的文件夹。打开文件夹 **SysInternalsSuite** > 打开 **procexp.exe**。

当同学们打开进程资源管理器时，同学们看到了什么？

答：会弹出协议需要选择是否同意，同意后发现注册表中的EulaAccpeted的值变为1。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_