实验 – 在 Windows 8 中监控和管理系统资源

简介

在本实验中，您将使用管理工具来监控和管理系统资源。

建议使用的设备

- 运行 Windows 8 且具有 Internet 访问权限的计算机

第 1 步：如何在 Windows 中停止和启动一项服务。

您将探索在停止某项服务后再启动它时会发生什么。

a. 以管理员身份登录 Windows。

注意：必须卸载计算机上的某些防病毒或反间谍软件程序，Windows Defender 才能工作。

b. 要查看 Windows Defender 是否关闭，请单击**“开始”**，在**“搜索程序和文件”**字段中键入 **Defender** 并选择 **Windows Defender**。**Windows Defender** 应该会运行。

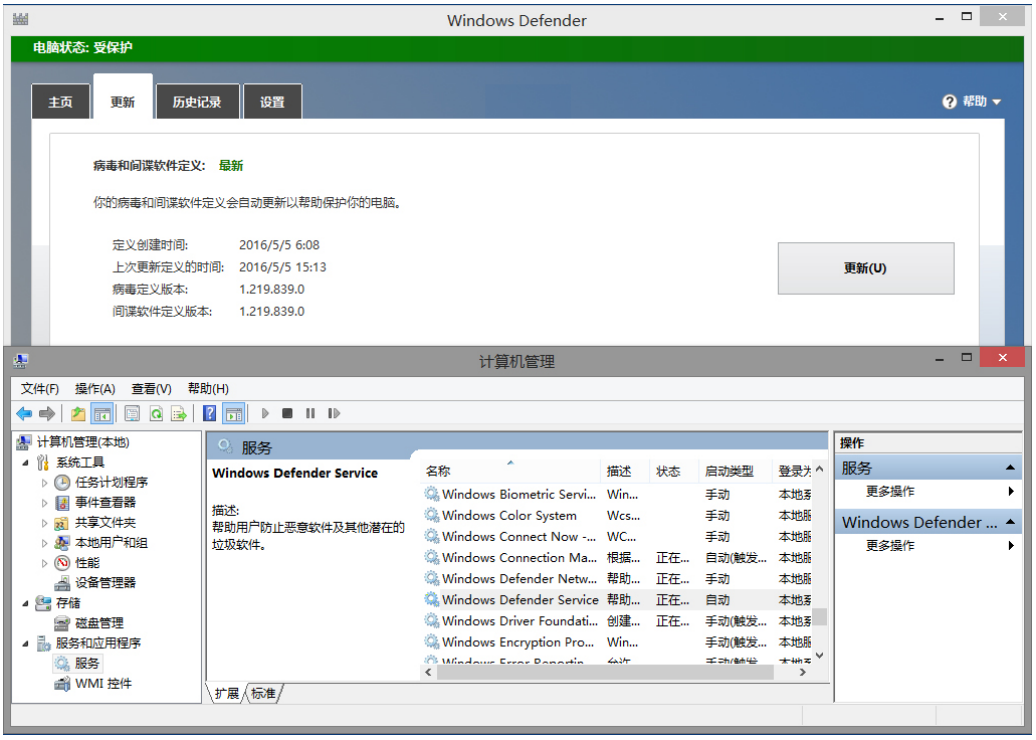
注意：在 Windows 8.0 中，请单击**“搜索”**，键入 **Defender**，并选择 **Windows Defender**。

注意：如果 **Windows Defender** 没有运行，一个警告窗口将打开，而且 **Windows Defender** 将无法启动。要启动 Windows Defender，请单击**“控制面板”** > **“操作中心”**。在**“操作中心”**的**“病毒防护(重要信息)”**区域，单击**“立即启用”**。

c. 在不关闭 **Windows Defender** 的情况下，打开**“服务”**控制台。单击**“控制面板”** > **“管理工具”** > **“计算机管理”**。

d. **“计算机管理”**窗口打开。在“服务和应用程序”下，选择**“服务”**。

e. 关闭**“Windows 资源管理器”**窗口，但 **Windows Defender** 和**“计算机管理”**窗口保持打开状态。调整并确定这两个窗口的大小，使其同时可见。



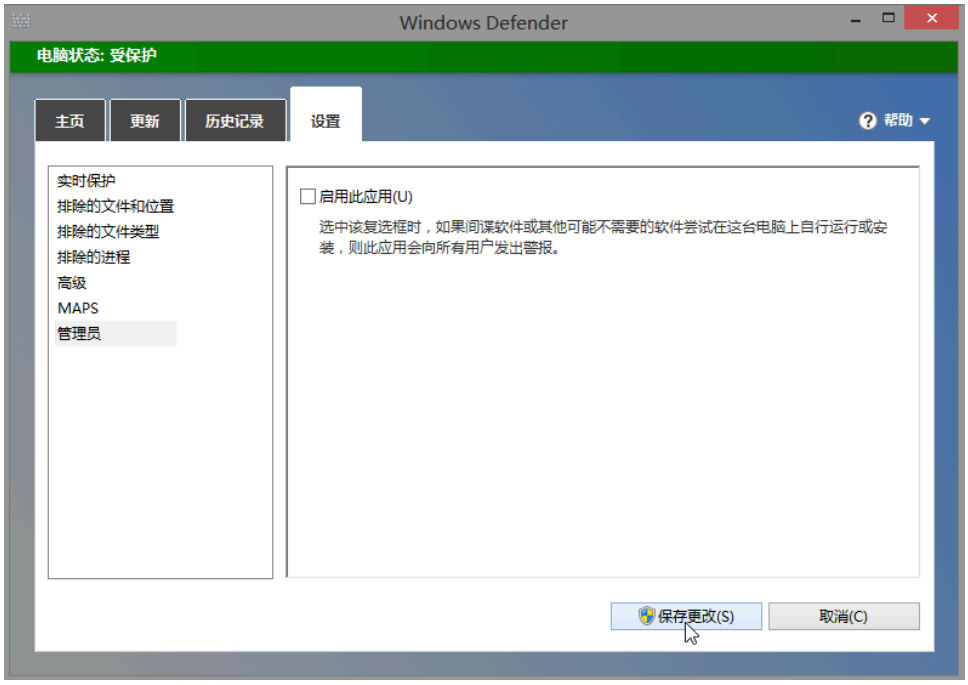
Windows Defender 可以检查更新吗？（请使用**“更新”选项卡**回答此问题）

f. 滚动**“计算机管理”**窗口，找到**“Windows Defender 服务”**。

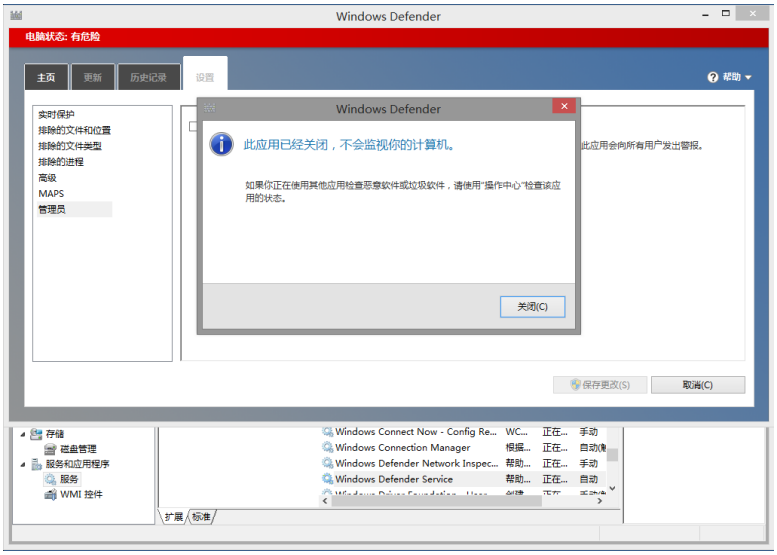
该服务处于什么状态？

注意：虽然可通过“服务”控制台管理大部分 Windows 服务，但是从 Windows 8 的**“服务”**控制台无法停止 **Windows Defender**。

g. 要关闭 **Windows Defender**，请将 **Windows Defender** 窗口激活。选择**“设置”**选项卡，并选择**“管理员”**。取消选中**“启用此应用”**复选框，然后单击**“保存更改”**。



h. 一个警告窗口打开。单击**“关闭”**。注意 **Windows Defender** 应用程序会完全关闭。



注意：停止此服务是为了让您可以轻松地查看结果。停止某个服务后，为了释放该服务所使用的系统资源，一定要了解总体的系统操作将受何影响。

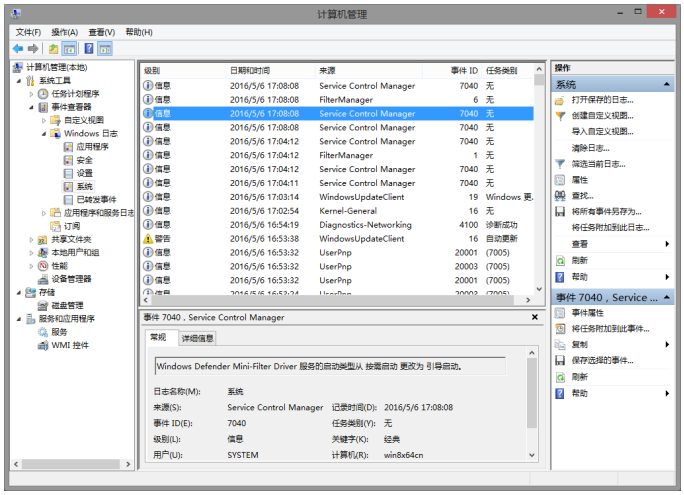
注意：尽管**“计算机管理服务”**窗口无法控制 Windows Defender 服务，但仍会监控并显示 Windows Defender 的状态。可能需要按 **F5** 来刷新**“计算机管理”**窗口。

i. 由于 **Windows Defender** 服务已经停止，请通过单击**“搜索”**，键入 **Defender** 并选择 **Windows Defender** 来重新运行 **Windows Defender**。

必须执行什么操作才能使 Windows Defender 运行？

j. 使用**“操作中心”**来启动 Windows Defender 服务。单击**“控制面板”>“操作中心”**。在 **“病毒防护(重要信息)”**部分，单击**“立即启用”**。

k. **Windows Defender** 窗口打开，因为该服务现在已重新运行。关闭 **Windows Defender** 窗口，但确保“计算机管理”窗口打开。

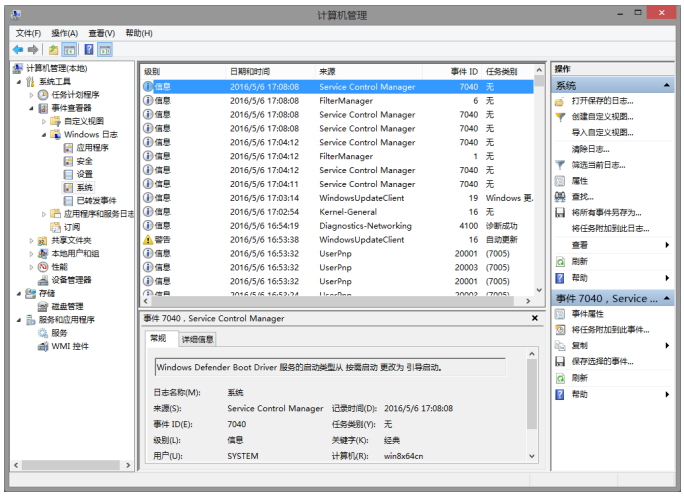


l. 展开**“事件查看器”**>**“Windows 日志”**>选择**“系统”**。

m. 选择列表中的第二个**“服务控制管理器”**事件。

查看下面的“常规”选项卡并解释 Windows Defender 服务发生了什么状况。

n. 单击键盘上的向上箭头按钮，或选择您刚刚查看的事件上方的事件。



查看下面的“常规”选项卡并解释 Windows Defender 服务发生了什么状况。

o. 关闭所有打开的窗口。

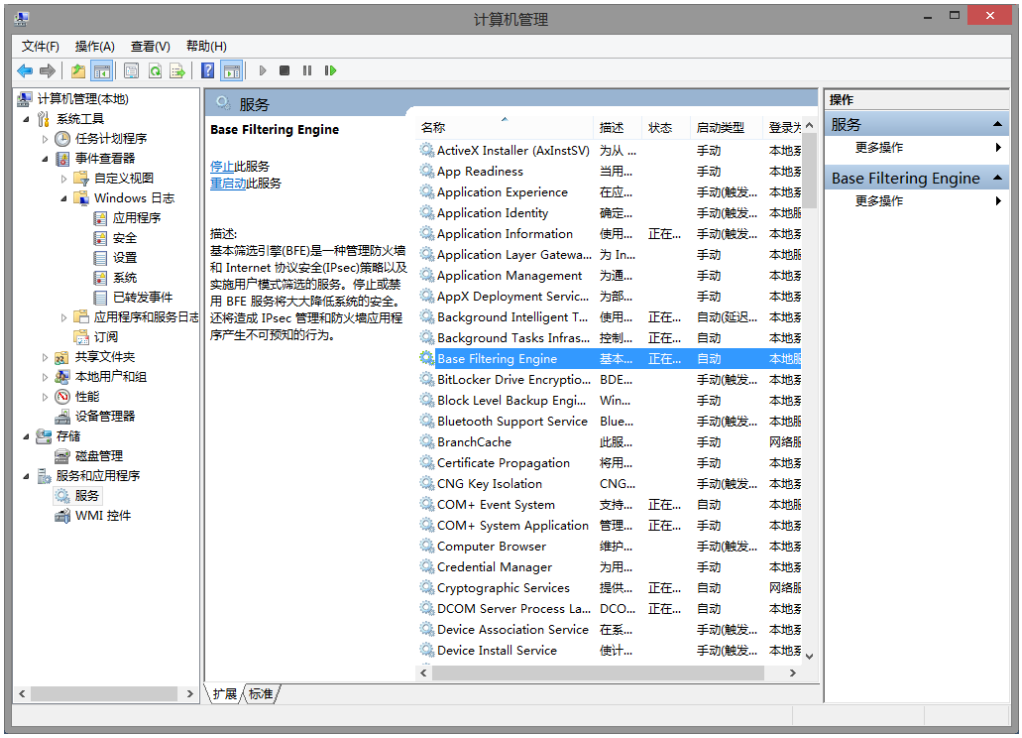
第 2 步: 了解服务的影响。

在这一部分中，您将停止**“Windows 基本筛选引擎 (BFE)”**，分析其系统影响，并重新启动 BFE。在 Windows 中，BFE 负责管理防火墙和其他一些安全策略。BFE 是一项重要的 Windows 服务，因为其他许多服务都依赖它运行。

a. 单击**“控制面板”> Windows Defender**，确保 **Windows Defender** 正在运行。

b. 打开“计算机管理”实用程序。单击**“控制面板”>“管理工具”>“计算机管理”**。选择**“服务”**，并找到**“基本筛选引擎”**服务。

c. 右键单击 BFE 服务并选择**“停止”**，停止 BFE 服务。或者，您可以在 BFE 服务选定时使用**“服务控制台”**上方工具栏中的停止按钮。



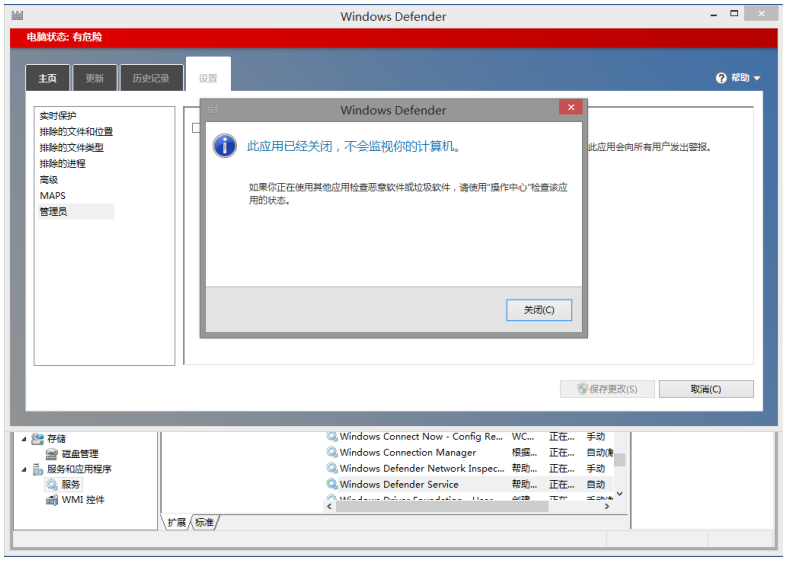
d. Windows 将显示一条警告消息，提醒您依赖 BFE 运行的所有服务。单击**“是”**停止 BFE 及其相关服务

注意：所列服务可能与此警告消息不同。

e. 如果 **Windows Defender** 服务显示在**“停止其他服务”**窗口中，则 Windows 应该不允许您停止 BFE。由于 **Windows Defender** 无法通过**“服务控制台”**停止，因此无法通过**“服务控制台”**停止 BFE。

注意：如果此错误窗口没有显示，请跳至**子步骤 h**。

f. 要停止 BFE，必须先停止 **Windows Defender**。打开 **Windows Defender** 并单击**“设置”**选项卡上的**“停止”**。请参阅本实验开头部分，了解有关详细信息。



g. 现在 **Windows Defender** 已经停止，请打开**“服务控制台”**并停止 BFE。右键单击 BFE 服务并选择**“停止”**。

“服务控制台”的状态列中显示 BFE 服务的状态是什么？

h. 由于一些安全相关服务依赖于 BFE，所以系统会发出警告，可在**“操作中心”**查看这些信息。

注意：所列问题可能与**“操作中心”**中的内容不同。

为什么在管理服务时谨慎操作很重要？

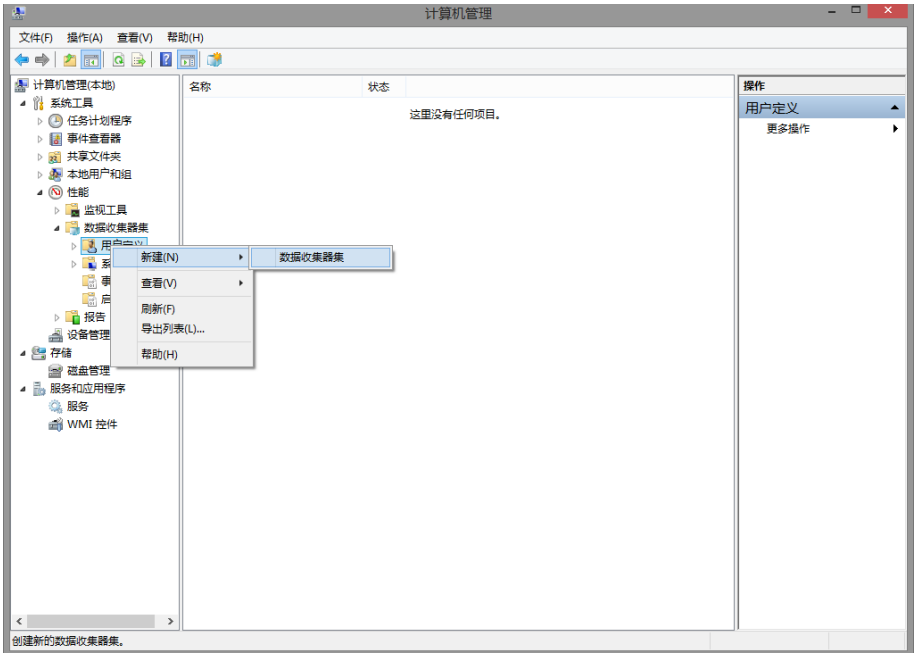
i. 通过在**“操作中心”**选择服务并单击**“立即启用”**，可重新启动任何已停止的服务。

第 3 步：在“管理工具”中配置高级功能。

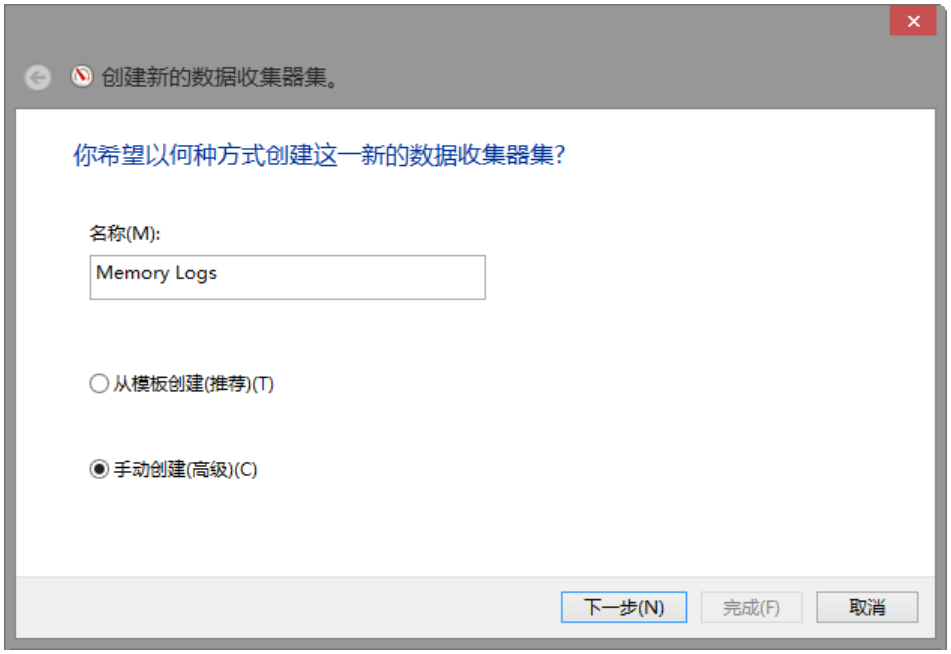
在本实验的其余部分，您将配置高级管理工具功能，并监控其如何影响计算机。

a. 在**“Windows 资源管理器”**中，右键单击**“此电脑”**，并选择**“管理”**。**“计算机管理”**窗口打开。

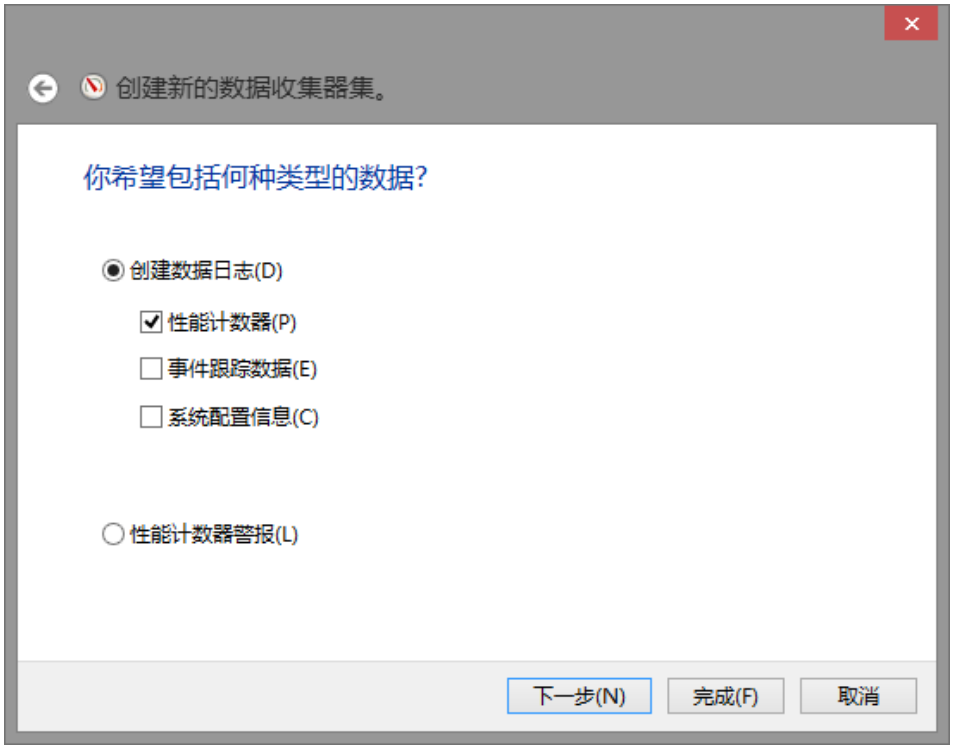
b. 展开**“系统工具”>“性能”>“数据收集器集”**。右键单击**“用户定义”**，然后单击**“新建”>“数据收集器集”**。



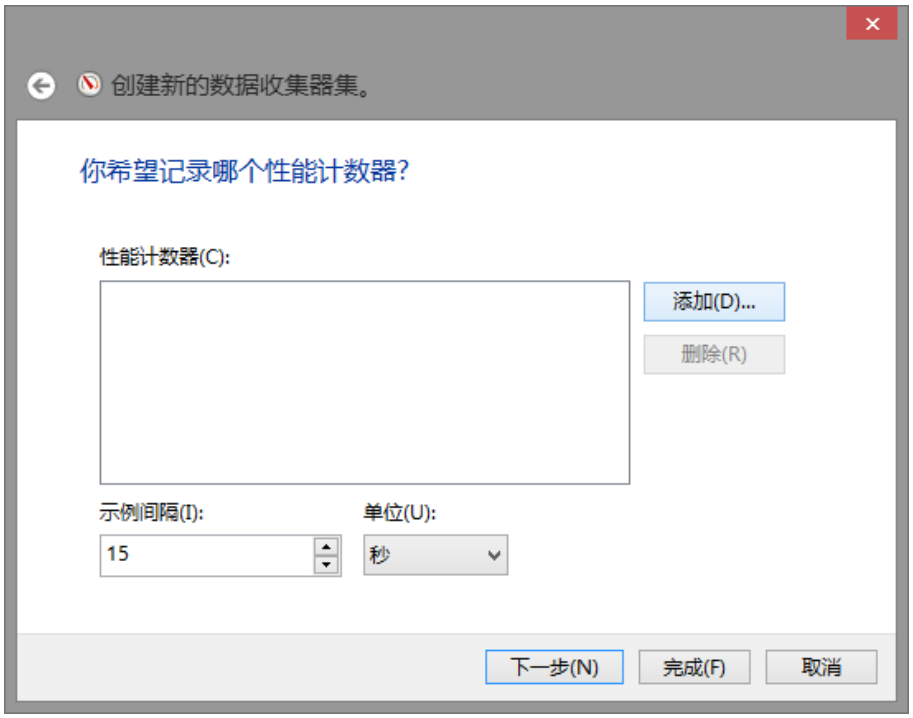
c. **“创建新的数据收集器集”**窗口打开。在“名称”字段中键入 **Memory Logs**。选择**“手动创建(高级)”**单选按钮并单击**“下一步”**。



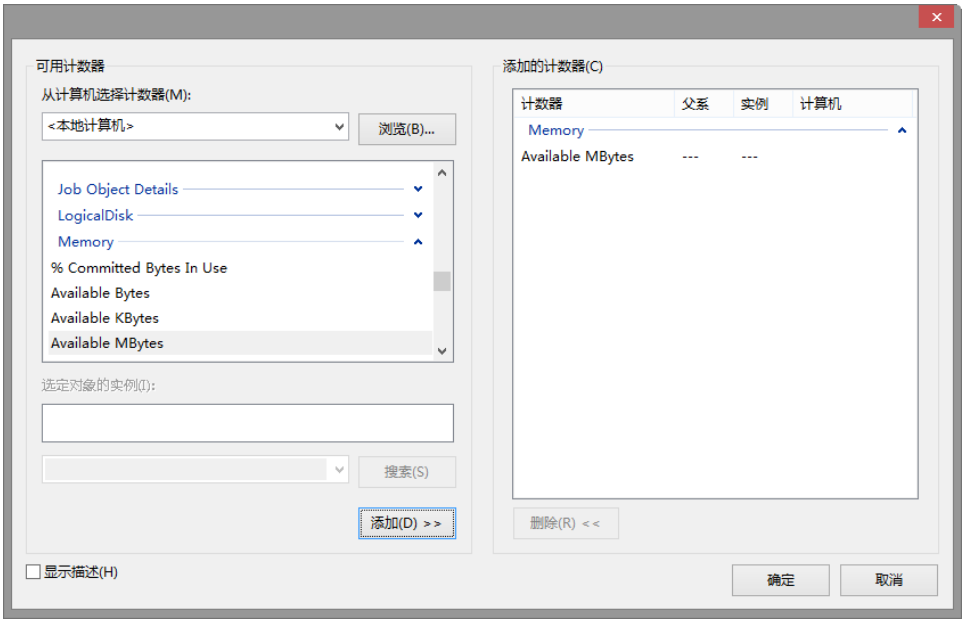
d. **“您希望包括何种类型的数据?”**窗口打开。选中**“性能计数器”**框，然后单击**“下一步”**。



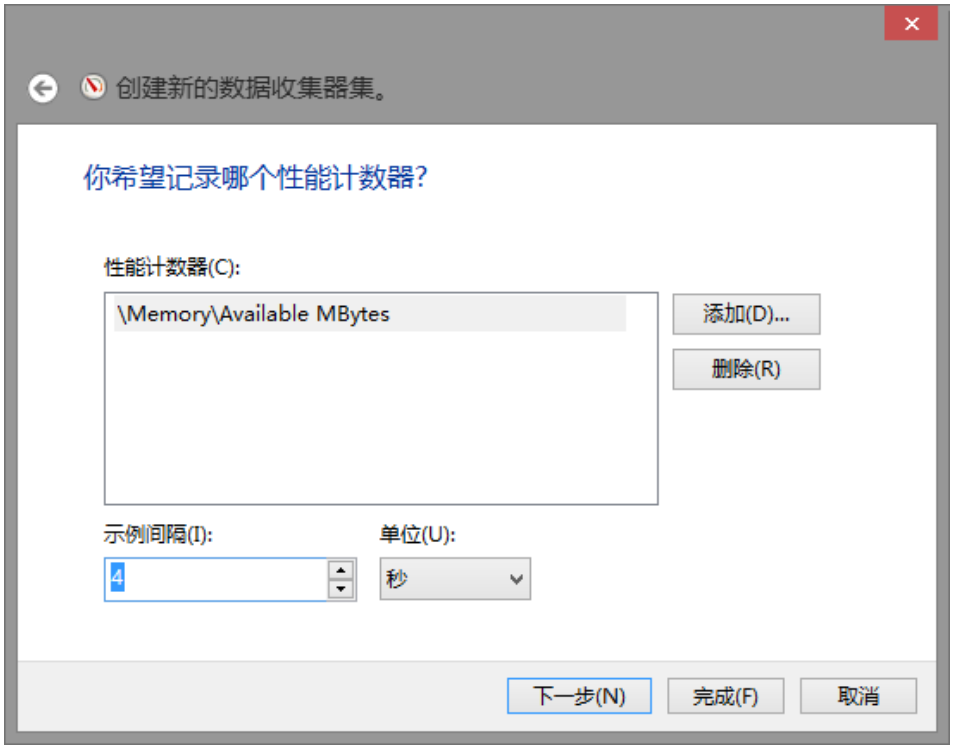
e. **“您希望记录哪个性能计数器?”**窗口打开。单击**“添加”**。



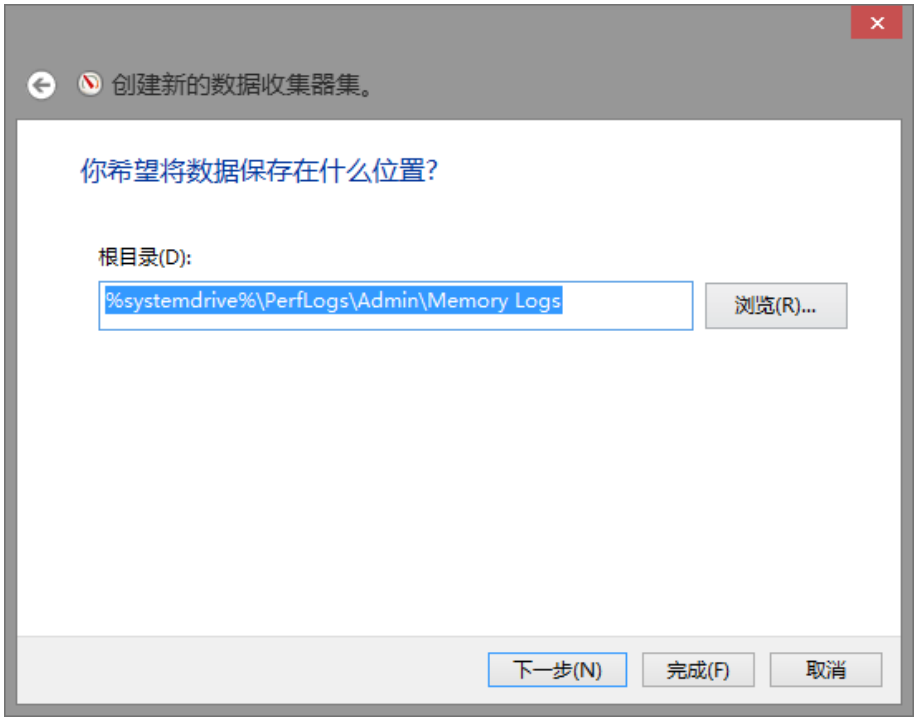
f. 从可用计数器列表中，查找并展开 **Memory**。选择 **Available MBytes>“添加”**并单击**“确定”**。



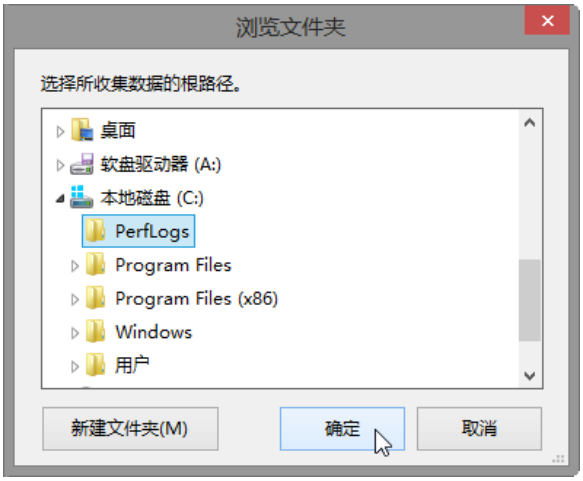
g. 将**“采样间隔：”**字段设置为 **4** 秒。单击**“下一步”**。



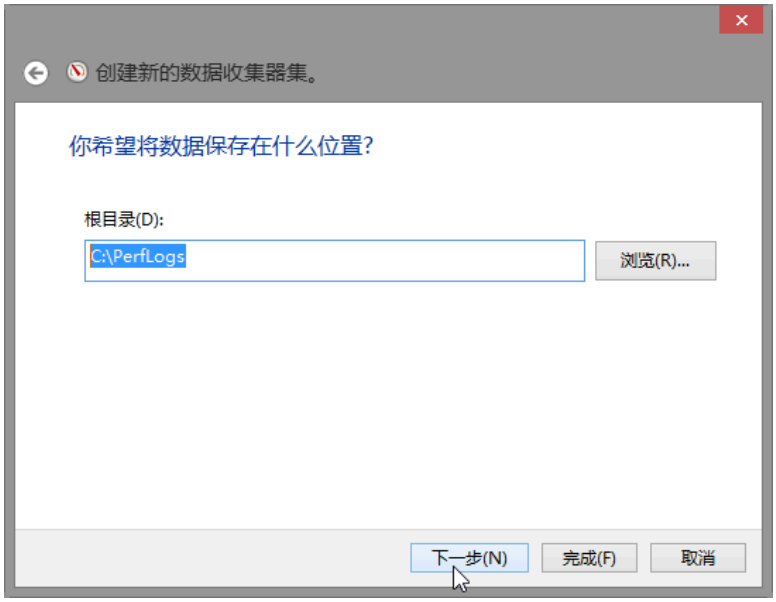
h. **“您希望将数据保存在什么位置?”**窗口打开。单击**“浏览…”**。



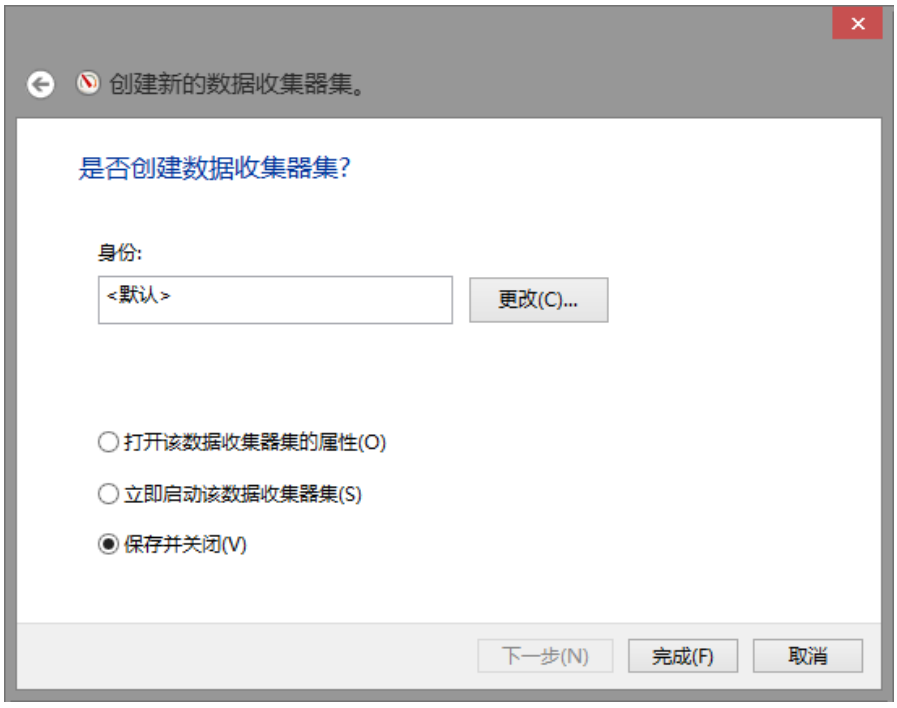
i. 选择本地磁盘 (**C:**)，然后选择 **\PerfLogs** 文件夹。单击**“确定”**。



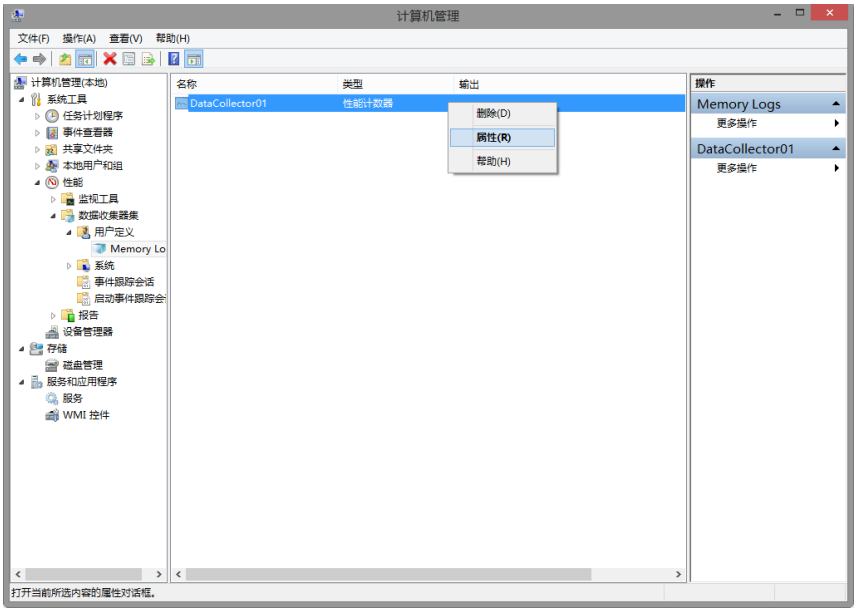
j. 确认已选择了正确的根目录路径，然后单击**“下一步”**。



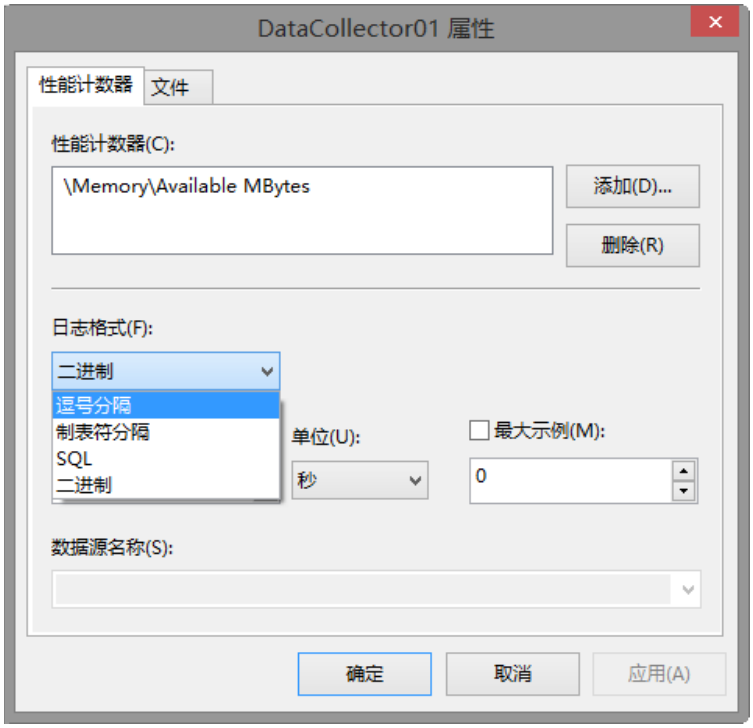
k. **“是否创建数据收集器集?”**窗口打开。单击**“完成”**。



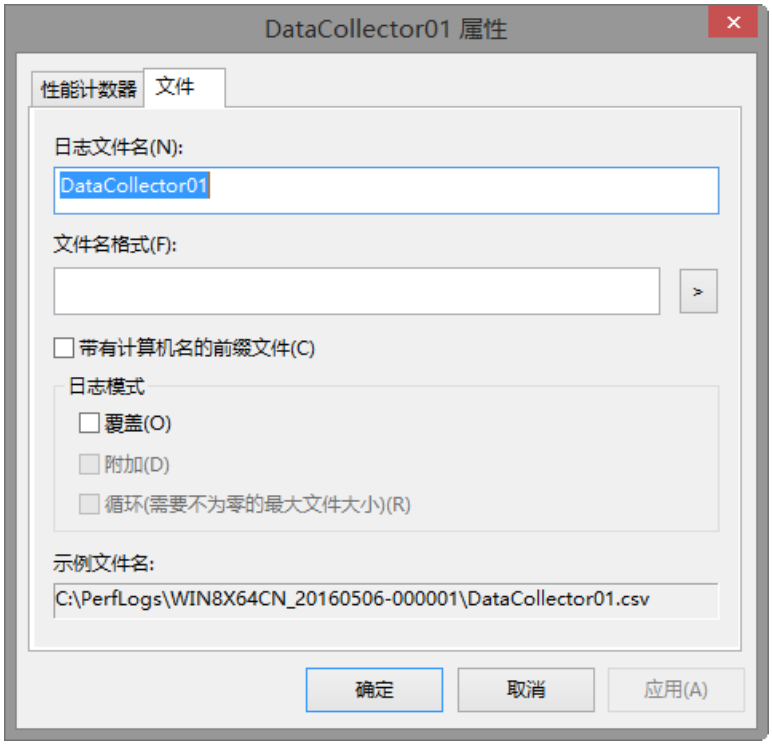
l. 展开**“用户定义”**并选择 **Memory Logs**。右键单击 **Data Collector01** 并选择**“属性”**。



m. **“DataCollector01 属性”**窗口打开。将**“日志格式:”**字段改为**“逗号分隔”**。



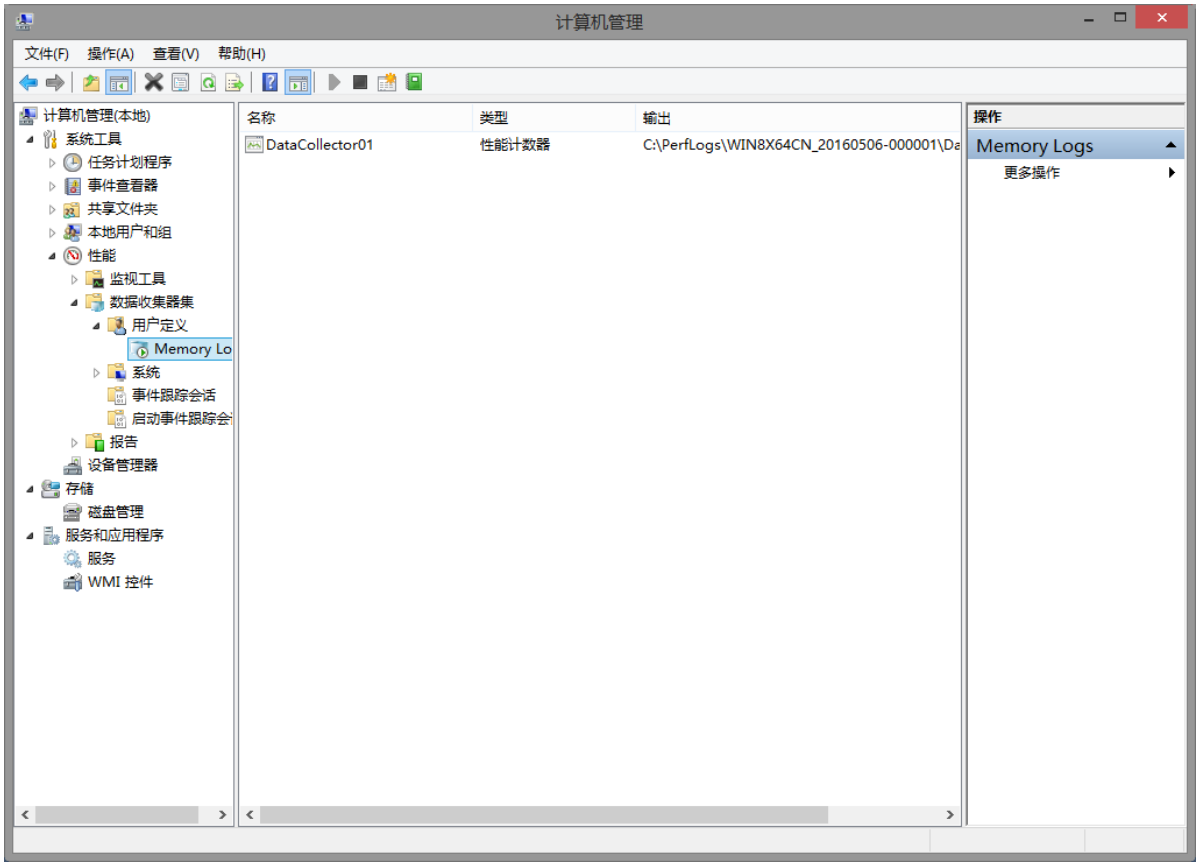
n. 单击**“文件”**选项卡。



示例文件名的完整路径名称是什么？

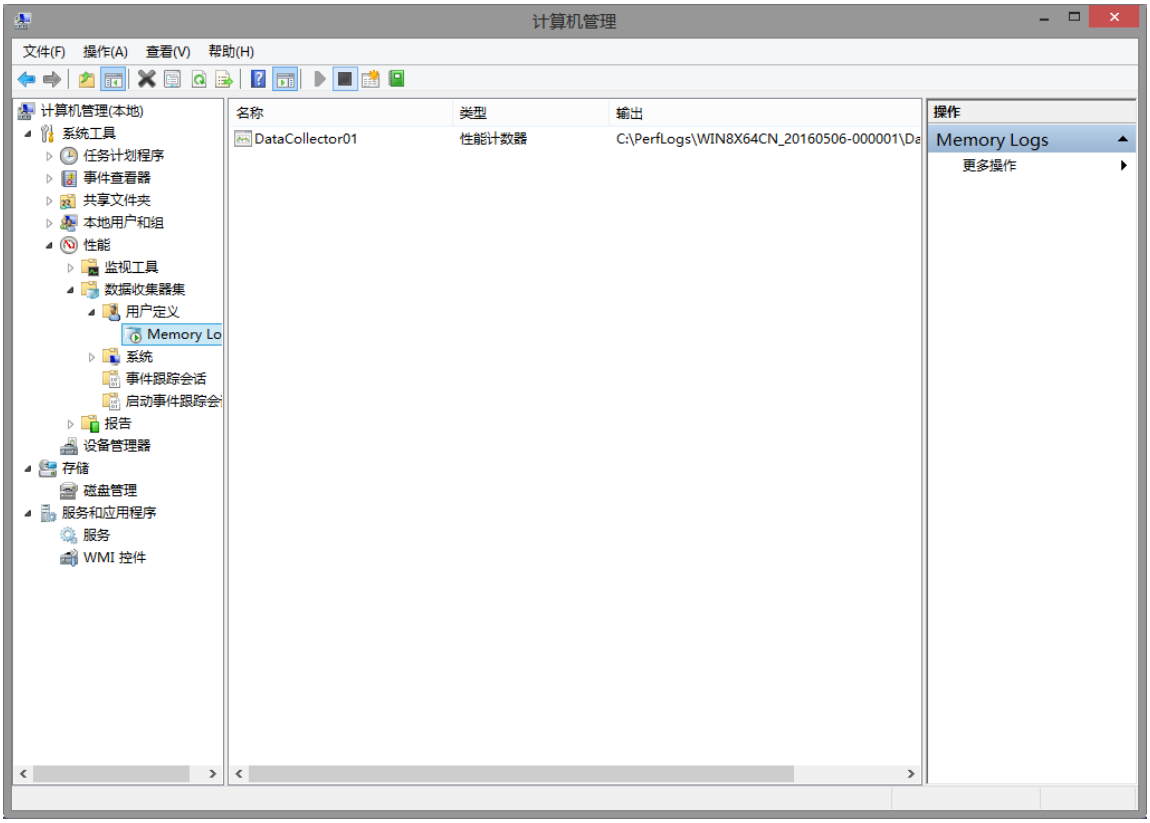
o. 单击**“确定”**。

p. 选择**“性能监视器”**窗口左窗格中的 **Memory Logs** 图标。单击**绿色箭头**图标启动数据收集组。注意 **Memory Logs** 图标上放置了一个绿色箭头。



q. 要强制计算机使用某些可用内存，请打开并关闭浏览器。

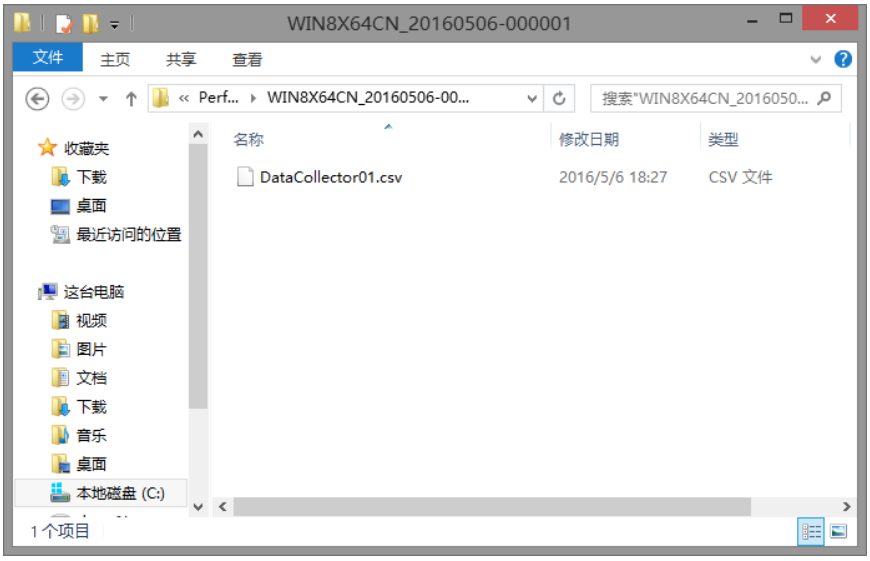
r. 单击**实心方形**图标停止数据收集组。



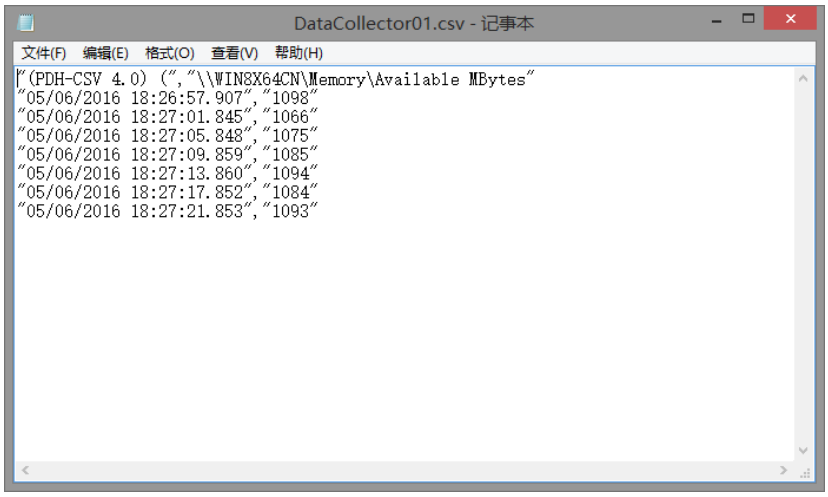
您注意到 Memory Logs 图标有何改变？

s. 打开**“Windows 资源管理器”**，并单击**“本地磁盘 (C:)”>PerfLogs**。单击先前创建的、用于保存内存日志的文件夹，并双击 **DataCollector01.csv** 文件。

注意：显示 Windows 警告消息时请单击**“继续”**。



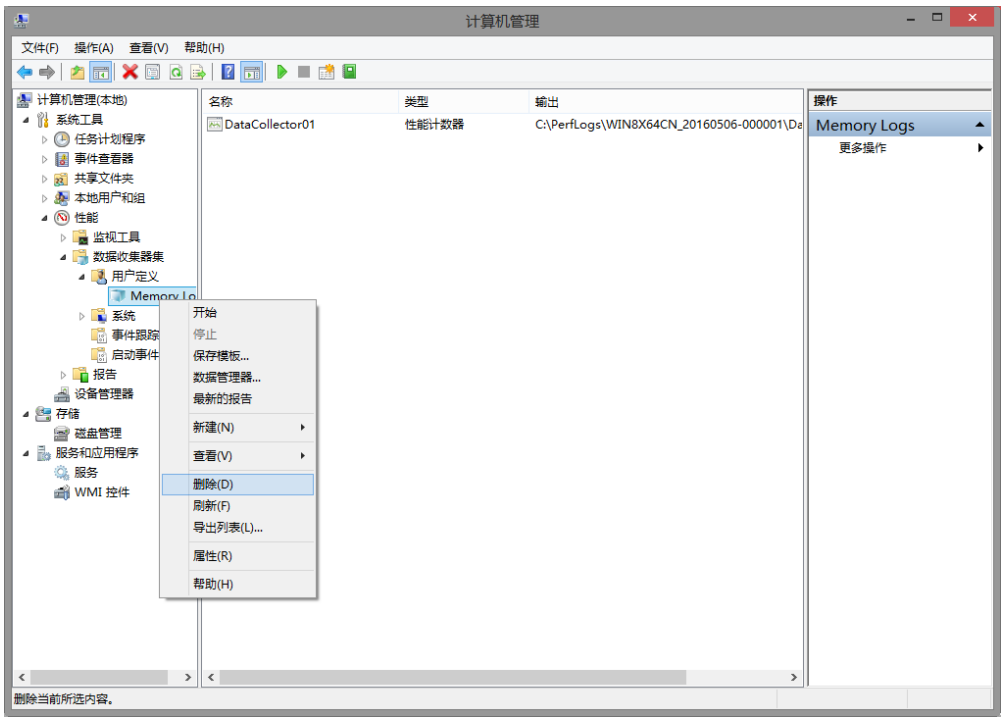
t. 如果出现**“Windows 不能打开此文件:”**消息，请选择单选按钮**“从已安装程序列表中选择程序”>“确定”>“记事本”>“确定”**。



最右边的列中将会显示什么？

u. 关闭 **DataCollector01.csv** 文件和**“Windows 资源管理器”**。

v. 选择**“性能监视器”**窗口。



w. 右键单击 **Memory Logs >“删除”**并单击**“是”**。

x. 打开**“Windows 资源管理器”**，并单击**“本地驱动器 C:”>PerfLogs** 文件夹。右键单击先前创建的、用于保存内存日志的文件夹，并单击**“删除”**。

y. 关闭所有打开的窗口。