用托管C 监视Windows事件日志 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/274/2021_2022__E7_94_A8_E6_89_98_E7_AE_A1C_c67_274981.htm 随着病毒、流氓软件、广告软件等的日益增多，许多人都开始使用注册表监视程序，这些监视程序通常会在安装软件试图修改注册表时，弹出一个警告窗口提示用户。然而，在安全问题上，经常被忽略的地方则是Windows事件日志--尤其是安全日志，安全日志通常记录了Windows操作系统及关键系统应用程序的操作，如试图非法登录、端口扫描、及其他安全相关的事件。 文中将演示如何在应用程序中监视Windows事件日志，当然了，还可以对程序进行扩充，如在事件日志记录到特定的事件类型时，发电子邮件通知用户。 用 .NET EventLog进行监视 文中的代码使用了 .NET 1.0/1.1托管C 语法，如果你在使用一个更高版本的 .NET，需要在工程属性对话框中设置/clr:oldSyntax 编译选项，或调整以下代码使之符合新的托管语法。 用于Windows事件日志的关键 .NET类型是Diagnostics::EventLog 类。 1、定义一个托管类并实现事件日志通知处理程序 处理程序（OnNewLogEntry）会在"新事件日志项"事件引发时调用，同时，请注意此处的EntryWrittenEventHandler，以下是示例代码：//用于监视新事件日志项的示例代码__gc class NewLogEntryEventHandler{ public: NewLogEntryEventHandler() {} public: void OnNewLogEntry(Object* sender, EntryWrittenEventArgs* e) { //获取并处理最近创建的项 EventLogEntry* entry = e->Entry. }}. 2、实例化一个EventLog对象，并把它的EnableRaisingEvents属性设为true 属

性EventLog::EnableRaisingEvents是一个布尔类型，其控制了在项目添加到EventLog对象指定的日志时，是否引发事件
：EventLog* log = new EventLog("Application").log->EnableRaisingEvents = true 3、把事件处理程序连接到"新事件日志项"事件 首先，实例化定义了事件处理程序的对象（在此例中为NewLogEntryEventHandler），接着，把事件方法（OnNewLogEntry）添加到EventLog::EntryWritten的事件处理程序列表中
：NewLogEntryEventHandler* handler = new NewLogEntryEventHandler().log->EntryWritten =new EntryWrittenEventHandler(handler,&amp.NewLogEntryEventHandler::OnNewLogEntry). 4、为特定事件的处理编写代码 回过头来看一个OnNewLogEntry方法，可以看到传递给事件处理程序的EntryWrittenEventArgs对象有一个名为EventLogEntry的成员，其包含了有关记录项目的详细情况，具体为以下属性： MachineName--创建事件日志的电脑系统名。 Source--创建此事件的事件源或程序源。 Message--用户可在事件查看器中读取这条文本值，其描述了记录的事件。 Event Type--此值（代表了EventLogEntryType）为一个枚举值，其代表记录的事件类型：信息（默认）、警告、错误、审核成功、审核失败。 Event ID--为有关事件程序特定的号码。 Data--此值通常用于存储二进制信息--如内存转储--也是与事件有关的。 不足之处 从以上可以看出，.NET使得访问事件日志非常简单，然而，以下也有一些有关处理事件日志时的限制条件： 只能在本地系统上监视事件。 .NET文档未说明，如果在短时间内记录了大量的事件，是否可保证

每个事件都可被引发。 如果监视了更新特别频繁的事件日志，事件有可能不会立即引发，在事件项之间很可能会有一个滞后，接着突然会有大量的事件通知进入消息队列。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com