 Windows Server 2008系统凭借其超强的系统功能、较高的智能化程度以及更甚一筹的安全性能，吸引了很多朋友创建条件前来尝鲜试用。在与Windows Server 2008系统亲密接触一段时间后，我们发现平时不怎么起眼的“ 审核 ”功能变得更加强大了，巧妙借助该功能，我们可以对服务器系统的一切操作进行跟踪监视，并能依照监视结果来快速排查服务器系统故障以及保障服务器系统的运行安全。现在，本文就对Windows Server 2008系统的审核功能进行挖掘，以方便各位朋友利用该功能更好地服务自己。 启用配置审核功能 Windows Server 2008系统的审核功能在默认状态下并没有启用，我们必须针对特定系统事件来启用、配置它们的审核功能，这样一来该功能才会对相同类型的系统事件进行监视、记录，网络管理员日后只要打开对应系统的日志记录就能查看到审核功能的监视结果了。审核功能的应用范围很广泛，不但可以对服务器系统中的一些操作行为进行跟踪、监视，而且还能依照服务器系统的运行状态对运行故障进行快速排除。当然，需要提醒各位朋友的是，审核功能的启用往往要消耗服务器系统的一些宝贵资源，并会造成服务器系统的运行性能下降，这是因为Windows Server 2008系统必须腾出一部分空间资源来保存审核功能的监视、记录结果。为此，在服务器系统空间资源有限的情况下，我们应该谨慎使用审核功能，确保该功能只对一些特别重要的操作进行监视、记录。 在启用、配置Windows Server

2008系统的审核功能时，我们可以先以系统超级权限登录进入对应系统，打开该系统桌面中的“ 开始 ”菜单，从中依次点选“ 设置 ”、“ 控制面板 ”命令，在弹出的系统控制面板窗口中依次单击“ 系统和维护 ”、“ 管理工具 ”图标，在其后出现的管理工具列表窗口中，找到“ 本地安全策略 ”图标，并用鼠标双击该图标，打开本地安全策略控制台窗口。 其次在目标控制台窗口的左侧显示窗格中，依次展开“ 安全设置 ”/“ 本地策略 ”/“ 审核策略 ”分支选项，在对应“ 审核策略 ”分支选项的右侧显示窗格中，我们会发现Windows Server 2008系统包含九项审核策略，也就是说服务器系统可以允许对九大类操作进行跟踪、记录。 审核进程跟踪策略，是专门用来对服务器系统的后台程序运行状态进行跟踪记录的，例如服务器系统后台突然运行或关闭了什么程序，handle句柄是否进行了文件复制或系统资源的访问等操作，审核功能都可以对它们进行跟踪、记录，并将监视、记录的内容自动保存到对应系统的日志文件中。 审核帐户管理策略，是专门用来跟踪、监视服务器系统登录账号的修改、删除、添加操作的，任何添加用户账号操作、删除用户账号操作、修改用户账号操作，都会被审核功能自动记录下来。 审核特权使用策略，是专门用来跟踪、监视用户在服务器系统运行过程中执行除注销操作、登录操作以外的其他特权操作的，任何对服务器系统运行安全有影响的一些特权操作都会被审核功能记录保存到系统的安全日志中，网络管理员根据日志内容就容易找到影响服务器运行安全的一些蛛丝马迹。 启用不同的审核策略，Windows Server 2008系统就会对不同类型的操作进行跟踪、记录，网络管理员应该依照自己的安全要求以及服

务器系统的性能配置，来启用适合自己的审核策略，而不要盲目地启用所有审核策略，那样一来审核功能的作用反而得不到充分发挥。比方说，要是我们想对服务器系统的登录状态进行跟踪、监视，以便确认局域网中是否存在非法登录行为时，那我们就可以直接用鼠标双击这里的审核登录事件策略，打开对应策略的选项设置对话框，选中其中的“成功”和“失败”选项，再单击“确定”按钮，如此一来Windows Server 2008系统日后就会自动对本地服务器系统的所有系统登录操作进行跟踪、记录，无论是登录服务器成功的操作还是登录服务器失败的操作，我们都能通过事件查看器找到对应的操作记录，仔细分析这些登录操作的记录我们就能发现本地服务器中是否真的存在非法登录甚至非法入侵行为。