深入WindowsServer2008的自我监控Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/557/2021_2022__E6_B7_B1_E5_85_A5Wind_c100_557319.htm 为了亲身体验Windows Server 2008系统与众不同的试用感觉，相信很多用户创建条件、强行为自己的计算机升级安装了该系统。尽管该系统的运行稳定性以及安全防范性能得到了显著提升，不过在Internet网络病毒与木马疯狂肆虐的今天，Windows Server 2008系统仍然还会时刻受到各式各样的安全威胁，比方说核心共享内容被远程修改、系统被非法入侵等，事实上不少安全威胁在真正发生之前都存在一些征兆现象，如果我们能够及时监控到这些可疑迹象，那么就能将安全隐患消除掉，那么我们该采取什么措施来自动监控Windows Server 2008系统的可疑事件呢?这样的任务在Windows Server 2008系统下很简单就能做到，因为该系统新增加了“ 任务附加到事件 ”功能，我们可以深入挖掘该功能，来实现Windows Server 2008系统自我监控的目的!自我监控思路 大家知道，每一个Windows系统都自带了事件查看器程序，不过与传统操作系统不一样的是，Windows Server 2008系统将常用的任务计划功能整合到事件查看器程序中了，有了这项功能的支持，我们可以在服务器系统中针对一些特殊系统事件附加任务计划，让该运行任务在特殊系统事件发生的那一刻及时提醒我们.当Windows Server 2008系统中的需要被监控的系统事件真正发生时，附加在该系统事件上的特定任务计划就能被自动触发，到时它就能根据事先设置好的方式来提醒我们采取应对措施了，这样一来就能实现不用外力工具，Windows Server 2008系统就能完成自我监控的

任务了。 依照上述思路，我们只要先在Windows Server 2008系统中对需要监控的系统事件启用审核功能，确保系统的事件查看器程序能够自动跟踪、记忆目标系统事件，接着人为创建一个特殊系统事件，让事件查看器程序自动生成这个事件记录，例如我们简单地注销系统并重新登录一次，那么Windows Server 2008系统的事件查看器程序就能自动把这个系统登录事件记忆保存下来，有了具体的事件记录后，下面我们就能利用“ 任务附加到事件 ”功能，将自动监控报警信息通过任务计划的方式附加到具体的事件记录上，日后当相同的系统再次发生时，附加的任务计划就能被自动触发，到时我们就能及时收到附加任务计划发送出来的报警信息了，看到报警信息后，我们要做的工作就是及时采取安全应对措施，防范这类有安全威胁的系统事件再次发生，那样一来Windows Server 2008系统的安全性在某种程度上又得到了更进一步地强化。为方便叙述，本文就以自动监控系统登录事件为例，让Windows Server 2008系统对那些偷偷登录系统的非法行为进行自动监控，谨防恶意攻击者暗地里攻击Windows Server 2008系统。 审核待监控事件 Windows Server 2008系统内置的事件查看器程序在默认状态下，不会对类似系统登录这样的事件进行跟踪记录的，也就是说平时我们登录系统时，事件查看器程序并没有这方面的事件记录，要想对系统登录这样的事件进行监控，我们首先要做的工作自然就是为待监控事件启用审核功能，让事件查看器程序可以自动记忆保存这些事件记录。在审核待监控事件时，我们可以按照下面的操作来进行： 首先打开Windows Server 2008系统的“ 开始 ”菜单，从中逐一点击“ 设置 ”、“ 控制面板 ”选项，打开对

应系统的控制面板窗口，再用鼠标双击该窗口中的“ 管理工具 ”图标选项，进入Windows Server 2008系统的管理工具列表界面. 其次双击管理工具列表界面中的“ 本地安全策略 ”图标选项，在其后出现的本地安全策略编辑器界面中，依次展开左侧子窗格区域中的“ 安全设置 ”/“ 本地策略 ”/“ 审核策略 ”分支选项，在“ 审核策略 ”分支选项下面，选中“ 审核登录事件 ”选项，并用鼠标右键单击该选项，从弹出的快捷菜单中执行“ 属性 ”命令进入的审核登录事件属性设置对话框. 下面同时将该设置对话框中的“ 成功 ”、“ 失败 ”复选项都选中，再单击“ 确定 ”按钮保存好上述设置操作，如此一来日后任何一位用户无论有没有成功登录进 Windows Server 2008系统，对应系统的事件查看器程序都会自动把这次系统登录事件记录保存到事件查看器列表中，仔细查看这些记录，我们就能大概判断出当前服务器系统中是否存在非法登录事件发生了。 手工生成目标事件 考虑到任务计划只能与具体的某件事件绑定在一起，为此要想利用任务计划功能对目标系统事件进行自动监控报警，我们还需要手工创建一个与待监控事件性质一样的具体事件记录.例如，要手工生成系统登录事件记录时，我们只要在Windows Server 2008服务器系统桌面中依次单击“ 开始 ”/“ 关机 ”选项，选中“ 待机 ”项目，单击“ 确定 ”按钮，将当前系统注销掉，之后重新以系统管理员账号登录一次 Windows Server 2008服务器系统，当系统登录操作成功后，对应系统的事件查看器程序就会自动将这次登录操作记录下来了。 在查看具体的事件记录时，我们可以在Windows Server 2008服务器系统桌面中用鼠标右键单击“ 计算机 ”图标，从弹出的快捷菜单中点选“ 管理 ”命令，打

开对应系统的计算机管理控制台界面. 其次在该管理控制台界面的左侧显示区域，用鼠标依次展开“ 诊断 ”/“ 事件查看器 ”/“ Windows日志 ”/“ 安全 ”分支选项，在对应“ 安全 ”分支选项的右侧显示区域，我们会看到事件ID为4625的系统登录事件记录，用鼠标双击该事件记录，打开目标事件属性设置窗口，在该窗口的“ 常规 ”标签页面中，我们发现系统自动生成了账户登录失败事件，并且还能查看到究竟是哪一个用户在哪一台工作站上尝试对本地Windows Server 2008服务器系统进行登录操作的，仔细分析这些信号，我们或许就能大概判断出当前是否有非法攻击者在偷偷登录本地服务器系统了。 附加监控报警任务 由于我们现在是要对系统登录事件进行自动监控，为此我们下面需要把监控报警任务附加到系统登录事件上，以确保Windows Server 2008服务器系统下次再次发生相同的事件时，被附加的指定任务能够自动触发运行，以便及时向我们发送报警提示信息，从而实现自动监控目的。在附加监控报警任务到系统登录事件时，我们可以按照下面的操作来进行： 首先按照前面的操作步骤，打开Windows Server 2008服务器系统的事件查看器程序，打开我们希望监视的安全事件日志，找到前面自动生成的相应事件记录，用鼠标右键点选该系统登录事件，从弹出的快捷菜单中执行“ 将任务附加到此事件 ”命令，当然也可以从右侧操作列表区域中点选“ 将任务附加到此事件 ”选项. 其次系统屏幕上将会自动出现一个向导提示窗口，我们可以为当前这个任务设置一个有针对性的名字和描述性文字，例如这里笔者将该任务计划的名称定为“ 自动监控报警 ”，之后单击该窗口中的“ 下一步 ”按钮，随后系统屏幕上会弹出一些提示说明文字，根

据这些说明文字我们可以确认这些内容的准确性，如果看到这些内容都正确无误时，继续单击向导窗口中的“ 下一步 ”按钮. 这时系统屏幕上会出现一个设置窗口，在这里我们可以选择使用不同的报警提示方式，例如可以选用显示消息、发送电子邮件或启动程序，要是我们选用了“ 启动程序 ”提示方式时，点选“ 下一步 ”按钮后，会自动看到选择程序对话框，单击其中的“ 浏览 ”按钮，再查找和选择任何可执行文件、批处理文件或脚本，当然我们也可以直接输入目标应用程序的启动路径，最后单击“ 完成 ”按钮结束任务计划的附加操作. 要是我们选用了“ 发送电子邮件 ”提示方式时，点选“ 下一步 ”按钮后，我们会自动看到一个发送电子邮件编辑对话框，在这里我们需要正确地添加任何需要的报警内容，比方说发信人、收信人、邮件主题、报警内容等，甚至我们还能直接将报警内容以附件文件形式添加到邮件当中，最后还需要设置好发送邮件所需的SMTP 服务器地址. 要是我们选用的是“ 显示消息 ”提示方式，那么点选“ 下一步 ”按钮后，我们可以在其后的设置窗口中添加报警消息的标题以及具体的报警内容，这个方式其实就是新建一个告警提示窗口。当我们在浏览事件查看器的具体日志内容时，或许会看到每隔一段时间系统会发生一个危险事件，不过要是我们不及时打开事件查看器去查看时，我们根本没有办法在第一时间知道该事件的发生，现在有了这个显示消息提示方式，日后一旦发生同样的危险事件时，我们就能在第一时间知道并采取安全应对措施了。 很显然，为了实现及时、自动监控目的，我们在这里应该选用“ 显示消息 ”提示方式，之后依照屏幕提示输入好消息标题以及报警主题内容，比方说输入“ 注意

了，可能有非法账号在偷偷登录系统!”，最后单击“完成”按钮保存好上述任务计划的创建操作。 实现自动监控报警 到了这里，Windows Server 2008系统就能实现自动监控报警的目的了。日后当有非法用户偷偷登录Windows Server 2008系统时，事先附加到系统登录事件上的指定报警任务就会自动触发运行，而该任务运行成功后，Windows Server 2008系统屏幕上会自动出现“注意了，可能有非法账号在偷偷登录系统!”这样的报警提示信息，见到这样的提示信息，我们就能知道当前有人在偷偷登录本地服务器系统，此时我们应该打开Windows Server 2008服务器系统的事件查看器程序窗口，找到系统自动生成下来的相应事件记录，用鼠标双击该目标事件，进入该事件的具体属性设置窗口，从中查看究竟是哪一位用户、在哪一台计算机上尝试登录操作，如果发现是陌生的用户或陌生的计算机，那么我们应该及时采取安全措施来阻止他们继续非法登录，以便确保 Windows Server 2008服务器系统的运行安全。 