产品指南
修订版 1.0

VirusScan® Enterprise

7.1.0 版

McAfee® SECURITY

目录

序言 9

读者 9
排版规范 10
获取信息 11
与 McAfee Security 和 Network Associates 联系 12

1 VirusScan Enterprise 简介 13

本版本的新功能 14
产品组件 15

2 入门 17

面向用户的界面 18
开始菜单 18
VirusScan 控制台 19
菜单栏 20
任务菜单 20
编辑菜单 21
视图菜单 21
工具菜单 21
帮助菜单 22
工具栏 22
任务列表 23
状态栏 24
右键菜单 24
控制台右键菜单 24
右键扫描 25
系统任务栏 25
系统任务栏右键扫描或更新 25
命令行 26
设置用户界面选项 26
显示选项 27
密码选项 28

解锁和锁定用户界面 30
设置扫描操作 31
按访问扫描与按需扫描的比较 31
自动扫描 32
定期扫描、选择性的扫描或按计划扫描 32
病毒信息库 33
提交病毒样本 33
设置远程管理 34

3 按访问扫描 35

配置按访问扫描程序 36
按访问扫描属性 37
常规设置 39
常规属性 39
消息属性 41
报告属性 43
进程设置 45
默认进程 46
进程属性 47
检测属性 48
高级属性 51
操作属性 53
低风险进程和高风险进程 55
为进程指定风险 55
进程属性 56
检测属性 59
添加文件类型扩展名 62
添加用户指定的文件类型扩展名 63
排除文件、文件夹和驱动器 64
高级属性 66
操作属性 68
查看扫描结果 71
查看扫描统计信息 71
查看活动日志 72
响应病毒检测 72
接收病毒检测通知 73
查看按访问扫描消息 74
在检测到病毒时采取措施 75

4 按需扫描 77

创建按需扫描任务 78
从开始菜单或系统任务栏创建任务 78
从控制台创建任务 80
配置按需扫描任务 81
扫描位置属性 82
添加删除和编辑项目 83
添加项目 83
删除项目 85
编辑项目 85
检测属性 86
高级属性 88
操作属性 90
报告属性 93
重设或保存默认设置 94
计划按需扫描任务 95
扫描操作 96
运行按需扫描任务 96
暂停和重新启动按需扫描任务 97
停止按需扫描任务 97
可恢复的扫描 98
查看扫描结果 98
查看扫描统计信息 99
查看活动日志 100
响应病毒检测 100
接收病毒检测通知 101
在检测到病毒时采取措施 102
VirusScan 警报对话框 102
按需扫描进程对话框 103

5 电子邮件扫描 105

按发送电子邮件扫描 106
为本地主机或远程主机配置按发送电子邮件扫描 106
配置按发送电子邮件扫描属性 107
检测属性 107
高级属性 109
操作属性 112
警报属性 114

报告属性 117
查看按发送电子邮件扫描结果 119
查看按发送电子邮件扫描统计信息 119
查看按发送电子邮件活动日志 120
按需电子邮件扫描 121
配置按需电子邮件任务 121
检测属性 121
高级属性 124
操作属性 127
警报属性 130
报告属性 132
运行按需电子邮件任务 135
查看按需电子邮件扫描结果 136
查看按需电子邮件活动日志 136

6 病毒警报 137

配置警报管理器 138
配置收件人和接收方式 142
关于添加警报方法的概述 143
发送测试消息 143
为接收者设置警报优先级 144
查看摘要页 145
将警报消息转发给其他计算机 145
以网络消息的形式发送警报 148
将警报消息发送到电子邮件地址 150
将警报消息发送到打印机 154
通过 SNMP 发送警报消息 155
将程序作为警报启动 156
在计算机的事件日志中记录警报通知 158
向终端服务器发送网络消息 160
使用集中警报 162
自定义警报消息 163
启用和禁用警报消息 164
编辑警报消息 164
更改警报优先级 164
编辑警报消息文本 166
使用警报管理器系统变量 166

7 更新 169

更新策略 170
系统变量 171
自动更新任务 172
自动更新任务概述 173
创建自动更新任务 174
配置自动更新任务 174
运行自动更新任务 176
运行更新任务 176
在更新任务执行过程中发生的活动 178
查看活动日志 178
自动更新资料库列表 179
自动更新资料库 179
配置自动更新资料库列表 180
导入自动更新资料库列表 180
编辑自动更新资料库列表 181
添加和编辑资料库 181
删除和重新组织资料库 186
指定代理服务器设置 187
镜像任务 189
创建镜像任务 190
配置镜像任务 191
运行镜像任务 193
查看镜像任务活动日志 194
回滚 DAT 文件 195
手动更新 196
从 DAT 存档文件更新 197

8 计划任务 199

配置任务计划 200
任务属性 201
计划属性 202
计划任务运行频率 203
高级计划选项 204
按频率计划任务 205
每天 205
每周 207
每月 208

一次 209
系统启动时 211
登录时 211
空闲时 213
立即运行 214
拨号时运行 215

A 命令行扫描程序 217

VirusScan Enterprise 命令行选项 218
按需扫描命令行选项 224
自定义的安装属性 226

B 安全注册表 229

要求写权限的注册表项 230

C 故障排除 237

最小扩展工具 238
常见问题 238
安装问题 239
扫描问题 240
病毒问题 240
常规问题 241
更新错误代码 244

词汇表 245

索引 257

序言

本指南为您介绍了 McAfee ® VirusScan® Enterprise 7.1.0 版，并提供了下列信息：

- 产品概述。
- 产品功能的描述。
- 本版软件中所有新功能的说明。
- 配置和部署本软件的详细说明。
- 执行任务的步骤。
- 故障排除信息。
- 术语表。

读者

这些信息主要面向两种读者：

- 负责公司防病毒程序和安全程序的网络管理员。
- 负责更新计算机中的病毒定义 (DAT) 文件或者配置本软件检测选项的用户。

排版规范

本指南使用了如下排版规范：

粗体	用户界面（包括选项、菜单、按钮和对话框名称）上的所有文字。 示例 键入所需帐户的“**用户名**”和“**密码**”。
`Courier`	表示用户键入的具体内容，例如按照系统提示输入的命令。 示例 要启用代理程序，请在客户机上运行下面这一行命令： `FRMINST.EXE /INSTALL=AGENT/SITEINFO=C:\TEMP\SITELIST.XML`
< 术语 >	普通术语用尖括号括起来。 示例 在控制台树中的 **ePolicy Orchestrator** 下，右键单击 < 服务器 >。
注释	补充信息，例如执行同一个命令的另一种方法。
警告	对保护用户、计算机系统、企业、数据或安装的软件的重要建议。

获取信息

安装指南 *†	安装和启动本软件的系统要求和指导。 《VirusScan Enterprise 7.1.0 安装指南》
产品指南 *	产品介绍和功能；关于配置本软件的详细说明；关于部署、重复执行任务和操作步骤的信息。 《VirusScan Enterprise 7.1.0 产品指南》
帮助 §	关于配置和使用本软件的高级信息和详细信息。 “这是什么？”上下文相关帮助。
配置指南 *	与 ePolicy Orchestrator™ 配合使用。通过 ePolicy Orchestrator 管理软件来配置、部署和管理 McAfee Security 产品的步骤。
实施指南 *	关于产品功能、工具和组件的补充信息。
发行说明 ‡	自述文件。产品信息、已解决的问题、所有已知问题以及对产品或其文档所做的最新增补或修订。
联系 ‡	McAfee Security 和 Network Associates 服务和资源的联系信息：技术支持、客户服务、 AVERT （防病毒紧急响应小组）、测试程序以及培训。该文件也包括 Network Associates 驻美国及全球办事处的电话号码、街道地址、网址和传真号码。

* 从产品光盘或 McAfee Security 下载站点可以获得 Adobe Acrobat .PDF 格式的文件。

† 以产品光盘附带的印刷手册形式提供。注释：有些语言的手册可能只有 .PDF 格式的文件。

‡ 软件应用程序和产品光盘中包含的文本文件。

§ 可从软件应用程序中访问的“帮助”：用来获得页面帮助信息的“帮助”菜单和 / 或“帮助”按钮；右键单击“这是什么？”帮助功能之后出现的选项。

与 McAfee Security 和 Network Associates 联系

技术支持	
主页	http://www.networkassociates.com/us/support/
KnowledgeBase 搜索	https://knowledgemap.nai.com/phpclient/homepage.aspx
PrimeSupport 服务门户网站 *	http://mysupport.nai.com
McAfee Security 测试程序	http://www.networkassociates.com/us/downloads/beta/
Security HQ - AVERT（防病毒紧急响应小组）	
主页	http://www.networkassociates.com/us/security/home.asp
病毒信息库	http://vil.nai.com
提交样本 -AVERT WebImmune	https://www.webimmune.net/default.asp
AVERT DAT 通知服务	http://www.networkassociates.com/us/downloads/updates/
下载站点	
主页	http://www.networkassociates.com/us/downloads/
DAT 文件和引擎更新	http://www.networkassociates.com/us/downloads/updates/
	ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
产品升级 *	https://secure.nai.com/us/forms/downloads/upgrades/login.asp
培训	
McAfee Security 大学	http://www.networkassociates.com/us/services/education/mcafee/university.htm
Network Associates 客户服务	
电子邮件	services_corporate_division@nai.com
网址	http://www.nai.com/us/index.asp http://www.networkassociates.com/us/products/mcafee_security_home.htm
美国、加拿大和拉丁美洲免费电话：	
电话	**+1-888-VIRUS NO** 或 **+1-888-847-8766** 星期一到星期五，中部时间上午 8:00 - 下午 8:00

McAfee 非常重视客户的反馈意见，并愿意根据客户的反馈信息改进我们的解决方案。如果您对 McAfee 产品中的语言问题存在任何意见或建议，请通过如下电子邮件地址与我们联系：

B2BLoc_ZH-CN@nai.com

关于与 Network Associates 和 McAfee Security 联系的详细信息（包括其他地区的免费电话号码），请参阅本产品附带的 Contact 文件。

* 需要登录证书。

VirusScan Enterprise 简介 1

VirusScan Enterprise 7.1.0 软件能够为服务器和工作站提供病毒防护措施。本软件提供的防护措施扩展方便、快速而且异常灵活。您可以将本地驱动器、网络驱动器以及 Microsoft Outlook 电子邮件及附件指定为扫描目标、将该应用程序配置为在扫描程序发现病毒时及时响应，并对其扫描操作生成报告。

VirusScan Enterprise 软件是如下软件的替代产品：

- VirusScan 4.5.1 工作站版本。
- NetShield® NT 4.5 服务器版本。
- 适用于 Celerra™ 文件服务器的 NetShield for Celerra™ 4.5。
- VirusScan Enterprise 7.0 工作站和服务器版本。

本 《产品指南》为您提供了配置和使用 VirusScan Enterprise 软件的相关信息。关于系统要求和安装说明，请参阅 《VirusScan Enterprise 7.1.0 安装指南》。

这部分包含下列主题：

- 本版本的新功能
- 产品组件

本版本的新功能

本版本的 VirusScan Enterprise 包括下列增强功能：

- **Check Point™ VPN-1® /FireWall-1® SCV 集成** - 改进之后，VirusScan Enterprise 软件可以与 Check Point VPN-1/FireWall-1 SCV 集成。安装并启用了 Check Point 产品之后，可以将其配置为禁止没有采用最新防病毒保护措施的客户端通过虚拟专用网络 (VPN) 访问公司网络。

  关于配置 Check Point 的详细信息，请参阅 《VirusScan Enterprise 7.1.0 安装指南》。

- **McAfee Installation Designer™ 及 McAfee Desktop Firewall™ 集成** - 使用 McAfee Installation Designer 可以针对 VirusScan Enterprise 7.1.0 配置 McAfee Desktop Firewall。配置之后，您可以同时部署这两个产品，并将重新启动的次数减少为一次。

  详细信息，请参阅 《McAfee Installation Designer Product Guide》。

- **更小的安装包** - 我们已使用 Netopsystems 的电子应用程序快速分发 (FEAD® Optimizer®) 技术对 VirusScan Enterprise 安装包进行了优化。这减少了部署时需要的网络带宽。您可以使用 McAfee Installation Designer 7.1 或更高版本来重新组织安装包，然后在更改之后重新对其优化。当从命令行执行 SETUP.EXE 时，可以使用特殊的命令和开关来重新组织安装文件。

  关于配置 Netopsystems 的 FEAD Optimizer 的详细信息，请参阅《VirusScan Enterprise 7.1.0 安装指南》。

- **引擎和 DAT 文件包含在 .MSI 文件中** - 引擎和 DAT 文件加入到了 VirusScan Enterprise 7.1.0 的 .MSI 文件中。这样，用户可以使用单个的 .MSI 文件来部署本产品。

- **ePolicy Orchestrator任务可见**-如果是用ePolicy Orchestrator 3.0或更高版本来管理 VirusScan Enterprise 软件，您可以在 VirusScan 控制台中查看 ePolicy Orchestrator 按需扫描任务、更新任务和镜像任务。这样，用户就可以查看他们的计算机中运行的各项任务，管理员和帮助台操作员也可以通过电话解决 ePolicy Orchestrator 任务的问题。

  关于启用 ePolicy Orchestrator 任务可见功能的详细信息，请参阅 《VirusScan Enterprise 7.1.0 配置指南 - 与 ePolicy Orchestrator 3.0 配合使用》。

产品组件

VirusScan Enterprise 软件包含若干个功能组件。所有功能共同构成了防御计算机病毒和其他有害软件的屏障。这些功能包括：

- **VirusScan 控制台**。控制台是一个控制点，允许您创建、配置和运行 VirusScan Enterprise 任务。任务可以包含任何操作，例如在指定的时间或按一定时间间隔在一组驱动器上运行扫描，或者执行更新操作。如果具有管理员权限并根据需要输入了密码，您还可以从控制台启用或禁用按访问扫描程序。

  请参阅第 19 页的 “VirusScan 控制台”。

- **按访问扫描程序**。按访问扫描程序可以为您提供连续的防病毒保护，以防范来自磁盘、网络或 Internet 上各种病毒来源的病毒。这一扫描程序在安装本软件时即已完全配置，它会在您启动计算机时启动，并驻留在内存中，直到计算机关闭。它提供了基于进程的扫描方式，允许您将扫描策略链接到 Internet Explorer 这样的应用程序。您可以使用一组灵活的属性页来配置扫描程序，以便确定要检查系统的哪些部分、查找哪些内容、忽略哪些部分以及如何处理扫描程序发现的感染病毒的文件。此外，这种扫描程序可以在发现病毒时向您发出警报，并为每个操作生成摘要报告。

  请参阅第 35 页的 “按访问扫描”。

- **按需扫描程序**。使用按需扫描程序，您可以随时开始扫描、指定扫描和不扫描的目标、确定扫描程序在检测到病毒时的响应方式以及查看病毒事件报告和警报。此外，也可以创建在特定时间或者在指定的时间间隔内运行的扫描任务。还可以根据需要定义各种按需扫描任务，然后保存配置好的任务，以便重新使用。

  请参阅第 77 页的 “按需扫描”。

- **电子邮件扫描程序**。电子邮件扫描程序允许您扫描 Microsoft Outlook 邮件、附件或者直接扫描计算机中您有权访问的公共文件夹。如果正在运行 Outlook，它将在您收发邮件时扫描电子邮件。您也可以随时执行按需电子邮件扫描。这一功能可以及时发现试图进入您计算机的潜在病毒。

  请参阅第 105 页的 “电子邮件扫描”。

- **自动更新**。自动更新功能允许您自动更新病毒定义 (DAT) 文件和扫描引擎，然后将这些更新分发给网络中的计算机。您也可以使用这一功能来下载 HotFix。根据网络的规模，您可以指定一台或多台信任的计算机（包括贵公司内部的 HTTP 站点主机）自动从 Network Associates HTTP 网站下载新文件。

  请参阅第 169 页的 “更新”。

  注释
  自动更新功能是许多产品共用的一种核心 (Common Framework) 技术。

- **计划程序**。该功能允许您命令按需扫描任务、更新任务和镜像任务在特定时间或按一定时间间隔运行。

  请参阅第 199 页的 “计划任务”。

  注释
  计划程序功能是许多产品共用的一种核心 (Common Framework) 技术。

- **警报管理器**。 Alert Manager ™ （警报管理器）产品使您能够接收或发送病毒警报消息。安装了警报管理器之后，您就可以将它配置为在扫描程序检测到计算机病毒时通过电子邮件、打印机、 SNMP 陷阱或其他方式通知您。默认情况下，警报管理器并未预先配置，因此您必须首先配置本软件，才能接收或发送病毒警报消息。

  详细说明，请参阅第 137 页的 “病毒警报”。

- **命令行扫描程序**。使用命令行扫描程序，您可以从 “命令提示符”对话框中对目标进行扫描。SCAN.EXE 是一个只能在 Windows NT 环境中使用的扫描程序，也是主要的命令行界面。

  通常情况下，您可以通过 VirusScan Enterprise 界面执行大多数扫描操作，但如果在启动 Windows 时遇到问题，或者 VirusScan Enterprise 功能无法在您的环境中运行，您可以转而使用命令行扫描程序。

  请参阅第 217 页的 “命令行扫描程序”。

入门 2

安装了 VirusScan Enterprise 软件之后，您就可以配置它的功能。

这部分包含下列主题：

- 面向用户的界面
- 设置用户界面选项
- 设置扫描操作
- 病毒信息库
- 提交病毒样本
- 设置远程管理

面向用户的界面

使用 VirusScan Enterprise 软件，您可以灵活地运用多种不同方法执行操作。尽管具体细节有所不同，但很多操作都可以从控制台、工具栏、菜单或桌面执行。下面这几部分为您详细介绍了每种方法。

这部分将介绍以下界面：

- 开始菜单
- VirusScan 控制台
- 右键菜单
- 系统任务栏
- 命令行

开始菜单

通过 “开始”菜单，您可以：

- 访问警报管理器配置，但前提是已经安装了警报管理器。
- 访问 “**VirusScan 控制台**”。
- 打开按访问扫描属性页。
- 打开按需扫描属性页。这是一种一次性未保存的按需扫描。

单击 “**开始**”并选择 “**程序**” | “**Network Associates**”，然后选择一个功能。

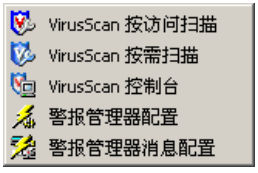

图 2-1. VirusScan - “开始”菜单

VirusScan 控制台

“**VirusScan 控制台**”是所有程序活动的控制点。

使用以下方法之一打开 “**VirusScan 控制台**”：

- 单击“**开始**”，并选择“**程序**” | “**Network Associates**” | “**VirusScan 控制台**”。
- 右键单击系统任务栏中的 VShield 图标，然后选择“**VirusScan 控制台**”。

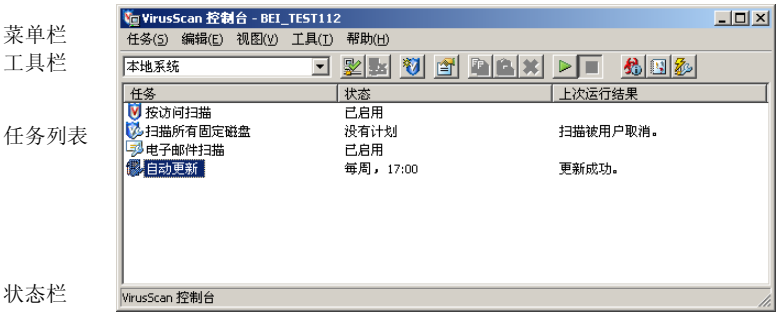

图 2-2. VirusScan 控制台

这部分包含下列主题：

- 菜单栏
- 工具栏
- 任务列表
- 状态栏

菜单栏

使用 “**VirusScan 控制台**”菜单中的命令，您可以创建、删除、配置、运行、启动、停止和复制扫描任务，从而满足自己哪怕极为苛刻的安全需要。您还可以建立或断开远程 VirusScan Enterprise 计算机连接。所有这些命令都可以从菜单中找到。此外，右键单击 “**VirusScan 控制台**”中的任务也可以找到某些命令。

这部分将介绍下列菜单：

- 任务菜单
- 编辑菜单
- 视图菜单
- 工具菜单
- 帮助菜单

任务菜单

使用 “**任务**”菜单，您可以创建和配置任务并查看统计信息及活动日志。

图 2-3. “任务”菜单

注释

“**启动**”、“**停止**”、“**禁用**”、“**删除**”、“**重命名**”、“**统计信息**”、“**活动日志**”和 “**属性**”等菜单项将应用于所选的任务。

编辑菜单

使用 “**编辑**”菜单，您可以复制和粘贴所选的任务。

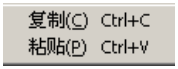

图 2-4. “编辑”菜单

视图菜单

使用 “**视图**”菜单，您可以指定是否显示工具栏和状态栏，也可以刷新控制台。

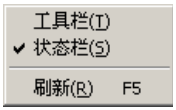

图 2-5. “视图”菜单

工具菜单

使用 “**工具**”菜单，您可以配置警报、启动事件查看器、指定用户界面选项、锁定或解锁用户界面安全性、在配置远程控制台时建立或断开计算机连接、导入或编辑资料库列表以及将 DAT 文件回滚至上一版本。

图 2-6. “工具”菜单

帮助菜单

使用“**帮助**”菜单，您可以访问联机帮助主题、病毒信息库或技术支持网站，还可以向防病毒紧急响应小组 (AVERT) 提交病毒样本。“**关于**”对话框提供了您的产品、 DAT 文件版本和扫描引擎的相关信息。

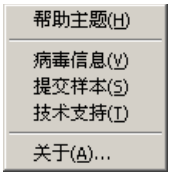

图 2-7. “帮助”菜单

工具栏

只需单击工具栏图标，您就可以快速存取多种命令。这些图标包括：

- 连接到计算机。
- 断开与计算机的连接。
- 创建新任务。
- 显示所选项的属性。
- 复制所选项。
- 粘贴所选项。
- 删除所选项。
- 启动所选项。
- 停止所选项。
- 访问病毒信息库。
- 打开事件查看器。
- 配置警报选项。

任务列表

“**VirusScan 控制台**”包括 VirusScan Enterprise 可以执行的任务列表。任务是一组命令，用来按照特定的配置、在特定的时间运行某个程序或扫描操作。

图 2-8. 任务列表

要配置某个任务，请选择这项任务并单击  ，或者双击这项任务打开它的属性页。 VirusScan Enterprise 软件具有以下几项默认任务：

- **按访问扫描**。使用这项任务，您可以执行自动按访问扫描。这项任务是唯一的，不能复制。要配置按访问扫描程序，请参阅第 35 页的 “按访问扫描”。
- **自动更新**。使用这项任务，您可以下载最新的病毒定义 (DAT) 文件和扫描引擎。为了满足自己的需要，您可以在使用这一默认更新任务的同时创建其他更新任务。要创建、配置和计划更新任务，请参阅第 169 页的 “更新”。
- **电子邮件扫描**。使用这项任务，您可以执行按发送电子邮件扫描。这项任务是唯一的，不能复制。要配置按发送任务或按需电子邮件任务，请参阅第 105 页的 “电子邮件扫描”。
- **扫描所有固定磁盘**。使用这项任务，您可以执行按需扫描。为了满足自己的需要，您可以在使用这一默认按需扫描任务的同时创建其他任务。要创建、配置和计划按需任务，请参阅第 77 页的 “按需扫描”。

您从 **VirusScan 控制台**创建的其他任务将被添加到任务列表中。例如：

- **新建镜像任务**。使用这项任务，您可以创建一个镜像站点以便下载更新文件。您可以创建任意多个镜像任务。关于镜像任务的详细信息，请参阅第 189 页的 “镜像任务”。

另外，如果需要，您可以查看通过 ePolicy Orchestrator 创建的任务。

- **ePO 任务 - 任务名称**。如果正在使用 ePolicy Orchestrator 3.0 或更高版本来管理 VirusScan Enterprise 软件，您可以选择在“**VirusScan 控制台**”中查看 ePolicy Orchestrator 任务。这适用于按需任务、更新任务和镜像任务。要了解如何启用 ePolicy Orchestrator 任务可见功能，请参阅《VirusScan Enterprise 配置指南 - 与 ePolicy Orchestrator 3.0 配合使用》。

状态栏

状态栏显示了当前活动的状态。

右键菜单

通过右键菜单可以快速访问常用的操作，例如创建新任务、查看任务统计信息和日志、打开任务属性页或者扫描特定的文件或文件夹。

- **控制台右键菜单**。“**VirusScan 控制台**”提供的右键菜单不尽相同，这主要取决于是否选择了任务列表中的任务以及选择了哪些任务。详细信息，请参阅第 24 页的 “控制台右键菜单”。
- **右键扫描**。使用右键扫描功能，您可以选择特定的文件或文件夹并立即扫描病毒。详细信息，请参阅第 25 页的 “右键扫描”。
- **系统任务栏右键扫描**。使用邮件扫描功能，您可以创建一次性未保存的按需扫描任务。详细信息，请参阅第 25 页的 “系统任务栏右键扫描或更新”。

控制台右键菜单

右键单击任务列表中的某一项时，您会获得如下选项：

- **按访问扫描**。通过右键单击任务列表中的按访问扫描任务，您可以启用或禁用这项任务、查看任务统计信息、打开属性页以及查看活动日志。
- **更新**。通过右键单击任务列表中的更新任务，您可以启动、停止、删除和重命名这项任务，也可以查看活动日志和打开属性页。
- **电子邮件扫描**。通过右键单击任务列表中的电子邮件扫描任务，您可以启用或禁用这项任务、查看任务统计信息、打开属性页以及查看活动日志。
- **按需扫描**。通过右键单击任务列表中的按需扫描，您可以启动、停止、复制、粘贴、删除、重命名这项任务，也可以查看任务统计信息、打开属性页以及查看活动日志。

当右键单击控制台中的空白区域时，无需选择任务列表中的任一项即可执行下列操作：

- **新建扫描任务**。创建新的按需扫描任务。
- **新建更新任务**。创建新的更新任务。

- **新建镜像任务**。创建新的镜像任务。
- **粘贴**。将复制的任务粘贴到任务列表中。
- **用户界面选项**。访问 “**用户界面选项**” 属性页。要了解如何设置这些选项，请参阅第 26 页的 “设置用户界面选项”。

右键扫描

只需在 Windows 资源管理器中右键单击某个文件或文件夹，然后选择 “**扫描病毒**”，即可对其执行立即按需扫描。这也被称作 Shell 扩展扫描。系统将直接调用按需扫描程序，并启用所有扫描设置（例如存档扫描、启发式扫描）和其他选项。如果怀疑特定的文件夹或文件感染了病毒，这样做会很有用。

发现的感染病毒的文件或文件夹会以列表形式列出，并在扫描对话框底部详细说明感染病毒的项目。您可以右键单击列表中感染病毒的项目并选择清除、删除或移动来对其采取措施。

当执行右键扫描时，不能自定义扫描选项。要详细了解如何自定义扫描选项或者创建新的按需扫描任务，请参阅第 78 页的 “创建按需扫描任务”。

系统任务栏

默认情况下，典型安装将安装按访问扫描程序，而且该程序会自动激活。一旦激活，该扫描程序就会在 Windows 系统任务栏中显示 Vshield 图标 。

双击系统任务栏中的 可查看 “**按访问扫描统计信息**”。

系统任务栏右键扫描或更新

使用这项功能，您可以创建一次性未保存的按需扫描任务或更新任务。如果希望在计划的定期按需扫描之外快速扫描某个驱动器、文件夹或文件，或者希望立即更新，该功能会很有用。

右键单击系统任务栏中的 会显示这个菜单。

图 2-9. 系统任务栏菜单

系统任务栏菜单包括如下选项：

- **VirusScan 控制台**。显示 “**VirusScan 控制台**”。
- **禁用按访问扫描**。取消激活按访问扫描程序。该功能会在 “**禁用按访问扫描**” 和 “**启用按访问扫描**” 之间切换。
- **按访问扫描属性**。打开按访问扫描程序属性页，从中可以配置按访问扫描程序。
- **按访问扫描统计信息**。查看按访问扫描程序统计消息。您可以启用或禁用按访问扫描程序，也可以打开按访问扫描程序属性页。
- **按访问扫描消息**。查看按访问扫描程序消息。您可以删除消息、清除文件病毒、删除文件或移动文件。
- **按需扫描**。打开按需扫描程序属性页，从中可以配置按需扫描程序以执行一次性未保存的按需扫描。
- **立即更新**。通过默认的更新任务立即更新。

  注释
  “**立即更新**”只对在安装本产品时创建的默认更新任务有效。您可以重命名和重新配置默认的更新任务，但如果删除了默认任务，“**立即更新**”将被禁用。

- **关于 VirusScan Enterprise**。查看本产品的许可信息以及与安装的软件有关的特定信息，例如病毒定义 (DAT) 文件和扫描引擎版本号。

命令行

您可以使用命令行功能从命令提示符执行操作。详细信息，请参阅第 217 页的 “命令行扫描程序”。

设置用户界面选项

您可以使用这些选项指定当通过 McAfee Installation Designer 安装本程序时使用的显示设置和密码设置，也可以在安装之后从 “**VirusScan 控制台**” 的 “**工具**” 菜单中指定这些设置。

这部分将介绍如何从控制台设置显示选项和密码选项。这部分包含下列主题：

- 显示选项
- 密码选项
- 解锁和锁定用户界面

显示选项

使用“**显示选项**”对话框，您可以决定用户可访问哪些系统任务栏选项并设置本地控制台的刷新时间。

要从控制台设置显示选项：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 选择“**工具**”|“**用户界面选项**”|“**显示选项**”。

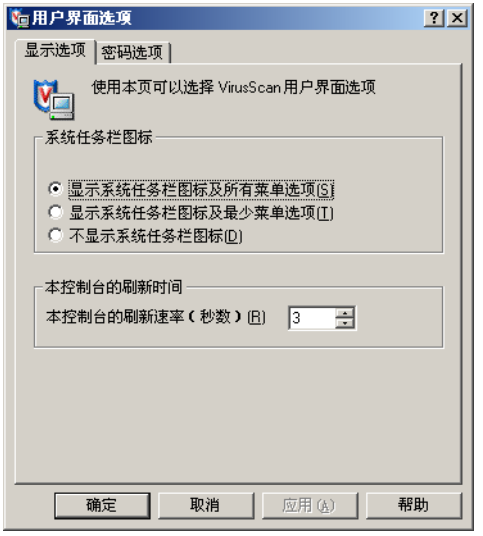

图 2-10. 显示选项

3 决定用户可以看到哪些系统任务栏选项。在“**系统任务栏图标**”下，选择一个选项：

- **显示系统任务栏图标及所有菜单选项**。该选项为默认选项，表示允许用户看到系统任务栏中的所有菜单选项。
- **显示系统任务栏图标及最少菜单选项**。将右键菜单项限制为只包括“**关于**”和“**按访问扫描统计信息**”。所有其他右键菜单项都将隐藏。
- **不显示系统任务栏图标**。不允许用户访问系统任务栏图标。

4 在“**本控制台的刷新时间**”下，选择以秒为单位的控制台刷新频率。

5 单击“**应用**”，然后单击“**确定**”保存更改并关闭该对话框。

密码选项

使用“**密码选项**”对话框，您可以设置整个系统的安全密码，也可以只为所选的选项卡和控件设置安全密码。同一个密码将应用于选定的所有选项卡和控件。

设置密码将对用户产生以下影响：

非管理员 - 不具有 Windows NT 管理员权限的用户。非管理员用户总是以只读模式运行所有 **VirusScan Enterprise** 应用程序。他们可以查看某些配置参数、运行以前保存的扫描任务以及运行立即扫描和更新，但不能更改任何配置参数或者创建、删除或修改以前保存的扫描任务和更新任务。

管理员 - 具有 Windows NT 管理员权限的用户。如果尚未设置密码，管理员可以以读 / 写模式运行所有 VirusScan Enterprise 应用程序。他们可以查看和修改所有配置参数、运行任务并创建、删除和修改以前保存的扫描任务和更新任务。如果设置了密码，则在输入安全密码之前，管理员只能以只读模式查看受保护的选项卡和控件。管理员也可以通过控制台锁定或解锁用户界面。详细信息，请参阅第 30 页的“解锁和锁定用户界面”。

> **注释**
> 一个锁住的红色挂锁表示这一项需要输入密码才能使用。开启的绿色挂锁表示这一项处于可以读 / 写的状态。

要从控制台设置密码选项：

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。
2. 选择“**工具**”|“**用户界面选项**”|“**密码选项**”。

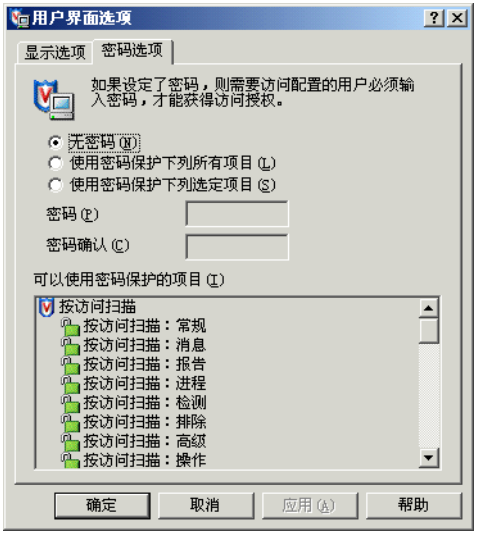

图 2-11. 密码选项

3 选择以下选项之一：

- **无密码**。该选项为默认选项。
- **使用密码保护下列所有项目**。用户必须输入指定的密码，才能访问本软件中锁定的任何选项卡或控件。
  - 选择 “**使用密码保护下列所有项目**”。
  - 键入并确认密码。
- **使用密码保护下列选定项目**。用户必须输入指定的密码，才能使用此处锁定的项目。未锁定的项目不要求输入密码。
  - 选择 “**使用密码保护下列选定项目**”。
  - 键入并确认密码。
  - 选择要受这个密码保护的所有项目。

4 单击 “**应用**” 保存更改。

5 单击 “**确定**”。

警告

如果 “**控制台和杂项**” 密码项被锁定，您将不能执行以下操作：

- 启用或禁用按访问扫描 - 用来启用和禁用按访问扫描功能的菜单项以及具有同等功能的工具栏图标将被禁用。另外，“**VirusScan 按访问扫描统计信息**” 对话框中的 “**禁用**” 按钮也将被禁用。
- 启用或禁用电子邮件扫描 - 用来启用和禁用电子邮件扫描功能的菜单项以及具有同等功能的工具栏图标将被禁用。另外，“**VirusScan 按发送电子邮件扫描统计信息**” 对话框中的 “**禁用**” 按钮也将被禁用。
- 创建新的按需扫描任务、更新任务或镜像任务 - 用来创建新任务的菜单项以及具有同等功能的工具栏图标将被禁用。除按需扫描任务之外，“**VirusScan 按需扫描属性**” 对话框中的 “**另存为**” 和 “**另存为默认值**” 按钮也将被禁用。
- 删除任务 - 用来删除任务的菜单项以及具有同等功能的工具栏图标将被禁用。
- 重命名任务 - 用来重命名任务的菜单项以及具有同等功能的工具栏图标将被禁用。
- 复制或粘贴任务 - 用来复制和粘贴任务的菜单项以及具有同等功能的工具栏图标将被禁用。
- 回滚 DAT 文件 - 用来回滚 DAT 文件的菜单项将被禁用。

解锁和锁定用户界面

管理员可以从控制台解锁和锁定受密码保护的选项卡和控件。

注释

如果为所有项目都选择了密码保护，则“**用户界面选项**”对话框也会自动受到保护。如果为所有项目都设置了密码保护而且用户退出了系统，则用户界面会再次自动锁定。

要解锁用户界面：

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的 “VirusScan 控制台”。
2. 选择“**工具**” | “**解锁用户界面**”。

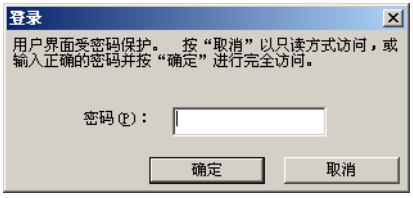

图 2-12. 安全密码

3. 键入密码。
4. 单击“**确定**”。

要锁定用户界面：

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的 “VirusScan 控制台”。
2. 选择“**工具**” | “**锁定用户界面**”。

设置扫描操作

本 VirusScan Enterprise 软件提供了可满足不同需要的各种扫描。

这部分包含下列主题：

- 按访问扫描与按需扫描的比较
- 自动扫描
- 定期扫描、选择性的扫描或按计划扫描

按访问扫描与按需扫描的比较

VirusScan Enterprise 软件可以执行两种类型的扫描活动，这两种扫描活动分别是：

- 自动扫描
- 定期扫描、选择性的扫描或按计划扫描

按访问扫描。自动扫描病毒称为按访问扫描。您必须有管理员权限和密码（如果需要）才能配置按访问扫描。详细信息，请参阅第 32 页的 “自动扫描”。

按需扫描。定期扫描、选择性的扫描或事先计划的扫描称为按需扫描。您必须有管理员权限和密码（如果需要）才能制定按需扫描任务计划，但所有用户都可以运行按需任务。详细信息，请参阅第 32 页的“定期扫描、选择性的扫描或按计划扫描”。

按访问扫描程序可以通过在后台持续扫描来保护您的计算机，因此表面看来运行按需扫描任务似乎是多余的。然而，良好的防病毒安全措施应同时包括彻底、定期的系统扫描，这是因为：

- **按访问扫描操作只在文件被访问或使用时检查文件**。按访问扫描程序只在文件被使用时查找文件中的病毒。如果系统中的文件很少使用但已感染了病毒，按访问扫描程序也只会在该文件被使用时对其进行检测。但按需扫描操作可以检测到硬盘中感染病毒的文件，即使您并未使用这些文件。因此，按需扫描操作可以在文件被使用之前检测到它们感染的病毒。
- **病毒通常无法预知**。如果在启动计算机时软盘还意外留在驱动器中，系统可能会在按访问服务启动之前将病毒加载到内存中，特别是在您未将这项服务配置为扫描软盘时。一旦进入内存，恶性病毒几乎可以感染所有程序。
- **按访问扫描占用时间和资源**。如果在运行、复制或保存文件时扫描病毒，软件和其他任务会被推迟启动。在某些情况下，这可能是您需要从事重要工作的时间。虽然影响非常小，但如果需要将可用的全部资源用于某些紧急任务，您也可以禁用按访问扫描。在这种情况下，应在空闲期间执行定期扫描操作，这样既可以防止系统感染病毒，又不会影响工作效率。
- **安全措施越多越好**。如今，大多数计算机用户所在的环境都以网络为中心，从某个来源下载病毒只需片刻时间，您甚至都意识不到自己访问过这个来源。这样，如果由于软件冲突而暂时禁用了后台扫描，或者尚未配置后台扫描来监视易受攻击的进入点，就可能会感染病毒。定期扫描操作通常可以在病毒传播或造成损害之前将其截获。

自动扫描

按访问扫描可以根据用户的活动提供连续、实时的病毒检测和响应。 VirusScan Enterprise 防病毒软件程序提供了一个单独的按访问扫描任务，即在网络用户每次向计算机写入文件或从计算机中读取文件时检查病毒。它会尝试清除找到的所有病毒，并在日志文件中记录它的活动。您可以更改它的设置来确定：

- 要扫描的文件和文件类型。
- 执行扫描的突发条件。
- 扫描程序在检测到病毒时采取的操作。
- 扫描程序活动报告的内容 （如果有）。
- 排除在按访问扫描操作之外的文件。

关于配置按访问扫描的详细信息，请参阅第 35 页的 “按访问扫描”。

定期扫描、选择性的扫描或按计划扫描

按需扫描任务共有两种类型：

- 未保存的一次性按需扫描任务。
- 可保存的按需扫描任务。

用户可以配置和事先计划未保存的一次性按需扫描任务，但除非您选择保存，否则它不会保存下来供日后使用。

您可以事先计划可保存的按需扫描任务，并在认为必要时运行或者按计划定期运行。您可以针对网络中的特定目标位置创建任意多个扫描任务。这个特殊位置可以小范围地定义为特定的驱动器、文件夹或文件，也可以广泛地定义为多个驱动器、文件夹或文件。一旦创建了可保存的扫描任务，在从“**VirusScan 控制台**”中将它们删除之前，它们将一直可用。您也可以根据需要编辑它们。

关于设置按需扫描活动的完整论述，请参阅第 77 页的 “按需扫描”。

病毒信息库

McAfee Security 防病毒紧急响应小组 (AVERT) 的病毒信息库包含关于病毒来源、它们如何感染系统以及应如何将它们删除的详细信息。

除真正的病毒外，病毒信息库还包含关于欺骗性病毒的有用信息以及关于能够摧毁硬盘的电子邮件附件的危险电子邮件警告。 Virtual Card For You 和 SULFNBK 是众多欺骗性病毒中最臭名昭著的两个病毒。下次收到善意的病毒警告时，请在将邮件发给您的朋友之前先查看我们的欺骗性病毒网页。

要访问病毒信息库：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 19 页的 “VirusScan 控制台”。

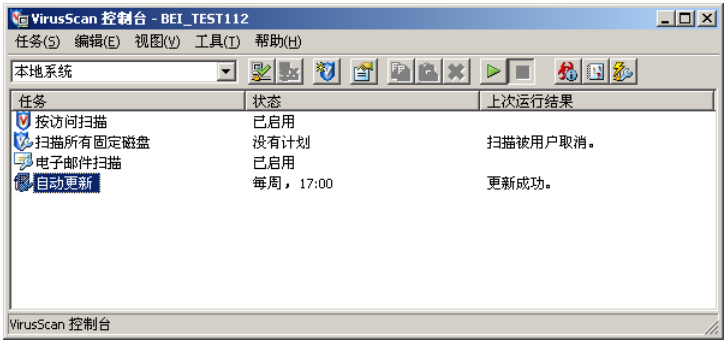

图 2-13. VirusScan 控制台

2 选择 “**帮助**”菜单中的 “**病毒信息**”。

提交病毒样本

如果怀疑某个文件含有病毒，或者遇到可能由病毒感染造成的系统问题， McAfee Security 建议您向 McAfee 的防病毒研究小组发送一个样本以进行分析。提交之后，小组会进行分析，如果您提供了担保，他们还将实时修复文件。

要向 AVERT 提交病毒样本：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 19 页的 “VirusScan 控制台”。

2 选择 “**帮助**”菜单中的 “**提交样本**”。

3 按照网站上的指示进行操作。

设置远程管理

您可以执行的操作包括在远程计算机中修改或计划扫描任务或更新任务以及启用或禁用按访问扫描程序。要这样做，您必须具有管理员权限，而且远程注册服务必须已经运行。

注释

如果不具有连接到远程计算机的管理员权限，您会收到“用户权限不足，拒绝访问”这样一条错误消息。

启动了“**VirusScan 控制台**”之后，已经连接的计算机的名称将出现在控制台标题栏以及控制台工具栏左侧的菜单中。如果没有连接到网络中的任何计算机，标题栏将显示本地计算机的名称。

要管理安装有 VirusScan Enterprise 程序的远程计算机：

1 从“**工具**”菜单中，选择“**远程连接**”，或者单击工具栏中的 。

屏幕上将显示“**连接到远程计算机**”对话框。

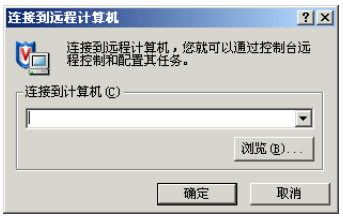

图 2-14. 连接到远程计算机

2 单击 并选择“**连接到计算机**”列表中的某个计算机，或者在文本框中输入要管理的计算机名称。也可以单击“**浏览**”查找网络中的计算机。

注释

如果在配置用于远程任务的文件或文件夹路径名时使用了环境变量，请确保远程计算机中存在这些环境变量。“**VirusScan 控制台**”无法在远程计算机中验证环境变量。

3 单击“**确定**”尝试连接目标计算机。

注释

当与远程计算机连接之后，标题栏会变化以反映这台计算机的名称，同时任务列表中的任务将变为供远程计算机使用的那些任务。用户可以为远程计算机添加、删除或重新配置任务。

“**控制台**”会读取远程计算机的注册表，并显示远程计算机的任务。一旦这些任务出现在控制台中，您就可以在本地计算机中执行它们。

要断开计算机连接，请单击控制台任务栏中的 ，或者选择“**工具**”菜单中的“**断开计算机**”。断开远程计算机连接之后，控制台会刷新以显示本地计算机的任务。

按访问扫描 3

VirusScan Enterprise防病毒程序通过其按访问扫描程序来根据您配置的设置持续、实时地检测和响应计算机病毒。您可以将基于进程的扫描配置为允许将扫描策略链接到应用程序。

如果检测到病毒，按访问扫描程序会详细记录感染病毒的文件信息，同时允许您快速访问这一信息并立即对感染病毒的文件采取措施。

这部分包含下列主题：

- 配置按访问扫描程序
- 查看扫描结果
- 响应病毒检测

配置按访问扫描程序

要确保按访问扫描程序在您的计算机或网络环境中的性能最佳，您需要配置该程序扫描哪些内容、在发现病毒时如何处理以及处理完毕之后如何通知您。

按访问扫描程序自带的配置启用了大多数响应属性。默认情况下，扫描程序被设置为清除它发现的病毒。如果病毒无法清除，默认的辅助操作是隔离病毒。扫描程序还会将这一事件记录到日志文件中。

这部分包含下列主题：

- 按访问扫描属性
- 常规设置
- 进程设置
- 添加文件类型扩展名
- 添加用户指定的文件类型扩展名
- 排除文件、文件夹和驱动器

按访问扫描属性

要配置按访问扫描程序：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

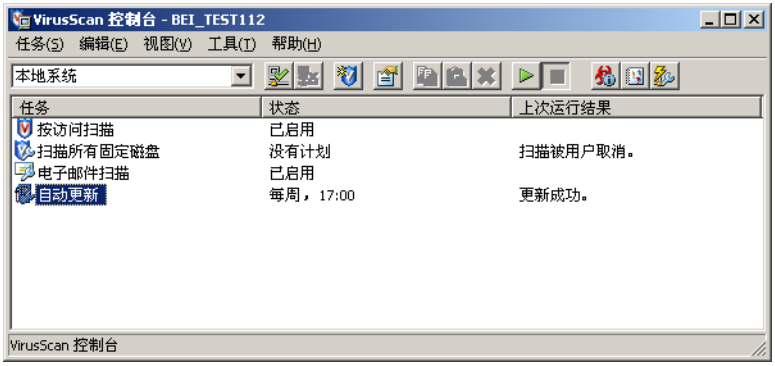

图 3-1. VirusScan 控制台

2 使用以下方法之一，打开 “**按访问扫描属性**”：

- 选择控制台 “**任务**”菜单中的 “**按访问扫描属性**”。
- 右键单击控制台中的 “**按访问扫描**”，然后选择 “**属性**”。
- 双击控制台中的 “**按访问扫描**”。
- 突出显示控制台中的 “**按访问扫描**”，然后单击控制台工具栏中的 。
- 右键单击系统任务栏中的 ，并选择 “**属性**”。
- 单击“**开始**”，然后选择“**程序**”|“**Network Associates**”|“**VirusScan 按访问扫描**”。

屏幕上将出现 “**按访问扫描属性**”对话框。

图 3-2. 按访问扫描属性 - 默认视图

“**按访问扫描属性**”对话框允许您配置常规设置和三种类型的进程。您可以使用该对话框左侧窗格中的图标访问可配置的选项。

首次打开 “**按访问扫描属性**”对话框时，可以从默认视图访问 “**常规设置**”和 “**所有进程**”的属性。

- **常规设置**。为所有进程设置常规检测、消息和报告属性。要详细了解如何设置这些属性，请参阅第 39 页的 “常规设置”。
- **所有进程**。为所有进程设置同样的进程属性、检测属性、高级属性和操作属性，或者为默认进程、低风险进程和 / 或高风险进程设置不同的属性。要详细了解如何设置这些属性，请参阅第 45 页的 “进程设置”。

常规设置

您在“**常规设置**”中指定的属性将作用于默认进程、低风险进程和高风险进程。

您可以配置下列属性：

- 常规属性
- 消息属性
- 报告属性

常规属性

使用“**常规**”选项卡上的选项，您可以为按访问扫描配置基本属性。

1 打开“**按访问扫描属性**”对话框，然后选择左侧窗格中的“**常规设置**”。

2 选择“**常规**”选项卡。

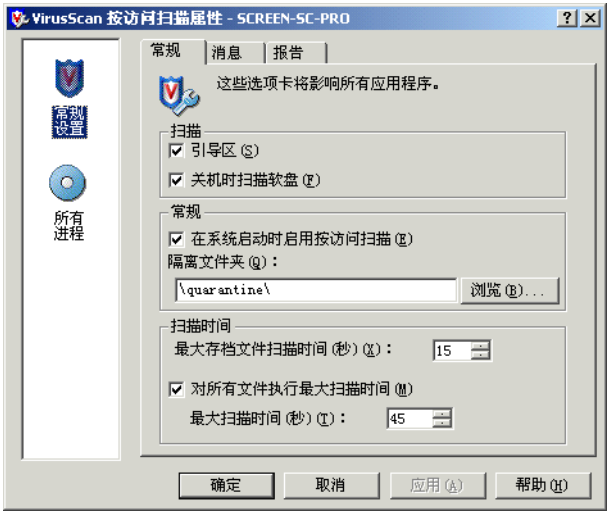

图 3-3. 常规设置 - “常规”选项卡

3 在“**扫描**”下，选择扫描程序要检查计算机的哪些部分。请从以下选项中选择：

- **引导区**。该选项为默认选项，表示将磁盘引导区包括在扫描范围内。如果发现了磁盘，扫描程序会扫描磁盘引导区。在某些情况下，如果磁盘包含无法扫描的个别引导区或特殊引导区，则应禁用引导区分析。
- **关机时扫描软盘**。该选项为默认选项，表示在关闭计算机时，扫描驱动器中的软盘的引导区。如果磁盘感染了病毒，在取出磁盘之前，计算机将不会关闭。

4 在 “常规” 下，选择下列选项之一：

- **在系统启动时启用按访问扫描**。该选项为默认选项，表示在计算机启动时启动按访问扫描服务。
- **隔离文件夹**。接受隔离文件夹的默认位置和名称、输入另一个隔离文件夹位置的路径，或者单击 “浏览” 在本地驱动器中查找适当的文件夹。

  隔离文件夹的默认位置和名称为：

  `< 驱动器 >:\quarantine\`

  注释
  隔离文件夹不应位于软驱或光驱中，它只能在硬盘上。

5 在 “扫描时间” 下，以秒为单位指定所有文件的最大存档和扫描时间。如果一个文件的扫描时间超过了指定的时间，此次扫描将干脆利落地停止，并记录一条消息。如果扫描不能干脆利落地停止，它将终止并重新启动，同时记录另一条消息。请从以下选项中选择：

- **最大存档文件扫描时间（秒）**。默认设置是 15 秒。接受默认设置，或者选择扫描程序在扫描存档文件时可以花费的最大秒数。您选择的存档文件扫描时间必须小于所有文件的扫描时间。
- **对所有文件执行最大扫描时间**。该选项为默认选项，表示为所有文件定义并实行最大扫描时间。
- **最大扫描时间（秒）**。默认设置是 45 秒。接受默认设置，或者选择扫描程序在扫描文件时可以花费的最大秒数。

6 单击 “应用” 保存更改。

消息属性

使用 “**消息**”选项卡上的选项，您可以为按访问扫描配置用户消息属性。

1 打开 “**按访问扫描属性**”对话框，然后选择左侧窗格中的 “**常规设置**”。

2 选择 “**消息**”选项卡。

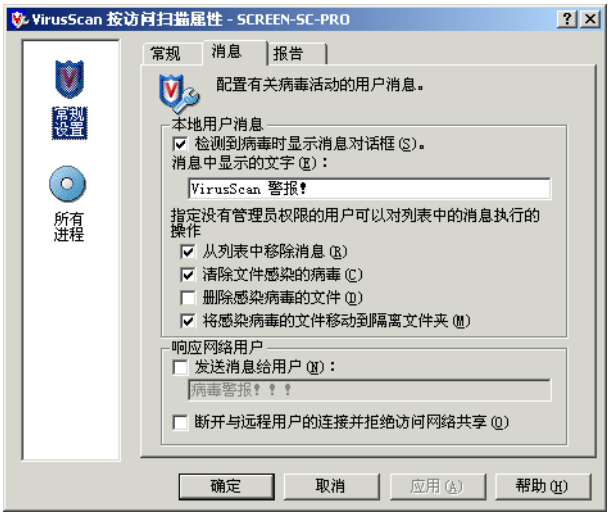

图 3-4. 常规设置 - “消息”选项卡

3 在 “**本地用户消息**”下，选择消息选项。有些消息选项作用于所有用户，而有些消息选项只作用于没有管理员权限的用户。

以下选项作用于所有用户：

- **检测到病毒时显示消息对话框**。该选项为默认选项，表示在检测到病毒时显示 “**按访问扫描消息**”对话框。关于 “**按访问扫描消息**”对话框的详细信息，请参阅第 72 页的 “响应病毒检测”。
- **消息中显示的文字**。如果选择了 “**检测到病毒时显示消息对话框**”，则您可以接受默认的消息，也可以输入要在检测到病毒时显示的自定义消息。默认的消息是 “VirusScan 警报 !”。

以下选项作用于没有管理员权限的用户可以对 “**按访问扫描消息**”对话框中列出的消息执行的操作。请选择以下选项的任意组合：

- **从列表中移除消息**。该选项为默认选项，表示允许没有管理员权限的用户删除列表中的消息。
- **清除文件感染的病毒**。该选项为默认选项，表示允许没有管理员权限的用户清除列表中消息所提及的文件感染的病毒。
- **删除感染病毒的文件**。允许没有管理员权限的用户删除列表中消息所提及的感染病毒的文件。
- **将感染病毒的文件移动到隔离文件夹**。该选项为默认选项，表示允许没有管理员权限的用户将列表中消息所提及的感染病毒的文件移到隔离文件夹中。

4 在 “**响应网络用户**”下，从下列选项中进行选择：

- **发送消息给用户**。在检测到病毒时向网络用户发送消息。例如，如果某个网络用户正在使用远程计算机并通过网络共享访问受保护的文件系统，您可以向这名用户发送一条警报消息。

  如果选择了该选项，您可以接受默认的消息，也可以在屏幕上显示的文本框中输入一个自定义消息。默认的消息是 “VirusScan 警报 !!!”。

  警告
  必须运行 Windows Messenger 服务，才能接收这条消息。

- **断开与远程用户的连接并拒绝访问网络共享**。自动断开那些从您计算机的共享文件夹中读取感染病毒的文件、或向此类文件执行写入操作的用户。之后，扫描程序会改写这些权限，从而将试图读取共享文件夹中感染病毒的文件或向此类文件执行写入操作的用户排除在外。

5 单击 “**应用**”保存更改。

报告属性

使用“报告”选项卡上的选项，您可以配置记录活动并为每个日志条目指定要捕获的信息。

注释

作为一个重要的管理工具，日志文件可以用来跟踪网络中的病毒活动，并记录扫描程序在发现病毒并做出响应时采用了哪些设置。此外，日志文件中记录的事件报告也有助于确定需要使用备份副本替换哪些文件、在隔离文件夹中检查哪些文件或者应从计算机中删除哪些文件。关于如何查看日志的详细信息，请参阅第 72 页的 “查看活动日志”。

要配置 “报告”属性：

1 打开 “按访问扫描属性”对话框，然后选择左侧窗格中的 “常规设置”。

2 选择 “报告”选项卡。

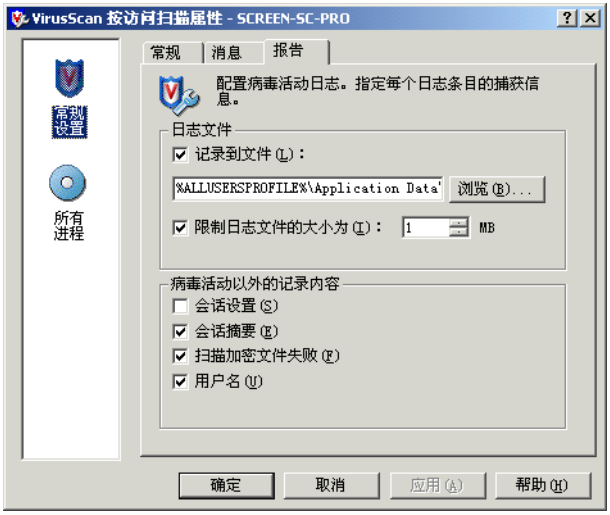

图 3-5. 常规设置 - “报告”选项卡

3 在“**日志文件**”下，选择下列选项之一：

- **记录到文件**。该选项为默认选项，表示在日志文件中记录按访问病毒扫描活动。
- 接受文本框中的默认日志文件名称和位置、输入其他日志文件名称和位置，或者单击“**浏览**”查找计算机或网络中的适当文件。

  注释
  默认情况下，扫描程序将日志信息写入到如下文件夹中的 ONACCESSSCANLOG.TXT 文件中：

  ```
  < 驱动器 >:Winnt\Profiles\All Users\Application
  Data\Network Associates\VirusScan
  ```

- **将日志文件的大小限制为**。该选项为默认选项，表示日志文件的默认大小为 1MB。接受默认的日志大小，或者设置不同的日志大小。如果选择了该选项，请输入一个介于 1MB 和 999MB 之间的值。

  注释
  如果日志文件中的数据超过了您设置的文件大小，则最早的 20% 的日志文件条目将被删除，而新数据将添加到该文件中。

4 在“**病毒活动以外的记录内容**”下，选择要在日志文件中记录的其他信息：

- **会话设置**。记录您为日志文件中的每个扫描会话选择的属性。

  注释
  扫描会话是指扫描程序位于计算机内存中的那段时间。当卸载该程序或者重新启动计算机时，扫描会话就会结束。

- **会话摘要**。该选项为默认选项，表示简要记录扫描程序在每次扫描会话过程中执行的操作，并将该信息添加到日志文件中。摘要信息包括已扫描的文件数量；检测到的病毒数量和类型；移动、清除或删除的文件数量以及其他信息。
- **扫描加密文件失败**。该选项为默认选项，表示在日志文件中记录扫描程序无法扫描的那些加密文件的名称。
- **用户名**。该选项为默认选项，表示将在扫描程序记录每个日志条目时已登录到计算机的用户的姓名记录在日志文件中。

5 单击“**应用**”保存更改。

进程设置

选择是对所有进程使用同样的设置，还是为默认进程、低风险进程和高风险进程指定不同的设置。

图 3-6. 按访问扫描属性 - 所有进程

- **对所有进程使用这些选项卡上的设置**。为所有进程指定同样的扫描属性。为所有进程设置属性的步骤和为默认进程设置属性的步骤相同。请参阅第 46 页的“默认进程”了解逐步操作。
- **对高风险和低风险进程使用不同的设置**。为默认进程、低风险进程和高风险进程指定不同的属性。详细信息，请参阅第 55 页的“低风险进程和高风险进程”。

> **注释**
> 选择了该选项之后，“**所有进程**”图标将变为“**默认进程**”，而且左侧窗格中的“**低风险进程**”和“**高风险进程**”图标均变为可用。

这部分包含下列主题：

- 默认进程
- 低风险进程和高风险进程

图 3-7. 按访问扫描属性

默认进程

未被定义为低风险或高风险进程的所有进程都是默认进程。

注释
当为所有进程设置属性时，您可以像设置默认进程属性那样操作。

您可以配置下列属性：

- 进程属性
- 检测属性
- 高级属性
- 操作属性

进程属性

使用 “进程” 选项卡上的选项，您可以为默认进程或所有进程指定属性：

1 打开 “按访问扫描属性” 对话框，然后选择左侧窗格中的 “所有进程”。

2 如果尚未选择 “进程” 选项卡，请选择它，然后选择下列选项之一：

- **对所有进程使用这些选项卡上的设置**。该选项为默认选项，表示如果选择了该选项并指定了属性，您选择的属性将作用于所有进程。您不能为默认进程、低风险进程和高风险进程设置不同的属性。
- **对高风险和低风险进程使用不同的设置**。为默认进程、低风险进程和高风险进程设置不同的属性。

注释

选择了该选项之后，“所有进程” 图标将变为 “默认进程”，而且左侧窗格中的 “低风险进程” 和 “高风险进程” 图标均变为可用。

图 3-8. 默认进程 - “进程” 选项卡

3 单击 “应用” 保存更改。

检测属性

使用“检测”选项卡，您可以指定按访问扫描程序要检查的文件类型以及扫描时间。

1 打开 “按访问扫描属性”对话框，然后选择左侧窗格中的 “所有进程”。

2 选择以下选项之一：

- **对所有进程使用这些选项卡上的设置**。该选项为默认选项，表示如果选择了该选项并指定了属性，您选择的属性将作用于所有进程。您不能为默认进程、低风险进程和高风险进程设置不同的属性。
- **对高风险和低风险进程使用不同的设置**。为默认进程、低风险进程和高风险进程设置不同的属性。

  注释
  选择了该选项之后，“所有进程”图标将变为 “默认进程”，而且左侧窗格中的“低风险进程”和“高风险进程”图标均变为可用。

3 选择 “检测”选项卡。

图 3-9. 默认进程 - “检测”选项卡

4 在“**扫描文件**”下，选择下列扫描选项的任意组合：

- **写入磁盘时**。该选项为默认选项，表示扫描写入到服务器、工作站或其他数据存储设备、或者在这些设备上被修改的所有文件。
- **读取磁盘时**。该选项为默认选项，表示扫描从服务器、工作站或其他数据存储设备中读取的所有文件。
- **在网络驱动器上**。在按访问扫描过程中，扫描对象将包括网络资源。这将有助于扩大病毒防护范围。

  注释

  当然，扫描网络资源也会对执行扫描的那些系统的总体性能产生负面影响。

  警告

  如果将文件从一台计算机复制或移到另一台计算机，并将这两台计算机的按访问扫描属性都配置为对写入到磁盘和从磁盘中读取的文件进行扫描，那么当从源计算机读取某个文件时会进行扫描，而在该文件写入到目标计算机时，会再次进行扫描。

  如果网络中的主要通讯模式是将文件从一台计算机复制或移到另一台计算机，您可以将扫描属性配置为只扫描写入到磁盘的文件，但不扫描从磁盘中读取的文件。这能够有效防止同一个文件被重复扫描。通过将所有计算机配置为只扫描从磁盘中读取的文件而不扫描写入到磁盘中的文件，也可以获得同样的效果。

  如果使用了以上两种配置之一，一定要为所有计算机设置同样的配置。切勿将某些计算机配置为只扫描写入到磁盘的文件，而将其他计算机配置为只扫描从磁盘中读取的文件。这样会将感染病毒的文件从只扫描写入到磁盘的文件的那些计算机复制到只扫描从磁盘中读取的文件的那些计算机中。

5 在“扫描内容”下，选择下列选项之一：

- **所有文件**。该选项为默认选项，表示扫描所有文件，而不论其扩展名如何。
- **默认类型 + 其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他扩展名。当前的 DAT 文件定义了默认的文件类型扩展名列表。您可以添加或删除用户指定的文件类型扩展名，但不能删除默认列表中的任何文件类型扩展名。然而，您可以排除默认列表中的扩展名。详细信息，请参阅第 64 页的“排除文件、文件夹和驱动器”。
  - **其他**。如果选择了“**默认类型 + 其他文件类型**”，您可以单击“**其他**”添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 62 页的“添加文件类型扩展名”。

    按访问扫描程序最多可以列出 1000 个其他扩展名。
  - **同时扫描所有文件中的宏病毒**。扫描所有文件是否含有宏病毒，而不论其扩展名如何。该选项只在选择了“**默认类型 + 其他文件类型**”选项后才可用。

    注释
    扫描所有文件中的宏病毒可能会影响性能。
- **指定的文件类型**。只扫描您指定的扩展名。
  - **指定项**。如果选择了“**指定文件类型**”，您可以单击“**指定项**”添加或删除用户指定的文件类型扩展名。您也可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 63 页的“添加用户指定的文件类型扩展名”。

    按访问扫描程序最多可以列出 1000 个指定的扩展名。

6 在“**不扫描内容**”下，您可以单击“**排除**”来指定不接受扫描的文件、文件夹和驱动器。详细说明，请参阅第 64 页的“排除文件、文件夹和驱动器”。

7 单击“**应用**”保存更改。

高级属性

使用“高级”选项卡上的选项，您可以为启发式扫描、非病毒程序文件以及压缩文件指定高级扫描选项。

1 打开“按访问扫描属性”对话框，然后选择左侧窗格中的“所有进程”。

2 选择以下选项之一：

- **对所有进程使用这些选项卡上的设置**。该选项为默认选项，表示如果选择了该选项并指定了属性，您选择的属性将作用于所有进程。您不能为默认进程、低风险进程和高风险进程设置不同的属性。
- **对高风险和低风险进程使用不同的设置**。为默认进程、低风险进程和高风险进程设置不同的属性。

  注释

  选择了该选项之后，“所有进程”图标将变为“默认进程”，而且左侧窗格中的“低风险进程”和“高风险进程”图标均变为可用。

3 选择“高级”选项卡。

图 3-10. 默认进程 - “高级”选项卡

4 在“**启发式**”下，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的可能性。启用了这项功能之后，扫描程序会分析这段代码是已知病毒变体的可能性。请选择以下选项的任意组合：

- **查找未知程序病毒**。对于默认进程和高风险进程，该选项是默认选项，表示将含有类似病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将应用您在“**操作**”选项卡中选择的操作。
- **查找未知宏病毒**。对于默认进程和高风险进程，该选项是默认选项，表示将含有类似病毒的代码的嵌入式宏视为病毒。扫描程序将应用您在“**操作**”选项卡中选择的操作。

  注释
  该选项不同于“**检测**”选项卡中的“**同时扫描所有文件中的宏病毒**”，后者会命令扫描程序查找所有已知的宏病毒。该选项会命令扫描程序评估未知宏是病毒的可能性。

5 在“**非病毒**”下，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的异常程序**。检测可能有害的程序。
  - **查找玩笑程序**。如果选择了“**查找潜在的异常程序**”，扫描程序还会扫描玩笑程序。

    警告
    VirusScan Enterprise 不会对检测到的可能有害的程序文件或玩笑程序采取任何措施。检测结果将记录在日志文件中。

    如果希望对检测到的玩笑程序或可能有害的程序采取措施，您必须手动操作。例如，要删除检测到的玩笑程序，您必须手动将其删除。

6 在“**压缩文件**”下，指定扫描程序要检查的压缩文件类型：

- **扫描压缩文件（如 UPX）中的可执行文件**。对于默认进程和高风险进程，该选项是默认选项，表示检查含有可执行文件的压缩文件。压缩的可执行文件在运行时只将自己解压缩到内存中。压缩的可执行文件永远不会解压缩到磁盘中。
- **扫描存档文件（如 ZIP）内部的文件**。检查存档文件及其内容。存档文件是一种压缩文件，要访问它包含的文件，必须首先将其解压缩。存档文件中包含的文件在被写入到磁盘时会接受扫描。
- **解码 MIME 编码的文件**。检测、解码并扫描多用途 Internet 邮件扩展 (MIME) 编码的文件。

  注释
  尽管该选项能够更好地保护用户，但扫描压缩文件还是增加了扫描所需的时间。

7 单击“**应用**”保存更改。

操作属性

使用“操作”选项卡中的选项，您可以指定扫描程序在检测到病毒时采取的主要操作和辅助操作。

1 打开“按访问扫描属性”对话框，然后选择左侧窗格中的“所有进程”。

2 选择以下选项之一：

- **对所有进程使用这些选项卡上的设置**。该选项为默认选项，表示如果选择了该选项并指定了属性，您选择的属性将作用于所有进程。您不能为默认进程、低风险进程和高风险进程设置不同的属性。
- **对高风险和低风险进程使用不同的设置**。为默认进程、低风险进程和高风险进程设置不同的属性。

注释

选择了该选项之后，“所有进程”图标将变为“默认进程”，而且左侧窗格中的“低风险进程”和“高风险进程”图标均变为可用。

3 选择“操作”选项卡。

图 3-11. 默认进程 - “操作”选项卡

4 在“发现病毒时”下，选择扫描程序在检测到病毒时采取的主要操作。

注释

默认的主要操作是“自动清除文件感染的病毒”。

单击 以选择以下操作之一：

- **拒绝访问感染病毒的文件**。拒绝所有用户访问扫描程序发现的任何感染病毒的文件。请确保启用了“**常规设置**”中“**报告**”选项卡的“**记录到文件**”属性，以记录感染病毒的文件。

  注释
  如果该文件是从外部来源（例如光盘或 Internet）写入到本地系统中，扫描程序会在其文件名后面添加一个 .VIR 扩展名。扫描程序会认为对文件进行的这种操作是一种写入操作。

  如果复制了这个文件，例如从硬盘中的一个位置复制到另一个位置，则其文件名后面不会添加 .VIR 扩展名。扫描程序会认为这是一种移动操作。

- **将感染病毒的文件移动到文件夹**。默认情况下，扫描程序将感染病毒的文件移到一个名为 quarantine 的文件夹中。您可以在“**常规设置**”中“**常规**”选项卡的“**隔离文件夹**”文本框中更改该文件夹的名称。

- **自动删除感染病毒的文件**。当检测到病毒时，扫描程序会立即删除感染病毒的文件。请确保启用了“**常规设置**”中“**报告**”选项卡的“**记录到文件**”属性，以记录感染病毒的文件。

  如果选择了这个选项，系统将要求您确认。单击“**是**”确认，或者单击“**否**”取消这个选项。

  警告
  如果选择了“**高级**”选项卡中的“**查找未知宏病毒**”，则您在这里选择的操作将应用于包含类似病毒的代码的所有宏。如果选择了“**自动删除感染病毒的文件**”，则包含类似于宏病毒的代码的所有文件以及包含感染病毒文件的所有存档文件都将被删除。如果不希望删除这些文件，请确保您选择的操作与您针对宏选择的操作一致。

- **自动清除文件感染的病毒**。该选项为默认选项，表示扫描程序会尝试删除文件感染的病毒。如果扫描程序无法删除病毒，或者受病毒侵害的文件已到了不可修复的地步，扫描程序将执行辅助操作。详细信息，请参阅步骤 5。

5 在“**如果以上操作失败**”下，选择扫描程序在首选操作失败后采取的辅助操作。可以选择的操作取决于您选择的主要操作。

  注释
  默认的辅助操作是“**将感染病毒的文件移到文件夹**”。

  单击 以选择辅助操作：

  - **拒绝访问感染病毒的文件**。
  - **将感染病毒的文件移动到文件夹**。该选项为默认选项。
  - **自动删除感染病毒的文件**。

如果选择了这个选项，系统将要求您确认。单击“是”确认，或者单击“否”取消这个选项。

6 单击“应用”保存更改。

低风险进程和高风险进程

基于进程的扫描允许您根据每种进程的预计感染风险来定义扫描策略。

请先确定应将哪些进程指定为低风险进程或高风险进程，然后为每种进程设置属性。

这部分包含下列主题：

- 为进程指定风险
- 进程属性
- 检测属性
- 高级属性
- 操作属性

为进程指定风险

进程是执行中的程序。一个程序可以启动一个或多个进程。在决定为某个特定父进程指定何种风险或扫描策略时，应记住只有这一进程的子进程与扫描策略保持一致。例如，如果将 Microsoft Word 可执行文件 WINWORD.EXE 定义为一个高风险扫描进程，则被访问的任何 Microsoft Word 文档都会按高风险扫描策略扫描。然而，当启动了父进程 Microsoft Word 之后， WINWORD.EXE 文件将按启动它的那个进程的策略扫描。

您可以为进程指定两种风险：

- 低风险进程是指不太可能感染病毒的那些进程，也可以是访问多个文件、但不太可能传播病毒的那些进程。例如：
  - 备份软件。
  - 编译进程。
- 高风险进程是指很有可能感染病毒的那些进程，例如：
  - 可以启动其他进程的进程。例如Microsoft Windows资源管理器或者命令提示符。
  - 可执行的进程。例如 WINWORD 或 CSCRIPT。
  - 可执行 Internet 下载的进程。例如浏览器、即时通讯程序和邮件客户端软件。

注释
在用默认设置安装 VirusScan Enterprise 时，“**对所有进程使用这些选项卡上的设置**”选项将被选定。如果选择了“**对高风险和低风险进程使用不同的设置**”，一些进程将被预先定义为高风险进程。您可以根据需要更改这个列表。

未被定义为低风险进程或高风险进程的那些进程将被视为默认进程，并会按您为默认进程设置的属性扫描。

要确定为哪些进程指定哪些风险，请按如下步骤操作：

1 确定您为何采用不同的扫描策略。在性能和风险之间寻求平衡的两个最常见原因是：

- 在扫描某些进程（例如网站下载）时，需要比默认扫描策略更全面的扫描。
- 为了根据风险和在扫描过程中对性能产生的影响而在更小的范围内扫描某些进程。例如，捕捉流式媒体（例如视频）虽然风险较低，但非常占用资源。

2 确定哪些进程是低风险进程，哪些进程是高风险进程。首先应确定哪个程序负责哪个进程，然后确定应将哪种风险与这个进程相关联。Windows 任务管理器或 Windows 性能监视器可以帮助您了解哪些进程占用了最多的 CPU 时间和内存。了解了这些信息之后，您可以根据每个进程的性能和风险将它们与扫描策略相关联。

3 为默认进程、低风险进程和高风险进程分别配置扫描策略。

注释
我们不建议降低高风险进程的扫描级别。高风险扫描策略最初被设置为与默认进程扫描策略相同，以确保高风险进程保持较高的扫描级别。

进程属性

使用“**进程**”选项卡上的选项，您可以将进程定义为低风险或高风险进程：

注释
未被定义为低风险进程或高风险进程的那些进程将被视为默认进程，并会按您为默认进程设置的属性扫描。

1 打开“**按访问扫描属性**”对话框，然后选择左侧窗格中的“**所有进程**”。

2 选择“**对高风险和低风险进程使用不同的设置**”。

注释
选择了该选项之后，“**所有进程**”图标将变为“**默认进程**”，而且左侧窗格中的“**低风险进程**”和“**高风险进程**”图标均变为可用。

3 选择“**低风险进程**”或“**高风险进程**”。

4 选择“**进程**”选项卡。

图 3-12. 低风险或高风险进程 - “进程”选项卡

该列表按文件名的字母顺序显示了当前进程的列表。每个进程都显示了各自的应用程序图标、文件名和相关描述 （如果有）。默认设置包括：

- “低风险进程”列表默认为空。
- “高风险进程”列表中包含McAfee Security认为感染病毒风险较高的进程。您可以根据自己的安全需要在这个列表中添加或删除进程。

  注释

  您添加或选择低风险进程和高风险进程的步骤相同。

5 要添加应用程序，请单击 “添加”。屏幕上将出现 “选择应用程序”对话框。

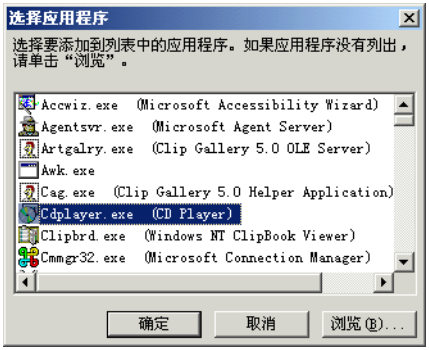

图 3-13. 选择应用程序

a 您可以通过以下方法选择要添加的应用程序：

- 从列表中选择应用程序。

  使用 CTRL + SHIFT 键可以选择多个应用程序。

- 单击 “浏览”查找网络中的应用程序。

b 选择完应用程序之后，单击 “确定”保存并返回到 “进程”选项卡。

6 要删除应用程序，请首先突出显示列表中的一个或多个应用程序，然后单击“删除”。

7 单击 “应用”保存更改。

8 重复步骤 3 到步骤 7 以便将应用程序定义为低风险或高风险进程。

检测属性

使用“检测”选项卡，您可以指定按访问扫描程序要检查的文件类型以及扫描时间。

1 打开 “按访问扫描属性”对话框，然后选择左侧窗格中的 “所有进程”。

2 选择 “对高风险和低风险进程使用不同的设置”。

注释
选择了该选项之后，“所有进程”图标将变为 “默认进程”，而且左侧窗格中的“低风险进程”和 “高风险进程”图标均变为可用。

3 选择 “低风险进程”或 “高风险进程”。

4 选择 “检测”选项卡。

图 3-14. 低风险或高风险进程 - “检测”选项卡

注释
选择了左侧窗格中的进程图标之后，为低风险进程和高风险进程设置 “检测”选项的步骤相同。

5 在“**扫描文件**”下，选择下列扫描选项的任意组合：

- **写入磁盘时**。该选项为默认选项，表示扫描写入到服务器、工作站或其他数据存储设备、或者在这些设备上被修改的所有文件。
- **读取磁盘时**。该选项为默认选项，表示扫描从服务器、工作站或其他数据存储设备中读取的所有文件。
- **在网络驱动器上**。在按访问扫描过程中，扫描对象将包括网络资源。这将有助于扩大病毒防护范围。

  注释
  当然，扫描网络资源也会对执行扫描的那些系统的总体性能产生负面影响。

  警告
  如果将文件从一台计算机复制或移到另一台计算机，并将这两台计算机的按访问扫描属性都配置为对写入到磁盘和从磁盘中读取的文件进行扫描，那么当从源计算机读取某个文件时会进行扫描，而在该文件写入到目标计算机时，会再次进行扫描。

  如果网络中的主要通讯模式是将文件从一台计算机复制或移到另一台计算机，您可以将扫描属性配置为只扫描写入到磁盘的文件，但不扫描从磁盘中读取的文件。这能够有效防止同一个文件被重复扫描。通过将所有计算机配置为只扫描从磁盘中读取的文件而不扫描写入到磁盘中的文件，也可以获得同样的效果。

  如果使用了以上两种配置之一，一定要为所有计算机设置同样的配置。切勿将某些计算机配置为只扫描写入到磁盘的文件，而将其他计算机配置为只扫描从磁盘中读取的文件。这样会将感染病毒的文件从只扫描写入到磁盘的文件的那些计算机复制到只扫描从磁盘中读取的文件的那些计算机中。

6 在“**扫描内容**”下，选择下列选项之一：

- **所有文件**。该选项为默认选项，表示扫描所有文件，而不论其扩展名如何。

- **默认类型+其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他扩展名。当前的 DAT 文件定义了默认的文件类型扩展名列表。您可以添加或删除用户指定的文件类型扩展名，但不能删除默认列表中的任何文件类型扩展名。然而，您可以排除默认列表中的扩展名。详细信息，请参阅第 64 页的 “排除文件、文件夹和驱动器”。

  - **其他**。如果选择了“**默认类型 + 其他文件类型**”，您可以单击“**其他**”添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 62 页的 “添加文件类型扩展名”。

    按访问扫描程序最多可以列出 1000 个其他扩展名。

  - **同时扫描所有文件中的宏病毒**。扫描所有文件是否含有宏病毒，而不论其扩展名如何。该选项只在选择了“**默认类型 + 其他文件类型**”选项后才可用。

    注释
    扫描所有文件中的宏病毒可能会影响性能。

- **指定的文件类型**。只扫描您指定的扩展名。

  - **指定项**。如果选择了“**指定的文件类型**”，您可以单击“**指定项**”添加或删除用户指定的文件类型扩展名。您也可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 63 页的 “添加用户指定的文件类型扩展名”。

    按访问扫描程序最多可以列出 1000 个指定的扩展名。

7. 在“**不扫描内容**”下，您可以单击“**排除**”来指定不接受扫描的文件、文件夹和驱动器。详细说明，请参阅第 64 页的 “排除文件、文件夹和驱动器”。
8. 单击“**应用**”保存更改。
9. 重复步骤 3 到步骤 8以便为低风险或高风险进程指定检测设置。

添加文件类型扩展名

将用户指定的文件类型添加到默认文件类型列表中。也可以使用该功能删除您指定的任何文件类型。默认列表以及用户指定的所有文件类型都将包括在扫描范围内。

注释

您不能更改或删除默认文件类型列表中的文件类型。默认列表由您下载的最新 DAT 文件定义。为防止某种扩展名接受扫描，您需要将其排除。详细信息，请参阅第 64 页的 “排除文件、文件夹和驱动器”。

1 单击 “**其他**” 打开 “**其他文件类型**” 对话框。

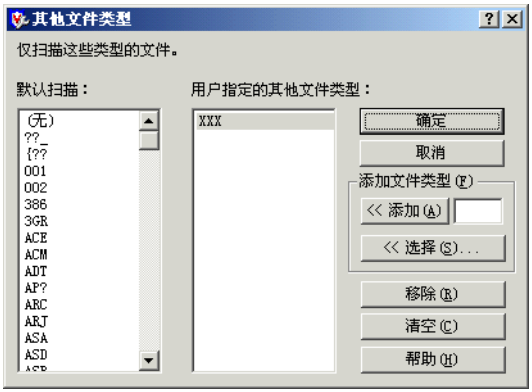

图 3-15. 其他文件类型

2 在 “**添加文件类型**” 下，您可以通过两种方式添加用户指定的文件类型扩展名：

- 在文本框中键入一个文件类型扩展名，然后单击 “**添加**”。

  注释

  只需输入文件类型扩展名的前三个字母即可。如果输入了 HTM 文件扩展名，扫描程序将扫描 HTM 和 HTML 文件。您可以使用通配符或者字符与通配符的组合。

- 单击 “**选择**” 打开 “**选择文件类型**” 对话框。从该列表中选择一个或多个文件类型扩展名，然后单击 “**确定**”。

  使用 CTRL + SHIFT 键可以选择多个文件类型扩展名。

添加的文件类型扩展名将显示在 “**用户指定的其他文件类型**” 列表中。

3 通过以下两种方法可以从用户指定的列表中删除用户指定的文件类型扩展名：

- 选择 “**用户指定的其他文件类型**” 列表中的一个或多个文件类型扩展名，然后单击 “**删除**”。
- 单击 “**清空**” 删除 “**用户指定的其他文件类型**” 列表中的所有项目。

添加用户指定的文件类型扩展名

创建要接受扫描的用户指定的文件类型扩展名列表。也可以使用该功能删除您以前指定的任何文件类型扩展名。

1 单击“**指定项**”打开“**指定的文件类型**”对话框。

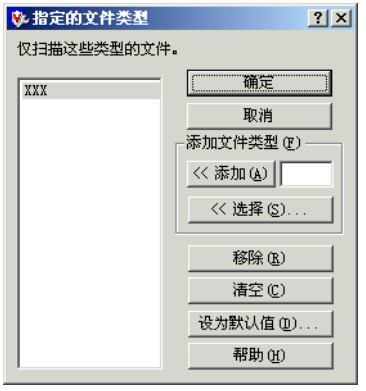

图 3-16. 指定的文件类型

2 在“**添加文件类型**”下，您可以通过两种方式添加用户指定的文件类型扩展名：

- 在文本框中键入一个文件类型扩展名，然后单击“**添加**”。

  注释
  只需输入文件类型扩展名的前三个字母即可。如果输入了 HTM 文件扩展名，扫描程序将扫描 HTM 和 HTML 文件。您可以使用通配符或者字符与通配符的组合。

- 单击“**选择**”打开“**选择文件类型**”对话框。从该列表中选择一个或多个文件类型扩展名，然后单击“**确定**”。

您添加的文件类型扩展名将显示在“**仅扫描这些类型的文件**”下面的列表中。

3 通过以下两种方法可以从该列表中删除您指定的文件类型扩展名：

- 在“**仅扫描这些类型的文件**”下面的列表中选择一个或多个文件类型扩展名，然后单击“**删除**”。
- 单击“**清空**”删除“**仅扫描这些类型的文件**”下面的列表中的所有项目。

4 单击“**设为默认值**”，以便使用默认列表替换当前用户指定的文件类型扩展名列表。当前的 DAT 文件定义了默认的文件类型扩展名列表。

5 单击“**确定**”保存更改并返回到“**检测**”选项卡。

排除文件、文件夹和驱动器

指定要从扫描操作中排除的文件、文件夹和驱动器。也可以使用该功能删除您以前指定的任何排除项。

1 单击“**排除**”打开“**设置排除**”对话框。

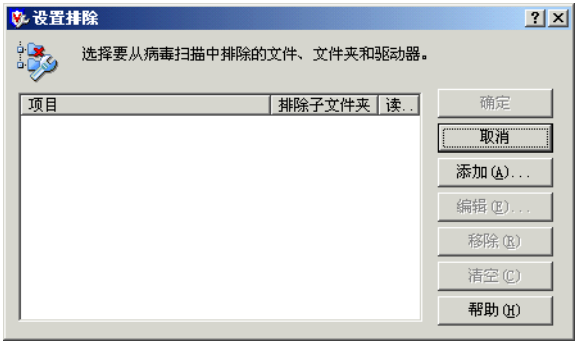

图 3-17. 设置排除

2 添加或编辑文件、文件夹或驱动器。“Windows 文件保护”功能会默认列出。

- 要添加项目，请单击“**添加**”打开“**添加排除项目**”对话框。
- 要编辑项目，请双击或选择它，然后单击“**编辑**”打开“**编辑排除项目**”对话框。

注释

无论您是添加还是编辑排除项目，排除选项都相同。

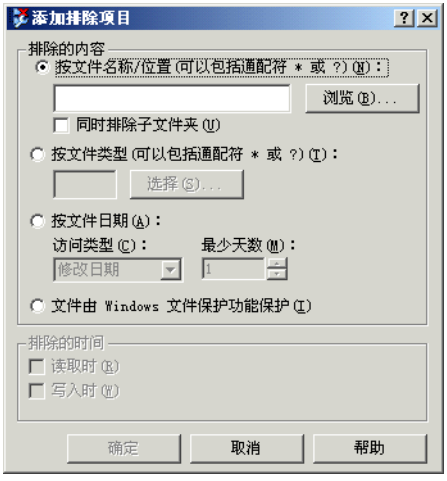

图 3-18. 添加排除项目

3 在“**排除的内容**”下，选择下列选项之一：

- **按文件名称 / 位置**。该选项为默认选项，表示文件的指定名称或位置。您可以在这里使用通配符 * 和 ?。在文本框中键入特定信息，或者单击“**浏览**”查找名称或位置。

  注释
  您可以指定完整的路径名（例如 C:\WINNIT\SYSTEM*）、文件名（例如 PAGEFILE.SYS、PAGEFILE.*、P*.* 或 *.SYS）或者文件夹名（例如 BACKUP）。例如，指定 BACKUP 文件夹将不包括名为 BACKUP 的所有文件夹，而且与它们的位置无关。

  使用通配符时存在如下限制：

  - 有效的通配符是 ? 和 *，分别代表个别字符和多个字符。
  - 通配符后面不能跟随反斜杠 \。例如， C:\ABC\WWW? 有效，而 C:\ABC\WWW?\123 无效。
  - 以路径或反斜杠 \ 开头的排除项（例如 WWW*）只会被作为文件处理。
  - 含有 ? 字符的排除项只有在文件或文件夹名称长度与排除项字符数匹配时才有效。例如，排除项 W?? 将排除 WWW，但不会排除 WW 或 WWWW。

  - **同时排除子文件夹**。如果选择了“**按文件名称 / 位置**”，您可以排除与指定格式相匹配的文件夹中的子文件夹。

- **按文件类型**。按类型指定文件扩展名。在文本框中键入文件扩展名，或者单击“**选择**”打开“**选择文件类型**”对话框，并从列表中选择一个或多个扩展名。单击“**确定**”保存并关闭该对话框。

  注释
  您指定的文件扩展名可以包括通配符。有效的通配符是 ? 和 *，分别代表个别字符和多个字符。

- **按文件日期**。指定您是否按日期排除文件。

  - **访问类型**。如果选择了“**按文件日期**”，您可以单击 指定访问类型为“**修改日期**”或“**创建日期**”。
  - **最少天数**。如果选择了“**按文件日期**”，您可以指定文件已经存在的最少天数。该文件必须至少已经存在上述天数，才能被排除。

- **文件由 Windows 文件保护功能保护**。指出这个排除项将取决于某个文件的“Windows 文件保护”功能状态。

4 在 “**排除的时间**” 下，指定何时不扫描这些项目：

- **读取时**。该选项为默认选项，表示指出当从磁盘中读取时，这些排除项将不接受扫描。
- **写入时**。该选项为默认选项，表示指出当写入到磁盘时，这些排除项将不接受扫描。

注释
“**读取时**” 和 “**写入时**” 选项对按需扫描任务无效。

5 单击 “**确定**” 保存更改并返回到 “**设置排除**” 对话框。

6 通过以下两种方法可以从项目列表中删除用户指定的文件类型扩展名：

- 从列表中选择一个或多个文件类型扩展名，然后单击 “**删除**”。
- 单击 “**清空**” 删除列表中的所有项目。

7 单击 “**确定**” 保存更改并返回到 “**检测**” 选项卡。

8 单击 “**应用**” 保存更改。

高级属性

使用 “**高级**” 选项卡上的选项，您可以为启发式扫描、非病毒程序文件以及压缩文件指定高级扫描选项。

1 打开 “**按访问扫描属性**” 对话框，然后选择左侧窗格中的 “**所有进程**”。

2 选择 “**对高风险和低风险进程使用不同的设置**”。

注释
选择了该选项之后，“**所有进程**” 图标将变为 “**默认进程**”，而且左侧窗格中的 “**低风险进程**” 和 “**高风险进程**” 图标均变为可用。

3 选择 “**低风险进程**” 或 “**高风险进程**”。

4 选择 “**高级**” 选项卡。

图 3-19. 低风险或高风险进程 - “高级”选项卡

注释

选择了左侧窗格中的进程图标之后，为低风险进程和高风险进程设置“**高级**”选项的步骤相同。

5 在“**启发式**”下，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的可能性。启用了这项功能之后，扫描程序会分析这段代码是已知病毒变体的可能性。请选择以下选项的任意组合：

- **查找未知程序病毒**。对于默认进程和高风险进程，该选项是默认选项。将含有类似于病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将应用您在“**操作**”选项卡中选择的操作。
- **查找未知宏病毒**。对于默认进程和高风险进程，该选项是默认选项。将含有类似病毒的代码的嵌入式宏视为病毒。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

  注释

  该选项不同于“**检测**”选项卡中的“**同时扫描所有文件中的宏病毒**”，后者会命令扫描程序查找所有已知的宏病毒。该选项会命令扫描程序评估未知宏是病毒的可能性。

6 在“**非病毒**”下，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的有害程序**。检测可能有害的程序。
  - **查找玩笑程序**。如果选择了“**查找潜在的有害程序**”，扫描程序还会扫描玩笑程序。

警告

VirusScan Enterprise 不会对检测到的可能有害的程序文件或玩笑程序采取任何措施。检测结果将记录在日志文件中。

如果希望对检测到的玩笑程序或可能有害的程序采取措施，您必须手动操作。例如，要删除检测到的玩笑程序，您必须手动将其删除。

7 在“**压缩文件**”下，指定扫描程序要检查的压缩文件类型。您可以选择下列选项：

- **扫描压缩文件（如 UPX）中的可执行文件**。对于默认进程和高风险进程，该选项是默认选项。检查含有可执行文件的压缩文件。压缩的可执行文件在运行时只将自己解压缩到内存中。压缩的可执行文件永远不会解压缩到磁盘中。
- **扫描存档文件（如 ZIP）内部的文件**。检查存档文件及其内容。存档文件是一种压缩文件，要访问它包含的文件，必须首先将其解压缩。存档文件中包含的文件在被写入到磁盘时会接受扫描。
- **解码 MIME 编码的文件**。检测、解码并扫描多用途 Internet 邮件扩展 (MIME) 编码的文件。

  注释

  尽管该选项能够更好地保护用户，但扫描压缩文件还是增加了扫描所需的时间。

8 单击“**应用**”保存更改。

9 重复步骤 3 到步骤 8 以便为低风险或高风险进程配置高级设置。

操作属性

使用“**操作**”选项卡中的选项，您可以指定扫描程序在检测到病毒时采取的主要操作和辅助操作。

1 打开“**按访问扫描属性**”对话框，然后选择左侧窗格中的“**所有进程**”。

2 选择“**对高风险和低风险进程使用不同的设置**”。

  注释

  选择了该选项之后，“**所有进程**”图标将变为“**默认进程**”，而且左侧窗格中的“**低风险进程**”和“**高风险进程**”图标均变为可用。

3 选择“**低风险进程**”或“**高风险进程**”。

4 选择“**操作**”选项卡。

图 3-20. 低风险或高风险进程 - “操作”选项卡

注释

选择了左侧窗格中的进程图标之后，为低风险进程和高风险进程设置“**操作**”选项的步骤相同。

5 在“**发现病毒时**”下，选择扫描程序在检测到病毒时采取的主要操作。

注释

默认的主要操作是“**自动清除文件感染的病毒**”。

单击 以选择以下操作之一：

- **拒绝访问感染病毒的文件**。拒绝所有用户访问扫描程序发现的任何感染病毒的文件。请确保启用了“**常规设置**”中“**报告**”选项卡的“**记录到文件**”属性，以记录感染病毒的文件。

  注释

  如果该文件是从外部来源（例如光盘或 Internet）写入到本地系统中，扫描程序会在其文件名后面添加一个 .VIR 扩展名。扫描程序会认为对文件进行的这种操作是一种写入操作。

  如果复制了这个文件，例如从硬盘中的一个位置复制到另一个位置，则其文件名后面不会添加 .VIR 扩展名。扫描程序会认为这是一种移动操作。

- **将感染病毒的文件移到文件夹**。默认情况下，扫描程序将感染病毒的文件移到一个名为 quarantine 的文件夹中。您可以在“**常规设置**”中“**常规**”选项卡的“**隔离文件夹**”文本框中更改该文件夹的名称。

- **自动删除感染病毒的文件**。当检测到病毒时，扫描程序会立即删除感染病毒的文件。请确保启用了“**常规设置**”中“**报告**”选项卡的“**记录到文件**”属性，以记录感染病毒的文件。

  如果选择了这个选项，系统将要求您确认。单击“**是**”确认，或者单击“**否**”取消这个选项。

  警告
  如果选择了“**高级**”选项卡中的“**查找未知宏病毒**”，则您在这里选择的操作将应用于包含类似病毒的代码的所有宏。如果选择了“**自动删除感染病毒的文件**”，则包含类似于宏病毒的代码的所有文件以及包含感染病毒文件的所有存档文件都将被删除。如果不希望删除这些文件，请确保您选择的操作与您针对宏选择的操作一致。

- **自动清除文件感染的病毒**。该选项为默认选项，表示扫描程序会尝试删除文件感染的病毒。如果扫描程序无法删除病毒，或者受病毒侵害的文件已到了不可修复的地步，扫描程序将执行辅助操作。详细信息，请参阅步骤 6。

6 在“**如果以上操作失败**”下，选择扫描程序在首选操作失败后采取的辅助操作。可以选择的操作取决于您选择的主要操作。

  注释
  默认的辅助操作是“**将感染病毒的文件移到文件夹**”。

  单击 以选择辅助操作：

  - **拒绝访问感染病毒的文件**。
  - **将感染病毒的文件移到文件夹**。该选项为默认选项。
  - **自动删除感染病毒的文件**。

    如果选择了这个选项，系统将要求您确认。单击“**是**”确认，或者单击“**否**”取消这个选项。

7 单击“**应用**”保存更改。

8 重复步骤 3 到步骤 7 以便为低风险或高风险进程配置操作设置。

查看扫描结果

您可以在统计信息摘要和活动日志中查看按访问扫描操作的结果。

这部分包含下列主题：

- 查看扫描统计信息
- 查看活动日志

查看扫描统计信息

“**按访问扫描统计信息**”摘要显示了扫描程序已检查的文件数量、发现的病毒数量以及采取的响应措施。

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一打开 “**按访问扫描统计信息**”对话框：

- 双击系统任务栏中的 。
- 右键单击任务列表中的按访问扫描任务，并选择 “**统计信息**”。

图 3-21. 按访问扫描统计信息

“**按访问扫描统计信息**”对话框在上部窗格中显示了 “**最后扫描的文件**”，在下部窗格中显示了统计信息摘要。

3 如果具有管理员权限并根据需要输入了密码，您可以使用以下任一项功能：

> **注释**
> 如果将用户界面配置为显示最少的菜单选项，则 “**禁用**”和 “**属性**”按钮将隐藏。您可以在 “**工具**” | “**用户界面选项**” | “**显示选项**”选项卡中设置这个选项。

- 单击 “**禁用**”以取消激活按访问扫描程序。这项功能将在 “**禁用**”和 “**启用**”之间切换。
- 单击 “**属性**”打开 “**按访问扫描属性**”对话框，然后根据需要更改扫描属性，并单击 “**应用**”保存更改。

扫描将会立即采用新的设置运行。

4 查看了扫描统计信息之后，单击 “**关闭**”。

查看活动日志

按访问扫描活动日志显示了关于扫描操作的详细信息。例如，它可以显示扫描程序已检查的文件数量、发现的病毒数量以及采取的响应措施。

1 打开“VirusScan 控制台”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一，打开活动日志文件：

- 突出显示一项任务，然后选择 “**任务**”菜单中的 “**活动日志**”。
- 右键单击任务列表中的这项任务，并选择 “**查看日志**”。

3 要关闭活动日志，请选择 “**文件**”菜单中的 “**退出**”。

响应病毒检测

按访问扫描程序会根据您在“**按访问扫描属性**”对话框中选择的配置设置来查找病毒。详细信息，请参阅第 36 页的“配置按访问扫描程序”。当检测到病毒后，系统会执行以下操作：

- 如果已将警报管理器和 / 或按访问扫描程序配置为在检测到病毒时发出通知，您将会收到通知。
- 按访问扫描程序将在 “**按访问扫描消息**”对话框中记录一条消息。

这部分包含下列主题：

- 接收病毒检测通知
- 查看按访问扫描消息
- 在检测到病毒时采取措施

接收病毒检测通知

按访问扫描程序可以在检测到病毒时发送三种类型的通知：

- **“按访问扫描消息”对话框 -“按访问扫描消息”**对话框将显示发现病毒的时间，但前提是您已将按访问扫描程序配置为这样做。关于配置消息选项的详细信息，请参阅第 41 页的 “消息属性”。

  关于 **“按访问扫描消息”**对话框的详细信息，请参阅第 74 页的 “查看按访问扫描消息”。

- **网络用户 Messenger 服务 -** 当检测到病毒时向网络用户发送消息，但前提是您已将按访问扫描程序配置为这样做。关于配置消息选项的详细信息，请参阅第 41 页的 “消息属性”。

  这条消息提供了与感染病毒的文件有关的详细信息，例如文件名、文件位置、检测到的病毒类型以及检测病毒时使用的扫描引擎和 DAT 文件版本。查看这条消息的详细信息，然后单击 **“确定”**离开。

- **Messenger 服务** - 显示网络消息，但前提是您已将警报管理器配置为这样做。详细信息，请参阅第 138 页的 “配置警报管理器”。

  以下是警报管理器发出的网络消息的示例。

图 3-22. 按访问扫描 - Messenger 服务

这条消息提供了与感染病毒的文件有关的详细信息，例如文件名、文件位置、检测到的病毒类型以及检测病毒时使用的扫描引擎和 DAT 文件版本。

根据警报管理器和按访问扫描程序的具体配置，您收到的通知可能不止一个。

查看这条消息的详细信息，然后单击 **“确定”**离开。

注释

如果没有将三个消息选项中的任一个配置为在检测到病毒时发送消息，您将不会收到任何通知。但您总是能够检查 **“按访问扫描消息”**对话框来查看检测到的病毒。详细信息，请参阅第 74 页的 “查看按访问扫描消息”。

查看按访问扫描消息

当检测到病毒时，按访问扫描程序会在“**按访问扫描消息**”对话框中记录一条消息。该对话框按时间顺序为当前用户列出了所有消息。如果用户是管理员，可以选择性地列出所有本地系统消息。

该对话框在检测到病毒时会自动显示，但前提是您已将按访问扫描程序配置为这样做。

您也可以右键单击系统任务栏中的 并选择“**按访问扫描消息**”来随时打开该对话框。

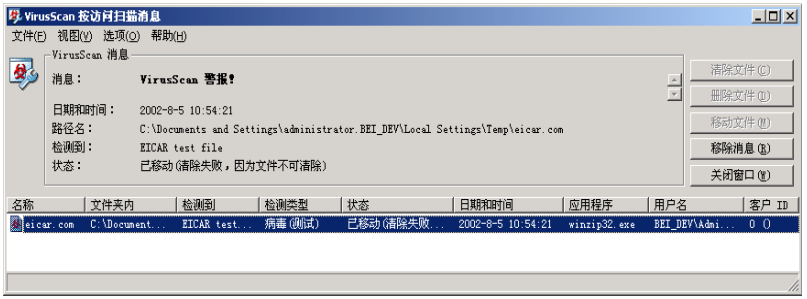

图 3-23. 按访问扫描消息

“**按访问扫描消息**”对话框分为几个部分：

- **菜单** - 提供了用来对文件或消息进行操作的菜单。
  - “**文件**”菜单提供了可以对列表中的文件或消息执行的操作。
  - “**视图**”菜单提供了用来控制对话框各部分是否可见的选项。
  - “**选项**”菜单提供了用来显示所有消息以及使“**按访问扫描消息**”对话框始终保持在最前面的选项。
  - “**帮助**”菜单允许您访问VirusScan Enterprise产品的帮助主题、访问病毒信息和技术支持网站、提交病毒样本，还允许您访问关于当前安装的产品、许可、扫描引擎及 DAT 文件的信息。
- **VirusScan 消息** - 显示了所选消息的具体信息。
- **按钮** - 显示了可用于所选消息的操作按钮。如果某个操作不能用于所选的消息，相应的按钮将被禁用。
- **消息列表**-列出了按访问扫描程序检测到的病毒的相关消息。您可以单击列表区域中的某个列标题来对这一列排序。
- **状态栏** - 显示所选消息的状态。

在检测到病毒时采取措施

这部分介绍了您可以在按访问扫描程序检测到病毒时采取的操作。

> **注释**
> 您还可以选择向 AVERT 发送病毒样本以便进行分析。详细信息，请参阅第 33 页的 “提交病毒样本”。

使用**“按访问扫描消息”**对话框，您可以在按访问扫描程序检测到病毒时采取措施。

1. 右键单击系统任务栏中的  ，并选择 **“按访问扫描消息”**。
2. 突出显示列表中的消息，然后使用以下方法之一选择一个操作：
   - **“文件”**菜单。
   - 使用按钮选择操作。
   - 右键单击突出显示的消息，然后选择操作。

   您可以对列表中的消息执行以下操作：

   清除文件 - 尝试对所选消息提及的文件清除病毒。

   在某些情况下，文件中的病毒可能无法清除，这可能是因为没有清除程序，或者是受病毒侵害的文件已到了不可修复的地步。如果无法清除文件病毒，扫描程序会为文件名添加一个 .VIR 扩展名，并拒绝访问该文件，同时在日志文件中记录。

   > **注释**
   > 如果发生这种情况，建议您删除该文件，并用未感染病毒的备份副本将其恢复。

   移动文件 - 将所选消息提及的文件移到隔离文件夹。**“按访问扫描属性”**中**“常规”**选项卡上的 **“常规设置”**中定义了隔离文件夹的位置。

   删除文件 - 删除所选消息提及的文件。文件名将记录在日志中，以使您能够从备份副本恢复它。

   全选 (CTRL ＋ A) - 选择列表中的所有消息。

   删除消息 (CTRL+D) - 从列表中删除所选的消息。已经从列表中删除的消息仍可以从日志文件中看到。

   如果某个操作不能用于当前的消息，相应的图标、按钮和菜单项将被禁用。例如，如果文件已经删除，**“清除文件感染的病毒”**将不可用。

   管理员可以使用 **“按访问扫描属性”**的 **“常规设置”**中 **“消息”**选项卡上的选项来配置没有管理员权限的用户可以对列表中的消息执行的操作。如果管理员禁止了某个操作，该操作的按钮将会隐藏，图标和菜单项也将被禁用。

其他的可用操作包括：

- **打开日志文件** - 打开活动日志文件。
- **关闭窗口** - 关闭 “**按访问扫描消息**”对话框。

按需扫描 4

按需扫描程序提供了一种在方便时或者按一定时间间隔扫描计算机各部分病毒的方法。它可以作为按访问扫描程序持续保护功能的一种补充，也可以用来计划与您的工作时间不冲突的定期扫描。

内存进程扫描和增量扫描大大提高了病毒检测的效率。

- 内存进程扫描会在按需扫描运行之前检查处于活动状态的所有进程。如果发现某个进程感染了病毒，它会突出显示并停止这一进程。这意味着只要按需扫描程序发现一次某种病毒，即可删除这种病毒的所有实例。
- 增量扫描或可恢复的扫描允许扫描程序从上次中断处重新开始。您可以为计划的扫描定义开始时间和停止时间。按需扫描程序逻辑上扫描每个文件夹和相关文件。当达到时间限制时，扫描会停止运行。当下次执行增量计划扫描时，按需扫描会从文件和文件夹结构中上次扫描停止的位置继续。

这部分包含下列主题：

- 创建按需扫描任务
- 配置按需扫描任务
- 重设或保存默认设置
- 计划按需扫描任务
- 扫描操作
- 查看扫描结果
- 响应病毒检测

创建按需扫描任务

您可以通过三种方法创建按需扫描任务。您创建的可保存或未保存的扫描类型都取决于您使用的方法。请从以下选项中选择：

- 从“**开始**”菜单 - 如果不选择保存以便供将来使用，从“**开始**”菜单创建的任务将是一次性未保存的任务。
- 从系统任务栏中的 图标 - 如果不选择保存以便供将来使用，从系统任务栏创建的任务将是一次性未保存的任务。
- 从“**VirusScan 控制台**” - 从控制台创建的任务会自动保存在任务列表中，以供将来使用。

> **注释**
> 如果通过 ePolicy Orchestrator 3.0 或更高版本创建了按需扫描任务并启用了任务可见功能，您还可以在 VirusScan 控制台中看到这些按需扫描任务。这些 ePolicy Orchestrator 任务是只读的，不能从 VirusScan 控制台中配置。详细信息，请参阅《VirusScan Enterprise 配置指南 - 与 ePolicy Orchestrator 3.0 配合使用》。

这部分包含下列主题：

- 从开始菜单或系统任务栏创建任务
- 从控制台创建任务

从开始菜单或系统任务栏创建任务

从“开始”菜单或系统任务栏创建的按需扫描任务都是一次性未保存的任务。您可以配置、计划和运行已经创建的任务，但如果不选择保存，这些任务将在关闭“**按需扫描属性**”对话框时被丢弃。

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。
2. 使用以下方法之一打开 “**按需扫描属性**”：
   - 单击“**开始**”，然后选择“**程序**”|“**Network Associates**”|“**VirusScan 按需扫描**”。
   - 右键单击系统任务栏中的 并选择 “按需扫描”。

屏幕上将出现 “按需扫描属性 （未保存的任务）”对话框。

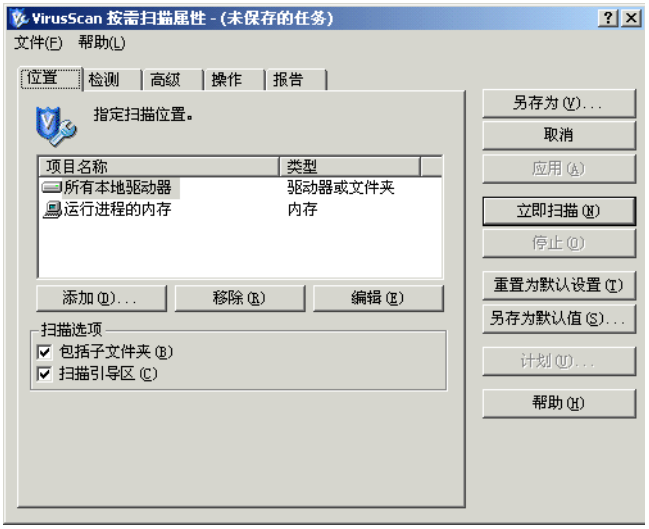

图 4-1. 按需扫描属性 - （未保存的任务）

注释

您可以看出这是一个未保存的按需扫描任务，因为标题栏中显示了 “（未保存的任务）”。单击 “另存为”可以将这项任务保存到控制台中以便重复使用。当保存了任务之后，“按需扫描属性”标题栏将从 “（未保存的任务）”变为您指定的任务名称。

3 配置一次性未保存的按需扫描任务。详细说明，请参阅第 81 页的 “配置按需扫描任务”。

4 单击 “应用”保存更改。

5 要计划某个任务，请先保存该任务，然后单击 “计划”。不能为未保存的任务制定计划。详细说明，请参阅第 199 页的 “计划任务”。

6 要运行任务，请单击 “立即扫描”。详细信息，请参阅第 96 页的 “运行按需扫描任务”。

从控制台创建任务

“**VirusScan 控制台**”具有默认的“**扫描所有固定磁盘**”按需扫描任务。您可以重命名这一任务并 / 或创建任意多个按需扫描任务。

要从控制台创建新的按需扫描任务：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

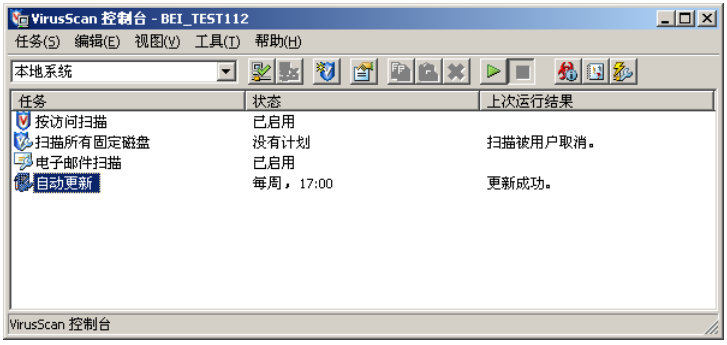

图 4-2. VirusScan 控制台

2 使用以下方法之一创建新的扫描任务：

- 无需选择任务列表中的任何项目，只需右键单击控制台中的空白区域，然后选择“**新建扫描任务**”。
- 选择“**任务**”菜单中的“**新建扫描任务**”。
- 单击控制台工具栏中的  。

“**VirusScan 控制台**”任务列表中将突出显示一个新的按需扫描任务。

3 为该任务键入一个新名称，然后按 ENTER 键打开 “按需扫描属性”对话框。

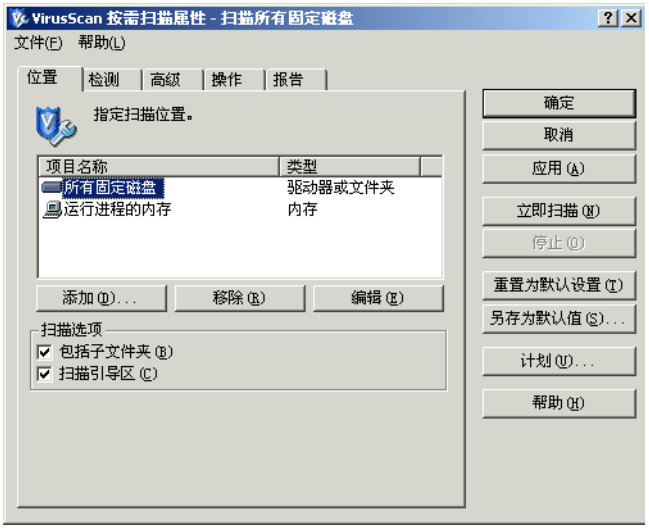

图 4-3. 按需扫描属性

配置按需扫描任务

您可以配置按需扫描程序以便确定扫描位置、扫描对象、在发现病毒时执行的操作以及在发现病毒时如何通知您。

这部分包含下列主题：

- 扫描位置属性
- 检测属性
- 高级属性
- 操作属性
- 报告属性
- 添加项目
- 删除项目
- 编辑项目

扫描位置属性

使用 “**位置**”选项卡中的选项，您可以指定要扫描的位置。

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 选择 “**位置**”选项卡。

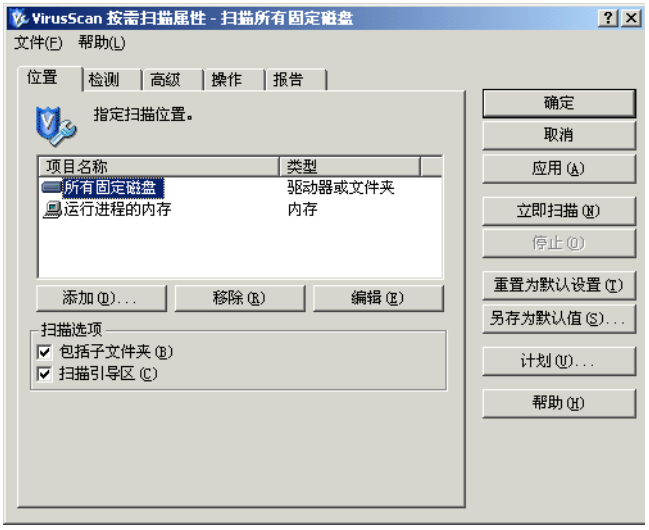

图 4-4. 按需扫描属性 - “扫描位置”选项卡

注释
默认情况下，该对话框会列出计算机的所有驱动器以及这些驱动器包含的所有子文件夹。这种大范围的扫描操作可能会花费较长的时间。以后定期扫描时，您可以缩小扫描的范围。

3 在 “**项目名称**”下，指定在何处进行扫描。默认情况下，系统会列出所有固定磁盘和正在运行进程的内存。

注释
如果正在创建新的扫描任务，系统会默认列出所有本地驱动器和正在运行进程的内存。

您可以使用 “**添加**”、“**删除**”和 / 或 “**编辑**”按钮指定要扫描的项目。详细说明，请参阅第 83 页的 “添加删除和编辑项目”。

4 在“扫描选项”下，选择其他扫描标准。请从以下选项中选择：

- **包括子文件夹**。该选项为默认选项，表示扫描程序会检查要扫描的目标卷中的所有子文件夹。如果准备只扫描所选卷的根一级目录，请取消选择“包括子文件夹”。
- **扫描引导区**。该选项为默认选项，表示扫描程序会检查磁盘引导区。如果磁盘包含无法接受病毒扫描的个别引导区或异常引导区，则应禁用引导区分析。

5 单击“应用”保存更改。

添加删除和编辑项目

您可以按照以下步骤“添加”、“删除”或“编辑”“按需扫描属性”中“项目名称”列表中的项目。

- 添加项目
- 删除项目
- 编辑项目

添加项目

1 为正在配置的任务打开“按需扫描属性”对话框。

2 在“位置”选项卡中，单击“添加”打开“添加扫描项目”对话框。

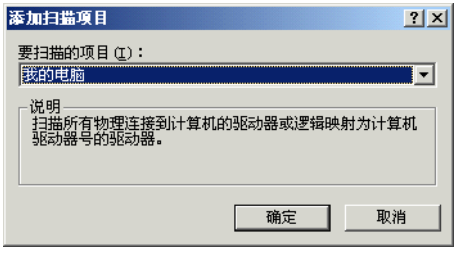

图 4-5. 添加扫描项目

3 单击 从列表中选择扫描项目。请从以下选项中选择：

- **我的电脑**。该选项为默认选项，表示扫描所有本地驱动器和映射驱动器。
- **所有本地驱动器**。扫描计算机中的所有驱动器以及它们包含的所有子文件夹。
- **所有固定磁盘**。扫描与计算机物理连接的硬盘。
- **所有可移动介质**。只扫描软盘、光盘、Iomega ZIP 磁盘或与计算机物理连接的类似存储设备。
- **所有网络驱动器**。扫描逻辑映射为计算机驱动器盘符的网络驱动器。
- **运行进程的内存**。扫描正在运行所有进程的内存。这种扫描会先于所有其他扫描启动。
- **用户的主文件夹**。扫描启动了扫描的那名用户的主文件夹。
- **用户的配置文件文件夹**。扫描启动了扫描的那名用户的配置文件。这包括“我的文档”文件夹。
- **驱动器或文件夹**。扫描特定的驱动器或文件夹。在“位置”文本框中输入驱动器或文件夹的路径，或者单击“浏览”查找并选择驱动器或文件夹。

  浏览完毕之后，单击“**确定**”返回到“**添加扫描项目**”对话框。
- **文件**。扫描特定的文件。在“位置”文本框中输入该文件的路径，或者单击“浏览”打开“选择要扫描的项目”以便查找并选择一个文件。

  选择了一个项目之后，单击“**打开**”返回到“**添加扫描项目**”对话框。

4 单击“**确定**”保存更改并返回到“**按需扫描属性**”对话框。

5 单击“**应用**”保存更改。

删除项目

1 为正在配置的任务打开“按需扫描属性”对话框。

2 在“位置”选项卡的“项目名称”列表中选择要删除的一个或多个项目，然后单击“删除”。

3 单击“是”确认您要删除这一项。

4 单击“应用”保存更改。

编辑项目

1 为正在配置的任务打开“按需扫描属性”对话框。

2 在“位置”选项卡的“项目名称”列表中选择一个项目，然后单击“编辑”打开“编辑扫描项目”对话框。

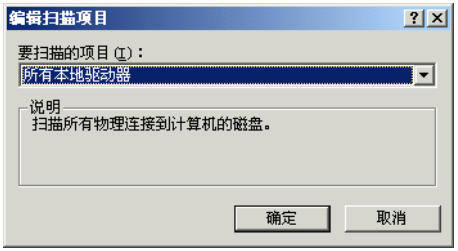

图 4-6. 编辑扫描项目

3 单击 以便从“要扫描的项目”列表中选择扫描项目。默认情况下会选择所有本地驱动器。

> **注释**
> 这里的选项与“添加项目”中的选项完全相同。请参阅第 84 页的步骤 3获得完整列表以及可用选项的描述。

4 单击“确定”返回到“按需扫描属性”对话框。

5 单击“应用”保存更改。

检测属性

使用“检测”选项卡上的选项，您可以指定按需扫描程序要检查哪些文件类型以及何时进行扫描。

1 为正在配置的任务打开“按需扫描属性”对话框。

2 选择“检测”选项卡。

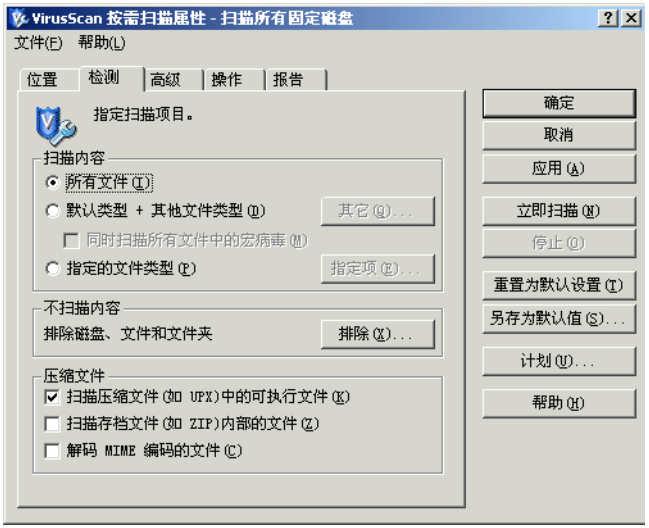

图 4-7. 按需扫描属性 - “检测”选项卡

3 在“扫描内容”下，选择下列选项之一：

- **所有文件**。该选项为默认选项，表示扫描所有文件，而不论其扩展名如何。
- **默认类型 + 其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他扩展名。当前的 DAT 文件定义了默认的文件类型扩展名列表。您可以添加或删除用户指定的文件类型扩展名，但不能删除默认列表中的任何文件类型扩展名。然而，您可以排除默认列表中的扩展名。详细信息，请参阅第 64 页的“排除文件、文件夹和驱动器”。
  - 其他。如果选择了“默认类型 + 其他文件类型”，您可以单击“其他”添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 62 页的“添加文件类型扩展名”。

    按需扫描程序最多可以列出 1000 个其他扩展名。
  - 同时扫描所有文件中的宏病毒。扫描所有文件是否含有宏病毒，而不论其扩展名如何。该选项只在选择了“默认类型 + 其他文件类型”选项后才可用。

    注释
    扫描所有文件中的宏病毒可能会影响性能。
- **指定的文件类型**。只扫描您指定的扩展名。
  - 指定项。如果选择了“指定文件类型”，您可以单击“指定项”添加或删除用户指定的文件类型扩展名。您也可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 63 页的“添加用户指定的文件类型扩展名”。

    按需扫描程序最多可以列出 1000 个指定的扩展名。

4 在“不扫描内容”下，您可以单击“排除”来指定不接受扫描的文件、文件夹和驱动器。详细说明，请参阅第 64 页的“排除文件、文件夹和驱动器”。

5 在“压缩文件”下，指定扫描程序要检查的压缩文件类型。您可以选择下列选项：

- **扫描压缩文件（如 UPX）中的可执行文件**。该选项为默认选项，表示检查含有可执行文件的压缩文件。压缩的可执行文件在运行时只将自己解压缩到内存中。压缩的可执行文件永远不会解压缩到磁盘中。
- **扫描存档文件（如 ZIP）内部的文件**。检查存档文件及其内容。存档文件是一种压缩文件，要访问它包含的文件，必须首先将其解压缩。存档文件中包含的文件在被写入到磁盘时会接受扫描。
- **解码 MIME 编码的文件**。检测、解码并扫描多用途 Internet 邮件扩展 (MIME) 编码的文件。

6 单击“应用”保存更改。

高级属性

使用“高级”选项卡中的选项，您可以指定高级扫描属性，例如扫描未知程序病毒和可能有害的程序、设置 CPU 利用率以及杂项。

1 为正在配置的任务打开“按需扫描属性”对话框。

2 选择“高级”选项卡。

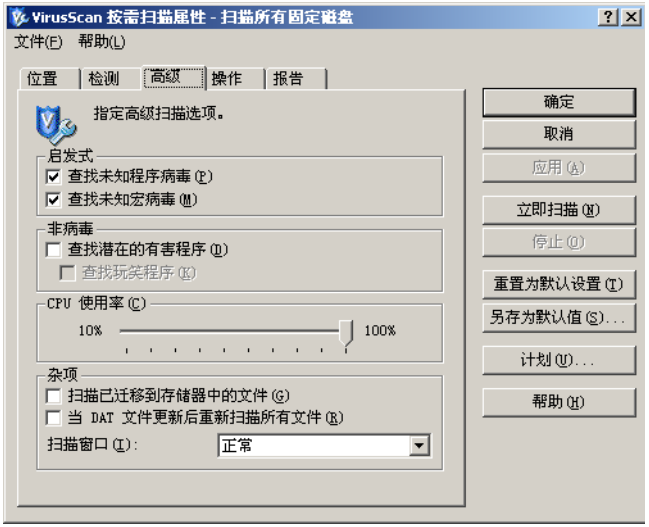

图 4-8. 按需扫描属性 - “高级”选项卡

3 在“启发式”下，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的可能性。启用了这项功能之后，扫描程序会分析这些内容是已知病毒变体的可能性。请选择以下选项的任意组合：

- **查找未知程序病毒**。该选项为默认选项，表示将含有类似于病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将应用您在“操作”选项卡中选择的操作。
- **查找未知宏病毒**。该选项为默认选项，表示将含有类似于病毒的代码的嵌入式宏作为真正感染了病毒的文件对待。扫描程序将对这些文件应用您在“操作”选项卡中选择的操作。

  注释

  该选项不同于“检测”选项卡中的“同时扫描所有文件中的宏病毒”，后者会命令扫描程序查找所有已知的宏病毒。该选项会命令扫描程序评估未知宏是病毒的可能性。

4 在“非病毒”下，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的有害程序**。检测可能有害的程序。
  - 查找玩笑程序。如果选择了“**查找潜在的有害程序**”，则您还会扫描可能有害的玩笑程序。

    警告
    VirusScan Enterprise 不会对检测到的可能有害的程序文件或玩笑程序采取任何措施。检测结果将记录在日志文件中。

    如果希望对检测到的玩笑程序或可能有害的程序采取措施，您必须手动操作。例如，要删除检测到的玩笑程序，您必须手动将其删除。

5 在“**CPU 使用率**”下，您可以使用滑块来对照计算机中正在运行的其他任务为扫描任务设置 CPU 利用率。 100% 为默认设置。这确保了其他软件的运行速度在扫描过程中不受影响，但扫描需要的时间也会更长。如果准备在 CPU 忙于处理其他必要操作时运行扫描任务，您需要降低扫描任务的利用率。

注释
您指定的 CPU 利用率极限值在扫描加密文件时无效。加密文件通过 LSASS.EXE 而非 SCAN32 进程处理。扫描加密的文件会大量占用 CPU 资源，因此即使 CPU 扫描线程极限值非常低，它也会以足够快的速度扫描加密文件，这也要求 LSASS.EXE 必须快速提供加密的数据。

6 在“**杂项**”下，选择下列选项之一：

- **扫描已迁移到存储器中的文件**。扫描已转移到离线存储器中的文件。

  注释
  如果用 Remote Storage 扩展了服务器的磁盘空间，则按需扫描程序可以扫描高速缓存中的文件。

  Remote Storage 可以按两个规定的级别分层存储数据。较高一级称为本地存储器，包括正在 Windows 2000 Server 上运行 Remote Storage 的计算机的 NTFS 磁盘卷。较低一级称为远程存储器，它位于连接到服务器计算机的自动磁带库或独立磁带驱动器中。

  Remote Storage 会将本地卷中符合条件的文件自动复制到磁带库中，然后监控本地卷上的可用空间。文件数据都在本地高速缓存，因此您可以在需要时快速存取这些数据。必要时，Remote Storage 可以将数据从本地存储器转移到远程存储器中。要访问存储在由 Remote Storage 管理的卷上的文件，只需正常打开该文件即可。如果该文件的数据没有在本地卷中高速缓存， Remote Storage 会从磁带库中重新调用这些数据。

- **当 DAT 文件更新后重新扫描所有文件**。在安装或更新了新的DAT文件之后，重新检查所有文件。这项功能最适于可恢复的计划扫描任务。该功能可以针对新病毒重新检查文件，从而降低病毒感染风险。

- **扫描窗口**。“正常”为默认选项。单击 以指定扫描窗口在按需扫描过程中的显示方式。这些选项包括：
  - 正常
  - 最小化
  - 隐藏

  注释
  尽管可以将扫描窗口配置为 “正常”、“最小化”或 “隐藏”，但无论您配置了哪种模式，计划任务窗口和远程任务窗口始终隐藏。

7 单击 “**应用**”保存更改。

操作属性

使用 “**操作**”选项卡中的选项，您可以指定扫描程序在检测到病毒时采取的主要操作和辅助操作。

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 选择 “**操作**”选项卡。

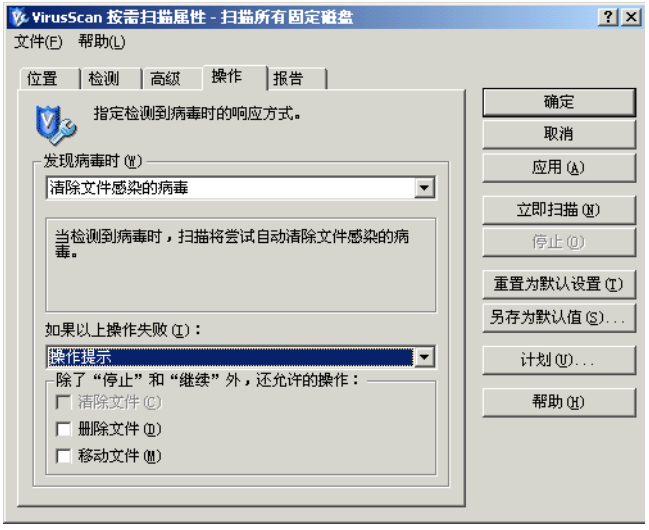

图 4-9. 按需扫描属性 - “操作”选项卡

3 在 “**发现病毒时**” 下，选择扫描程序在检测到病毒时采取的主要操作。

注释
默认的主要操作是 “**清除文件感染的病毒**”。

单击 以选择以下操作之一：

- **操作提示**。提示用户指定在检测到病毒时采取的措施。

  如果选择了这个选项，您还可以选择除 “**停止**” 和 “**继续**” 以外的操作。其他选择包括：

  - 清除文件。允许清除文件感染的病毒。
  - 删除文件。允许删除感染病毒的文件。
  - 移动文件。允许移动感染病毒的文件。

  该选项不允许使用辅助操作。

- **继续扫描**。在发现感染了病毒的文件时继续扫描。

  该选项不允许使用辅助操作。

  将感染病毒的文件移到文件夹。扫描程序会将感染病毒的文件移到隔离文件夹中。您可以接受 “**文件夹**” 文本框中的默认文件夹位置，也可以单击 “**浏览**” 找到文件夹所在的位置。

  隔离文件夹的默认位置和名称为：

  `< 驱动器 >:\quarantine\`

  注释
  隔离文件夹不应位于软驱或光驱中，它只能在硬盘上。

- **清除文件感染的病毒**。该选项为默认选项，表示扫描程序会尝试删除文件感染的病毒。如果扫描程序无法删除病毒，或者受病毒侵害的文件已到了不可修复的地步，扫描程序将执行辅助操作。详细信息，请参阅步骤 4。

- **删除感染病毒的文件**。当检测到病毒时，扫描程序会立即删除感染病毒的文件。请确保启用了 “报告” 选项卡中的 “记录到文件” 属性，以记录那些被感染的文件。

  如果选择了这个选项，系统将要求您确认。单击 “**是**” 确认，或者单击 “**否**” 取消这个选项。

  警告
  如果选择了 “**高级**” 选项卡中的 “**查找未知宏病毒**”，则您在这里选择的操作将应用于包含类似病毒的代码的所有宏。如果选择了 “**删除感染病毒的文件**”，则包含类似于宏病毒的代码的所有文件以及包含感染病毒文件的所有存档文件都将被删除。如果不希望删除这些文件，请确保您选择的操作与您针对宏选择的操作一致。

4 在“**如果以上操作失败**”下，选择扫描程序在首选操作失败后采取的辅助操作。

注释
默认的辅助操作是“**将感染病毒的文件移到文件夹**”。

单击 以选择以下操作之一：

- **操作提示**。如果选择了这个选项，您还可以选择除“停止”和“继续”以外的操作。其他选择包括：
  - 清除文件。允许清除文件感染的病毒。如果选择了“清除文件感染的病毒”作为主要操作，则该选项将被禁用。
  - 删除文件。允许删除感染病毒的文件。如果选择了“删除文件”作为主要操作，则该选项将被禁用。
  - 移动文件。允许移动感染病毒的文件。如果选择了“移动文件”作为主要操作，则该选项将被禁用。
- **继续扫描**。在发现感染了病毒的文件时继续扫描。
- **将感染病毒的文件移到文件夹**。该选项为默认选项，表示扫描程序会将感染病毒的文件移到隔离文件夹中。您可以接受“**文件夹**”文本框中的默认文件夹位置，也可以单击“**浏览**”找到文件夹所在的位置。

  隔离文件夹的默认位置和名称为：

  `< 驱动器 >:\quarantine\`

  注释
  隔离文件夹不应位于软驱或光驱中，它只能在硬盘上。
- **删除感染病毒的文件**。当检测到病毒时，扫描程序会立即删除感染病毒的文件。请确保启用了“**报告**”选项卡中的“**记录到文件**”属性，以记录那些被感染的文件。

5 单击“**应用**”保存更改。

报告属性

使用“**报告**”选项卡上的选项，您可以配置日志活动。指定日志文件的位置和大小以及每个日志条目要捕捉的信息。

注释

作为一个重要的管理工具，日志文件可以用来跟踪网络中的病毒活动，并记录扫描程序在发现病毒并做出响应时采用了哪些设置。此外，日志文件中记录的事件报告也有助于确定需要使用备份副本替换哪些文件、在隔离文件夹中检查哪些文件或者应从计算机中删除哪些文件。详细信息，请参阅第 100 页的“查看活动日志”。

1 打开“**按需扫描属性**”对话框。

2 选择“**报告**”选项卡。

图 4-10. 按需扫描属性 - “报告”选项卡

3 在“**日志文件**”下，选择下列选项之一：

- **记录到文件**。该选项为默认选项，表示在日志文件中记录按需病毒扫描活动。

- 接受文本框中的默认日志文件名称和位置、输入其他日志文件名称和位置，或者单击“浏览”查找计算机或网络中的适当文件。

  注释
  默认情况下，扫描程序将日志信息写入到如下文件夹中的 ONDEMANDSCANLOG.TXT 文件中：

  `<驱动器>:Winnt\Profiles\All Users\Application Data\Network Associates\VirusScan`。

- **将日志文件大小限制为**。该选项为默认选项，表示日志文件的默认大小为 1MB。接受默认的日志大小，或者设置不同的日志大小。如果选择了该选项，请输入一个介于 1MB 和 999MB 之间的值。

  注释
  如果日志文件中的数据超过了您设置的文件大小，则最早的 20% 的日志文件条目将被删除，而新数据将添加到该文件中。

4 在“**病毒活动以外的记录内容**”下，选择要记录在日志文件中的其他信息：

- **会话设置**。记录您为日志文件中的每个扫描会话选择的属性。
- **会话摘要**。该选项为默认选项，表示简要记录扫描程序在每次扫描会话过程中执行的操作，并将该信息添加到日志文件中。摘要信息包括已扫描的文件数量；检测到的病毒数量和类型；移动、清除或删除的文件数量以及其他信息。
- **扫描加密文件失败**。该选项为默认选项，表示在日志文件中记录扫描程序无法扫描的那些加密文件的名称。
- **用户名**。该选项为默认选项，表示将在扫描程序记录每个日志条目时已登录到计算机的用户的姓名记录在日志文件中。

5 单击“**应用**”保存更改。

重设或保存默认设置

当配置完按需扫描任务之后，您可以选择将配置设置重设为默认设置，也可以将当前配置设置保存为默认设置。

如果不希望重设默认设置或将当前设置保存为默认设置，请跳过这几步。

1 请从以下选项中选择：

- **重置为默认设置**。恢复默认的扫描设置。
- **另存为默认值**。将当前的扫描配置另存为默认配置。如果选择了“**另存为默认值**”，则系统将按照这个配置创建所有新任务。

2 单击“**应用**”保存更改。

计划按需扫描任务

当配置完按需扫描任务之后，您可以命令它在特定的日期和时间或者按一定时间间隔运行。

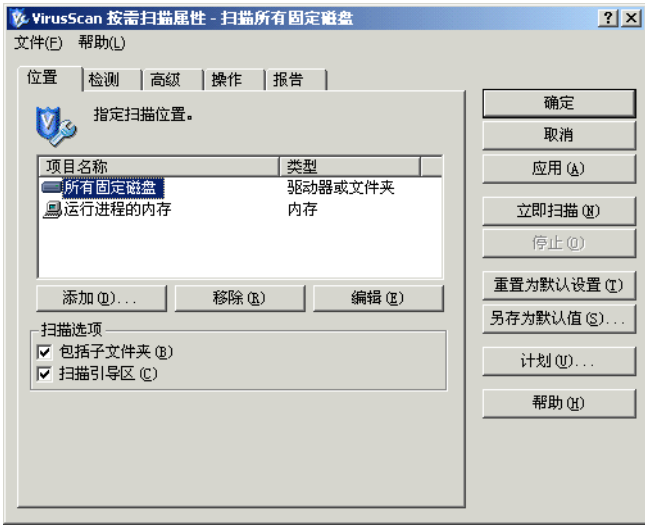

图 4-11. 按需扫描属性 - 计划

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 单击 “**计划**”。请参阅第 199 页的 “计划任务”详细了解如何计划任务。

扫描操作

您可以在无人值守的情况下运行预先计划的按需扫描任务或者直接启动扫描任务，也可以在扫描操作过程中暂停、停止和重新启动任务。

注释

在扫描操作过程中，按需扫描任务不扫描它自己的隔离文件夹。按需扫描程序故意将隔离文件夹排除在扫描操作之外，其目的在于避免重复扫描或循环扫描。

这部分包含下列主题：

- 运行按需扫描任务
- 暂停和重新启动按需扫描任务
- 停止按需扫描任务
- 可恢复的扫描

运行按需扫描任务

一旦使用所需的扫描属性配置了您的任务，就可以通过以下方法之一运行扫描任务：

- **按计划扫描**。计划的扫描任务可以在无人值守的情况下运行。

图 4-12. 按需扫描任务 - 进行中

注释

要使扫描程序运行您的任务，计算机必须处于开机状态。如果您的计算机在计划任务准备运行时处于关机状态，那么这项任务将在计算机处于开机状态时的下一个计划时间运行，但如果选择了 **“计划设置”**的 **“计划”**选项卡中的 **“运行错过的任务”**选项，这项任务将在计算机启动时运行。

注释

扫描程序总是在执行完由计划程序启动的计划任务以及远程计算机中运行的远程任务之后退出。

- **立即扫描**。您可以通过几种方法立即启动按需扫描任务：
  - 从系统任务栏或“**开始**”菜单创建按需扫描任务，然后在“**按需扫描属性**”对话框中单击 “立即扫描”。
  - 在 “**VirusScan** 控制台”中，右键单击按需扫描任务，并选择 “**启动**”。
  - 在 Windows 资源管理器中右键单击某个文件、文件夹、驱动器或其他项目，然后选择 “扫描病毒”。

  屏幕上将出现 “**按需扫描进程**”对话框。

图 4-13. 按需扫描 - 进行中

注释
扫描程序不会在执行完这几种直接扫描之后自动退出。要退出扫描程序，请选择 “**扫描**”菜单中的 “**退出**”。

暂停和重新启动按需扫描任务

您可以在扫描过程中暂停和重新启动按需扫描任务。

- 要暂停按需扫描任务，请单击 “**按需扫描**”对话框中的  。
- 要重新启动按需扫描任务，请单击 “**按需扫描**”对话框中的  。

停止按需扫描任务

您可以通过以下方法之一在扫描操作过程中停止按需扫描任务：

- 单击 “**按需扫描进程**”对话框中的  。
- 在 “**按需扫描属性**”对话框中单击 “**停止**”。

可恢复的扫描

按需扫描程序可以从上次扫描中断处自动恢复运行。按需扫描程序的增量扫描功能可以识别它扫描的最后一个文件，因此下次启动扫描时，您可以选择从中断处开始扫描，或者从头开始扫描。

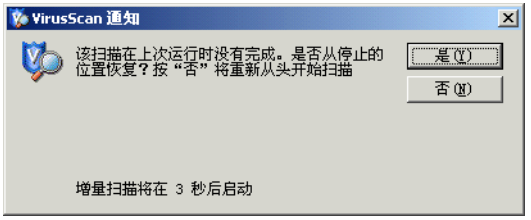

图 4-14. 可恢复的扫描

查看扫描结果

您可以在统计信息摘要和活动日志中查看按需扫描操作的结果。

这部分包含下列主题：

- 查看扫描统计信息
- 查看活动日志

查看扫描统计信息

“**按需扫描统计信息**”摘要显示了扫描程序已检查的文件数量、发现的病毒数量以及采取的响应措施。

要查看扫描任务的统计信息和结果：

1 打开“**VirusScan 控制台**”，右键单击任务列表中的按需扫描任务，然后选择“**统计信息**”。

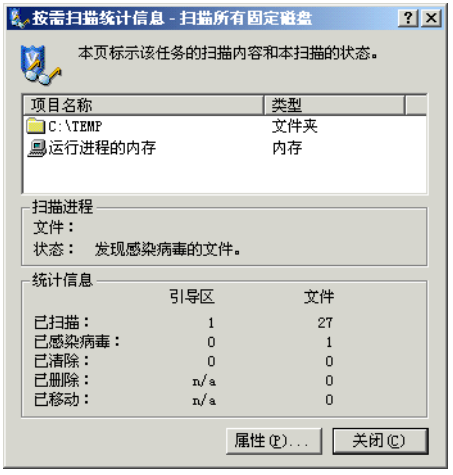

图 4-15. 按需扫描统计信息

“**按需扫描统计信息**”对话框在上部窗格中显示了为这项任务选择的所有扫描目标，在中间窗格中显示了扫描进程，在下部窗格中显示了统计信息摘要。

当扫描任务运行时，扫描程序正在检查的文件和扫描操作的状态将显示在中间窗格中。

注释
当这项任务再次运行时，下部窗格中将只显示上次扫描的统计信息。

2 单击“**属性**”打开“**按需扫描属性**”对话框并根据需要更改扫描属性，然后单击“**应用**”保存更改。

当按需扫描下次启动时，将采用新的设置运行。如果更改扫描属性时某个按需扫描正在运行，则直到按需扫描下次启动时，新设置才会生效。

3 查看了扫描统计信息之后，单击“**关闭**”。

查看活动日志

按需扫描活动日志显示了关于扫描操作的详细信息。例如，它可以显示扫描程序已检查的文件数量、发现的病毒数量以及采取的响应措施。

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一，打开活动日志文件：

- 突出显示一项任务，然后选择 “**任务**”菜单中的 “**活动日志**”。
- 右键单击任务列表中的这项任务，并选择 “**查看日志**”。

3 要关闭活动日志，请选择 “**文件**”菜单中的 “**退出**”。

响应病毒检测

按需扫描程序会根据您在 “**按需扫描属性**”对话框中选择的配置设置查找病毒。详细信息，请参阅第 81 页的 “配置按需扫描任务”。

如果警报管理器和 / 或按需扫描程序已被配置为在检测到病毒时发出通知，则您将在检测到病毒之后收到通知。

这部分包含下列主题：

- 接收病毒检测通知
- 在检测到病毒时采取措施

接收病毒检测通知

按需扫描程序可以在检测到病毒时发送三种类型的通知：

- **VirusScan 警报** - 如果已经在“**操作**”选项卡中将“**操作提示**”配置为按需扫描程序的主要操作或辅助操作，则检测到病毒时，屏幕上将显示一个警报对话框。详细信息，请参阅第 90 页的 “操作属性”。

  关于 “**VirusScan 警报**”对话框的详细信息，请参阅第 102 页的 “在检测到病毒时采取措施”。

- **Messenger 服务** - 显示一条网络消息，但前提是您已将警报管理器配置为这样做。详细信息，请参阅第 138 页的 “配置警报管理器”。

  以下是警报管理器发出的网络消息的示例：

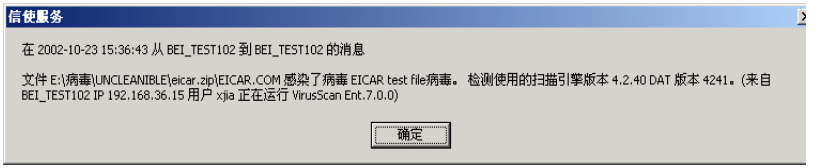

图 4-16. 按需扫描 - Messenger 服务

  这条消息提供了与感染病毒的文件有关的详细信息，例如文件名、文件位置、检测到的病毒类型以及检测病毒时使用的扫描引擎和 DAT 文件版本。查看这条消息的详细信息，然后单击 “**确定**”离开。

- “**按需扫描进程**”对话框 - 当按需扫描程序正在执行任务时，屏幕上会显示“**按需扫描进程**”对话框。一旦发现病毒，系统就会将它们显示在该对话框的下部窗格中。详细信息，请参阅第 103 页的 “按需扫描进程对话框”。

根据警报管理器和按需扫描程序的具体配置，您收到的通知可能不止一个。

> **注释**
> 如果没有将按需扫描程序或警报管理器配置为发送通知，您将不会收到 “**VirusScan 警报**”或网络消息。但在扫描操作过程中，您总是能够从 “**按需扫描进程**”对话框中查看检测到的病毒。

在检测到病毒时采取措施

这部分介绍了您可以在按需扫描程序检测到病毒时采取的操作。

注释

您还可以选择向 AVERT 发送病毒样本以便进行分析。详细信息，请参阅第 33 页的 “提交病毒样本”。

根据您在检测到病毒时收到通知的方式，使用 **“VirusScan 警报”**对话框或 **“按需扫描进程”**对话框对检测到的病毒采取措施。

- 如果收到 **“VirusScan 警报”**通知，您需要通过该对话框对检测到的病毒进行操作。
- 如果从 **“按需扫描进程”**对话框中发现了检测到的病毒，请在那里对检测到的病毒进行操作。

VirusScan 警报对话框

“VirusScan 警报”对话框将显示在屏幕上，并通知您检测到了病毒，但前提是您已将按需扫描程序配置为 **“操作提示”**。该对话框指出了感染病毒的文件所在的位置和感染的病毒类型。

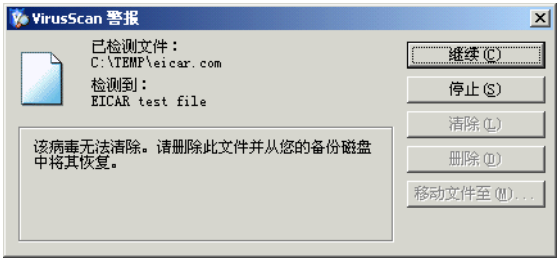

图 4-17. VirusScan 警报

选择要对感染病毒的文件执行的操作：

- **继续** - 继续扫描操作、记录此次活动中的每项检测并在 **“按需扫描”**对话框中列出感染病毒的各个文件。
- **停止** - 立即停止扫描操作。
- **清除病毒** - 尝试清除所选消息提及的文件所感染的病毒。

  如果由于没有病毒清除程序或者受病毒侵害的文件已到了不可修复的地步而导致文件感染的病毒无法清除，系统将在日志文件中记录一个条目，同时可能建议您采取某种应对措施。例如，如果无法清除文件感染的病毒，您应删除这个文件，并用备份副本恢复它。
- **删除** - 删除所选消息提及的文件。文件名将记录在日志中，以使您能够从备份副本恢复它。

- **移动文件至** - 将所选消息提及的文件移到您在该对话框中选择的文件夹中。

按需扫描进程对话框

当按需扫描程序正在执行任务时，屏幕上会显示“**按需扫描进程**”对话框。下部窗格为您列出了在按需扫描操作过程中检测到的病毒。

图 4-18. 按需扫描进程 - 检测到的病毒

1 您可以使用以下方法之一处理检测到的病毒：

   - 右键单击下部窗格中的文件名，并从菜单中选择要执行的操作。
   - 突出显示下部窗格中的文件名，并从“**扫描**”菜单中选择要执行的操作。

2 对列表中感染病毒的所有文件都执行了操作之后，选择“**扫描**”菜单中的“**退出**”关闭该对话框。

电子邮件扫描 5

电子邮件扫描程序允许您采用两种方式扫描本地主机或远程主机中的电子邮件文件夹、附件和邮件正文：

- 如果 Microsoft Outlook 正在运行，按发送电子邮件扫描程序可以在发送电子邮件时检查邮件及其附件。您可以从“**VirusScan 控制台**”配置和运行按发送电子邮件扫描程序。
- 如果需要，您可以从 Microsoft Outlook 中运行按需电子邮件扫描程序来检查电子邮件和附件。您可以从 Microsoft Outlook 中配置和运行按需电子邮件扫描程序。

  您可以将按需电子邮件扫描程序看成是对按发送电子邮件扫描程序防护功能的一种补充。例如，如果关闭了 Microsoft Outlook 或是首次安装 VirusScan Enterprise 产品，我们建议您首先运行按需电子邮件扫描。

这部分包含下列主题：

- 按发送电子邮件扫描
- 按需电子邮件扫描

按发送电子邮件扫描

按发送电子邮件扫描程序将在通过 Microsoft Outlook 收发电子邮件时扫描邮件附件和邮件正文。

警告

当 Microsoft Outlook 离线时，按发送扫描程序不会扫描入站的电子邮件。如果您的 Microsoft Outlook 离线，建议您在 Outlook 在线之后立即运行按需电子邮件扫描。详细说明，请参阅第 121 页的 “按需电子邮件扫描”。

这部分包含下列主题：

- 为本地主机或远程主机配置按发送电子邮件扫描
- 配置按发送电子邮件扫描属性
- 查看按发送电子邮件扫描结果

为本地主机或远程主机配置按发送电子邮件扫描

要通过“**VirusScan 控制台**”为本地主机或远程主机配置按发送“**电子邮件扫描**”：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

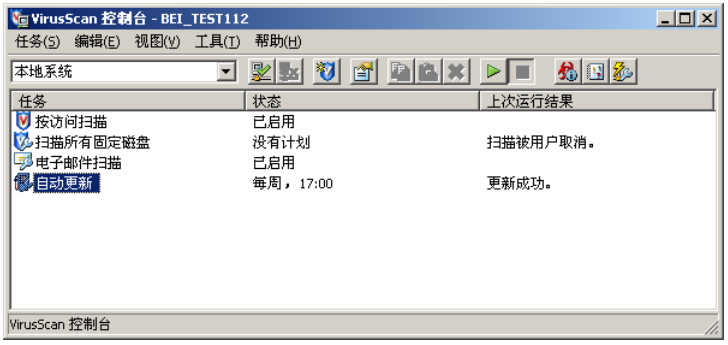

图 5-1. VirusScan 控制台

如果正在为本地主机配置 “**电子邮件扫描**”，请跳过步骤 2 并转到第 107 页的“配置按发送电子邮件扫描属性”。

2 如果正在为远程主机配置 “**电子邮件扫描**”：

a 从 “**工具**”菜单中选择 “**远程连接**”。

b 输入计算机的名称，或者单击 “**浏览**”查找计算机。

c 单击 “**确定**”返回到 “**VirusScan 控制台**”。

配置按发送电子邮件扫描属性

您可以将按发送电子邮件扫描程序配置为在通过 Microsoft Outlook 收发电子邮件时扫描电子邮件。

这部分包含下列主题：

- 检测属性
- 高级属性
- 操作属性
- 警报属性
- 报告属性

检测属性

使用 “**检测**” 选项卡上的选项，您可以指定要扫描的附件和文件类型扩展名。

1 使用以下方法之一，打开 “**按发送扫描属性**” 对话框：

- 突出显示任务列表中的 “**电子邮件扫描**”，然后单击  。
- 右键单击任务列表中的 “**电子邮件扫描**”，然后选择 “**属性**”。
- 双击任务列表中的 “**电子邮件扫描**”。

注释
如果尚未配置 Outlook，“Microsoft Outlook 配置” 对话框将启动。如果尚未登录到邮箱，系统会提示您登录。

2 选择“检测”选项卡。

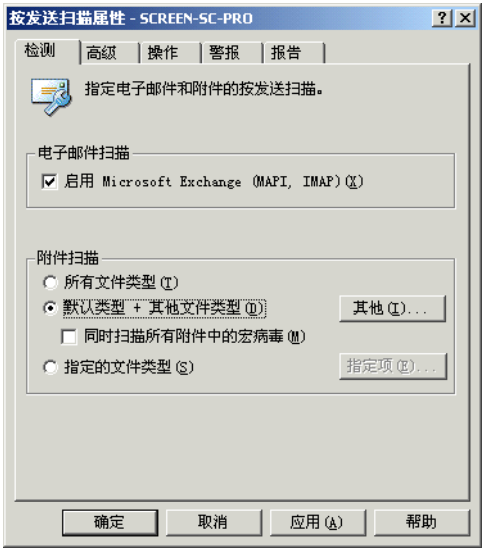

图 5-2. 按发送扫描属性 - “检测”选项卡

3 在“**电子邮件扫描**”下，“**启用 Microsoft Exchange（MAPI、IMAP）**”将被默认选定。如果不希望执行电子邮件扫描，请取消选择该选项。

4 在“**要扫描的附件**”下，选择下列选项之一：

- **所有文件类型**。该选项为默认选项，表示扫描所有附件，而不论其扩展名如何。
- **默认类型 + 其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他扩展名。当前的 DAT 文件定义了默认的文件类型扩展名列表。您可以添加或删除用户指定的文件类型扩展名，但不能删除默认列表中的任何文件类型扩展名。
  - **其他**。如果选择了“**默认类型 + 其他文件类型**”，您可以单击“**其他**”添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 62 页的“添加文件类型扩展名”。

    按发送电子邮件扫描程序最多可以列出 1000 个其他扩展名。
  - **同时扫描所有附件中的宏病毒**。扫描所有附件是否含有宏病毒，而不论其扩展名如何。该选项只在选择了“**默认类型 + 其他文件类型**”选项后才可用。

    注释
    扫描所有附件中的宏病毒可能会影响性能。

- **指定的文件类型**。只扫描您指定的扩展名。

  - **指定项**。如果选择了 **“指定文件类型”**，您可以单击 **“指定项”**添加或删除用户指定的文件类型扩展名。您也可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 63 页的“添加用户指定的文件类型扩展名”。

    按发送电子邮件扫描程序最多可以列出 1000 个指定的扩展名。

    注释
    电子邮件扫描功能不允许排除文件类型。

5 单击 **“应用”**保存更改。

高级属性

使用 **“高级”**选项卡上的选项，您可以指定高级扫描属性，例如扫描未知程序病毒、可能有害的程序、压缩文件以及电子邮件正文。

1 使用以下方法之一，打开 **“按发送扫描属性”**对话框：

- 突出显示任务列表中的 **“电子邮件扫描”**，然后单击  。
- 右键单击任务列表中的 **“电子邮件扫描”**，然后选择 **“属性”**。
- 双击任务列表中的 **“电子邮件扫描”**。

  注释
  如果尚未配置 Outlook，“Microsoft Outlook 配置”对话框将启动。如果尚未登录到邮箱，系统会提示您登录。

2 选择 **“高级”**选项卡。

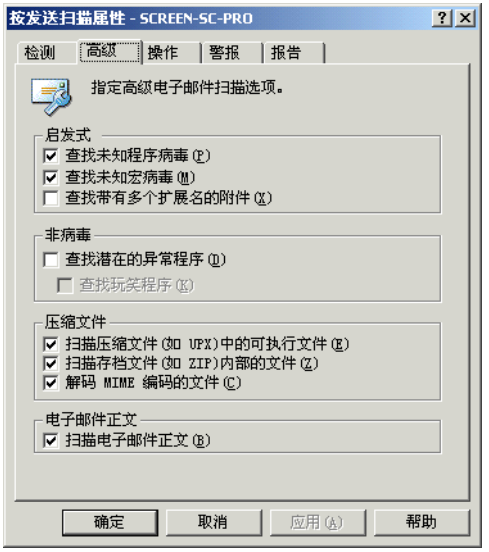

图 5-3. 按发送扫描属性 - “高级”选项卡

3 在“**启发式**”下，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的可能性。启用了这项功能之后，扫描程序会分析这些内容是已知病毒变体的可能性。请选择以下选项的任意组合：

- **查找未知程序病毒**。该选项为默认选项，表示将含有类似于病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将应用您在“**操作**”选项卡中选择的操作。
- **查找未知宏病毒**。该选项为默认选项，表示将含有类似病毒的代码的嵌入式宏视为病毒。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

  注释
  该选项不同于“**检测**”选项卡中的“**同时扫描所有文件中的宏病毒**”，后者会命令扫描程序查找所有已知的宏病毒。该选项会命令扫描程序评估未知宏是病毒的可能性。

- **查找带有多个扩展名的附件**。将带有多个扩展名的附件作为真正感染了病毒的附件对待。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

  选择了该选项之后，屏幕上将出现“**电子邮件扫描警告**”对话框。

  - **电子邮件扫描警告**。请仔细阅读警告。单击“**确定**”继续并同意将具有多个扩展名的附件作为真正感染了病毒的附件对待，或者单击“**取消**”取消选择该选项。

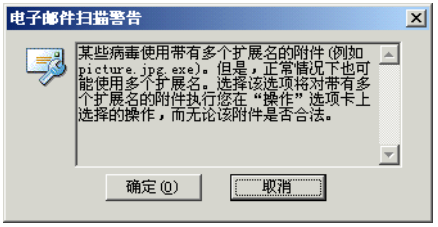

图 5-4. 电子邮件扫描警告

4 在“**非病毒**”下，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的有害程序**。检测可能有害的程序。
  - **查找玩笑程序**。如果选择了“**查找潜在的有害程序**”，扫描程序还会扫描玩笑程序。

警告

VirusScan Enterprise 不会对检测到的可能有害的程序文件或玩笑程序采取任何措施。检测结果将记录在日志文件中。

如果希望对检测到的玩笑程序或可能有害的程序采取措施，您必须手动操作。例如，要删除检测到的玩笑程序，您必须手动将其删除。

5 在“**压缩文件**”下，指定扫描程序要检查的压缩文件类型。您可以选择下列选项：

- **扫描压缩文件（如 UPX）中的可执行文件**。该选项为默认选项，表示检查含有可执行文件的压缩文件。压缩的可执行文件在运行时只将自己解压缩到内存中。压缩的可执行文件永远不会解压缩到磁盘中。
- **扫描存档文件（如 ZIP）内部的文件**。该选项为默认选项，表示检查存档文件及其内容。存档文件是一种压缩文件，要访问它包含的文件，必须首先将其解压缩。存档文件中包含的文件在被写入到磁盘时会接受扫描。
- **解码 MIME 编码的文件**。该选项为默认选项，表示检测、解码并扫描多用途 Internet 邮件扩展 (MIME) 编码的文件。

注释

尽管该选项能够更好地保护用户，但扫描压缩文件还是增加了扫描所需的时间。

6 在“**电子邮件正文**”下，“**扫描电子邮件正文**”将被默认选定。如果取消选择了这个选项，将不扫描电子邮件正文。

7 单击“**应用**”保存更改。

操作属性

使用“操作”选项卡中的选项，您可以指定扫描程序在检测到病毒时采取的主要操作和辅助操作。

1 使用以下方法之一，打开“按发送扫描属性”对话框：

- 突出显示任务列表中的“电子邮件扫描”，然后单击 。
- 右键单击任务列表中的“电子邮件扫描”，然后选择“属性”。
- 双击任务列表中的“电子邮件扫描”。

注释
如果尚未配置 Outlook，“Microsoft Outlook 配置”对话框将启动。如果尚未登录到邮箱，系统会提示您登录。

2 选择“操作”选项卡。

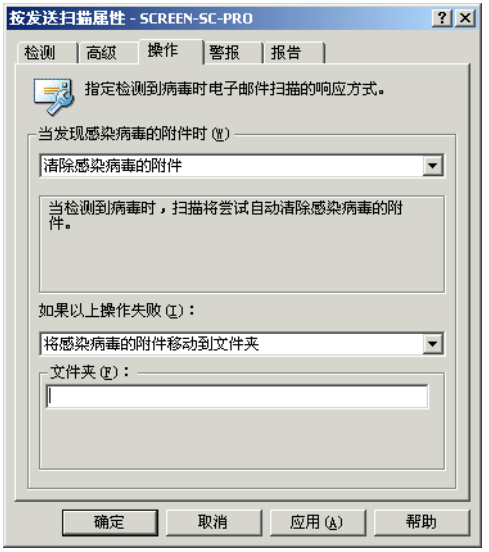

图 5-5. 按发送扫描属性 - “操作”选项卡

3 在“发现感染病毒的附件时”下，选择扫描程序在检测到病毒时采取的主要操作。

注释
默认的主要操作是“清除感染病毒的附件”。

单击 以选择以下操作之一：

- **操作提示**。提示用户指定在检测到病毒时采取的措施。

如果选择了这个选项，您还可以选择除停止和继续以外的操作。其他选择包括：

- **清除附件**。允许清除附件感染的病毒。
- **移动附件**。允许移动感染了病毒的附件。
- **删除附件**。允许删除感染了病毒的附件。

该选项不允许使用辅助操作。

- **继续扫描**。在发现感染了病毒的附件时继续扫描。

  该选项不允许使用辅助操作。

- **将感染病毒的附件移动到文件夹**。将感染了病毒的附件移到隔离文件夹中。默认的隔离文件夹名称是Quarantine。您可以接受默认的隔离文件夹名称，也可以输入一个新名称。

  注释
  Quarantine 文件夹创建于 MAPI 数据库中，可通过 Microsoft Outlook 的 **“文件夹列表”**查看。

- **清除感染病毒的附件**。该选项为默认选项，表示扫描程序会尝试删除附件感染的病毒。如果扫描程序无法删除附件中的病毒，或者受病毒侵害的附件已到了不可修复的地步，扫描程序将执行辅助操作。

- **删除感染病毒的附件**。当检测到病毒时，扫描程序会立即删除感染了病毒的附件。请确保启用了 **“报告”**选项卡中的 **“记录到文件”**属性，以记录感染了病毒的那些附件。

  如果选择了这个选项，系统将要求您确认。单击 **“是”**确认，或者单击 **“否”**取消这个选项。

4 在**“如果以上操作失败”**下，选择扫描程序在首选操作失败后采取的辅助操作。

  注释
  默认的辅助操作是 **“将感染病毒的附件移动到文件夹”**。

单击 以选择以下操作之一：

- **操作提示**。提示用户指定在检测到病毒时采取的措施。

如果选择了这个选项，您还可以选择除停止和继续以外的操作。其他选择包括：

- **清除附件**。允许清除附件感染的病毒。如果选择了“**清除附件病毒**”作为主要操作，则该选项将被禁用。
- **移动附件**。允许移动感染了病毒的附件。如果选择了“**移动附件**”作为主要操作，则该选项将被禁用。
- **删除附件**。允许删除感染了病毒的附件。如果选择了“**删除附件**”作为主要操作，则该选项将被禁用。

- **继续扫描**。在发现感染了病毒的文件时继续扫描。
- **将感染病毒的附件移动到文件夹**。该选项为默认选项，表示将感染了病毒的附件移到隔离文件夹。默认的隔离文件夹名称是 Quarantine。您可以接受默认的隔离文件夹名称，也可以输入一个新名称。

  注释
  Quarantine 文件夹创建于 MAPI 数据库中，可通过 Microsoft Outlook 的“**文件夹列表**”查看。

- **删除感染病毒的附件**。当检测到病毒时，扫描程序会立即删除感染了病毒的附件。请确保启用了“**报告**”选项卡中的“**记录到文件**”属性，以记录感染了病毒的那些附件。

  如果选择了这个选项，系统将要求您确认。单击“**是**”确认，或者单击“**否**”取消这个选项。

5 单击“**应用**”保存更改。

警报属性

使用“**警报**”选项卡中的选项，您可以配置检测到感染了病毒的电子邮件或附件时如何向用户发出警告。

1 使用以下方法之一，打开“**按发送扫描属性**”对话框：

- 突出显示任务列表中的“**电子邮件扫描**”，然后单击  。
- 右键单击任务列表中的“**电子邮件扫描**”，然后选择“**属性**”。
- 双击任务列表中的“**电子邮件扫描**”。

  注释
  如果尚未配置 Outlook，“Microsoft Outlook 配置”对话框将启动。如果尚未登录到邮箱，系统会提示您登录。

2 选择“警报”选项卡。

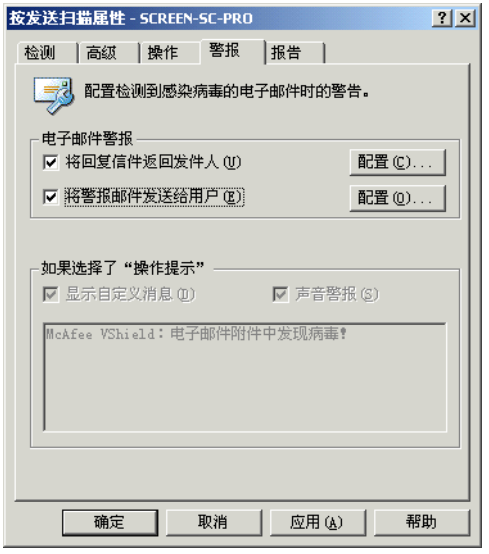

图 5-6. 按发送扫描属性 - “警报”选项卡

3 在“电子邮件警报”下，指定检测到感染了病毒的电子邮件时如何通知邮件发件人和其他用户。您可以选择下列选项：

- 将回复信件返回发件人。向发件人发送回复邮件。
  - 如果选择了该选项，请单击“配置”打开“返回邮件配置”对话框。

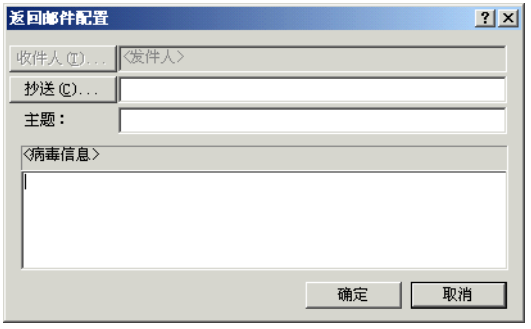

图 5-7. 电子邮件扫描 - 返回邮件配置

  - 输入要发送的内容，然后单击“确定”。

- **将警报邮件发送给用户**。向其他用户发送电子邮件警报。
  - 如果选择了该选项，请单击“**配置**”打开“**发送邮件配置**”对话框。

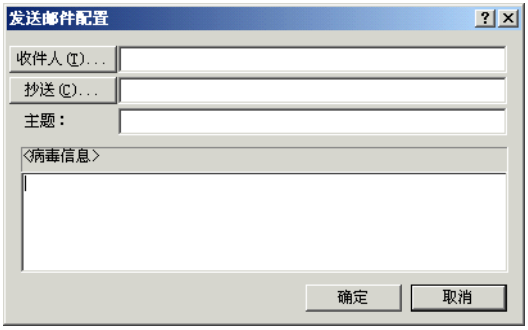

图 5-8. 电子邮件扫描 - 发送邮件配置

  - 输入要发送的内容，然后单击“**确定**”。

4 单击“**应用**”保存更改。

5 在“**如果选择了‘操作提示’**”下，指定检测到感染了病毒的电子邮件时如何通知用户。您可以选择下列选项：

- **显示自定义消息**。该选项为默认选项，表示使用自定义的消息通知用户。如果选择了该选项，您可以在文本框中输入自定义的消息。
- **声音警报**。该选项为默认选项，表示使用声音警报通知用户。

6 单击“**应用**”保存更改。

报告属性

使用“**报告**”选项卡上的选项，您可以配置日志活动。指定日志文件的位置和大小以及每个日志条目要捕捉的信息。

注释

作为一个重要的管理工具，日志文件可以用来跟踪网络中的病毒活动，并记录扫描程序在发现病毒并做出响应时采用了哪些设置。此外，日志文件中记录的事件报告也有助于确定需要使用备份副本替换哪些文件、在隔离文件夹中检查哪些文件或者应从计算机中删除哪些文件。详细信息，请参阅第 120 页的“查看按发送电子邮件活动日志”。

1 使用以下方法之一，打开“**按发送扫描属性**”对话框：

- 突出显示任务列表中的“**电子邮件扫描**”，然后单击  。
- 右键单击任务列表中的“**电子邮件扫描**”，然后选择“**属性**”。
- 双击任务列表中的“**电子邮件扫描**”。

注释

如果尚未配置 Outlook，“Microsoft Outlook 配置”对话框将启动。如果尚未登录到邮箱，系统会提示您登录。

2 选择“报告”选项卡。

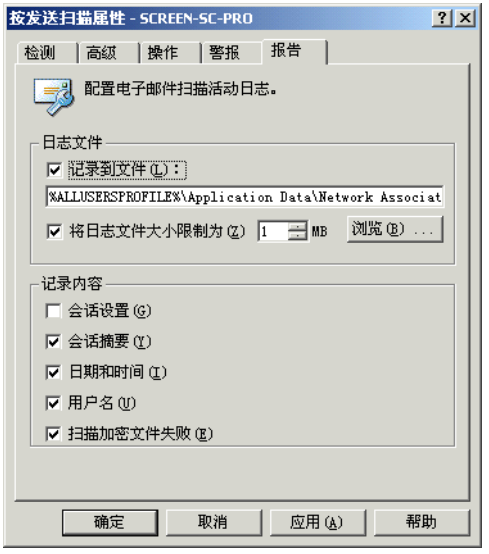

图 5-9. 按发送扫描属性 - “报告”选项卡

3 在“日志文件”下，选择下列选项之一：

- **记录到文件**。该选项为默认选项，表示在日志文件中记录按发送电子邮件病毒扫描活动。
- 接受文本框中的默认日志文件名称和位置、输入其他日志文件名称和位置，或者单击“浏览”查找计算机或网络中的适当文件。

  注释
  默认情况下，扫描程序将日志信息写入到如下文件夹中的 EmailOnDeliveryLog.txt 文件中：

  ```
  <驱动器>:Winnt\Profiles\All Users\
  Application Data\Network Associates\VirusScan
  ```

- **将日志文件大小限制为**。该选项为默认选项，表示日志文件的默认大小为 1MB。接受默认的日志大小，或者设置不同的日志大小。如果选择了该选项，请输入一个介于 1MB 和 999MB 之间的值。

  注释
  如果日志文件中的数据超过了您设置的文件大小，则最早的 20% 的日志文件条目将被删除，而新数据将添加到该文件中。

4 在“**记录内容**”下，选择要记录在日志文件中的其他信息：

- **会话设置**。记录您为日志文件中的每个扫描会话选择的属性。
- **会话摘要**。该选项为默认选项，表示简要记录扫描程序在每次扫描会话过程中执行的操作，并将该信息添加到日志文件中。摘要信息包括已扫描的文件数量；检测到的病毒数量和类型；移动、清除或删除的文件数量以及其他信息。
- **日期和时间**。该选项为默认选项，表示记录检测到病毒时的日期和时间。
- **用户名**。该选项为默认选项，表示将在扫描程序记录每个日志条目时已登录到电子邮件的用户的姓名记录在日志文件中。
- **扫描加密文件失败**。该选项为默认选项，表示在日志文件中记录扫描程序无法扫描的那些加密文件的名称。

5 单击“**应用**”保存更改。

查看按发送电子邮件扫描结果

您可以在统计信息摘要和活动日志中查看扫描操作的结果。

这部分包含下列主题：

- 查看按发送电子邮件扫描统计信息
- 查看按发送电子邮件活动日志

查看按发送电子邮件扫描统计信息

“**按发送电子邮件扫描统计信息**”摘要显示了扫描程序已检查的文件数量、发现的病毒数量以及采取的响应措施。

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 通过以下方法之一，打开“**按发送电子邮件扫描统计信息**”对话框：

- 突出显示任务列表中的电子邮件扫描任务，然后从“**任务**”菜单中选择“**统计信息**”。

- 右键单击任务列表中的电子邮件扫描任务，并选择 “**统计信息**”。

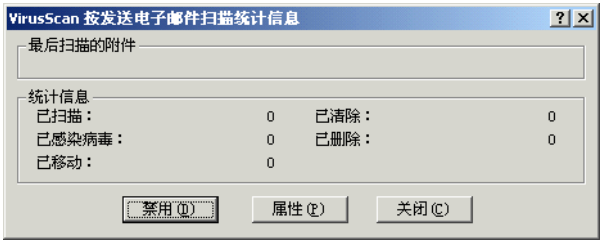

图 5-10. 按发送电子邮件扫描统计信息

“**按发送电子邮件扫描统计信息**”对话框的上部窗格中显示了 “**最后扫描的附件**”，下部窗格中显示了统计信息摘要。

如果扫描操作仍在运行，则显示扫描程序当前检查的文件以及扫描操作的状态。

3 如果具有管理员权限并根据需要输入了密码，您可以使用以下任一项功能：

- 单击 “**禁用**”以取消激活电子邮件按发送扫描程序。这项功能将在 “**禁用**”和 “**启用**”之间切换。
- 单击 “**属性**”打开 “**按发送电子邮件扫描属性**”对话框，并根据需要更改扫描属性，然后单击 “**应用**”保存更改。

  扫描会立即采用新的设置运行。

4 查看了扫描统计信息之后，单击 “**关闭**”。

查看按发送电子邮件活动日志

按发送扫描活动日志显示了关于扫描操作的详细信息。例如，它可以显示扫描程序已检查的文件数量、发现的病毒数量以及采取的响应措施。

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一，打开活动日志文件：

- 突出显示电子邮件扫描任务，然后选择 “**任务**”菜单中的 “**活动日志**”。
- 右键单击任务列表中的电子邮件扫描任务，并选择 “**查看日志**”。

3 要关闭活动日志，请选择 “**文件**”菜单中的 “**退出**”。

按需电子邮件扫描

如果需要，您可以从 Microsoft Outlook 中直接运行按需电子邮件扫描任务来扫描所选的电子邮件和附件。在 Microsoft Outlook 关闭了一段时间之后，您可以将按需电子邮件扫描程序用作对按发送电子邮件扫描程序的补充。

注释
如果在 VirusScan Enterprise 安装过程中 Microsoft Outlook 一直在运行，我们建议您在安装进程结束后重新启动 Microsoft Outlook。

这部分包含下列主题：

- 配置按需电子邮件任务
- 运行按需电子邮件任务
- 查看按需电子邮件扫描结果

配置按需电子邮件任务

您可以用 Microsoft Outlook 来配置按需电子邮件扫描任务，以便对邮件及附件进行扫描。

这部分包含下列主题：

- 检测属性
- 高级属性
- 操作属性
- 警报属性
- 报告属性

检测属性

使用 “**检测**”选项卡上的选项，您可以指定要扫描的附件和文件类型扩展名。

1. 启动 Microsoft Outlook。
2. 通过以下方法之一，打开 “**按需电子邮件扫描属性**”对话框：
   - 选择 “**工具**”菜单中的 “**电子邮件扫描属性**”。
   - 单击 Outlook 工具栏中的 。

     注释
     如果该图标在 Outlook 工具栏中不可见，请单击标准工具栏右侧的 ，然后选择该图标。
3. 选择 “**检测**”选项卡。

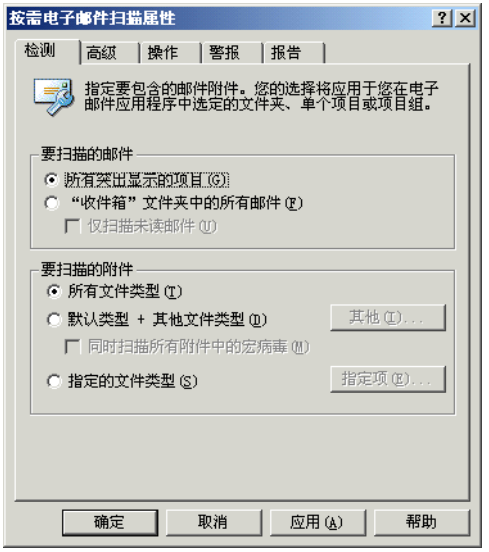

图 5-11. 按需电子邮件扫描属性 - “检测”选项卡

4 在“**要扫描的邮件**”下，指定要扫描的邮件。您可以选择下列选项：

- **所有突出显示的项目**。该选项为默认选项，表示扫描选定的电子邮件或文件夹。
- **“收件箱”文件夹中的所有邮件**。扫描当前“**收件箱**”文件夹及其子文件夹中的所有邮件。
  - **仅扫描未读邮件**。只扫描当前“**收件箱**”文件夹及其子文件夹中的未读文件。如果未选择“‘**收件箱**’**文件夹中的所有邮件**”，该选项将被禁用。

5 在“**要扫描的附件**”下，指定要扫描的文件、文件夹或驱动器。您可以选择下列选项：

- **所有文件类型**。该选项为默认选项，表示扫描所有附件，而不论其扩展名如何。

- **默认类型+其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他扩展名。当前的 DAT 文件定义了默认的文件类型扩展名列表。您可以添加或删除用户指定的文件类型扩展名，但不能删除默认列表中的任何文件类型扩展名。

  - **其他**。如果选择了“**默认类型 + 其他文件类型**”，您可以单击“**其他**”添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 62 页的“添加文件类型扩展名”。

    按需电子邮件扫描程序最多可以列出 1000 个其他扩展名。

  - **同时扫描所有附件中的宏病毒**。扫描所有附件是否含有宏病毒，而不论其扩展名如何。该选项只在选择了“**默认类型 + 其他文件类型**”选项后才可用。

    注释
    扫描所有附件中的宏病毒可能会影响性能。

- **指定的文件类型**。只扫描您指定的扩展名。

  - **指定项**。如果选择了“**指定文件类型**”，您可以单击“**指定项**”添加或删除用户指定的文件类型扩展名。您也可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 63 页的“添加用户指定的文件类型扩展名”。

    按需电子邮件扫描程序最多可以列出 1000 个指定的扩展名。

    注释
    电子邮件扫描功能不允许排除文件类型。

6 单击“**应用**”保存更改。

高级属性

使用“高级”选项卡上的选项，您可以指定高级扫描属性，例如扫描未知程序病毒、可能有害的程序、压缩文件以及电子邮件正文。

1 启动 Microsoft Outlook。

2 通过以下方法之一，打开“按需电子邮件扫描属性”对话框：

- 选择“工具”菜单中的“电子邮件扫描属性”。
- 单击 Outlook 工具栏中的 。

注释

如果该图标在 Outlook 工具栏中不可见，请单击标准工具栏右侧的 ，然后选择该图标。

3 选择“高级”选项卡。

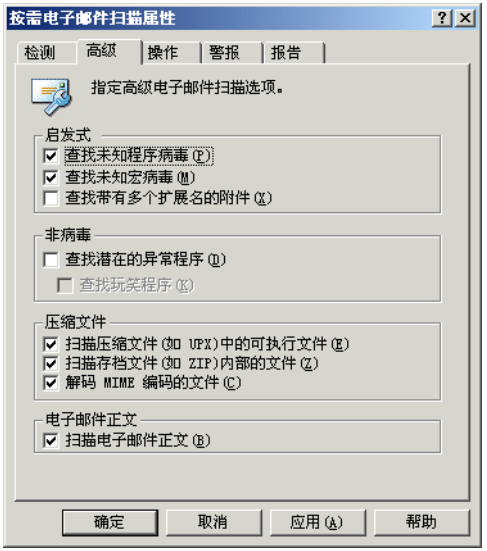

图 5-12. 按需电子邮件扫描属性 - “高级”选项卡

4 在“**启发式**”下，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的可能性。启用了这项功能之后，扫描程序会分析这些内容是已知病毒变体的可能性。您可以选择下列选项：

- **查找未知程序病毒**。该选项为默认选项，表示将含有类似于病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。
- **查找未知宏病毒**。该选项为默认选项，表示将含有类似病毒的代码的嵌入式宏视为病毒。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

  注释

  该选项不同于“**检测**”选项卡中的“**同时扫描所有文件中的宏病毒**”，后者会命令扫描程序查找所有已知的宏病毒。该选项会命令扫描程序评估未知宏是病毒的可能性。
- **查找带有多个扩展名的附件**。将带有多个扩展名的附件作为真正感染了病毒的附件对待。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

  选择了该选项之后，屏幕上将出现“**电子邮件扫描警告**”对话框：

  - **电子邮件扫描警告**。请仔细阅读警告。单击“**确定**”继续并同意将具有多个扩展名的附件作为真正感染了病毒的附件对待，或者单击“**取消**”取消选择该选项。

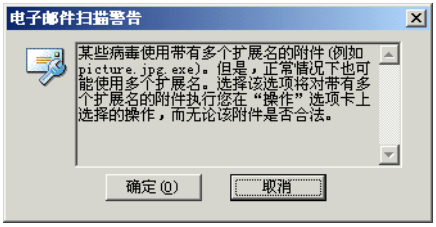

图 5-13. 电子邮件扫描警告

5 在“**非病毒**”下，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的有害程序**。检测可能有害的程序。
  - **查找玩笑程序**。如果选择了“**查找潜在的有害程序**”，扫描程序还会扫描玩笑程序。

警告
VirusScan Enterprise 不对可能有害的程序文件或玩笑程序采取任何操作。检测结果将记录在日志文件中。

6 在“**压缩文件**”下，指定扫描程序要检查的压缩文件类型。您可以选择下列选项：

- **扫描压缩文件（如 UPX）中的可执行文件**。该选项为默认选项，表示检查含有可执行文件的压缩文件。压缩的可执行文件在运行时只将自己解压缩到内存中。压缩的可执行文件永远不会解压缩到磁盘中。
- **扫描存档文件（如 ZIP）内部的文件**。该选项为默认选项，表示检查存档文件及其内容。存档文件是一种压缩文件，要访问它包含的文件，必须首先将其解压缩。存档文件中包含的文件在被写入到磁盘时会接受扫描。
- **解码 MIME 编码的文件**。该选项为默认选项，表示检测、解码并扫描多用途 Internet 邮件扩展 (MIME) 编码的文件。

注释
尽管该选项能够更好地保护用户，但扫描压缩文件还是增加了扫描所需的时间。

7 在“**电子邮件正文**”下，“**扫描电子邮件正文**”将被默认选定。如果取消选择了这个选项，将不扫描电子邮件正文。

8 单击“**应用**”保存更改。

操作属性

使用“操作”选项卡中的选项，您可以指定扫描程序在检测到病毒时采取的主要操作和辅助操作。

1 启动 Microsoft Outlook。

2 通过以下方法之一，打开“按需电子邮件扫描属性”对话框：

- 选择“工具”菜单中的“电子邮件扫描属性”。
- 单击 Outlook 工具栏中的 。

注释

如果该图标在 Outlook 工具栏中不可见，请单击标准工具栏右侧的 ，然后选择该图标。

3 选择“操作”选项卡。

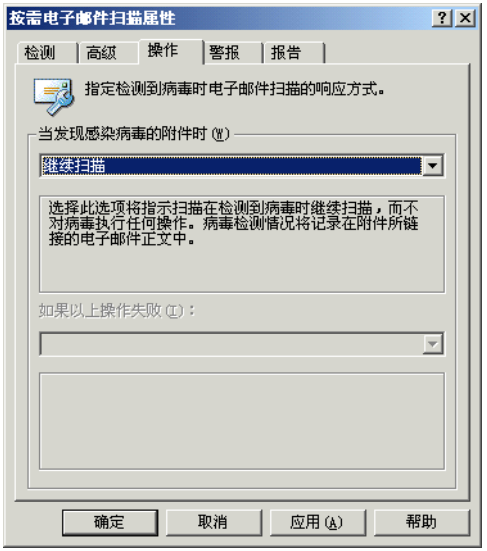

图 5-14. 按需电子邮件扫描属性 - “操作”选项卡

4 在“**发现感染病毒的附件时**”下，选择扫描程序在检测到病毒时采取的主要操作。

注释
默认的主要操作是“**清除感染病毒的附件**”。

单击 以选择以下操作之一：

- **操作提示**。提示用户指定在检测到病毒时采取的措施。

  如果选择了这个选项，您还可以选择除停止和继续以外的操作。其他选择包括：

  - **清除附件**。允许清除附件感染的病毒。如果选择了“**清除感染病毒的附件**”作为主要操作，则该选项将被禁用。
  - **移动附件**。允许移动感染了病毒的附件。如果选择了“**将感染病毒的附件移动到文件夹**”作为主要操作，则该选项将被禁用。
  - **删除附件**。允许删除感染了病毒的附件。如果选择了“**删除感染病毒的附件**”作为主要操作，则该选项将被禁用。

  该选项不允许使用辅助操作。

- **继续扫描**。在发现感染了病毒的附件时继续扫描。

  该选项不允许使用辅助操作。

- **将感染病毒的附件移动到文件夹**。将感染了病毒的附件移到隔离文件夹。默认的隔离文件夹名称是 quarantine。您可以接受默认的隔离文件夹名称，也可以输入一个新名称。

  注释
  quarantine 文件夹创建于 MAPI 数据库中，可通过 Microsoft Outlook 的“**文件夹列表**”查看。

- **清除感染病毒的附件**。该选项为默认选项，表示扫描程序会尝试删除附件感染的病毒。如果扫描程序无法删除附件中的病毒，或者受病毒侵害的附件已到了不可修复的地步，扫描程序将执行辅助操作。

- **删除感染病毒的附件**。当检测到病毒时，扫描程序会立即删除感染了病毒的附件。请确保启用了“**报告**”选项卡中的“**记录到文件**”属性，以记录感染了病毒的那些附件。

  如果选择了这个选项，系统将要求您确认。单击“**是**”确认，或者单击“**否**”取消这个选项。

5 在“**如果以上操作失败**”下，选择扫描程序在首选操作失败后采取的辅助操作。

注释
默认的辅助操作是“**将感染病毒的附件移动到文件夹**”。

单击 以选择以下操作之一：

- **操作提示**。提示用户指定在检测到病毒时采取的措施。

  如果选择了这个选项，您还可以选择除停止和继续以外的操作。其他选择包括：

  - **清除附件**。允许清除附件感染的病毒。
  - **移动附件**。允许移动感染了病毒的附件。
  - **删除附件**。允许删除感染了病毒的附件。

- **继续扫描**。在发现感染了病毒的文件时继续扫描。
- **将感染病毒的附件移动到文件夹**。该选项为默认选项，表示将感染了病毒的附件移到隔离文件夹。默认的隔离文件夹名称是 Quarantine。您可以接受默认的隔离文件夹名称，也可以输入一个新名称。

  注释
  Quarantine 文件夹创建于 MAPI 数据库中，可通过 Microsoft Outlook 的“**文件夹列表**”查看。

- **删除感染病毒的附件**。当检测到病毒时，扫描程序会立即删除感染了病毒的附件。请确保启用了“**报告**”选项卡中的“**记录到文件**”属性，以记录感染了病毒的那些附件。

  如果选择了这个选项，系统将要求您确认。单击“**是**”确认，或者单击“**否**”取消这个选项。

6 单击“**应用**”保存更改。

警报属性

使用“警报”选项卡中的选项，您可以配置检测到感染了病毒的电子邮件或附件时如何向用户发出警告。

1 启动 Microsoft Outlook。

2 通过以下方法之一，打开“按需电子邮件扫描属性”对话框：

- 选择“工具”菜单中的“电子邮件扫描属性”。
- 单击 Outlook 工具栏中的 。

注释

如果该图标在 Outlook 工具栏中不可见，请单击标准工具栏右侧的 ，然后选择该图标。

3 选择“警报”选项卡。

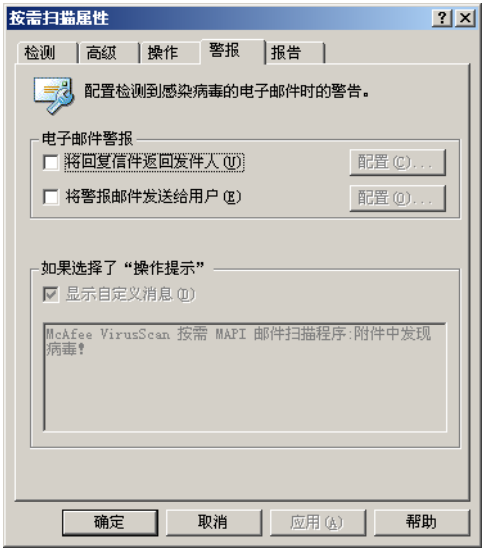

图 5-15. 按需电子邮件扫描属性 - “警报”选项卡

4 在 “**电子邮件警报**” 下，指定检测到感染了病毒的电子邮件时如何通知邮件发件人和其他用户。您可以选择下列选项：

- **将回复信件返回发件人**。向发件人发送回复邮件。
  - 如果选择了该选项，请单击 “**配置**” 打开 “**返回邮件配置**” 对话框。

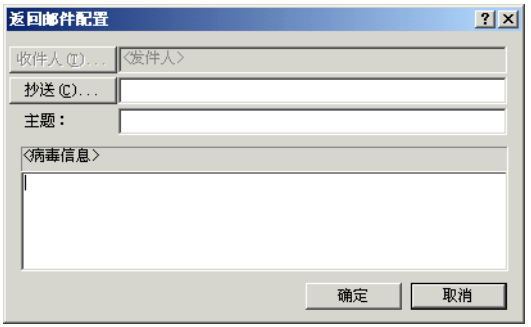

图 5-16. 电子邮件扫描 - 返回邮件配置

  - 输入要发送的内容，然后单击 “**确定**”。
- **将警报邮件发送给用户**。向其他用户发送电子邮件警报。
  - 如果选择了该选项，请单击 “**配置**” 打开 “**发送邮件配置**” 对话框。

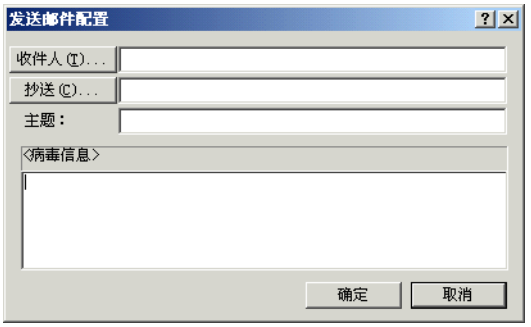

图 5-17. 电子邮件扫描 - 发送邮件配置

  - 输入要发送的内容，然后单击 “**确定**”。

5 在 “**如果选择了 ‘操作提示’**” 下，指定检测到感染了病毒的电子邮件时如何通知用户。您可以选择下列选项：

- **显示自定义消息**。使用自定义的消息通知用户。如果选择了该选项，您可以在文本框中输入自定义的消息。
- **声音警报**。使用声音警报通知用户。

6 单击“**应用**”保存更改。

报告属性

使用“**报告**”选项卡上的选项，您可以配置日志活动。指定日志文件的位置和大小以及每个日志条目要捕捉的信息。

> **注释**
> 作为一个重要的管理工具，日志文件可以用来跟踪电子邮件中的病毒活动，并记录扫描程序在发现病毒并做出响应时采用了哪些设置。以后查阅时，您可以在文本编辑器中打开日志文件。此外，日志文件中记录的事件报告也有助于确定需要使用备份副本替换哪些文件、在隔离文件夹中检查哪些文件或者应从计算机中删除哪些文件。

1 启动 Microsoft Outlook。

2 通过以下方法之一，打开“**按需电子邮件扫描属性**”对话框：

- 选择“**工具**”菜单中的“**电子邮件扫描属性**”。
- 单击 Outlook 工具栏中的  。

> **注释**
> 如果该图标在 Outlook 工具栏中不可见，请单击标准工具栏右侧的  ，然后选择该图标。

3 选择“报告”选项卡。

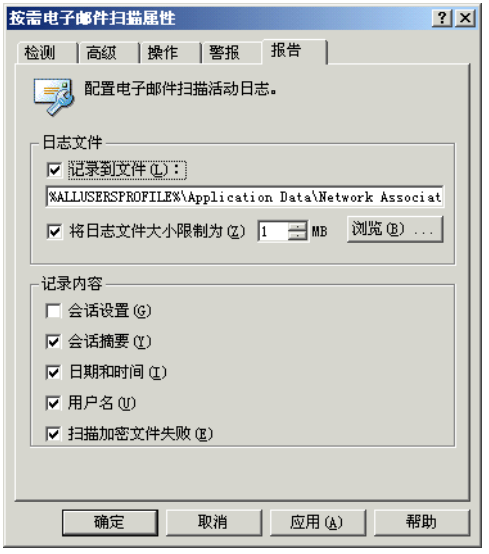

图 5-18. 按需电子邮件扫描属性 - “报告”选项卡

4 在“日志文件”下，选择下列选项之一：

- **记录到文件**。该选项为默认选项，表示在日志文件中记录按需电子邮件病毒扫描活动。
- 接受文本框中的默认日志文件名称和位置、输入其他日志文件名称和位置，或者单击“浏览”查找计算机或网络中的适当文件。

  注释
  默认情况下，扫描程序将日志信息写入到如下文件夹中的 EMAILONDEMANDLOG.TXT 文件中：

  `<驱动器>:Winnt\Profiles\All Users\Application Data\Network Associates\VirusScan`。

- **将日志文件大小限制为**。该选项为默认选项，表示日志文件的默认大小为 1MB。接受默认的日志大小，或者设置不同的日志大小。如果选择了该选项，请输入一个介于 1MB 和 999MB 之间的值。

  注释
  如果日志文件中的数据超过了您设置的文件大小，则最早的 20% 的日志文件条目将被删除，而新数据将添加到该文件中。

5 在“**记录内容**”下，选择要在日志文件中记录的其他信息：

- **会话设置**。记录您为日志文件中的每个扫描会话选择的属性。
- **会话摘要**。该选项为默认选项，表示简要记录扫描程序在每次扫描会话过程中执行的操作，并将该信息添加到日志文件中。摘要信息包括已扫描的文件数量；检测到的病毒数量和类型；移动、清除或删除的文件数量以及其他信息。
- **日期和时间**。该选项为默认选项，表示记录检测到病毒时的日期和时间。
- **用户名**。该选项为默认选项，表示将在扫描程序记录每个日志条目时已登录到计算机的用户的姓名记录在日志文件中。
- **扫描加密文件失败**。该选项为默认选项，表示在日志文件中记录扫描程序无法扫描的那些加密文件的名称。

6 单击“**应用**”保存更改。

运行按需电子邮件任务

要运行按需电子邮件扫描任务：

1 启动 Microsoft Outlook。

2 使用以下方法之一，从 Microsoft Outlook 启动按需电子邮件扫描：

- 从 “**工具**”菜单中选择 “**扫描病毒**”。
- 单击 Outlook 工具栏中的 。

注释

如果该图标在 Outlook 工具栏中不可见，请单击标准工具栏右侧的 ，然后选择该图标。

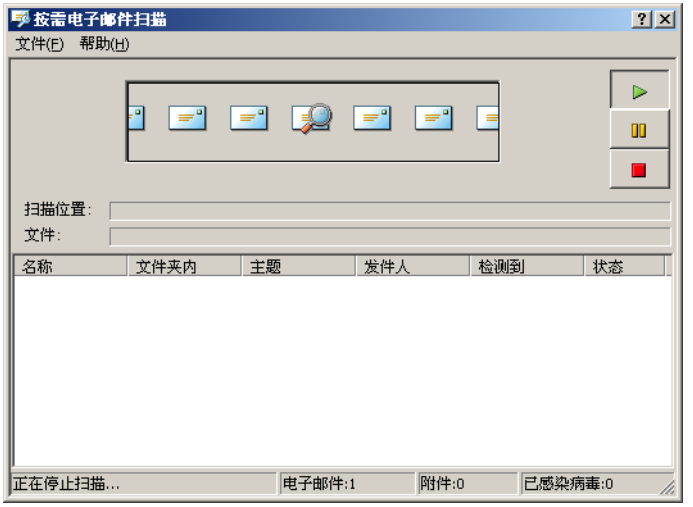

图 5-19. 按需电子邮件扫描

3 当按需电子邮件扫描结束后，关闭该对话框。

查看按需电子邮件扫描结果

在扫描过程中，您可以在“**按需电子邮件扫描**”对话框中查看扫描结果，当扫描结束后，您可以从活动日志查看结果。

这部分包含下列主题：

- 查看按需电子邮件活动日志

查看按需电子邮件活动日志

按需电子邮件扫描活动日志显示了关于扫描操作的详细信息。例如，它可以显示扫描程序已检查的附件数量、发现的病毒数量以及采取的响应措施。

1. 在如下位置找到 EMAILONDEMANDLOG.TXT 文件：

   `< 驱动器 >:Winnt\Profiles\All Users\Application Data\Network Associates\VirusScan`

2. 打开活动日志文件。
3. 要关闭活动日志，请选择“**文件**”菜单中的“**退出**”。

病毒警报 6

VirusScan Enterprise 软件可以通过多种方式通知您扫描活动的进程和结果。例如，当扫描操作结束之后，您可以在“活动日志”中查看扫描结果。此外，您也可以在 VirusScan Enterprise 控制台中查看所有扫描的结果。然而，上述两种方式都不会在扫描程序在计算机中检测到病毒时立即通知您。尽管控制台也能够实时显示扫描活动，但您不可能总是守在屏幕前观看。警报管理器是集成在 VirusScan Enterprise 软件和其他 Network Associates 客户端 / 服务器安全和管理解决方案中的一个独立组件，它可以在检测到病毒时立即通知您。

警报管理器总是实时处理您的防病毒软件生成的警报和事件。通常情况下，警报管理器位于中央服务器中，负责监听网络客户端或服务器防病毒软件发来的警报。客户端软件可以是工作站，也可以是服务器应用程序。警报管理器允许您为警报配置两方面内容：

- 警报发送目标和发送方式。
- 警报消息内容。

详细信息，请参阅 《警报管理器产品指南》。

这部分包含下列主题：

- 配置警报管理器
- 配置收件人和接收方式
- 自定义警报消息

配置警报管理器

使用“警报属性”对话框中的选项，您可以确定当扫描程序检测到病毒之后何时以及如何通知您。

要打开“警报属性”对话框：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

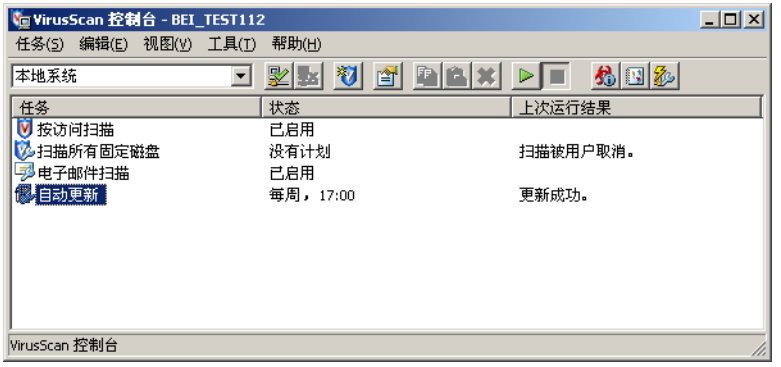

图 6-1. VirusScan 控制台

2 从“工具”菜单中选择“警报”。

屏幕上将出现 “**警报属性**”对话框。

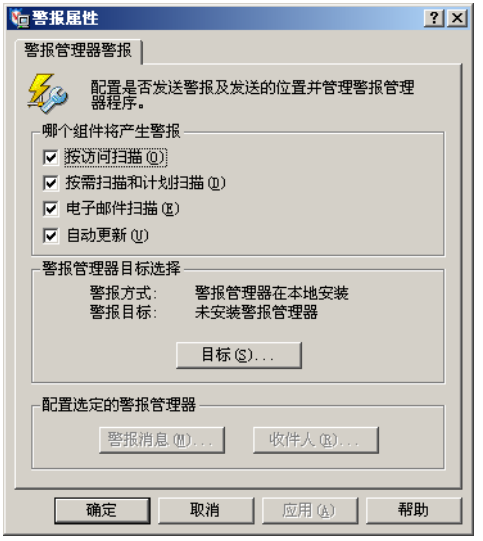

图 6-2. 警报属性

3 在 “**哪个组件将产生报警**”下，选择您希望哪些组件与警报管理器通讯。请选择以下选项的任意组合：

- **按访问扫描**。该选项为默认选项。
- **按需扫描和计划扫描**。该选项为默认选项。
- **电子邮件扫描**。该选项为默认选项。
- **自动更新**。该选项为默认选项。

4 在“警报管理器目标选择”下，单击“目标”打开“警报管理器客户端程序配置”对话框。

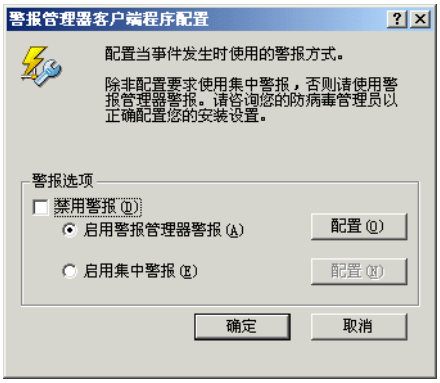

图 6-3. 警报管理器客户端程序配置

您可以禁用或启用警报功能、确定事件发生时采用哪种警报方式以及指定哪些服务器要接收警报。

a 在“警报选项”下，根据您的需要指定警报方式：

- **禁用警报**。事件发生时不发送警报。
- **启用警报管理器警报**。该选项为默认选项，表示激活警报管理器警报方式。

  配置。如果选择了“**启用警报管理器警报**”，请单击“**配置**”打开“**选择警报管理器服务器**”对话框。

图 6-4. 选择警报管理器服务器

在“**警报目标**”下，输入负责接收警报的警报管理器服务器的位置，或者单击“**浏览**”查找位置。

单击“**确定**”保存更改并返回到“**警报管理器客户端程序配置**”对话框。

- **启用集中警报**。激活集中警报方式。集中警报是常规警报管理器警报的另一种警报方式。详细信息，请参阅第 162 页的“使用集中警报”。

  注释
  考虑到共享文件夹的安全问题， McAfee Security 建议您不要使用集中警报功能。

  配置。如果选择了“**启用集中警报**”，请单击“**配置**”打开“**集中警报配置**”对话框。

图 6-5. 集中警报配置

在“**警报目标**”下，输入集中警报共享目录的位置，或者单击“**浏览**”查找位置。

单击“**确定**”保存更改并返回到“**警报管理器客户端程序配置**”对话框。

b 单击“**确定**”保存更改并返回到“**警报属性**”对话框。

5 在“**配置选定的警报管理器**”下：

a 单击“**警报消息**”以配置“**警报管理器消息**”。详细说明，请参阅第 163 页的“自定义警报消息”。

注释
如果尚未安装警报管理器，“**警报消息**”按钮将被禁用。

b 单击“**收件人**”以配置“**警报管理器属性**”。详细说明，请参阅第 142 页的“配置收件人和接收方式”。

注释
如果尚未安装警报管理器，“**收件人**”按钮将被禁用。

c 单击“警报消息”以配置“警报管理器消息”。详细说明，请参阅第 163 页的“自定义警报消息”。

注释
如果尚未安装警报管理器，“警报消息”按钮将被禁用。

d 配置完“警报管理器属性”和“警报管理器消息”之后，单击“确定”关闭“警报属性”对话框。

配置收件人和接收方式

在“警报属性”对话框中，单击“收件人”打开“警报管理器属性”对话框。

使用“警报管理器属性”对话框，您可以为警报管理器发出的警报消息配置接收者以及接收者接收警报消息的方式。接收者既可以是电子邮件地址，也可以是网络中的计算机。接收者可以通过电子邮件或网络弹出式消息来接收警报通知。

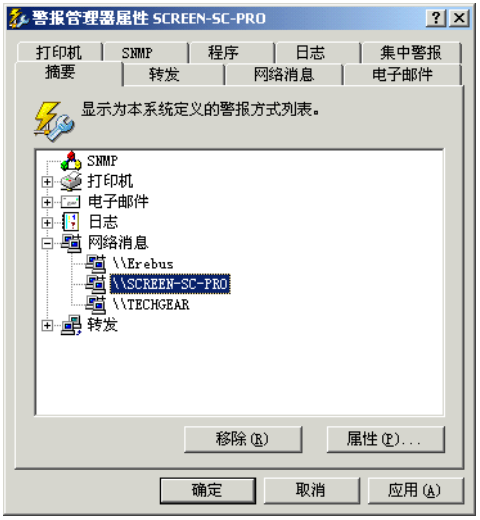

图 6-6. 警报管理器属性

要为特定的警报方式配置接收者：

1 单击给定的警报方式所对应的选项卡，例如“日志”。

2 配置要使用这种方式接收警报通知的接收者。

3 单击其他选项卡，以根据需要为其他任何警报方式配置接收者。

4 完成之后，请单击“确定”保存您的配置并关闭“警报管理器属性”对话框。

要详细了解如何配置特定的警报方式以及警报管理器通过这些方式向哪些接收者发送警报消息，请参阅 《产品指南》的下列部分。

- 第 145 页的 “查看摘要页”
- 第 145 页的 “将警报消息转发给其他计算机”
- 第 148 页的 “以网络消息的形式发送警报”
- 第 150 页的 “将警报消息发送到电子邮件地址”
- 第 154 页的 “将警报消息发送到打印机”
- 第 155 页的 “通过 SNMP 发送警报消息”
- 第 156 页的 “将程序作为警报启动”
- 第 158 页的 “在计算机的事件日志中记录警报通知”
- 第 160 页的“向终端服务器发送网络消息”。只有当安装了警报管理器的计算机正在运行终端服务时，这种方法才可用。
- 第 162 页的 “使用集中警报”

关于添加警报方法的概述

您可以使用“**警报管理器属性**”对话框中的各个选项卡来配置不同的警报方式。当配置每种新方式时，您可以：

- 发送测试消息
- 为接收者设置警报优先级

发送测试消息

当使用“**警报管理器属性**”对话框中的选项卡添加新的警报通知接收者（例如网络计算机或电子邮件地址）时，您可以测试目标地址是否能够收到消息。要在配置某种方式时向选定的目标发送一条测试消息，请单击“**测试**”按钮。

如果所有配置都正确，这条消息会出现在所配置的目标位置。

注释

电子邮件警报可能需要花费一段时间才能到达目标位置，这取决于您的 SMTP 服务器和接收方的电子邮件服务器。

测试消息没有到达目标

如果目标位置收不到这条消息，请查看列表并根据实际情况确认：

- 已经启用实施所选警报方式所需的通讯服务，例如电子邮件或 SNMP。
- 发送或接收这条消息所需的任何设备 （例如调制解调器或寻呼机）存在而且正常运行。

- 为响应检测到的病毒而需要运行的所有程序都位于指定的路径中，而且安装正确。
- 任何目标打印机或计算机都在网络中存在。
- 网络正常运行。
- 您提供的配置信息正确而且完整。某些属性页包括二级页面。例如，“**电子邮件**”页可以链接到“邮件设置”页。确保查看了这些二级页面的信息。
- 如果安装警报管理器时使用了帐户和密码，请确保指定的帐户具有足够权限，可以执行您需要的操作。

为接收者设置警报优先级

您可以为添加到警报管理器配置中的每个接收者指定优先级。警报管理器只向指定的接收者（例如电子邮件地址）发送同级或优先级更高的警报通知。

这对于过滤警报通知而言非常有用。例如，使用“**警报管理器属性**”对话框中的“**日志**”选项卡，您可以在计算机的事件日志中记录各种优先级的警报消息（请参阅第 158 页的“在计算机的事件日志中记录警报通知”）。当然，您也可能希望警报管理器只通过电子邮件向网络管理员的寻呼机发送严重的警报通知。为此，请为日志和电子邮件接收者分别设置优先级阀值。

要为特定的接收者设置警报优先级：

1. 在某种警报方式的“**属性**”对话框中单击“**优先级**”按钮。请参阅第 150 页的图 6-13中的示例。

图 6-7. 优先级

2. 在“**优先级**”对话框中，向右或向左拖动滑块以设置优先级。

   向右拖动表示向接收者发送数量较少、但优先级较高的警报消息。向左拖动表示向接收者发送数量较多、但优先级较低的警报消息。

3. 单击“**确定**”保存优先级设置。

注释

在“**优先级**”对话框中，您可以为特定的接收者（例如网络中的计算机或者某个电子邮件地址）指定优先级，但不能在此设置个别警报消息的优先级。要了解如何为个别警报消息设置优先级，请参阅第 163 页的“自定义警报消息”。

查看摘要页

“警报管理器属性”对话框中的“摘要”选项卡上列出了要接收警报管理器警报通知的那些接收者。系统会按警报方式将接收者分组。

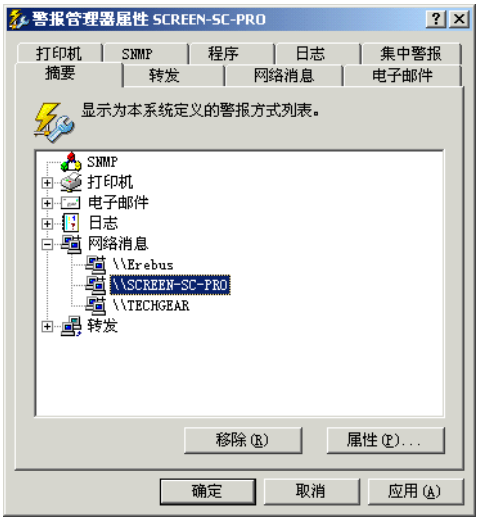

图 6-8. 警报管理器属性 - “摘要”选项卡

单击所列出的每种警报方式旁边的⊞可以显示作为接收方的计算机、打印机或电子邮件地址。要删除警报通知接收者，请选择它，然后单击“移除”。要为列出的接收者更改配置选项，请选择该接收者，然后单击“属性”打开这种警报方式的“属性”对话框。

安装警报管理器时，默认配置是向安装了警报管理器的计算机发送弹出式网络消息，并将警报通知记录在这台计算机的事件日志中。因此，如果尚未为警报管理器警报通知配置任何接收者，“摘要”选项卡将只显示这两种方式。警报管理器会为这两种默认方式设置优先级，以便发送除最低优先级（“信息”）以外的各种优先级的警报通知。关于优先级的详细信息，请参阅第 144 页的“为接收者设置警报优先级”。

以下几部分将介绍每种方式的可用选项。

将警报消息转发给其他计算机

警报管理器可以将从 McAfee 防病毒客户端或服务器产品收到的警报消息转发给网络中安装有警报管理器的其他计算机。通常情况下，如果希望将消息转发给另一台警报管理器服务器来扩大分发范围，您需要执行这一操作。

注释

警报管理器 4.7 只能在运行同一版本的警报管理器的服务器之间相互转发警报通知。如果服务器运行早期版本的警报管理器，则它们之间不能相互转发警报通知。

本部分包括下列主题：

- 在大型公司中转发警报。
- 在小型公司中转发警报。
- 配置警报转发选项。

在大型公司中转发警报

如果公司规模很大，您可以使用转发功能将警报通知发送到中央通知系统或 MIS（“管理信息系统”）部，以便跟踪病毒统计信息和问题区域。此外，大型公司通常会跨地域存在，分支机构可能会分布在若干个不同的国家或地区。在这种情况下，您可能希望在本地服务器上安装一个警报管理器来处理本地子网络中的警报。之后，您可以将本地警报管理器服务器配置为将优先级较高的警报通知转发给网络中其他位置的服务器，以便于将来分发。

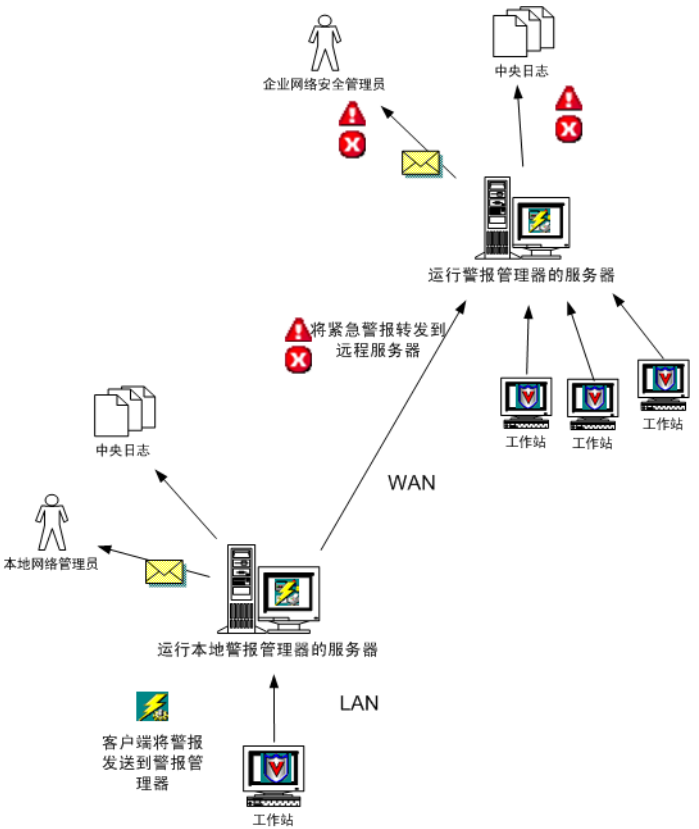

图 6-9. 将警报转发给另一个警报管理器

为此，请将本地的警报管理器配置为将警报转发给安装有第二个警报管理器的计算机。之后，您需要将第二个警报管理器配置为根据需要分发警报通知。有关说明，请参阅第 147 页的 “配置警报转发选项”。

在小型公司中转发警报

在规模较小的公司中，转发功能同样非常有用。假设您希望通过电子邮件将优先级较高的所有警报通知发送给特定的寻呼机，但网络中只有一台服务器可以直接连接到 Internet。

要解决这一问题：

1 在每台警报管理器服务器上配置警报管理器，以便将优先级较高的警报消息转发给安装有调制解调器的计算机。

2 然后配置这些计算机上的警报管理器，以便将优先级较高的消息发送给目标寻呼机的电子邮件地址。

配置警报转发选项

要配置转发选项：

1 单击 “**警报管理器属性**”对话框中的 “**转发**”选项卡。

“**转发**”页将显示您选择要接收转发消息的所有计算机列表。如果尚未选择目标计算机，该列表将为空。

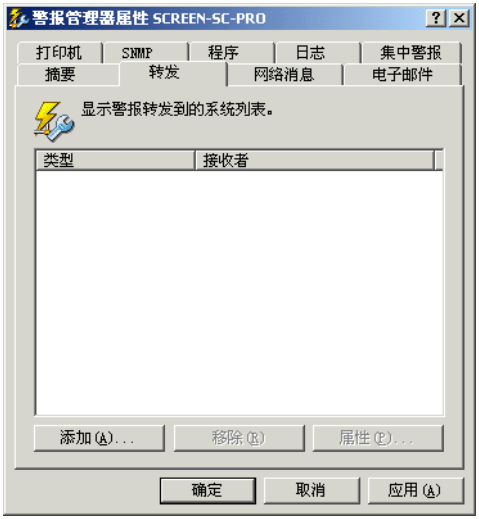

图 6-10. 警报管理器属性 - “转发”选项卡

2 要更新这个列表，请执行下列任一操作：

- 要添加计算机，请单击“**添加**”打开“**转发**”对话框，然后在文本框中输入要接收转发消息的计算机名称。您可以按通用命名约定 (UNC) 格式输入计算机的名称，也可以单击“**浏览**”在网络中查找计算机。
- 要删除列出的计算机，请选择列出的某个目标计算机，然后单击“**移除**”。
- 要更改配置选项，请选择列出的某个目标计算机，然后单击“**属性**”。警报管理器将打开“**转发**”对话框。输入要从警报管理器接收转发消息的计算机名称，或者单击“**浏览**”在网络中查找计算机。

图 6-11. 转发

3 单击“**优先级**”指定目标计算机要接收哪种警报消息。请参阅第 144 页的“为接收者设置警报优先级”。

4 单击“**测试**”向目标计算机发送一条测试消息。请参阅第 143 页的“发送测试消息”。

5 单击“**确定**”返回到“**警报管理器属性**”对话框。

以网络消息的形式发送警报

警报管理器可以将警报消息发送到其他计算机中。接收方计算机的屏幕上将显示一个标准的弹出式消息框，并要求接收者确认。

接收者的计算机无需安装警报管理器。然而，您可能需要针对接收方计算机的操作系统安装适当的客户端通讯软件。这个通讯软件通常预装在较新版本的 Windows 操作系统（例如 Windows NT、Windows 2000 和 Windows XP）中。默认情况下，这项服务总是在运行中。

要配置警报管理器以便将警报通知作为网络消息发送：

1 打开 “**警报管理器属性**”对话框。

2 单击 “**网络消息**”选项卡。“**网络消息**”页中将显示被配置为接收网络消息的计算机列表。如果尚未选择接收方计算机，该列表将为空。

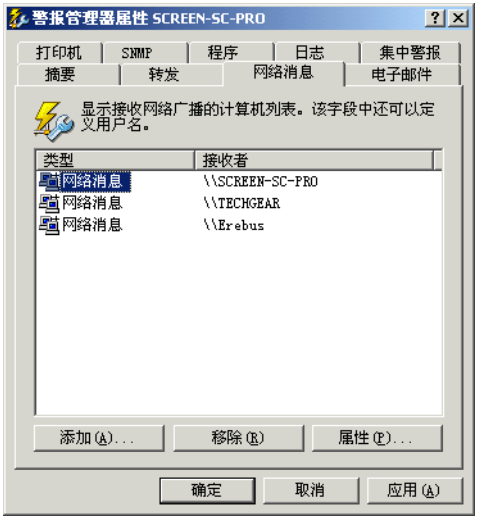

图 6-12. 警报管理器属性 - “网络消息”选项卡

3 要更新这个列表，请执行下列任一操作：

- 要添加计算机，请单击 “**添加**”打开 “**网络消息**”对话框。您可以通过两种方式指定接收方计算机。以 UNC 格式直接在 “**计算机：**”文本框中输入计算机的名称，或者选择 “**浏览**”查找网络中的计算机。
- 要删除列出的某个计算机，请选择列出的某个接收者名称，然后单击 “**移除**”。
- 要更改配置选项，请选择列出的某个接收者名称，然后单击 “**属性**”。警报管理器将打开 “**网络消息**”对话框。根据需要更改 “**计算机：**”文本框中的信息。

图 6-13. 网络消息

4 单击“**优先级**”指定接收者要接收的警报消息类型。请参阅第 144 页的“为接收者设置警报优先级”。

5 单击“**测试**”向接收者发送一条测试消息。请参阅第 143 页的“发送测试消息”。

6 单击“**确定**”返回到“**警报管理器属性**”对话框。

将警报消息发送到电子邮件地址

警报管理器可通过简单邮件传输协议 (SMTP) 将警报消息发送到接收者的电子邮件地址。警报消息将显示在接收者的邮箱中。如果消息非常紧急，您可以用其他方法（例如弹出式网络消息）作为电子邮件消息的补充，以确保接收者及时看到警报并采取适当措施。

注释
电子邮件警报可能需要花费一段时间才能到达目标位置，这取决于您的 SMTP 服务器和接收方的电子邮件服务器。

要将警报管理器配置为以电子邮件的形式发送警报通知：

1 打开“**警报管理器属性**”对话框。

2 单击“**电子邮件**”选项卡。

“**电子邮件**”页将显示您选择接收警报消息的电子邮件地址列表。如果尚未选择电子邮件地址，该列表将为空。

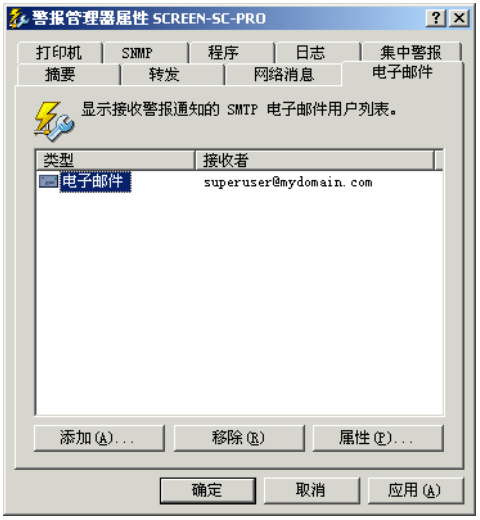

图 6-14. 警报管理器属性 - “电子邮件”选项卡

3 要更新这个列表，请执行下列任一操作：

- 要将一个电子邮件地址添加到列表中，请单击 “**添加**”打开 “**电子邮件**”对话框。在“**地址**”文本框中输入警报通知接收者的电子邮件地址，在“**主题**”文本框中输入主题，然后在 “**发件人**”文本框中输入您的电子邮件地址。请使用标准的 Internet 地址格式 <用户名>@<域>（例如 `administrator_1@mail.com`）。

  为了截短较长的消息（例如包含长文件名和路径名的消息），系统会在地址后面附加一个星号 (*)，例如：`administrator_1@mail.com*`。详细信息，请参阅第 153 页的 “强制截短发送给特定电子邮件地址的消息”。

- 要删除列出的地址，请选择一个列出的电子邮件地址，然后单击“**移除**”。

- 要更改配置选项，请选择一个列出的电子邮件地址，然后单击“**属性**”。警报管理器将打开 “**电子邮件**”对话框。您可以根据需要更改文本框中的信息。

图 6-15. 电子邮件

4 单击“**邮件设置**”指定用来通过 SMTP 发送 Internet 邮件的网络服务器。

注释

您必须单击“**邮件设置**”并指定一个 SMTP 服务器才能发送电子邮件警报通知。请不要跳过这一步。此外，首次配置 SMTP 邮件设置之后，只有当 SMTP 邮件服务器信息发生变化时，才需要重新进行配置。

图 6-16. SMTP 邮件设置

a 在屏幕上出现的对话框中，输入邮件“**服务器**”。这个服务器名称应按 Internet 协议 (IP) 地址、本地域名服务器能够识别的名称或者通用命名约定 (UNC) 的格式输入。

b 如果 SMTP 服务器要求，还需要键入在邮件服务器上使用的“**登录**”名称。

注释

只有当您的 SMTP 邮件服务器被配置为使用登录名时，才应在“**登录**”字段中输入登录名。请检查您的 SMTP 配置以确定是否需要这样做。如果您在邮件服务器不要求的情况下输入了一个登录名，则会导致电子邮件警报出错。

c 单击“**确定**”返回到“**电子邮件**”对话框。

5 单击“**优先级**”指定接收方计算机要接收的警报消息类型。请参阅第 144 页的“为接收者设置警报优先级”。

6 单击“**测试**”向接收方计算机发送一条测试消息。请参阅第 143 页的“发送测试消息”。

7 如果测试消息发送成功，请单击“**确定**”返回到“**警报管理器属性**”对话框。

强制截短发送给特定电子邮件地址的消息

警报通知消息有时会很长，当消息中的 `%FILENAME%` 系统变量被含有冗长路径信息的文件名替代时，情况尤其如此。包含长文件名的复杂消息容易造成混乱，也不便于使用。例如，将电子邮件发送到寻呼机时，某些寻呼机服务会强制将长消息截短，这样就有可能删除邮件中的重要信息。另一方面，如果非常长的消息实际传送到了寻呼机，接收者也必须滚动浏览文件名中的路径信息才能阅读警报中的关键信息。

您可以使用两个选项来控制电子邮件警报通知中的长消息：

- 在电子邮件地址后面附加一个星号 (*)，例如 `administrator_1@mail.com*`。警报管理器会根据当前系统的 SMTP 消息长度设置截短发送到带有星号的电子邮件地址的警报。默认的 SMTP 长度为 240 个字符。

  当警报管理器通过电子邮件向寻呼机发送警报时，这一设置非常有用。某些寻呼机服务具有短消息长度限制，例如 200 个字符。当准备通过电子邮件地址向寻呼机发送消息时，如果在地址后面附加一个星号 (*)，您（而非寻呼服务公司）就可以控制是否截短这条消息。

- 您也可以在“**警报管理器消息**”对话框中编辑消息文本，以确保重要的消息内容尽保留在被截短之后的消息中。为此，您可以缩写消息的某些部分，或者将重要信息移到消息的开头，还可以将长文件名放在消息的末尾。

将警报消息发送到打印机

警报管理器可以向打印机发送警报消息，以便打印出硬拷贝的消息。要将警报管理器配置为将警报通知发送到打印队列：

1 打开 “**警报管理器属性**”对话框。

2 单击 “**打印机**”选项卡。

“**打印机**”页将显示您选择要接收警报消息的所有打印机队列列表。如果尚未选择打印机队列，该列表将为空。

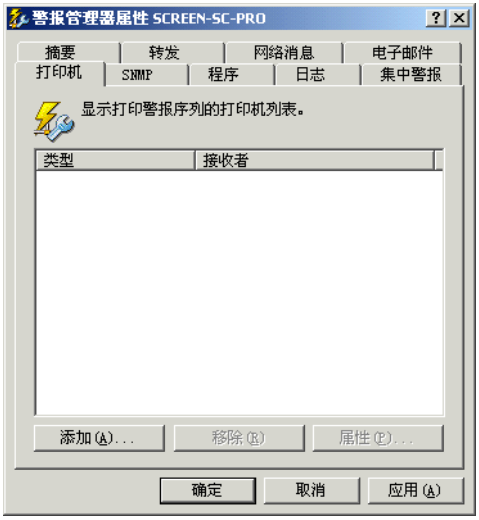

图 6-17. 警报管理器属性 - “打印机”选项卡

3 要更新这个列表，请执行下列任一操作：

- 要向该列表添加打印队列，请单击 “**添加**”打开 “**打印机**”对话框，然后输入要接收消息的打印队列名称。您可以输入打印队列的名称，也可以单击 “**浏览**”查找网络中的打印机。
- 要删除列出的打印队列，请选择一个列出的打印机，然后单击 “**移除**”。
- 要更改配置选项，请选择一个列出的打印机，然后单击 “**属性**”。警报管理器将打开 “**打印机**”对话框。您可以根据需要更改 “**打印机**”文本框中的信息。

图 6-18. 打印机

4 单击“**优先级**”指定接收方打印机要接收的警报通知类型。请参阅第 144 页的“为接收者设置警报优先级”。

5 单击“**测试**”向接收方打印机发送一条测试消息。请参阅第 143 页的“发送测试消息”。

6 单击“**确定**”返回到“**警报管理器属性**”对话框。

通过 SNMP 发送警报消息

警报管理器可以通过简单网络管理协议 (SNMP) 向其他计算机发送警报消息。要使用该选项，您必须在计算机上安装并激活 Microsoft SNMP 服务。详细说明，请参阅操作系统文档。要查看客户端防病毒软件发送的警报消息，还必须使用 SNMP 查看器正确配置 SNMP 管理系统。要安装并配置 SNMP 管理系统，请参阅 SNMP 管理产品的文档。

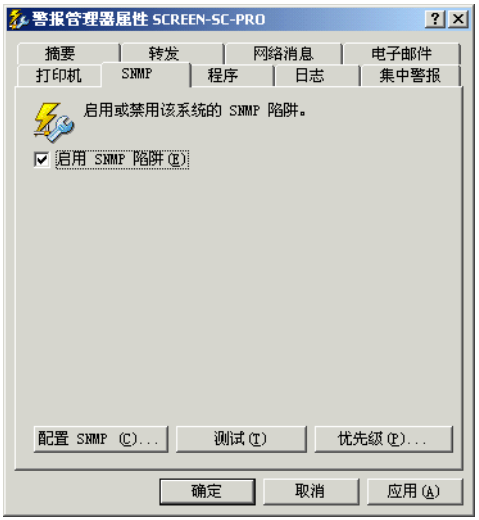

图 6-19. 启用 SNMP 警报

要配置扫描程序以便通过 SNMP 发送警报消息：

1 打开 “**警报管理器属性**”对话框。

2 单击 “**SNMP**”选项卡。

3 选择 “**启用 SNMP 陷阱**”。

4 如果安装了警报管理器的计算机运行的操作系统是 Windows NT 4，请单击“**配置 SNMP**”以显示 Windows “**网络**”对话框，并配置 Microsoft SNMP 服务。详细信息，请参阅您的操作系统文档。

5 单击 “**优先级**”指定接收方计算机要接收的警报消息类型。请参阅第 144 页的“为接收者设置警报优先级”。

6 单击“**测试**”通过 SNMP 向接收方计算机发送一条测试消息。请参阅第 143 页的“发送测试消息”。

7 单击 “**确定**”保存更改并返回到 “**警报管理器属性**”对话框。

将程序作为警报启动

每当收到表明检测到了病毒的警报时，警报管理器会自动启动计算机或网络中的任一个可执行程序。默认情况下，警报管理器会运行您的警报管理器安装文件夹中的 VIRNOTFY.EXE。在安装了警报管理器的那台计算机的屏幕上，VIRNOTFY.EXE 会在一个滚动对话框中显示已感染病毒的文件名称。

注释

警报管理器只在收到关于病毒的特定警报时才启动一个程序。警报消息中必须包含系统变量 %VIRUSNAME% 和 %FILENAME%。请参阅第 166 页的 “使用警报管理器系统变量”。如果警报中没有包含这些字段，则无论为 “程序” 这种通知方式设置的优先级如何，警报管理器将不会启动任何程序。关于优先级的详细信息，请参阅第 144 页的 “为接收者设置警报优先级”。

要将警报管理器配置为在发现病毒时执行某个程序：

1 打开 “**警报管理器属性**” 对话框。

2 单击 “**程序**” 选项卡打开 “**程序**” 页。

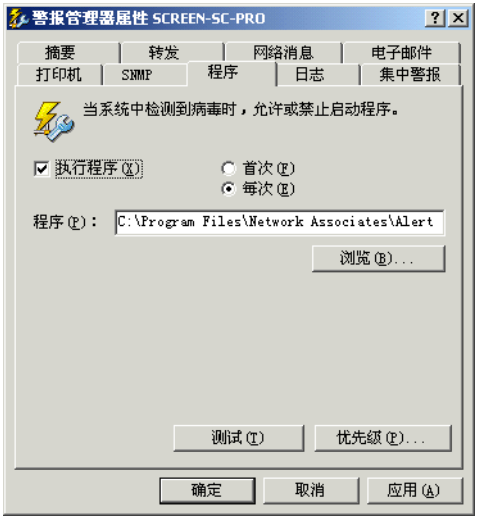

图 6-20. 警报管理器属性 - “程序” 选项卡

3 选择 “**执行程序**”。

4 输入要在防病毒软件发现病毒时运行的可执行程序的名称和路径，或者单击 “**浏览**” 在计算机或网络中找到这个程序文件。

5 选择以下操作之一：

- 如果希望只在防病毒软件首次发现某个特定病毒时启动该程序，请单击 “**首次**”。
- 要在扫描程序每次发现病毒时都启动该程序，请单击 “**每次**”。

注释

如果选择了“**首次**”，则当扫描程序第一次发现特定的病毒（例如病毒 1）时，您指定的程序就会立即启动。如果在同一个文件夹中多次发现病毒 1，扫描程序也不会再次启动该程序。然而，如果扫描程序在发现病毒 1 之后又遇到了其他病毒（病毒 2），随后又检测到了病毒 1，则在每次检测到病毒时都会启动这个程序。在本例中，该程序会连续启动三次。多次启动同一个程序可能会导致服务器内存不足。

6 单击“**优先级**”指定接收方计算机要接收的警报消息类型。请参阅第 144 页的“为接收者设置警报优先级”。

请注意，除非警报中包含关于病毒的特定消息，否则“程序”这种通知方法不会运行任何程序。也就是说，警报中必须包含系统变量 `%VIRUSNAME%` 和 `%FILENAME%`。所有其他警报都将被忽略，而不论其优先级如何。

7 单击“**测试**”向接收方计算机发送一条测试消息。请参阅第 143 页的“发送测试消息”。

在计算机的事件日志中记录警报通知

警报管理器可以将警报消息记录到本地计算机或网络中其他计算机的事件日志中。

要配置日志选项：

1 打开“**警报管理器属性**”对话框。

2 单击“**日志**”选项卡。

“**日志**”页显示了您选择要接收并在日志中记录警报消息的所有计算机列表。如果尚未选择接收方计算机，该列表将为空。

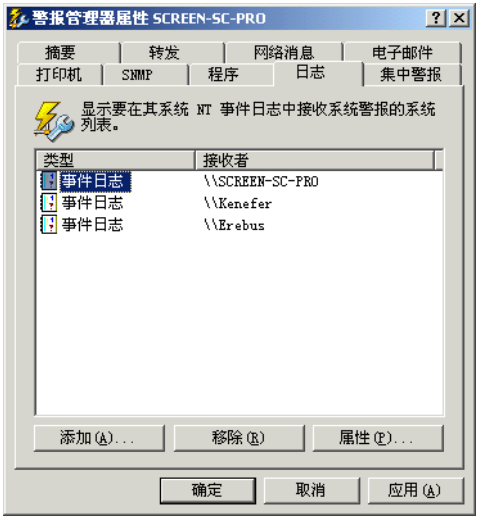

图 6-21. 警报管理器属性 - “日志”选项卡

3 要更新这个列表，请执行下列任一操作：

- 要添加计算机，请单击“**添加**”打开“**日志**”对话框，然后在文本框中输入要接收转发消息的计算机名称。您可以按通用命名约定 (UNC) 格式输入计算机的名称，也可以单击“**浏览**”在网络中查找计算机。
- 要删除列出的计算机，请单击列表中的某个计算机，然后单击“**移除**”按钮。
- 要更改配置选项，请选择列出的某个接收方计算机，然后单击“**属性**”。警报管理器将打开“**日志**”对话框。输入要接收并记录警报管理器转发消息的计算机名称。单击“**浏览**”查找目标计算机。

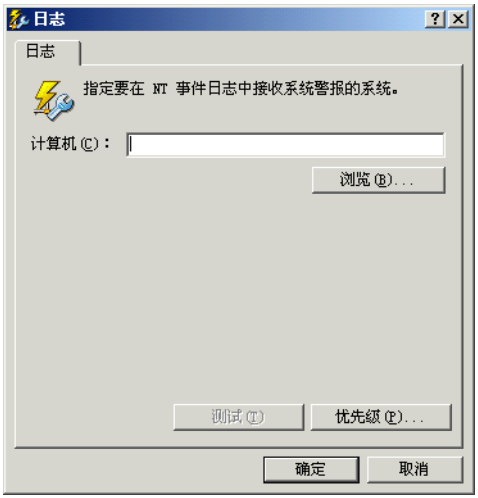

图 6-22. 日志

4 单击 **“优先级”** 指定接收方计算机要接收的警报消息类型。请参阅第 144 页的“为接收者设置警报优先级”。

5 单击 **“测试”** 向接收方计算机发送一条测试消息。请参阅第 143 页的“发送测试消息”。

6 单击 **“确定”** 返回到 **“警报管理器属性”** 对话框。

向终端服务器发送网络消息

警报管理器可以向终端服务器发送警报消息。用户会收到他们的会话产生的弹出式网络消息警报。

如果安装了警报管理器的计算机是终端服务器，**“警报管理器属性”** 对话框将只显示 **“终端服务器”** 选项卡。

要将警报管理器配置为向终端服务器发送消息：

1 打开 **“警报管理器属性”** 对话框。

2 单击 **“终端服务器”** 选项卡。

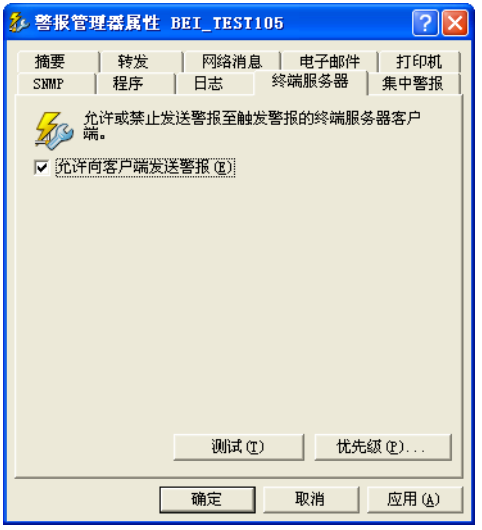

图 6-23. 警报管理器属性 - “终端服务器”选项卡

3 要启用终端服务器警报，请选择 **“允许向客户端发送报警”**。

4 单击 **“测试”**向接收方计算机发送一条测试消息。屏幕上将显示 **“选择客户端以测试消息”**对话框，其中列出了该计算机的当前终端服务器用户会话。

图 6-24. 向终端服务器用户发送一条测试消息

5 从列表中选择一个用户，然后单击 **“确定”**向这名用户发送一条测试消息并返回到 **“警报管理器属性”**对话框。

6 单击**“优先级”**指定终端服务器用户要接收的警报消息类型。请参阅第 144 页的“为接收者设置警报优先级”。

7 单击 **“确定”**保存终端服务器设置并返回到 **“警报管理器属性”**对话框。

使用集中警报

集中警报是常规警报管理器警报的另一种警报方式。使用集中警报功能，您可以将防病毒软件（例如 VirusScan Enterprise）生成的警报消息保存在服务器上的一个共享文件夹中，然后将警报管理器配置为从这个文件夹读取警报通知。共享文件夹中的内容如果发生变化，警报管理器将按事先配置的警报方式（例如向寻呼机发送电子邮件消息）发送新警报通知。

警告

考虑到共享文件夹的安全问题，McAfee Security 建议您不要使用集中警报功能。相反，您应将客户端防病毒软件配置为使用常规的警报管理器警报通知方式。

要使用集中警报：

1. 配置客户端计算机上的防病毒软件，以便将警报消息发送到相应的警报文件夹中。请参阅您的防病毒软件文档来了解如何进行配置。

   注释

   要允许网络中的其他工作站将消息发送到这个文件夹，您必须为所有用户和计算机赋予对该文件夹文件的扫描、写入、创建和修改权限。详细信息，请参阅您的操作系统文档。

2. 请确保所有用户和计算机都能够读写这个共享的警报文件夹。如果该文件夹所在的计算机运行的操作系统是 Windows NT，则您还应正确配置一个空的会话共享。详细信息，请参阅您的操作系统文档。

3. 配置警报管理器以监控集中警报文件夹的活动。为此：

   a 从“**警报管理器属性**”对话框中选择“**集中警报**”选项卡。

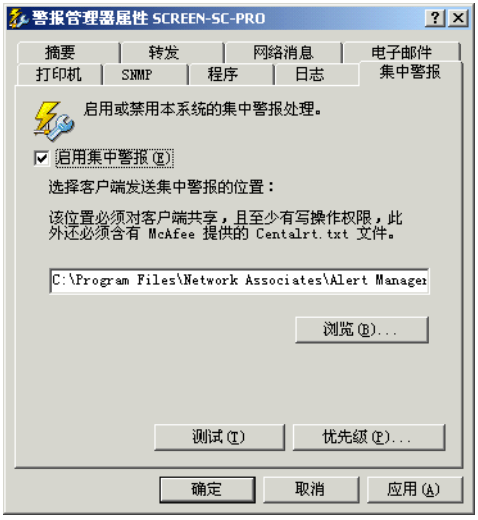

图 6-25. 集中警报属性

b 选择“启用集中警报”。

c 键入警报文件夹的位置，或者单击“浏览”在服务器或网络中查找文件夹。该文件夹必须与客户机上的防病毒软件所用的集中警报文件夹相同（请参阅步骤 1）。警报文件夹的默认位置是：

C:\Program Files\Network Associates\Alert Manager\Queue\。

4 单击“优先级”指定接收方计算机要接收的警报消息类型。请参阅第 144 页的“为接收者设置警报优先级”。

5 单击“测试”向接收方计算机发送一条测试消息。请参阅第 143 页的“发送测试消息”。

6 单击“确定”保存集中警报设置并返回到“警报管理器属性”对话框。

自定义警报消息

警报管理器带有多种警报消息，几乎可以满足在网络中检测到病毒时所遇到的各种情况。警报消息包括预先设置的优先级、用来识别感染病毒文件和系统的系统变量、感染的病毒以及用来快速、全面查看感染情况的其他信息。

为满足您的需要，您可以启用或禁用个别警报消息，也可以更改任何消息的内容及优先级。但由于警报管理器主要针对特殊触发事件激活警报消息，因此当编辑警报消息时，您应尽量保留其基本含义。

使用“警报管理器消息”对话框可以自定义警报消息。请参阅第 138 页的“配置警报管理器”来详细了解如何访问“警报管理器消息”对话框。

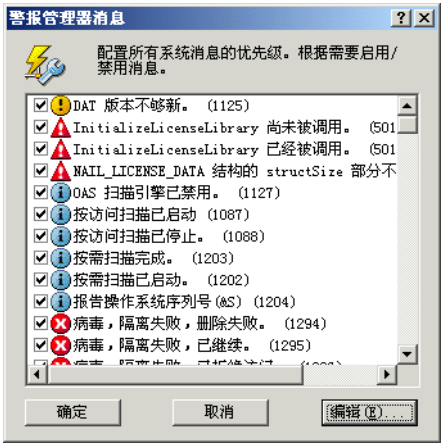

图 6-26. 警报管理器消息

在该对话框中，您可以执行如下操作：

- 启用和禁用警报消息
- 编辑警报消息

启用和禁用警报消息

尽管 VirusScan Enterprise 会在其常规操作的任何方面发生明显改动或者防病毒软件发现病毒时发出警报，但您也许并不希望在这些情况下接收警报消息。使用“**警报管理器消息**”对话框，您可以禁用不希望接收的警报消息。

“**警报管理器消息**”对话框中列出的每个警报的旁边都有一个复选框。如果选定了这个复选框，则表示已启用警报功能。如果未选定，则表示禁用。默认设置为启用可用的所有警报消息。

要启用或禁用警报消息：

1. 根据您要启用还是禁用警报消息，选择或取消选择相应的复选框。
2. 单击“**确定**”保存所做的更改并关闭“**警报管理器消息**”对话框。

编辑警报消息

您可以通过如下两种方式来编辑警报消息：

- 更改警报优先级
- 编辑警报消息文本

更改警报优先级

警报管理器从您的客户端防病毒软件接收的某些警报要求您更及时地响应和处理。根据大多数系统管理员可能会分配的紧急程度，系统为每个警报消息都设置了默认的优先级。您可以重新指定这些优先级，以满足自己的需要。使用这些优先级可以过滤警报管理器向接收者发送的消息，这样接收者就可以首先处理最重要的消息。

要更改分配给警报消息的优先级：

1. 在“**警报管理器消息**”对话框 （请参阅第 163 页的 “自定义警报消息”）中，单击并选择列表中的一条消息。
2. 单击“**编辑**”打开“**编辑警报管理器消息**”对话框。

图 6-27. 编辑警报消息的优先级和文本

3 从“**优先级**”列表中选择一个优先级。您可以为每个警报消息分配“**关键**”、“**主要**”、“**次要**”、“**警告**”或“**信息**”优先级。

“**警报管理器消息**”对话框中列出的每个消息的旁边都有一个图标，用来识别当前分配给这条消息的优先级。每个图标都对应于“**优先级**”下拉列表中的一个选项。这些优先级包括：

关键。表示防病毒软件无法清除、隔离或删除检测到的文件病毒。

主要。或者表示成功地检测到并清除了病毒，或者表示可能导致防病毒软件停止运行的严重错误和问题。例如“已删除感染病毒的文件”、“未安装指定产品的许可”或“内存不足！”。

次要。表示比较不重要的检测消息或状态消息。

警告。表示比“信息”消息更严重的状态消息。这种消息通常和在病毒扫描过程中遇到的非关键问题相关。

信息。表示标准状态消息和通知消息，例如“按访问扫描已启动”或“扫描已完成，未发现病毒。”

重新为某个消息指定了优先级之后，这条消息旁边的图标将发生变化，以显示新的优先级状态。

4 单击“**确定**”。

按优先级过滤消息

要过滤消息，请将您在警报管理器中设置的每种警报方法配置为只接收某个优先级的消息。例如，假设您希望客户端防病毒软件在网络中发现病毒时要求警报管理器呼叫您，但不希望它发送日常事务运行消息。为此，您需要为病毒警报指定“关键”或“主要”优先级，并为日常事务通知消息指定“次要”或“警告”优先级。然后配置警报管理器，以使它只将优先级较高的消息发送到寻呼机的电子邮件地址。

关于为特定接收者应用优先级过滤规则的说明，请参阅第 144 页的“为接收者设置警报优先级”。

编辑警报消息文本

为了帮助您对需要注意的情况做出响应，警报管理器在其消息中包括了足够的信息，以识别问题的来源以及问题环境的相关信息。您可以根据需要编辑消息文本。例如，您可以向警报消息添加注释，以便更详细地描述问题或者列出支持人员的联系信息。

> **注释**
> 尽管可以编辑警报消息文本以表达您自己的想法，但仍应尽量保留主旨，原因在于警报管理器只有在遇到某些具体情况时才发送相应的消息。例如，只有当警报管理器启动了某项任务时才会发送“任务已启动”警报消息。

要编辑警报消息文本：

1. 单击并选择“**警报管理器消息**”对话框中列出的警报消息。
2. 单击“**编辑**”打开“**编辑警报管理器消息**”对话框。
3. 您可以根据需要编辑消息文本。用百分号括起来的文本（例如 %COMPUTERNAME%）表示一个变量，警报管理器会在生成警报消息时用相应文字将其替换。请参阅第 166 页的“使用警报管理器系统变量”。
4. 单击“**确定**”保存更改并返回到“**警报属性**”对话框。

使用警报管理器系统变量

警报管理器 4.7 包含您可以在警报消息文本中使用的系统变量。这些变量指的是系统特性，例如系统日期和时间、文件名或计算机名称。在发送警报通知时，警报管理器会使用特定的值来动态替换这种变量。

例如，“**警报管理器消息**”对话框中列出的主要警报“已成功清除文件感染的病毒 (1025)”默认设置如下：

> 文件 %FILENAME% 感染了 %VIRUSNAME% %VIRUSTYPE%。已使用 %ENGINEVERSION% 版扫描引擎和 %DATVERSION% 版 DAT 成功清除该文件感染的病毒。

当这个警报从防病毒应用程序发往警报管理器时，警报管理器会用实际的值来动态对系统变量赋值，例如将 %FILENAME% 变量赋值为 MYDOCUMENT.DOC。

最常用的系统变量包括：

%DATVERSION%	生成警报的防病毒软件当前使用的DAT文件版本。
%ENGINEVERSION%	防病毒软件当前用来检测病毒或其他问题的防病毒引擎版本。
%FILENAME%	文件的名称，可包括发现已感染病毒的文件名称或者排除在扫描操作之外的文件名称。
%TASKNAME%	处于活动状态的任务（例如 VirusScan Enterprise 的按访问扫描或自动更新任务）名称。警报管理器可以使用这个变量来报告发现病毒的那个任务的名称或者在扫描过程中报告出错的那个任务的名称。
%VIRUSNAME%	感染的病毒名称。
%DATE%	运行警报管理器的那台计算机的系统日期。
%TIME%	运行警报管理器的那台计算机的系统时间。
%COMPUTERNAME%	计算机在网络中的名称。可包括感染病毒的计算机、报告设备驱动程序错误的计算机以及与该程序交互的其他任何计算机。
%SOFTWARENAME%	可执行文件的名称。可包括病毒检测应用程序、报告出错的应用程序或者与该程序交互的其他任何应用程序。
%SOFTWAREVERSION%	从处于活动状态的软件包中取得的版本号。可包括病毒检测应用程序、报告出错的应用程序或者与该程序交互的其他任何应用程序。
%USERNAME%	当前登录到服务器的用户名。例如，它可以通知您是否有人取消了扫描。

警告

如果要在消息文本中包括某些系统变量，但生成警报消息的事件可能不会用到这些变量，那么在编辑这样的消息文本时要当心。要在某个警报中使用系统变量，但这个警报却不使用系统变量字段，则可能会导致无法预料的结果，包括语义晦涩的消息文本甚至系统崩溃。

下面列出了可在警报管理器消息中使用的所有警报管理器系统变量：

%ACCESSPROCESSNAME%
%CLIENTCOMPUTER%
%COMPUTERNAME%
%DATVERSION%
%DOMAIN%
%ENGINESTATUS%
%ENGINEVERSION%
%EVENTNAME%
%FILENAME%
%GMTDAY%
%GMTHOUR%
%GMTMIN%
%GMTMONTH%
%GMTSEC%
%GMTTIME%
%GMTYEAR%
%INFO%
%MAILIDENTIFIERINFO%
%MAILSUBJECTLINE%
%MAILTONAME%
%NOTEID%
%NOTESDBNAME%
%NOTESSERVERNAME%
%LANGUAGECODE%
%LOCALDAY%
%LOCALHOUR%
%LOCALMIN%
%LOCALMONTH%
%LOCALSEC%
%LOCALTIME%
%LOCALYEAR%
%LONGDESCRIPT%
%MAILCCNAME%
%MAILFROMNAME%
%NUMCLEANED%
%NUMDELETED%
%NUMQUARANTINED%
%NUMVIRS%
%OBRULENAME%
%OS%
%PROCESSORSERIA%
%RESOLUTION%
%SCANRETURNCODE%
%SEVERITY%
%SHORTDESCRIPT%
%SOFTWARENAME%
%SOFTWAREVERSION%
%SOURCEIP%
%SOURCEMAC%
%SOURCESEG%
%TARGETCOMPUTERNAME%
%TARGETIP%
%TARGETMAC%
%TASKID%
%TASKNAME%
%TRAPID%
%TSCLIENTID%
%URL%
%USERNAME%
%VIRUSNAME%
%VIRUSTYPE%

更新 7

VirusScan Enterprise 软件根据病毒定义 (DAT) 文件中的信息来识别病毒。如果没有不断更新的文件，本产品软件将无法检测到新病毒变种或者作出有效响应。某些不使用最新 DAT 文件的软件可能会对您的防病毒程序构成威胁。

每个月都会出现 500 多种新病毒。为迎接这一挑战， McAfee Security 每周会发布新的 DAT 文件，并采用最新的研究成果来识别新病毒或病毒变种的特征。自动更新功能可以帮助您轻松地充分利用这项服务。它允许您使用立即更新或计划更新功能同时下载最新的 DAT 文件、扫描引擎和 EXTRA.DAT。

这部分包含下列主题：

- 更新策略
- 系统变量
- 自动更新任务
- 自动更新资料库列表
- 镜像任务
- 回滚 DAT 文件
- 手动更新

更新策略

更新可以通过多种方式完成。您可以以更新任务、手动更新、登录脚本方式进行更新，也可以使用管理工具来计划更新。本文档将介绍如何使用 VirusScan Enterprise 中提供的更新工具及手动更新方式进行更新。其他方法不在本文档讨论之列。

高效的更新策略通常至少要求贵公司的一个客户端或服务器能够从 Network Associates 下载站点获取更新。这样，贵公司的所有其他计算机就可以访问这个客户端或服务器并复制更新文件。最理想的情况是，通过将更新后的文件自动复制到共享位置将网络中传输的数据量降至最低。

高效更新要考虑的主要因素是客户端和站点的数量。也可能会有其他因素影响您的更新方案，例如每个远程站点拥有的系统数量以及远程站点访问 Internet 的方式。但对于任何规模的公司而言，都可以通过共用共享站点并制定更新计划这种基本方式进行更新。

通过更新任务进行更新，您可以：

- 在整个网络范围内将 DAT 文件传输安排在合适的时间进行，并尽可能减少管理员或网络用户的参与。例如，您可以将更新任务错开，或者制定一个计划以便在网络的不同部分分时段或轮流执行 DAT 文件更新。
- 在各个服务器或域控制器之间、广域网的不同区域之间或其他网段之间分担传输管理任务。将更新时产生的通讯流量基本限制在内部还可以防止网络安全轻易遭到破坏。
- 降低不得不等待下载新的 DAT 或升级后的引擎文件的可能性。McAfee 计算机上的通讯流量在定期发布 DAT 文件和推出新版本的产品时会显著增长。避免网络带宽过于繁忙可以保证您在部署新软件时极少中断。

关于更新和使用 McAfee Installation Designer 或 McAfee AutoUpdate Architect 配置和管理更新的详细信息，请参阅 《VirusScan Enterprise 更新实施指南》。

系统变量

当配置自动更新任务、镜像任务和资料库时，您可以使用系统变量来定义路径。常用的系统变量包括：

变量	定义
<COMPUTER_NAME>	计算机在网络中的名称。
<USER_NAME>	当前登录到计算机的用户名。
<DOMAIN_NAME>	域的名称。
<SYSTEM_DRIVE>	系统驱动器的名称。例如： C:
<SYSTEM_ROOT>	根目录的路径。例如： C:\WinNT
<SYSTEM_DIR>	系统目录的路径。例如： C:\WinNT\System32
<TEMP_DIR>	临时目录的路径。例如： C:\Document and Settings\Administrator\Local Settings\Temp
<PROGRAM_FILES_DIR>	Program Files 目录的路径。例如： C:\Program Files
<PROGRAM_FILES_COMMON_DIR>	Common Files 目录的路径：例如： C:\Program Files\Common Files
<SOFTWARE_INSTALLED_DIR>	本软件安装位置的路径。
<PP_VAR_NAME>	McAfee 产品变量名称。例如： %ALLUSERSPROFILE%

自动更新任务

自动更新任务能够执行计划更新或立即更新。您可以更新 DAT 文件、扫描引擎和 EXTRA.DAT 文件。关于下载 HotFix、Service Pack、SuperDAT 软件包或 .CAB 文件的信息，请参阅《VirusScan Enterprise 更新实施指南》。

VirusScan Enterprise 产品带有一个默认的更新任务，这项任务会在每周五下午 5:00 前后一个小时的某个随机时间进行更新。默认的这项更新任务称为“**自动更新**”，您也可以重新命名并配置默认的“**自动更新**”任务。您还可以创建其他更新任务以满足自己的更新需要。

这部分包含下列主题：

- 自动更新任务概述
- 创建自动更新任务
- 配置自动更新任务
- 运行自动更新任务
- 查看活动日志

自动更新任务概述

下图显示了自动更新任务的大致情况：

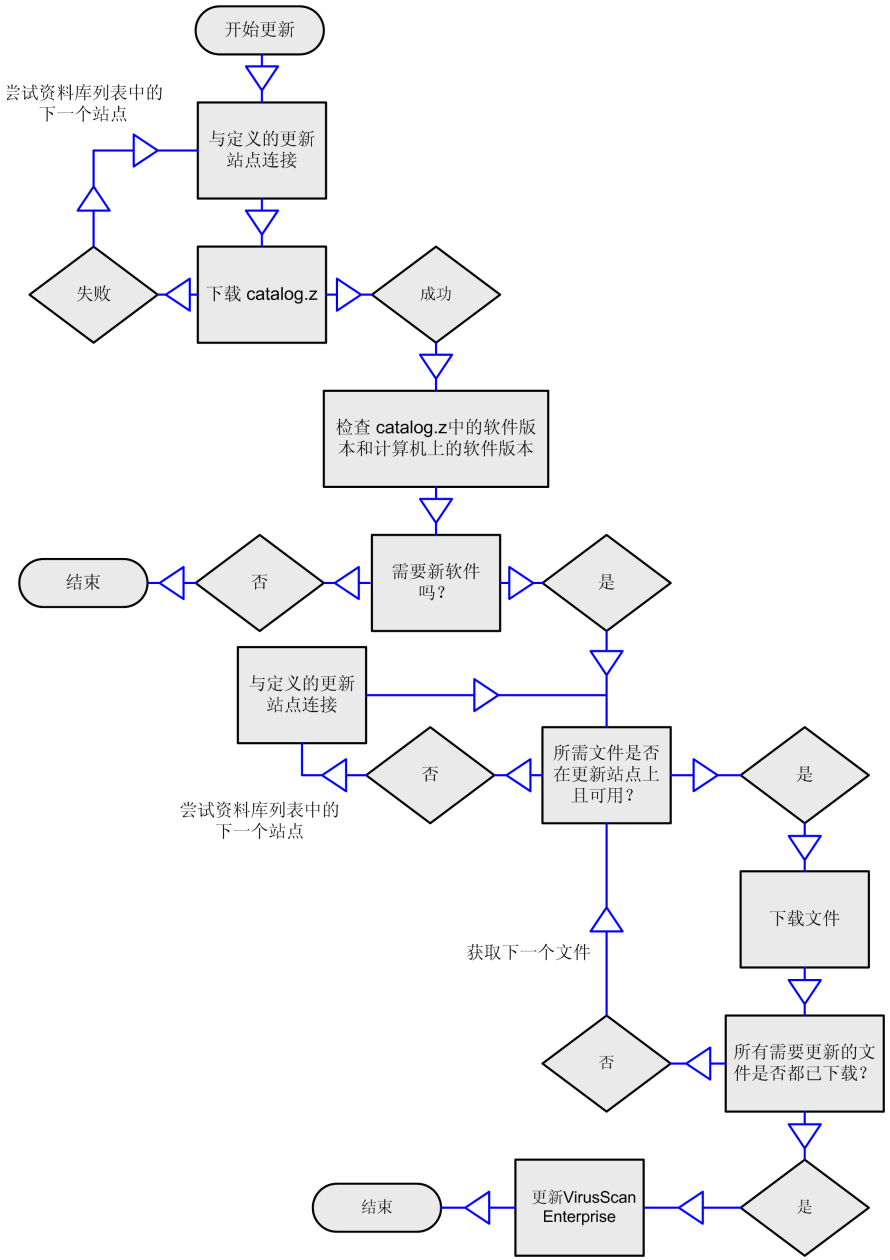

图 7-1. 自动更新任务概述

创建自动更新任务

要创建新的自动更新任务：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一创建新的更新任务：

- 右键单击控制台中的空白区域而无需从任务列表中选择任何项目，然后选择“**新建更新任务**”。
- 选择“**任务**”菜单中的“**新建更新任务**”。

“**VirusScan 控制台**”任务列表中将突出显示一个新的更新任务。

3 接受默认的任务名称或者键入一个新的任务名称，然后按 ENTER 键打开“**自动更新属性**”对话框。要详细了解配置信息，请参阅第 174 页的“配置自动更新任务”。

注释

如果通过 ePolicy Orchestrator 3.0 或更高版本创建了更新任务并启用了任务可见功能，则可以在 VirusScan 控制台中看到这些更新任务。这些 ePolicy Orchestrator 任务是只读的，不能从 VirusScan 控制台中配置。详细信息，请参阅《VirusScan Enterprise 配置指南 - 与 ePolicy Orchestrator 3.0 配合使用》。

配置自动更新任务

您可以根据自己的需要配置和计划自动更新任务。

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一打开“**自动更新属性**”对话框：

- 突出显示控制台任务列表中的任务，然后从“**任务**”菜单中选择“**属性**”。
- 双击任务列表中的任务。
- 右键单击任务列表中的任务，然后选择“**属性**”。
- 突出显示任务列表中的任务，然后单击  。

图 7-2. 自动更新属性 - 新建更新任务

注释
在单击“**计划**”或“**立即更新**”之前，请先配置更新任务。

3 在“**日志文件**”文本框中，接受默认的日志文件名和位置、输入其他日志文件名和位置，或者单击“**浏览**”查找合适的位置。这里支持系统变量。详细信息，请参阅第 171 页的 “系统变量”。

注释
默认情况下，日志信息被写入到位于以下文件夹中的 UPDATELOG.TXT 文件中：

```
< 驱动器 >:Winnt\Profiles\All Users\Application
Data\Network Associates\VirusScan
```

4 在“**运行选项**”下，您可以指定要在“**自动更新**”任务结束后启动的可执行文件。例如，您可以使用这个选项启动一个网络消息实用程序来通知管理员更新操作已成功完成。

- **请输入更新完成后运行的可执行文件**。输入要运行的可执行文件的路径，或者单击“**浏览**”进行查找。
- **仅在成功更新后运行**。只在成功更新之后运行可执行程序。如果更新失败，指定的程序将不会运行。

注释
当前登录的用户必须能够执行您指定的程序文件。如果当前登录的用户无权访问这个程序文件所在的文件夹或者目前没有任何用户登录，该程序也不会运行。

5 单击“**计划**”以计划更新任务。详细信息，请参阅第 199 页的 “计划任务”。

6 单击“**应用**”保存更改。

7 要立即运行更新任务，请单击“**立即更新**”。

8 单击“**确定**”关闭“**自动更新属性**”对话框。

注释
更新任务将使用“自动更新”资料库列表中的配置设置来进行更新。详细信息，请参阅第 179 页的“自动更新资料库列表”。

运行自动更新任务

一旦用所需的更新属性配置了更新任务，您就可以运行这项任务。这部分包含下列主题：

- 运行更新任务
- 在更新任务执行过程中发生的活动

运行更新任务

您可以根据需要立即执行更新，也可以命令它在方便时运行。如果更新任务在执行过程中中断，它会按以下步骤自动恢复：

- **从 HTTP、 UNC、或本地站点更新的任务**。如果由于某种原因在更新过程中中断，更新任务会在下次启动时从中断处继续运行。
- **从 FTP 站点更新的任务**。如果在下载某个文件时中断，则任务不可恢复。但如果在下载多个文件时中断，那么任务会从中断时正在下载的文件之前恢复运行。

要运行更新任务：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一运行更新任务：

- **按计划更新**。如果计划了更新任务，则它可以在无人值守的情况下运行。

  注释
  但计算机必须处于开机状态，更新任务才能运行。如果计算机在任务即将开始运行时处于关机状态，这项任务将在计算机处于开机状态时的下一个计划时间运行，而如果选择了“**计划设置**”中“**计划**”选项卡上的“**运行错过的任务**”选项，这项任务将在计算机启动时开始运行。

- **立即更新**。您可以通过三种方式立即启动更新任务：
  - 用于默认更新任务的“**立即更新**”命令。
  - 用于所有更新任务的“**启动**”命令。
  - 用于所有更新任务的“**立即更新**”命令。

用于默认更新任务的立即更新命令。

您可以使用 “**立即更新**” 命令立即启动默认的更新任务。

> **注释**
> “**立即更新**” 只对在安装本产品时创建的默认更新任务有效。您可以重命名和重新配置默认的更新任务，但如果删除了默认任务，“**立即更新**” 将被禁用。

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。
2. 按照以下方法之一，使用 “**立即更新**” 命令立即进行更新：
   - 在 “**VirusScan 控制台**” 中，选择 “**任务**” 菜单中的 “**立即更新**”。
   - 右键单击系统任务栏中的  ，然后选择 “**立即更新**”。
3. 当这项任务结束之后，单击 “**关闭**” 退出 “**McAfee 自动更新**” 对话框，或者等待该对话框自动关闭。

用于所有更新任务的启动命令

您可以使用 “**VirusScan 控制台**” 中的 “**启动**” 命令来立即启动任何更新任务。

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。
2. 按照以下方法之一，从 “**VirusScan 控制台**” 启动立即更新：
   - 突出显示控制台任务列表中的任务，然后从“**任务**”菜单中选择“**启动**”。
   - 右键单击任务列表中的任务，然后选择 “**启动**”。
   - 突出显示任务列表中的任务，然后单击  。
3. 当这项任务结束之后，单击 “**关闭**” 退出 “**McAfee 自动更新**” 对话框，或者等待该对话框自动关闭。

用于所有更新任务的立即更新命令

您可以使用 “**自动更新属性**” 对话框中的 “**立即更新**” 来立即启动任何更新任务。

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。
2. 打开所选更新任务的 “**自动更新属性**” 对话框。有关说明，请参阅第 174 页的“配置自动更新任务”。
3. 单击 “**自动更新属性**” 对话框中的 “**立即更新**”。
4. 当这项任务结束之后，单击 “**关闭**” 退出 “**McAfee 自动更新**” 对话框，或者等待该对话框自动关闭。

在更新任务执行过程中发生的活动

当运行自动更新任务时，将发生下列活动：

- 连接到资料库列表中的第一个已启用的资料库 （更新站点）。如果这个资料库不存在，则连接下一个资料库，直到连接成功或者到达列表末尾。
- 从资料库下载已加密的 CATALOG.Z 文件。CATALOG.Z 文件包含完成更新所需的重要数据。这些数据用来判断哪些文件和 / 或更新可用。
- 将 CATALOG.Z 中的软件版本与计算机中的版本进行比较。如果存在新的软件更新，则下载这些更新。
- 当更新被登记到资料库中之后，即对该更新进行验证以确定它是否适用于 VirusScan Enterprise 以及这一版本是否比当前版本更高。验证完毕之后，当更新任务下次运行时， VirusScan Enterprise 会下载这个更新。

EXTRA.DAT 文件可以用来在紧急情况下检测新的病毒威胁，直到新病毒被添加到每周病毒定义文件中。每次更新时都会从资料库下载 EXTRA.DAT 文件。这样，如果您修改了 EXTRA.DAT 并将其作为软件包重新登记，所有 VirusScan Enterprise 客户端就可以下载并使用这个更新之后的 EXTRA.DAT 软件包。例如，您可以将 EXTRA.DAT 用作一个改进的检测程序来检测同一种病毒或其他新病毒。VirusScan Enterprise 允许只使用一个 EXTRA.DAT 文件。

> **注释**
>
> 当使用了 EXTRA.DAT 文件之后，您应将其从主资料库中删除并运行一个复制任务，以确保它已从所有分布式资料库站点中移除。这将阻止 VirusScan Enterprise 客户端在更新过程中尝试下载 EXTRA.DAT 文件。
>
> 默认情况下，如果在新病毒定义添加到了每周的 DAT 文件中之后又在 EXTRA.DAT 中发现了这种新病毒，这种病毒将被忽略。

要了解更新进程的图示，请参阅第 173 页的 “自动更新任务概述”。

查看活动日志

更新任务活动日志显示了更新操作的详细信息。例如，它显示了更新后的 DAT 文件和引擎版本号。

要查看活动日志：

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。
2. 使用以下方法之一，打开活动日志文件：
   - 突出显示一项任务，然后选择 “**任务**”菜单中的 “**活动日志**”。
   - 右键单击任务列表中的这项任务，并选择 “**查看日志**”。
3. 要关闭活动日志，请选择 “**文件**”菜单中的 “**退出**”。

自动更新资料库列表

自动更新资料库列表 (SITELIST.XML) 中指定了执行更新任务所需的资料库和配置信息。

例如：

- 资料库信息和位置。
- 资料库顺序首选项。
- 代理设置 （如果需要）。
- 访问每个资料库所需的证书。

  注释
  这些证书都已加密。

操作系统不同，自动更新资料库列表 (SITELIST.XML) 的位置也不同。

例如，对于 Windows NT：

```
C:\Program Files\Network Associates\Common Framework\Data
```

例如，对于 Windows 2000：

```
C:\Documents and Settings\All Users\Application Data\Network
Associates\Common Framework
```

这部分包含下列主题：

- 自动更新资料库
- 配置自动更新资料库列表

自动更新资料库

资料库是指您要从中接收更新的那个位置。

VirusScan Enterprise 软件预先配置有两个资料库：

ftp://ftp.nai.com/CommonUpdater

http://update.nai.com/Products/CommonUpdater

FTP资料库是默认的站点。如果计划使用FTP资料库来执行更新，系统会在VirusScan Enterprise 7.1.0 安装过程结束后自动配置为这样做。

如果正在独占使用 VirusScan Enterprise 7.1.0，或者正在一个混合环境中将 VirusScan Enterprise 7.1.0 与 VirusScan 4.5.1 或 NetShield 4.5 配合使用，则您可以使用其中一个站点下载最新的更新。

您可以重新组织列表中的资料库，也可以创建新的资料库来满足自己的需要。您需要的资料库数量取决于您的更新需要。详细信息，请参阅第 181 页的“编辑自动更新资料库列表”。

配置自动更新资料库列表

您可以在安装之前、安装过程中或安装之后配置自动更新资料库列表(SITELIST.XML)。

本指南也介绍了安装之后的选项。关于安装选项的详细信息，请参阅《VirusScan Enterprise 更新实施指南》。

这部分包含下列主题：

- 导入自动更新资料库列表
- 编辑自动更新资料库列表

导入自动更新资料库列表

要从其他位置导入自动更新资料库列表：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 选择“**工具**”|“**导入自动更新资料库列表**”。

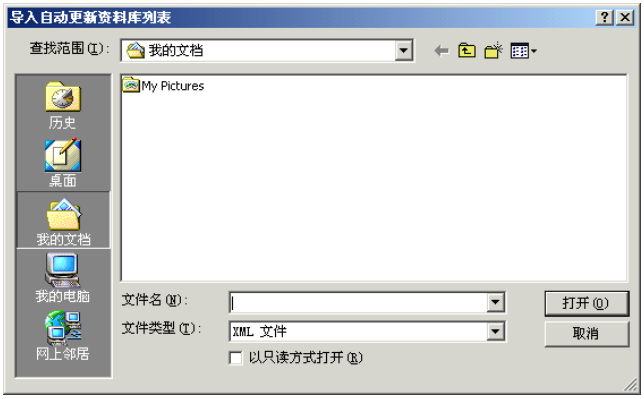

图 7-3. 导入自动更新资料库列表

3 在“**查找范围**”框中，输入 .XML 文件的位置，或者单击 找到这个位置，然后选择一个文件。

4 单击“**打开**”导入自动更新资料库列表。

注释

要导入自定义的自动更新资料库列表、指定作为软件来源的资料库或者使用可以从主资料库中复制的多个更新位置，您必须将 McAfee AutoUpdate Architect ™ 实用程序与 VirusScan Enterprise配合使用。详细信息，请参阅《McAfee AutoUpdate Architect Product Guide》。

编辑自动更新资料库列表

使用“**编辑自动更新资料库列表**”对话框，您可以向列表中添加新的自动更新资料库，也可以配置、编辑和删除现有的资料库以及组织该列表中的资料库。

这部分包含下列主题：

- 添加和编辑资料库
- 删除和重新组织资料库
- 指定代理服务器设置

添加和编辑资料库

您可以在“**编辑自动更新资料库列表**”对话框中添加或编辑自动更新资料库。

> **注释**
> 也可以使用 McAfee AutoUpdate Architect 创建资料库并将其导出到 VirusScan Enterprise 中。关于如何使用 McAfee AutoUpdate Architect 创建并导出自动更新资料库的详细信息，请参阅《McAfee AutoUpdate Architect Product Guide》。

自动更新资料库的状态可以是“已禁用”或“已启用”。

- **已启用** - 一种具有固定状态的资料库，可以在自动更新过程中使用。
- **已禁用** - 一种具有固定状态的资料库，不能在自动更新过程中使用。

要在自动更新资料库列表中添加或编辑资料库：

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。
2. 选择“**工具**” | “**编辑自动更新资料库列表**”。
3. 选择“**资料库**”选项卡。FTP 资料库是默认的下载站点。

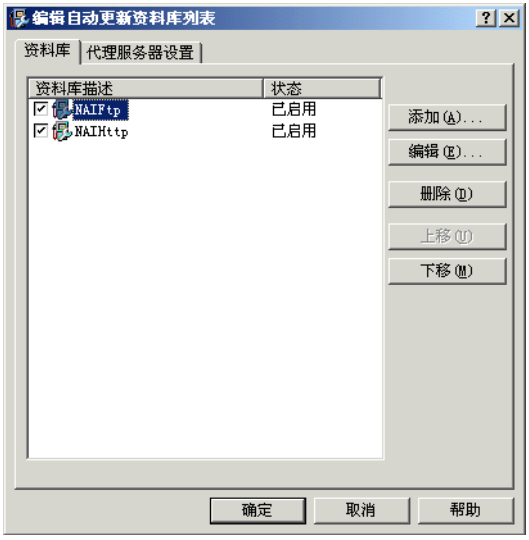

图 7-4. 编辑自动更新资料库列表 - “资料库”选项卡

4 请从以下操作中选择：

- 要添加资料库，请单击 “**添加**”打开 “**资料库设置**”对话框。
- 要编辑某个资料库，请在 “**资料库描述**”列表中突出显示该资料库，然后单击 “**编辑**”打开 “**资料库设置**”对话框。

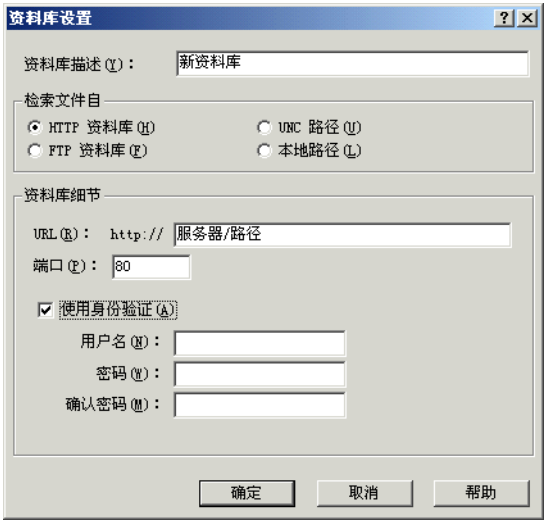

图 7-5. 资料库设置

5 在“**资料库描述**”文本框中，输入该资料库的名称或说明。

6 在“**检索文件自**”下，从下列选项中选择资料库类型或路径：

- **HTTP 资料库**。该选项为默认选项，表示使用您指定为更新文件所在资料库的 HTTP 资料库位置。

  注释
  和 FTP 站点一样，HTTP 站点也可以独立于网络安全之外提供更新，但它可以支持的并发连接要比 FTP 更高级。

- **FTP 资料库**。使用您指定为更新文件所在资料库的 FTP 资料库位置。

  注释
  FTP 站点提供的更新方式更加灵活，不必局限于网络安全权限。FTP 比 HTTP 更不易受到恶意代码的攻击，因此它可以提供更高的稳定性。

- **UNC 路径**。使用您指定为更新文件所在资料库的 UNC 路径。

  注释
  UNC 站点速度最快，也最容易建立。跨越域的 UNC 进行更新要求对每个域具有安全权限，因此需要更多的更新配置。

- **本地路径**。使用您指定为更新文件所在资料库的本地站点。

7 在“**资料库细节**”下，您输入的信息取决于您在“**检索文件自**”下选择的资料库类型或路径。这里支持系统变量。详细信息，请参阅第 171 页的“系统变量”。请从以下选项中进行选择：

- 如果选择了“**HTTP 资料库**”或“**FTP 资料库**”，请参阅第 184 页的“HTTP 或 FTP 资料库细节”获取详细说明。
- 如果选择了“**UNC 路径**”或“**本地路径**”，请参阅第 185 页的“UNC 路径或本地路径资料库细节”获取详细说明。

HTTP 或 FTP 资料库细节

如果选择了 HTTP 或 FTP 资料库：

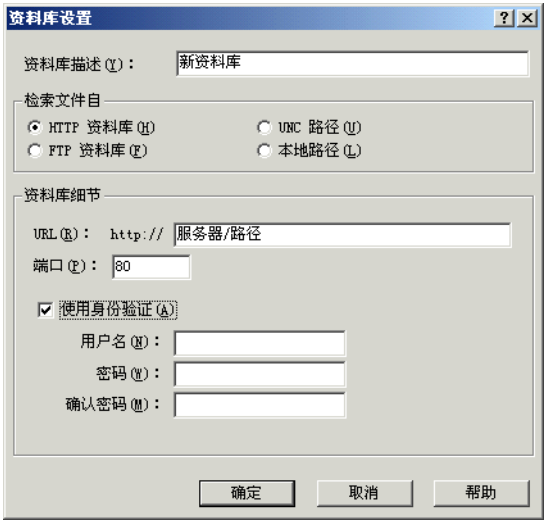

图 7-6. 资料库细节 - HTTP 或 FTP 站点

1 在 “**资料库细节**”下，输入所选资料库的路径以及端口号，并指定用来访问该资料库的安全证书。

- **URL**。输入资料库位置的 HTTP 或 FTP 路径：
  - **HTTP**。输入 HTTP 服务器和更新文件所在文件夹的位置。DAT 更新文件的默认 McAfee HTTP 资料库位于：

    http://update.nai.com/Products/CommonUpdater
  - **FTP**。输入FTP服务器和更新文件所在文件夹的位置。DAT更新文件的默认 McAfee FTP 资料库位于：

    ftp://ftp.nai.com/CommonUpdater
- **端口**。输入所选 HTTP 或 FTP 服务器的端口号。
- “**使用身份验证**”或“**使用匿名登录**”。标题将取决于您选择了 HTTP 路径还是选择了 FTP 路径。指定用来访问该资料库的安全证书。输入“**用户名**”和 “**密码**”，然后 “**确认密码**”。

注释

FTP 和 UNC 资料库需要下载证书，但 HTTP 资料库不要求。自动更新功能将使用您指定的证书来访问资料库，以便下载所需的更新文件。在资料库中配置帐户证书时，您应确保该帐户对更新文件所在的文件夹有读取权限。

FTP 更新支持匿名资料库连接。

2 单击“**确定**”保存更改并返回到“**自动更新资料库列表**”对话框。

UNC 路径或本地路径资料库细节

如果选择了 UNC 或本地路径：

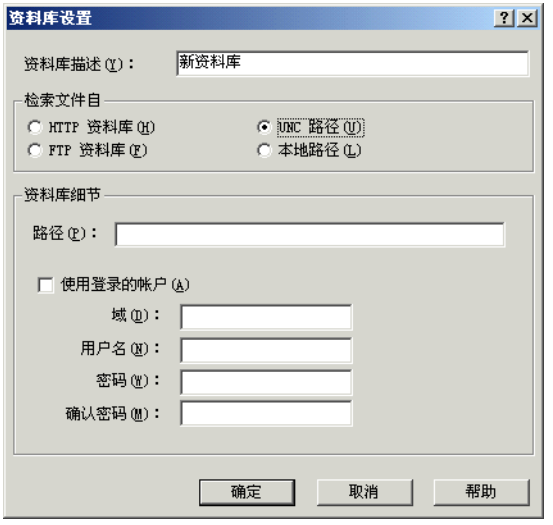

图 7-7. 资料库细节 - UNC 或本地路径

1 在“**资料库细节**”下，输入所选资料库的路径，并确定是使用已登录的帐户还是通过指定用户名和密码来加强安全性。这里支持系统变量。详细信息，请参阅第 171 页的“系统变量”。

- **路径**。输入更新文件所在位置的路径。
  - **UNC路径**。使用UNC格式（\\服务器名称\路径）输入更新文件所在资料库的路径。
  - **本地路径**。输入更新文件所在的本地文件夹的路径，或者单击“**浏览**”查找该文件夹。

注释

路径可以是本地驱动器或网络驱动器上的文件夹。

- **使用登录的帐户**。确定要使用哪个帐户：
  - 要使用当前登录的帐户，请选择 **“使用登录的帐户”**。
  - 要使用另一个帐户，请取消选择**“使用登录的帐户”**，然后输入**“域”**、**“用户名”**、**“密码”**并 **“确认密码”**。

    注释

    FTP 和 UNC 资料库需要下载证书，但 HTTP 资料库不要求。自动更新功能将使用您指定的证书来访问资料库，以便下载所需的更新文件。在资料库中配置帐户证书时，您应确保该帐户对更新文件所在的文件夹有读取权限。

    对于 UNC 更新，您还可以选择使用已登录的帐户。这允许更新任务使用已登录用户的权限来访问资料库。

2 单击 **“确定”**保存更改并返回到 **“资料库”**选项卡。

删除和重新组织资料库

要删除或重新组织资料库列表中的资料库：

1 打开**“VirusScan 控制台”**。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 选择 **“工具”** | **“编辑自动更新资料库列表”**。

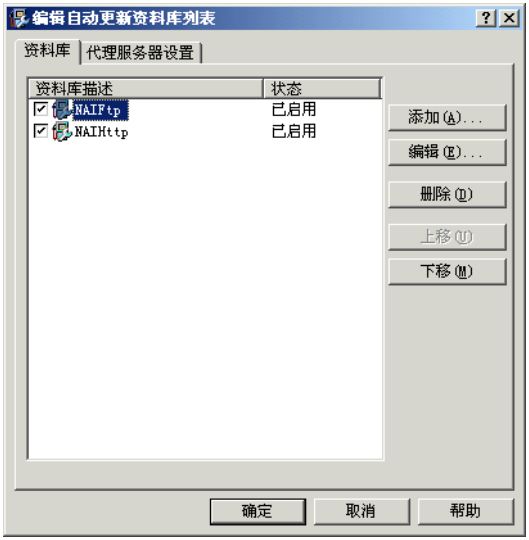

图 7-8. 编辑自动更新资料库列表 - “资料库”选项卡

3 选择“资料库”选项卡。

4 要删除或重新组织资料库列表中的资料库，请从下面的操作中选择：

- 要删除某个资料库，请在列表中突出显示它，然后单击“删除”。
- 要重新组织列表中的资料库，请先突出显示一个资料库，然后反复单击“上移”或“下移”，直到资料库移到列表中的理想位置为止。

注释
资料库在列表中的排列顺序，就是在更新过程中资料库被访问的顺序。

指定代理服务器设置

作为 Internet 安全防范措施的一部分，代理服务器可以将 Internet 用户的计算机屏蔽，并通过高速缓存经常访问的站点来提高访问速度。

如果网络中使用了代理服务器，您可以指定代理服务器要使用的设置和代理服务器的地址，并确定是否使用身份验证。代理服务器信息存储在自动更新资料库列表 (SITELIST.XML) 中。您在这里配置的代理服务器设置将应用于资料库列表中的所有资料库。

要指定代理服务器设置：

1 打开“VirusScan 控制台”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 选择“工具” | “编辑自动更新资料库列表”。

3 选择“代理服务器设置”选项卡。

图 7-9. 编辑自动更新资料库列表 - “代理服务器设置”选项卡

4 确定是否需要使用代理服务器，如果需要，请确定要使用的设置。请从以下选项中选择：

- **不使用代理服务器**。不需要指定代理服务器。选择该选项，然后单击“**确定**”保存设置并关闭“**编辑自动更新资料库列表**”对话框。
- **使用Internet Explorer代理服务器设置**。该选项为默认选项，表示使用当前安装的 Internet Explorer 的代理服务器设置。选择该选项，然后单击“**确定**”保存设置并关闭“**编辑自动更新资料库列表**”对话框。
- **人工配置代理服务器设置**。配置代理服务器设置以满足您自己的需要。这里支持系统变量。详细信息，请参阅第 171 页的“系统变量”。

  选择该选项，然后输入所选资料库的地址和端口信息：

  - **HTTP 地址**。输入 HTTP 代理服务器的地址。
  - **HTTP 端口**。输入 HTTP 代理服务器的端口号。
  - **FTP 地址**。输入 FTP 代理服务器的地址。
  - **FTP 端口**。输入 FTP 代理服务器的端口号。

  确定是否为您指定的 HTTP 或 FTP 代理服务器使用身份验证。请从以下选项中选择：

  - **使用 HTTP 身份验证**。要对 HTTP 代理服务器使用身份验证，请选择该选项，然后输入“**HTTP 用户名**”、“**HTTP 密码**”和“**HTTP 确认密码**”。
  - **使用 FTP 身份验证**。要对 FTP 代理服务器使用身份验证，请选择该选项，然后输入“**FTP 用户名**”、“**FTP 密码**”和“**FTP 确认密码**”。

5 要为代理服务器指定例外情况，请单击“**例外**”。如果不想指定例外情况，请跳过这个步骤并转到步骤 6。

图 7-10. 代理服务器例外情况

a 选择“**指定例外项**”，然后输入例外情况，各项之间用分号隔开。

b 单击“**确定**”保存更改并返回到“**代理服务器设置**”选项卡。

6 单击“**确定**”保存更改并关闭“**编辑自动更新资料库列表**”对话框。

镜像任务

VirusScan Enterprise 软件依靠目录结构来自行更新。镜像任务允许您将更新文件从资料库列表中定义的第一个可访问的资料库复制到网络中的某个镜像站点。当镜像某个站点时，一定要复制整个目录结构。只要整个目录结构被复制到 VirusScan 4.5.1 更新时使用的那个位置，这个目录结构就会同时也支持早期版本的 VirusScan 和 NetShield。

下面显示了通过镜像任务复制 Network Associates 资料库之后资料库中的目录结构：

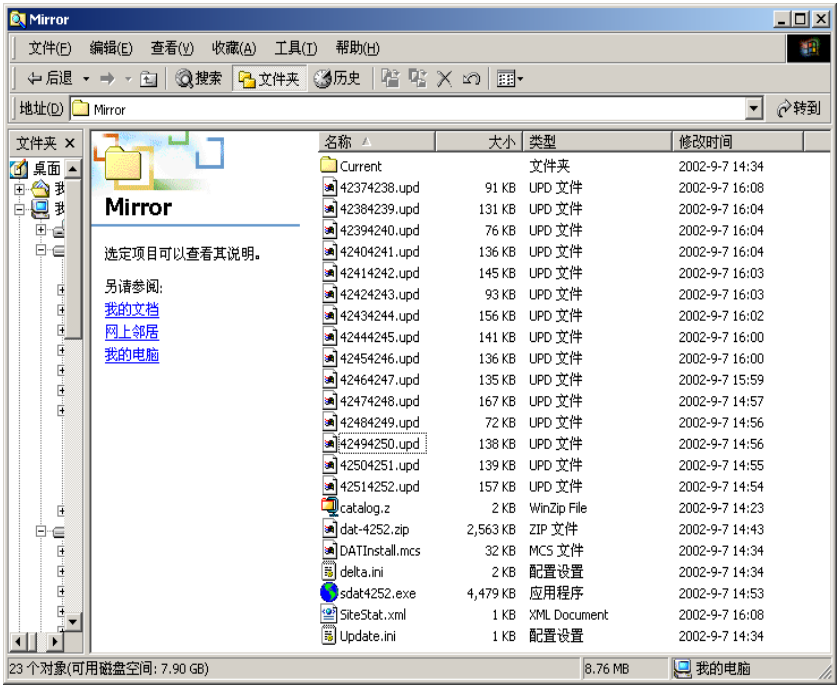

图 7-11. 镜像站点

复制了包含更新文件的 Network Associates 站点之后，网络中的计算机就可以从这个镜像站点下载文件。这种方法非常实用，原因在于无论网络中的计算机是否能够访问 Internet，您都可以更新它们，同时，由于这些计算机所连接的服务器可能比 Network Associates 的 Internet 站点距离您更近，因此可以节省访问和下载时间，所以这种方法也更为有效。这项任务最常见的用途是将 Network Associates 下载站点的内容镜像到本地服务器。

这部分包含下列主题：

- 创建镜像任务
- 配置镜像任务
- 运行镜像任务
- 查看镜像任务活动日志

创建镜像任务

您可以为所需的每个镜像位置创建一个镜像任务：

要创建新的镜像任务：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 您可以使用以下方法之一创建镜像任务：

- 右键单击控制台中的空白区域而无需从任务列表中选择任何项目，然后选择 “**新建镜像任务**”。
- 选择 “**任务**”菜单中的 “**新建镜像任务**”。

“**VirusScan 控制台**”任务列表中将突出显示一个新的镜像任务。

3 接受默认的任务名称或者键入一个新的任务名称，然后按 ENTER 键打开“**自动更新属性**”对话框。要详细了解配置信息，请参阅第 191 页的“配置镜像任务”。

注释

如果通过 ePolicy Orchestrator 3.0 或更高版本创建了镜像任务并启用了任务可见功能，则可以在 VirusScan 控制台中看到这些镜像任务。这些 ePolicy Orchestrator 任务是只读的，不能从 VirusScan 控制台中配置。详细信息，请参阅《VirusScan Enterprise 配置指南 - 与 ePolicy Orchestrator 3.0 配合使用》。

配置镜像任务

您可以根据自己的需要配置和计划镜像任务。

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一打开 “**自动更新属性**”对话框：

- 突出显示控制台任务列表中的任务，然后从 “**任务**”菜单中选择 “**属性**”。
- 双击任务列表中的任务。
- 右键单击任务列表中的任务，然后选择 “**属性**”。
- 突出显示任务列表中的任务，然后单击  。

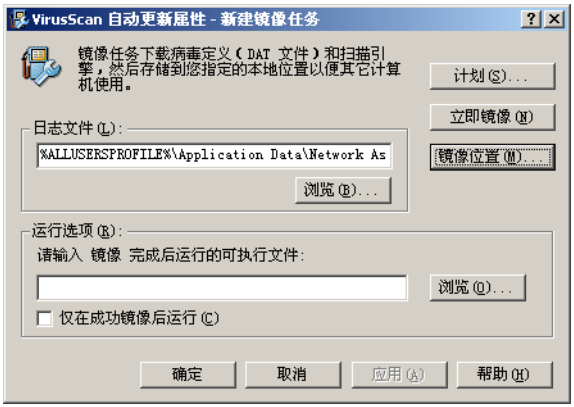

图 7-12. 自动更新属性 - 新建镜像任务

注释
在单击 “**计划**”或 “**立即镜像**”之前，请先配置镜像任务。

3 在 “**日志文件**”文本框中，接受默认的日志文件名和位置、输入其他日志文件名和位置，或者单击“**浏览**”查找合适的位置。这里支持系统变量。详细信息，请参阅第 171 页的 “系统变量”。

注释
默认情况下，日志信息被写入到位于以下文件夹中的 VSEMIRRORLOG.TXT 文件中：

```
<驱动器>:Winnt\Profiles\All Users\Application
Data\Network Associates\VirusScan
```

4 单击“镜像位置”打开“镜像位置设置”对话框：

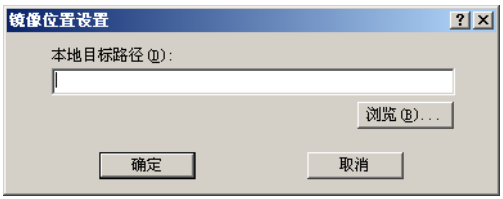

图 7-13. 镜像位置设置

a 输入本地系统中用作镜像站点的目标位置路径，或者单击“浏览”找到所需的位置。这里支持系统变量。详细信息，请参阅第 171 页的“系统变量”。

b 单击“确定”返回到“自动更新属性”对话框。

5 在“运行选项”下，您可以指定要在镜像任务结束后启动的可执行文件。例如，您可以使用这个选项启动一个网络消息实用程序来通知管理员更新操作已成功完成。

- **请输入镜像完成后运行的可执行文件**。输入要运行的可执行文件的路径，或者单击“浏览”进行查找。
- **仅在成功镜像后运行**。只在成功更新之后运行可执行程序。如果更新失败，所选的程序将不会运行。

注释
当前登录的用户必须能够执行您指定的程序文件。如果当前登录的用户无权访问这个程序文件所在的文件夹或者目前没有任何用户登录，该程序也不会运行。

6 单击“计划”以计划镜像任务。关于计划任务的详细说明，请参阅第 199 页的“计划任务”。

7 单击“应用”保存更改。

8 要立即运行镜像任务，请单击“立即镜像”。

9 单击“确定”关闭“自动更新属性”对话框。

注释
“镜像”任务使用资料库列表中的配置设置来执行更新。详细信息，请参阅第 179 页的“自动更新资料库列表”。

运行镜像任务

用所需的属性配置了镜像任务之后，您就可以通过以下方法之一来运行镜像任务：

- **按计划镜像**。如果计划了镜像任务，则它可以在无人值守的情况下运行。

  注释
  计算机必须处于开机状态，镜像任务才能运行。如果计算机在任务即将开始运行时处于关机状态，这项任务将在计算机处于开机状态时的下一个计划时间运行，而如果选择了“**计划设置**”中“**计划**”选项卡上的“**运行错过的任务**”选项，这项任务将在计算机启动时开始运行。

- **立即镜像**。您可以通过两种方式立即启动镜像任务：
  - 用于镜像任务的“**启动**”命令。
  - 用于镜像任务的“**立即镜像**”命令。

用于镜像任务的“启动”命令

您可以使用“**VirusScan 控制台**”中的“**启动**”命令来立即启动任何镜像任务。

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。
2. 按照以下方法之一，从“**VirusScan 控制台**”启动立即镜像任务：
   - 突出显示控制台任务列表中的任务，然后从“**任务**”菜单中选择“**启动**”。
   - 右键单击任务列表中的任务，然后选择“**启动**”。
   - 突出显示任务列表中的任务，然后单击  。
   - 当这项任务结束之后，单击“**关闭**”退出“**McAfee 自动更新**”对话框，或者等待该对话框自动关闭。

用于镜像任务的立即镜像命令

您可以使用“**自动更新属性**”对话框中的“**立即镜像**”命令来立即启动任何镜像任务。

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 打开所选镜像任务的 “**自动更新属性**”对话框。有关说明，请参阅第 191 页的“配置镜像任务”。

3 单击 “**自动更新属性**”对话框中的 “**立即镜像**”。

4 当这项任务结束之后，单击 “**关闭**”退出 “**McAfee 自动更新**”对话框，或者等待该对话框自动关闭。

查看镜像任务活动日志

镜像任务活动日志显示了更新操作的详细信息。例如，它显示了更新后的 DAT 文件和引擎版本号。

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 使用以下方法之一，打开活动日志文件：

- 突出显示一项任务，然后选择 “**任务**”菜单中的 “**活动日志**”。
- 右键单击任务列表中的这项任务，并选择 “**查看日志**”。

3 要关闭活动日志，请选择 “**文件**”菜单中的 “**退出**”。

回滚 DAT 文件

如果发现由于某种原因当前的 DAT 文件已损坏或者不兼容，您可以使用该功能将 DAT 文件回滚至上一个备份版本。在更新 DAT 文件时，上一版本将存储在如下位置：

```
C:\Program Files\Common Files\Network Associates\Engine\OldDats
```

当回滚 DAT 文件时，系统会用 OldDats 文件夹中的版本替换当前的 DAT 文件，并在注册表中的如下位置添加一个标记：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\VirusScan
Enterprise\CurrentVersion\szRollbackedDATS
```

在回滚之后，您将无法再次返回到上一个版本。下次进行更新时，系统会将注册表中的 DAT 版本与更新资料库中的 DAT 文件进行比较。如果新的 DAT 文件与注册表中标记的文件相同，则不执行更新。

要回滚 DAT 文件：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 19 页的“VirusScan 控制台”。

2 选择“**工具**”|“**回滚 DAT**”。“**McAfee 自动更新**”对话框将打开。

图 7-14. 回滚 DAT - 正在更新

3 回滚操作表面看来与更新相同，不同之处在于详细信息中会显示“正在执行DAT回滚”。当回滚结束之后，单击“**关闭**”退出“**McAfee 自动更新**”对话框，或者等待该对话框自动关闭。

注释

执行回滚时，恢复的是备份的上一个 DAT 文件。

手动更新

McAfee Security 建议您使用 VirusScan Enterprise 软件自带的自动更新任务来安装新版本的 DAT 文件或扫描引擎。这个实用程序可以准确无误地快速更新 DAT 文件和扫描引擎。然而，要自行安装 DAT 文件，您可以从以下更新站点手动下载 DAT 文件和引擎文件：

http:www.networkassociates.com/us/downloads/updates

ftp://ftp.nai.com/CommonUpdater

- **常规 DAT 文件**。McAfee Security 将这些文件以名为 DAT-XXXX.ZIP 的 .ZIP 存档文件形式存储在它的 FTP 站点中。文件名中的 XXXX 表示序列号，每发布一个 DAT 文件，序列号都会随之改变。要下载这些文件，请使用 Web 浏览器或 FTP 客户端程序登录：

  ftp://ftp.nai.com/CommonUpdater

- **可安装的 .EXE 文件**。McAfee Security 以名为 XXXXUPDT.EXE 的自执行安装程序文件形式将这些文件存储在它的网站中。其中的 XXXX 也是序列号，每发布一个 DAT 文件，序列号都会随之改变。要下载这些文件，请使用 Web 浏览器登录：

  http:www.networkassociates.com/us/downloads/updates

  这两个文件都包含完全相同的 DAT 文件。不同之处在于如何使用它们来更新您的 VirusScan Enterprise 软件。

要使用 DAT-XXXX.ZIP 存档文件，您必须下载并解压缩该文件、将这些文件复制到 DAT 文件夹中，然后重新启动按访问扫描程序。详细说明，请参阅第 197 页的“从 DAT 存档文件更新”。

要安装安装程序附带的 DAT 文件，只需将这些文件下载到硬盘上的一个临时文件夹中，然后运行或双击 XXXUPDT.EXE 文件。安装程序会停止按访问扫描程序、将这些文件复制到适当的文件夹中，然后重新启动按访问扫描程序。

> **注释**
> 您需要具有管理员权限才能向 DAT 文件夹执行写入操作。

更新之后，当按访问扫描程序、按需扫描程序和电子邮件扫描程序下次启动时，就会采用新的 DAT 文件。

从 DAT 存档文件更新

要不使用自动更新功能而直接从 .ZIP 存档文件安装 DAT 文件更新：

1. 在硬盘中创建一个临时文件夹，然后将下载的DAT文件.ZIP存档复制到该文件夹中。
2. 备份或重命名现有的 DAT 文件。
   - CLEAN.DAT
   - NAMES.DAT
   - SCAN.DAT

   如果接受了默认的安装路径，这些文件将位于：

   < 驱动器 >:\Program Files\Common Files\Network Associates\Engine
3. 使用 WINZIP、PKUNZIP 或同类实用程序打开 .ZIP 存档并解压缩更新后的 DAT 文件。
4. 登录到您要更新的服务器。您必须对目标计算机拥有管理员权限。
5. 将 DAT 文件复制到 DAT 文件夹中。
6. 通过停止McShield服务来禁用按访问扫描，然后再通过启动McShield服务来启用这种扫描。
7. 停止 Microsoft Outlook，然后重新启动它。
8. 停止按需扫描任务，然后重新启动它们。

计划任务 8

您可以命令任务在特定的日期和时间运行或按一定时间间隔运行。您可以配置计划以满足自己公司的需要。

这部分包含下列主题：

- 配置任务计划

配置任务计划

您可以计划三种任务：

- 按需扫描任务 - 要计划按需扫描任务，请打开该任务的“**按需扫描属性**”，然后单击 “**计划**”。“**计划设置**”对话框将打开。

  关于按需扫描任务的详细信息，请参阅第 77 页的 “按需扫描”。

- 自动更新任务 - 要计划一个自动更新任务，请打开自动更新任务的“**自动更新属性**”，然后单击 “**计划**”。“**计划设置**”对话框将打开。

  关于自动更新任务的详细信息，请参阅第 172 页的 “自动更新任务”。

- 镜像任务 - 要计划一个镜像任务，请打开镜像任务的“**自动更新属性**”，然后单击 “**计划**”。“**计划设置**”对话框将打开。

  关于镜像任务的详细信息，请参阅第 189 页的 “镜像任务”。

这部分包含下列主题：

- 任务属性
- 计划属性

任务属性

使用“**任务**”选项卡上的选项，您可以启用计划功能、指定任务运行的时限并对这项任务使用身份验证。

1 选择“**任务**”选项卡。

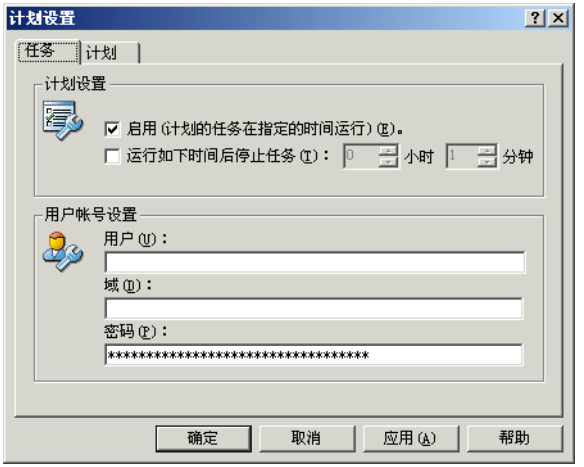

图 8-1. 计划设置 - “任务”选项卡

2 在“**计划设置**”下，指定是否希望任务在特定的时间运行。您可以选择下列选项：

- **启用**（**计划的任务在指定的时间运行**）。命令任务在指定的时间运行。
- **运行如下时间后停止任务**。在限定的时间后停止运行任务。如果选择了该选项，您还需要输入或选择“**小时**”和“**分钟**”。

  注释
  一旦任务在结束之前中断，而且 DAT 文件尚未更新、您也没有选择在 DAT 文件更新之后重新扫描所有文件，则在下次启动时，这项任务将从中断处继续扫描。但如果 DAT 文件已经更新、而且您也选择在 DAT 文件更新之后重新扫描所有文件，则此次扫描将重新开始而不是从中断处继续。

3 在“**任务**”下，输入以下信息来指定这项任务需要使用的身份验证证书：

  注释
  证书是可选的。如果不在此处输入证书，计划的任务将以本地系统帐户名义运行。

- **用户**。输入负责运行这项任务的用户的 ID。
- **域**。输入指定的用户 ID 的域。
- **密码**。输入指定的用户 ID 和域的密码。

4 单击“应用”保存更改。

注释
如果在计划任务时使用了证书，您指定的帐户需要具有作为批处理作业登录权限。如果没有这个权限，即使具有正确的证书，生成的进程也无法访问网络资源。这是一种已知的 Windows NT 行为。

要为某个帐户赋予这种权限：

- 选择“开始”|“设置”|“控制面板”|“管理工具”|“本地安全策略”。
- 选择“安全设置”|“本地策略”|“用户权利指派”。
- 双击“作为批处理作业登录”。
- 将这名用户添加到列表中。
- 单击“确定”保存更改并关闭该对话框。

计划属性

使用“计划”选项卡上的选项，您可以指定任务运行频率、任务在各个时区内的运行时间、是否在指定的时间间隔内随机运行任务、是否运行错过的任务并为错过的任务指定延迟时间。

这部分包含下列主题：

- 计划任务运行频率
- 高级计划选项
- 按频率计划任务

计划任务运行频率

您在此处选择的计划频率会影响日、周和月等计划选项以及其他频率选项。频率选项包括：

- **每天**。该选项为默认选项，表示在指定的那些天中每天运行一次任务。请参阅第 205 页的 “每天”。
- **每周**。在指定的那些星期和天中每周运行一次任务。请参阅第207页的“每周”。
- **每月**。在指定的那些月份和天中每月运行一次任务。请参阅第208页的“每月”。
- **一次**。在指定的日期运行一次任务。请参阅第 209 页的 “一次”。
- **系统启动时**。在系统启动时运行任务，并指定是否每天运行一次该任务以及该任务延迟的分钟数。请参阅第 211 页的 “系统启动时”。
- **登录时**。在登录时运行任务，并指定是否每天运行一次该任务以及该任务延迟的分钟数。请参阅第 211 页的 “登录时”。
- **空闲时**。在计算机空闲时运行任务，并指定分钟数。请参阅第 213 页的 “空闲时”。
- **立即运行**。立即运行该任务。请参阅第 214 页的 “立即运行”。
- **拨号时运行**。在拨号时运行任务，并指定是否每天运行一次该任务。请参阅第 215 页的 “拨号时运行”。

高级计划选项

1 在“计划”选项卡的“计划”下，单击“高级”打开“高级计划选项”对话框。

图 8-2. 高级计划选项

- **开始日期**。单击 从日历中选择一个日期。该字段并非必填字段。
- **结束日期**。单击 从日历中选择一个日期。该字段并非必填字段。
- **重复任务**。按选定的频率重复运行任务。
- **每**。输入一个频率，或者使用箭头来选择一个值，然后选择频率是以分钟还是小时为单位。
- **直到**。选择“时间（本地）”并输入或选择时间，或者选择“持续时间”并输入或选择“小时”和“分钟”。

2 单击“确定”返回到“计划”选项卡。

按频率计划任务

您可以根据自己的需要为任务安排运行日期和 / 或时间。

这部分将介绍以下任务频率：

- 每天
- 每周
- 每月
- 一次
- 系统启动时
- 登录时
- 空闲时
- 立即运行
- 拨号时运行

每天

1 在 “计划” 选项卡的 “计划” 下：

- **计划任务**。单击 ▼ 选择 “每天”。

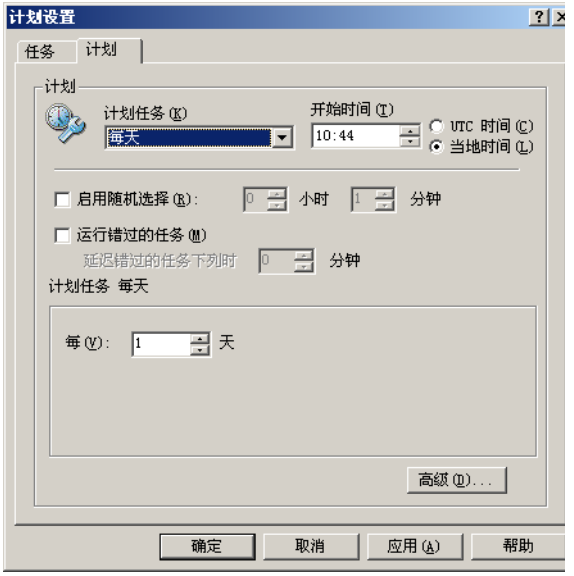

图 8-3. “计划” 选项卡 - 每天

- **开始时间**。输入计划任务的开始时间，或者用箭头选择一个时间。
- **UTC 时间**。全球统一时间 (UTC)。选择该选项将在所有时区内同时运行任务。
- **当地时间**。该选项为默认选项，表示在每个当地时区内独立运行任务。
- **启用随机选择**。在指定时间间隔内的某个随机时刻运行任务。如果选择了该选项，您还需要输入或选择 “**小时**”和 “**分钟**”来设置最长时段。

  您可以输入或选择一个介于 1 分钟到 24 小时之间的时段间隔。例如，将任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则该任务将在 1:00 和 4:00 之间的任意时刻运行。
- **运行错过的任务**。可确保错过的任务在计算机再次启动时运行。如果计算机在任务按计划运行时处于离线状态，这项任务将被错过。这项功能可确保远程用户和网络即使在任务按计划运行时处于离线状态，也仍能完全受到保护。
- **延迟错过的任务**。输入错过的任务要延迟的分钟数，或者使用箭头选择分钟数。请在 0 到 99 分钟之间选择。
- **高级**。单击该按钮可设置高级计划属性。详细信息，请参阅第 204 页的 “高级计划选项”。

2 在“**计划任务 - 每天**”下，输入或选择任务间隔天数，或者使用箭头选择一个值。

> **注释**
> 按天任务可以每隔若干天运行一次，也可以从星期一到星期日每天运行一次。如果只希望在每周的某几天而不是从星期一到星期日的每一天运行任务，我们建议您使用每周任务频率。

3 单击 “**确定**”保存设置并关闭 “**计划设置**”对话框。

每周

1 在 “计划”选项卡的 “计划”下：

- **计划任务**。单击 选择 “每周”。

图 8-4. “计划”选项卡 - 每周

- **开始时间**。输入计划任务的开始时间，或者用箭头选择一个时间。
- **UTC 时间**。全球统一时间 (UTC)。选择该选项将在所有时区内同时运行任务。
- **当地时间**。该选项为默认选项，表示在每个当地时区内独立运行任务。
- **启用随机选择**。在指定时间间隔内的某个随机时刻运行任务。如果选择了该选项，您还需要输入或选择 “小时”和 “分钟”来设置最长时段。

  您可以输入一个介于 1 分钟到 24 小时之间的时段间隔。例如，将任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则该任务将在 1:00 和 4:00 之间的任意时刻运行。

- **运行错过的任务**。可确保错过的任务在计算机再次启动时运行。如果计算机在任务按计划运行时处于离线状态，这项任务将被错过。这项功能可确保远程用户和网络即使在任务按计划运行时处于离线状态，也仍能完全受到保护。
- **延迟错过的任务**。输入错过的任务要延迟的分钟数，或者使用箭头选择分钟数。请在 0 到 99 分钟之间选择。
- **高级**。单击该按钮可设置高级计划属性。详细信息，请参阅第 204 页的 “高级计划选项”。

2 在 “计划任务 - 每周” 下：

- **每**。输入任务间隔的星期数。
- **周的**。选择在星期几运行任务。

3 单击 “确定” 保存设置并关闭 “计划设置” 对话框。

每月

1 在 “计划” 选项卡的 “计划” 下：

- **计划任务**。单击 选择 “每月”。

图 8-5. “计划” 选项卡 - 每月

- **开始时间**。输入计划任务的开始时间，或者用箭头选择一个时间。
- **UTC 时间**。全球统一时间 (UTC)。选择该选项将在所有时区内同时运行任务。
- **当地时间**。该选项为默认选项，表示在每个当地时区内独立运行任务。
- **启用随机选择**。在指定时间间隔内的某个随机时刻运行任务。如果选择了该选项，您还需要输入 “小时” 和 “分钟” 来设置最长时段。

  您可以输入一个介于 1 分钟到 24 小时之间的时段间隔。例如，将任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则该任务将在 1:00 和 4:00 之间的任意时刻运行。

- **运行错过的任务**。可确保错过的任务在计算机再次启动时运行。如果计算机在任务按计划运行时处于离线状态，这项任务将被错过。这项功能可确保远程用户和网络即使在任务按计划运行时处于离线状态，也仍能完全受到保护。
- **延迟错过的任务**。输入错过的任务要延迟的分钟数，或者使用箭头选择分钟数。请在 0 到 99 分钟之间选择。
- **高级**。单击该按钮可设置高级计划属性。详细信息，请参阅第 204 页的“高级计划选项”。

2 在“**计划任务 - 每月**”下，选择下列选项之一：

- **每月几号**。选择该选项并指定在每月的哪一天运行任务。
- **每月的星期几**。选择该选项将在每月的某个具体日期（例如第一个星期日或第二个星期三）运行任务。
  - 选择“**第一个**”、“**第二个**”、“**第三个**”、“**第四个**”或“**最后一个**”选项。
  - 选择在每月中的哪些天运行这项任务。
- 单击“**选择月份**”选择具体的月份：
  - 选择在哪些月份运行任务。

    注释
    默认选择所有月份。
  - 单击“**确定**”返回到“**计划**”选项卡。

3 单击“**确定**”保存设置并关闭“**计划设置**”对话框。

一次

1 在“**计划**”选项卡的“**计划**”下：

- **计划任务**。单击选择“**一次**”。

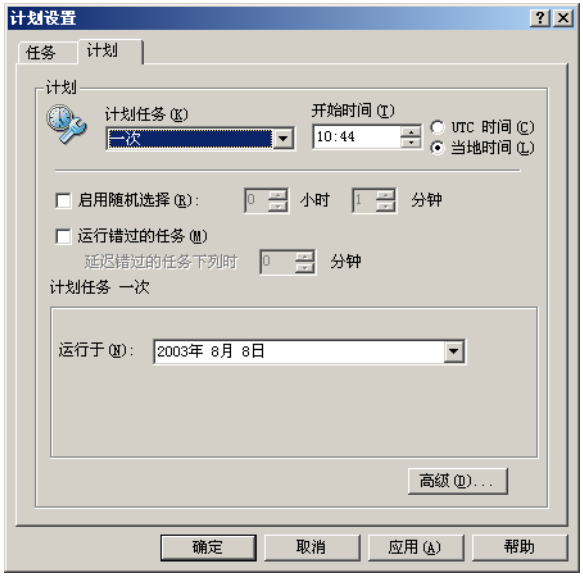

图 8-6. “计划”选项卡 - 一次

- **开始时间**。输入计划任务的开始时间，或者用箭头选择一个时间。
- **UTC 时间**。全球统一时间 (UTC)。选择该选项将在所有时区内同时运行任务。
- **当地时间**。该选项为默认选项，表示在每个当地时区内独立运行任务。
- **启用随机选择**。在指定时间间隔内的某个随机时刻运行任务。如果选择了该选项，您还需要输入或选择 “**小时**”和 “**分钟**”来设置最长时段。

  您可以输入或选择一个介于 1 分钟到 24 小时之间的时段间隔。例如，将任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则该任务将在 1:00 和 4:00 之间的任意时刻运行。

- **运行错过的任务**。可确保错过的任务在计算机再次启动时运行。如果计算机在任务按计划运行时处于离线状态，这项任务将被错过。这项功能可确保远程用户和网络即使在任务按计划运行时处于离线状态，也仍能完全受到保护。
- **延迟错过的任务**。输入错过的任务要延迟的分钟数，或者使用箭头选择分钟数。请在 0 到 99 分钟之间选择。
- **高级**。单击该按钮可设置高级计划属性。详细信息，请参阅第 204 页的 “高级计划选项”。

2 在 “**计划任务 - 一次**”下，单击 选择任务运行的日期。

3 单击 “**确定**”保存设置并关闭 “**计划设置**”对话框。

系统启动时

1 在“计划”选项卡的“计划”下：

- 计划任务。单击 选择“系统启动时”。

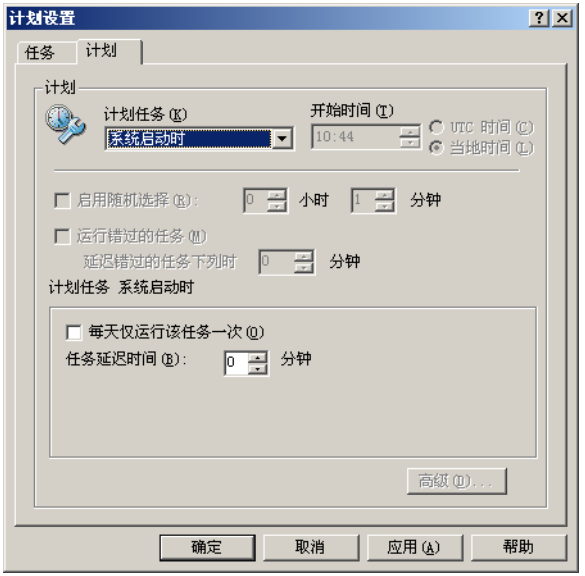

图 8-7. “计划”选项卡 - 系统启动时

2 在“计划任务 - 系统启动时”下：

- **每天仅运行该任务一次**。选择该选项将使这项任务每天只运行一次。如果不选择这个选项，该任务将在每次启动时运行。
- **任务延迟时间**。选择任务延迟的分钟数。请在 0 到 99 分钟之间选择。这为运行登录脚本或用户登录节省了时间。

3 单击“确定”保存设置并关闭“计划设置”对话框。

登录时

1 在“计划”选项卡的“计划”下：

- 计划任务。单击 选择“登录时”。

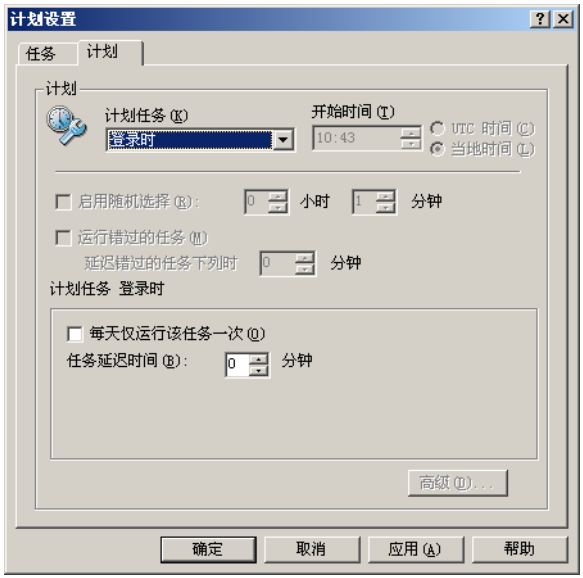

图 8-8. “计划”选项卡 - 登录时

2 在 “**计划任务 - 登录时**”下：

- **每天仅运行该任务一次**。选择该选项将使这项任务每天只运行一次。如果不选择这个选项，该任务将在每次登录时运行。
- **任务延迟时间**。输入任务延迟的分钟数。请在 0 到 99 分钟之间选择。这为运行登录脚本或用户登录节省了时间。

3 单击 “**确定**”保存设置并关闭 “**计划设置**”对话框。

空闲时

1 在“计划”选项卡的“计划”下：

- 计划任务。单击 选择“空闲时”。

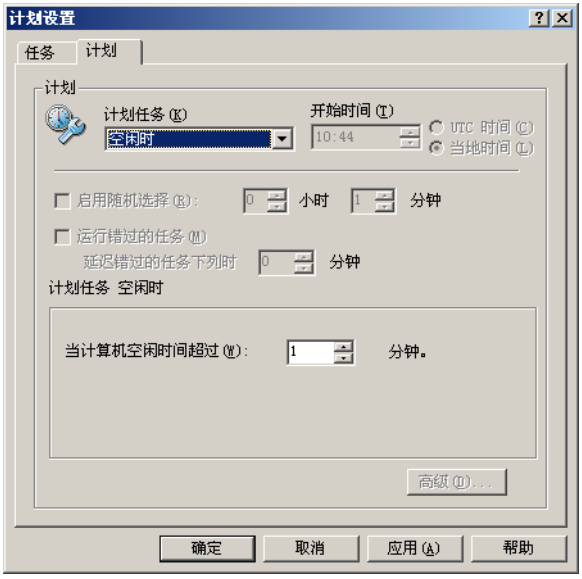

图 8-9. “计划”选项卡 - 空闲时

2 在“计划任务 - 空闲时”下，输入或选择在任务启动之前您希望计算机保持为空闲状态的分钟数。请在 0 到 999 分钟之间选择。

3 单击“确定”保存设置并关闭“计划设置”对话框。

立即运行

1 在“计划”选项卡的“计划”下：

- 计划任务。单击 选择“立即运行”。

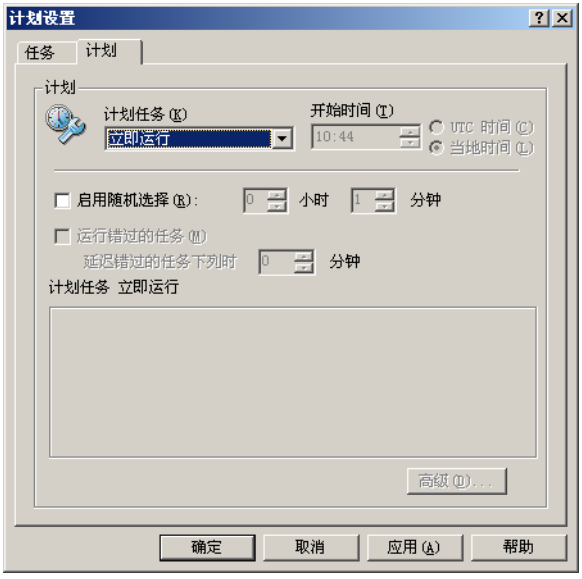

图 8-10. “计划”选项卡 - 立即运行

- **启用随机选择**。在指定时间间隔内的某个随机时刻运行任务。如果选择了该选项，您还需要输入或选择“**小时**”和“**分钟**”来设置最长时段。

  您可以输入或选择一个介于 1 分钟到 24 小时之间的时段间隔。例如，将任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则该任务将在 1:00 和 4:00 之间的任意时刻运行。

2 单击“**确定**”保存设置并关闭“**计划设置**”对话框。

拨号时运行

1 在“计划”选项卡的“计划”下：

- 计划任务。单击 选择“拨号时运行”。

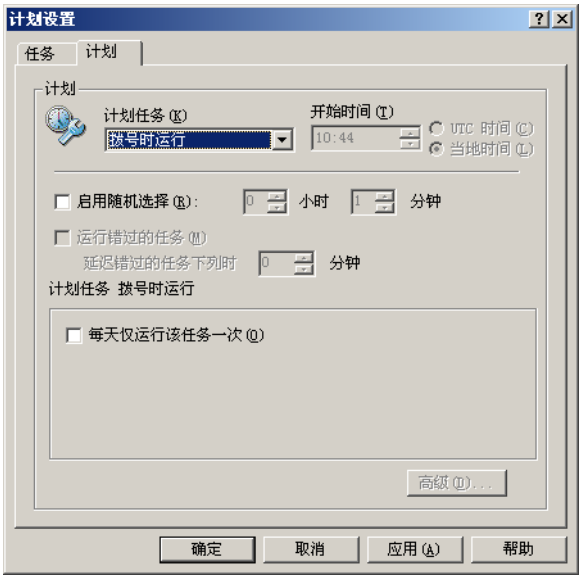

图 8-11. “计划”选项卡 - 拨号时运行

- **启用随机选择**。在指定时间间隔内的某个随机时刻运行任务。如果选择了该选项，您还需要输入或选择“小时”和“分钟”来设置最长时段。

  您可以输入或选择一个介于 1 分钟到 24 小时之间的时段间隔。例如，将任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则该任务将在 1:00 和 4:00 之间的任意时刻运行。

2 在“计划任务 - 拨号时”下，选择是否每天运行一次任务。

> **注释**
> 对于自动更新任务而言，将任务安排在“拨号时运行”比按需扫描任务更有用。

3 单击“确定”保存设置并关闭“计划设置”对话框。

命令行扫描程序 A

典型安装的 VirusScan Enterprise 软件通常包括 McAfee Security VirusScan Enterprise 命令行程序。该程序可以从 Windows 命令行提示符运行。

这部分包含下列主题：

- VirusScan Enterprise 命令行选项
- 按需扫描命令行选项
- 自定义的安装属性

VirusScan Enterprise 命令行选项

要运行 VirusScan Enterprise 命令行程序，请打开 SCAN.EXE 文件所在的文件夹并键入 SCAN。如果将 VirusScan Enterprise 程序安装在了默认位置，该文件将位于：

```
C:\Program Files\Common Files\Network Associates\Engine
```

下表列出了可以添加到 SCAN 命令中的选项。除非另行说明，否则下面列出的所有选项都可以用来配置按需扫描和按访问扫描。

表 A-1. VirusScan 命令行选项

命令行选项	描述
/? 或 /HELP	显示一个 VirusScan 命令行选项列表，每个选项都带有一个简短说明。 您可能会发现，向 VirusScan 程序创建的报告文件添加一组扫描选项会很有用。为此，您可以在命令提示符中键入 scan /? /REPORT < 文件名 >。扫描报告结果中附加了可供此次扫描任务使用的全部选项。
/ADL	除了扫描在命令行中指定的其他任何驱动器之外，还扫描所有本地驱动器，包括压缩驱动器和 PC 卡，但不包括磁盘。 要同时扫描本地驱动器和网络驱动器，请在同一个命令行中同时使用 /ADL 和 /ADN 命令。
/ADN	除了扫描在命令行中指定的其他任何驱动器之外，还扫描所有网络驱动器 （包括光驱）是否感染了病毒。 **注释：**要同时扫描本地驱动器和网络驱动器，请在同一个命令行中同时使用 /ADL 和 /ADN 命令。
/ALERTPATH < 目录 >	将目录 < 目录 > 指定为受集中警报功能监控的远程 NetWare 卷或 Windows NT 目录的网络路径。 VirusScan 将在检测到感染病毒的文件后向服务器发送一个 .ALR 文本文件。 在这个目录中， VirusScan Enterprise 将使用它的集中警报功能按照现有的配置来广播或编辑警报和报告。 要求： • 您必须对指定的目录具有写入权限。 • 这个目录中必须含有 VirusScan Enterprise 自带的 CENTALRT.TXT 文件。

表 A-1. VirusScan 命令行选项 (续)

命令行选项	描述
/ALL	通过扫描有可能感染病毒的所有文件（而不考虑扩展名）来覆盖默认的扫描设置。 **注释：** 使用 /ALL 选项将显著增加所需的扫描时间。只有当发现或怀疑感染了病毒时，才应使用这个选项。 要获得当前的文件类型扩展名列表，请在命令提示符中运行 /EXTLIST。
/ANALYZE	设置本软件，以使其同时启用程序启发式扫描和宏启发式扫描。 **注释：** /MANALYZE 只针对宏病毒， /PANALYZE 只针对程序病毒。
/APPEND	与 /REPORT < 文件名 > 配合使用，可以将报告消息文本附加到指定的报告文件中，而不是覆盖它。
/BOOT	只扫描引导区和主引导记录。
/CLEAN	清除所有文件和系统区域中感染的病毒。
/CLEANDOCALL	作为防范宏病毒的一项措施，当只查到一处病毒感染时，/CLEANDOCALL 会清除 Microsoft Word 和 Office 文档中的所有宏。 **注释：** 该选项会删除所有的宏，包括未被病毒感染的宏。
/CONTACTFILE < 文件名 >	在发现病毒时显示 < 文件名 > 的内容。这样可以为用户提供联系人信息并说明当遇到病毒时如何处理。 （McAfee Security 建议将 /LOCK 与该选项配合使用。） 该选项在网络环境中尤其有用，它使您可以在一个中央文件中方便地维护消息文本，而不必在每个工作站中维护。 **注释：** 在联系人信息中，除反斜杠 (\) 以外的任何字符都有效。以斜杠 (/) 或连字符 (-) 开头的消息应放在引号内。
/DAM	修复开关：如果发现某个宏感染了病毒，将删除所有宏。如果未发现任何感染了病毒的宏，将不会执行删除操作。 如果怀疑文件感染了病毒，可以选择从数据文件中剥离所有宏，以便将感染病毒的可能性降至最低。为了在感染病毒之前删除文件中的所有宏，请将该选项与 /FAM 配合使用： scan < 文件名 > /fam /dam 当这两个选项配合使用时，发现的所有宏都将被删除，而不论是否发现了病毒。
/DEL	永久删除感染病毒的文件。

表 A-1. VirusScan 命令行选项 (续)

命令行选项	描述
/EXCLUDE < 文件名 >	不扫描 < 文件名 > 中列出的文件。 使用该选项可以将特定文件从扫描操作中排除。请将要排除的每个文件的完整路径列在单独的一行中。可以使用通配符 * 和 ?。
/EXTLIST	使用该选项可以从当前 DAT 文件中获取当前的文件类型扩展名列表。
/FAM	查找所有宏：不只是怀疑感染了病毒的宏。它会将找到的所有宏都视为可能的病毒。除非与 /DAM 选项配合使用，否则不会删除找到的宏。 如果怀疑文件感染了病毒，可以选择从数据文件中剥离所有宏，以便将感染病毒的可能性降至最低。为了在感染病毒之前删除文件中的所有宏，请将该选项与 /FAM 配合使用： scan < 文件名 > /fam /dam 当这两个选项配合使用时，发现的所有宏都将被删除，而不论是否发现了病毒。
/FREQUENCY <n>	在上次扫描操作 <n> 小时后不进行扫描。 在病毒感染风险较低的环境中，使用该选项可防止不必要的扫描。 值得一提的是，扫描频率越高，对病毒的防范越有效。
/HELP 或 /?	显示一个扫描选项列表，每个选项都带有一个简短说明。 您可能会发现 , 向 VirusScan 程序创建的报告文件添加一组扫描选项会很有用。为此，您可以在命令提示符中键入 scan /? /REPORT < 文件名 >。扫描报告结果中附加了可供此次扫描任务使用的全部选项。
/LOAD < 文件名 >	从指定的文件加载扫描选项。 使用该选项可以通过从一个 ASCII 格式的文件中加载自定义设置来执行预先配置的扫描操作。
/MANALYZE	针对宏病毒启用启发式扫描。 **注释：**/PANALYZE 只针对程序病毒，而 /ANALYZE 同时针对程序病毒和宏病毒。
/MANY	在个别驱动器上连续扫描多个磁盘。扫描程序会提示您指定每个磁盘。 使用该选项可快速检查多个磁盘。 如果您只有一个软驱而且是从启动盘运行的 VirusScan 软件，则无法使用 /MANY 选项。

表 A-1. VirusScan 命令行选项 (续)

命令行选项	描述
/MOVE < 目录 >	将在扫描过程中发现的所有感染病毒的文件移到指定的目录中，同时保留驱动器盘符和目录结构。 **注释：**当主引导记录或引导区感染了病毒时，由于它们并非文件，该选项将不起作用。
/NOBEEP	禁止在扫描程序发现病毒时播放声音。
/NOBREAK	在扫描期间禁用 CTRL+C 和 CTRL+BREAK。 当使用 /NOBREAK 选项时，用户将无法停止正在运行的扫描操作。
/NOCOMP	跳过而不检查使用 LZ.EXE 或 PkLite 文件压缩程序压缩的可执行文件。 当不需要完全扫描时，这样做可以减少扫描时间。 否则，VirusScan 会默认查看这些可执行文件的内部，或者在内存中自解压缩每个文件并检查病毒特征。
/NODDA	不直接存取磁盘。该选项可防止扫描程序访问引导记录。 增加这项功能的目的是使扫描程序能够在 Windows NT 下运行。 您可能需要对某些设备驱动的驱动器使用该选项。 当访问空光驱或空 Zip 驱动器时，将 /NODDA 与 /ADN 或 /ADL 开关配合使用可能会产生错误。如果出现错误，请键入 F（表示 “失败”）对错误消息作出响应以继续扫描。
/NOXMS	不使用扩展内存 (XMS)。
/PANALYZE	针对程序病毒启用启发式扫描。 **注释：**/MANALYZE 只针对宏病毒，而 /ANALYZE 同时针对程序病毒和宏病毒。
/PAUSE	启用屏幕暂停功能。 当扫描程序在屏幕上显示消息时，会出现 “按任意键继续” 的提示。否则，默认情况下，扫描程序会不停顿地连续显示消息并滚动屏幕，这使它可以在具有多个驱动器或严重感染了病毒的计算机上运行，而不需要用户输入。 McAfee Security 建议您在使用报告选项（/REPORT、/RPTALL、 /RPTCOR 和 /RPTERR）时略去 /PAUSE。

表 A-1. VirusScan 命令行选项 (续)

命令行选项	描述
/REPORT < 文件名 >	针对感染病毒的文件和系统错误创建报告，并以 ASCII 文本文件格式将数据保存到 < 文件名 > 中。 如果 < 文件名 > 已存在，/REPORT 会将其覆盖。为避免覆盖文件，请将 /APPEND 选项与 /REPORT 配合使用，这样，本软件会将报告信息添加到该文件的末尾，而不是覆盖它。 您也可以使用 /RPTALL、/RPTCOR 和 /RPTERR 在报告中添加已扫描的文件、已损坏的文件、已修改的文件以及系统错误。 您可能会发现，向 VirusScan 程序创建的报告文件添加一组扫描选项会很有用。为此，您可以在命令提示符中键入 /? /report < 文件名 >。扫描报告结果中附加了可供此次扫描任务使用的全部选项。 可以包括目标驱动器和目录（例如 D:\VSREPRT\ALL.TXT），但如果目标驱动器是网络驱动器，您必须具有在该驱动器上创建和删除文件的权限。 McAfee Security 建议在使用任何报告选项时都略去 /PAUSE。
/RPTALL	将扫描过的所有文件名附加到 /REPORT 文件中。 您可以在同一个命令行中使用 /RPTERR 和 /RPTCOR 选项。 McAfee Security 建议在使用任何报告选项时都略去 /PAUSE。
/RPTCOR	将已损坏的文件附加到 /REPORT 文件中。 当与 /REPORT 配合使用时，该选项可以在报告文件中添加已损坏的文件的名称。VirusScan 扫描程序发现的已损坏的文件可能是由病毒造成的。 您可以在同一个命令行中使用 /RPTERR 和 /RPTCOR 选项。 某些文件中可能含有错误的内容，这些文件需要被覆盖或者用另一个可执行文件才能正确运行 （即该文件无法自己执行）。 McAfee Security 建议在使用任何报告选项时都略去 /PAUSE。
/RPTERR	将错误附加到 /REPORT 文件中。 当与 /REPORT 配合使用时，该选项可以在报告文件中添加一个系统错误列表。 /LOCK 适用于极易受到攻击的网络环境，例如对外开放的计算机实验室。 您可以在同一个命令行中使用 /RPTERR 和 /RPTCOR。 系统错误可以包括读取或写入磁盘或硬盘错误、文件系统问题或网络问题、创建报告时的问题以及与系统有关的其他问题。 McAfee Security 建议在使用任何报告选项时都略去 /PAUSE。

表 A-1. VirusScan 命令行选项 (续)

命令行选项	描述
/SUB	扫描目录中的子目录。 默认情况下，如果指定要扫描的是目录而非驱动器，VirusScan 扫描程序将只检查该目录所包含的文件，而不检查其子目录。 使用 /SUB 可以扫描任何指定目录中的所有子目录。如果指定扫描整个驱动器，则不需要使用 /SUB。
/UNZIP	扫描压缩文件内部。
/VIRLIST	显示 VirusScan 软件检测到的每个病毒的名称。 这个文件非常大，可能超过 250 页，因此 MS-DOS 的“编辑”程序无法打开它。McAfee Security 建议使用 Windows 的“记事本”或其他文本编辑器来打开这个病毒列表。

按需扫描命令行选项

VirusScan Enterprise 按需扫描程序可以从 Windows 命令行提示符或“开始”菜单的“运行”对话框中运行。要运行该程序，请打开 SCAN32.EXE 文件所在的文件夹，并键入 SCAN32。如果将 VirusScan Enterprise 程序安装在了默认位置，该文件将位于：

```
C:\Program Files\Network Associates\VirusScan
```

下表列出了可以添加到 SCAN32 命令中的选项。

表 A-2. 按需扫描命令行参数

命令行选项	描述
SPLASH	在打开按需扫描程序时显示 VirusScan 启动对话框。
NOSPLASH	在打开按需扫描程序时隐藏 VirusScan 启动对话框。
AUTOEXIT	在非交互式扫描结束后，退出按需扫描程序。
NOAUTOEXIT	在非交互式扫描结束后，不退出按需扫描程序。
ALWAYSEXIT	强制退出按需扫描操作，即使扫描出错而且运行完毕。
NOALWAYSEXIT	不强制退出。
UINONE	启动扫描程序，但隐藏用户界面对话框。
SUB	扫描目标文件夹的子文件夹。
NOSUB	不扫描目标文件夹的子文件夹。
ALL	扫描目标文件夹中的所有文件。
NOALL	只扫描目标文件夹中具有指定文件类型列表中所列文件扩展名的那些文件。
COMP	扫描存档文件，例如 .ZIP、 .CAB、 .LZH 和 .UUE 文件。
NOCOMP	不扫描存档文件。
CONTINUE	在检测到病毒后继续扫描。
PROMPT	在检测到病毒时提示用户采取操作。
NOPROMPT	不在检测到病毒时提示用户采取操作。
CLEAN	在检测到病毒时清除目标文件感染的病毒。
DELETE	在检测到病毒时删除感染病毒的文件。
MOVE	当检测到病毒时，将感染病毒的文件移动（隔离）到预先指定的隔离文件夹。
BEEP	如果检测到了病毒，则在扫描结束时发出蜂鸣声。
NOBEEP	即便检测到了病毒，也不在扫描结束时发出蜂鸣声。

表 A-2. 按需扫描命令行参数 (续)

命令行选项	描述
RPTSIZE	以千字节为单位设置警报日志的大小。
BOOT	在运行当前扫描任务之前，扫描引导区。
NOBOOT	不扫描引导区。
EXT	您在这个参数后面作为参数添加的文件扩展名将取代扫描时使用的所选文件类型列表中的扩展名。
DEFEXT	您在这个参数后面作为参数添加的文件扩展名将添加到扫描时使用的所选文件类型列表中。
TASK	启动在 VirusScan Enterprise 控制台中指定的按需扫描程序任务。该选项还要求其他参数，以便在如下注册表位置中指定特定的任务 ID： HKEY_LOCAL_MACHINE;SOFTWARE; NETWORK ASSOCIATES;TVD; VirusScan EnterpriseNT;CurrentVersion;Tasks。
SERVER	这个参数负责指定在哪台计算机上启动或停止扫描任务。
CANCEL	如果任务失败但控制台表明它仍在运行，您可以使用这个参数来调整注册表，以表明该任务不再运行。
LOG	在事先指定的日志文件中记录病毒报告。
NOLOG	不记录病毒报告。
LOGALL	将对病毒采取的所有措施都作为事件记录。这些措施包括“提示”、“清除病毒”、“删除”和 “移动”。
LOGDETECT	将病毒检测活动作为事件记录。
NOLOGDETECT	不将病毒检测活动作为事件记录。
LOGCLEAN	无论是否成功清除病毒，都将清除活动作为事件记录。
NOLOGCLEAN	无论是否成功清除病毒，都不将清除活动作为事件记录。
LOGDELETE	将删除感染病毒的文件这一操作作为事件记录。
NOLOGDELETE	不将删除感染病毒的文件这一操作作为事件记录。
LOGMOVE	将感染病毒的文件移到隔离文件夹这一操作作为事件记录。
NOLOGMOVE	不将移动感染病毒的文件这一操作作为事件记录。
LOGSETTINGS	记录扫描任务的配置设置。
NOLOGSETTINGS	不记录扫描任务的配置设置。
LOGSUMMARY	记录扫描任务结果摘要。
NOLOGSUMMARY	不记录扫描任务结果摘要。
LOGDATETIME	记录扫描活动的日期、开始时间和结束时间。

表 A-2. 按需扫描命令行参数 (续)

命令行选项	描述
NOLOGDATETIME	不记录扫描活动的日期或时间。
LOGUSER	记录执行扫描任务的用户的识别信息。
NOLOGUSER	不记录用户信息。
PRIORITY	设置扫描任务相对于其他 CPU 进程的优先级。该选项还要求其他数值型参数。值为 1 时，为所有其他 CPU 进程指定优先级。值为 5 时，为扫描任务指定最高的优先级。

自定义的安装属性

当从命令行安装时，您可以使用这些属性来自定义安装过程。

表 A-3. 自定义的安装属性

命令行属性	功能
ALERTMANAGERSOURCEDIR	设置警报管理器的默认源路径。 默认路径为 \AMG。 您也可以在 SETUP.INI 中自行设置这一属性。
CMASOURCEDIR	设置 SITELIST.XML 的源路径。默认路径是作为 SETUP.EXE 运行出发点的当前目录。
ENABLEONACCESSSCANNER	False = False 值无法设置。 True = 在安装完毕之后启用按访问扫描程序。这是默认设置。 **注释** 如果不希望启用按访问扫描程序，请将该属性设置为 ""。 这样此函数即为 ENABLEONACCESSSCANNER=""，表示它是一个空字符串。
EXTRADATSOURCEDIR	设置 EXTRA.DAT 的源路径。在安装过程中，EXTRA.DAT 会被复制到引擎文件所在的位置中。
FORCEAMSINSTALL	True = 安装警报管理器 （如果有）。
INSTALLDIR	设置默认的安装目录。
INSTALLCHECKPOINT	False = 不安装 Check Point SCV 集成。 True = 安装 Check Point SCV 集成。

表 A-3. 自定义的安装属性 (续)

命令行属性	功能
LOCKDOWNVIURUSSCANSHORTCUTS	False = False 值无法设置。 True = 不在开始菜单中显示任何快捷方式。 **注释：**要允许安装快捷方式，请将属性设置为 ""。这样此函数即为 LOCKDOWNVIURUSSCANSHORTCUTS=""，表示它是一个空字符串。这是默认设置。
PRESERVESETTINGS	在升级 NetShield 4.5 或 VirusScan 4.5.1 时保留设置。 False = False 值无法设置。 True = 保留设置。这是默认设置。 **注释：**如果不希望保留设置，请将该属性设置为 ""。这样此函数即为 PRESERVESETTINGS=""，表示它是一个空字符串。
RUNAUTOUPDATE	False = False 值无法设置。 True = 在安装完毕之后运行更新。这是默认设置。 **注释：**如果不希望在安装完毕之后运行更新，请将该属性设置为 ""。这样此函数即为 RUNAUTOUPDATE=""，表示它是一个空字符串。
RUNONDEMANDSCAN	False = False 值无法设置。 True = 在安装完毕之后扫描所有本地驱动器。这是默认设置。 **注释：**如果不希望在安装完毕之后运行按需扫描程序，请将该属性设置为 ""。这样此函数即为 RUNONDEMANDSCAN=""，表示它是一个空字符串。
RUNAUTOUPDATESILENTLY	False = False 值无法设置。 True = 在安装完毕之后运行无提示更新。 **注释：**如果不希望在安装完毕之后运行无提示更新，请将该属性设置为 ""。 这样此函数即为 RUNAUTOUPDATESILENTLY=""，表示它是一个空字符串。

表 A-3. 自定义的安装属性 (续)

命令行属性	功能
RUNONDEMANDSCANSILENTLY	False = False 值无法设置。 True = 在安装完毕之后运行无提示按需扫描。 **注释：**如果不希望在安装完毕之后运行无提示按需扫描，请将该属性设置为 ""。这样此函数即为 RUNONDEMANDSCANSILENTLY=""，表示它是一个空字符串。
SUPPRESSAMSINSTALL	True = 禁止安装警报管理器。
VIRUSSCANICONLOCKDOWN	以两种不同的级别锁定本产品。 NORMAL = 在系统任务栏的 VirusScan 图标菜单中显示所有菜单项。这是默认设置。 MINIMAL = 只在系统任务栏的 VirusScan 图标菜单中显示“启用按访问扫描”和“关于 VirusScan Enterprise”菜单项。 NOICON = 不在系统任务栏中显示 VirusScan 图标菜单。

安全注册表 B

VirusScan Enterprise 程序与 Windows 安全注册表功能兼容。该程序将基于用户的安全许可权限写入注册表项。用户无权使用的任何程序功能都将被禁用，表示不可选择或不响应。早期版本的本产品有时会在 VirusScan Enterprise 程序尝试为用户无权使用的某个功能写入注册表项时出错。

本部分包括下列主题：

- 要求写权限的注册表项

要求写权限的注册表项

该列表是 VirusScan Enterprise 程序及其警报管理器组件要求写权限的注册表项列表。该表格还显示了权限不足的用户写入这些键值时的结果。

该表格中显示的所有注册表项均为如下主键的子键：

```
hkey_local_machine\software\network associates\tvd
```

表 B-1. 锁定 VirusScan Enterprise 注册表项的结果

功能	程序或 Windows 服务	描述	需要写权限才能获得完整功能的注册表项	当由于注册表被锁定而没有写权限时的结果
按访问扫描程序	Network Associates McShield 服务	只能通过本地系统帐户运行的一项 Windows 服务。这项服务会在某个文件被使用时执行扫描。	Shared Components On-Access Scanner	由于这项服务只能通过系统帐户运行，因此通常不受影响。然而，如果这项服务对该键值不具有写权限，则按访问扫描程序不起作用。
按访问扫描程序	ShCfg32.exe	一个可以运行按访问配置界面的程序。	Shared Components On-Access Scanner McShield Configuration	用户可以看到按访问扫描程序属性页，但不能更改配置。
按访问扫描程序	ShStat.exe	一个负责收集按访问扫描程序活动统计信息的程序。该程序还会在系统任务栏中显示 VirusScan Enterprise 图标。通过右键单击这个图标，用户可以查看扫描统计信息、禁用和启用该程序以及打开若干个程序组件。	Shared Components On-Access Scanner McShield Configuration	用户不能通过系统任务栏中的图标启用或禁用按访问扫描程序。

表 B-1. 锁定 VirusScan Enterprise 注册表项的结果 (续)

功能	程序 或 Windows 服务	描述	需要写权限才能获得完整功能的注册表项	当由于注册表被锁定而没有写权限时的结果
按需扫描程序	ScnCfg32	一个可以运行按需配置界面的程序。您可以从 VirusScan Enterprise 控制台访问这个界面。	VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion Tasks VirusScan Enterprise CurrentVersion DefaultTask VirusScan Enterprise CurrentVersion Tasks	如果不能对上述任何键值进行写访问，用户还是可以看到按需扫描程序属性页，但不能更改配置。
按需扫描程序	ScnStat.exe	一个负责收集按需扫描程序活动统计信息的程序。	VirusScan Enterprise CurrentVersion Tasks VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion Tasks	无效。

表 B-1. 锁定 VirusScan Enterprise 注册表项的结果 (续)

功能	程序 或 Windows 服务	描述	需要写权限才能获得完整功能的注册表项	当由于注册表被锁定而没有写权限时的结果
按需扫描程序	Scan32.exe	一个可以对在 VirusScan Enterprise 控制台中指定的目标执行按需扫描活动的程序。	VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion\ Tasks **注释：**还要求对以下各项具有读权限： • Shared Components • VirusScan Engine • 4.0.xx	如果 Scan32 对自身的任务不具有可写键值，则它将运行，但不更新统计信息，因此不会生成扫描结果数据。 这不影响由下一部分内容中介绍的任务管理器服务管理的按需计划扫描任务。

表 B-1. 锁定 VirusScan Enterprise 注册表项的结果 (续)

功能	程序或 Windows 服务	描述	需要写权限才能获得完整功能的注册表项	当由于注册表被锁定而没有写权限时的结果
任务管理器	Network Associates 任务管理器服务	一项 Windows 服务，可以通过系统帐户或管理员帐户运行。这个程序允许您制定扫描和更新活动计划。	VirusScan Enterprise NT CurrentVersion VirusScan Enterprise NT CurrentVersion Alerts VirusScan Enterprise NT CurrentVersion Tasks 所有子键 Shared Components On-Access Scanner McShield Shared Components On-Access scanner McShield Configuration	这项服务只能通过系统帐户或管理员帐户运行，因此通常不受影响。然而，如果这项服务对上述任何键值不具有读 / 写权限，则该服务无法启动。

表 B-1. 锁定 VirusScan Enterprise 注册表项的结果 (续)

功能	程序 或 Windows 服务	描述	需要写权限才能获得完整功能的注册表项	当由于注册表被锁定而没有写权限时的结果
McUpdate	McUPdate.exe	一个可以更新 DAT 文件并升级软件的程序。	VirusScan Enterprise NT Current Version Shared Components On-Access Scanner McShield Configuration	DAT 信息不会更新。 McShield 可能不会重新加载 DAT。 状态信息无法发送到 VirusScan Enterprise 控制台。
			VirusScan Enterprise NT CurrentVersion Tasks	用户可以看到 “更新” 属性页，但不能更改配置。
			VirusScan Enterprise NT CurrentVersion Tasks Update	用户可以看到 “升级” 属性页，但不能更改配置。
			VirusScan Enterprise NT CurrentVersion Tasks Upgrade	

表 B-1. 锁定 VirusScan Enterprise 注册表项的结果 (续)

功能	程序或 Windows 服务	描述	需要写权限才能获得完整功能的注册表项	当由于注册表被锁定而没有写权限时的结果
VirusScan Enterprise 控制台	McConsol.exe	一个可以运行 VirusScan Enterprise 程序管理界面的程序。	VirusScan Enterprise NT CurrentVersion	病毒定义更新功能不能可靠地运行。此外，用户还可以看到当前的屏幕刷新率，但不能更改它。
			VirusScan Enterprise NT CurrentVersion Alerts CurrentVersion	通过选择 “工具” 菜单中的 “警报” 而可见的警报管理器设置将被禁用，而且即使被选定也不会作出响应。同时，由 VirusScan Enterprise 控制台控制的部分启动 / 停止任务也可能不起作用。
			VirusScan Enterprise NT CurrentVersion Tasks	下列选项将被禁用，而且即使被选定也不会作出响应： • 启用 / 禁用按访问扫描任务。 • 复制、粘贴、删除、重命名、导入和导出任务。 • 停止扫描控件。
			Shared Components On-Access Scanner McShield Configuration	
			VirusScan Enterprise NT CurrentVersion Tasks Xxxx	无法配置、启用或禁用按访问扫描任务。 无法配置锁定的任何键值。
警报管理器	NAI 警报管理器	一个在扫描程序检测到病毒、或者事件计划程序遇到问题时能够立即发出通知的组件。	Shared Components Alert Manager	用户可以看到警报方法和警报消息的属性页，但不能更改配置。

故障排除 C

这部分将介绍有关 VirusScan Enterprise 产品的故障排除信息。

这部分包含下列主题：

- 最小扩展工具
- 常见问题
- 更新错误代码

最小扩展工具

作为一款实用程序， McAfee 最小扩展工具 (MERTool) 专门负责收集系统上有关 Network Associates 软件的报告和日志。它获取的信息将有助于您分析问题。

要获得 MERTool 的详细信息并访问该实用程序，请单击与 VirusScan Enterprise 产品一起安装的 MERTool 文件。

该文件位于安装文件夹中。如果接受了默认的安装路径，该文件将位于：

```
<驱动器>:\Program Files\Network Associates\VirusScan
```

当单击 MERTool 文件时，它会访问 MERTool 网站的 URL。请按照网站上的说明进行操作。

常见问题

这部分将以常见问题的形式介绍故障排除信息。问题分为以下几类：

- 安装问题
- 扫描问题
- 病毒问题
- 常规问题

安装问题

我刚刚使用 “无提示安装”方法安装完本软件，但 Windows 系统任务栏中没有显示 VirusScan Enterprise 图标。

只有重新启动系统之后，该图标才会出现在系统任务栏中。但即使该图标没有显示， VirusScan Enterprise 仍在运行并保护您的计算机。

您可以通过检查下列注册表项来验证它：

HKEY_Local_Machine\SOFTWARE/Microsoft\Windows\CurrentVersion\Run
ShStatEXE=C:\Program Files\Network
Associates\VirusScan\SHSTAT.EXE\STANDALONE

为什么网络中的有些用户可以在 VirusScan Enterprise 中配置自己的设置，而其他用户不能？

如果管理员将用户界面配置为使用密码保护任务，用户将无法更改这些设置。

不同的 Microsoft Windows 操作系统有不同的用户权限。 Windows NT 用户有权写入系统注册表，但 Windows XP 或 Windows 2000 用户没有这样的权限。关于用户权限的详细信息，请参阅 Microsoft Windows 文档。

在命令行安装过程中，怎样才能防止没有管理员权限的用户通过 VirusScan 控制台获得管理员权限？

添加如下属性可以在命令行安装过程中防止用户获得管理员权限：

DONOTSTARTSHSTAT=True

这可以防止 SHSTAT.EXE 在安装完毕之后启动。

扫描问题

对于按访问扫描，“在写入磁盘时”扫描和 “从磁盘读取时”扫描有什么区别？

写入时扫描是一种文件写入操作。它扫描以下项目：

- 被写入到本地硬盘驱动器的文件。
- 在本地硬盘驱动器或映射的网络驱动器上创建的文件 （包括新文件、修改后的文件或者从一个驱动器复制或移到另一个驱动器的文件）。

读取时扫描是一种文件读取操作。它扫描以下项目：

- 从本地硬盘驱动器读取的文件。

  注释
  在 “**按访问扫描属性**”对话框中选择 “**在网络驱动器上**”，以便包括远程网络文件。

- 在本地硬盘驱动器中执行的任何文件。
- 在本地硬盘驱动器中打开的任何文件。
- 在本地硬盘驱动器中重命名的任何文件 （如果文件属性已更改）。

当使用按需电子邮件扫描或按发送电子邮件扫描功能检测病毒时，这两个操作选项有什么区别？

请参阅第 112 页的 “操作属性”了解每个操作选项的详细说明。

病毒问题

我怀疑感染了病毒，但 VirusScan Enterprise 没有检测到。

您可以下载正处于正式发布前测试阶段的最新 DAT 文件。要使用每天的 DAT 文件，请参考：

www.mcafeeb2b.com/naicommon/avert/avert-research-enter/virus-4d.asp

VirusScan Enterprise 总是无法安装，我想可能已经感染病毒了。怎么才能知道我的计算机是否感染了病毒？

如果无法安装 VirusScan Enterprise，您仍可以使用从 Network Associates 网站下载的单个文件从命令行中运行扫描。要在尚未安装防病毒软件的计算机中运行命令行扫描：

1. 在 C 驱动器的根目录下创建一个名为 Scan 的文件夹。
2. 右键单击 Scan 文件夹并选择 “**属性**”。确保选择了只读属性。
3. 转到 http://nai.com/naicommon/download/dats/superdat.asp。单击 “**sdatxxxx.exe for Windows-Intel**”开始下载。

4 将该文件下载到新文件夹 (C:\Scan)

5 从“**开始**”菜单中选择“**运行**”，并在文本框中键入 C:\Scan\sdatxxxx.exe /e。单击“**确定**”。

6 打开 DOS 提示符 （也称为 “命令提示符”）。在 **C:\>** 提示符下，键入 cd c:\Scan。此时的提示符为：**C:\Scan>**

7 在 **C:\Scan>** 提示符下，键入：

```
scan.exe /clean /all /adl /unzip /report report.txt
```

这会扫描所有本地驱动器并创建一个名为 REPORT.TXT 的报告文件。

8 扫描之后，浏览到 **C:\Scan** 目录并查看 REPORT.TXT 文件。

注释
建议您在扫描之前断开系统与网络的连接。

在 Windows 2000 和 Windows XP 系统中，启动进入 “带有命令行提示的安全模式”并执行扫描。在 Windows NT 系统中，在 VGA 模式下运行扫描，然后在命令提示符下执行扫描。

建议您在找不到病毒文件之后重新运行一次命令行扫描程序。您可以将报告文本文件重命名为 REPORT2.TXT 以便记录第二次扫描，重命名为 REPORT3.TXT 以便记录第三次扫描，依此类推，从而防止每次覆盖报告文件。

警告
您可能会收到一条错误消息，表明某个应用程序正尝试直接访问 Windows NT 系统上的硬盘。单击 “**忽略**”继续。如果不单击 “**忽略**”，此次扫描将终止。

常规问题

我系统任务栏中的 VirusScan Enterprise 图标好像被禁用了。

如果 VirusScan Enterprise 图标上出现一个红圈和一条线，则表明按访问扫描功能已被禁用。以下是一些最常见的原因和解决方案。如果这些方案都不能解决您的问题，请与技术支持部门联系。

- 确保按访问扫描功能已启用。为此：
  - 右键单击系统任务栏中的 VirusScan Enterprise 图标。如果按访问扫描程序被禁用，菜单中会出现 “**启用按访问扫描**”字样。
  - 选择 “**启用按访问扫描**”以启用按访问扫描程序。

- 确保这项服务正在运行。为此：
  - 使用以下方法之一打开 “控制面板”中的 “服务”：
    - 对于 Windows NT，请选择“**开始**”|“**设置**”|“**控制面板**”|“**管理工具**”|“**服务**”，并确保“**Network Associates McShield**”的“状态”为“**已启动**”。
    - 对于 Windows 2000 或 XP，请选择“**开始**”|“**设置**”|“**控制面板**”|“**管理工具**”|“**服务**”，并确保“**Network Associates McShield**”的“状态”为“**已启动**”。
  - 如果尚未启动，请突出显示服务列表中的“**Network Associates McShield**”，并单击“**启动**”或“**继续**”。

    您也可以选择“**开始**”|“**运行**”，然后键入“**NetStart McShield**”。
- 确保这项服务被设置为自动启动。为此：
  - 使用以下方法之一打开 “控制面板”中的 “服务”：
    - 对于 Windows NT，请选择“**开始**”|“**设置**”|“**控制面板**”|“**管理工具**”|“**服务**”，并确保“**Network Associates McShield**”的“启动类型”为“**自动**”。

      如果没有被设置为“**自动**”，请突出显示服务列表中的“**Network Associates McShield**”并单击“**启动**”，然后选择“**自动**”作为“启动类型”。
    - 对于 Windows 2000 或 XP，请选择“**开始**”|“**设置**”|“**控制面板**”|“**管理工具**”|“**服务**”，并确保“**Network Associates McShield**”的“启动类型”为“**自动**”。

      如果没有被设置为“**自动**”，请右键单击服务列表中的“**Network Associates McShield**”并选择“**属性**”和“**常规**”选项卡，然后选择“**自动**”作为“启动类型”。

我得到一条错误消息，说我不能下载 catalog.z。

产生这个错误的原因有很多。下面给出了一些有助于您找出问题所在的建议。

- **如果使用 Network Associates 默认下载站点进行更新**，请确定您是否能够通过 Web 浏览器来下载 `catalog.z` 文件。为此，请转到 URL：

  http://update.nai.com/Products/CommonUpdater/catalog.z

  并尝试下载该文件。
  - 如果不能下载该文件但可以看到它（也就是说，您的浏览器不允许您下载这个文件），则可能是您的代理服务器出现了问题，需要告知网络管理员。

- 如果能下载这个文件，则意味着 VirusScan Enterprise 也应该能够下载该文件。请与您的技术支持人员联系，让他们帮助您解决安装 VirusScan Enterprise 时出现的问题。

- **如果使用镜像站点进行更新**，请确保镜像站点指向正确的更新站点。如果没有把握，请尝试更改您的设置以便使用默认的 Network Associates 站点。

我有些计算机继续使用 VirusScan 4.5x，而其他一些则使用 VirusScan Enterprise 7.0。是否所有的计算机都能对 DAT 文件使用同一个资料库？

是的，如果网络中的计算机运行多个版本的 VirusScan，则它们可以对 DAT 文件使用同一个资料库。首先，请确保您在使用 VirusScan 4.5.x 资料库列表中的正确目录结构，然后请确保在 McAfee AutoUpdate Architect 控制台中选择了“**我希望使我的站点与原有软件兼容**”选项。详细信息，请参阅《McAfee AutoUpdate Architect Product Guide》。

能否告诉我 HTTP 下载站点的地址？

您可以从如下网站下载包含最新更新的 CATALOG.Z 文件：

http://update.nai.com/Products/CommonUpdater/catalog.z

能否告诉我 FTP 下载站点的地址？

您可以从如下 FTP 站点下载包含最新更新的 CATALOG.Z 文件：

ftp://ftp.nai.com/CommonUpdater/catalog.z

如果我确实发现了病毒而且已经选择 “提示用户操作”，我该选择什么操作 （“清除病毒”、“删除”、“移动”）？

如果不清楚如何处理感染病毒的文件，我们一般建议您选择“**清除病毒**”。VirusScan Enterprise 的默认操作是对文件“**清除病毒**”，然后“**移动**”它。

我试图 “移动”或 “删除”一个文件，但没有成功。

原因可能在于文件被另一个程序锁定，或者您没有权限移动或删除这个文件。作为一种解决办法，您可以查找 VirusScan Enterprise 日志并查看该文件的位置，然后通过 Windows 资源管理器手动移动或删除该文件。

更新错误代码

当自动更新失败时，请查看更新日志。关于如何查看日志文件的信息，请参阅第 178 页的 “查看活动日志”。下面是您可能遇到的常见错误代码：

- **-215：无法获得站点状态** - 本软件无法验证资料库是否可用。请尝试使用网络协议手动下载 PKGCATALOG.Z 文件。如果仍然失败，请验证路径和用户证书。
- **-302：获取代理程序的 Framework 界面失败** - 计划程序界面不可用。请停止并重新启动 Framework 服务。
- **-409：找不到主站点** - 用于更新的主资料库不可用、无法访问或正在使用中。请尝试使用网络协议手动下载 PKGCATALOG.Z 文件。如果仍然失败，请验证路径和用户证书。
- **-414：验证您键入的 “域”、“用户名”和 “密码”是否正确。验证用户帐户是否有权访问资料库所在的位置** - 当创建资料库时，选择了 “验证”之后，会将输入的证书判定为无效。请在现在或者创建了资料库之后更正证书信息，然后再次单击 “验证”。重复这个过程，直到证书通过验证为止。
- **-503：找不到产品包** - 更新文件不在资料库中，或者已经损坏。请确保更新文件已位于资料库中。如果这些文件存在，请创建一个复制或获取任务来覆盖当前的任务设置。如果这些文件不存在，请将这些文件复制到资料库中，然后再次尝试更新。
- **-530：找不到站点目录** - 您从资料库执行了获取任务，但该资料库没有目录文件或者目录文件已损坏。要更正这个问题，请确保源资料库包含有效的目录。
- **-531：找不到软件包目录** - 在资料库中找不到 PKGCATALOG.Z。请尝试使用网络协议下载这个文件。如果该文件无法下载，请执行复制或获取任务 （这取决于资料库的类型）。
- **-601：下载文件失败** - 资料库无法访问。请尝试使用网络协议下载这个文件。如果无法下载该文件，请验证路径和用户权限。如果下载了该文件，请尝试停止并启动这项服务。
- **-602：上传文件失败** - 您执行了一个获取任务，但主资料库证书或设置无效（或者找不到位置）。请验证证书和位置。
- **-804：找不到 Sit 状态** - 您执行了一个复制任务，但主资料库不可用（或者证书无效）。请确保主资料库处于活动状态并可以访问，而且证书有效。
- **-1113: 只复制了一部分** - 一个或多个资料库在复制过程中无法访问。因此，并非所有资料库都是最新的。请确保所有资料库都可以访问，而且没有任何文件被标记为只读，然后再次执行这项任务。

词汇表

.MSI 文件
一种 Microsoft Windows Installer 软件包，包括要部署的软件的安装和配置说明。

.NAP 文件
Network Associates 软件包文件。这个文件扩展名指定了软件资料库中安装的 McAfee 软件程序文件，以便供 ePolicy Orchestrator 管理。

AVERT
即防病毒紧急响应小组，作为 Network Associates, Inc. 的防病毒研究部门，它通过研究最新的病毒威胁并查明将来可能出现的威胁来为计算机用户和 Network Associates 客户提供支持。它由三个负责提供防病毒服务和支持、病毒分析和高级病毒研究的综合团队组成。

DAT 文件
病毒定义文件，它使防病毒软件能够识别病毒以及文件中嵌入的有害代码。

另请参阅 EXTRA.DAT 文件、增量 DAT 文件和 SuperDAT。

EICAR
欧洲防计算机病毒研究机构开发了一个字符串，可以用来测试防病毒软件的安装和运行是否正确。

ePolicy Orchestrator 代理程序
ePolicy Orchestrator 服务器和防病毒产品及安全产品之间的一种智能链接。它负责收集和报告数据、执行策略和任务、安装产品、在客户机上执行策略和任务，并将事件发送回 ePolicy Orchestrator 服务器。

ePolicy Orchestrator 服务器
一个资料库，用来存放从分布式 ePolicy Orchestrator 代理程序收集的所有数据。它包括一个数据库，负责不断收集与网络中客户机上的产品操作有关的数据；一个用来生成报告的引擎，负责监控贵公司的病毒防护性能；以及一个软件资料库，用来存储要在您的网络中部署的产品和产品更新。

ePolicy Orchestrator 控制台
查看所有病毒活动和状态的一种方式，可以用来管理和部署代理程序及产品。使用 ePolicy Orchestrator 控制台，您可以设置防病毒和安全策略并对客户机上的所有代理程序或选定的计算机实施，也可以使用它的任务计划功能对特定的计算机或组应用计划任务和策略，还可以查看和自定义报告以监控部署情况、病毒发作和当前的保护水平。

EXTRA.DAT 文件
补充的病毒定义文件，它是针对新病毒或现有病毒新变种的发作而创建的。

另请参阅 DAT 文件、增量 DAT 文件和 SuperDAT。

FRAMEPKG.EXE
代理程序安装包。当执行时，该文件会将 ePolicy Orchestrator 代理程序安装到客户机中。

Lost&Found 组
ePolicy Orchestrator 服务器上用来存储那些无法确定其 “**目录**” 位置的计算机的位置。服务器使用 IP 管理设置、计算机名称、域名和站点名称或组名称来确定这些计算机的位置。只有全局管理员能够完全访问全局 **Lost&Found**，站点管理员只能访问他们有权访问的站点中的 **Lost&Found** 组。

McAfee AutoUpdate Architect
一个 McAfee Security 软件，与 ePolicy Orchestrator 配合使用时可以在企业内部署产品和产品更新。

SPIPE
即受保护的 PIPE，是 ePolicy Orchestrator 服务器使用的一种受保护的通讯协议。

SuperDAT
一个实用程序，负责安装更新后的病毒定义 (SDAT*.EXE) 文件并在必要时升级扫描引擎。

另请参阅 DAT 文件、 EXTRA.DAT 文件和增量 DAT 文件。

UTC 时间
全球统一时间 (UTC)。指本初子午线或格林威治子午线上的时间。

VirusScan Enterprise 控制台
用来控制程序活动的控制点。

“获取”任务
请参阅 “资料库获取”服务器任务。

“资料库复制”服务器任务
一项用来更新全局分布式资料库和超级代理程序分布式资料库的任务，它为主资料库中所有分支内的软件包保留了相同的副本。您还可以更新所选的分布式资料库。

“资料库获取”服务器任务
这项任务指定了源资料库或备用资料库，以便从这些库中获取软件包，然后将这些软件包与主资料库中指定的分支整合。

按访问扫描
对使用中的文件进行检查，以判断它们是否感染了病毒或其他可能有害的代码。它会在从磁盘中读取文件和 / 或向磁盘写入文件时发生。

与按需扫描相对。

按需扫描
按计划对所选的文件进行检查，以判断是否感染了病毒或其他可能有害的代码。它可以立即运行、在计划的某个未来时间运行或者按计划的时间间隔运行。

与按访问扫描相对。

备用资料库
当资料库列表 (SITELIST.XML) 中的资料库都不可用时，客户机会从这个资料库中获取更新。只能定义一个备用资料库。

本地分布式资料库
只能从客户机访问的位置，例如映射的驱动器或者其地址只能从本地 DNS 服务器解析的 FTP 服务器。本地分布式资料库在所选客户机的代理程序策略中定义。

病毒定义 (DAT) 文件
请参阅 DAT 文件。

病毒扫描引擎
使扫描进程能够得以运行的机制。

病毒
一种程序，能够在用户很少干预或不干预的情况下复制，而且复制的程序还能够进一步复制。

补充的病毒定义文件
请参阅 EXTRA.DAT 文件。

部署
为组、计算机及用户发送和安装产品 （以及代理程序）。

策略继承
决定 “**目录**”下的任何控制台树项目的策略设置是否直接从上一级的项目中获得。

策略
可以通过 ePolicy Orchestrator 管理的每个产品的配置设置，这些设置决定了客户机上的产品如何运行。

与任务相对。另请参阅代理程序策略。

策略实施间隔
决定了代理程序每隔多长时间执行一次从 ePolicy Orchestrator 服务器收到的策略。策略会在本地执行，因此这个时间间隔没有任何带宽要求。

策略页
ePolicy Orchestrator 控制台的一部分，您可以使用它们来设置策略并为产品创建计划任务。它们存储在个别的 ePolicy Orchestrator 服务器 （它们不会添加到主资料库中）上。

产品部署客户端任务
一个计划的任务，它可以将当前登记到主资料库中的所有产品一次性部署完毕。您可以通过这项任务将产品的安装和删除安排在非高峰期或策略实施间隔期间。

常用 Framework
一种常见的核心技术架构，它允许各种 McAfee Security 产品共享某些常用的组件和代码。这种架构称为常用 Framework。计划程序、自动更新和 ePolicy Orchestrator 代理程序组件是常用 Framework 中的常见组件。

超级代理程序分布式资料库
主资料库的一个副本，用来替代全局分布式资料库使用的专用服务器。

超级代理程序唤醒呼叫
一种计划的任务或按需命令，它会在必要时提示超级代理程序（以及每个超级代理程序所在子网中的所有代理程序）与 ePolicy Orchestrator 服务器联系，而不是等待下一个 ASCI。

另请参阅代理程序唤醒呼叫。

超级代理程序
一种代理程序，能够使用超级代理程序唤醒呼叫联系超级代理程序所在子网中的所有代理程序。您可以使用它来执行全局更新并支持分布式软件资料库，从而减少对专用服务器的依赖。通过采用发送代理程序唤醒呼叫这种方法，它有效节约了带宽。

另请参阅 ePolicy Orchestrator 代理程序。

出站扫描
与入站扫描相对。

窗格
控制台的一小部分。

请参阅详细资料窗格和控制台树。

存档文件
一种压缩文件，要访问它包含的文件，必须首先将其解压缩。

代理程序策略
影响代理程序行为的设置。

代理程序唤醒呼叫
一种计划的任务或按需命令，它会在必要时提示代理程序与 ePolicy Orchestrator 服务器联系，而不是等待下一个 ASCI。

另请参阅超级代理程序唤醒呼叫。

代理程序监视器
一个对话框，用来提示代理程序向 ePolicy Orchestrator 服务器发送属性或事件、在本地实施策略和任务、检查 ePolicy Orchestrator 服务器上是否有新的或更新后的策略和任务并在收到这些策略和任务之后立即实施。

代理程序
请参阅 ePolicy Orchestrator 代理程序。

代理程序与服务器通讯间隔 (ASCI)
决定代理程序与 ePolicy Orchestrator 服务器交换信息的频率。

代理程序与服务器通讯
一种通讯技术，使用这种技术，代理程序可以按预先定义的时间间隔联系服务器，以查看是否有新的策略或任务需要实施或执行。

代理程序主机
请参阅客户机。

单向扫描
即用一个设备负责入站扫描，用另一个设备负责出站扫描。

低风险进程
在 VirusScan Enterprise 中，这些进程是 McAfee Security 认为不太可能感染病毒的进程。例如：

备份软件。

代码编译程序 / 链接程序进程。

另请参阅默认进程和低风险进程。

防病毒策略
请参阅策略。

防火墙
一个程序，在您的计算机和网络或 Internet 之间起着过滤器的作用。它可以扫描到达您计算机的所有通讯 （入站通讯）以及您的计算机发出的所有通讯 （出站通讯）。它会深入到数据包这一级扫描通讯，并根据您设置的规则阻塞或允许它。

非活动代理程序
在指定的时间段内未与 ePolicy Orchestrator 服务器通讯的代理程序。

分布式软件资料库
用来在企业内部署产品和产品更新的一种架构，它会在主资料库中为支持的产品和产品更新创建一个中心库。

服务器任务
服务器为维护 ePolicy Orchestrator 数据库和 **“资料库”** 而执行的任务。默认的服务器任务包括 **“非活动代理程序维护”**、**“获取资料库”**、**“复制资料库”** 以及 **“同步域”**。

复制任务
请参阅 “资料库复制”服务器任务。

高风险进程
在 VirusScan Enterprise 中，这些进程是 McAfee Security 认为很可能感染病毒的进程。例如：

可以启动其他进程的进程。例如 Microsoft Windows 资源管理器或者命令提示符。

可执行的进程。例如 WINWORD 或 CSCRIPT。

可执行 Internet 下载的进程。例如浏览器、即时通讯程序和邮件客户端软件。

另请参阅默认进程和低风险进程。

隔离
强制孤立某个文件或文件夹以防止受到病毒感染。VirusScan Enterprise 会隔离感染病毒的文件或文件夹，直至可以清除病毒或删除感染病毒的项目。

更新包
来自 Network Associates 的软件包文件，用来为某个产品提供更新。所有软件包都被视为产品更新，但本产品的二进制 （安装程序）文件除外。

更新
将更新安装到现有产品或者升级到新版本产品的过程。

更新站点
一种资料库，您可以从中获取产品或 DAT 更新。

另请参阅下载站点。

宏病毒
一种会在不经意间执行的恶意宏 （宏是指为在某些应用程序或系统中自动执行任务而创建并保存的一组指令），从而自我复制或造成破坏。

后台扫描
一种按访问扫描， Microsoft 的 API2 使它成为可能，这种扫描不会扫描被访问的每个文件，因此能够在扫描程序繁忙时降低它的工作负荷。它会扫描自己所在的数据库，例如邮箱存储位置和公共文件夹存储位置。

集中警报
除常规警报管理器以外的另一种警报方式。可以将防病毒软件 （例如 VirusScan Enterprise 7.0）生成的警报消息保存在服务器上的一个共享文件夹中。警报管理器被配置为从这个文件夹读取警报通知。共享文件夹中的内容如果发生变化，警报管理器将按事先配置的警报方式 （例如向寻呼机发送电子邮件消息）发送新警报通知。

计算机
网络中的物理计算机。

继承
请参阅任务继承和策略继承。

节点
请参阅控制台树项目。

警报
与计算机活动 （例如病毒检测）有关的消息或通知。它可以按预先定义的配置通过电子邮件、寻呼机或电话自动发送给系统管理员和用户。

警告优先级
出于通知目的而为每条警报消息分配的值。可以为警报消息分配的优先级包括 “关键”、“主要、“次要”、“警告”或 “信息”。

镜像分布式资料库
客户机上的一个本地目录，它是通过 “**镜像**”客户端任务被复制的，其他客户机可以从它这里获取更新。

镜像任务
一种任务，它可以将资料库列表中第一个资料库的内容复制到您指定的客户机本地目录中。

拒绝服务攻击
一种攻击方式，它会影响计算机、服务器或网络对合法连接请求的响应。拒绝服务攻击会用错误的连接请求对目标进行攻击，从而导致目标忽略合法的请求。

客户端任务
在客户机上执行的任务。

客户机
在程序客户端一侧的计算机。

安装有 ePolicy Orchestrator 代理程序的计算机。

控制台树
控制台的左侧窗格，其中包含所有的控制台树项目。

控制台树项目
控制台树中的每个项目。

垃圾邮件
未经请求而收到的不受欢迎的所有电子邮件，包括商业电子邮件、近乎宣传资料的商业邮件以及不需要的非商业电子邮件，例如欺骗性病毒、玩笑程序和连锁邮件。

默认进程
在 VirusScan Enterprise 中，没有被定义为低风险进程或高风险进程的任何进程。

另请参阅高风险进程和低风险进程。

目录
列出了要通过ePolicy Orchestrator管理的所有计算机，并可以链接到主界面以便管理这些计算机。

频率
您要安排任务重复运行的时间间隔。

启发式分析，启发式
一种扫描方式，通过查找类似病毒的特征或活动来检测新病毒或以前没发现过的病毒。

强制安装，强制卸载
请参阅产品部署客户端任务。

全局报告设置
影响所有 ePolicy Orchestrator 数据库服务器、报告和查询的报告设置。

全局分布式资料库
主资料库中的软件包的相同副本。

全局更新
部署产品更新的一种方法，在将相应的软件包登记到主资料库中之后立即进行。软件包将被立即复制到所有超级代理程序和全局分布式资料库中， ePolicy Orchestrator 服务器向所有超级代理程序发送一个唤醒呼叫，超级代理程序向同一子网中的所有代理程序广播唤醒呼叫，之后所有代理程序从最近的资料库获取更新。

全局管理员
一个具有读写和删除权限的用户帐户，有权进行各种操作。可能对整个安装造成影响的操作只为全局管理员用户帐户而保留。

与站点管理员和全局审阅者相对。

全局审阅者
一个具有只读权限的用户帐户。全局审阅者可以查看软件中的所有设置，但无权更改这些设置。

与站点审阅者和全局管理员相对。

任务
被安排在特定时间或按指定时间间隔运行的一种操作，既包括一次性的按需扫描等操作，也包括日常更新等操作。

与策略相对。

任务继承
决定为 “**目录**”下的任何控制台树项目安排的客户端任务是否直接从上一级的项目中获得。

日志
McAfee 防病毒软件组件的活动记录。日志文件会记录安装、扫描或更新任务过程中采取的措施。

另请参阅事件。

蠕虫
一种病毒，通过在其他驱动器、系统或网络中自我复制进行传播。

入站扫描
与出站扫描相对。

软件包
包含二进制文件、检测功能、安装脚本以及一个用来安装产品和产品更新的软件包目录 (PKGCATALOG.Z) 文件。

软件包目录文件
一个包含每个更新包详细信息的文件 (PKGCATALOG.Z)，这些信息包括要更新的产品名称、语言版本以及安装的关联性。

软件包签名及安全
一个能够确保软件包是由 Network Associates 创建和发放的签名验证系统。软件包都用 DSA（数字签名算法）签名验证系统密钥对进行了签名，并使用 168 位 3DES 加密技术进行了加密。密钥用来加密或解密敏感数据。

扫描操作
在发现感染病毒的文件时执行的操作。

扫描
对文件进行检查，以判断是否感染了病毒或其他可能有害的代码。

请参阅按访问扫描和按需扫描。

上部详细资料窗格
控制台上半部分的详细资料窗格，其中包含 “**策略**”、“**属性**”和 “**任务**”选项卡。

另请参阅详细资料窗格和下部详细资料窗格。

实时扫描
请参阅按访问扫描。

事件
由支持的产品生成，可以识别客户机上从服务事件到病毒检测事件的各种活动。每个事件都被指定了一个介于“信息”和“关键”之间的严重程度。事件和属性包括在报告和查询中出现的数据。

属性
属性是某个对象的特性或特征，用来确定对象的状态、外观或值。

随机选择
您为计划任务设置的时间间隔内的一个随机时间点。

特洛伊木马程序
一种伪装成具有或自称具有一组有用功能或令人想要的功能、但实际包含破坏性内容的程序。特洛伊木马程序不会复制，因此从技术角度而言它们并非病毒。

玩笑程序
一种不会复制的程序，可能会警告或骚扰最终用户，但不会实际破坏任何文件或数据。

完全复制

与增量复制相对。

无提示安装
一种安装方法，在不显示任何提示、无需用户参与的情况下将软件包安装到计算机中。

系统扫描
对指定的系统进行的扫描。

下部详细资料窗格
控制台下半部分的详细资料窗格，它为上部详细资料窗格中“**策略**”选项卡上列出的产品显示了配置设置。

另请参阅详细资料窗格和上部详细资料窗格。

下载站点
一个资料库，您可以从中获取产品或 DAT 更新。

另请参阅更新站点。

详细资料窗格
控制台的右侧窗格，其中显示了当前选定的控制台树项目的详细信息。根据选定的控制台树项目，详细资料窗格可以分为上下两个窗格。

另请参阅上部详细资料窗格和下部详细资料窗格。

项目
请参阅控制台树项目。

选择性更新
指定您希望客户机获取哪个版本 （“**评估版**”、“**最新版**”还是 “**早期版本**”）的更新。

压缩的可执行文件
压缩的可执行文件在运行时只将自己解压缩到内存中。压缩的可执行文件永远不会解压缩到磁盘中。

用户帐户
ePolicy Orchestrator 用户帐户包括全局管理员、全局审阅者、站点管理员以及站点审阅者。管理员级的用户帐户具有读写和删除权限，审阅者级的用户帐户具有只读权限。

另请参阅全局管理员、全局审阅者、站点管理员和站点审阅者。

源资料库
主资料库要从中获取软件包的那个位置。

远程控制台
在没有安装 ePolicy Orchestrator 服务器的那些计算机上运行的控制台。远程控制台允许多个人员访问服务器并查看操作或者管理站点和安装。

另请参阅 ePolicy Orchestrator 控制台。

增量 DAT 文件
用来补充当前安装的病毒定义的新病毒定义。允许更新实用程序只下载最新的 DAT 文件，而不是整个 DAT 文件集。

另请参阅 DAT 文件、 EXTRA.DAT 文件和 SuperDAT。

增量复制
与完全复制相对。

站点管理员
一个对控制台中指定站点及其所有组和计算机具有读写和删除权限的用户帐户，有权进行各种操作 （但只限于全局管理员执行的那些操作除外）。

与全局管理员和站点审阅者相对。

站点
控制台树中为便于管理而组合起来的一个逻辑实体集合。站点可以包含组或计算机，并可以按 IP 地址范围、 IP 子网掩码、位置、部门和其他方法进行组织。

站点审阅者
一个具有只读权限的用户帐户。站点审阅者可以查看的设置与站点管理员相同，但无权更改这些设置。

与全局审阅者和站点管理员相对。

主机
请参阅客户机。

主资料库

ePolicy Orchestrator 服务器，它为源资料库中的软件包保留了原始副本，可以将这些软件包复制到分布式资料库中。在主资料库这一级，您可以登记产品和产品更新包、计划一些任务以便将软件包复制到全局分布式资料库或超级代理程序分布式资料库中，也可以计划一些任务以便从源资料库或备份资料库获取软件包，并将它们与主资料库集成。

资料库列表

即 SITELIST.XML 文件，采用了自动更新 7.0 的 McAfee 防病毒产品会使用这个文件来访问分布式资料库并从中获取软件包。

资料库

一个负责存储用来管理产品的策略页的位置。

自动更新

McAfee Security 防病毒产品中的自动更新程序，它会自动将更新安装到现有产品或者升级到新版本产品。

组

控制台树中为便于管理而组合起来的一个逻辑实体集合。组可以包含其他组或计算机。您可以为组指定 IP 地址范围或 IP 子网掩码，以便按 IP 地址对计算机排序。如果通过导入一个 Windows NT 域创建了一个组，您可以自动将代理程序安装包发送给这个域中导入的所有计算机。

索引

A

按访问扫描
- 病毒检测，响应， 72
- 活动日志，查看， 72
- 配置， 36
  - 报告属性， 43
  - 操作属性， 53, 68
  - 常规属性， 39
  - 高级属性， 51, 66
  - 检测属性， 48, 59
  - 进程属性
    - 低风险， 46, 55
    - 高风险， 46, 55
    - 默认， 46 到 47
    - 指定风险， 55
  - 消息属性， 41
- 扫描统计信息，查看， 71
- 消息，查看， 74

按访问扫描与按需扫描的比较， 31
安全注册表， 229 到 235
按需扫描
- 病毒检测，响应， 100
- 活动日志，查看， 100
- 任务
  - 创建， 78
    - 从“开始”菜单， 78
    - 从控制台， 80
    - 从系统任务栏， 78
  - 计划， 95
  - 可恢复的扫描， 98
  - 配置， 81
    - 报告属性， 93
    - 操作属性， 90
    - 高级属性， 88
    - 检测属性， 86
    - 扫描位置属性， 82
  - 运行
    - 从 Windows 命令行中， 224
    - 从控制台， 96
    - 停止， 97
    - 暂停， 97
    - 重新启动， 97
- 扫描统计信息，查看， 99

按需扫描与按访问扫描的比较， 31
安装 （请参阅 《安装指南》）
安装问题，故障排除， 239
AVERT （防病毒紧急响应小组），联系， 12

B

“帮助”菜单， 21
报告属性，配置
- 按发送电子邮件扫描， 117
- 按访问扫描， 43
- 按需电子邮件扫描， 132
- 按需扫描， 93

本版本的新功能， 14
本手册读者， 9
本手册中使用的排版规范， 10
“编辑”菜单， 21
变量，系统， 171

病毒
常见问题， 240
检测
按访问扫描， 72
按需扫描， 100
提交样本， 33
病毒，提交样本， 12
病毒信息库， 12, 33

C

.CAB，扫描具有扩展名的文件， 224
菜单
开始， 18
在 VrusScan 控制台中， 20
帮助， 21
编辑， 21
工具， 21
任务， 20
视图， 21
右键单击， 24
菜单栏， 20
参数，适用于按需扫描程序， 224
CATALOG.Z 文件， 178
测试程序，联系， 12
测试警报配置， 143
常规设置属性，按访问扫描， 39
常规问题，故障排除， 241
常见问题 (FAQ)， 238
产品功能， 15
产品培训，联系， 12
产品文档， 11
重新启动按需扫描任务， 97
词汇表， 245
存档文件，扫描， 224

D

DAT 文件
回滚， 195
DAT 文件更新，网站， 12
电子邮件，发送病毒警报， 150
电子邮件扫描，按发送
活动日志，查看， 120
任务，配置， 106
报告属性， 117
操作属性， 112
高级属性， 109
检测属性， 107
警报属性， 114
扫描统计信息，查看， 119
电子邮件扫描，按需
活动日志，查看， 136
任务，配置， 121
报告属性， 132
操作属性， 127
高级属性， 124
检测属性， 121
警报属性， 130
任务，运行， 135
低风险进程， 46, 55
定义， 55

E

EXTRA.DAT， 169, 178

F

FAQ（常见问题）， 238
FTP 默认下载站点， 179, 184, 196
服务门户网站， PrimeSupport， 12

G

高风险进程， 46, 55
定义， 55
隔离文件夹
按发送电子邮件扫描， 113
按访问扫描， 40
按需电子邮件扫描， 129
按需扫描， 91
更新
策略， 170
错误代码， 244
代理服务器设置， 187
活动， 178
镜像任务， 191

任务
配置， 174
运行
可恢复的更新， 176
立即更新， 176
手动， 196
下载站点， 179
FTP 默认下载站点， 179, 184, 196
HTTP 默认下载站点， 179, 184
资料库列表， 179
编辑资料库， 181
删除和重新组织资料库， 186
更新时使用的代理服务器设置， 187
“工具”菜单， 21
工具栏， 22
功能，描述， 15
广播网络消息， 148
关机时扫描软盘
使用按访问扫描， 39
故障排除， 237
常见问题
安装， 239
病毒， 240
常规， 241
扫描， 240
更新错误代码， 244
最小扩展工具， 238

H

HTTP 默认下载站点， 179, 184
会话设置，记录在日志文件中， 44, 94, 119, 134
会话摘要，记录在日志文件中， 44, 94, 119, 134
活动日志
按发送电子邮件扫描， 120
按访问扫描， 72
按需电子邮件扫描， 136
按需扫描， 100
镜像任务， 194
自动更新任务， 178
获取信息， 11

J

检测，病毒
按访问扫描
采取措施， 75
接收通知， 73
消息，查看， 74
按需扫描
采取措施， 102
接收通知， 101
截短警报消息，强制， 153
解锁用户界面， 29
计划， 199
高级选项， 204
计划属性， 202
频率， 203
启用随机选择， 206
任务
按需扫描， 95
拨号时运行， 215
登录时， 211
镜像， 193
空闲时， 213
立即运行， 214
每天， 205
每月， 208
每周， 207
系统启动时， 211
一次， 209
自动更新， 176
任务属性， 201
警报方式
配置接收者， 142
警报管理器
“摘要”页， 145
配置
SNMP， 155
打印的消息， 154
电子邮件警报， 150
启动程序， 156
网络广播， 148
转发警报， 145
系统变量， 166
警报管理器属性
摘要， 145
警报文件夹

功能， 162
警报消息
编辑， 166
变量， 167
电子邮件， 150
发送到打印机， 154
广播网络警报， 148
集中警报， 162
截短， 153
禁用， 164
启动程序以响应， 156
启用， 164
通过 SNMP 陷阱发送， 155
转发， 145
自定义， 163
警报优先级
更改， 164
类型， 165
镜像任务， 189
创建， 190
活动日志，查看， 194
计划， 193
配置， 191
运行， 193
按计划， 193
从“启动”命令， 193
立即， 193
使用“立即镜像”， 194
集中警报， 162
技术支持， 12

K

“开始”菜单， 18
客户服务，联系， 12
可恢复的扫描， 98
KnowledgeBase 搜索， 12
控制台（请参阅 VirusScan 控制台）

L

连接到远程服务器， 34
“立即更新”命令， 177
“立即镜像”命令， 194
.LZH，扫描具有扩展名的文件， 224

M

McAfee Security 大学，联系， 12
MERTool（最小扩展工具）， 238
密码选项， 28
命令行， Windows， 26
选项， 218
运行按需扫描程序， 224
默认进程， 46 到 47

P

排除文件、文件夹和驱动器（使用“排除”功能）， 64
培训网站， 12
配置
按发送电子邮件扫描， 106
按访问扫描， 35
按需电子邮件扫描， 121
按需扫描， 78
镜像任务， 190
通过 ePolicy Orchestrator（请参阅配置指南）
自动更新任务， 174
PrimeSupport， 12

Q

启动，扫描， 40
启用随机选择， 206

R

“任务”菜单， 20
任务
定义， 23
可以在 VirusScan Enterprise 中使用的类型， 23
立即运行， 96
配置
按发送电子邮件扫描程序， 106
按访问扫描程序， 35
按需电子邮件扫描程序， 121
按需扫描程序， 78
镜像任务， 190
自动更新任务， 174
停止， 97
暂停， 97
重新启动， 97

任务列表， 23
日期和时间，记录在日志文件中， 44, 94, 119, 134
日志文件
    按发送电子邮件扫描， 120
    按访问扫描， 72
    按需电子邮件扫描， 136
    按需扫描， 100
    镜像任务， 194
    自动更新任务， 178
日志文件大小
    限制， 44, 94, 118, 133
入门， 17

S

“扫描”菜单
    统计信息， 120
扫描
    Shell 扩展扫描， 25
    按发送电子邮件， 106
    按访问， 35
    按访问扫描与按需扫描的比较， 31
    按计划， 32
    按需， 78
    按需电子邮件， 121
    操作
        按计划， 32
        定期， 32
        设置， 31
        选择性， 32
        自动， 32
    定期， 32
    故障排除问题， 240
    结果，查看
        按发送电子邮件扫描
            活动日志， 120
            统计信息， 119
        按访问扫描
            活动日志， 72
            统计信息， 71
        按需电子邮件扫描活动日志， 136
        按需扫描
            活动日志， 100
            统计信息， 99
        镜像任务活动日志， 194
        自动更新活动日志， 178
    立即， 96
    配置
        按发送电子邮件扫描程序， 106
        按访问扫描程序的， 35
        按需电子邮件扫描程序， 121
        按需扫描程序， 78
    选择性， 32
    右键扫描， 25
        系统任务栏， 25
    自动， 32
扫描，事先计划的， 32
“扫描”菜单
    统计信息， 71 到 72
扫描时间
    按访问扫描， 40
Security HQ，与 AVERT 联系， 12
升级网站， 12
“视图”菜单， 21
手册， 11
术语定义（请参阅词汇表）
SMTP 邮件服务器，配置电子邮件警报， 152
SNMP
    发送警报，通过， 155
锁定用户界面， 29
锁定注册表， 229 到 235

T

添加文件类型扩展名（使用“其他”功能）， 62
提交病毒样本， 12
统计信息，查看

按发送电子邮件扫描， 119
按访问扫描， 71
按需扫描， 99
统计信息，在 “扫描”菜单中， 71 到 72, 120

U

UTC 全球统一时间 (UTC)， 206
.UUE，扫描具有扩展名的文件， 224

V

VirusScan Enterprise
本版本的新功能， 14
产品功能， 15
VirusScan 控制台， 19
菜单 （请参阅菜单）
工具栏， 22
连接到远程服务器，通过， 34
配置
按发送电子邮件扫描，通过 （请参阅电子邮件扫描，按发送）
按访问扫描，通过 （请参阅按访问扫描）
按需电子邮件扫描，通过 （请参阅电子邮件扫描，按需）
按需扫描，通过 （请参阅按需扫描）
镜像任务，通过 （请参阅镜像任务）
自动更新，通过 （请参阅自动更新）
任务列表， 23
状态栏， 24
VirusScan 控制台中的任务列表， 23

W

为发送的消息设置优先级
到其他计算机， 144
通过网络， 148, 150, 153, 155 到 156, 158, 160 到 161
文件类型扩展名，扫描内容
排除文件类型 （使用 “排除”功能）， 64
添加文件类型 （使用 “其他”功能）， 62
添加用户指定的类型 （使用 “指定项”功能）， 63

X

下载网站， 12
显示选项， 27
限制日志文件大小， 44, 94, 118, 133
消息，按访问扫描， 41
查看， 74
从列表中删除消息， 42
断开远程用户， 42
拒绝访问网络共享， 42
清除所提及的文件感染的病毒， 42
删除所提及的感染病毒的文件， 42
显示消息对话框， 41
向用户发送消息， 42
要显示的文字， 41
移动所提及的感染病毒的文件， 42
新功能， 14
系统变量， 171
系统变量，警报， 166
系统启动，扫描， 40
系统任务栏，设置选项， 25

Y

压缩文件
从命令行扫描
存档类型， 224
引导区
从命令行扫描， 219
使用按访问扫描， 39
使用按需扫描， 83
用户界面
面向， 18
选项
解锁， 29
密码， 28
设置， 26
锁定， 29
显示， 27
用户名，记录在日志文件中， 44, 94, 119, 134
右键菜单， 24
邮件服务器，配置电子邮件警报， 152
右键扫描， 25
系统任务栏， 25
优先级，为警报设置， 144
与 McAfee Security 联系， 12
远程管理， 34
远程连接，在 “工具”菜单中， 34

Z

暂停按需扫描任务， 97
指定文件类型扩展名 （使用 “指定项”功能）， 63
转发警报
    大型公司， 146
    小型公司， 147
状态栏， 24
注册表，安全， 229 到 235
自动更新
    错误代码， 244
    代理服务器设置， 187
    活动日志，查看， 178
    任务
        创建， 174
        更新过程概述， 173
        更新过程中的活动， 178
        计划， 176
        配置， 174
        运行， 176
            从 “开始”菜单， 177
            从控制台， 176
            可恢复的更新， 176
            立即更新， 176
            使用 “立即更新”， 177
    实施 （请参阅 《VirusScan Enterprise 更新实施指南》）
    说明， 172
    下载站点， 179
        FTP 默认下载站点， 179, 184, 196
        HTTP 默认下载站点， 179, 184
    资料库列表， 179
        编辑资料库， 181
        导入资料库， 180
        删除和重新组织资料库， 186
        添加资料库， 181
自动扫描， 32
资料库， 186
资料库列表
    编辑资料库， 181
    导入资料库， 180
    删除和重新组织资料库， 186
    添加资料库， 181
.ZIP，扫描具有扩展名的文件， 224
最小扩展工具 (MERTool)， 238