# Symantec<sup>™</sup> Endpoint Protection 及 Symantec Network Access Control 管理 指南



# Symantec<sup>™</sup> Endpoint Protection 和 Symantec Network Access Control

本手册介绍的软件基于授权许可协议提供,且只能在遵守协议条款的前提下使用。

文档版本 11.00.03.00.00

#### 法律声明

Copyright © 2008 Symantec Corporation. © 2008 年 Symantec Corporation 版权所有。All rights reserved. 保留所有权利。

Symantec、Symantec 徽标、LiveUpdate、Sygate、Symantec AntiVirus、Bloodhound、 Confidence Online、Digital Immune System、Norton 和 TruScan 是 Symantec Corporation 或其附属公司在美国和其他国家/地区的商标或注册商标。"Symantec"和"赛门铁克"是 Symantec Corporation 在中国的注册商标。其他名称可能为其各自所有者的商标,特此声明。

本 Symantec 产品可能包括 Symantec 必须向第三方支付许可费的第三方软件("第三方程 序")。部分第三方程序是以开放源或免费软件许可方式获得的。本软件随附的许可证协议 并未改变这些开放源或免费软件许可所规定的任何权利或义务。请参见本文档"第三方版权 声明附录"或本 Symantec 产品随附的 TPIP ReadMe 文件,以获取有关第三方程序的详细信 息。

本文档中介绍的产品根据限制其使用、复制、分发和反编译/逆向工程的授权许可协议分发。 未经 Symantec Corporation(赛门铁克公司)及其特许人(如果存在)事先书面授权,不得 通过任何方式、以任何形式复制本文档的任何部分。

本文档按"现状"提供,对于所有明示或暗示的条款、陈述和保证,包括任何适销性、针对 特定用途的适用性或无侵害知识产权的暗示保证,均不提供任何担保,除非此类免责声明在 法律上视为无效。Symantec Corporation(赛门铁克公司)不对任何与提供或使用本文档相 关的伴随或后果性损害负责。本文档所含信息如有更改,恕不另行通知。

根据 FAR 12.212 中的定义,授权许可的软件和文档被视为"商业计算机软件",受 FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" (商业计算机软件受限权利)和DFARS 227.7202 "Rights in Commercial Computer Software or Commercial Computer Software Documentation" (商业计算机软件或商业计算机软件文档权利)中的适用规定,以及所有后续法规中规定的权利的制约。美国政府仅可根据本协议的条款对授权许可的软件和文档进行使用、修改、发布复制、执行、显示或披露。

Symantec Corporation 20330 Stevens Creek Blvd. Cupertino, CA 95014

http://www.symantec.com/region/cn

# 技术支持

赛门铁克技术支持具有全球性支持中心。技术支持的主要任务是响应有关产品特性和功能的特定查询。技术支持小组还负责为我们的联机知识库创建内容。技术支持小组与 Symantec 内的其他职能部门相互协作,及时解答您的问题。例如,技术支持小组与产品工程和 Symantec 安全响应中心协作,提供警报服务和病毒定义更新服务。

Symantec 提供的维护服务包括:

- 一系列支持服务, 使您能为任何规模的单位选择适用的支持服务
- 通过电话和 Web 支持快速响应并提供最新信息
- 升级保证可提供自动软件升级防护
- 全天候提供全球支持。
- 高级功能,包括"客户管理服务"

有关 Symantec 维护计划的更多信息,请访问我们的网站:

www.symantec.com/techsupp/

#### 与技术支持联系

具有有效维护协议的客户可以通过以下网址访问技术支持信息:

#### www.symantec.com/techsupp/

在联系技术支持之前,请确保您的计算机符合产品文档中所列的系统要求。此外, 您应当坐在发生问题的计算机旁边,以便需要时重现问题。

联系技术支持时,请准备好以下信息:

- 产品版本信息
- 硬件信息
- 可用内存、磁盘空间和 NIC 网卡信息
- 操作系统
- 版本和补丁程序级别
- 网络结构
- 路由器、网关和 IP 地址信息
- 问题说明:
  - 错误消息和日志文件
  - 联系 Symantec 之前执行过的故障排除操作

#### ■ 最近所做的软件配置更改和网络更改

#### 授权许可与产品注册

如果您的 Symantec 产品需要注册或许可证密钥,请访问我们的技术支持网页: www.symantec.com/techsupp/

## 客户服务

可从以下网站获得客户服务信息:

#### www.symantec.com/techsupp/

客户服务可帮助您解决以下几类问题:

- 有关产品许可或序列号的问题
- 产品注册更新(例如,更改地址或名称)
- 一般产品信息(功能、可用的语言、当地经销商)
- 有关产品更新和升级的最新信息
- 有关升级保证和维护合同的信息
- 有关 Symantec 购买计划的信息
- 有关 Symantec 技术支持选项的建议
- 非技术性的售前问题
- 与光盘或手册相关的问题

## 维护协议资源

如果想就现有维护协议事宜联络 Symantec,请通过以下方式联络您所在地区的维护协议管理部门:

亚太区和日本	contractsadmin@symantec.com	
欧洲、中东和非洲	semea@symantec.com	
北美洲和拉丁美洲	supportsolutions@symantec.com	

# 其他企业服务

Symantec 全面提供各种服务以使您能够充分利用您对 Symantec 产品的投资,并 拓展您的知识、技能和全球视野,让您在管理企业安全风险方面占据主动。 现有下列企业服务:

Symantec 预警解决方案	这些解决方案提供计算机攻击的预警、	全面的威胁分析以及防止攻击发生的应对
	措施。	

安全托管服务 这些服务消除了管理和监控安全设备和事件的负担,确保能够对实际威胁快速响 应。

咨询服务 Symantec咨询服务由 Symantec及其可信赖的合作伙伴提供现场专业技术指导。 Symantec咨询服务提供各种预先包装和可自定义的服务选项,其中包括评估、 设计、实施、监控和管理功能,每种功能都注重于建立和维护您的 IT 资源的完 整性和可用性。

#### 教育服务 教育服务提供全面的技术培训、安全教育、安全认证和安全意识交流计划。

要访问有关企业服务的更多信息,请通过以下 URL 访问我们的网站:

www.symantec.com

从站点索引选择您所在的国家/地区或所用的语言。



技术支持		4
部分1	基本管理任务	23
第1章	Symantec Endpoint Protection Manager 概述	25
	关于管理任务       2         登录 Symantec Endpoint Protection Manager 控制台       2         Symantec Endpoint Protection Manager 控制台的组织方法       2         主页       2         监视器页面       2         报告页面       3         策略页面       3         客户端页面       3         管理员页面       3	25 26 28 29 30 31 31 32 33
第2章	基本防护简介	35
	防护类别	35 36 37 37 38
第3章	管理组、客户端、用户和计算机	39
	关于组结构       4         关于默认组和子组       4         关于客户端安装软件包中指定的组       4         关于导入现有组织结构       4         添加组       4         重命名组       4         移动组       4         查看组的属性       4         关于组从其他组继承位置及策略       4         禁用与启用组的继承       4         关于添加到组的客户端       4	10 11 11 12 12 13 13 13 13 14 14

关于受管和非受管客户端	45
关于用户模式和计算机模式	45
以用户或计算机的形式添加客户端	46
在用户模式和计算机模式之间切换客户端	47
将非受管客户端转换为受管客户端	48
禁止各尸端添加至组	
任组间移动各尸瑜	
天丁各尸缅状态图标	
並示各尸缅和各尸缅汀昇机的状态	
值有各户项的属性	
过您哪些用户和打异机击现住。各户缅 匹坝下上	
投系用广、谷广垧和归昇饥的信息	
癿且各广圳位侧不冲以田 土王通讨坊制台五家户进上运行会会	
大丁迪过程前口任谷广缅上运行即マ	
管理域和管理员	59
关于域	59
添加域	
指定当前域	
关于管理员	
添加管理员帐户	63
关于访问权限	64
配置受限管理员访问权限	65
在管理员和受限管理员之间切换	66
在登录尝试太多次后,锁定管理员帐户	67
设置管理员帐户的验证	67
重命名管理员帐户	68
更改管理员的密码	68
删除管理员帐户	69
使田家白端安奘软件句	71
大丁各尸缅女装软件包	
配置各尸缅安装软件包选坝	
配直各尸场安装软件包切能	
即直各尸 <b>师</b> 女滚软件包 <b>以直</b>	
収集用尸信息	
守出各尸师女装软件包 住田 "本地北亚您儿您相"如果它已进步他	
使用"查找非受管计算机"	
天丁浴加各尸嗝安装软件包里新相井级各尸嗝	76

# 第5章

第4章

配置各尸즓安装软件包设置	
收集用户信息	73
导出客户端安装软件包	73
使用"查找非受管计算机"部署客户端软件	75
关于添加客户端安装软件包更新和升级客户端	
添加客户端安装软件包更新	
升级一个或多个组中的客户端	77
删除升级软件包	77

# 第6章

更新定义与内容
---------

关于内容类型	80
关于更新客户端与管理服务器的内容	81
关于内容分发方法	81
关于确定要使用何种内容分发方法	82
关于在 Symantec Endpoint Protection Manager 上存储内容修订	85
关于使用不是最新版本的内容修订	86
关于使用默认管理服务器更新客户端的内容	86
关于同时内容下载	86
配置下载内容更新的站点	87
关于 LiveUpdate 策略	89
配置 LiveUpdate 设置策略	89
配置 LiveUpdate 内容策略	90
查看和更改应用于组的自定义 IPS 策略	91
关于使用组更新提供者更新客户端的内容	92
配置组更新提供者	93
关于智能更新程序	94
使用智能更新程序下载要分发的防病毒内容更新	94
关于使用第三方分发工具将内容更新分发至受管客户端	95
使用 LiveUpdate 设置策略对受管客户端启用第三方内容分发	95
使用第三方分发工具将内容分发到受管客户端	96
关于使用第三方分发工具将内容更新分发给非受管客户端	97

# 第7章

# 

关于访问客户端接口	
锁定和解除锁定管理的设置	100
更改用户控制级别	101
关于混合控制	103
配置用户界面设置	103
使用密码保护客户端	105

# 第8章

# 

关于管理服务器	107
指定管理服务器列表	108
添加管理服务器列表	109
将管理服务器列表分配给组和位置	110
查看将管理服务器列表分配至的组和位置	110
编辑管理服务器列表的服务器名称和说明	111
编辑管理服务器列表中的管理服务器 IP 地址、主机名和端口号	111
更改管理服务器连接的顺序	112
替换管理服务器列表	113

复制和粘贴管理服务器列表	113
导出和导入管理服务器列表	113
配置位置的通信设置	114
使用 SylinkDrop 工具恢复客户端通信设置	115
报告基础篇	117
关工报生	110
大丁112日	110
入了芯可以色行的派音	119
大丁亚小日心神报日 ····································	120
10日 使用 数	120
大」內均十七次的事件	120
大丁可血红的日心	121
奶巴我自动能	121
示用四环地址时何平地工机与 II 地址相入状	122
大丁行 USL 马报日列祀 起使用	123
入了 Symance Endpoint Hotection 上页	123
<u>出重工买工印版百秋购入</u>	120
有田 Symantec Network Access Control 主面	120
同時時代的 L · · · · · · · · · · · · · · · · · ·	130
半千主页和近海器显示冼项	132
<b>了</b> 工火作血优丽亚尔达·贝 ···································	132
n111 (1)1111 (1)11111 (1)11111 (1)111111 (1)111111 (1)11111111	133
关于报告和日本中使用的客户端扫描时间	134
关于在报告和日本中使用过去 24 小时过滤器	134
关于在报告和日志中使用搜索组的讨滤器	135
	100
杳看和配置报告	137
	10.
关于查看报告	137
关于查看报告中的线条图	138
关于查看条形图	139
关于以业洲语言查看报告	139
关于报告	140
关于报告的重要须知	149
创建快速报告	150
保存和删除已保存的报告过滤器	153
天十重复的过滤器名称	154
打印和保存报告副本	154
创建和删除调度报告	155

I

第9章

第10章

# 第11章

关于减少发送至日志的事件量	175
导出日志数据	175
将日志数据导出到文本文件	176
将数据导出到 Syslog 服务器	178
将日志数据导出为逗号分隔文本文件	179
使用通知	179
查看和过滤管理员通知信息	179
用于管理员通知的阈值指南	180
创建管理员通知	180
关于编辑现有通知	184

# 第12章

# 

关于使用监视器和报告来帮助确保网络安全	185
关于应用程序控制与设备控制报告和日志中的信息	186
关于审核报告和日志中的信息	187
关于遵从性报告和日志中的信息	187
关于计算机状态报告和日志中的信息	189
关于网络威胁防护报告和日志中的信息	190
关于 TruScan 主动型威胁扫描报告和日志中的信息	192
关于风险报告和日志中的信息	192
关于扫描报告和日志中的信息	193
关于系统报告和日志中的信息	194
关于排除病毒和安全风险	196
标识受感染及有风险的计算机	196
更改操作并重新扫描标识出的计算机	197
重新启动需重新启动才能完成补救的计算机	197
更新定义并重新扫描	198
关于调查及清除残留的风险	198
清除可疑事件	198
查找脱机客户端	199

部分 2	高级管理任务	201
第13章	管理站点	203
	关于站点管理	203
	关于跨越不同公司站点的站点复制	204
	关于在站点选用 Enforcer	205
	关于远程站点	205
	编辑站点属性	205
	备份站点	206
	删除现性站员	207
第14章	管理服务器	209
	关于服务器管理	209
	关于服务器和第三方密码	209
	启动和停止管理服务器服务 授权或拒绝远程 Symantec Endpoint Protection Manager 控制台的访	210
	问	210
	删除所选服务器	212
	导出和导人服务器设置	212
第15章	管理目录服务器	215
	关于目录服务器的管理	215
	添加目录服务器	215
	同步目录服务器和 Symantec Endpoint Protection Manager 之间的用	
	户帐户	216
	关于从 LDAP 目录服务器导入用户和计算机帐户信息	217
	在 LDAP 目录服务器上搜索用户	217
	从 LDAP 日求服务益搜索结果列表守入用户	220
	大丁组织毕位和 LDAP 服务器	220
		221
	关于同步组织单位	221
第16章	管理电子邮件服务器	223
	关于管理电子邮件服务器	223
	建立 Symantec Endpoint Protection Manager 和电子邮件服务器之间	
	的通信	223

第17章	管理代理服务器	225
	关于代理服务器	225
	间的连接 设置 FTP 代理服务器与 Symantec Endpoint Protection Manager 之间 的连接	225 226
第18章	管理 RSA 服务器	227
	关于将 RSA SecurID 与 Symantec Endpoint Protection Manager 配合 使用的前提条件	227
	将 Symantec Endpoint Protection Manager 配置为使用 RSA SecurID 验证	 วาง
	为 Symantec Endpoint Protection Manager 管理员指定 SecurID 验	220
	证 配置管理服务器以支持 HTTPS 通信	229 229
第19章	管理服务器证书	231
	关于服务器证书类型 更新服务器证书	231 232
	备份服务器证书	233
	找出 Keystore 密码	234
体って主	找出 Keystore 密码	234
第 20 章	找出 Keystore 密码 管理数据库	234 235
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理	<ul><li>234</li><li>235</li><li>235</li></ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于数据库命名惯例	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>236</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         美于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于数据库备份	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>236</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于数据库备份         关于重新配置数据库	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>236</li> <li>237</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于数据库备份         关于重新配置数据库         备份 Microsoft SQL 数据库	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>236</li> <li>237</li> <li>238</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于数据库备份         关于重新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份	234 235 235 236 236 236 237 238
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于数据库备份         关于重新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库	234 235 235 236 236 236 237 238 238
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于数据库备份         关于重新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库         使用数据库维护向导备份 Microsoft SQL 数据库	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>236</li> <li>237</li> <li>238</li> <li>238</li> <li>239</li> <li>242</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于管理服务器配置向导与 Symantec Database Tools         关于数据库备份         关于重新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库         使用数据库维护向导备份 Microsoft SQL 数据库         从控制台按需备份嵌入式数据库         从 Symantec Endpoint Protection Manager 调度自动数据库备份	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>236</li> <li>237</li> <li>238</li> <li>238</li> <li>238</li> <li>238</li> <li>238</li> <li>239</li> <li>242</li> <li>242</li> <li>242</li> <li>242</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于電新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库         使用数据库维护向导备份 Microsoft SQL 数据库         从控制台按需备份嵌入式数据库         从 Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>236</li> <li>237</li> <li>238</li> <li>238</li> <li>239</li> <li>242</li> <li>242</li> <li>242</li> <li>243</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于管理服务器配置向导与 Symantec Database Tools         关于重新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库         使用数据库维护向导备份 Microsoft SQL 数据库         从控制台按需备份嵌入式数据库         从 Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库         在 Symantec Endpoint Protection Manager 控制台中编辑数据库的名	234 235 235 236 236 236 236 236 237 238 238 238 239 242 242 242 243
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于数据库备份         关于重新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库         使用数据库维护向导备份 Microsoft SQL 数据库         从控制台按需备份嵌入式数据库         从 Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库         本 Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库         Microsoft SQL 数据库         Mather Endpoint Protection Manager 调度自动数据库备份         还原数据库         Mather Endpoint Protection Manager 调度自动数据库备份         还原数据库         本 Symantec Endpoint Protection Manager 控制台中编辑数据库的名         称和说明	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>237</li> <li>238</li> <li>238</li> <li>239</li> <li>242</li> <li>242</li> <li>243</li> <li>245</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于重新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库         从控制台按需备份嵌入式数据库         从 Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库         在 Symantec Endpoint Protection Manager 控制台中编辑数据库的名         本和说明         重新配置 Microsoft SQL 数据库	234 235 235 236 236 236 237 238 239 242 242 242 243 245 245
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于電新配置数据库         备份 Microsoft SQL 数据库         人 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库         使用数据库维护向导备份 Microsoft SQL 数据库         从控制台按需备份嵌入式数据库         从Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库         在 Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库         在 Symantec Endpoint Protection Manager 控制台中编辑数据库的名         亦和说明         重新配置 Microsoft SQL 数据库         重新配置 Microsoft SQL 数据库	<ul> <li>234</li> <li>235</li> <li>235</li> <li>236</li> <li>236</li> <li>236</li> <li>237</li> <li>238</li> <li>239</li> <li>242</li> <li>242</li> <li>243</li> <li>245</li> <li>245</li> <li>247</li> <li>247</li> </ul>
第 20 章	找出 Keystore 密码         管理数据库         关于数据库的管理         关于数据库命名惯例         关于管理服务器配置向导与 Symantec Database Tools         关于電新配置数据库         备份 Microsoft SQL 数据库         从 Symantec Endpoint Protection Manager 控制台按需备份         Microsoft SQL 数据库         使用数据库维护向导备份 Microsoft SQL 数据库         从控制台按需备份嵌入式数据库         从 Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库         在 Symantec Endpoint Protection Manager 调度自动数据库备份         还原数据库         重新配置 Microsoft SQL 数据库         重新配置 Microsoft SQL 数据库         重新配置 Microsoft SQL 数据库         重新配置嵌入式数据库         关于管理日志数据         关于目 = 数据和在依区	234 235 235 236 236 236 237 238 237 238 238 239 242 242 242 242 242 242 245 245 247 248 248

从数据库手动清除日志数据	249
来自旧版客户端的日志数据	250
为站点中的服务器配置日志设置	250
关于配置事件汇总	250
配置客户端日志设置	251
关于配置防病毒和防间谍软件策略的客户端日志处理选项	252
备份站点日志	252
关于上传大量客户端日志数据	253
关于管理数据库中的日志事件	254
配置日志的数据库维护选项	254
关于使用 Interactive SQL 实用程序搭配嵌入式数据库	255
史改超时参数	255
关于在 64 位计算机上还原损坏的客户端系统日志	256
有判粉捉	257
乏п奴加	
关于数据的复制	257
关于复制的影响	259
关于复制的设置	259
复制期间如何合并更改	260
添加和断开复制伙伴	260
断开复制伙伴的连接	262
调度自动和按需复制	262
按需复制数据	
史改复制频举	
复制各尸缅软件包	
发刑口芯	
管理防算改	267
关于防篡改	
配置防暴改	268
当有各些专用方力	
吊规束略官埋仕穷	271
管理组的位置	273
<b>土</b> 干细的位置	273
入 J 组时世直	273 274
入」 医电冲巴里滤波 ····································	
关于组的默认位置	
启用客户端的策略自动分配	
使用向导添加位置	
不使用向导添加位置	
	从数据库手动清除日志数据         次封点中的服务器配置日志设置         关于配置事件汇总         配置客户端日志设置         关于配置防病毒和防间谍软件策略的客户端日志处理选项         备份站点日志         关于全配置防病毒和防间谍软件策略的客户端日志处理选项         备份站点日志         关于生作大量客户端日志数据         关于管理数据库中的日志事件         配置日志的数据库维护选项         关于使用 Interactive SQL 实用程序搭配嵌入式数据库         更改超时参数         关于使用 Interactive SQL 实用程序搭配嵌入式数据库         更改超时参数         关于使用 Interactive SQL 实用程序搭配嵌入式数据库         更改超时参数         关于复制的影响         美于复制的影响         关于复制的设置         复制期间如何合并更改         溶加和断开复制伙伴         断开复制伙伴的影响         更改复制频率         复制名力动称需复制         英言复制数据         更改复制频率         复制名力         更改复制频率         复制名户端软件包         复制日志         管理防篡改         常知 管 理 任 务         管理 的位置         关于组的应置         美于短 氧和位置感测         美于短 氧和位置         美丁 组的位置         美丁 组的方配         使用 合力量         广告 如 位置         黄田 位置         美丁 金 章         自动和位置         大丁 位置 和位置

	分配默认位置	278
	编辑组位置的名称和说明	279
	删除组的位置	279
第 24 章	使用策略	281
	关于策略	282
	关于共享和非共享策略	283
	关于添加策略	283
	添加共享策略	284
	在客户端页面中使用向导添加非共享策略	285
	在客户端页面中添加新的非共享策略	286
	在客户端页面中从现有策略添加新的非共享策略	287
	在客户端页面中从先前导出的策略文件添加新的非共享策略	287
	编辑策略	288
	分配共享策略	289
	撤回策略	289
	删除策略	290
	导出策略	291
	导入策略	292
	关于复制策略	292
	在策略页面中复制共享策略	292
	在客户端页面中复制共享或非共享策略	293
	粘贴策略	293
	复制和粘贴组策略	294
	替换策略	294
	将共享策略转换为非共享策略	295
	将共享策略的副本转换为非共享策略	296
	关于更新客户端的策略	296
	配置推模式或拉模式来更新客户端策略和内容	297
第 25 章	设置已知应用程序	299
	关于已知应用程序	299
	自用已知应用程序	
	相索应用程序	
	保存应用程序搜索的结果	303
部分 4	配置防病毒和防间谍软件防护	305
··· ·		
第26章	基本防病毒和防间谍软件策略设置	307
	防病毒和防间谍软件防护基础篇	308
	关于创建计划以响应病毒和安全风险	308

关于查看网络的防病毒和防间谍软件状态	310
关于运行防病毒和防间谍软件防护的命令	310
关于防病毒和防间谍软件策略	310
关于预先配置的防病毒和防间谍软件策略	311
关于锁定"防病毒和防间谍软件策略"中的设置	312
关于旧版客户端的防病毒和防间谍软件策略	312
关于处理可疑文件的默认设置	312
关于使用策略管理隔离区项目	313
关于使用防病毒和防间谍软件策略	313
关于病毒和安全风险	313
关于扫描	316
关于自动防护扫描	316
关于管理员定义的扫描	320
关于 TruScan 主动型威胁扫描	321
关于更新定义文件之后的扫描	322
关于扫描选定扩展名或文件夹	322
关于排除指定的文件及文件夹	326
关于针对扫描检测到的病毒与安全风险所采取的操作	326
在防病毒和防间谍软件策略中设置日志处理参数	327
关于客户端与防病毒和防间谍软件交互的选项	328
更改扫描映射网络驱动器所需的密码	328
指定 Windows 安全中心与 Symantec Endpoint Protection 客户端的	
交互方式	329
将Symantec Endpoint Protection 客户端配置为禁用 Windows 安	
全中心	329
配置在主机计算机上显示 Symantec Endpoint Protection 警	
报	329
配置定义的过期时间	330
在定义过期或丢失时显示警告	331
指定出现在防病毒和防间谍软件错误通知中的 URL	331
指定浏览器主页的 URL	332
配置应用于防病毒和防间谍软件扫描的选项	332
配置所选文件扩展名的扫描	332
配罢选完文件业的扫描	~~~
癿且匹疋又什て町1-1油	333
能且远足又伴关的口油 关于安全风险的例外	333 334
乱量远足又伴哭的口油 关于安全风险的例外 配置要针对检测到的已知病毒和安全风险执行的操作	333 334 334
配置远足又开关的口油 关于安全风险的例外 配置要针对检测到的已知病毒和安全风险执行的操作 关于受感染计算机上的通知消息	333 334 334 335
配量远足又开关的口油 关于安全风险的例外 配置要针对检测到的已知病毒和安全风险执行的操作 关于受感染计算机上的通知消息 在受感染的计算机上自定义并显示通知	333 334 334 335 336
<ul> <li>配置远足叉杆关的扫描</li> <li>关于安全风险的例外</li> <li>配置要针对检测到的已知病毒和安全风险执行的操作</li> <li>关于受感染计算机上的通知消息</li> <li>在受感染的计算机上自定义并显示通知</li> <li>将有关扫描的信息提交给 Symantec</li> </ul>	333 334 334 335 336 337
<ul> <li>配置远足叉杆关的扫描</li> <li>关于安全风险的例外</li> <li>配置要针对检测到的已知病毒和安全风险执行的操作</li> <li>关于受感染计算机上的通知消息</li> <li>在受感染的计算机上自定义并显示通知</li> <li>将有关扫描的信息提交给 Symantec</li> <li>关于提交调节</li> </ul>	333 334 334 335 336 337 338
<ul> <li>配置远足叉杆关的口油</li> <li>关于安全风险的例外</li> <li>配置要针对检测到的已知病毒和安全风险执行的操作</li> <li>关于受感染计算机上的通知消息</li> <li>在受感染的计算机上自定义并显示通知</li> <li>将有关扫描的信息提交给 Symantec</li> <li>关于提交调节</li> <li>配置提交选项</li> </ul>	333 334 334 335 336 337 338 339
<ul> <li>配置远足又件关的口油</li> <li>关于安全风险的例外</li> <li>配置要针对检测到的已知病毒和安全风险执行的操作</li> <li>关于受感染计算机上的通知消息</li> <li>在受感染的计算机上自定义并显示通知</li> <li>将有关扫描的信息提交给 Symantec</li> <li>关于提交调节</li> <li>配置提交选项</li> <li>管理已隔离的文件</li> </ul>	333 334 334 335 336 337 338 339 339
<ul> <li>配置远足又件关的口抽</li> <li>关于安全风险的例外</li> <li>配置要针对检测到的已知病毒和安全风险执行的操作</li> <li>关于受感染计算机上的通知消息</li> <li>在受感染的计算机上自定义并显示通知</li> <li>将有关扫描的信息提交给 Symantec</li> <li>关于提交调节</li> <li>配置提交选项</li> <li>管理已隔离的文件</li> <li>关于隔离区设置</li> </ul>	333 334 334 335 336 337 338 339 339 339 339

	指定本地隔离区目录 配置自动清除选项	340 340
	将隔离项目提交至中央隔离服务器	341
	将已隔离的项目提交至 Symantec	342
	配置新定义到达时要采取的操作	342
第 27 章	配置自动防护	345
	关于配置自动防护	345
	关于自动防护的类型	345
	启用文件系统自动防护	346
	配置文件系统自动防护	347
	关于自动防护安全风险扫描与禁止	348
	配置高级扫描和监控选项	348
	关于风险跟踪程序	349
	关于文件高速缓存	350
	配置 Internet 电子邮件自动防护	350
	配置 Microsoft Outlook 自动防护	352
	配置 Lotus Notes 自动防护	352
	配置自动防护的通知选项	353
	在受感染的计算机上显示自动防护结果	354
	在受感染的电子邮件中添加警告	355
	通知受感染电子邮件消息的发件人	356
	就受感染的电子邮件消息通知其他人	357
	配置 Internet 电子邮件目动防护扫描的进度通知	358
第 28 章	使用管理员定义的扫描	359
	关于使用管理员定义的扫描	359
	添加调度扫描到防病毒和防间谍软件策略	360
	配置按需扫描选项	361
	运行按需扫描	362
	配置管理员定义的扫描的扫描进度选项	363
	设置管理员定义的扫描的高级选项	364
<b>部分</b> 5	配置网络威胁防护	365
第 29 章	基本网络威胁防护设置	367
	关于网络威胁防护与网络攻击 Symantec Endpoint Protection 如何防止计算机受到网络攻	367
	击	368
	关于防火墙	368
	关于使用防火墙策略	369

# 第 27 章

关于防火墙规则	370
关于防火墙规则的各部分	370
关于规则处理顺序	374
关于状态检查	377
添加空白规则	378
使用向导添加规则	380
添加继承自父组的规则	381
导入和导出规则	382
复制并粘贴规则	383
更改规则的顺序	383
启用与禁用规则	383
后用智能通信过滤	384
后用迪信与隐藏设置	385
配置对等验证	385
<b>町                                    </b>	
能直入它防护	387
关于入侵防护系统	387
关于 Symantec IPS 特征	388
关于自定义 IPS 特征	388
配置入侵防护	389
关于使用入侵防护策略	389
启用人侵防护设置	390
更改 Symantec IPS 特征的行为	390
禁止攻击计算机	392
设置排除的计算机列表	392
创建自定义 IPS 特征	393
将多个自定义 IPS 库分配给组	395
史改特征的顺序	396
复制开粘贴特征	396
定义特征的受量	397
白宁ツ网络武陆防护	
日足又网络威励防护	399
启用和禁用网络威胁防护	400
针对混合控制配置网络威胁防护设置	400
添加主机和主机组	401
编辑和删除主机组	402
添加主机和主机组至规则	403
添加网络服务	404
编辑和删除自定义网络服务	405
添加网络服务至规则	405
启动网络文件和打印机共享	406
添加网络适配器	408

# 第 30 章

第 31 章

	添加网络适配器至规则	408
将应用程序添加到规则       410         添加调度至规则       411         配置网络威胁防护的通知       412         配置信事件的电子邮件       413         设置网络应用程序监控       414         配置主动型威胁方护       417         配置 TruScan 主动型威胁力描       419         关于 TruScan 主动型威胁力描所的护       417         配置 TruScan 主动型威胁力描所的护       419         关于 TruScan 主动型威胁力描所检测的进程       420         关于 TruScan 主动型威胁力描如何与隔离区配合工作       422         关于 TruScan 主动型威胁力描如何与隔离区配合工作       424         TruScan 主动型威胁力描如何与隔离区配合工作       424         TruScan 主动型威胁力描如何与隔离区配合工作       424         了解 TruScan 主动型威胁力描如何为量       427         指定检测商商业应用程序与设备控制       431         文产应用程序与设备控制策略的结构       432         关于应用程序与设备控制       431         关于应用程序与设备控制规则       431         关于应用程序与设备控制规则集和规则集和规则       434         关于应用程序控制规则集和规则	编辑和删除自定义网络适配器	409
添加调度至规则       411         配置网络威胁防护的通知       412         配置通信事件的电子邮件       413         设置网络应用程序监控       414 <b>配置主动型威胁防防护</b> 417 <b>配置 TruScan 主动型威胁扫描</b> 419         关于 TruScan 主动型威胁扫描       419         关于使用 Symantec 默认设置       420         关于 TruScan 主动型威胁扫描的总理       421         关于管理 TruScan 主动型威胁扫描忽略的进程       422         关于 TruScan 主动型威胁扫描忽略的进程       422         关于 TruScan 主动型威胁扫描忽略的进程       424         TruScan 主动型威胁扫描忽何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       424         了解 TruScan 主动型威胁扫描如何与集中式例外配合工作       427         指定检测销格伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测到商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       426         配置 TruScan 主动型威励助扫描频率       427         指定检测到商业应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略       433         关于应用程序与设备控制策略       436         大	将应用程序添加到规则	410
配置网络威胁防护的通知       412         配置通信事件的电子邮件       413         设置网络应用程序监控       414 <b>配置主动型威胁防疗</b> 417 <b>配置</b> TruScan 主动型威胁扫描       419         关于 TruScan 主动型威胁扫描       419         关于 TruScan 主动型威胁扫描//       419         关于 TruScan 主动型威胁扫描//       419         关于使用 Symantec 默认设置       420         关于 TruScan 主动型威胁扫描//       421         文子 TruScan 主动型威胁扫描//       422         关于 TruScan 主动型威胁扫描//       424         TruScan 主动型威胁扫描//       424         TruScan 主动型威胁扫描//       425         指定 TruScan 主动型威胁扫描//       425         方面 TruScan 主动型威胁扫描//       426         了解 TruScan 主动型威胁扫描//       427         指定 TruScan 主动型威胁扫描//       427         指定 TruScan 主动型威胁扫描//       428         配置 TruScan 主动型威胁扫描//       428         配置 TruScan 主动型威胁扫描//       428         配置 TruScan 主动型威胁扫描//       429 <b>配置应用程序与设备控制</b> 431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       432         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则集	添加调度至规则	411
配置通信事件的电子邮件       413         设置网络应用程序监控       414         配置主动型威胁防防护       417         配置TruScan 主动型威胁扫描       419         关于TruScan 主动型威胁扫描       419         关于使用Symantc 默认设置       420         关于TruScan 主动型威胁扫描/>关于TruScan 主动型威胁扫描/>20       420         关于TruScan 主动型威胁扫描/>20       420         关于TruScan 主动型威胁扫描/>20       420         关于TruScan 主动型威胁扫描/20       421         关于TruScan 主动型威胁扫描/20       422         关于TruScan 主动型威胁扫描/20       424         TruScan 主动型威胁扫描//>加付与爆肉/       425         指定 TruScan 主动型威胁扫描//>加付与爆肉/       425         指定 TruScan 主动型威胁扫描//>加付与爆肉/       426         介留 TruScan 主动型威胁扫描//>加付       427         指定检测到商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描//>加付       427         指定 检测每点       427         指定 检测可和       427         指定 TruScan 主动型威胁扫描//       428         配置 TruScan 主动型威胁扫描//       428         配置 TruScan 主动型威胁扫描//       429         配置 应用程序与设备控制策//       431 <th>配置网络威胁防护的通知</th> <th>412</th>	配置网络威胁防护的通知	412
设置网络应用程序监控       414         配置主动型威胁防防护       417         配置TruScan 主动型威胁扫描       419         关于TruScan 主动型威胁扫描       419         关于使用 Symantec 默认设置       420         关于TruScan 主动型威胁扫描所检测的进程       421         关于管理 TruScan 主动型威胁扫描所检测的进程       422         关于TruScan 主动型威胁扫描如何与魔离区配合工作       424         TruScan 主动型威胁扫描如何与魔离区配合工作       424         TruScan 主动型威胁扫描如何与魔离区配合工作       424         了解 TruScan 主动型威胁扫描如何与魔事中式例外配合工作       424         了解 TruScan 主动型威胁扫描如何与魔离区配合工作       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       127         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       131         别       427         指定检测转应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制案略的结构       432         关于应用程序与设备控制集略的结构       433         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略       437         启用默认的应用程序控制规则集和规则       438         创建应用程序与设备控制策略       437         启用默认的应用程序控制规则集和规则集和问该集添加新规则       438         创建应用程序与设备控制策略       437         启用默认的应用程序控制规则集和规则集和和成为       439         创建应用程序与设备控制策略       437	配置通信事件的电子邮件	413
配置主动型威胁防抗       417         配置 TruScan 主动型威胁扫描       419         关于 TruScan 主动型威胁扫描       419         关于使用 Symantec 默认设置       420         关于 TruScan 主动型威胁扫描於       421         关于管理 TruScan 主动型威胁扫描检测的误报       422         关于 TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与爆中式例外配合工作       424         TruScan 主动型威胁扫描如何与爆中式例外配合工作       425         指定 TruScan 主动型威胁扫描如何与爆中式例外配合工作       427         指定检测导路伊木马、蠕虫和击键记录程序的操作和敏感级       9         列       427         指定检测导商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429 <b>配置 应用程序与设备控制</b> 431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       438         创建应用程序与设备控制策略       437         启用默认的应用程序控制规则集和规则       438         创建应的是在的是和策略的应用程序控制制策略的应用程序控控制       438	设置网络应用程序监控	414
配置主动型威胁防护       417         配置 TruScan 主动型威胁扫描       419         关于 TruScan 主动型威胁扫描       419         关于使用 Symantec 默认设置       420         关于使用 Symantec 默认设置       421         关于管理 TruScan 主动型威胁扫描检测的进程       422         关于 TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描检测的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测转洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测转洛伊木马、蠕虫和击键记录程序的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429 <b>配置应用程序与设备控制</b> 431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略的结构       435         关于应用程序与设备控制策略的应用程序控制规则集       438         创建应用程序与设备控制策略的应用程序控制规则集       438         创建应用程序与设备控制策略的应用程序控制       439         均建应用程序与设备控制策略的应用程序		
<b>RUE</b> TruScan 主动型威胁扫描       419 $\xi$ 于 TruScan 主动型威胁扫描所检测的进程       420 $\xi$ 于 TruScan 主动型威胁扫描忽略的进程       421 $\xi$ 于 TruScan 主动型威胁扫描忽略的进程       421 $\xi$ 于 TruScan 主动型威胁扫描忽略的进程       422 $\xi$ 于 TruScan 主动型威胁扫描忽略的进程       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与降离区配合工作       424         TruScan 主动型威胁扫描如何与降离区配合工作       424         TruScan 主动型威胁扫描忽略的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       9         别       27         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测转洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测转洛伊木马、蠕虫和击键记录取的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429 <b>RT Con 用程序与设备控制</b> 431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制规则集和规则       434         关于应用程序与设备控制策略的结构       433         发于应用程序与设备控制策略的应用程序控制规则集       434         关于应用程序与设备控制策略的应用程序控制规则集并向该集添加新规则       439         创建新的应用程序控制规则集       438         创建方的应用程序控制规则集       439	配置主动型威胁防护	417
配置 TruScan 主动型威胁扫描       419         关于 TruScan 主动型威胁扫描       419         关于使用 Symantec 默认设置       420         关于 TruScan 主动型威胁扫描所检测的进程       421         关于管理 TruScan 主动型威胁扫描忽略的进程       422         关于 TruScan 主动型威胁扫描忽略的进程       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       424         了解 TruScan 主动型威胁扫描如何与集空式例外配合工作       425         指定 TruScan 主动型威胁扫描短筒       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429 <b>配置 应用程序与设备控制</b> 431         关于应用程序与设备控制集略的结构       432         关于应用程序与设备控制集略的结构       432         关于应用程序控制规则集和规则       434         关于应用程序与设备控制规则集和规则       434         关于应用程序与设备控制规则集和规则集并向该集添加新规则       438         创建应用程序与设备控制策略的应用程序控制规则集并向该集添加新规则       439         创建新的应用程序控制规则集并向该集添加新规则       439         均量如用程序与设备控制策略的应用程序控制规则集并向该集添加新规则		
第10日       中的全球加力中加       119         关于 TruScan 主动型威胁扫描       419         关于使用 Symantec 默认设置       420         关于 TruScan 主动型威胁扫描所检测的进程       421         关于管理 TruScan 主动型威胁扫描忽略的进程       422         关于 TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测转离业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       429         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429         配置 TruScan 主动型威胁扫描频率       429         配置 DruB程序 与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制规则集和规则       434         关于使用程序与设备控制策略       437         启用默认的应用程序控制规则集和规则       438         创建应用程序与设备控制策略       438         创建应用程序与设备控制策略       438         创建面用程序与设备控制策略       439         创建面用程序与设备控制策略	配置 TruScan 主动型威胁扫描	110
$\xi$ 于 TruScan 主动型威胁扫描       419 $\xi$ 于 $f$ truScan 主动型威胁扫描於检测的进程       420 $\xi$ 于 TruScan 主动型威胁扫描检测的误报       421 $\xi$ 는 $f$ truScan 主动型威胁扫描检测的误报       422 $\xi$ 는 TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       424         J m TruScan 主动型威胁扫描检测的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       别         别       427         指定检测每面业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       426         配置 TruScan 主动型威胁扫描频率       427         指定检测每面业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       429 <b>配置 应用程序与设备控制</b> 431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序与设备控制策略的结构       434         关于应用程序与设备控制策略       436         关于使用应用程序控制规则集和规则集       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         创建应用程序与设备控制策略       438         创建应用程序与设备控制策略      439         约是前的应用程序控制规则集并向该集添加新规则集并有该集添加		415
关于使用 Symantec 默认设置       420         关于 TruScan 主动型威胁扫描所检测的进程       421         关于管理 TruScan 主动型威胁扫描忽略的进程       422         关于 TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与原离区配合工作       424         了解 TruScan 主动型威胁扫描如何与集中式例外配合工作       425         指定 TruScan 主动型威胁扫描检测的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       9         别       427         指定检测每商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       426         配置 TruScan 主动型威胁扫描频率       427         指定检测每面业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       429 <b>配置 应用程序与设备控</b> 制策略的结构       431         关于应用程序与设备控制策略的结构       432         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       436         关于使用程序与设备控制策略       437         启用程序与设备控制策略       438         创建应用程序与设备控制策略	关于 TruScan 主动型威胁扫描	419
关于 TruScan 主动型威胁扫描标检测的进程       421         关于管理 TruScan 主动型威胁扫描忽略的进程       422         关于 TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       424         了解 TruScan 主动型威胁扫描检测的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       9         别       427         指定检测钥商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429         配置 TruScan 主动型威胁扫描频率       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于位用程序与设备控制策略       437         启用程序与设备控制策略       438         创建应用程序与设备控制策略       438         创建应用程序与设备控制策略       438	关于使用 Symantec 默认设置	420
关于管理 TruScan 主动型威胁扫描忽略的进程.       422         关于 TruScan 主动型威胁扫描忽略的进程.       424         TruScan 主动型威胁扫描如何与隔离区配合工作.       424         TruScan 主动型威胁扫描如何与集中式例外配合工作.       424         了解 TruScan 主动型威胁扫描如何与集中式例外配合工作.       424         了解 TruScan 主动型威胁扫描如何与集中式例外配合工作.       425         指定 TruScan 主动型威胁扫描检测的进程类型.       427         指定检测转洛伊木马、蠕虫和击键记录程序的操作和敏感级.       427         指定检测转洛伊木马、蠕虫和击键记录程序的操作和敏感级.       427         指定检测到商业应用程序时应采取的操作.       428         配置 TruScan 主动型威胁扫描频率.       428         配置 TruScan 主动型威胁扫描频率.       429 <b>配置应用程序与设备控制</b> .       431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构.       432         关于应用程序与设备控制集略的结构.       433         关于应用程序与设备控制策略的结构.       434         关于应用程序控制规则集和规则.       434         关于应用程序与设备控制策略的结构.       436         关于应用程序与设备控制策略的应用程序控制规则集.       438         创建应用程序与设备控制策略的应用程序控制规则集.       438         创建应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集.       439         档量的过品和算行控制规则集.       434         美于应用程序与设备控制策略的应用程序控制规则集.       438         创建应用程序与设备控制策略的应用程序控制规则集.       439         创建新的应用程序控制规则则集.       439	关于 TruScan 主动型威胁扫描所检测的进程	421
关于 TruScan 主动型威胁扫描忽略的进程       424         TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       424         了解 TruScan 主动型威胁扫描检测的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测转洛伊木马、蠕虫和击键记录程序的操作和敏感级       9         别       427         指定检测转洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测转洛伊木马、蠕虫和击键记录程序动操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429         配置应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略       436         关于使用起用程序与设备控制策略      438         创建应用程序与设备控制策略的应用程序控制规则集并向该集添加新规则       439         创建应用程序与设备控制策略的应用程序控制规则集并向该集添加新规则       439         将条件添加	关于管理 TruScan 主动型威胁扫描检测的误报	422
TruScan 主动型威胁扫描如何与隔离区配合工作       424         TruScan 主动型威胁扫描如何与集中式例外配合工作       424         了解 TruScan 主动型威胁扫描检测的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测钥查业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429         配置 TruScan 主动型威胁扫描频率       429         配置 D 用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略的结构       432         关于应用程序控制规则集和规则       434         关于应用程序与设备控制规则集和规则       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集和规则       438         创建应用程序与设备控制策略       439         创建新的应用程序控制规则集并向该集添加新规则       439         创建新的应用程序控制规则集并向该集添加新规则       439         利用程序与设备控制策略       439         利用程序与设备控制策略       439         创建面印程序与设备控制策略       439         利用程序与设备控制策略       439         资量面积       431         我名       431         其行行员员员在的行行所有任       432 </th <th>关于 TruScan 主动型威胁扫描忽略的进程</th> <th>424</th>	关于 TruScan 主动型威胁扫描忽略的进程	424
TruScan 主动型威胁扫描如何与集中式例外配合工作       424         了解 TruScan 主动型威胁扫描检测的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测到商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429         配置应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略的结构       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集和规则       438         创建应用程序与设备控制策略       439         创建面的应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       439         利和的应用程序控制规则集并向该集添加新规则       431         配置规则的条件属性       441         配置规则的条件属性       441	TruScan 主动型威胁扫描如何与隔离区配合工作	424
了解 TruScan 主动型威胁扫描检测的进程类型       425         指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测到商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描频率       429 <b>配置 Cn用程序与设备控制</b> 431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略的结构       437         自用默认的应用程序控制规则集和规则       434         关于使用程序与设备控制策略       437         自用默认的应用程序控制规则集和规则       438         创建应用程序与设备控制策略       439         创建亦的应用程序控制规则集并向该集添加新规则       439         创建新的应用程序控制规则集并向该集添加新规则       431         配置规则的条件属性       441         配置匹配条件时要采取的操作       443	TruScan 主动型威胁扫描如何与集中式例外配合工作	424
指定 TruScan 主动型威胁扫描检测的进程类型       427         指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级       427         指定检测到商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描的通知       429         配置 Cn用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序与设备控制策略的结构       433         关于应用程序与设备控制规则集和规则       434         关于应用程序与设备控制策略的结构       436         关于应用程序与设备控制策略       437         启用默认的应用程序控制规则集和规则       438         创建应用程序与设备控制策略       439         创建应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集计向该集添加新规则       434         化量定应用程序与设备控制策略的应用程序控制       437         雇用数认的应用程序控制规则集       438         配置应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       434         和行为应用程序控制规则集优的应用程序控制规则集优的应用程序控制       439         创建新的应用程序与设备控制策略的应用程序控制       439         省理定应用程序与设备控制策略的应用程序控制规则集       439         有量定应用程序与设备控制策略的应用程序控制规则集         指       439         百量       434         配置应用程序与设备控制策略的应用程序控制规则集       435         型应用程序与设备控制策略的应用程序控制规则集       436         工具定的应用程序控制	了解 TruScan 主动型威胁检测	425
指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级 别	指定 TruScan 主动型威胁扫描检测的进程类型	427
别       427         指定检测到商业应用程序时应采取的操作       428         配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描的通知       429 <b>配置应用程序与设备控制</b> 431         关于应用程序与设备控制       431         关于应用程序与设备控制       432         关于应用程序与设备控制       433         关于应用程序与设备控制策略的结构       432         关于应用程序控制       433         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于使用应用程序与设备控制策略       437         启用默认的应用程序与设备控制策略       438         创建应用程序与设备控制策略       438         创建应用程序与设备控制策略       439         创建新的应用程序控制规则集并向该集添加新规则       439         将条件添加到规则       441         配置规则的条件属性       441         配置匹配条件时要采取的操作       443	指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级	
指定检测到商业应用程序时应采取的操作	别	427
配置 TruScan 主动型威胁扫描频率       428         配置 TruScan 主动型威胁扫描的通知       429         配置应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制       432         关于应用程序与设备控制       433         关于应用程序控制       433         关于应用程序控制       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略       437         启用默认的应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制规则集并向该集添加新规则       439         约建新的应用程序控制规则集并向该集添加新规则       431         配置规则的条件属性       441         配置匹配条件时要采取的操作       443	指定检测到商业应用程序时应采取的操作	428
配置 TruScan 主动型威胁扫描的通知       429         配置应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制       432         关于应用程序与设备控制策略的结构       432         关于应用程序控制       433         关于应用程序控制       433         关于应用程序控制       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略       437         启用默认的应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       434         配置规则的条件属性       441         配置匹配条件时要采取的操作       443	配置 TruScan 主动型威胁扫描频率	428
配置应用程序与设备控制       431         关于应用程序与设备控制、       431         关于应用程序与设备控制策略的结构       432         关于应用程序控制       433         关于应用程序控制       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制       439         約建新的应用程序控制规则集并向该集添加新规则       431         配置规则的条件属性       441         配置匹配条件时要采取的操作       443	配置 TruScan 主动型威胁扫描的通知	429
配置应用程序与设备控制       431         关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序控制       433         关于应用程序控制       433         关于应用程序控制       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       439         将条件添加到规则       441         配置匹配条件时要采取的操作       443		
关于应用程序与设备控制       431         关于应用程序与设备控制策略的结构       432         关于应用程序控制       433         关于应用程序控制       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       439         将条件添加到规则       441         配置规则的条件属性       443	配重应用程序与设备控制	431
关于应用程序与设备控制策略的结构       432         关于应用程序控制       433         关于测试模式       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于设备控制       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       439         将条件添加到规则       441         配置规则的条件属性       441         配置匹配条件时要采取的操作       443	关于应用程序与设备控制	431
关于应用程序控制       433         关于测试模式       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         创建应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       439         将条件添加到规则       441         配置匹配条件时要采取的操作       443	关于应用程序与设备控制策略的结构	432
关于過出模式       434         关于应用程序控制规则集和规则       434         关于应用程序控制规则集和规则       434         关于设备控制       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略       439         创建新的应用程序控制规则集并向该集添加新规则       439         将条件添加到规则       441         配置匹配条件时要采取的操作       443	关于应用程序控制	433
关于应用程序控制规则集和规则       434         关于设备控制       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略       439         创建新的应用程序控制规则集并向该集添加新规则       439         将条件添加到规则       441         配置匹配条件时要采取的操作       443	关于测试模式	434
关于运备控制       436         关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       439         化素件添加到规则       441         配置规则的条件属性       443	关于应田程序控制抑则集和抑则	434
关于使用应用程序与设备控制策略       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       439         化建新的应用程序控制规则集并向该集添加新规则       439         化量新的应用程序控制规则集并向该集添加新规则       439         化量新的应用程序控制规则集并向该集添加新规则       439         化量新的应用程序控制规则集并向该集添加新规则       439         化量新的应用程序控制规则集并向该集添加新规则       439         化量新的应用程序控制规则集并向该集添加新规则       439         化量规则的条件属性       441         配置匹配条件时要采取的操作       443	关于過各控制	436
尺寸使用遮闭住力与使留压的乘船       437         启用默认的应用程序控制规则集       438         创建应用程序与设备控制策略       438         配置应用程序与设备控制策略的应用程序控制       439         创建新的应用程序控制规则集并向该集添加新规则       439         化量新的应用程序控制规则集并向该集添加新规则       439         化量新的应用程序控制规则集并向该集添加新规则       439         化量新的应用程序控制规则集并向该集添加新规则       441         配置规则的条件属性       441         配置匹配条件时要采取的操作       443	关于庙田应田程序与设备控制策略	437
泊州氣((石))       102,000       102,000       103,000       103,000         创建应用程序与设备控制策略       438       102       102       103,000       103,000         创建新的应用程序控制规则集并向该集添加新规则       439       102       103,000	自田野认的应用程序控制规则集	438
<ul> <li> 130 10 10 10 10 10 10 10 10 10 10 10 10 10</li></ul>	们承认的应用程序与设备控制等政	430
111       111	时是这些10年11月7日中国来吧····································	430
将条件添加到规则	们建新的应田程序控制规则集并向该集添加新规则	433
配置规则的条件属性	齿元初间加生力1年1月200000000000000000000000000000000000	433
配置匹配条件时要采取的操作 441	的示目称加拉风对	441 1/1
电电毕电示于PI女不收时床下	电量/2/2010万日/周日 ···································	113
	电电毕起不口吗女个状的沐仔	440

# **部分**6

# 第 32 章

第	33	章

	将规则应用于特定应用程序以及将应用程序排除在规则的应用范	
		443
	更改应用程序控制规则集的应用顺序	445
	任应用程序与设备控制束略甲等用应用程序控制规则集和个别规 即	445
	则	445
	史改应用程序控制规则集的模式	446
	7应用程序与反备控制束哈配直反备控制	447
第 34 章	自定义应用程序与设备控制策略	449
	关于硬件设备	449
	关于类 ID	450
	关于设备 ID	450
	获取类 ID 或设备 ID	450
	将硬件设备添加至硬件设备列表	451
	编辑硬件设备列表中的硬件设备	451
	关于授权使用应用程序、补丁程序和实用程序	452
	创建及导入文件指纹列表	452
	创建文件指纹列表	453
	编辑文件指纹列表	454
	将文件指纹列表导入共享策略	454
	合并共享策略中的文件指纹列表	455
	删除文件指纹列表	456
	关于系统锁定	456
	系统锁定先决条件	457
	设置系统锁定	457
部分 7	配置集中式例外	461
第 35 章	配置集中式例外策略	463
	关于集中式例外策略	463
	关于使用集中式例外策略	464
	关于防病毒和防间谍软件扫描的集中式例外	464
	关于 TruScan 主动型威胁扫描的集中式例外	465
	关于防篡改的集中式例外	465
	关于客户端与集中式例外的交互	465
	配置集中式例外策略	465
	配置防病毒和防间谍软件扫描的集中式例外	466
	配置 TruScan 主动型威胁扫描的集中式例外	468
	配置防篡改的集中式例外	470
	配置集中式例外的客户端限制	470
	从日志事件创建集中式例外	471

添加风险事件的集中式例外	471
添加 TruScan 主动型威胁扫描事件的集中式例外	472
添加防篡改事件的集中式例外	472

# 部分 8 配置主机完整性以实现端点策略遵从 ........ 475

## 基本主机完整性设置 ...... 477 主机完整性强制执行的工作方式 ...... 477 关于使用主机完整性策略 ...... 479 关于主机完整性要求 ...... 480 启用和禁用主机完整性要求 ...... 483 更改主机完整性要求的顺序 ...... 483 从模板添加主机完整性要求 ...... 483 关于主机完整性检查的设置 ...... 484 配置主机完整性检查的通知 ...... 486 关于为满足主机完整性而还原应用程序和文件 ...... 487 主机完整性补救和 Enforcer 设置 ...... 487 指定客户端等候补救的时间长度 ...... 488 允许用户推迟或取消主机完整性补救 ...... 488 在用户未登录时隐藏补救 ...... 490

## 第37章

第36章

# 

关于自定义要求	491
关于条件	492
关于防病毒的条件	492
关于防间谍软件的条件	493
关于防火墙的条件	493
关于文件的条件	493
关于操作系统的条件	495
关于注册表的条件	496
关于功能	497
关于匀定》要求逻辑 关于白定》要求逻辑	498
关于 BFTIIRN 语句	/198 /198
关于 IF THEN 和 ENDIE 语句	
入了II、IIILI、神LIUII 旧号 土王 FI SE 通句	490
入 J LLSL	
大」NOI 大健于 关工 AND OD 关键字	
天丁 AND、OR 天键子	498

	编写自定义要求脚本	499
	添加 IF THEN 语句	500
	在 IF 及 IF NOT 语句之间切换	500
	添加 ELSE 语句	501
	添加注释	501
	复制和粘贴 IF 语句、条件、函数和注释	501
	删除语句、条件或函数	502
	显示消息对话框	502
	下载文件	503
	生成日志消息	503
	运行程序	504
	运行脚本	505
	设置文件的时间戳	506
	指定脚本的等待时间	506
附录 A	使用命令行界面	509
	客户端服务	509
	错误代码	512
	在客户端有密码防护时键入参数	513
附录 B	关于客户端和服条器诵信设置	515
	关于客户端和服务器通信设置	515
索引		517





# 基本管理任务

- Symantec Endpoint Protection Manager 概述
- 基本防护简介
- 管理组、客户端、用户和计算机
- 管理域和管理员
- 使用客户端安装软件包
- 更新定义与内容
- 限制用户对客户端功能的访问
- 设置管理服务器与客户端之间的连接
- 报告基础篇
- 查看和配置报告
- 查看和配置日志和通知
- 使用监视器和报告来确保网络安全

# Symantec Endpoint Protection Manager 概述

本章节包括下列主题:

- 关于管理任务
- 登录 Symantec Endpoint Protection Manager 控制台
- Symantec Endpoint Protection Manager 控制台的组织方法

# 关于管理任务

在 Symantec Endpoint Protection Manager 中执行管理任务前,您必须已经在测试环境中安装管理服务器。安装管理服务器的管理员可执行 Symantec Endpoint Protection 和 Symantec Network Access Control 的管理任务。

有关详细信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

管理任务包括基本和高级的管理任务。大部分的组织都只需要执行基本管理任务。 较不复杂的较小组织不太需要执行高级的管理任务。大部分的默认设置应该已足够 满足基本管理任务的要求。第1篇说明基本的管理任务。第2篇则说明组织自定义 默认设置执行的高级管理任务。

表1-1包括管理任务、信息所在位置和可读取信息的用户等概述。

位置	读者
第1部分:	适合所有管理员。
基本管理任务	包括管理管理员、管理客户端、更新定义和内容, 以及报告和监控的基本任务。

表1-1 管理任务说明

位置	读者
第2部分:	适合规模较大组织中的管理员。
高级管理任务	包括管理多个站点、管理各种类型的服务器、从一 个站点复制数据至另一站点,以及管理防篡改功 能。
第3部分:	适合所有管理员。
常规策略管理任务	包括所有策略类型概述、继承与位置的概念,以及 使用已知应用程序。
第4部分:	适合所有管理员。
配置防病毒和防间谍软件防护	包括防病毒和防间谍软件策略设置、配置自动防护以及设置管理员定义的扫描。
第5部分:	适合需要配置防火墙的管理员。
配置网络威胁防护	包括用于微调防火墙的设置。默认设置通常已足 够,但是熟知网络的管理员可能会想要微调其中的 设置。
第6部分: 配置主动型或助防护	适合需要不仅止于防病毒、防间谍软件、入侵防护 及防火墙防护技术的管理员。
距直土列型威胁的护	包括用于检测未知威胁的启发式设置。
第7部分:	适合规模较大组织中的管理员。
配置集中式例外	包括如何针对防病毒和防间谍软件扫描、TruScan 主动型威胁扫描和防篡改设置例外的相关信息。
第8部分:	适合对于此可选组件感兴趣的管理员。
配置主机完整性以实现端点策略遵从	说明如何设置主机完整性策略,确保端点遵循安全 策略。
附录 A:	适合所有管理员。
使用命令行界面	包括可与 smc 命令一起使用的客户端服务参数。

# 登录 Symantec Endpoint Protection Manager 控制台

您可以在安装 Symantec Endpoint Protection 后登录 Symantec Endpoint Protection Manager 控制台。可以通过两种方式登录控制台。您可以从另一台符合远程控制台系统要求的计算机进行远程登录。您也可以使用已安装管理服务器的计算机从本地登录控制台。

许多管理员从远程登录,他们可以执行和本地登录的管理员一样的任务。若要远程登录,您需要知道已安装管理服务器的计算机的IP地址或主机名。您还应确保Web 浏览器的 Internet 选项允许您查看所登录的服务器的内容。

您可以使用控制台查看哪些内容以及执行哪些操作取决于您属于哪一管理员类型。 您能以系统管理员、管理员或受限管理员的身份登录。系统管理员拥有所有域的全 部权限。管理员拥有仅限于特定域的权限。受限管理员则拥有管理员权限的子集, 同时其权限还仅限于特定域。如果您是安装管理服务器的用户,则您是系统管理 员。如果管理服务器是其他用户安装的,则您的状态可能会有所不同。不过,在大 多数组织内,并不需要关注域管理员或受限管理员的状态。

小型组织中的大多数管理员都以系统管理员身份登录。

请参见第62页的"关于管理员"。

#### 远程登录控制台

1 打开 Web 浏览器, 然后在地址框中输入下列地址:

#### http://host name:9090

其中, host name 是管理服务器的主机名或 IP 地址。默认情况下, 控制台会使 用端口号 9090, 但您可以通过运行管理服务器配置向导更改它。

**2** 看见 Symantec Endpoint Protection Manager 控制台网页时,单击相应链接 以显示登录屏幕。

您登录的计算机必须已安装 Java 2 Runtime Environment (JRE)。如果没有, 您会收到下载和安装提示。按照提示安装 JRE。

计算机还必须已启用 Active X 及脚本。

3 在您登录时,可能会看见警告主机名不匹配的消息。如果出现此消息,请响应 提示,单击"是"。

此消息表示您指定的远程控制台 URL 与 Symantec Endpoint Protection 证书 名称不符。如果您登录并指定一个IP地址,而不是管理服务器的计算机名称, 就会发生此问题。

- **4** 在出现的 Symantec Endpoint Protection Manager 下载窗口中,单击相应链 接来下载 Symantec Endpoint Protection Manager。
- 5 当系统提示您是否要创建桌面并启动菜单快捷方式时,请根据需要单击"是" 或"否"。

这两个选项都可以接受。

6 在显示的 Symantec Endpoint Protection Manager 控制台登录窗口中,键入您的用户名和密码。如果这是您在安装后第一次登录 Symantec Endpoint Protection,请输入帐户名称:admin。然后,输入您在安装产品时所配置的密码。

7 如果您的网络只有一个域,请忽略此步骤。

如果您的网络有多个域,请在"域"文本框中,输入所要登录的域名。

如果没有显示"域"文本框,请单击"选项>>"。"域"文本框是否出现取决于您上次登录时的状态。

8 单击"登录"。

您可能会在远程控制台启动时收到一条或多条安全警告消息。如果确实如此, 请单击"是"、"运行"、"启动"或同等功能的选项,然后继续操作直到显 示控制台。

#### 从本地登录控制台

- 在 Windows "开始"菜单上,依次单击 "程序" > Symantec Endpoint Protection Manager > "Symantec Endpoint Protection Manager 控制台"。
- 2 在 Symantec Endpoint Protection Manager 登录提示中, 键入您在安装期间 配置的用户名(默认为 admin)和密码。

如果您是管理员,但没有安装管理服务器,请使用您的管理员为您配置的用户 名和密码。

- 3 执行下列操作之一:
  - 如果控制台只有一个域,请跳至步骤4。
  - 如果控制台有一个以上的域,请单击"选项">>,然后键入相应域名。
- 4 单击"登录"。

# Symantec Endpoint Protection Manager 控制台的组织 方法

Symantec Endpoint Protection Manager 控制台可深入查看您的网络安全。使用它可集中管理 Symantec Endpoint Protection 和 Symantec Network Access Control。该控制台可用来更改客户端安全策略。

第一次登录控制台时,您会看到控制台主页和包含页面选项卡的导航栏。控制台导 航栏位于窗格左侧。控制台包括六个页面。每个页面表示一项主要管理功能类别。 每个图标表示一项功能类别,并附有关于该页面功能的说明性文本。您可以单击导 航栏中的图标以显示相应的页面。始终可以使用这些图标浏览各个页面。

**注意**:系统管理员和受限管理员可能仅能看到较少的选项,具体视分配给其帐户的 权限而定。 "主页"页面、"监视器"页面和"报告"页面提供您用以监控网络安全的报告功 能。"策略"页面、"客户端"页面和"管理员"页面用于配置和管理您的网络安 全策略。

表1-2列出了每个导航栏图标并说明了与其关联的功能。

表1-2 控制台导航图标

标签	说明
主页	显示您的网络安全状态和病毒定义摘要信息。
	使用此页面作为您的控制面板。控制台始终以主页面打开。
监视器	显示监控日志。
	使用此页面可查看日志、配置日志过滤器、查看并配置通知,以及监控命令状态。
报告	显示报告。您可以选择预定义和可自定义的快速报告,以及可配置的调度报告。
	使用此页面可运行并查看报告、配置报告过滤器,以及调度报告。
策略	显示每个策略类型的策略。
	使用此页面可配置和管理您的策略。
客户端	显示客户端和组的策略信息。
	使用此页面可管理通过安装软件包推送到客户端的客户端软件和策略。
管理员	显示特定于管理员的配置信息。
	使用此页面可管理管理员、域、站点、服务器、数据库,以及安装软件包。

# 主页

主页显示常规安全状态和病毒定义摘要信息。如果您安装了 Symantec Endpoint Protection,则主页会显示网络的安全信息。如果您只安装了 Symantec Network Access Control,则主页会显示自动生成的网络遵从性状态报告。

Symantec Endpoint Protection 主页包含下列部分:

- 安全状态
- 按检测计数列出的操作摘要
- 每小时攻击数、风险数或感染数: 过去 12 小时
- 状态摘要,包括过去24小时未确认的通知
- 病毒定义分发或入侵防护特征

- 安全响应中心信息和链接
- 受监控的应用程序摘要
- 报告收藏夹

请参见第 123 页的"关于 Symantec Endpoint Protection 主页"。

Symantec Network Access Control 主页包含下列部分:

- 网络遵从性状态为失败
- 遵从性状态分布
- 遵从性失败的客户摘要
- 遵从性失败详细信息

请参见第 130 页的"使用 Symantec Network Access Control 主页"。

## 安全状态

安全状态可以是"良好"或"需要注意"。如果状态是"需要注意",您可以单击 红色X图标或"更多详细信息"链接来查看更多信息。您也可以单击"首选项"访问"首选项"页面,您可在其中配置报告的首选项。

请参见第133页的"配置安全状态阈值"。

#### 报告收藏夹

默认情况下, 主页面的"报告收藏夹"部分包括下列报告:

- 首要攻击源
- 前几个风险检测关联
- TruScan 主动型威胁分布

您可以单击"报告收藏夹"右侧的加号图标,更改显示于主页面此部分的报告。 请参见第128页的"配置主页上的报告收藏夹"。

# 监视器页面

您可以使用"监视器"页面,显示日志信息,查看和配置通知,以及查看命令状态。此页面包含日志及通知,管理员可以使用它们来监控网络。

"监视器"页面包含下列选项卡:

∎ 摘要

如果已安装 Symantec Endpoint Protection,则会有多种摘要视图供您选择。 您可以选择查看"防病毒和防间谍软件防护"、"网络威胁防护"、"遵从性" 或"站点状态"。如果只安装了 Symantec Network Access Control,则"摘 要"选项卡会显示站点状态信息。如果只安装了 Symantec Network Access Control,主页上会显示遵从性信息。 请参见第 165 页的"使用监视器摘要选项卡"。

■ 日志

日志显示从您的安全产品收集的详细信息。日志包含管理服务器及客户端的事 件数据。您也可以从某些日志执行操作。有些管理员更愿意主要使用日志来监 控网络。

请参见第160页的"关于日志类型、内容和命令"。

■ 命令状态

"命令状态"选项卡显示您从 Symantec Endpoint Protection Manager 控制台 所运行命令的状态及其详细信息。 请参见第 173 页的"从日志运行命令和操作"。

∎ 通知

通知是一种消息,向您发出有关网络中潜在安全问题的警报。您可以配置多种 不同的事件来触发通知。"通知"选项卡上的通知针对的是管理员,而不是用 户。

请参见第179页的"使用通知"。

# 报告页面

您可以使用"报告"页来获取有关网络安全状态的概述。报告是您网络中发生事件 的图表快照,以及有关事件的统计。您可以使用"报告"页面上的过滤器来生成预 定义或自定义报告。预定义报告位于"快速报告"选项卡上。在"调度报告"选项 卡上,您可以安排定期运行报告,并设置以电子邮件形式将这些报告发送给您自己 或其他人。

请参见第140页的"关于报告"。

# 策略页面

您可以使用"策略"页来创建下载至客户端的策略。客户端连接到服务器获取最新 策略和安全设置,并据此部署软件更新。显示的策略取决于您安装的产品组件。

"策略"页面包含下列窗格:

■ 查看策略

"查看策略"窗格列出可在右上方窗格中查看的策略类型:防病毒和防间谍软件、防火墙、入侵防护、应用程序与设备控制、LiveUpdate以及集中式例外。如果已安装 Symantec Network Access Control,则您也可以查看主机完整性策略。单击策略组件旁边的箭头以展开组件列表(如果尚未显示的话)。

■ 策略组件

"策略组件"窗格列出各种类型的可用策略组件。这些组件包括管理服务器列 表、文件指纹列表等等。

∎ 任务

"任务"窗格列出您在"查看策略"下为策略选择的相应任务。

■ "<策略类型>策略"窗格

右窗格会随着您在"查看策略"下选择的策略而更改。部分选项会使窗格水平 分隔。在这种情况下,窗格的下半部显示所选策略的最近更改。

如需不同类型的策略及其选项的相关信息,请参见描述这些策略的章节。

# 客户端页面

您可以使用"客户端"页面管理网络中的计算机和用户。

"客户端"页面包括下列窗格:

- 查看客户端 "查看客户端"窗格会显示客户端管理结构中的组,这些组采用树结构以层级 式排列。默认情况下,此结构包含 My Company 组和位于该组下方的默认组。
- 任务
   "任务"窗格会列出您可以执行的客户端相关任务。
- <组名称>窗格

右窗格包括四个选项卡: "客户端"、"策略"、"详细信息"和"安装软件 包"。每个选项卡会显示您在"查看客户端"窗格中所选组的相关内容。

您可以从"客户端"选项卡执行下列任务:

- 添加组、计算机帐户和用户帐户。
- 导入组织单位或容器。
- 从 Active Directory 服务器或 LDAP 服务器直接导入用户。
- 对组运行命令。
- 搜索客户端。
- 显示组或用户。
- 搜索非受管计算机。

从"策略"选项卡,您可以设置 LiveUpdate 内容、客户端日志、通信和一些常规 设置的某些位置相关选项。您还可以设置一些特定于位置的选项,例如控制模式以 及服务器与客户端之间的推模式或拉模式通信。您可以从"策略"选项卡执行下列 任务:

- 添加位置。
- 管理位置。

- 复制组策略。
- 添加组。

您可以从"详细信息"选项卡执行下列任务:

- 添加组。
- 导入组织单位或容器。
- 删除组。
- 重命名组。
- 移动组。
- 编辑组属性。

从"安装软件包"选项卡,您可以配置和添加新的客户端安装软件包。先使用管理 服务器来创建,然后再将一个或多个客户端安装软件包导出到站点中的管理服务 器。在您将客户端安装软件包导出到管理服务器之后,将软件包中的文件安装到客 户端计算机上。

# 管理员页面

您可以使用"管理员"页面管理您网络的管理员帐户、域属性、服务器属性和站点 属性以及客户端安装软件包。当您选择"管理员"选项卡时,"查看"窗格会显示 管理当前登录域的所有管理员。这包括系统管理员、管理员和受限管理员。

"管理员"页面包含下列窗格:

- "查看管理员"、"查看域"、"查看服务器"或"查看安装软件包"。
   显示的视图取决于您在浏览窗格底部所做的选择。
- 任务

"任务"窗格会列出您可以从"管理员"页面执行的任务。这些任务会根据您 在浏览窗格底部所做的选择而有所更改。

■ 右窗格

右窗格显示您在浏览窗格底部所做的选择的相关内容。

选择"管理员"时,您可以添加、删除及编辑管理员帐户。

选择"域"时,您可以添加、重命名及编辑域属性。域提供在大型网络中分组计算 机的逻辑性方法。如果您使用的是小型网络,您可能仅会使用一个名为默认值的默 认域.

选择"服务器"时,可用的任务因您在"查看服务器"浏览树中所做的选择而异。 您可以选择本地站点、特定服务器或本地主机。

当您选择本地站点时,您可以执行下列任务:

■ 编辑站点属性,例如控制台超时时间段、LiveUpdate设置和数据库设置。

- 34 | Symantec Endpoint Protection Manager 概述 Symantec Endpoint Protection Manager 控制台的组织方法
  - 配置外部日志记录,以将日志数据发送到文件服务器或 Syslog 服务器。
  - 添加站点复制伙伴。
  - 下载 LiveUpdate 内容。
  - 显示 LiveUpdate 状态。
  - 显示 LiveUpdate 下载内容。

当您选择特定服务器时,您可以执行下列任务:

- 编辑服务器属性,例如邮件服务器、目录服务器和代理服务器选项。
- 删除服务器。
- 管理服务器验证证书。
- 配置 RSA SecurID 验证。
- 以XML文件导入和导出此服务器的属性。

选择"安装软件包"时,您可以添加、删除、编辑和导出客户端安装软件包。您还可以将软件包发送到组,并可以设置选项来收集用户信息。

# 2

# 基本防护简介

本章节包括下列主题:

■ 防护类别

# 防护类别

Symantec Endpoint Protection 可为您安全网络中的计算机提供若干种类型的防护。

这些类别包括:

- 防病毒和防间谍软件防护
- 网络威胁防护
- 主动型威胁防护
- 主机完整性

**注意:** 只有 Symantec Network Access Control 产品提供主机完整性策略。Symantec Network Access Control 可以独立安装,也可以与 Symantec Endpoint Protection 一起安装。所有其他类别的防护都是 Symantec Endpoint Protection 的标准功能,并不包括在 Symantec Network Access Control 中。

图 2-1 显示各种防护类型所禁止的威胁类别。



# 关于防病毒和防间谍软件防护

Symantec Endpoint Protection 的防病毒和防间谍软件防护可使计算机免受病毒和 安全风险的威胁,并可在许多情况下弥补病毒和风险带来的负面影响。此项防护包 括文件和电子邮件的实时扫描,以及调度扫描和按需扫描。防病毒和防间谍软件扫
描可检测病毒及安全风险,例如,间谍软件、广告软件及其他可能给计算机和网络 带来风险的文件。

这类扫描也可以检测内核级的Rootkit。Rootkit是试图在计算机操作系统内藏匿自 身并可能用于恶意目的的程序。

您可以将默认防病毒和防间谍软件策略应用于网络中的各客户端计算机。您可以视 需要创建其他防病毒和防间谍软件策略并加以应用。当安全网络中的要求改变时, 您也可以编辑此类策略。

默认防病毒和防间谍软件策略可适用于各种规模的公司。它不但可提供强大的防 护,还能将对端点资源的影响降到最低。

请参见第 308 页的"防病毒和防间谍软件防护基础篇"。

#### 关于网络威胁防护

网络威胁防护提供防火墙和入侵防护保护功能,以此阻挡入侵攻击及有害内容进入 运行 Symantec Endpoint Protection 客户端的计算机。防火墙会根据管理员或最终 用户所设置的各种条件来允许或禁止网络通信。

防火墙规则会决定相应端点是允许还是禁止传入或传出的应用程序或服务通过其网 络连接进行访问。通过防火墙规则,客户端可以系统地允许或禁止来自或传至特定 IP地址及端口的传入或传出应用程序及通信。安全设置可检测并标识常见的攻击, 在受到攻击之后发送电子邮件,显示可自定义消息以及执行其他相关的安全任务。

客户端还可分析所有传入及传出信息是否存在具有典型攻击特征的数据模式。客户 端可检测并禁止恶意通信以及外部用户攻击计算机的企图。入侵防护还可用于监控 出站通信和防止蠕虫传播。

默认网络威胁防护策略适用于各种规模的公司。它不但可提供强大的防护,还能将 对端点资源的影响降到最低。您可以编辑默认策略或创建新策略,然后将它们应用 到您网络上的端点。

请参见第367页的"关于网络威胁防护与网络攻击"。

## 关于主动型威胁防护

主动型威胁防护能针对网络中的零时差攻击漏洞提供防护。零时差攻击漏洞是尚未 为人熟知的一种新漏洞。利用这些漏洞的威胁可避开以特征为基础的检测(例如防 间谍软件和防间谍软件定义)。零时差攻击可以用于针对特定目标的攻击和恶意代 码的传播。

主动型威胁防护包括下列几项:

- TruScan 主动型威胁扫描
- 应用程序与设备控制策略

主动型威胁防护的默认设置可适用于各种规模的公司。您可以编辑这些设置,也可 以在需要更改时创建新设置。

主动型威胁扫描使用启发式扫描来标记可能有害的进程和应用程序。启发式扫描会检查客户端计算机上进程的行为。例如,打开端口。

请参见第 419 页的"关于 TruScan 主动型威胁扫描"。

应用程序与设备控制策略则提供禁止或限制客户端计算机上的进程或硬件设备的方法。

请参见第 431 页的"关于应用程序与设备控制"。

## 关于主机完整性和端点策略遵循

主机完整性是用于定义、强制执行并还原用以保护企业网络和数据的客户端安全措施的功能。主机完整性策略可设置用来检查尝试访问网络的客户端是否在运行防病 毒软件、补丁程序、Hotfix以及其他应用程序条件。您可以将主机完整性策略设置 为在客户端计算机启动时运行和在客户端计算机启动后定期运行。

请参见第 477 页的"主机完整性强制执行的工作方式"。

主机完整性包括在 Symantec Network Access Control 中。主机完整性策略可确保 计算机满足您的 IT 指导方针并且修正发现的安全问题。您可以单独使用主机完整 性,也可将其与用于自我强制执行的隔离策略合并使用,或与网络 Enforcer 设备合 并使用。主机完整性策略与可选 Enforcer 合并使用时最为有效,因为该设备可确保 每台计算机只有在具备客户端软件且已适当配置的情况下,才能连接到网络。 Enforcer 可以是使用多种类型 Enforcer 软件的其中之一的硬件设备,也可以是多 种基于软件的 Enforcer 中的一种。与 Enforcer 合并使用时,主机完整性可允许或 禁止计算机访问网络。每一种 Enforcer 都是针对不同的网络要求设计的。

有关 Enforcers 的详细信息,请参见《Symantec Network Access Control Enforcer 操作指南》。

# 3

# 管理组、客户端、用户和 计算机

本章节包括下列主题:

- 关于组结构
- 关于导入现有组织结构
- 添加组
- 重命名组
- 移动组
- 查看组的属性
- 关于组从其他组继承位置及策略
- 禁用与启用组的继承
- 关于添加到组的客户端
- 以用户或计算机的形式添加客户端
- 在用户模式和计算机模式之间切换客户端
- 将非受管客户端转换为受管客户端
- 禁止客户端添加至组
- 在组间移动客户端
- 关于客户端状态图标
- 显示客户端和客户端计算机的状态

- 查看客户端的属性
- 过滤哪些用户和计算机出现在"客户端"选项卡上
- 搜索用户、客户端和计算机的信息
- 配置客户端检测未知设备
- 关于通过控制台在客户端上运行命令

## 关于组结构

在 Symantec Endpoint Protection Manager 中首先要进行的几项操作之一就是创 建组。组包含运行客户端软件的计算机。利用组可以管理具有相似安全需求和网络 访问需求的用户和计算机。

您可以添加组、用户和计算机,以满足您组织的业务需求。

您可以用以下任意参数为基础来建立组结构:

- 基于功能。 您可以针对笔记本电脑、台式机和服务器添加组。或者,您可以添加基于远程 用户(移动计算机)和本地用户(办公室内的计算机)的组。
- 基于职能或地理位置。 您可以针对部门职能添加组,例如销售、工程和营销部门中的所有客户端。
- 基于功能和职能的组合。 您可以基于职能添加父组,基于功能添加子组,如下所示:
  - 销售,下设有笔记本电脑、台式机和服务器子组。
  - 工程,下设有笔记本电脑、台式机和服务器子组。

组会定义安全设置和安全策略。您可以根据每个组的安全需求定义安全策略。这样 便可以将不同的策略分配给不同的客户端。

例如,一家公司有电话销售和会计部门。这些部门在公司的纽约、伦敦和法兰克福 办公室都有职员。这两个部门的所有计算机都分配给相同的组,使它们从相同来源 接收病毒及安全风险定义更新。但是,IT报告指出电话销售部门比会计部门更容易 受到风险的威胁。因此,系统管理员创建了电话销售组和会计组。电话销售客户端 会共享严格限制用户与病毒和安全风险防护交互方式的配置选项。

您可以手动添加组、用户和计算机,从目录服务器导入它们,或通过客户端注册自 动添加它们。

请参见第 42 页的"关于导入现有组织结构"。

## 关于默认组和子组

My Company 组是此层次结构树的根。在 My Company 组下,您可以添加子组。 您可以创建多个子组,各个子组可包括多个子级子组。子级子组可使用与父级组相 同的安全设置,也可以使用不同的安全设置。

请参见第44页的"关于组从其他组继承位置及策略"。

在 My Company 组下,树包括 Default 组。用户和计算机第一次注册 Symantec Endpoint Protection 时,不一定都会分配至组。若它们不属于预定义的组,就会给 分配至 Default 组。

注意:您不能在 Default 组下创建子组。

某些安全设置属于组特定,而某些设置属于位置特定。当您需要自定义特定于位置 的任何设置时,可以将位置添加到组中。

请参见第 273 页的"关于组的位置"。

## 关于客户端安装软件包中指定的组

创建客户端安装软件包进行部署时,您可以指定要使客户端计算机成为其中成员的 组。在计算机上安装客户端安装软件包后,客户端计算机会成为此首选组的成员。 然而,管理服务器可以覆盖客户端安装软件包中的首选组设置。例如,在"客户 端"页面上,您可以添加客户端的计算机帐户。您可以在除客户端安装软件包中首 选组之外的其他组下添加计算机。客户端连接至管理服务器后,在"客户端"页面 上将计算机帐户添加到的组会覆盖首选组。

请参见第 46 页的"以用户或计算机的形式添加客户端"。 基于下列任一原因,服务器可能不允许客户端加入到首选组:

- 首选组不存在或已经删除。
   客户端会置入"默认组"。
- 客户端是新的客户端,但是服务器阻止客户端加入到组中。
   客户端会置入"默认组"。
   请参见第49页的"禁止客户端添加至组"。
- 客户端先前注册到其他组,而您使用"导出通信设置"命令试图将客户端转至新的组。
   客户端会停留在原始的组中。
   请参见第 48 页的"将非受管客户端转换为受管客户端"。

## 关于导入现有组织结构

您可以导入组结构(或称组织单位)。若要导入组织单位,您可以使用 LDAP 目录 服务器或 Active Directory 服务器。Symantec Endpoint Protection 接着便会自动 将"客户端"选项卡上的组与目录服务器上的组同步。

在导入这些组之后,您不可用"客户端"选项卡加以管理。您不能在导入的组织单位中添加、删除或移动组。您可以将安全策略分配给导入的组织单位。您也可以将用户从导入的组织单位复制到"查看客户端"窗格中所列出的其他组。导入组前分配给该组的策略会优先采用。用户帐户可以同时存在于组织单位和外部组中。应用于外部组的策略会优先采用。

您可以从 Active Directory 服务器或 LDAP 服务器导入和同步用户帐户和计算机帐 户的相关信息。

请参见第 220 页的"关于组织单位和 LDAP 服务器"。

请参见第 221 页的"从 Active Directory 服务器或 LDAP 目录服务器导入组织单位"。

请参见第 217 页的"关于从 LDAP 目录服务器导入用户和计算机帐户信息"。

请参见第 215 页的"添加目录服务器"。

请参见第216页的"同步目录服务器和Symantec Endpoint Protection Manager之间的用户帐户"。

请参见第 221 页的"关于同步组织单位"。

## 添加组

您可以在定义组织的组结构之后添加组。

组说明最多可包含 1024 个字符。组名称和组说明可以包含除以下字符之外的任何 字符:["/\\*?<>|:].

注意:您不能向"默认组"添加组。

#### 添加组

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择要添加新子组的组。
- 3 在"客户端"选项卡的"任务"下,单击"添加组"。
- 4 在"添加 <组名> 的组"对话框中,键入组名和说明。
- 5 单击"确定"。

## 重命名组

您可以重命名组和子组以反映组织结构中的更改。您可以重命名组,自动为分配给 该组的所有用户和计算机,更新该组的名称。系统不会强制重命名后组中的客户端 计算机切换组或下载新的组配置文件。

#### 重命名组

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"选项卡的"查看客户端"下,右键单击要重命名的组,然后单击
   "重命名"。
- 3 在"重命名 <组名称>的组"对话框中,键入新的组名称。
- 4 单击"确定"。

## 移动组

任何组及其所包含的子组、计算机和用户都可以从组树的一个节点移动至另一节 点。然而,您不能移动MyCompany组或Default组。此外,您也不能移动Default 组下的组,也不能移动其子组下的组。

如果某组使用的是继承的策略,那么移动之后该组会使用其移动至的新组的继承策 略;如果该组已应用了某特定策略,则移动之后会继续使用该策略。

如果您所移动的组未显式应用任何组策略,那么它就会使用目标组的组策略。所移 动的组中的客户端会使用新的配置文件。

#### 移动组

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"选项卡的"查看客户端"下,右键单击要移动的组,然后单击"移动"。
- 3 在"移动组"对话框中,选择要将组转至的目标组。
- 4 单击"确定"。

## 查看组的属性

每个组都有其属性页。此页用于列出组的相关信息,

#### 查看组的属性

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"窗格中,选择您要查看其属性的组。
- 3 单击"详细信息"选项卡。

## 关于组从其他组继承位置及策略

在组结构中,子组起初会自动从其父组继承有关位置、策略和设置的信息。默认情况下,为每个组都启用了继承。不过,您可以随时禁用任何组的继承。

例如,您可能要创建一个"工程"组,并且带有名为"质量保证"的子组。"质量 保证"子组会自动包括与"工程"组相同的位置、策略和设置。

如果您想要更改"质量保证"子组中的策略和设置,首先必须禁用"质量保证"子 组的继承。如果您未禁用继承,则会显示一则消息说明您不能修改位置、策略或设 置,因为这些信息是从"工程"组继承而来的。

如果您创建一个子组,然后禁用子组的继承功能,子组的初始化设置将不会更改。 它将继续保持从源组所继承的位置和策略。

然而,对于独立于最初从其继承位置和策略信息的组的子组,您可以进行更改。如 果您在进行更改后又启用继承,则会覆盖子组设置中的所有更改。所继承其策略的 组的当前位置和策略会覆盖这些更改。

您也许想要将这些策略和设置分配到每个组。因此,在禁用子组的继承前,应当将 这些策略和设置添加到最上层的组中。如此,所有子组都可共享相同的位置和策略 信息,即使您之后再次启用继承。

请参见第381页的"添加继承自父组的规则"。

## 禁用与启用组的继承

您可以随时禁用和启用组的继承。在默认情况下,每当您为组创建新位置时,便会 启用继承。

#### 禁用或启用组的继承

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择要禁用或启用继承的组。 您可以选择与默认组关联的组以外的任何组。
- 3 在"策略"选项卡的 < 组名称> 窗格中, 运行下列其中一项任务:
  - 若要禁用继承,请取消选中"从父组 <组名称>继承策略和设置"。
  - 若要启用继承,请选中"从父组<组名称>继承策略和设置",然后在询问 是否继续时,选中"是"。

## 关于添加到组的客户端

客户端是指连接到企业网络并运行 Symantec Endpoint Protection 软件的任何网络 计算机或设备。网络设备可能包括笔记本电脑、台式机计算机及服务器。Symantec Endpoint Protection 客户端软件包用于部署到网络中的每一台计算机或设备。您可使用客户端软件来保护并管理网络中的计算机及用户。

每个客户端皆会执行下列任务:

- 连接到管理服务器以接收最新的策略与配置设置。
- 将各策略中的设置应用到每一台客户端计算机。 请参见第 35 页的"防护类别"。
- 更新最新的内容和病毒与安全风险定义。
- 将信息记在日志中,并将日志信息上载到管理服务器。

您可以设置客户端,在客户端物理位置更改时自动切换到另一安全策略;无伦您是 将客户端设为用户或计算机,皆可运行此项操作。客户端在办公室连接时会应用一 种策略,而进行远程连接时则应用另一种策略。

#### 关于受管和非受管客户端

Symantec Endpoint Protection 客户端分类如下:

- 受管客户端是已指派给管理服务器和组的Symantec客户端。这些客户端会从实际连接的服务器接收定义和内容文件。不过,客户端接收的配置设置和更新, 是以管理服务器策略被分配至的组为基础。 请参见第48页的"将非受管客户端转换为受管客户端"。
- 非受管客户端是未分配给管理服务器和组的客户端。这些客户端不会从任何管理服务器接收配置设置和更新。在非受管网络中,您必须单独管理每台计算机,或将管理职责转交给该计算机的主要用户。在信息技术支持有限或无支持的小型网络中,可以使用这种方法。 请参见第101页的"更改用户控制级别"。

## 关于用户模式和计算机模式

根据您希望策略工作的方式,可以将客户端设置为用户或计算机。设置为用户的客 户端会处于用户模式。设置为计算机的客户端会处于计算机模式。如果客户端设置 为用户,则基于登录网络的用户的名称。如果客户端设置为计算机,则基于登录网 络的计算机。您可以通过将用户和计算机添加到现有组,将客户端设置为用户或计 算机。将用户或计算机添加到组之后,相应的用户或计算机会采用之前分配至该组 的策略。

会使用哪一策略需视客户端软件运行时所处的模式而定。

#### 模式 说明

计算机模式 不论哪个用户登录到计算机,客户端都会使用相同的策略保护计算机。策略 会以计算机所在的组为准。计算机模式为默认设置。

#### 模式 说明

用户模式 策略会根据登录到客户端的用户而发生更改。策略会以用户为准。

如果客户端软件以用户模式运行,则客户端计算机软件会从相应用户所属组中获取 策略。如果客户端软件以计算机模式运行,则客户端计算机软件会从相应计算机所 属组中获取策略。

添加计算机之后,该计算机默认为计算机模式。计算机模式通常优先于用户模式。 登录相应计算机的用户会受应用于该计算机所属组的策略的限制。

请参见第46页的"以用户或计算机的形式添加客户端"。

添加为计算机模式的客户端可启用为非受管检测器,并且用于检测未授权的设备。 请参见第 55 页的"配置客户端检测未知设备"。

## 以用户或计算机的形式添加客户端

所有客户端都必须分配给组。组应包含具有相同安全要求和设置的客户端。

可以手动向组添加用户。但是,在大多数情况下,这是不切实际的做法,除非您想 针对维护目的,添加有限数目的用户。大多数管理员都会从 LDAP 服务器或域服务 器导入用户列表。

请参见第 42 页的"关于导入现有组织结构"。

您可以先手动将用户添加到特定组,然后再安装已为其分配首选组的客户端。可通 过在创建软件包时关联组策略,完成此任务。客户端会添加到服务器上指定的组, 而不是软件包中指定的组。

可以将客户端以计算机的形式添加到任何组。以计算机的形式添加客户端的主要原因是,不论登录到计算机的用户是谁,均可对计算机进行保护。例如,计算机可能位于易受攻击或未受保护的位置,例如公共大厅。可以将此计算机添加到包含其他公用计算机的组中,并为该组分配非常严格的安全策略。

向组添加计算机时,请注意以下几点事项:

- 您可以将计算机添加到多个组。
- 必须知道实际的计算机名和域,才能添加计算机。
- 计算机名的最大长度为64个字符。
- 说明字段的最大长度为 256 个字符。

请确保没有禁止客户端添加到组。

请参见第49页的"禁止客户端添加至组"。

查找新计算机并将其添加至组的最佳方法是使用"查找非受管计算机"工具。找到 未知和非受管计算机之后,您就可以将客户端安装软件包远程部署和安装到多台计 算机。

请参见第75页的"使用"查找非受管计算机"部署客户端软件"。

#### 以用户的形式添加客户端

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,找到要向其添加客户端的组。
- 3 在"客户端"选项卡中的"任务"下,单击"添加用户帐户"。
- 4 在"添加 <组名> 的用户"对话框中的"用户名"文本框中,键入新用户的名称。
- 5 在"域名"下,选择是要登录指定域,还是要登录本地计算机。
- 6 在"说明"文本框中,键入对此用户的可选说明。
- 7 单击"确定"。

#### 以计算机的形式添加客户端

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,找到要向其添加客户端的组。
- 3 在"客户端"选项卡中的"任务"下,单击"添加计算机帐户"。
- 4 在"添加计算机"对话框中,键入计算机的名称以及要将此计算机添加到的 域。
- 5 在"说明"文本框中,键入对此计算机的简短说明(此操作可选)。
- 6 单击"确定"。

## 在用户模式和计算机模式之间切换客户端

您可以配置客户端在用户模式或计算机模式下运行。在用户模式下,用户登录的客 户端计算机会采用用户所属组的策略。在计算机模式下,客户端会采用计算机所属 组的策略。应用的策略与登录计算机的用户无关。

如果从用户模式切换到计算机模式,您需要注意下列状况:

- 计算机名可能尚未包含在任何组中。切换到计算机模式时,会从组中删除客户端的用户名,并将客户端的计算机名称添加到该组。
- 客户端的计算机名和用户名位于同一个组中。从用户模式切换到计算机模式时, 会从组中删除用户名,然后客户端会采用该计算机名称。
- 客户端的计算机名与用户名包含在不同的组中。切换到计算机模式时,会将客 户端的组更改为计算机的组。系统会显示消息,通知您组的名称已更改。

如果从计算机模式切换到用户模式,您需要注意下列状况:

- 登录用户名尚未包含在任何组中。切换到用户模式时,会从组中删除客户端的 计算机名称。然后,将客户端的用户名添加到组中。
- 组可能包括客户端的登录用户名和计算机的登录用户名。从计算机模式切换到 用户模式时,会从组中删除计算机名称。客户端会采用该用户名。
- 客户端的计算机名与用户名包含在不同的组中。切换到用户模式时,会将客户端的组更改为用户的组。系统会显示消息,通知您组的名称已更改。

#### 在用户模式和计算机模式之间切换客户端

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择包括用户或计算机的组。
- 3 在"客户端"选项卡上,右键单击表中的计算机或用户名,然后选择"切换到 计算机模式"或"切换到用户模式"。

此模式为切换设置,因此始终会显示其中一种模式。表中的信息会更改以反映 新设置。

## 将非受管客户端转换为受管客户端

如果用户是从安装光盘安装客户端,客户端即为非受管客户端,而且不会与管理服 务器进行通信。

您可以使用下列步骤将非受管客户端转换为受管客户端:

- 针对要使客户端出现在其中的组,导出包括全部通信设置的文件。 默认的文件名称为 <组名称>\_sylink.xml。
- 您可将文件部署至客户端计算机。
   您能够将文件保存在网络位置,也可以将其发送至客户端计算机上的单个用户。
- 在客户端计算机上,用户可导入文件。
   您或用户都不需要重新启动客户端计算机。
   有关用户如何导入文件的详细信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 客户端指南》。

客户端会立即连接至管理服务器。管理服务器会将客户端放置于通信文件中所指定 的组中。客户端会使用组的策略和设置进行更新。客户端与管理服务器进行通信 后,通知区域图标会出现在客户端计算机的桌面上。

非受管客户端未受到密码保护,因此用户不需要在客户端键入密码。然而,如果用 户要将文件导入至受密码保护的受管客户端,则用户必须键入密码。此密码与用来 导入或导出策略的密码相同。

请参见第105页的"使用密码保护客户端"。

您可能也需要将受管客户端重定向到其他服务器。

请参见第 115 页的"使用 SylinkDrop 工具恢复客户端通信设置"。

请参见第110页的"将管理服务器列表分配给组和位置"。

#### 将非受管客户端转换为受管客户端

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择要使客户端在其中出现的组。
- 3 在组上单击鼠标右键,然后单击"导出通信设置"。
- 4 在"导出 <组名称> 的通信设置"对话框中,单击"浏览"。
- 5 在"选择导出文件"对话框中,找出要将.xml文件导出至的文件夹,然后单击 "确定"。
- 6 在"导出 <组名称> 的组注册设置"对话框中,选择下列其中一个选项:
  - 若要从计算机为其中成员的组中应用策略,请单击"计算机模式"。
  - 若要从用户为其中成员的组中应用策略,请单击"用户模式"。
- 7 单击"导出"。

如果文件名称已经存在,请单击"确定"以覆盖文件,或单击"取消"以新的文件名称保存文件。

## 禁止客户端添加至组

您可以设置已定义组成员资格的客户端安装软件包。如果您在软件包中定义了组,则客户端会自动添加到相关组。第一次添加客户端时,会连接至管理服务器。 如果您不希望客户端在连接至网络时自动添加到特定组,可以打开禁止功能。

**注意**:禁止选项可阻止用户自动添加到组。您可以禁止新客户端添加到已在客户端 安装软件包中分配给用户的组。在此情况下,该客户端会添加到 Default 组。您可 以手动将用户或计算机移到禁止的组。

#### 禁止客户端添加至组

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"中,选择您要禁止新客户端的组。
- **3** 单击"详细信息"选项卡。
- 4 在"详细信息"选项卡的"任务"下方,单击"编辑组属性"。
- 5 在 "<组名称> 的组属性"对话框中,单击"禁止新客户端"。
- 6 单击"确定"。

## 在组间移动客户端

您可以在组和子组之间移动客户端。移动客户端后,客户端会切换到新组。 您不能在组织单位中移动客户端。您可以将客户端从组织单位复制到 Symantec Endpoint Protection Manager 组。

#### 在组间移动客户端

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,找出含有所需移动客户端的组。
- 3 在"客户端"选项卡上,右键单击要移动的客户端,然后单击"移动"。 使用 Shift 键或 Ctrl 键可选择所有客户端或特定客户端。
- 4 在"移动组: <组名称>"对话框中,选择要将所选择客户端移动到其中的组。
- 5 单击"确定"。

## 关于客户端状态图标

查看组中的客户端时,客户端旁会显示图标,指示客户端的状态。 表 3-1 列出并说明这些图标。

图标	说明
<b>⊡1</b> ∵0	此图标指示下列状态: ■ 客户端正与 Symantec Endpoint Protection Manager 进行通信。 ■ 客户端处于计算机模式。
	<ul> <li>此图标指示下列状态:</li> <li>客户端未与 Symantec Endpoint Protection Manager 进行通信。</li> <li>客户端处于计算机模式。</li> <li>客户端可能已从控制台添加,但可能尚未安装任何 Symantec 客户端软件。</li> </ul>
ä	此图标指示下列状态: ■ 客户端正与 Symantec Endpoint Protection Manager 进行通信。 ■ 客户端处于计算机模式。 ■ 客户端为非受管检测器。

表 3-1 客户端状态图标

图标	说明
	此图标指示下列状态: ■ 客户端未与 Symantec Endpoint Protection Manager 进行通信。 ■ 客户端处于计算机模式。 ■ 客户端为非受管检测器。
2	此图标指示下列状态: ■ 客户端正与 Symantec Endpoint Protection Manager 进行通信。 ■ 客户端处于用户模式。
8	<ul> <li>此图标指示下列状态:</li> <li>客户端未与 Symantec Endpoint Protection Manager 进行通信。</li> <li>客户端处于用户模式。</li> <li>客户端可能已从控制台添加,但可能尚未安装任何 Symantec 客户端软件。</li> </ul>
8	<ul> <li>此图标指示下列状态:</li> <li>■ 客户端正与另一站点上的 Symantec Endpoint Protection Manager 进行通信。</li> <li>■ 客户端处于计算机模式。</li> </ul>
9	<ul> <li>此图标指示下列状态:</li> <li>客户端正与另一站点上的 Symantec Endpoint Protection Manager 进行通信。</li> <li>客户端处于计算机模式。</li> <li>客户端为非受管检测器。</li> </ul>
<b>3</b>	<ul> <li>此图标指示下列状态:</li> <li>■ 客户端正与另一站点上的 Symantec Endpoint Protection Manager 进行通信。</li> <li>■ 客户端处于计算机模式。</li> </ul>

客户端的用户会看见图标指出与管理服务器进行通信的状态。有关详细信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 客户端 指南》。

## 显示客户端和客户端计算机的状态

您可以查看关于网络中客户端与计算机实时操作状态的信息。例如,您可以查看哪 些客户端具有最新的策略和定义。您可以查看计算机的IP地址,或者哪些计算机运 行特定的操作系统。

表 3-2	客戶端与计算机状态视图
视图	说明
默认视图	显示受管客户端、用户帐户以及未安装客户端的计算机帐户的列表。您可以查看计算机名称、域名,以及登录用户名。
	默认情况下为默认视图。
	"名称"栏会在各个客户端旁显示图标以指示状态。
	请参见第 50 页的"关于客户端状态图标"。
客户端状态	显示客户端的信息,例如组的策略序列号和客户端的版本号码。
防护技术	指示"防病毒和防间谍软件防护"、"网络威胁防护"和"自动防护" 是打开还是关闭。此视图也会显示最新特征与内容的日期和修订编号。
网络信息	显示客户端计算机网络组件的信息,例如计算机使用的网卡MAC地址。
客户端系统	显示客户端计算机的系统信息,例如可用磁盘空间量和操作系统版本编 号。

\_ \_ 

了解特定客户端的状态后,即可解决客户端计算机的任何安全问题。例如,您可能 必须下载最新的防病毒定义。您也可以从各个组远程运行命令,以进行启用"自动 防护"之类的操作。

请参见第56页的"关于通过控制台在客户端上运行命令"。

您也可以使用状态信息,运行已调度的快速报告。

请参见第150页的"创建快速报告"。

您也可以在各个客户端上单击鼠标右键,然后单击"属性",以查看这项信息的大 部分内容。您可以编辑的唯一字段是"默认视图"中的"说明"字段。

请参见第52页的"查看客户端的属性"。

#### 显示客户端和客户端计算机的状态

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,找出需要查看其信息的客户端所在的 组。
- 3 在"客户端"选项卡上,单击"查看"下拉列表,然后选择类别。

## 杳看客户端的属性

每个用户和计算机都有属性页。您可以编辑的唯一字段是"常规"选项卡的"描 述"字段。

该页面包括下列选项卡:

∎ 常规

显示组、域、登录名及计算机的硬件配置等相关信息。

■ 网络

显示 DNS 服务器、DHCP 服务器、WINS 服务器及计算机 IP 地址等相关信息。

∎ 客户端

显示从客户端计算机收集到的信息。此信息包括运行于计算机的客户端类型。 此外,它还列出特定软件和策略信息。此信息包括客户端软件版本、当前配置 文件序列号、当前特征序列号以及上次联机时间。

用户信息 显示当前登录计算机的用户相关信息。管理员选择启用用户信息收集时,系统 就会填入此信息。

请参见第73页的"收集用户信息"。

#### 查看客户端的属性

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"窗格中,选择要查看其中客户端属性的组。
- 3 在"客户端"选项卡上,选择客户端。
- 4 在"任务"下方,单击"编辑属性"。
- 5 在"客户端名称"对话框中,您可以查看客户端的信息。
- 6 单击"确定"。

## 过滤哪些用户和计算机出现在"客户端"选项卡上

您可以使用过滤功能,控制"客户端"选项卡上出现的用户和计算机。您可以配置 各页面出现的客户端数量。您也可以在"页码"字段中键入页码,直接转至特定的 页面。

#### 过滤哪些用户和计算机出现在"客户端"选项卡上

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"窗格中,选择要搜索的组。
- 3 在"任务"窗格中,单击"设置显示过滤器"。
- 4 在"设置显示过滤器"对话框中,选择下列其中一个选项:
  - 显示全部用户和计算机
  - 显示全部用户
  - 显示全部计算机
  - 显示联机状态(由用户名旁边的绿灯指示)

- 5 设置页面显示的客户端数量。有效值的范围为1到5000。
- 6 单击"确定"。

## 搜索用户、客户端和计算机的信息

您可以搜索客户端、客户端计算机和用户的信息,以便在充分掌握信息的状况下, 决定网络的安全。例如,您可以找出 Sales 组的哪些计算机运行最新的操作系统。 您也可以找出 Finance 组的哪些客户端计算机需要安装最新的防病毒定义。在"客 户端"页面上,您可以查看组中各客户端的信息。如果有许多客户端,您可以缩小 搜索范围。

请参见第51页的"显示客户端和客户端计算机的状态"。

您可以将查询中包括的数据导出至文本文件。

**注意:**若要搜索大多数关于用户的信息,您必须在客户端软件安装期间,或此后收 集用户信息。这项用户信息也会显示在客户端"编辑属性"对话框的"常规"选项 卡和"用户信息"选项卡上。

请参见第73页的"收集用户信息"。

请参见第 43 页的"查看组的属性"。

#### 搜索用户、客户端和计算机的信息

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"选项卡的"查看客户端"下,选择要搜索的组。
- 3 在"任务"下,单击"搜索客户端"。
- 4 在"搜索客户端"对话框的"查找"下拉列表中,单击"计算机"或"用户"。
- 5 单击"浏览"可选择默认组以外的其他组。
- 6 在"选择组"对话框中,选择组,然后单击"确定"。
- 7 在"搜索条件"下,单击"搜索字段"下拉列表,然后选择搜索的条件。
- 8 单击"比较运算符"下拉列表,然后选择比较运算符。 您可以在搜索条件中使用标准的布尔运算符。
- 9 在"值"单元格中,键入搜索字符串。
- 10 单击"搜索"。

您可以将结果导出至文本文件。

11 单击"关闭"。

## 配置客户端检测未知设备

未授权的设备能够以多种方式连接至网络,例如,会议室的物理访问或非授权无线 网络接入点。若要在各个端点强制执行策略,您必须能够迅速检测出是否有新的设 备出现。未知设备是未运行客户端软件的非受管设备。您必须判断这些设备是否安 全。您可以启用任何客户端作为非受管检测器,以检测未知设备。

设备启动时,操作系统会将ARP通信发送至网络,以告知其他计算机有设备出现。 启用成为非受管检测器的客户端会收集ARP数据包信息,然后发送至管理服务器。 管理服务器会在ARP数据包中搜索设备的MAC地址和IP地址。服务器会将这些 地址与服务器数据库中的现有MAC地址与IP地址列表相互比较。如果服务器找不 到匹配的地址,服务器会将该设备记录为新设备。然后您可以确定该设备是否安 全。由于客户端只传输信息,因此不会使用额外的资源。

您可以配置非受管检测器以忽略某些设备,例如打印机。您也可以设置电子邮件通知,以便在非受管检测器检测出未知设备时通知您。

若要将客户端配置为非受管检测器,必须执行下列操作:

- 启用网络威胁防护
- 将客户端切换为计算机模式。
   请参见第 47 页的"在用户模式和计算机模式之间切换客户端"。
- 在一台任何时间都在运行的计算机上安装客户端。
- 只启用 Symantec Endpoint Protection 客户端作为非受管检测器。 Symantec Network Access Control 客户端不可成为非受管检测器。

#### 配置客户端检测未授权设备

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择要从其中导出设置的组。
- **3** 在"客户端"选项卡上,在要启用为非受管检测器的客户端上单击鼠标右键, 然后单击"启用为非受管检测器"。
- 4 若要将一个或多个设备指定为排除在非受管检测器的检测范围之外,请单击 "配置非受管检测器"。
- 5 在"<客户端名称>发生非受管检测器异常"对话框中,单击"添加"。
- 6 在"添加非受管检测器异常"对话框中,单击下列其中一个选项:
  - "排除检测 IP 地址范围",然后键入多个设备的 IP 地址范围。
  - "排除检测 MAC 地址",然后键入设备的 MAC 地址。
- 7 单击"确定"。
- 8 单击"确定"。

#### 显示客户端检测的未授权设备列表

- 1 在控制台上,单击"主页"。
- 2 在"主页"页面的"安全状态"区段中,单击"更多详细信息"。
- 3 在"安全状态详细信息"对话框中, 滚动至"未知设备失败"表。
- 4 关闭对话框。

在"查找非受管计算机"对话框的"未知计算机"选项卡中,您也可以显示未 授权设备的列表。

有关详细信息,请参见《Symantec Endpoint Protection Manager 及 Symantec Network Access Control 安装指南》。

## 关于通过控制台在客户端上运行命令

通过 Symantec Endpoint Protection Manager 控制台,您可以在客户端或整个组 上运行命令。您可以从控制台的"客户端"选项卡或"监视器"选项卡运行命令。 请参见第 173 页的"从日志运行命令和操作"。

命令	说明
扫描	在客户端上运行按需扫描。
	请参见第 362 页的"运行按需扫描"。
取消所有扫描	取消当前在客户端计算机上运行的全部扫描。
更新内容	在客户端初始化 LiveUpdate 会话,以更新客 户端的内容。客户端计算机会从 Symantec LiveUpdate 接收最新的内容。
更新内容并扫描	初始化LiveUpdate 会话以更新内容,然后在 客户端上运行按需扫描。
重新启动客户端计算机	重新启动客户端计算机。
启用自动防护	在客户端启用"文件系统自动防护"。
	请参见第 346 页的"启用文件系统自动防 护"。
启用网络威胁防护	在客户端启用"网络威胁防护"。
	请参见第 400 页的"启用和禁用网络威胁防 护"。

<b>耒 २</b> ₋२	可在客户端上运行的命令
12 3-3	可任在广州上是门的职人

命令	说明
禁用网络威胁防护	在客户端禁用"网络威胁防护"。

您可以配置受限管理员有权使用其中某些命令或无权使用任何命令。默认为受限管理员有权使用全部的命令,但不包括"重新启动客户端计算机"。

58 | 管理组、客户端、用户和计算机 | **关于通过控制台在客户端上运行命令** 

# 4

# 管理域和管理员

本章节包括下列主题:

- 关于域
- 添加域
- 指定当前域
- 关于管理员
- 添加管理员帐户
- 关于访问权限
- 配置受限管理员访问权限
- 在管理员和受限管理员之间切换
- 在登录尝试太多次后,锁定管理员帐户
- 设置管理员帐户的验证
- 重命名管理员帐户
- 更改管理员的密码
- 删除管理员帐户

## 关于域

域是 Symantec Endpoint Protection Manager 控制台中的结构性容器,可用来组织组、客户端、计算机和策略的层次结构。您可以设置域以管理网络资源。Symantec Endpoint Protection Manager 中的域与 Microsoft 域无关。

如果您的公司规模相当大,在许多地区都有办公场所,您可能需要能够集中查看管 理信息。然而,您可以委派管理权限、实际分隔安全数据,或在用户、计算机和策 略的组织方式上具备更大灵活性。如果您是受管服务提供者 (MSP),可能需要管理 多家独立的公司以及 Internet 服务供应商。为满足这些要求,您可以创建多个域。 例如,针对各个国家/地区、区域或公司,您可以创建单独的域。

安装管理服务器时,控制台已含有一个域。您添加的各个域会共享相同的管理服务器和数据库。各个域都会提供额外的控制台实例。各个域的全部数据都会完全分隔。这种分隔可防止一个域的管理员查看其他域中的数据。您可以添加管理员帐户,以便各个域有各自的管理员。这些管理员可查看和管理自身域的内容,但是不能查看和管理其他域的内容。

请参见第63页的"添加管理员帐户"。



第一次添加域时,域中空无内容。您必须将该域配置为当前域,然后将组、客户 端、计算机和策略添加到此域。

请参见第61页的"指定当前域"。

您可以将策略和客户端从一个域复制到另一个域。若要在域间复制策略,您可以从 源域导出策略,然后将此策略导入目标域。若要在域间复制客户端,您可以使用 SylinkDrop工具。此工具会替换客户端的通信文件,以允许客户端与不同的管理服 务器进行通信。SylinkDrop工具位在光盘3的Tools\Nosupport\Sylinkdrop文件 夹中。

请参见第 291 页的"导出策略"。

请参见第 115 页的"使用 SylinkDrop 工具恢复客户端通信设置"。

您可以定义所需数量的域。

## 添加域

如果您想使用多个域,则可以添加域。举例来说,如果您管理多个相互独立的公司,则可以为每个公司使用独立的域。

请参见第59页的"关于域"。

**注意**:您可以使用域ID来进行灾难恢复。如果组织内的管理服务器都发生了故障,则必须使用与旧服务器相同的ID来重建管理服务器。您可以从任何客户端的 sylink.xml 文件获取旧的域ID。

#### 添加域

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"域"。
- **3** 在"任务"下,单击"添加域"。
- 4 在"添加域"对话框中,键入域名和公司名称(可选)。
- 5 在"联系人列表"文本框中,还可以选择键入其他信息,例如负责相应域的用户的名称。
- 6 如果您要添加域 ID,请单击"高级",然后在文本框中键入相应的值。
- 7 单击"确定"。

## 指定当前域

第一次在 Symantec Endpoint Protection Manager 控制台中新建域时,域中空无 内容。若要将新的组、客户端、策略和管理员添加到域,必须先指定何者为当前 域。在"域名"窗格中,文本内容(当前域)即得自域名。默认域名为 Default。 如果您有多个域,必须滚动浏览"查看域"列表,以显示何者为当前域。

如果您以系统管理员的身份登录控制台,不论何者为当前域,您都会看见全部的 域。不过,您只会看见当前域中创建的管理员和受限管理员。如果您以管理员或受 限管理员的身份登录控制台,则只会看见您有权访问的域。

如果删除当前的域,管理服务器会将您注销。只能删除不是当前域且不是唯一域的 域。

#### 指定当前域

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"域"。
- **3** 在"任务"下,单击"管理域"。

- 4 在"管理员域"对话框中,若要进行确认,请单击"是"。
- 5 单击"确定"。

## 关于管理员

使用管理员可管理公司的组织结构和网络安全。针对小公司,您可能只需要一个管理员。如果是拥有多个站点和域的大公司,则需要多个管理员,其中某些管理员比 其他管理员拥有更多访问权。

为帮助您管理网络, Symantec Endpoint Protection Manager 控制台提供了下列类型的管理员角色:系统管理员、管理员以及受限管理员。

系统管理员是网络的超级管理员。系统管理员可以查看和修改整个组织。管理员和 受限管理员都较系统管理员低一个级别。管理员只能查看和管理一个域内的所有任 务。受限管理员则只能管理域内的特定任务。例如,受限管理员只能管理域内有限 数量的组。

表4-1列出每种管理员角色的责任。

管理员角色	责任
系统管理员	<ul> <li>系统管理员可以执行下列任务:</li> <li>管理所有域。</li> <li>创建和管理全部域的所有其他管理员帐户、管理员帐户和受限管理员帐户。</li> <li>管理数据库和管理服务器。</li> <li>可以查看和使用所有控制台设置。</li> </ul>
管理员	<ul> <li>管理员可以执行下列任务:</li> <li>管理单个域</li> <li>创建和管理单个域内的管理员帐户和受限管理员帐户。 这些权限包括通知、安全设置、组设置和策略设置。</li> <li>不能管理数据库或管理服务器。</li> <li>只能查看和使用单个域的所有控制台设置。</li> </ul>

表 4-1 管理员类型角色和责任

管理员角色	责任
受限管理员	<ul> <li>受限管理员可以执行下列任务:</li> <li>执行域内的任务,但不能管理域。</li> <li>在单个域内管理报告、运行远程命令和配置特定组的策略。</li> <li>受限管理员没有特定策略和相关设置的访问权,因此不能查看或修改策略。此外,他们也不能应用、更换或撤回策略。</li> <li>不能创建其他受限管理员此户</li> </ul>
	<ul> <li>■ 只有系统管理员或管理员可以配置受限管理员的权限。</li> <li>■ 只能管理自己帐户的密码权限。</li> <li>■ 只在拥有提供的报告权限时,才能在控制台中查看"主页"、"监视器"或"报告"页面。</li> </ul>

您可以在组织中定义每个管理员类型的管理员角色。例如,大公司可能会使用下列 管理员类型:

- 负责安装管理服务器和客户端安装软件包的管理员。安装产品后,将由负责操作的管理员接管。
- 操作管理员,将负责维护服务器、数据库以及安装修补程序。
- 防病毒管理员,负责在客户端上创建和管理防病毒和防病毒策略以及LiveUpdate 策略。
- 桌面管理员,负责客户端安全和为客户端创建、维护防火墙策略和入侵防护策略。
- 服务台管理员,负责创建报告,对策略具有只读访问权。防病毒管理员和桌面 管理员会读取服务台管理员发送的报告。

在此方案中,安装管理服务器的管理员和操作管理员应为系统管理员。防病毒管理员和桌面管理员则只是所属域的管理员。服务台管理员则为受限管理员。

当您安装 Symantec Endpoint Protection Manager 时,会创建名为 admin 的默认 系统管理员。然后您可以为任何添加的管理员创建帐户。

## 添加管理员帐户

随着网络的扩展或变化,您可能会发现管理员数目不足以满足需要。您可以添加一 个或多个管理员。添加管理员时,您可以指定管理员的权利和限制。作为系统管理 员,您可以添加其他系统管理员、管理员或受限管理员。作为域管理员,您可以添 加其他管理员和受限管理员,并可以配置其权限。

请参见第62页的"关于管理员"。

**警告:**如果为自己创建一个新的管理员帐户,则可以覆盖您自己的登录用户名和密 码。

#### 添加管理员

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"管理员"。
- 3 在"任务"下方,单击"添加管理员"。
- 4 在"添加管理员"对话框中,输入管理员名称。 此名称是管理员登录时使用的名称,也是在应用程序中用来标识管理员的名称。
- 5 第二个文本框为可选字段,可输入管理员的全名。
- 6 键入密码,再重新键入一次。 密码不得少于六个字符。允许使用所有字符。
- 7 若要配置身份验证方法,请单击"更改"。

默认值为"Symantec Management Server 验证"。可以为默认方法配置密码 到期时间,也可以更改身份验证方法。

请参见第67页的"设置管理员帐户的验证"。

- 8 单击"确定"。
- 9 选择以下管理员类型之一:
  - 系统管理员
  - 管理员 管理员可以针对所有组运行报告。如果从 Symantec AntiVirus 10.x 进行了 迁移,并且希望管理员针对这些迁移后的服务器组运行报告,请单击"报 告权限",
  - 受限管理员
     请参见第 65 页的"配置受限管理员访问权限"。
- 10 单击"确定"。

## 关于访问权限

默认情况下,管理员可访问单个域的全部功能。这些管理员也可以在域的全部组运行报告,但不包括从 Symantec AntiVirus 10.x 迁移的组。您必须明确配置这些已 迁移组的报告权限。 默认情况下,受限管理员不拥有任何访问权限。您必须明确配置此类管理员的报告 权限、组权限、命令权限和策略权限。

注意: 当您限制访问权限时, 部分用户界面不能供受限管理员使用。

当您限制权限时,也会限制这些受限管理员可在"监视器"选项卡上查看或操作的 日志类型。您也可以限制"客户端"页面的"策略"选项卡设置。

默认情况下,管理员拥有全部的访问权限,但不包括 Symantec AntiVirus 10.x 服务器组的报告权限。默认情况下,受限管理员不拥有任何访问权限,您必须明确配置其权限。

访问权限的类型	说明
报告权限	对于管理员,指定管理员可查看其报告的运行 Symantec AntiVirus 10.x 的服务器组。管理员可查 看其他所有的报告。
	对于受限管理员,指定管理员可运行报告的所有计算机。另外指定管理员可查看其报告的运行 Symantec AntiVirus 10.x 的服务器组。
组权限	仅针对受限管理员,指定受限管理员可查看和管理 (完全访问权)、仅可查看(只读访问权)或不能查 看(没有访问权)的组。
命令权限	仅针对受限管理员,指定受限管理员可在客户端计算机上运行的命令。只有在具有完全访问权的客户端和 组上,受限管理员才能运行这些命令。
	仅当为受限管理员配置了报告权限或组权限时,才提供命令权限。
策略类型权限	仅针对受限管理员,指定管理员可管理的策略与策略 相关设置。

表 4-2 访问权限的类型

## 配置受限管理员访问权限

如果您添加受限管理员帐户,也必须指定管理员的访问权限。您必须在所创建的受限管理员处于禁用状态且不能登录管理服务器时指定访问权限。

#### 配置受限管理员权限

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"管理员"。

- 选择受限管理员。
   创建受限管理员帐户时,您也可以配置访问权限。
   请参见第 63 页的"添加管理员帐户"。
- 4 在"任务"下方,单击"编辑管理员属性",然后单击"访问权限"。
- 5 在"访问权限"选项卡上,确定已选择"受限管理员",然后运行下列其中一 项操作:
  - 选中"查看报告",然后单击"报告权限"。
  - 选中"管理组",然后单击"组权限"。
  - 选中"在客户端计算机上远程运行命令",然后单击"命令权限"。
  - 选中"管理策略",然后单击"策略类型权限"。 您可以选中"仅允许编辑特定于位置的策略",许可管理员只创建位置的 非共享策略。
- 6 单击"确定"。

## 在管理员和受限管理员之间切换

您可以将管理员更改为受限管理员,或是将受限管理员更改为管理员。如果某个管理员的职责有所更改,则您最好更改其管理员类型。例如,您或许想要让一个受限 管理员能够创建其他管理员帐户。或者,您可能想要将某个管理员切换为受限管理 员,以便限制其访问权限。

#### 在管理员和受限管理员之间切换

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"管理员"。
- 3 在"查看管理员"下方,选择管理员。
- 4 在"任务"下方,单击"编辑管理员属性",然后单击"访问权限"。
- 5 在"访问权限"选项卡上,执行下列其中一项操作:
  - 单击"管理员"。 如果从 Symantec AntiVirus 10.x 进行了迁移,并且希望管理员针对这些迁移后的服务器组运行报告,请单击"报告权限"、
  - 单击"受限管理员"。 配置该受限管理员的权限。
- 6 单击"确定"。

## 在登录尝试太多次后,锁定管理员帐户

经过特定次数的登录尝试后,您可以锁定管理员帐户。您也可以配置管理服务器发 送电子邮件消息给管理员,告知已锁定帐户的状况。通知会警告管理员有其他用户 尝试以管理员证书登录。

管理员帐户默认会在5次登录尝试后遭锁定。登录尝试值会重置为0(在管理员成 功登录并于稍后注销之后)。

稍后管理员再次尝试登录的次数达到最大次数。管理员达到登录尝试失败次数限制 后,就会锁定该帐户。此后管理员必须等待指定的分钟数之后,才能尝试再次登 录。

#### 在登录尝试太多次之后,锁定管理员帐户

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"管理员"。
- 3 在"查看管理员"下方,选择管理员。
- 4 在"任务"下方,单击"编辑管理员属性"。
- 5 在"常规"选项卡的"电子邮件"文本框中,键入管理员的电子邮件地址。 管理服务器已锁定管理员的帐户时,管理服务器会将电子邮件消息发送到此电 子邮件地址。您必须选中"帐户被锁定时发送电子邮件警报"复选框,以提交 电子邮件消息。
- 6 在"登录尝试次数阈值"之下,移动滑块以设置允许登录尝试错误的次数。
- 7 若要在管理员超过登录尝试次数时锁定帐户,请单击"当尝试次数超过阈值 时,锁定这个帐户"。
- 8 选中或取消选中"帐户被锁定时发送电子邮件警报",然后设置分钟数。
- 9 单击"确定"。

## 设置管理员帐户的验证

添加管理员时,您可以指定管理服务器要使用哪一种验证方法来验证管理员帐户。

您可以使用管理服务器搭配 RSA SecurID 来验证管理员。您必须确保您已有一台现成的 RSA 服务器,而且已在另一台计算机上安装和配置了 RSA SecurID 服务器。此外还将验证 RSA SecurID 服务器是否能与 SecurID Agent 通信。

您可以为 Symantec Endpoint Protection Manager 上的管理器帐户启用 RSA 安全。 支持的 RSA 登录机制包括:

- RSA SecurID 令牌(非软件 RSA 令牌)
- RSA SecurID 卡

■ RSA 键区卡(非 RSA 智能卡)

#### 设置管理员帐户的验证

1 添加管理员帐户。

请参见第63页的"添加管理员帐户"。

- 2 在"管理员"页面的"查看管理员"下,选择管理员。
- 3 在"任务"下方,单击"编辑管理员属性",然后单击"验证"。
- 4 在"验证"选项卡上,选择下列其中一个要用来验证管理员帐户的选项:
  - Symantec Management Server 验证, 然后选择验证密码何时过期。 请参见第 215 页的"添加目录服务器"。
  - RSA SecurID 验证 请参见第 228 页的"将 Symantec Endpoint Protection Manager 配置为使 用 RSA SecurID 验证"。
  - 目录验证 然后键人目录服务器和管理员帐户名称。
- 5 单击"确定"。

## 重命名管理员帐户

为了更改组织内的职责或分配,您可能想要更改您设置的管理员帐户的名称。

#### 重命名管理员帐户

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"管理员"。
- 3 在"查看管理员"下,选择要重命名的管理员。
- 4 在"任务"下,单击"重命名管理员"。
- 5 在"重命名 <名称> 的管理员"对话框中,更改该帐户名称。
- 6 单击"确定"。

## 更改管理员的密码

基于安全理由,您可能需要更改管理员的密码。

当您在管理服务器配置向导中配置管理服务器时,请选择简单或高级安装。若您选 择简单安装,则输入的密码与加密密码相同。若您更改管理员的密码,则加密密码 不会有所更改。

#### 更改管理员的密码

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"管理员"。
- 3 在"查看管理员"下方,选择管理员。
- 4 在"任务"下方,单击"更改管理员密码"。
- 5 输入并确认新密码。

密码必须包括六个或六个以上字符,任何字符都可使用。

6 单击"确定"。

## 删除管理员帐户

您可以删除不再需要的管理员帐户。

#### 删除管理员帐户

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面中,单击"管理员"。
- 3 在"查看管理员"下,选择要删除的管理员。
- 4 在"任务"窗格下,单击"删除管理员"。
- 5 在消息框中,单击"是"以确认您要删除此管理员。

70 | 管理域和管理员 | 删除管理员帐户

## 使用客户端安装软件包

本章节包括下列主题:

- 关于客户端安装软件包
- 配置客户端安装软件包选项
- 导出客户端安装软件包
- 使用"查找非受管计算机"部署客户端软件
- 关于添加客户端安装软件包更新和升级客户端
- 添加客户端安装软件包更新
- 升级一个或多个组中的客户端
- 删除升级软件包

## 关于客户端安装软件包

若要管理具有 Symantec Endpoint Protection Manager 控制台的计算机,您必须 将至少一个客户端安装软件包导出至站点中的管理服务器。导出客户端安装软件包 之后,将软件包中的文件安装在客户端计算机上。您可以导出 Symantec 受管客户 端、第三方受管客户端,以及非受管客户端的软件包。

您可以使用控制台将这些软件包以单个可执行文件的形式或目录中一系列文件的形 式导出。您选择的方法取决于您的部署方法,以及您是否要从控制台升级组中的客 户端软件。单个可执行文件可用于第三方安装工具和潜在带宽守恒。通常,如果您 使用 Active Directory 组策略对象,则不会选择导出至单个可执行文件。

导出期间,您可以选择默认提供的32位安装软件包或64位安装软件包。如果您并不想安装所有的组件,则可以选择安装特定的客户端防护技术。您也可以指定安装 程序与最终用户的交互方式。最后,您可以将导出的文件(一个软件包)一次安装 到一台计算机,也可以将导出的文件同时部署到多台计算机。 有关客户端安装部署选项,请参见光盘上的《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

Symantec 有时会提供安装文件的更新软件包。当客户端软件安装在客户端计算机 上时,您可以用自动升级功能,自动更新组中所有客户端上的客户端软件。您无需 使用安装部署工具来重新部署软件。

## 配置客户端安装软件包选项

导出客户端安装软件包时,您可以选择要安装哪些客户端组件及如何安装。您可以 选择提示用户发送其自身的相关信息,此信息会在控制台中显示为计算机的属性。

#### 配置客户端安装软件包功能

安装功能是可用于安装的客户端组件。例如,如果您创建 Symantec Endpoint Protection 软件包,则可以选择安装防病毒功能和防火墙功能。另外,您也可以选择只安装防病毒功能。

您必须命名每组选项。然后,在导出 32 位客户端软件包或 64 位客户端软件包时,选择已命名的功能集。

#### 配置客户端安装软件包功能

- 1 在控制台中,单击"管理员",再单击"安装软件包"。
- 2 在"查看安装软件包"下,单击"客户端安装功能集"。
- 3 在"任务"下,单击"添加客户端安装功能集"。
- 4 在"添加客户端安装功能集"对话框的"名称"框中键入名称。
- 5 在"说明"框中,键入客户端安装功能集的说明。
- 6 有关设置此对话框中其他选项的详细信息,请单击"帮助"。
- 7 单击"确定"。

#### 配置客户端安装软件包设置

安装设置会影响客户端安装软件在客户端计算机上的安装方式。您必须命名每组选项。然后,在导出 32 位客户端软件包或 64 位客户端软件包时,选择已命名的一组软件包设置。

#### 配置客户端安装软件包设置

- **1** 在"管理员"选项卡的左下方窗格中,单击"安装软件包"。
- 2 在"查看安装软件包"下,单击"客户端安装设置"。
- 3 在"任务"下,单击"添加客户端安装设置"。
- 4 在"客户端安装设置"对话框的"名称"框中键入名称。
- 5 有关设置此对话框中其他选项的详细信息,请单击"帮助"。
- 6 单击"确定"。

#### 收集用户信息

在进行客户端软件安装或策略更新时,您可以提示客户端计算机的用户键入自己的 相关信息。您可以收集员工的有关信息,包括移动电话号码、职务和电子邮件地址 等。收集此信息之后,您必须对其进行手动维护和更新。

**注意**:在第一次启用在客户端计算机上显示的消息后,如果用户已通过提供所需的 信息予以响应,则该消息不会再次出现。即使之后编辑任何字段,或禁用并再次启 用消息,客户端也不会显示新消息。然而,用户可以随时编辑信息,而且管理服务 器也会检索此类信息。

#### 收集用户信息

- 1 在控制台中,单击"管理员",再单击"安装软件包"。
- 2 在"查看安装软件包"下,单击"客户端安装软件包"。
- 3 在"客户端安装软件包"窗格中,单击您要收集其用户信息的软件包。
- 4 在"任务"下方,单击"设置用户信息收集"。
- 5 在"设置用户信息收集"对话框中,选择"收集用户信息"。
- 6 在"消息"文本框中,键入您想要用户在收到需要其提供相应信息的提示时阅 读的消息。
- 7 如果您想让用户能够推迟用户信息收集,请选中"启用"以后提醒我"",然 后设置一个以分钟为单位的时间。
- 8 在"选择要显示给用户以提供输入的字段"下,选择要收集的信息类型,然后 单击"添加"。

您可以通过按 Shift 键或 Ctrl 键来同时选择一个或多个字段。

- 9 在"可选"栏中,在您要定义为用户选填的字段旁选中复选框。
- 10 单击"确定"。

### 导出客户端安装软件包

导出客户端软件时,会创建客户端安装文件以便用于部署。导出软件包时,您必须 浏览至要包含导出软件包的目录。如果您指定的目录不存在,则会自动为您创建该 目录。导出进程会在此目录中创建具有叙述性名称的子目录,并将安装文件放在这 些子目录中。

例如,如果您为"我的公司"下名为 MyGroup 的组创建一个安装软件包,则会创建一个名为 My Company\_MyGroup 的目录。此目录会包含导出的安装软件包。

**注意**:此命名惯例不会区分 Symantec Endpoint Protection 和 Symantec Network Access Control 的客户端安装软件包。对于 Symantec Endpoint Protection 和 Symantec Network Access Control,单个可执行文件的导出软件包的名称都为 Setup.exe。因此,请务必创建目录结构,以便区分 Symantec Endpoint Protection 和 Symantec Network Access Control 的安装文件。

导出软件包时,您必须做出一项重要决定。您必须决定是创建受管客户端的安装软件包还是非受管客户端的安装软件包。如果您创建受管客户端的软件包,则可以使用 Symantec Endpoint Protection Manager 控制台管理这些客户端。如果您创建 非受管客户端的软件包,则不能从控制台管理这些客户端。

**注意**:如果从远程控制台导出客户端安装软件包,就会在运行远程控制台的计算机 上创建软件包。此外,如果您使用多个域,则必须导出每个域的软件包,否则这些 软件包不能用于域组。

导出一或多个安装软件包文件后,您可以在客户端计算机上部署安装文件。

有关客户端软件安装的详细信息,请参见光盘上的《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

#### 导出客户端安装软件包

- 1 在控制台中,单击"管理员",再单击"安装软件包"。
- 2 在"查看安装软件包"下,单击"客户端安装软件包"。
- 3 在"客户端安装软件包"窗格中的"软件包名称"下,单击要导出的软件包。
- 4 在"任务"下,单击"导出客户端安装软件包"。
- 5 在"导出软件包"对话框中,单击"浏览"。
- 6 在"选择导出文件夹"对话框中,浏览并选择要包含导出软件包的目录,然后 单击"确定"。

不支持并禁止包含双字节或高位 ASCII 字符的目录.

- 7 在"导出软件包"对话框中,根据您的安装目的设置其他选项。
- 8 有关设置此对话框中其他选项的详细信息,请单击"帮助"。
- 9 单击"确定"。

### 使用"查找非受管计算机"部署客户端软件

您可使用 Symantec Endpoint Protection Manager 控制台中的"查找非受管计算机"来部署客户端软件。使用此实用程序,您可以发现没有运行客户端软件的客户端计算机,然后在这些计算机上安装客户端软件。

**注意**:如果 LAN Manager 的身份验证级别与六个定义的身份验证级别不兼容,这 个实用程序就会将非受管计算机归为未知的类别。Symantec 建议使用"仅发送 NTLM 2 响应"级别。可编辑的策略位于"本地策略设置">"安全设置">"本地 策略">"安全选项">"[网络安全] LAN Manager 身份验证级别"下。此外,从 默认的 Windows Server 2003 安装运行此实用程序时,此实用程序不能正确识别 Windows 2000 操作系统。若要避开此限制,请在"服务"面板中,以"管理员" 而非"系统"的身份运行 Symantec Endpoint Protection Manager 服务。

警告:此实用程序会检测各种网络设备,并将其显示在未知计算机选项卡上。例如,此实用程序检测到路由器接口,并会将这些接口放置在未知计算机选项卡上。 在将客户端软件部署至出现在非受管计算机选项卡上的设备时,应格外谨慎。请确 认这些设备都是客户端软件部署的有效目标。

#### 使用"查找非受管计算机"部署客户端软件

- **1** 在 Symantec Endpoint Protection Manager 控制台中,单击"客户端"。
- 2 在"任务"窗格中,单击"查找非受管计算机"。
- 3 在"搜索非受管计算机"窗口中的"搜索依据"下,选中"IP地址范围"后, 再键入搜索范围的 IP 地址。

扫描 100 个不存在的 IP 地址大约需要 5 分半钟。或者,可以指定计算机名。

- **4** 在"登录证书"下,用允许管理和安装的登录凭据完成"用户名"、"密码" 和"域工作组"框的填写。
- 5 单击"立即搜索"。
- 6 在"未知的计算机"或"非受管计算机"选项卡上,执行下列任一操作:
  - 选中每台要安装客户端软件的计算机。
  - 单击"全选"。
- 7 在"安装"下,选择安装软件包、安装选项以及要安装的功能。
- 8 若要不安装到 Temporary 组,请单击"更改",选择其他组,然后单击"确 定"。
- 9 准备好安装客户端软件后,请单击"开始安装"。

### 关于添加客户端安装软件包更新和升级客户端

Symantec提供客户端安装软件包的更新时,您必须先将这些更新添加到Symantec Endpoint Protection Manager,并且使这些更新可供导出。但您不需要使用客户端 部署工具重新安装这些更新。若要使用最新软件更新组中的客户端,最简易的方式 是使用控制台更新包括客户端的组。您应该先更新测试计算机数量较少的组。如果 您允许客户端运行 LiveUpdate,而且 LiveUpdate 设置策略允许更新,则您也可以 使用 LiveUpdate 更新客户端。

### 添加客户端安装软件包更新

您从 Symantec 接收客户端安装软件包更新,然后您将它们添加到站点数据库,以 使其可从 Symantec Endpoint Protection Manager 进行分发。您可以选择在此过 程中导出软件包,以使软件包可用于部署到不包含客户端软件的计算机上。

**注意**:您导入的安装软件包包括两个文件。一个文件名为 product\_name.dat,另一个文件名为 product\_name.info。

#### 添加客户端安装软件包更新

- 1 将软件包复制到运行 Symantec Endpoint Protection Manager 的计算机的目录中。
- 2 在控制台中,单击"管理员",再单击"安装软件包"。
- 3 在"任务"下方,单击"添加客户端安装软件包"。
- 4 在"添加客户端安装软件包"对话框中,键入软件包的名称和描述。
- 5 单击"浏览"。
- 6 在"选择文件夹"对话框中,找到并选择新软件包的*product\_name*.info文件, 然后单击"选择"。
- 7 当显示"成功完成"提示时,执行下列操作之一:
  - 如果您不打算导出安装文件并使它们可用于部署,请单击"关闭"。
     您已完成此过程。
  - 如果要导出安装文件并使它们可用于部署,请单击"**导出此软件包"**,然 后完成此过程。
- 8 在"导出软件包"对话框中,单击"浏览"。
- 9 在"选择导出文件夹"对话框中,浏览并选择要包含导出软件包的目录,然后 单击"确定"。
- 10 在"导出软件包"对话框中选择组,然后根据个人安装要求设置其他选项。

11 有关设置此对话框中其他选项的详细信息,请单击"帮助"。

12 单击"确定"。

### 升级一个或多个组中的客户端

您可以从"管理员"窗格和"客户端"窗格更新一个或多个组中的客户端。

注意:如果从"客户端"窗格更新客户端,则您可更好地控制软件包的分发方式。

从"管理员"页更新一个或多个组中的客户端

- 1 在控制台中,单击"管理员",再单击"安装软件包"。
- 2 在"任务"下,单击"使用软件包升级组"。
- 3 在"升级组向导"面板中,单击"下一步"。
- 4 在"选择客户端安装软件包"面板中的"选择新的客户端安装软件包"下,选 择您已添加的软件包,然后按"下一步"。
- 5 在"指定组"面板中,选中您想要升级的组,然后单击"下一步"。
- 6 在"软件包升级设置"面板中,选中"从管理服务器下载",然后单击"下一步"。
- 7 在"升级组向导完成"面板中,单击"完成"。
- 从"客户端"窗格更新一个或多个组中的客户端
- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"窗格中,选择要将软件包分配至的组。
- 3 在"安装软件包"选项卡的"任务"下,单击"添加客户端安装软件包"。
- 4 在"常规"和"通知"选项卡上,选择用于控制更新分发方式的选项。 如需设置其他选项的详细信息,请单击"帮助"。
- 5 当您完成配置更新分发选项后,单击"确定"。

### 删除升级软件包

升级软件包存储在数据库中。这些升级软件包皆需要最多 180 MB 的数据库空间,因此您应该删除不再使用的旧版软件升级软件包。您不可从文件系统中删除软件 包;仅可从数据库删除软件包。因此,如果您以后需要这些软件包,可以再次添加 它们。 注意:请勿删除安装于您客户端计算机上的软件包。

#### 删除升级软件包

- 1 在控制台中,单击"管理员"。
- 2 在"任务"下方,单击"安装软件包"。
- 3 在"客户端安装软件包"窗格中,选择要删除的软件包。
- 4 在"任务"下,单击"删除客户端安装软件包"。
- 5 在"删除客户端安装软件包"对话框中,单击"是"。

## 更新定义与内容

本章节包括下列主题:

- 关于内容类型
- 关于更新客户端与管理服务器的内容
- 关于内容分发方法
- 关于确定要使用何种内容分发方法
- 关于在 Symantec Endpoint Protection Manager 上存储内容修订
- 关于使用不是最新版本的内容修订
- 关于使用默认管理服务器更新客户端的内容
- 关于同时内容下载
- 配置下载内容更新的站点
- 关于 LiveUpdate 策略
- 配置 LiveUpdate 设置策略
- 配置 LiveUpdate 内容策略
- 查看和更改应用于组的自定义 IPS 策略
- 关于使用组更新提供者更新客户端的内容
- 配置组更新提供者
- 关于智能更新程序
- 使用智能更新程序下载要分发的防病毒内容更新
- 关于使用第三方分发工具将内容更新分发至受管客户端

- 使用 LiveUpdate 设置策略对受管客户端启用第三方内容分发
- 使用第三方分发工具将内容分发到受管客户端
- 关于使用第三方分发工具将内容更新分发给非受管客户端

### 关于内容类型

内容包括病毒与间谍软件定义、IPS特征,以及产品软件。您可以查看"LiveUpdate 内容策略"和站点属性设置中的内容类型。

**注意**: LiveUpdate内容包括定义和内容,但不包括 Symantec Endpoint Protection 策略更新。当您分配新策略或编辑现有策略时, Symantec Endpoint Protection Manager 会更新客户端中的策略。

表 6-1 列出更新类型。

内容类型	说明
客户端更新	这些更新包括客户端软件的产品更新。
防病毒和防间谍软件定义	这些定义包含两种类型的更新:完全版更新和直接增量更新。 更新类型包括在更新软件包中。x86和x64平台提供了单独的病毒定义软件包。
解压缩程序特征	这些特征支持防病毒和防间谍软件防护引擎,可用于解压缩 和读取以不同格式存储的数据。
TruScan 主动型威胁扫描启发 式特征	这些特征用于防范零时差攻击威胁。
TruScan 主动型威胁扫描商业 应用程序列表	这些应用程序列表列出的是过去曾经生成误报的合法商业应用程序。
入侵防护特征	这些特征用于防范网络威胁,并支持入侵防护和检测引擎。
提交控制特征	这些特征用于控制向 Symantec 安全响应中心提交相关内容的流程。
主机完整性模板	这些模板包括预定义的要求,此类要求会强制在客户端计算机上执行更新的补丁程序以及安全措施。仅当您安装 Symantec Network Access Control 后才能在"站点属性"对话框中使用这些模板。

#### 表 6-1 内容类型

### 关于更新客户端与管理服务器的内容

客户端会定期接收病毒与间谍软件定义、IPS特征、产品软件等的更新。LiveUpdate 是一项技术的名称,可将内容更新分发至客户端,或分发至服务器,然后再将内容 分发至客户端。

"LiveUpdate 设置策略"可用来控制将 LiveUpdate 内容分发至客户端的方式和时间。此策略可以定义客户端计算机使用的更新方法。通常,网络架构会决定应使用的分发方法。

"LiveUpdate设置策略"会指定客户端是否从下列来源接收内容更新:

- Symantec Endpoint Protection Manager
- 网络上的内部 LiveUpdate 服务器
- 指定为"组更新提供者"的客户端计算机
- 直接从 Symantec LiveUpdate

除了设置策略,您也应该配置"LiveUpdate 内容策略"控制内容更新的类型。 Symantec Network Access Control 客户端不支持此策略类型。

除非策略限制或禁止某些类型,否则客户端计算机默认会接收全部内容类型的更新。如果组使用 Symantec Endpoint Protection Manager 分发更新(默认),则 也必须配置管理服务器下载相同的更新。否则,这些更新将不可用于组分发。

您也可以定义客户端检查管理服务器是否有更新的频率。

### 关于内容分发方法

您可使用多种内容分发方法来更新客户端。您可基于网络设置方式及拥有的客户端 数目,决定使用何种内容分发方法。

请参见第82页的"关于确定要使用何种内容分发方法"。

以下是可用的分发方法:

■ 默认管理服务器

此为默认方法。Symantec Endpoint Protection Manager 会从 Symantec LiveUpdate 下载内容,然后再将内容分发到其客户端。

■ 组更新提供者

"组更新提供者"选项可用于任何组。创建组的LiveUpdate策略时,可以指定 一个客户端来下载更新。您可以将更新发送到组中的其他客户端。组更新提供 者不一定要在组中,并可以更新多个组。

内部 LiveUpdate 服务器 您可以设置内部 LiveUpdate 服务器以保留网络带宽。无论是否已安装 Symantec Endpoint Protection Manager 软件,计算机上皆可存放内部 LiveUpdate 服务 器。您也可以使用代理服务器,此代理服务器位于内部 LiveUpdate 服务器与它 所更新的管理服务器和客户端之间。

有关设置内部 LiveUpdate 服务器的详细信息,请参见《LiveUpdate 管理指 南》。您可以从安装光盘和 Symantec 支持网站获取此指南。

- 外部 LiveUpdate 服务器 您可以让客户端直接从 Symantec LiveUpdate 提取更新。
- 第三方管理工具
   第三方管理工具包括 Microsoft SMS 和 IBM Tivoli。

### 关于确定要使用何种内容分发方法

构建网络的方式取决于带宽可用性和带宽守恒。微型网络可以调度客户端直接从 Symantec 获取更新。拥有多达几千个客户端的中小型网络可使用默认设置。默认 设置是让 Symantec Endpoint Protection Manager 从 Symantec LiveUpdate 服务 器获取更新,再将这些更新提供给受管客户端。大型网络可以引入组更新提供者。

表 6-2 说明分发方法及使用时机。

方法	说明	何时使用
Symantec Endpoint Protection Manager 至客 户端 (默认)	默认情况下, Symantec Endpoint Protection Manager 会更新它们所管理的客户端,管理 服务器会从站点数据库提取这些更新。站点 数据库通常会从 Symantec LiveUpdate 服务 器接收更新。	最初使用此体系结构,因为它是实现的最简 便方法。默认情况下,管理服务器安装后会 安装和配置此体系结构。您也可以将此方法 与组更新提供者结合使用。
组更新提供者至客户端	组更新提供者是充当 Symantec Endpoint Protection Manager 与组中客户端之间的代 理的客户端。组更新提供者从管理服务器或 LiveUpdate 服务器接收更新,再将更新转发 至组中的其他客户端。组更新提供者可以更 新多个组。	对于共同位于具有最小带宽的远程位置的组, 使用此方法。另外,此方法还可以减轻管理 服务器的负担。 请注意,组更新提供者会分发全部类型的 LiveUpdate内容,但不包括客户端软件更 新。

表 6-2 内容分发方法及使用时机

方法	说明	何时使用
内部 LiveUpdate 服务器 至客户端	内部 LiveUpdate 服务器从外部 Symantec LiveUpdate 服务器接收更新后,客户端即可 直接从内部 LiveUpdate 服务器提取更新。	在大型网络中使用内部 Live Update 服务器以 减轻 Symantec Endpoint Protection Manager 服务器的负担。
		通常,内部 LiveUpdate 服务器适用于超过 10,000 个客户端的大型网络。使用此体系结 构,管理服务器不负责 LiveUpdate 内容更 新,但仍处理日志和策略更新。对于运行多 个 Symantec 产品且这些产品也运行 LiveUpdate 更新客户端的网络,内部 LiveUpdate 服务器也非常有用。
		不管是否已安装 Symantec Endpoint Protection Manager 软件,您都可以在一台 计算机上设置内部 LiveUpdate 服务器。在任 一种情况下,您都应该使用 LiveUpdate Administrator 实用程序更新 LiveUpdate 服 务器。LiveUpdate Administrator 实用程序 从 Symantec LiveUpdate 服务器提取定义更 新。然后,此实用程序会将软件包置于 Web 服务器、FTP 站点或用 UNC 路径指定的位 置。接着,您必须将 Symantec Endpoint Protection Manager 配置为从此位置提取定 义更新。
外部 LiveUpdate 服务器 至客户端	客户端可以直接从外部SymantecLiveUpdate 服务器接收更新。	对于并非始终连接至公司网络的非受管客户 端计算机,使用外部 Symantec LiveUpdate 服务器。
		<b>注意</b> :请勿将大量的受管网络客户端配置为 从外部 Symantec LiveUpdate 服务器提取更 新。此配置会对 Internet 网关带宽造成不必 要的浪费。
第三方工具分发 (未说明)	使用 Microsoft SMS 等第三方工具可将特定 的更新文件分发至客户端。您可以从 Symantec 网站检索智能更新程序自我解压缩 文件,这些文件包含扩展名为 jdb 及 vdb 的 病毒及安全风险定义文件。不再支持 idb 扩 展名。若要检索其他更新文件,您必须设置 和配置 Symantec Endpoint Protection Manager 服务器以下载和预备更新文件。	要在分发更新文件之前测试这些文件时使用 此方法。如果您有第三方工具分发基础结构, 并想利用此基础结构,则也可以使用此方法。

图 6-1 显示小型网络的分发体系结构示例。

84 | 更新定义与内容 | 关于确定要使用何种内容分发方法



图 6-2 显示大型网络的分发体系结构示例。



# 关于在 Symantec Endpoint Protection Manager 上存 储内容修订

您可以在 Symantec Endpoint Protection Manager 上存储内容修订。之所以要存储内容修订,是因为在将最新的内容提交给所有客户端之前,可能需要先测试这些内容。您可能需要保留旧版的内容,这样在必要时可以恢复。

请参见第86页的"关于使用不是最新版本的内容修订"。

您可以修改"站点属性"对话框中 LiveUpdate 选项卡的设置,以配置要保留的内容版本。可以保留的修订数目默认为 3。

请参见第87页的"配置下载内容更新的站点"。

**注意**:保留大量的修订时,Symantec Endpoint Protection Manager 需要更多的磁 盘空间。

### 关于使用不是最新版本的内容修订

如果您在 Symantec Endpoint Protection Manager 上存储多个版本的内容,您可 能需要在"LiveUpdate内容策略"中指定特定的修订。例如,您可以先测试最新修 订,然后将此提交至客户端。您可以在策略中指定旧版修订。

在某些情况下,策略中指定的修订会不匹配 Symantec Endpoint Protection Manager 上存储的修订。例如,您可能导入引用了服务器上不存在的修订的策略。您可能复 制策略而非来自其他站点的 LiveUpdate 内容。在这两种情况下,策略都会显示修 订不可用。即使服务器上不存在此修订,使用该策略的客户端仍会受到防护。客户 端会使用最新修订的内容。

请参见第 90 页的"配置 LiveUpdate 内容策略"。

### 关于使用默认管理服务器更新客户端的内容

默认设置是使用默认管理服务器更新客户端的内容。使用默认的管理服务器时,应 该执行下列配置操作:

- 配置下载内容更新的站点。
   请参见第 87 页的"配置下载内容更新的站点"。
- 配置"LiveUpdate设置策略"和"LiveUpdate内容策略",并且将这两项策略 分配给客户端。
   请参见第 89 页的"配置 LiveUpdate 设置策略"。
- 请参见第 90 页的"配置 LiveUpdate 内容策略"。

站点必须存储要分发至客户端的内容更新。您应该在"LiveUpdate内容策略"中配 置属性更新列表,以匹配针对站点指定的列表。

### 关于同时内容下载

Symantec Endpoint Protection Manager 支持从默认管理服务器或组更新提供者随 机将内容同时下载至您的客户端。它也支持从 LiveUpdate 服务器随机将内容下载 至您的客户端。随机下载可减少高峰期网络通信流量,此方式默认为启动。

您可以启用或禁用随机化功能。已启用默认设置。您也可以配置随机化窗口。 Symantec Endpoint Protection Manager 会使用随机化窗口错开内容下载的时间。 一般而言,您应该不需要更改默认的随机化设置。 然而,在某些状况下,可能需要提高随机化窗口值。例如,在运行 Symantec Endpoint Protection Manager 的相同物理计算机上,您可能在多个虚拟机上运行 Symantec Endpoint Protection 客户端。较高的随机化值可以改善服务器的性能,但是会延迟虚拟机的内容更新。

当您有多台实体客户端计算机连接至运行 Symantec Endpoint Protection Manager 的单个服务器时,也可能需要增加随机化窗口。通常,客户端与服务器的比例愈 高,可能需要设置的随机化窗口也愈多。较高的随机化值可减少服务器的高峰负 载,但是会延迟客户端计算机的内容更新。

客户端较少且需要快速的内容提交时,可以将随机化窗口设置为较低的值。较低的 随机化值会增加服务器的高峰负载,但是可加速客户端的内容提交。

对于来自于默认管理服务器或组更新提供者的下载,您可以在所选组的"通信设置"对话框中配置随机化设置。这些设置不属于"LiveUpdate设置策略"的一部分。

如果是从 LiveUpdate 服务器下载至客户端,您可以将随机化设置配置为 "LiveUpdate 设置策略"的一部分。

请参见第 89 页的"配置 LiveUpdate 设置策略"。

### 配置下载内容更新的站点

配置下载更新的站点时,要决定下列项:

- 检查更新的频率。
- 下载的内容类型。 LiveUpdate 策略也会指定要下载到客户端的内容类型。请确保站点下载客户端 LiveUpdate 策略中指定的所有内容更新。
- 要下载的更新类型的语言。
- 将内容提供给站点的 LiveUpdate 服务器。
   您可以指定外部 Symantec LiveUpdate 服务器(建议),也可以指定先前已安装和配置的内部 LiveUpdate 服务器。
- 要保留的内容修订数目以及是否要存储经过解压的客户端软件包。

如果使用复制,则仅需配置一个站点来下载更新文件。复制会自动更新另一数据 库。然而,作为最好的做法,您不应在站点间复制产品更新。这些更新可能非常 大,您所选择的每种语言都会对应一个更新版本。如果您选择使用 LiveUpdate 将 产品更新下载到 Symantec Endpoint Protection Manager,则这些更新会自动显示 在"安装软件包"窗格中。接着,您可以使用自动升级更新客户端。如果您使用此 方法进行版本控制,您就不应在 LiveUpdate 设置策略中选择自动产品升级。 **注意:** 站点会下载用于产品更新的 MSP 文件,然后创建新的 MSI 文件。如果您选择复制产品更新,则站点会复制 MSI 文件。MSP 文件的大小只是 MSI 文件大小的一小部分。默认调度 Symantec Endpoint Protection Manager 每 4 小时运行一次 LiveUpdate 是最好的做法。

#### 配置下载更新的站点

- 1 在控制台中,单击"管理员"。
- **2** 在"任务"下,单击"服务器"。
- 3 在"查看"窗格中,右键单击"本地站点",然后单击"编辑属性"。
- 4 在"站点属性"对话框中,在 LiveUpdate 选项卡的"下载调度"下,设置服务器应该检查更新的频率的调度选项。
- 5 在"要下载的内容类型"下,检查下载的更新类型列表。
- 6 若要添加或删除更新类型,请单击"更改选择",修改列表,然后单击"确 定"。
- 7 在"要下载的语言"下,检查下载的更新类型的语言列表。
- 8 若要添加或删除语言,请单击"更改选择",修改列表,然后单击"确定"。
- 9 在"LiveUpdate源服务器"之下,检查当前用于更新管理服务器的LiveUpdate服务器。此服务器默认为SymantecLiveUpdate服务器。然后执行下列操作之一:
  - 若要使用现有的 LiveUpdate 源服务器,请单击"确定"。 不要继续此过程;您已完成操作。
  - 若要使用内部 LiveUpdate 服务器,请单击"编辑源服务器",然后继续执 行此过程。
- **10** 在 "LiveUpdate 服务器"对话框中,选中 "使用指定的内部 LiveUpdate 服务器",并单击 "添加"。
- 11 在"添加 LiveUpdate 服务器"对话框中,在各框中填写用于标识 LiveUpdate 服务器的信息,然后单击"确定"。
- 12 在"站点属性"对话框的"针对下载内容的磁盘空间管理"下,键入要保留的 LiveUpdate 内容修订数量。

存储大量内容修订需要更多磁盘空间。以展开的格式存储的客户端软件包也需要更多磁盘空间。

- 13 选中或取消选中"存储经过解压的客户端软件包以便为升级提供更高的网络性 能"。
- 14 单击"确定"。

帮助列出并说明了要在各框中输入的数据。有关故障转移支持,您可以安装、 配置及选择多个 LiveUpdate 服务器。如果一台服务器脱机,其他服务器会提 供支持。

### 关于 LiveUpdate 策略

LiveUpdate 策略有两种类型。一种称为 LiveUpdate 设置策略,适用于 Symantec Endpoint Protection 和 Symantec Network Access Control 客户端。另一种称为 LiveUpdate 内容策略,仅适用于 Symantec Endpoint Protection 客户端。 LiveUpdate 设置策略可指定客户端要联系以检查更新的计算机,并控制客户端检查 更新的频率。必要时,您可以将此策略应用于组中的特定位置。

LiveUpdate内容策略指定允许客户端检查和安装的更新类型。针对每种类型,可以 指定客户端查看和安装最新的更新。或者,也可以指定客户端在未运行某个更高版 本时安装该版本。此策略不能应用于组中的特定位置。此策略只能在组级别应用。

### 配置 LiveUpdate 设置策略

添加及应用 LiveUpdate 设置策略时,应计划要让客户端计算机检查更新的频率。 默认设置是每 4 小时一次。您还应该知道检查客户端计算机及获取更新的位置。一 般而言,需要让客户端计算机从 Symantec Endpoint Protection Manager 检查及 获取更新。创建策略之后,您可以将策略分配到一个或多个组和位置。

**注意**:用户可使用其中一项高级设置从他们的客户端计算机手动启动LiveUpdate, 默认情况下此设置为禁用状态。如果您启用此设置,用户可以启动LiveUpdate并 下载最新的内容病毒定义、组件更新和产品更新。如果使用LiveUpdate下载产品 更新的高级策略设置已启用,则用户下载的产品更新将是Symantec客户端软件的 维护版本和补丁程序。根据用户人数的多寡,您可能不想让用户未经测试即下载所 有内容。此外,如果客户端计算机上同时运行两个LiveUpdate 会话,则可能会发 生冲突。最好禁用此设置。

#### 配置 LiveUpdate 设置策略

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下方,单击 LiveUpdate。
- **3** 在 "LiveUpdate 设置"选项卡的"任务"下方,单击"添加 LiveUpdate 设置 **策略"**。

- 4 在"概述"窗格的"策略名称"框中,键入策略名称。
- **5** 在 LiveUpdate 策略下方, 单击"服务器设置"。
- 6 在"服务器设置"窗格中的"内部或外部 LiveUpdate 服务器"下,至少选中 并启用一个将从其中检索更新的源。

多数组织都应该使用默认管理服务器。

- **7** 如果您选择了"使用 LiveUpdate 服务器",请在"LiveUpdate 策略"下方单击"调度"。
- 8 在"调度"窗格中,接受或更改调度选项。
- 9 如果您选择了"使用 LiveUpdate 服务器",请在"LiveUpdate 策略"下方单击
   "高级设置"。
- 10 决定是保留还是更改默认设置。

通常情况下,您不希望用户修改更新设置。但是,如果客户端太多而不能支持,您不妨让他们手动启动LiveUpdate会话。

- 11 完成策略配置后,单击"确定"。
- 12 在"分配策略"对话框中,执行下列操作之一:
  - 单击"是"以保存策略并将策略分配到组或组中的位置。
  - 单击"否"以仅保存策略。
- 13 如果您单击了"是",请在"分配 LiveUpdate 策略"对话框中选中要分配策略的组与位置,然后单击"分配"。

如果您不能选择嵌套组,该组会继承其父组的策略,这些策略在"客户端"页 面的"策略"选项卡上设置。

### 配置 LiveUpdate 内容策略

默认情况下,组中所有的 Symantec Endpoint Protection 客户端都会收到所有内容 和产品更新的最新版本。如果客户端组从管理服务器获取更新,则客户端只会接收 配置服务器下载的更新。例如,您可以将 LiveUpdate 内容策略配置为允许所有更 新。如果管理服务器未配置为下载所有更新,则客户端只会接收服务器所下载的内 容。

请参见第87页的"配置下载内容更新的站点"。

如果将组配置为从 LiveUpdate 服务器获取更新,则组的客户端会接收 LiveUpdate 内容策略中允许的所有更新。如果 LiveUpdate 内容策略指定了特定的内容修订, 则除非将此设置从特定修订更改为最新可用,否则客户端永远不会接收此特定更 新。LiveUpdate 服务器不了解命名版本功能。 使用命名版本可更密切地控制分发给客户端的更新。一般而言,在将最新更新分发 给客户端之前,测试最新更新的环境使用命名版本功能。

注意:使用特定修订可提供回滚功能。

#### 配置 LiveUpdate 内容策略

- 1 在控制台中,单击"策略"。
- **2** 在"查看策略"下方,单击 LiveUpdate。
- **3** 在"LiveUpdate 内容"选项卡中,单击"添加 LiveUpdate 内容策略"。
- 4 在"概述"窗格的"策略名称"框中,键入策略名称。
- 5 在 "LiveUpdate 内容" 窗格中, 单击 "安全定义"。
- 6 在"安全定义"窗格中,选中要下载并安装的更新,取消选中要禁用的更新。
- 7 针对每个更新,执行下列操作之一:
  - 选中"使用最新的可用组更新提供程序"
  - 选中"选择修订"
- 8 若要继续,执行下列其中一项:
  - 如果您未针对更新类型选中"选择修订",请单击"确定",然后继续执行步骤 11。
  - 如果您已针对更新类型选中"选择修订",请单击"编辑",然后继续执行下一步骤。
- 9 在"选择修订"对话框中的"修订"列中,选择要使用的修订,然后单击"确 定"。
- **10** 在 "LiveUpdate 内容策略" 窗口中, 单击 "确定"。
- 11 在"分配策略"对话框中,单击"是"。 您可以选择取消此过程,稍后再分配策略。
- 12 在 "分配 LiveUpdate 内容策略"对话框中,选中一个或多个要向其分配此策 略的组,然后单击"分配"。

### 查看和更改应用于组的自定义 IPS 策略

自定义入侵策略应用于组及组中的所有位置。因此,这类策略不会和其他策略一起 出现在控制台中的位置下。

#### 查看和更改应用于组的自定义 IPS 策略

- 1 在控制台中,至少创建两个自定义入侵防护策略。
- 2 将其中一个策略应用至组。
- **3** 单击"计算机 & 用户"。
- 4 在"查看"窗格中,选择要应用策略的组,然后单击"策略"选项卡。
- 5 在"策略"选项卡右窗格的"其他设置"下,单击"IPS 库"。
- 6 在"组设置"对话框中,记下当前所使用策略的名称。
- 7 若要更改表中已应用于组的策略,请针对该组要应用或撤回的策略,选中或取 消选中"已启用"复选框。

单击"确定"。.

### 关于使用组更新提供者更新客户端的内容

组更新提供者提供组中客户端的更新。针对 Symantec Endpoint Protection Manager 的网络访问权限售受限制的组客户端,您可以使用组更新提供者。如有需要,使用 组更新提供者可减轻 Symantec Endpoint Protection Manager 的处理负担。

若要配置组更新提供者,您可以在"LiveUpdate设置策略"中指定组更新提供者设置。您必须将策略分配至应使用组更新提供者的全部组,以及组更新提供者所在的组。

在您配置组更新提供者时,指定一个主机名称或IP地址和TCP端口号。默认的TCP端口号是 2967,该端口以前用于 Symantec AntiVirus 10.x 和 Symantec Client Security 3.x 网络通信。如果您的组更新提供者计算机使用 DHCP 接收 IP 地址,您应该为计算机分配一个静态IP 地址,或者使用主机名称。如果您的组更新提供者计算机位于远程位置,并且该远程位置使用网络地址转译(NAT),请使用主机名称。

您可以在创建策略或修改现有策略时配置组更新提供者。您应该先创建一个没有组 更新提供者的策略,并验证客户端计算机是否接收更新。在验证完成后,可以添加 组更新提供者。此方法可帮助解决通信上的问题。如果组更新提供者计算机脱机, 组中的客户端默认会直接从其管理服务器获取更新。

您也可以配置设置策略,以便客户端只从组更新提供者获取更新,而非从管理服务 器获取。您可以另行配置策略,以便客户端忽略组更新提供者。您也可以指定客户 端必须忽略组更新提供者前等候的时间。您也可以配置存储组更新提供者上的内容 更新以及同时下载数目上限等设置。

请参见第93页的"配置组更新提供者"。

### 配置组更新提供者

您可以使用组更新提供者将内容分发至客户端。

请参见第 92 页的"关于使用组更新提供者更新客户端的内容"。

您可以使用 LiveUpdate 设置策略,以便让客户端能够使用组更新提供者。您也可 以使用 LiveUpdate 设置策略来指定组更新提供者的设置。您必须将策略分配至要 使用组更新提供者的所有组。您也必须将策略分配至包含组更新提供者计算机的 组。

**注意:**如果组更新提供者运行 Windows 防火墙、旧版 Symantec Client Firewall 或 第三方防火墙,您必须修改防火墙策略以使其允许从 TCP 端口 2967(或使用的其 他端口)接收 Symantec Endpoint Protection Manager 的通信。如果组更新提供 者运行 Symantec Endpoint Protection 防火墙,则会自动配置防火墙策略。

#### 配置组更新提供者策略

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下方,单击 LiveUpdate。
- **3** 在 "LiveUpdate策略" 窗格中,在 "LiveUpdate设置" 选项卡的 "名称"下, 选择要编辑的策略。
- 4 在"任务"窗格中,单击"编辑策略"。
- 5 在 "LiveUpdate 策略" 窗口中, 单击 "服务器设置"。
- 6 在"LiveUpdate 服务器"选项卡的"局域网"服务器选项下,选中"将组更新 提供者用作默认 LiveUpdate 服务器"。
- 7 单击"组更新提供者"。
- 8 在"组更新提供者"对话框的"主机"框中,键入一个 IP 地址或主机名。
- 9 在"端口"框中,键入端口号或接受默认端口号。
- 10 指定当组更新提供者不可用时,是否要客户端绕过组更新提供者。您可以指定 客户端必须绕过组更新提供者前经过的时间。
- 11 指定组更新提供者用于内容更新的最大磁盘缓存大小。
- 12 指定组更新提供者删除未使用内容更新的等候时间。
- 13 指定同时进行的下载的最大数目。
- 14 单击"确定"。

### 关于智能更新程序

您可以使用智能更新程序将病毒和安全风险内容更新下载至管理服务器。Symantec 建议您使用 LiveUpdate 来更新内容。不过,若您不想使用 LiveUpdate,或是 LiveUpdate不可用,则可以使用智能更新程序。您在下载文件后,可以采用首选的 发布方法来更新客户端。

**注意**:智能更新程序仅提供病毒和安全风险内容更新。它不提供任何其他类型的内容更新。

智能更新程序作为单个文件或分隔软件包提供,后者通过若干个小文件分发。单个 文件适用于具有网络连接的计算机。分隔软件包适用于没有网络连接、Internet 访 问或 CD-ROM 驱动器的计算机。可以将分隔软件包复制到可移动介质进行分发。

注意:防病毒和防间谍软件定义包含在您可以分发的 vdb 和 jdb 文件中。Vdb 文件 仅支持 32 位客户端。Jdb 文件可支持 32 位客户端和 64 位客户端。这些是您放在客 户端计算机收件箱中的文件。您可以从下列站点下载更新:

ftp://ftp.symantec.com/AVDEFS/symantec\_antivirus\_corp/

### 使用智能更新程序下载要分发的防病毒内容更新

若只要分发更新的病毒及安全风险更新,请下载新的智能更新程序。然后使用您首选的分发方法,将更新提交给您的客户端。

**注意**:当前,智能更新程序只更新病毒和安全风险更新。请确保使用的是企业版的 智能更新程序文件,而非该产品的个人用户版。

#### 下载智能更新程序

1 使用 Web 浏览器,转到以下 URL:

http://www.symantec.com/zh/cn/business/security\_response/index.jsp

- 2 在"病毒定义"下,单击"手动下载病毒定义"。
- 3 单击"下载病毒定义(仅限智能更新程序)"。
- 4 选择适当的语言和产品。
- 5 单击 Download Updates。
- 6 单击扩展名为.exe 的文件。
- 7 当系统提示您提供保存文件的位置时,请选择硬盘驱动器中的文件夹。

更新定义与内容 | 95 关于使用第三方分发工具将内容更新分发至受管客户端 |

#### 安装病毒及安全风险定义文件

- 1 找到您已从 Symantec 下载的智能更新程序文件。
- 2 双击该文件,然后按照屏幕上的指示进行操作。

### 关于使用第三方分发工具将内容更新分发至受管客户 端

大型网络可能依赖诸如 IBM Tivoli、Microsoft SMS 之类的第三方分发工具来将更 新分发至客户端计算机。Symantec 客户端软件支持使用这些工具分发更新。若要 使用第三方分发工具,您需要先获取更新文件,然后使用分发工具分发更新文件。

对于受管客户端,在安装并配置 Symantec Endpoint Protection 管理服务器作为站 点唯一的服务器后,即可获取更新文件。然后您可以调度并选择要下载至站点的 LiveUpdate 内容更新。

请参见第87页的"配置下载内容更新的站点"。

更新文件会下载到下列(默认)目录的子目录中:

\Program Files\Symantec Endpoint Protection Manager\data\outbox\

然后您可以将文件分发至客户端计算机上的收件箱文件夹中。

默认情况下,此文件夹不存在并且客户端软件不会检查和处理此文件夹中的内容。 对于受管客户端,您必须为组配置一个 LiveUpdate 设置策略,允许对组中的客户 端使用第三方分发,然后分配策略。接着会在组的客户端计算机中显示收件箱文件 夹。对于非受管客户端,您必须在客户端计算机上手动启用注册表项。

收件箱文件夹会显示在未运行 Windows Vista 的客户端计算机的下列位置中:

\\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\inbox\

收件箱文件夹会显示在运行 Windows Vista 的客户端计算机的下列位置中:

\\Program Data\Symantec\Symantec Endpoint Protection\inbox\

### 使用LiveUpdate设置策略对受管客户端启用第三方内 容分发

当您创建一个支持对受管客户端进行第三方内容分发的 LiveUpdate 策略时,您还 有一些其他目标。一个目标是减小客户端检查更新的频率。另一个目标通常是使客 户端用户无法手动运行 LiveUpdate。会按 Symantec Endpoint Protection Manager 策略对受管客户端进行管理。

完成此过程后,组中不运行 Windows Vista 的客户端计算机上将显示下列目录:

\\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\inbox\

组中运行 Windows Vista 的客户端计算机上将显示下列目录:

\\Program Data\Symantec\Symantec Endpoint Protection\inbox\

#### 使用 LiveUpdate 策略对受管客户端启用第三方内容分发

- 1 在控制台中,单击"策略"。
- **2** 在"查看策略"下方,单击 LiveUpdate。
- **3** 在 "LiveUpdate 策略" 窗格的 "LiveUpdate 设置"选项卡上,单击"任务" 下的 **"添加 LiveUpdate 设置策略"**。
- 4 在"LiveUpdate策略"窗口的"策略名称"和"说明"框中,分别键入名称和 说明。
- 5 在"第三方管理"下,选中"启用第三方内容管理"。
- 6 取消选中其他所有 LiveUpdate 源选项。
- 7 单击"确定"。
- 8 在"分配策略"对话框中,单击"是"。 您可以选择取消此过程,稍后再分配策略。
- **9** 在"分配 LiveUpdate 策略"对话框中,选中一个或多个要向其分配此策略的 组,然后单击"分配"。

### 使用第三方分发工具将内容分发到受管客户端

在您将LiveUpdate策略配置为启用第三方内容管理之后,请在SymantecEndpoint Protection Manager 中查找并复制内容。查找并复制内容后,便可以将内容分发至 客户端。您还可以决定要复制和分发的内容。

**注意**:如果将更新文件放至/inbox目录之前,先在客户端计算机上预备更新文件,则必须复制文件。不能移动文件。还可以将.vdb和.jdb文件复制到收件箱进行处理。

#### 使用第三方分发工具将内容分发到受管客户端

- 在运行 Symantec Endpoint Protection Manager 的计算机上,创建工作目录, 例如 \Work\_Dir。
- 2 在控制台的"客户端"选项卡上,右键单击要更新的组,然后单击"属性"。
- 3 记下策略序列号的前四位十六进制数值,例如7B86。

4 浏览到以下目录:

\\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent

- 5 找到包含与您的客户端组策略序列号匹配的前四位十六进制数值的目录。
- **6** 打开该目录,然后将 index2.dax 复制到您的工作目录,例如 \Work\_Dir\index2.dax。
- 7 浏览到以下目录:

\\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\content

**8** 打开并阅读 ContentInfo.txt, 搜索每个 << target moniker>> 目录所包括的 内容。

每个目录的内容为 <<target moniker>>\<sequence num>\full.zip|full。

- **9** 将每个 \<< target moniker>> 目录的内容复制到您的工作目录,例如 \Work\_Dir。
- 10 删除每个 \<< target moniker>> 中的所有文件和目录,只在您的工作目录中保留以下目录结构和文件:

\\Work\_Dir\<<target moniker>>\<latest sequence number>\full.zip

现在,您的工作目录包含要分发至客户端的目录结构和文件。

**11** 使用第三方分发工具,将 \Work\_Dir 目录的内容分发至组中客户端的 \\Symantec Endpoint Protection\inbox\ 目录中。

最后的结果必须类似如下:

\\Symantec Endpoint Protection\inbox\index2.dax

\\Symantec Endpoint Protection\inbox\<<target moniker>>\<latest sequence number>\full.zip

如果文件消失, \inbox\目录因而为空,即表示操作成功。如果出现 \inbox\invalid\目录,表示没有成功,必须重试。

### 关于使用第三方分发工具将内容更新分发给非受管客 户端

如果您从安装光盘安装非受管客户端,则基于安全理由,客户端不会信任且不会处理 LiveUpdate 内容或策略更新。若要让这些客户端可以处理更新,您必须创建下列注册表项:

HKLM\Software\Symantec\Symantec Endpoint Protection\SMC\TPMState

将值设为十六进制数字 80,以便让项像这样: 0x00000080 (128) 在设置此项后,您必须重新启动计算机或从 \Symantec\Symantec Endpoint Protection\ 目录执行下列命令:

smc.exe -stop

smc.exe -start

收件箱文件夹会显示在未运行 Windows Vista 的客户端计算机的下列位置中:

\\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\inbox\

收件箱文件夹会显示在运行 Windows Vista 的客户端计算机的下列位置中:

\\Program Data\Symantec\Symantec Endpoint Protection\inbox\

您现在可以使用第三方分发工具将内容或策略更新复制到此目录中。然后,Symantec 客户端软件将信任并处理这些内容。

您从 Symantec Endpoint Protection Manager 获取要分发的内容的方式与为受管 客户端获取内容的方式几乎相同。

但是,请复制 My Company 组的 index2.xml,不要复制您所管客户端组目录的 index2.dax。依照受管客户端的说明,复制 full.dax 文件。接下来您即可分发这些 文件。您也可以将 .vdb 和 .jdb 文件放到客户端收件箱中以进行处理。

**注意**:如果您在计算机上预备更新文件,则必须将它们复制到收件箱。如果您将更 新文件移动到收件箱,则不会处理更新文件。

请参见第96页的"使用第三方分发工具将内容分发到受管客户端"。

**注意**:完成受管客户端的安装后,会出现值为0的TPMState注册表项,您可以更改这个值。(完成非受管客户端的安装后不会出现此项。)此外,完成受管客户端的安装后不需重新启动计算机或执行 smc.exe 命令。一旦更改注册表项,即会出现此目录。

## 限制用户对客户端功能的 访问

本章节包括下列主题:

- 关于访问客户端接口
- 锁定和解除锁定管理的设置
- 更改用户控制级别
- 使用密码保护客户端

### 关于访问客户端接口

您可以决定用户在 Symantec Endpoint Protection 客户端上拥有的交互级别。请选择哪些功能可供用户配置。例如,您可以控制出现的通知数,以及限制用户创建防 火墙规则和防病毒扫描的能力。您也可以让用户完整访问用户界面。

用户可自定义的用户界面功能称为受管设置。用户不能访问所有客户端功能,例如 密码保护就是不能访问的功能。

若要决定用户交互级别,您可以用下列方式自定义用户界面:

- 针对防病毒和防间谍软件设置,您可以锁定或解除锁定设置。
- 针对防火墙设置、入侵防护设置以及部分客户端用户界面设置,您可以设置用 户控制级别并配置关联的设置。
- 您可以使用密码保护客户端。
   请参见第 105 页的"使用密码保护客户端"。

### 锁定和解除锁定管理的设置

通过锁定和解除锁定的方式,您可以决定用户可在客户端上配置哪些防病毒和防间 谍软件防护及防篡改功能。用户可以配置已解除锁定的设置,但用户不能配置已锁 定的设置。只有 Symantec Endpoint Protection Manager 控制台中的管理器可以 配置已锁定设置。

表 7-1 锁定和解除锁定的挂锁图标

图标	图标代表的意义
1	设置已解除锁定,用户可以在客户端用户界面中更改设置。 挂锁图标不会显示在客户端上,选项可以使用。
۵	设置已锁定,用户不可以在客户端用户界面中更改设置。 挂锁图标显示在客户端上,选项会变成灰色。

可在显示设置的页面或对话框中锁定和解除锁定相应设置。

#### 锁定和解除锁定管理的设置

打开防病毒和防间谍软件策略。
 请参见第 288 页的"编辑策略"。

2 在"防病毒和防间谍软件"页面上,单击下列其中一页:

- 文件系统自动防护
- Internet 电子邮件自动防护
- Microsoft Outlook 自动防护
- Lotus Notes 自动防护
- TruScan 主动型威胁扫描
- 提交
- 其他
- 3 单击挂锁图标锁定或解除锁定设置。
- 4 完成此策略的配置后,单击"确定"。 您还可以锁定和解除锁定防篡改设置。 请参见第 268 页的"配置防篡改"。

### 更改用户控制级别

您可以决定用户可在 Symantec Endpoint Protection 客户端上配置哪些网络威胁防 护功能和客户端用户界面设置。若要决定可用的设置,请指定用户控制级别。用户 控制级别决定了客户端是完全不可见、显示部分功能还是显示完整的用户界面。

**注意:** Symantec Network Access Control 客户端仅在服务器控制中运行。用户无 法配置任何用户界面设置。

表7-2	用户控制级别	
用户控制级别	说明	
服务器控制	授予用户最低的客户端控制权。服务器控制会锁定受管理的设置, 以使用户无法配置这些设置。	
	服务器控制具有如下特征:	
	<ul> <li>用户不能配置或启用防火墙规则、特定于应用程序的设置、防火墙设置、入侵防护设置,或"网络威胁防护"和"客户端管理"日志。您可以在 Symantec Endpoint Protection Manager 控制台上为客户端配置所有防火墙规则和安全设置。</li> <li>用户可以查看日志、客户端的通信记录,以及客户端运行的应用程序列表。</li> <li>您可以配置特定用户界面设置以及是否要在客户端显示防火墙通知。例如,您可以隐藏客户端用户界面。</li> <li>您设为服务器控制的设置在客户端用户界面中会显示为灰色或不</li> </ul>	
	可见。 当你创建新位罢时 这位罢合自动设为服务界按制	
客尸端控制	授予用尸最尚的客尸端控制权。客尸端控制会解除锁定受管理的 设置,以使用户可以配置这些设置。	
	客户端控制具有如下特征:	
	<ul> <li>用户可以配置或启用防火墙规则、特定于应用程序的设置、防火墙通知、防火墙设置、入侵防护设置以及客户端用户界面设置。</li> <li>客户端会忽略您为客户端配置的防火墙规则。</li> </ul>	
	您可以将客户端控制授予员工在远程位置或在家中使用的客户端 计算机。	

用户控制级别	说明
混合控制	<ul> <li>授予用户对客户端的混合控制权。</li> <li>混合控制具有如下特征:</li> <li>用户可以配置防火墙规则和特定于应用程序的设置。</li> <li>您可以配置防火墙规则,这些规则可能会也可能不会覆盖用户 配置的规则。服务器规则是否会覆盖客户端规则,视服务器规</li> </ul>
	<ul> <li>则在防火墙策略的"规则"列表中的位置而定。</li> <li>您可以指定客户端上的某些设置是否可让用户启用和配置。这些设置包括"网络威胁防护"日志、"客户端管理"日志、防火墙设置、入侵防护设置以及部分用户界面设置。</li> <li>您可以将防病毒和防间谍软件防护设置配置为即使已解除锁定客户端上的设置,也要覆盖这些设置。例如,如果您解除锁定自动防护功能,而用户却禁用了它,则您可以启用自动防护。</li> </ul>
	您设为客户端控制的设置可供用户使用。您设为服务器控制的设置在客户端用户界面中会显示为灰色或不可见。 请参见第 103 页的"关于混合控制"。

部分受管设置具有相依性。例如,用户可能有权限配置防火墙规则,但不能访问客 户端用户界面。由于用户不能访问"配置防火墙规则"对话框,也就不能创建规则。

您可以在每个位置设置不同的用户控制级别。

**注意**:当服务器应用隔离策略时,在客户端控制或混合控制中运行的客户端会切换 到服务器控制。

#### 更改用户控制级别

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下方,选择要修改位置的组。
- **3** 单击"策略"选项卡。
- 4 在"特定于位置的策略与设置"下,在要修改的位置下,展开"特定于位置的 设置"。
- 5 在"客户端用户界面控制设置"的右侧,单击"任务">"编辑设置"。
- 6 在"客户端用户界面控制设置"对话框中,运行下列选项之一:
  - 单击"服务器控制",再单击"自定义"。 配置任意设置,再单击"确定"。
  - 单击"客户端控制"。

- 单击"混合控制",再单击"自定义"。
   配置任意设置,再单击"确定"。
   请参见第 103 页的"关于混合控制"。
- 对于 Symantec Network Access Control 客户端,您可以单击"显示客户 端"与"显示通知区域图标"。
- 7 单击"确定"。

#### 关于混合控制

对于处于混合控制状态的客户端,您可以决定哪些管理选项可由用户或者不可由用 户配置。管理选项包括防火墙策略、入侵防护策略的设置以及客户端用户界面设 置。

对于每个选项,您都可以指定为服务器控制或者客户端控制。在客户端控制中,只 有用户才可以启用或禁用设置。在服务器控制中,只有您可以启用或禁用设置。客 户端控制是默认的用户控制等级。如果您将某选项指定为服务器控制,则接下来需 要您在 Symantec Endpoint Protection Manager 控制台的对应页面或对话框中配 置相应设置。例如,您可以启用防火墙策略中的防火墙设置。您可以在"客户端" 页面的"策略"选项卡上的"客户端日志设置"对话框中配置日志。

您可以配置下列类型的设置:

- 用户界面设置
- 常规网络威胁防护设置
- 防火墙策略设置
- "入侵防护策略"设置

#### 配置用户界面设置

如果您运行下列任一项任务,则可以配置客户端上的用户界面设置:

- 将客户端的用户控制等级设置为服务器控制。
- 将客户端用户控制级别设置为混合控制,并将"客户端/服务器控制设置"选项 卡上的父级功能设置为"服务器"。 例如,您可以将"显示/隐藏通知区域图标"选项设置为"客户端"。通知区域 图标会出现在客户端上,而用户可以选择显示或隐藏图标。如果您将"显示/隐 藏通知区域图标"选项设置为"服务器",则您可以选择是否要在客户端上显 示通知区域图标。

#### 在混合控制中配置用户界面设置

1 将用户控制等级更改为混合控制。

请参见第101页的"更改用户控制级别"。

- 2 在"<位置名称>的客户端用户界面控制设置"对话框中的"混合控制"旁,单击"自定义"。
- 3 在"客户端用户界面混合控制设置"对话框的"客户端/服务器控制设置"选项 卡上,执行下列操作之一:
  - 锁定某个选项,这样您就只能从服务器配置它。针对要锁定的选项,单击 "服务器"。
     您在这里设置为"服务器"的任何防病毒和防间谍软件防护设置会覆盖客 户端上的设置。
  - 解除锁定某个选项,让用户可以在客户端上配置它。针对所要的选项,单击"客户端"。默认情况下,为除防病毒和防间谍软件设置之外的所有设置选择"客户端"。
- 4 针对下列您设置为"服务器"的选项,请单击"客户端用户界面设置"选项卡 来配置它们:

显示/隐藏通知区域图标	显示通知区域图标
启用/禁用网络威胁防护	允许用户启用和禁用网络威胁防护
"测试网络安全" 菜单命令	允许用户执行安全测试
显示/隐藏入侵防护通知	显示入侵防护通知

若需了解在控制台何处配置其余设置为"服务器"的选项,请单击"帮助"。 若要启用防火墙设置和入侵防护设置,请在"防火墙策略"和"入侵防护策 略"中配置它们。

请参见第 384 页的"启用智能通信过滤"。

请参见第 385 页的"启用通信与隐藏设置"。

请参见第 389 页的"配置入侵防护"。

- 5 在"客户端用户界面设置"选项卡上,选中选项的复选框,这样就能在客户端 上使用该选项。
- 6 单击"确定"。
- 7 单击"确定"。

#### 在服务器控制中配置用户界面设置

1 将用户控制等级更改为混合控制。

请参见第101页的"更改用户控制级别"。

- 2 在 "<位置名称>的客户端用户界面控制设置"对话框中的"服务器控制"旁, 单击"自定义"。
- **3** 在"客户端用户界面设置"对话框中,选中选项的复选框,让该选项出现在客 户端上供用户使用。
- 4 单击"确定"。
- 5 单击"确定"。

### 使用密码保护客户端

您可以要求用户每次在客户端计算机上执行特定任务时都必须启用密码保护,以提 高企业安全性。

您可以要求用户在尝试执行下列操作之一时必须键入密码:

- 打开客户端的用户界面。
- 停止客户端。
- 导入和导出安全策略。
- 卸载客户端。

您只能为不是从父组继承设置的子组修改密码保护设置。

#### 使用密码保护客户端

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下方,选择要为期设置密码保护的组。
- **3** 在"策略"选项卡的"与位置无关的策略与设置"下方,单击"常规设置"。
- **4** 单击"安全设置"。
- 5 在"安全设置"选项卡上,选择下列任一复选框:
  - 需要密码才能打开客户端用户界面
  - 需要密码才能停止客户端服务
  - 需要密码才能导入或导出策略
  - 需要密码才能卸载客户端
- 6 在"密码"文本框中键入密码。 密码不得超过15个字符。

#### 106 | 限制用户对客户端功能的访问 | 使用密码保护客户端

- 7 在"确认密码"文本框中,再次键入密码。
- 8 单击"确定"。

## 设置管理服务器与客户端 之间的连接

本章节包括下列主题:

- 关于管理服务器
- 指定管理服务器列表
- 添加管理服务器列表
- 将管理服务器列表分配给组和位置
- 查看将管理服务器列表分配至的组和位置
- 编辑管理服务器列表的服务器名称和说明
- 编辑管理服务器列表中的管理服务器 IP 地址、主机名和端口号
- 更改管理服务器连接的顺序
- 替换管理服务器列表
- 复制和粘贴管理服务器列表
- 导出和导入管理服务器列表
- 配置位置的通信设置
- 使用 SylinkDrop 工具恢复客户端通信设置

### 关于管理服务器

客户端必须能够连接到管理服务器,才能下载安全策略和设置。SymantecEndpoint Protection Manager包括一个文件,可帮助管理客户端与管理服务器之间的通信。

此文件可指定客户端连接到的管理服务器。而且也会指定在管理服务器失败的情况 下,客户端要连接到哪一个管理服务器。

这个文件称为管理服务器列表。管理服务器列表包括管理服务器的 IP 地址或主机 名,可供客户端在初始安装之后连接。部署任何客户端前,您可以自定义管理服务 器列表。

安装 Symantec Endpoint Protection Manager 时,会创建默认的管理服务器列表, 以允许客户端与管理服务器之间的 HTTP 通信。默认的管理服务器列表包括站点上 所有管理服务器的所有已连接网络接口卡 IP 地址。

您可能希望列表仅包括外部 NIC。虽然您不能编辑默认管理服务器列表,但是您可 以创建自定义的管理服务器列表。自定义管理服务器列表可包括确切管理服务器和 您希望客户端连接的正确 NIC。在自定义列表中,也可以使用 HTTPS 协议,验证 服务器证书,以及自定义 HTTP 或 HTTPS 端口号。

您也可以使用管理服务器列表,指定选用的 Enforcer 连接到哪个服务器。

请参见第114页的"配置位置的通信设置"。

### 指定管理服务器列表

您可以指定管理服务器的列表,以随时连接至客户端和选用Enforcer的组。不过,您通常会在创建自定义管理服务器列表之后、部署任何客户端软件包之前,执行此任务。

#### 指定管理服务器列表

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择要指定管理服务器列表的组。
- 3 在"策略"选项卡中,取消选中"从父组继承策略和设置"。 只有在组不再从父组继承任何策略和设置时,您才能为该组设置任何通信设置。
- 4 在"与位置无关的策略与设置"下的"设置"区域中,单击"通信设置"。
- 5 在"用于 <组名称> 的通信设置"的"管理服务器列表"下方,选择管理服务器列表。

与管理服务器通信时,您选择的组就会使用此管理服务器列表。

6 单击"确定"。
### 添加管理服务器列表

如果企业具有多个 Symantec Endpoint Protection Manager,您可以创建自定义管理服务器列表。管理服务器列表指定特定组中客户端连接的顺序。客户端会先尝试连接到以最高优先级添加的管理服务器。

如果最高优先级的管理服务器不可用,则客户端会尝试连接到次高优先级的管理服务器。每个站点的默认管理服务器列表会自动创建。该站点所有可用的管理服务器 会以相同的优先级添加到默认管理服务器列表。

如果您以相同的优先级添加多个管理服务器,则客户端可连接到其中任何一个管理 服务器。客户端会自动平衡该优先级的可用管理服务器之间的负载。

您可以不使用默认 HTTP 协议,改用 HTTPS 进行通信。如果您要进一步保护通信 的安全,可以通过创建自定义管理服务器列表,来自定义HTTP和HTTPS端口号。 不过,您必须在安装客户端前自定义端口,否则客户端与管理服务器之间的通信将 中断。如果您更新管理服务器的版本,请务必记得要再次自定义端口,以便客户端 恢复通信。

在添加新的管理服务器列表后,您必须将它分配给特定组、位置或这两者。 请参见第110页的"将管理服务器列表分配给组和位置"。

#### 添加管理服务器列表

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"任务"下方,单击"添加管理服务器列表"。
- **4** 在"查看管理服务器列表"对话框的"名称"文本字段中,键入管理服务器列 表的名称和可选说明。
- 5 若要指定管理服务器与客户端之间要使用的协议,请选择下列其中一个选项:
  - 使用 HTTP 协议
  - 使用 HTTPS 协议 如果您要管理服务器使用 HTTPS进行通信,而且服务器运行 Secure Sockets Layer (SSL),请使用这个选项。
- 6 如果您请求使用可信的第三方证书颁发机构验证证书,请选中"使用 HTTPS 协议时验证证书"。
- 7 若要新建服务器,请单击"添加">"新服务器"。
- 8 在"添加管理服务器"对话框的"服务器地址"文本字段中,键入管理服务器的IP地址或主机名。
- **9** 如果您要更改此服务器的 HTTP 或 HTTPS 协议所使用的端口号,请执行下列 其中一项任务:

#### 110 | 设置管理服务器与客户端之间的连接 将管理服务器列表分配给组和位置

- 选中"自定义 HTTP 端口号",然后输入新的端口号。 HTTP 协议的默认端口号为 80。
- 选中"自定义 HTTPS 端口号",然后输入新的端口号。 HTTPS 协议的默认端口号为 443。 如果在客户端部署之后自定义 HTTP或 HTTPS 端口号,则客户端会不能与 管理服务器进行通信。
- 10 单击"确定"。
- 11 如果您需要添加与刚才添加的管理服务器不同优先级的管理服务器,请单击
   "添加">"新优先级"。
- 12 请重复步骤7至10,以添加更多的管理服务器。
- 13 在"管理服务器列表"对话框中,单击"确定"。

### 将管理服务器列表分配给组和位置

添加策略后,您需要将该策略分配给组或/和位置。否则,管理服务器列表不会生效。您也可以使用管理服务器列表,将客户端的组从某个管理服务器转至另一个管理服务器。

您必须先完成添加或编辑管理服务器列表,才能分配该列表。

请参见第109页的"添加管理服务器列表"。

#### 将管理服务器列表分配给组和位置

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"管理服务器列表"窗格中,选择要分配的管理服务器列表。
- 4 在"任务"下方,单击"分配列表"。
- 5 在"应用管理服务器列表"对话框,选中要应用管理服务器列表的组和位置。
- 6 单击"分配"。
- 7 屏幕出现提示时,请单击"是"。

### 查看将管理服务器列表分配至的组和位置

您可能想要显示已分配管理服务器列表的组和位置。

#### 查看将管理服务器列表分配至的组和位置

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"管理服务器列表"窗格中,选择要显示其组和位置的管理服务器列表。
- 4 在"任务"下,单击"显示分配的组或位置"。 已分配所选择管理服务器列表的组或位置,会显示绿色小圆圈与白色选中标记。
- 5 在"管理服务器列表名称:分配的组和位置"对话框中,单击"确定"。

### 编辑管理服务器列表的服务器名称和说明

您可以更改管理服务器列表的名称和说明。

请参见第110页的"将管理服务器列表分配给组和位置"。

#### 编辑管理服务器列表的服务器名称和说明

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"管理服务器列表"窗格中,选择要修改名称和描述的管理服务器列表。
- 4 在"任务"下方,单击"编辑列表"。
- 5 在"管理服务器列表"对话框中,编辑管理服务器列表的名称和非必填的描述。
- 6 单击"确定"。

# 编辑管理服务器列表中的管理服务器IP地址、主机名 和端口号

如果管理服务器的IP地址或主机名改变,则您需要在管理服务器列表中予以更改。 您也可以更改 HTTP 或 HTTPS 通信协议的端口号。

请参见第 110 页的"将管理服务器列表分配给组和位置"。

#### 编辑管理服务器列表中的管理服务器 IP 地址、主机名和端口号

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。

- 3 在"管理服务器列表"窗格中,选择要修改的管理服务器列表。
- 4 在"任务"下方,单击"编辑列表"。
- 5 在"管理服务器列表"对话框中,选择要修改的管理服务器。
- 6 单击"编辑"。
- 7 在"添加管理服务器"对话框中,在"服务器地址"框中键入管理服务器的新 IP地址或主机名。

您也可以更改 HTTP 或 HTTPS 协议的端口号。

- 8 单击"确定"。
- 9 在"管理服务器列表"对话框中,单击"确定"。

### 更改管理服务器连接的顺序

如果网络情况改变,您可能需要重新分配管理服务器列表中的IP地址或主机名以及 优先级。例如,您安装 Symantec Endpoint Protection Manager 的其中一台服务 器出现磁盘故障。此管理服务器已作为负载平衡服务器,且已分配优先级1。但是, 您还有另一台管理服务器分配了优先级2。如果要解决此问题,则可以重新分配此 管理服务器的优先级。您可以将管理服务器的优先级从2分配为1,以替换故障的 管理服务器。

#### 更改管理服务器连接的顺序

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"管理服务器列表"窗格中,选择要更改管理服务器顺序的管理服务器列表。
- 4 在"任务"下方,单击"编辑列表"。
- 5 在"管理服务器列表"对话框的"管理服务器"下,选择管理服务器的 IP 地址、主机名或优先级。

您可以将IP地址或主机名重新转至不同的优先级。如果您决定更改优先级,系统还会自动更改所有相关IP地址和主机名的优先级。

- 6 单击"上移"或"下移"。
- 7 在"管理服务器列表"对话框中,单击"确定"。

### 替换管理服务器列表

您可能想要将先前应用于特定组或位置的管理服务器列表替换为另一个管理服务器 列表。

#### 替换管理服务器列表

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"管理服务器列表"窗格中,选择要替换的管理服务器列表。
- 4 在"任务"下方,单击"替换列表"。
- 5 从"替换管理服务器列表"对话框的"新建管理服务器"下拉列表中,选择替 代管理服务器列表。
- 6 选中要应用替代管理服务器列表的组或位置。
- 7 单击"替换"。
- 8 屏幕出现提示时,请单击"是"。

### 复制和粘贴管理服务器列表

您可能需要多份几乎完全相同的管理列表,少数更改除外。您可以复制管理服务器 列表。复制并粘贴管理服务器列表后,管理服务器列表的副本会显示在"管理服务 器列表"窗格中。

#### 复制和粘贴管理服务器列表

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"管理服务器列表"窗格中,选择要复制的管理服务器列表。
- 4 在"任务"下方,单击"复制列表"。
- 5 在"任务"下方,单击"粘贴列表"。

### 导出和导入管理服务器列表

您可能需要导出和导入现有的管理服务器列表。管理服务器列表的文件格式是:.dat

#### 导出管理服务器列表

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"管理服务器列表"窗格中,选择要导出的管理服务器列表。
- 4 在"策略"页面的"任务"下,单击"导出列表"。
- 5 在"导出策略"对话框中,浏览到要将管理服务器列表文件导出至的目标文件 夹。
- 6 单击"导出"。
- 7 如果系统在"导出策略"对话框中提示您更改文件名,请修改文件名,然后单击"确定"。

#### 导入管理服务器列表

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击"策略组件">"管理服务器列表"。
- 3 在"任务"下方,单击"导入管理服务器列表"。
- 4 在"导人策略"对话框中,浏览至要导入的管理服务器列表文件,然后单击 "导入"。
- 5 如果系统在"输入"对话框中提示您更改文件名,请修改文件名,然后单击 "确定"。

### 配置位置的通信设置

在默认情况下,在组中全部位置的管理服务器与客户端之间,您可以配置相同的通 信设置。然而,您也可以分别配置各个位置的设置。例如,对于客户端计算机通过 VPN进行连接的位置,您可以使用单独的管理服务器。另外,若要将同时连接至管 理服务器的客户端数目降至最低,您可以针对各个位置指定不同的检测信号。

请参见第 297 页的"配置推模式或拉模式来更新客户端策略和内容"。

您可以针对位置配置下列通信设置:

下列设置将取决于具体位置:

- 客户端运行时采用的控制模式。
- 客户端使用的管理服务器列表。
- 客户端运行时采用的下载模式。
- 是否要收集客户端上执行的所有应用程序列表并将其提交给管理服务器。

- 客户端进行下载时使用的检测信号时间间隔。
- 管理服务器是否会随机从默认管理服务器或组更新提供者下载内容。

#### 配置位置的通信设置

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面上,选择组。
- **3** 在"策略"选项卡的"特定于位置的设置与策略"下方,展开某位置下方的 "特定于位置的设置"。
- 4 在"通信设置"右边,单击"任务",然后取消选中"使用组通信设置"。
- 5 单击"任务",然后单击"编辑设置"。
- 6 在"用于 <位置名称> 的通信设置"对话框中, 仅修改该位置的设置。
- 7 单击"确定"。

### 使用 SylinkDrop 工具恢复客户端通信设置

Sylink.xml 文件包含客户端与 Symantec Endpoint Protection Manager 服务器之间的通信设置。如果客户端丢失与管理服务器之间的通信,则必须使用新的 Sylink.xml 文件来替换旧的文件。SylinkDrop 工具会自动使用新的 Sylink.xml 文件来替换客户端计算机上的 Sylink.xml 文件。

运行 SylinkDrop 工具时,亦会执行下列任务:

- 将客户端迁移或移动至新的域或管理服务器。
- 将不能在管理服务器上修复的通信损坏还原至客户端。
- 将客户端从一台服务器移动至另一台不是复制伙伴的服务器。
- 将客户端从一个域移动至另一个域。
- 将非受管客户端转换为受管客户端。
- 将受管客户端转换为非受管客户端。

您可以使用该工具来编写脚本,以便修改大量客户端的通信设置。

#### 使用 SylinkDrop 工具恢复客户端通信设置

在控制台中,将连接至管理服务器的组的通信文件导出至您要客户端计算机进行连接的服务器。

请参见第48页的"将非受管客户端转换为受管客户端"。

2 将通信文件部署至客户端计算机。

**3** 在第3片安装光盘中找到\Tools\NoSupport\SylinkDrop文件夹,然后打开 SylinkDrop.exe。

您可以远程运行该工具,或是先保存该工具,然后再于客户端计算机运行该工 具。如果您是在命令行中使用该工具,请读取 SylinkDrop.txt 文件以了解关于 工具的命令参数的列表。

- **4** 在 Sylink Drop 对话框中,单击"浏览",找到您在步骤 2 中部署至客户端计 算机的.xml 文件。
- 5 单击"更新 Sylink"。
- 6 如果您看到确认对话框,请单击"确定"。
- 7 在 Sylink Drop 对话框中,单击"退出"。

# 报告基础篇

本章节包括下列主题:

- 关于报告
- 关于您可以运行的报告
- 关于显示日志和报告
- 报告使用数据库的方式
- 关于网络中记录的事件
- 关于可监控的日志
- 访问报告功能
- 禁用回环地址时将本地主机与 IP 地址相关联
- 关于将 SSL 与报告功能一起使用
- 关于 Symantec Endpoint Protection 主页
- 配置主页上的报告收藏夹
- 关于使用安全响应中心链接
- 使用 Symantec Network Access Control 主页
- 配置报告首选项
- 关于报告和日志中使用的客户端扫描时间
- 关于在报告和日志中使用过去 24 小时过滤器
- 关于在报告和日志中使用搜索组的过滤器

# 关于报告

报告功能可提供监控网络安全并做出最佳决策所需的最新信息。Symantec Endpoint Protection Manager 控制台的主页会显示自动生成的图表,这些图表包含有关最近 发生于网络中的重要事件的信息。您可以使用"报告"页面上的过滤器来生成预定 义或自定义报告。可以使用"报告"页面,查看网络中所发生事件相关的图形表示 和统计信息。可以使用"监视器"页面上的过滤器,从日志查看有关网络的更详细 的实时信息。

如果您安装了 Symantec Endpoint Protection,则报告会包括下列功能:

- 可自定义的主页,包括最重要的报告、整体安全状态,以及指向Symantec安全 响应中心的链接
- 关于防病毒状态、网络威胁防护状态、遵从性状态以及站点状态的报告摘要视
   图
- 预定义的快速报告和可自定义的图形报告,包括可配置的多个过滤器选项
- 调度报告定期以电子邮件方式发送给收件人的功能
- 支持使用 Microsoft SQL 或嵌入式数据库来存储事件日志
- 运行客户端扫描、打开客户端网络威胁防护和自动防护及直接从日志重新启动 客户端计算机的功能
- 直接从日志添加应用程序排除项的功能
- 基于安全事件的可配置通知

如果您安装了 Symantec Network Access Control,则报告会包括下列功能:

- 包含遵从性状态整体摘要视图的主页
- 预定义且可自定义的图形报告,包括多个过滤器选项
- 支持使用 Microsoft SQL 或嵌入式数据库来存储事件日志
- 调度报告定期以电子邮件方式发送给收件人的功能
- 基于安全事件的可配置通知

报告会以控制台内的 Web 应用程序运行。应用程序使用 Web 服务器传递此信息。 您也可以从连接至管理服务器的独立 Web 浏览器,访问报告功能。

基本的报告任务包括下列几项:

- 使用 Web 浏览器登录报告
- 使用主页和摘要视图,快速获取有关安全网络中的事件的信息
- 配置报告首选项
- 使用指向 Symantec 安全响应中心的链接

# 关于您可以运行的报告

Symantec Endpoint Protection 和 Symantec Network Access Control 会收集您网 络中安全事件的相关信息。您可以查看预定义的快速报告,也可以根据所选过滤器 设置来生成自定义报告。您也可以保存过滤器配置,以便日后可以生成同样的自定 义报告并可删除不再需要的报告。

表 9-1 说明了可用的报告类型。

报告类型	说明
应用程序与设备控制	显示有关禁止某些类型行为的事件的信息。这些报告包括应 用程序安全警报、禁止的目标及禁止的设备等相关信息。禁 止的目标可能是注册表项、dll、文件和进程。
审核	显示客户端和位置当前使用的策略的相关信息。
遵从性	显示网络遵从性状态的相关信息。这类报告包括有关Enforcer 服务器、Enforcer 客户端、Enforcer 通信和主机遵从性的信息。
计算机状态	显示网络中计算机操作状态(例如哪些计算机关闭了安全功能)的相关信息。这类报告包括有关版本、尚未签入服务器的客户端、客户端清单及联机状态等的信息。
网络威胁防护	显示有关入侵防护、对防火墙的攻击以及防火墙通信和数据 包的信息。
风险	显示有关管理服务器及其客户端上风险事件的信息。它包括 有关 TruScan 主动型威胁扫描的信息。
扫描	显示有关防病毒和防间谍软件扫描活动的信息。
系统	显示关于事件时间、事件类型、站点、域、服务器及严重性 等级的信息。

表 9-1 报告类型

请参见第140页的"关于报告"。

**注意**:某些预定义的报告会包括来自 Symantec Network Access Control 的信息。 如果您并未购买该产品,但却运行该产品的其中一种报告,则该报告会是空的。

您可以修改预定义的报告,然后保存配置;也可以根据预定义的配置或您所创建的 现有自定义配置来创建新的过滤器配置。此外,您也可以删除不再需要的自定义配 置。如果您已配置日志和报告首选项设置将过滤器包括在报告中,则活动的过滤器 设置会列出在报告中。 请参见第133页的"配置日志和报告首选项"。

当您创建报告时,报告会出现在另一个窗口中。您可以用Web存档格式保存报告的 副本,也可以打印报告。保存后的文件或打印的报告均可提供报告数据库中当前数 据的快照,因而您可以将历史记录保留下来。

您也可以创建根据所配置的调度自动生成的调度报告。您可设置报告过滤器和运行 报告的时间。报告创建完成后,就会以电子邮件形式发送给一位或多位收件人。

调度报告通常默认为运行。对于尚未运行的任何调度报告,您可以更改此设置。您 也可以删除单个或所有调度报告。

请参见第155页的"创建和删除调度报告"。

# 关于显示日志和报告

报告功能的最佳显示分辨率是1024x768或更高。不过,您可以使用滚动条将屏幕 分辨率设成低达800x600,来查看报告功能。

# 报告使用数据库的方式

Symantec Endpoint Protection 可从存储在数据库中的管理服务器日志收集及读取 您网络中所发生的事件。此数据库可以是网络中现有的 Microsoft SQL 数据库,也可以是随报告软件安装的嵌入式数据库。

此数据库具有一些与报告相关的维护要求。

请参见第 254 页的"关于管理数据库中的日志事件"。

如果您想要使用第三方软件来建构自己的报告,则可获取 Symantec Endpoint Protection 所使用的数据库架构。如需数据库架构的相关信息,请参见 Symantec 知识库。

## 关于网络中记录的事件

Symantec Endpoint Protection 会从管理服务器上的事件日志提取报告中所显示的 事件。事件日志包含客户端时区的时间戳。管理服务器收到事件后,会将事件的时 间戳转换成插入数据库所需的格林威治标准时间(GMT)。当您创建报告后,报告软 件会以您查看报告所在计算机的当地时间来显示事件信息。

某些类型的事件(例如病毒爆发)可以导致生成大量的安全事件。这些类型的事件 会在汇总后转发给管理服务器。

如需主页上显示的事件的相关信息,请参见 Symantec 安全响应中心网站的 Attack Signatures 页面。在 Internet 上,请转到以下 URL:

http://securityresponse.symantec.com/avcenter/attack\_sigs/

# 关于可监控的日志

如果您要重点关注某些特定事件,可以直接查看事件数据。日志所包括的事件数据 来自管理服务器以及向这些服务器报告的所有客户端。

您可以过滤日志数据,方法就跟过滤报告数据一样。您可以将日志数据导出为逗号 分隔文件,也可以将部分数据导出为文本文件或导出至Syslog服务器。此项功能对 于备份事件数据或是想要在电子表格或其他应用程序中使用数据非常有用。

请参见第175页的"导出日志数据"。

## 访问报告功能

报告会在 Symantec Endpoint Protection Manager 控制台内以 Web 应用程序运行。应用程序使用 Web 服务器传递此信息。您可以从控制台访问位于主页面、监视器页面和报告页面的报告功能。

您可以从与您的管理服务器连接的独立Web浏览器,访问主页面、监视器和报告页 面功能。您可以从控制台或独立Web浏览器执行所有报告功能。然而,在使用独立 浏览器时所有其他控制台功能都不可用。

若要从 Web 浏览器访问报告,您必须具备下列信息:

- 管理服务器的 IP 地址或主机名称。
- 管理员的帐户名称和密码。

当您使用Web浏览器访问报告功能时,屏幕中不会显示页面或页面图标。主页、监视器和报告控制台页面上的所有选项卡都位于浏览器窗口的最上方。

报告页面和日志页面通常会以安装管理服务器时所用的语言显示。若要在使用远程 控制台或浏览器时显示这些页面,您必须在所使用的计算机上安装适当的字体。

**注意**:无论以任何一种方法访问报告功能,您都必须安装 Internet Explorer 6.0 或 更高版本。不支持其他 Web 浏览器。

此处提供的信息是假定您使用控制台访问报告功能,而非使用Web浏览器。无论访问报告的方式为何,使用报告的步骤都很类似。不过,本指南除了说明如何使用独立Web浏览器登录以外,并未特别说明在独立浏览器中使用报告的步骤。

注意:您还可以在通过远程终端会话登录时,使用控制台或Web浏览器查看报告。

请参见第 26 页的"登录 Symantec Endpoint Protection Manager 控制台"。 在用于报告功能的控制台页面上单击"更多信息"链接,可获得上下文相关帮助。 **注意**:如果您在安装针对报告的帮助页面时未使用默认端口,您便无法访问联机的 上下文相关帮助。若要在使用非默认端口时访问上下文相关帮助,您必须将一个变 量添加到 Reporter.php 文件。

### 从独立 Web 浏览器登录报告

- **1** 打开 Web 浏览器。
- 2 以如下格式在地址文本框中键入报告的 URL:

#### http://server name /reporting/index.php?

3 当登录对话框显示时,键入您的用户名和密码,然后单击"登录"。 如果您有多个域,则需要在"域"文本框中键入您的域名。

### 更改用来访问针对报告的上下文相关帮助的端口

- 1 将目录更改为 *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Resources。
- 2 使用编辑器打开 Reporter.php 配置文件。
- 3 在此文件中添加下面一行,并将 port number 替换成您在安装报告帮助时使用 的端口号。

#### \$scm\_http\_port=port number

4 存储并关闭文件。

# 禁用回环地址时将本地主机与 IP 地址相关联

如果您在计算机上禁用回环地址,则报告页面不会显示。如果您尝试登录Symantec Endpoint Protection Manager 控制台,或尝试访问报告功能,您会看见下列错误 消息:

无法与报告组件通信

主页、"监视器"页和"报告"页为空;"策略"页、"客户端"页和"管理员" 页正常显示且功能正常。

若要使"报告"组件在已禁用回环地址时显示,必须将单词 localhost 与计算机的 IP 地址相关联。您可以编辑 Windows 主机文件,使本地主机与 IP 地址相关联。

### 在运行 Windows 的计算机上使本地主机与 IP 地址相关联

1 将目录更改至主机文件的位置。

主机文件默认位在 %SystemRoot%\system32\drivers\etc

2 用编辑器打开主机文件。

3 将下列一行添加到主机文件:

xxx.xxx.xxx localhost #以登录报告功能

其中 xxx.xxx.xxx 表示您计算机的 IP 地址。您可以在井字符号 (#) 后加上 任何需要的注释。例如,您可以键入下列一行:

192.168.1.100 localhost # this entry is for my console computer

4 存储并关闭文件。

# 关于将 SSL 与报告功能一起使用

您可以将 SSL 与报告功能一起使用,以提高安全性。SSL 可确保客户端和服务器之间的机密性和数据的完整性,并可在二者之间进行验证。

如需 SSL 与报告功能一起使用的相关信息,请参见 Symantec 知识库中的 Configuring SSL to work with the Symantec Endpoint Protection reporting functions(配置 SSL 与 Symantec Endpoint Protection 报告功能一起使用), URL 如下:

http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007072512593748

# 关于 Symantec Endpoint Protection 主页

如果您已安装 Symantec Endpoint Protection,并且您的管理员帐户权限包括查看 报告的权限,那么您的主页会显示自动生成的报告。这些报告包括关于网络安全的 重要信息。如果您没有查看报告的权限,那么主页不会包括这些自动生成的报告。

图 9-1 显示有查看报告权限的管理员所看到的主页示例。



ec Endpoint Protection nantec™ Endpoint Pro	otection Man	ager Trialware		和道	E XI	租助
安全状态			病毒定义分发			
		首选项	見去「病毒定义分发			
安全状态 -	良好		20 1. Htt			
		更多详细信息	此义 计异机线	1		
按检测计数列出的提	作摘要					
<b>操作</b>	病毒	安全风险				
「「「「「」」「「」」「「」」「」」「「」」「」」「「」」「」」「」」「」」「	0	0				
可数に	0	U				
ロ奈正	0	U		1		
	0	U				
金印度之	0	0	最新的 Symantec 版本: 200	38-06-26 rev. 023		
仍發展边	0		<b>並教官理番原本:</b> 信息目前/	下可用		
有上时时外他里, 社	+ 43 + 0+		安全响应	上次更新时间: 2008-11-05 11:13:45		
每小时八陸双里: 12	去 12 小时		首要威胁	上次爆发更改: 2007-04-04-08:08:00		
显示: 风险	<b>•</b>					
A			» 元亲日可重示			
			最新威胁			
			》 无条目可显示			
			(Look) District to the dealer D.	a Trus I death		
			即时仅有止任于即的突刑	3 DOLLENDRUB).		
			Symantec Three	atCon • 🗶 🛨 🕾 🔣		
			Level 1: Norma	· 定义		
				<ul> <li>最新威胁</li> </ul>		
0 9				Security Focus		
状态摘要			受监视的应用程序摘要			
		计算机数		出現次数		
防病毒引擎关闭		0	商业应用程序检测	0		
自动防护关闭		0	强制性 TruScan 主动型威胁相	金剛 0		
防篡改关闭		0	报告收藏夹 🚭			
需要重新启动		0	首要攻击源			
主机完整性检查未通过		0	前几个风险检测关联			
	未确认的通知		TruScan 主动型威胁分布			
L						

主页包括自动生成的报告和数个状态项。其中一些主页报告中还包含指向更详细报告的超链接。您可以通过单击主页报告中的数字和一些图表来查看详细信息。

**注意**:报告会自动根据登录用户的权限进行过滤。如果您是系统管理员,您可以看见所有域的信息。如果您是仅能访问一个域的受限管理员,您只能看见该域的信息。

表 9-2 详细说明了 Symantec Endpoint Protection 主页上的每个项。

报告或状态信息	说明
安全状态	安全状态可以是"良好"或"需要注意"。您在"安全状态"选项卡上所设置 的阈值将决定"良好"和"需要注意"的定义.可以在主页上通过"首选项" 链接访问"安全状态"选项卡。
	请参见第 133 页的"配置安全状态阈值"。
	您可以在主页上单击安全状态图标以查看详细信息。

报告或状态信息	说明
按检测计数列出的操作摘要 按计算机 数列出的操作摘要	在默认情况下,主页上会显示过去 24 小时内按病毒和安全风险感染数列出的 操作摘要。您可以单击"首选项"链接将使用的时间间隔从过去 24 小时更改 为过去一周。您可以使用同一个链接将显示方式从按检测数更改为按计算机 数。
	请参见第 132 页的"关于主页和监视器显示选项"。
	"按检测计数列出的操作摘要"包含如下摘要信息:
	<ul> <li>■ 已对病毒和安全风险采取的操作数。</li> <li>■ 检测新病毒和安全风险的频率。</li> <li>■ 仍受病毒感染和仍有风险的计算机数。</li> </ul>
	"按计算机数列出的操作摘要"包含如下摘要信息:
	<ul> <li>■ 已对病毒和安全风险采取各种操作的计算机的数目。</li> <li>■ 新病毒和安全风险检测的总数。</li> <li>■ 仍受病毒感染和仍有风险的计算机总数。</li> </ul>
	例如,假设您在"检测计数"视图中有五个"已清除"操作。如果所有的检测 都发生在同一台计算机上,那么"计算机数"视图上会显示数量为一,而不是 五。
	针对任何操作,您都可以单击病毒或安全风险数目来查看更详细的报告。
	可疑安全风险表示 TruScan 主动型威胁扫描检测到需要调查的情况。检测到的 情况可能是有害的,也可能是无害的。如果您确定此风险无害,可以使用集中 式例外策略将此风险排除在日后的检测范围之外。如果您已将 TruScan 主动 型威胁扫描配置为记入日志,并且确定此风险有害,则可以使用集中式例外策 略来终止或隔离此风险。如果您使用了默认的 TruScan 主动型威胁扫描设置, 则 Symantec Endpoint Protection 无法补救此风险。如果您确定此风险有害, 应手动删除此风险。

报告或状态信息	说明
按检测计数列出的操作摘要 按计算机 数列出的操作摘要 (续)	"新感染"数目仅显示在选定时间间隔内受感染计算机的风险数目。"新感染"是"仍受感染"的子集。"仍受感染"数目显示的是在此配置的时间间隔 内扫描会继续将其归类为受感染的风险总计。例如,计算机可能会因为 Symantec Endpoint Protection 只能删除部分风险而仍受感染。在您对该风险 进行调查之后,可以从计算机状态日志中清除"仍受感染"数目。
	"新感染"数目和"仍受感染"数目所显示的风险,都需要您采取进一步的操作才能清除。在大多数情况下,您可以从控制台上执行此操作,而无需到计算机上执行。
	<b>注意</b> :如果检测事件是在主页的时间范围内发生的,则计算机会计入"新感染"数目。例如,如果在过去 24 小时内有未经补救的风险感染了计算机,则 主页上的"新感染"数目就会增加。此风险未经补救,可能是因为它只经过部 分补救或它的安全策略设为"仅记录"。
	您可以对数据库清除进行配置,以删除或保留导致未经补救的风险的检测事件。如果清除配置为删除未经补救的风险事件,则主页上的"仍受感染"数目将不再包括这些事件。这些事件将过期并从数据库中删除。虽然事件会消失,但并不代表计算机已得到补救。
	"仍受感染"项没有时间限制。您可在清除风险之后更改计算机的受感染状态。单击"受感染"列中该计算机的图标可以更改计算机状态日志中的状态。
	<b>注意:</b> 清除计算机状态日志中的计算机感染状态,不会使"新感染"数目降低; "仍受感染"数目确实会降低。
	您可以计算在配置的过去一段时间内所发生的事件总数,以将其显示在主页 上。若要确定总数,将"操作摘要"中所有行("仍受感染"除外)中的数目 相加即可。
	请参见第167页的"查看日志"。
每小时攻击数量 风险数量 感染数量: 过去12小时   过去24小时	此报告由折线图组成。折线图显示安全网络在过去12个小时或24个小时内发 生攻击、检测或感染的频率。您可以选择显示下列选项之一:
	<ul> <li>■ 攻击是指网络威胁防护阻挡的事件。</li> <li>■ 风险是指所有防病毒、防间谍软件以及TruScan主动型威胁扫描检测结果。</li> <li>■ 感染是指已检测出但不能正确予以补救的病毒和安全风险。</li> </ul>
	您可以单击列表框中的新视图来更改显示。
	注意: 单击"首选项"链接可以更改使用的默认时间间隔。
	请参见第 132 页的"关于主页和监视器显示选项"。
通知状态摘要	"通知"状态摘要会以一行摘要来显示您所配置的通知的状态。例如,过去24 小时内有 100 个未确认的通知。
	请参见第 180 页的"创建管理员通知"。

报告或状态信息	说明
状态摘要	"状态摘要"会显示网络中计算机工作状态的摘要。此摘要包含网络中出现下 列问题的计算机数:
	<ul> <li>■ 防病毒引擎已关闭。</li> <li>■ 自动防护已关闭。</li> <li>■ 防篡改已关闭。</li> </ul>
	<ul> <li>计算机需要重新启动才能完成某种风险补救或完成所下载的LiveUpdate软件的安装。</li> <li>计算机未通过主机完整性检查。</li> </ul>
	如果您没有安装 Symantec Network Access Control,此数目始终为零。
	您可以单击"状态摘要"中的每个数目,以查看详细信息。
	还会显示过去 24 小时内未确认的通知数。
病毒定义分发 入侵防护特征	主页的"病毒定义分发"和"入侵防护特征"部分会显示当前病毒定义和 IPS 特征的分发情况。
	您可以单击列表框中的新视图来切换这两项。
安全响应中心	安全响应中心会显示 Symantec 安全响应中心所确定的首要威胁和最新威胁。 该中心还会显示网络中为其提供针对这些威胁的防护的计算机数量。网络风险 指数 (ThreatCon) 计量表可指示网络中的计算机当前所受威胁的严重性等级。 严重性等级是根据 Symantec 安全响应中心所做的威胁评估而定。ThreatCon 严重性等级提供了全球 Internet 安全性的总体情况。
	您可以单击其中的任意链接获取更多信息。
	请参见第 129 页的"关于使用安全响应中心链接"。
	<b>注意</b> : Symantec 不支持在运行 Symantec Endpoint Protection Manager 的 计算机上安装 Symantec Client Firewall。如果您将两者安装到同一台计算机 上,那么当您在主页上单击"安全响应中心"链接时,就会发生 CGI 错误。
受监控的应用程序摘要	"受监控的应用程序摘要"会使用下列列表来显示网络中的应用程序出现次数:
	<ul> <li>Symantec 商业应用程序列表</li> <li>强制性 TruScan 主动型威胁检测列表,这是您自定义的受监视的应用程序 列表</li> </ul>
	您可以单击数字显示更详细的报告。
报告收藏夹	"报告收藏夹"部分包括三种默认的报告。在自定义此部分时,您可以用所需的任何其他默认报告或自定义报告替换其中的一个或多个报告。每次查看报告收藏夹时,这些报告都会运行一次,因此其数据会是最新的。这些报告会显示在新的窗口中。
	若要选择想从主页访问的报告,您可以单击"报告收藏夹"旁的加号(+)图标。

可以使用"首选项"链接来更改显示在这些页面上的报告和摘要的时间范围。默认 值是"过去 24 小时";另一个选项是"过去一周"。您也可以更改显示在主页上 "报告收藏夹"中的默认报告。

## 配置主页上的报告收藏夹

您可以将主页上的"报告收藏夹"部分配置为包含最多三个要定期查看的报告的链接。您可以使用此功能在每次登录 Symantec Endpoint Protection Manager 控制 台时显示您要最频繁查看的报告。每次查看"报告收藏夹"时,报告都会运行一次,因此报告会显示有关网络状态的最新信息。

报告收藏夹默认显示下列报告:

- 首要攻击源
- 前几个风险检测关联
- TruScan 主动型威胁分布

注意:在自定义显示时,您只可自定义当前登录的用户帐户的显示。

您在本页面上所做的配置会保存起来,适用于所有会话。当您下次使用相同的用户 凭据登录控制台时,主页便会使用这些设置进行显示。

表 9-3 介绍了主页的显示选项。

### 表 9-3 主页报告收藏夹的显示选项

选项	定义
报告类型	指定可用的报告类型。
	Symantec Endpoint Protection 提供下列报告类型:
	<ul> <li>应用程序与设备控制</li> <li>审核</li> <li>遵从性</li> <li>计算机状态</li> <li>网络威胁防护</li> <li>风险</li> <li>扫描</li> <li>系统</li> </ul>
报告名称	列出所选报告类型的可用报告名称。
过滤	如果您已将与所选报告相关联的过滤器保存下来,这些过滤器便会 显示在列表框中。默认过滤器通常都会在其中列出。

#### 配置主页上的报告收藏夹

- 1 单击"主页"。
- 2 单击"报告收藏夹"旁的加号图标。
- 3 从您要更改的报告的列表框,单击报告类型。例如,单击"风险"。
- 4 从下一个列表框,单击您要的报告名称。例如,单击"某段时间内的风险分 布"。
- 5 如果您已保存与所选报告相关联的过滤器,请选择所要使用的过滤器或选择默认过滤器。
- 6 视需要针对第二或第三个报告链接重复此过程。
- 7 单击"确定"。

指向所选报告的链接便会显示在主页上。

### 关于使用安全响应中心链接

主页上有一个根据来自 Symantec 安全响应中心网站的信息生成的摘要。此摘要上除了显示网络风险指数 (ThreatCon) 等级严重程度图之外,还有 Symantec 安全响应中心网站和其他安全网站的链接。ThreatCon 等级显示过去 24 小时 Internet 的状况。除非 Internet 活动的状况达到需要尽快进行评估的程度,否则会每隔 24 小时重新评估一次此等级。

网络风险指数 (ThreatCon) 等级包括:

■ 1-正常

没有可检测到的网络事故活动,也没有具有中度或严重风险等级的恶意代码活动。在"正常"状况下,只需要可防范常规网络威胁的例行安全措施。应该使用自动化系统和通知机制。

■ 2-提升

存在已确认或者可能的攻击活动,但没有发生特定的事件。当恶意代码达到中 度风险等级时,会使用此等级。在此情况下,您应该仔细检查易受攻击或存在 风险的系统。当新特征和规则可用时,您应该立即使用这些特征和规则来更新 安全应用程序。建议详细监控日志,但不需要更改实际的安全基础结构。

■ 3-高

如当前正在隔离针对计算机基础设施的威胁,或恶意代码已达到严重风险等级, 就会应用此等级。在此情况下,您有必要更频繁地进行监控。当新特征和规则 可用时,您应该立即使用这些特征和规则来更新安全应用程序。建议您重新部 署并重新配置安全系统。

■ 4-极高

当极端全局网络事件活动正在进行时,便会应用此等级。在此威胁情况下,如 果没有尽快运行相关措施,便可能会导致棘手的问题,并且可能会影响网络基 础设施的正常工作。

如需威胁等级的详细信息,请单击 Symantec 链接以转到 Symantec 网站。

**注意**:特定的安全风险等级为1至5。

每一个链接都会在新窗口中显示网页。

表 9-4 说明了安全响应中心链接。

表 9-4	报告主页上的安全响应中心链接

链接	显示的内容
安全警报	根据来自 Symantec 安全响应中心的信息,显示安全网络中的潜在 威胁的摘要。此摘要包括最新威胁和首要威胁,以及删除工具链 接。
	您也可以搜索 Symantec 安全响应中心的威胁数据库。
Symantec	显示 Symantec 网站。您可以在此获取风险和安全风险的信息、下载病毒定义,以及关于 Symantec 安全产品的最新消息。
定义	显示 Symantec 网站的病毒定义下载网页。
最新威胁	显示 Symantec 安全响应中心网站,该网站会提供最新的威胁和安全建议。
安全焦点	显示 Security Focus 网站,该网站会提供最新病毒的相关信息。

# 使用 Symantec Network Access Control 主页

如果您已安装 Symantec Network Access Control,并且您有查看报告的权限,则 主页会显示自动生成的摘要。这些报告包括网络遵从性状态的重要信息。部分摘要 带有指向详细报告的超链接。您可以通过单击摘要中的图表和数字来查看详细信 息。

**注意**:报告会自动根据登录用户的权限进行过滤。如果您是系统管理员,您可以看见所有域的信息。如果您是仅能访问一个域的受限管理员,您只能看见该域的信息。

图 9-2 展示了 Symantec Network Access Control 主页的显示方式。

(m) Smarte	a Undersist Destantion Managar 約組合	
🔘 Syn	nantec™ Endpoint Protection Manager	
(1) 注页	( <b>鎮変 日志 命令状态 通知</b> 摘要类型: 選从性 ■ 网络溶血、性球素 为失敗	上次更報时间: 2007-09-18 09:21:48 <b>拾落从性生败装写列出的实户端</b>
上 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一		甜: Gkbal'hicheck
ж-а	遵从性状态分布	蓬从性失败详细信息
客户端		组: Globalthicheck 组中的总客户端数量:3
	状态 計 配数 比	3
管理员	主机完整性检 查未通过 2 100.1	9%
	2it 2 100.	9%

### 图 9-2 Symantec Network Access Control 主页

表 9-5 介绍了 Symantec Network Access Control 的主页报告。

### 表 9-5 Symantec Network Access Control 主页摘要

摘要	说明
网络遵从性状态为失败	"失败网络遵从性状态"部分简单地描述了网络在配置的时间段内的整体遵从性。它显示了试图连接到网络但因不符合遵从性要求而失败的客户端。
遵从性状态分布	显示未通过其计算机上运行的主机完整性检查的客户端。
遵从性失败的客户摘要	此摘要显示整体遵从性要求的不符合率。它按控制失 败事件的类型以条形图显示各类工作站的计数。控制 失败事件类型包括防病毒、防火墙或 VPN 问题等。
遵从性失败详细信息	提供比"按遵从性失败摘要的客户端"更详细的条形 图。例如,假设"按遵从性失败摘要的客户端"显示 了防病毒遵从性失败的十个客户端。
	相比之下,此报告会显示下列详细信息:
	<ul> <li>四个客户端当前未运行防病毒软件。</li> <li>两个客户端未安装防病毒软件。</li> <li>四个客户端的防病毒定义已过期。</li> </ul>

如果您仅安装了 Symantec Network Access Control,您不能自定义主页报告(报告和摘要的时间范围除外)。您可以使用"首选项"链接更改时间范围。选项包括过去一周和过去 24 小时。

**注意**:如果您是系统管理员,您可以看见所有域的信息。如果您是仅能访问一个域的受限管理员,您只能看见该域的信息。

### 配置报告首选项

您可以配置下列报告首选项:

- 主页和监视器页显示选项
- 安全状态阈值
- 用于日志和报告以及旧版日志文件上载的显示选项

有关可设置的首选项选项的信息,可单击"首选项"对话框的各个选项卡上的"帮助"。

### 配置报告首选项

- 1 从控制台的主页上,单击"首选项"。
- 2 根据要设置的首选项类型,单击下列选项卡之一:
  - 主页和监视器
  - 安全状态
  - 日志和报告
- 3 设置要更改的选项的值。
- 4 单击"确定"。

### 关于主页和监视器显示选项

对于主页和"监视器"页的"摘要视图"选项卡,您可以设置下列首选项:

- 主页和"监视器"页的"摘要视图"选项卡上报告使用的时间单位
- 主页和"监视器"页的"摘要视图"选项卡的刷新速率
- 主页上未确认通知计数中包括的通知范围
- 主页上"操作摘要"的内容

默认情况下,会显示过去24小时的信息,但您可根据需要将其更改为过去一周。 您也可以配置主页和"监视器"页的"摘要视图"选项卡的刷新速率。有效值范围 从"从不"至"每5分钟"。 **注意**:若要配置个别日志的刷新速率,您可以显示要查看的日志。然后,从该日志 视图的 "自动刷新"列表框中选择所需速率。

如果您是系统管理员,则可以配置主页计数,以便只包括您创建而未确认的通知。 默认情况下,不论通知由谁创建,系统管理员都可以看到未确认的通知总数。如果 您是受限管理员,未确认通知计数只会包括您自己创建而未确认的通知。

您可以将主页上的"操作摘要"配置为按计算机检测计数或计算机数显示。

请参见第 123 页的"关于 Symantec Endpoint Protection 主页"。

有关这些显示选项的说明,请参见主页和"监视器"选项卡的上下文关联帮助。您 可以从主页上的"首选项"链接访问上下文关联帮助。

### 配置安全状态阈值

您设置的安全状态阈值可确定何时将 Symantec Endpoint Protection Manager 控制台主页上的安全状态消息视为"差"。阈值以百分比表示,反映何时将您的网络视为不遵从安全策略。例如,您可以设置病毒定义过期的计算机数量百分比,从而触发差安全状态。您也可以设置需要将定义视为过期的天数。Symantec Endpoint Protection 会按如下方式确定在计算特征或定义是否过期时哪些条目是最新的。其标准是运行控制台的管理服务器上提供的最新病毒定义和 IPS 特征日期。

**注意**:如果您只安装了 Symantec Network Access Control,则不会有用于配置安全阈值的"安全状态"选项卡。

有关这些显示选项的说明,请参见"安全状态"选项卡的上下文关联帮助。您可以 从主页上的"首选项"链接访问上下文关联帮助。

#### 配置安全状态阈值

- 1 从控制台的主页上,单击"首选项"。
- **2** 在"安全状态"选项卡上,选中要在确定整体主页安全状态的条件中包括的条目。
- 3 对于每个条目,键入要触发"需要注意"安全状态的数字。.
- 4 单击"确定"。

### 配置日志和报告首选项

您可以为日志和报告设置下列区域中的首选项:

- 用于日期显示的日期格式和日期分隔符
- 用于表显示的列数、时区和 IP 地址格式

- 报告和通知中的过滤器显示
- 运行 Symantec Antivirus 10.x 软件的网络计算机的日志数据的可用性

有关这些显示选项的说明,请参见"日志和报告"选项卡的上下文关联帮助。您可 以从主页上的"首选项"链接访问上下文关联帮助。

**注意**:您在此处设置的日期显示格式不会应用于表列中显示的病毒定义日期和版本。这些条目始终使用 Y-M-D (年-月-日)格式。

# 关于报告和日志中使用的客户端扫描时间

报告和日志会使用 Symantec Endpoint Protection Manager 控制台的时区显示客 户端扫描时间。例如,假设客户端位于太平洋时间时区,在 8:00 PM PST 进行扫描。如果控制台位于东部时间时区,则此次扫描所显示的时间就是11:00 PM EST。

如果受管客户端与管理服务器位于不同时区,而您使用"设置特定日期"过滤器选项,可能会看到意外的结果。

下列情况会影响"设置特定日期"时间过滤器:

- 客户端上的数据和时间精确度
- 管理服务器上的数据和时间精确度

**注意**:如果您在服务器上更改时区,请注销控制台后重新登录,以便在日志和报告 中看到准确的时间。

## 关于在报告和日志中使用过去 24 小时过滤器

如果您选择"过去24小时"作为报告或日志视图的时间范围,则此时间范围会从 您选择此过滤器时开始算起。如果您刷新页面,并不会重置此24小时范围的开始 时间。如果您先选择过滤器,然后等待创建报告,那么时间范围也会从您选择过滤 器时开始算起。此情况也适用于查看事件日志或警报日志。时间范围不会从您创建 报告或查看日志时开始算起。

如果您要确定此过去 24 小时时间范围是从现在开始算起,请先选择另一个时间范围,然后重新选择"过去 24 小时"。

注意: 主页上的过去 24 小时时间范围过滤器从访问主页的时间开始计算。

# 关于在报告和日志中使用搜索组的过滤器

由于所有组都是MyCompany父组的子组,因此,当过滤器搜索组时,会从字符串MyCompany开始进行层级式搜索。如果组名称的开头不是英语字母m,请在要搜索的字符串前面加上一个星号。或者,当您使用通配符时,可以使用m\*作为字符串开头。

例如,如果有个组名为 Services,而您在此框键入 s\*,则在视图中将找不到任何被 使用的组。若要查找名为 Services 的组,您需要改用字符串 \*s\*。如果有一个以上 的组包括英语字母 s,可以使用如 \*ser\* 的字符串。

- 136 | 报告基础篇
  - 关于在报告和日志中使用搜索组的过滤器

# 查看和配置报告

本章节包括下列主题:

- 关于查看报告
- 关于报告
- 关于报告的重要须知
- 创建快速报告
- 保存和删除已保存的报告过滤器
- 打印和保存报告副本
- 创建和删除调度报告

# 关于查看报告

使用"报告"页可运行、查看、打印报告以及调度报告定期运行。 图 10-1 显示一个风险报告示例。 10

图10-1	示例	报告	
🦉 报告 -	按域显示风险检测数量和格	꾏 - ∎icrosoft Internet Expl	or er
Syma	ntec Endpoint Protec	tion	Symantec.
按域显	示风险检测数量和检测		
2007年:	2007年九月 17 1:07 下午 至 2007年九月 18 1:07 下午 打印 保存 关闭		
风险分	布		
	风险	计算机数	
	Adware.BDE	1	
	Adware.Searchq	1	
	Another World.707	1	
	Backdoor.Trojan	1	_
	Bloodhound.DirActCOM	1	
	Bloodhound.WordMacro	1	
	Cascade (1)	1	
	DA.1800	1	
	Dialer./WebDialler	1	
	DSCE.2100	1	
	DSCE.Demo	1	
	EICAR Test String	1	
	Gergana.182	1	
	Hydra.1	1	
	Jeru.1808	1	
	Jeru 1808 Frere Jac	1	

### 关于查看报告中的线条图

线条图显示随时间的进度。X 轴上显示的单位取决于您选择的时间范围。 表 10-1 显示了用于您可为线条图选择的每个时间范围的 X 轴单位。

### 表10-1 对应于所选时间范围的 X 轴单位

时间范围	X 轴单位
过去 24 小时	小时

时间范围	X轴单位
过去一周	Н
过去一个月	
当前的月份	
过去3个月	
过去一年	月
时间范围	一天(任意24小时)是按小时计算
	大于1天而小于或等于7天是按小时计算
	大于7天而小于或等于31天是按天计算
	大于 31 天而小于或等于 2 年是按月计算
	大于2年是按年计算

### 关于查看条形图

在包括有关威胁的直方图或条形图报告中,将光标放在条形图上方,即可看见威胁 名称。

### 关于以亚洲语言查看报告

将图表提交到浏览器之前,服务器上会创建直方图和三维条形图的映像。根据默 认,您用来创建图表的服务器会查找 MS Arial Unicode 字体。MS Arial Unicode 是属于 Microsoft Office 的一部分,可正确显示所有支持的语言。如果找不到 MS Arial Unicode 字体,服务器会使用 Lucida sans Unicode 字体。

服务器上一些以亚洲语言显示的报告不能正确显示图表文本,除非服务器安装 MS Arial Unicode。这样的问题会发生在当您的报告包括直方图或三维条形图的时候。如果服务器未安装 MS Arial Unicode 字体,您可以配置服务器以解决此问题。您可以配置 Symantec Endpoint Protection 从而使用在您的环境中支持这些语言的任何现有 Unicode 支持字体。

### 更改用于显示报告的字体

- 1 将目录更改为 *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Common。
- 2 使用编辑器打开 i18nCommon.bundle 配置文件。
- **3** 在 SPECIAL\_FONT 变量的等号 (=) 之后,键入您要使用的字体文件名称。例 如,如果您想要使用 Arial,则可以键入如下内容:

**SPECIAL\_FONT**=*arial.ttf* 

- 4 将文件存储为UTF-8格式,然后关闭文件。
- 5 确定您键入的字体文件位于 %WINDIR%\fonts 目录中。

### 关于报告

快速报告是可打印的报告,可按照需要从"报告"页面的"快速报告"选项卡获取。

表 10-2 说明了快速报告的报告类型。

#### 表10-2 快速报告类型

报告类型	说明
应用程序与设备控制	应用程序与设备控制报告包含有关禁止访问计算机或拒绝设备连至网络等事件的信息。
审核	"审核"报告包括关于策略修改活动的信息,如事件时间和类型、策略修改、域、站 点、管理员以及说明。
遵从性	"遵从性"报告包括关于 Enforcer 服务器、Enforcer 客户端、Enforcer 通信及主机遵 从性的信息。
计算机状态	"计算机状态"报告包括关于网络中计算机的实时运行状态的信息。
网络威胁防护	"网络威胁防护"报告用来跟踪计算机的活动及其与其他计算机和网络的交互情况。 它们记录有关试图通过网络连接进出计算机的通信的信息。
风险	"风险"报告包含有关管理服务器及其客户端上的风险事件的信息。
扫描	"扫描"报告提供关于防病毒和防间谍软件扫描活动的信息。
系统	"系统"报告包括有助于解答客户端疑难问题的信息。

本节按照名称及报告的一般内容来介绍报告。您可以为所有报告配置"基本设置" 和"高级设置",以精简所要查看的数据。您还可以命名并保存自定义过滤,以便 日后运行相同的自定义报告。

如果您的网络包括多个域,可通过许多报告查看所有域、一个站点或几个站点的数据。所有快速报告均默认为显示适用于您选择要创建的报告的所有域、组、服务器 等。

**注意**:如果您只安装了 Symantec Network Access Control,则会有大量的报告是空的。应用程序与设备控制报告、网络威胁防护报告、风险报告和扫描报告都不包含数据。"遵从性"和"审核"报告则与部分"计算机状态"和"系统"报告一样,确实包含数据。

如需每个可配置选项的说明,可在 Symantec Endpoint Protection Manager 控制 台上单击该报告类型的"更多信息"链接。"更多信息"会显示上下文关联帮助。 请参见第 150 页的"创建快速报告"。

表10-3说明可用的应用程序与设备控制报告。

表10-3 应用程序与设备控制报告

报告名称	说明
含警报次数最多的应用程序控 制日志的前几组	此报告由一个饼图和一些相关条块组成。它显示了含生成最多安全警报的应用程序控制日志的一些组。
首要已禁止目标	<ul> <li>此报告由一个饼图和一些表示以下每个目标(如果有)的相关条块组成:</li> <li>● 前几个文件</li> <li>● 前几个注册表项</li> <li>● 前几个进程</li> <li>● 前几个模块(dll)</li> </ul>
首要已禁止设备	此报告由一个饼图和一个相关条块组成,该条块显示了最常被禁止访问网络的设备。

表10-4 说明了可用的"审核"报告。

表10-4

"审核"报告

报告名称	说明
使用的策略	此报告显示了客户端和位置当前所使用的策略。其中所含的信息包括域名、组名称, 以及应用于各个组的策略的序列号。

表 10-5 说明了可用的"遵从性"报告。

表10-5

"遵从性"报告

报告名称	说明
网络遵从性状态	此报告由一个折线图和一个表组成。它显示了事件时间、攻击次数以及每个事件所涉 及的攻击的百分比。
	您可以显示在您所选时间范围内,已应用下列遵从性操作的客户端总数:
	■ 已验证
	■ 已断开
	■ 失败
	■ 已通过
	■ 已拒绝

报告名称	说明
遵从性状态	您可以选择一项操作,以显示一个显示以下其中一项的折线图:
	<ul> <li>■ 在您所选的时间范围内您的网络中通过主机完整性检查的客户端总数</li> <li>■ 在您所选时间的范围内您的网络中未通过主机完整性检查的客户端总数</li> </ul>
	此报告还包括一个表,该表显示了事件时间、客户端数量以及每一事件所涉及的客户 端的百分比。
遵从性失败的客户摘要	此报告包含一个显示下列信息的条形图:
	<ul> <li>■ 按控制失败事件的类型(如防病毒、防火墙或 VPN)列出的不重复工作站数量。</li> <li>■ 组内客户端的总数。</li> </ul>
遵从性失败详细信息	此报告包含一个表,该表按控制失败显示了不重复计算机的数量。它显示了每一项失 败所涉及的条件和规则。它包括部署的客户端百分比及失败的百分比。
按位置列出的不遵从客户端	此报告包含一个显示遵从性失败事件的表。这些事件会按其位置显示在组中。所含信 息包括失败的不重复计算机数量以及总失败和位置失败的百分比。

表 10-6 说明了可用的"计算机状态"报告。

### 表10-6 "计算机状态"报告

报告名称	说明
病毒定义分发	此报告显示了用于整个网络的不重复病毒定义文件版本,以及使用每种版本的计算机 数量和百分比。它由一个饼图、一个表和一些相关条块组成。
未登入服务器的计算机	此报告显示了未签入其服务器的所有计算机的列表。它还显示了计算机的 IP 地址、其最后一次签入的时间,以及当时登录的用户。
Symantec Endpoint Protection 产品版本	此报告显示了网络中所有 Symantec Endpoint Protection 产品版本的版本号列表。它还包含了使用各版本的域和服务器,以及使用各版本的计算机数量和百分比。它由一个饼图和一些相关条块组成。
人侵防护特征分布	此报告显示了用于整个网络的 IPS 特征文件版本。它还包含了使用各版本的域和服务器,以及使用各版本的计算机数量和百分比。它由一个饼图和一些相关条块组成。
客户端清单	<ul> <li>此报告包含了下列图表及相关条块,这些条块显示了每一项对应的计算机总数和百分比:</li> <li>操作系统</li> <li>总内存</li> <li>可用内存</li> <li>总磁盘空间</li> <li>可用磁盘空间</li> <li>处理器类型</li> </ul>

报告名称	说明
遵从性状态分布	此报告由一个饼图和一些相关条块组成,这些条块按组或按子网显示了遵从性的通过 和未通过情况。它显示了计算机的数量和符合遵从性的计算机的百分比。
客户端联机状态	此报告包含了一些饼图及对应于每组或每个子网的相关条块。它显示了联机的计算机的百分比。
	联机包含如下含义:
	<ul> <li>对于推模式下的客户端,联机表示客户端当前已连接到服务器。</li> <li>对于拉模式下的客户端,联机表示客户端在上两个客户端检测信号期间内已连上服务器。</li> <li>对于运费站点中的客户端,联机表示客户端在上次复制时处无联机状态</li> </ul>
	■ 刈了起性如点牛的谷广调,状况农小谷广调任工队发前时处于状况状态。
有最新策略的客户端	此报告包含了一些饼图及对应于每组或每个子网的相关条块。它显示了应用最新策略的计算机数量和百分比。
按组显示客户端计数	此报告包含一个按组列出主机信息统计的表。它列出了客户端和用户的数量。如果您 使用多个域,这些信息会按域显示。
安全状态摘要	此报告反映了网络的常规安全状态。
	此报告显示了具有下列状态的计算机数量和百分比:
	■ 防病毒引擎已关闭。
	■ 自动防护已关闭。
	<ul> <li>■ 防暴改已天闭。</li> <li>■ 需要重新启动</li> </ul>
	■ 主机完整性检查未通过。
	■ 网络威胁防护已关闭。
防护内容版本	此报告在单个报告中显示用于整个网络的所有主动型防护内容版本。针对每种类型的防护显示一个饼图。
	以下是可用的内容类型:
	<ul> <li>■ 解压缩程序版本</li> <li>■ 清除引擎版本</li> </ul>
	■ TruScan 主动型威胁扫描内容版本
	■ TruScan 主动型威胁扫描引擎版本
	■ 商业应用程序列表版本 -  大計測也容处理程序可能低本
	<ul> <li>■ 土切型內谷处理程序引擎成本</li> <li>■ 允许的应用程序列表版本</li> </ul>
	■ Symantec 安全响应中心已增加的新内容类型
客户端迁移	此报告包含一些按域、组和服务器说明客户端迁移状态的表。它显示了客户端IP地址, 以及迁移是成功、失败,还是尚未开始。

报告名称	说明
客户端软件分装(快照)	此报告包含一些跟踪客户端软件包部署进度的表。利用快照信息,您可以了解分装的
此报告仅可用作调度报告。	进度情况,以及尚未完全部署的客户端数量。
某段时间内的联机/脱机客户 端(快照)	此报告由一些折线图和表组成,这些表显示了联机或脱机的客户端数量。针对每个首 要目标显示一个图表。目标是组或操作系统。
此报告仅可用作调度报告。	
某段时间内有最新策略的客户 端(快照)	此报告包含一个显示已应用最新策略的客户端的折线图。针对前几个客户端中的每一个显示一个图表。
此报告仅可用作调度报告。	
某段时间内的非遵从性客户端 (快照)	此报告包含一个折线图,此图显示了某段时间内未通过主机完整性检查的客户端百分 比。针对前几个客户端中的每一个显示一个图表。
此报告仅可用作调度报告。	
病毒定义分装(快照)	此报告列出了已分装到客户端的病毒定义包版本。这些信息有助于从控制台跟踪新病
此报告仅可用作调度报告。	· 每定乂的茚者进度。

表 10-7 说明了可用的"网络威胁防护"报告。

报告名称	说明
首要遭攻击目标	此报告由一个饼图和相关条块组成。您可以使用组、子网、客户端或端口作为目标来 查看信息。它包括攻击的数量和百分比、攻击类型和严重性、攻击分布等信息。
首要攻击源	此报告由一个饼图和一些相关条块组成,这些条块显示了向您的网络发动攻击的首要 主机。它包括攻击的数量和百分比、攻击类型和严重性、攻击分布等信息。
首要攻击类型	此报告由一个饼图和关联的相关条块组成。它包括事件的数量和百分比等信息,还包括组和严重性,以及按组显示的事件类型和数量。
首要禁止的应用程序	此报告由一个饼图和一些相关条块组成,这些条块显示了被禁止访问您的网络的首要 应用程序。它包括攻击的数量和百分比、组和严重性、按组显示的攻击分布等信息。
某段时间内的攻击	此报告由一个或多个折线图组成,显示了在所选时间段内的攻击情况。例如,如果时间范围是上个月,则此报告会显示上个月每天的攻击总数。它包括攻击的数量和百分比。您可以查看所有计算机的攻击情况,或者按首要操作系统、用户、IP地址、组或攻击类型查看攻击情况。
按严重性显示安全事件	此报告包含一个饼图,该图显示了网络中按严重性排列的安全事件的总数和百分比。

### 表10-7 "网络威胁防护"报告
报告名称	说明
某段时间内禁止的应用程序	此报告由折线图和表组成。它显示了在您所选的时间段内被禁止访问您的网络的应用 程序总数。它包括事件时间、攻击数量和百分比。您可以显示所有计算机的信息,或 者按组、IP 地址、操作系统或用户来显示信息。
某段时间内的通信通知	此报告包含一个折线图。它显示了某段时间内根据防火墙违规情况生成的通知数。计 入的规则就是您在"防火墙策略规则"列表的"记录"列中选中"发送电子邮件警报" 的规则。您可以在此报告中显示所有计算机的信息,或者按组、IP地址、操作系统或 用户来显示信息。
前几项通信通知	此报告由一个饼图和一些相关条块组成,这些条块列出了组或子网以及通知的数量和 百分比。它显示了根据您配置为务必通知的防火墙违规情况生成的通知数量。计入的 规则就是您在"防火墙策略规则"列表的"记录"列中选中"发送电子邮件警报"的 规则。您可以查看按前几个组或子网分组的全部信息、通信日志信息或数据包日志信 息。
完整报告	<ul> <li>此报告在单个报告中提供下列网络威胁防护信息:</li> <li>首要攻击类型</li> <li>按组列出首要遭攻击目标</li> <li>按子网列出首要遭攻击目标</li> <li>按客户端列出首要遭攻击目标</li> <li>按客户端列出首要遭攻击目标</li> <li>首要攻击源</li> <li>按组显示前几项通信通知(通信)</li> <li>按组显示前几项通信通知(数据包)</li> <li>按子网显示前几项通信通知(数据包)</li> <li>按子网显示前几项通信通知(数据包)</li> <li>此报告包含所有域的相关信息。</li> </ul>

表 10-8 说明了可用的"风险"报告。

表10-8	风险报告

报告名称	说明
受感染和有风险的计算机	此报告由两个表组成。其中一个表列出了受病毒感染的计算机。另一个表列出了含尚未补救的安全风险的计算机。
检测操作摘要	此报告包含一个表,该表显示了在检测到风险时可能采取的所有操作的数量。可能的操作有"已清除"、"可疑"、"已禁止"、"已隔离"、"已删除"、"新感染"和"仍受感染"。此信息也会显示在 Symantec Endpoint Protection 主页上。
风险检测数量	此报告由一个饼图、一个风险表和一个关联的相关条块组成。它按域、服务器或计算 机显示了风险检测总数。如果您用的是旧版 Symantec AntiVirus 客户端,则此报告会 使用服务器组,而非域。

报告名称	说明
网络中检测到的新风险	此报告包含一个表和一个分布饼图。 针对每一个新风险,此表提供了下列信息:
	<ul> <li>风险名称</li> <li>风险类别或类型</li> <li>首次发现日期</li> <li>组织中的第一次出现情况</li> <li>最先检测到它的扫描类型</li> <li>发现它时它所在的域(在旧版计算机上为服务器组)</li> <li>发现它时它所在的服务器(在旧版计算机上为父服务器)</li> <li>发现它时它所在的组(在旧版计算机上为父服务器)</li> <li>发现它时它所在的计算机以及当时登录的用户名</li> <li>此饼图按以下所选目标类型显示新风险的分布情况:域(在旧版计算机上为服务器 组) 组 服务器(在旧版计算机上为父服务器) 计算机或用户名。</li> </ul>
前几个风险检测关联	此报告包含一个三维条形图,该图使用两个变量来关联病毒和安全风险检测。您可以 从计算机、用户名、域、组、服务器或风险名称中选择作为 x 和 y 轴变量的项。此报 告显示每个轴变量的前五个实例。如果您选择了计算机作为其中的一个变量,而受感 染的计算机少于五台,则图中可能会显示未受感染的计算机。
	<b>注意</b> :对于运行旧版 Symantec AntiVirus 的计算机,使用的是服务器组和父服务器,而不是域和服务器。
风险分布摘要	此报告包括一个饼图和一个关联的条形图,该条形图显示了所选目标类型中每个不重 复项的相对百分比。例如,如果选择的目标是风险名称,则此饼图会显示每个不重复 风险的切片。针对每个风险名称显示一个条块,详细信息包括检测数目及其占检测总 计的百分比。目标包括风险名称、域、组、服务器、计算机、用户名、源、风险类型 或风险严重性。对于运行旧版 Symantec AntiVirus 的计算机,使用的是服务器组和父 服务器,而不是域和服务器。
某段时间内的风险分布	此报告由一个表及一个相关条块组成,该表显示了单位时间内检测到的病毒和安全风 险数量。
TruScan 主动型威胁扫描检测 结果	<ul> <li>此报告由一个饼图和一些条形图组成,这些条形图显示了下列信息:</li> <li>●标记为风险但您已将其添加到网络可接受的例外中的应用程序列表。</li> <li>■已检测到且已确认为风险的应用程序列表。</li> <li>■已检测到但其状态仍未确认为风险的应用程序列表。</li> <li>对于每个列表,此报告都会显示公司名称、应用程序哈希及版本以及所涉及到的计算机。对于允许的应用程序,此报告还会显示授予允许的源。</li> </ul>

报告名称	说明
TruScan 主动型威胁分布	此报告由一个饼图以及一些相关条块和一个摘要表组成,此图显示了检测到的前几个 应用程序的名称。这些检测包括"商业应用程序列表"和"强制检测"列表上的应用 程序。第一个摘要表包含应用程序名称以及检测的数目和百分比。
	此摘要表显示每个检测的下列信息:
	<ul> <li>应用程序名称和哈希</li> <li>应用程序类型,为击键记录程序、特洛伊木马、蠕虫、远程控制或商业击键记录程序</li> <li>公司名称</li> <li>应用程序版本</li> </ul>
	■ 报告该检测的不重复计算机数量
	<ul> <li>■ 粒测中的前三个路径名</li> <li>■ 上次检测日期</li> </ul>
某段时间内的 TruScan 主动 型威胁检测	此报告包含一个折线图,该图显示了所选时间段内的主动型威胁检测数目。它还包括 一个含相关条块的表,该表列出了某段时间内检测到的威胁总数。
前几个风险的操作摘要	此报告列出了网络中发现的前几个风险。对于每个风险,此报告都会显示操作摘要条 块,这些条块显示在检测到风险时所采取的每项操作的百分比。操作包括"已隔离"、 "已清除"、"已删除"等。此报告还会显示每一个特定操作为第一个配置的操作、 第二个配置的操作、两者皆非或为未知的时间百分比。
通知数	此报告由一个饼图和一个关联的相关条块组成。图表显示了您配置为务必通知的防火墙违规情况所触发的通知数。它包含了每个通知的类型和数量。
	请参见第 413 页的"配置通信事件的电子邮件"。
某段时间内的通知数	此报告包含一个折线图,此图显示了在所选时间段内网络中的通知数。它还包含一个 表,该表列出了某段时间内的通知数量和百分比。您可以过滤数据,使其按通知类型、 确认状态、创建者和通知名称显示。
每周爆发	此报告显示在指定的时间范围内检测到的病毒和安全风险的数目,并针对每周检测到 的每种病毒或安全风险的数目显示一个相关条块。时间范围为一天时会显示过去一周 的情况。
全面风险报告	默认情况下此报告包括所有的分布报告和新风险报告。不过,您可以将其配置为只包 含特定的报告。此报告包含所有域的相关信息。

表 10-9 说明了可用的"扫描"报告。

表10-9 "扫描"报告			
报告名称	说明		
扫描统计信息直方图	此报告以直方图形式显示。您可以选择此扫描报告中信息的分布方式。您可以选择以 下方式之一:		
	<ul> <li>按扫描时间(秒)</li> <li>按检测到的风险数</li> <li>按检测到风险的文件数</li> <li>按扫描的文件数</li> <li>按扫描时省略的文件数</li> </ul>		
	您还可以配置直方宽度和直方图中使用的直方数目。直方宽度是用于所选分组依据的 数据间隔。直方数目指定直方图中重复使用几次此数据间隔。		
	显示的信息包括条目数、最大值和最小值,以及平均值和标准偏差。		
	您可能需要更改报告值,以使报告的直方图中生成最大数量的信息。例如,您可能需 要考虑所查看的网络规模和信息量。		
按上次扫描时间显示计算机	此报告按上次扫描时间显示安全网络内的计算机列表。它还包含 IP 地址和扫描时登录的用户名。		
未扫描的计算机	此报告显示安全网络中尚未扫描的计算机列表。		
	此报告提供下列附加信息:		
	<ul> <li>■ IP 地址</li> <li>■ 上次扫描的时间</li> <li>■ 当前用户名或上次扫描时登录的用户名</li> </ul>		

表 10-10 说明了可用的"系统"报告。

表10-10 "系统"报告

报告名称	说明
按生成错误多少排列最靠前的	此报告包含一个饼图,该图显示每个警告状况和错误状况。图表按客户端显示相关错
客户端	误数和相关警告数及百分比。
按生成错误多少排列最靠前的	此报告包含一个饼图,该图显示每个警告状况和错误状况。图表按服务器显示相关错
服务器	误数和相关警告数及百分比。
按生成错误多少排列最靠前的	此报告包含一个饼图,该图显示每个警告状况和错误状况。图表按 Enforcer 显示相关
Enforcer	错误数和相关警告数及百分比。
某段时间内的数据库复制失败	此报告由一个折线图和一个关联表组成,该表列出所选时间范围内的复制失败情况。

报告名称	说明
站点状态	此报告显示本地站点中所有服务器的当前状态和吞吐量。它还会显示本地站点的客户 端安装、客户端联机状态及客户端日志量的相关信息。此报告的数据来源每10秒钟更 新一次,但您需要重新运行报告,才能看到更新后的数据。
	<b>注意</b> :如果您有多个站点,此报告会显示本地站点(而不是所有站点)已安装的客户端总计和联机的客户端总计。
	如果您作为管理员存在站点或域限制,则您只会看到允许您查看的信息。
	服务器的运行状态分类如下:
	<ul> <li>良好:服务器已启动,并且正常工作</li> <li>差:服务器的内存或磁盘空间不足,或有大量的客户端请求失败。</li> <li>重要:服务器宕机</li> </ul>
	对于每一台服务器,此报告都包含状态、运行状态和原因、CPU 和内存使用,以及可 用磁盘空间。它还包含服务器吞吐量信息,如已下载的策略,以及从上次检测信号期 间抽样所得的站点吞吐量。
	它包含下列站点吞吐量信息:
	■ 已安装的和联机的客户端总计
	■ 每秒下载的策略数
	■ 每秒下载的入侵防护特征数 年14月2日年1月1日年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日
	■ 母杪巳知的应用程序数 ■ 每秒的 Enforcer 系统日主教 通信日主教和教握句日主教
	<ul> <li>■ 母校的 Enforcer 示沉白心致、适信白心致和致语色白心致</li> <li>■ 每秒客户端信息更新数</li> </ul>
	■ 每秒接收的客户端安全日志数、系统日志数、通信日志数和数据包日志数
	■ 每秒接收的应用程序与设备控制日志数
	在此报告中,联机有以下含义:
	■ 对于推模式下的客户端,联机表示客户端当前已连接到服务器。
	<ul> <li>■ 对于拉模式下的客户端,联机表示客户端在上两个客户端检测信号期间内已连上服务器。</li> </ul>
	■ 对于远程站点中的客户端,联机表示客户端在上次复制时处于联机状态。

## 关于报告的重要须知

使用报告时,请务必注意下列信息:

- 报告中的时间戳会以用户的当地时间为准。报告数据库所包括的事件则是以格 林威治标准时间(GMT)为准。当您创建报告时,GMT 值会转换成您查看报告所 在计算机的当地时间。
- 在某些情况下,报告数据不会与安全产品中所出现的事件——对应。发生不对 应的情况是因为报告软件会汇总安全事件。

- 报告中的风险类别信息是从 Symantec 安全响应中心网站获取的。在 Symantec Endpoint Protection Manager 控制台能检索此项信息之前,您生成的任何报告 在风险类别字段中都会显示为"未知"。
- 您生成的报告可提供网络中受威胁计算机的准确状况。这些报告基于日志数据, 而非 Windows 注册表数据。
- 报告页面和日志页面通常会以安装管理服务器时所用的语言显示。若要在使用 远程控制台或浏览器时显示这些页面,您必须在所使用的计算机上安装适当的 字体。
- 如果在运行含大量数据的报告时收到数据库错误,您可能要更改数据库超时参数。

请参见第 255 页的"更改超时参数"。

 如果收到 CGI 或终止进程错误,您最好更改其他超时参数。
 请参见 Symantec 知识库中标题为 "Reporting server does not report or shows a timeout error message when you query large amounts of data"的文章。

如果您的网络中有正在运行旧版 Symantec AntiVirus 的计算机,请务必注意下列 信息:

- 使用报告和日志过滤器时,服务器组会归类为域。客户端组会归类为组,而父服务器则归类为服务器。
- 如果您生成的报告中包含旧式计算机, "IP 地址"和 "MAC 地址"字段会显示 "无"。

## 创建快速报告

通过从"您要使用何种过滤器设置"下方的"基本设置"选项选择,生成快速报告。如果您要配置生成报告的其他选项,请单击"高级设置"。每个报告的"基本 设置"和"高级设置"各不相同。

可以单击 Symantec Endpoint Protection Manager 控制台上该类型报告的"更多信息",查看有关各项可配置的高级设置的说明。单击"更多信息"会显示该类型报告的上下文关联帮助。

您可以保存报告设置,以便日后可运行相同的报告,并且可以打印和保存报告。

**注意**: 接受通配符和搜索匹配条目的过滤器选项文本框不区分大小写。ASCII 星号 字符是唯一可用作通配符的星号字符。

请参见第154页的"打印和保存报告副本"。

表 10-11 说明适用于所有类型的快速报告的所有"基本设置"。

设置	说明
时间范围	指定您要在报告中查看的事件的时间范围。
	请从下列时间中进行选择:
	■ 过去 24 小时
	■ 过去一周
	■ 以去一个月 ■ 当前的目份
	■ 过去三个月
	■ 过去一年
	■ 设置特定日期
	如果选择"设置特定日期",则某些报告会要求设置"开始日期"和"结束日期"。其他报告会要求您设置"上次登录时间",也就是计算机上次登录服务器的时间。
	默认为"过去 24 小时"。
开始日期	指定日期范围的开始日期。
	仅在对时间范围选择"设置特定日期"时才可用。
结束日期	指定日期范围的结束日期。
	仅在对时间范围选择"设置特定日期"时才可用。
	<b>注意</b> :设置的结束日期不能等于或早于开始日期。
在上次签入后	指定要查看自上次签入之后就未再签入服务器的计算机的所有条目。
	仅在您为时间范围选择"设置特定日期"时,才适用于计算机状态报告。
状态	适用于"网络遵从性状态"遵从性报告。从以下选项进行选择:
	■ 已验证
	■ 已断开
	■
	■ 已拒绝
	适用于"遵从性状态"遵从性报告。选择下列任一操作:
	 ■ 已通过
	■ 失败
分组依据	许多报告都能适当分成不同的组。例如,最常见的选择是仅查看一个组或子网的信息,而某 些报告则提供其他适当的选择。

表10-11 快速报告的基本过滤器设置

设置	说明
目标	<ul> <li>适用于"首要遭攻击目标"网络威胁防护报告。从以下选项进行选择:</li> <li>组</li> <li>子网</li> <li>客户端</li> <li>端口</li> <li>适用于"某段时间内的攻击"网络威胁防护报告。从以下选项进行选择:</li> <li>所有</li> <li>组</li> <li>P地址</li> <li>操作系统</li> <li>用户名</li> <li>攻击类型</li> <li>适用于"某段时间内禁止的应用程序"和"某段时间内的通信通知"网络威胁防护报告。从以下选项进行选择:</li> <li>所有</li> <li>组</li> <li>P地址</li> <li>操作系统</li> <li>用户名</li> <li>适用手"前几项通信通知"网络威胁防护报告。从以下选项进行选择:</li> <li>所有</li> <li>通信</li> <li>通信</li> <li>数据包</li> </ul>
X 轴 Y 轴	适用于"前几个风险检测关联"风险报告。从以下选项进行选择: <ul> <li>计算机</li> <li>用户名</li> <li>域</li> <li>组</li> <li>服务器</li> <li>风险名称</li> </ul>
直方宽度	指定构成直方图的直方宽度。适用于"扫描统计信息直方图"扫描报告。
直方数目	指定用于构成直方图的直方条数目。适用于"扫描统计信息直方图"扫描报告。

"高级设置"可进一步控制您要查看的数据。这些设置专用于报告类型和内容。

有关各个可配置的高级设置的说明,可以单击控制台上该类型报告的"更多信息"。 单击"更多信息"会显示该类型报告的上下文关联帮助。

#### 创建快速报告

- 1 在控制台中,单击"报告"。
- 2 在"快速报告"选项卡的"报告类型"列表框中,选择要创建的报告类型。例如,选择"风险"。
- **3** 在"您想查看哪种类型的扫描报告"下方的"选择报告"列表框中,选择您要 查看的报告名称。例如,选择"风险检测数量"。
- 4 在"使用保存的过滤器"列表框中,选择要使用的保存的过滤器配置,或者保 留默认过滤器。
- 5 在"您要使用何种过滤器设置"下方的"时间范围"列表框中,选择报告的时间范围。
- 6 如果您已选择"设置特定日期",则使用"开始日期"和"结束日期"列表框。这些选项可设置您要查看有关信息的时间间隔。
- 7 如果您要配置报告的其他设置,请单击"高级设置",并设置您想要的选项。 您可以单击"快速报告"选项卡中的"更多信息",以在上下文关联帮助中查 看过滤器选项的说明。

若有3个点的按钮,则可显示该选择的已知选项列表。例如,此选项可显示已 知服务器列表或已知域列表。

如果您日后要再次运行此报告,则可以保存报告配置设置。

请参见第153页的"保存和删除已保存的报告过滤器"。

**8** 单击"创建报告"。

## 保存和删除已保存的报告过滤器

您可以保存自定义报告设置,以便日后可以再生成同样的报告。保存设置时,设置 会保存到数据库中。您提供给过滤器的名称会显示在适用于该类型日志和报告的 "使用保存的过滤器"列表框中。

**注意**:您保存的过滤器配置设置仅供您的用户登录帐户使用。其他具有报告权限的 用户不能访问您保存的设置。

您可以删除您所创建的任何报告配置。删除配置后,您就不能再使用相应报告。默 认报告配置名称会出现在"使用保存的报告"列表框中,屏幕会重新填入此默认配 置设置。

#### 保存过滤器

- 1 在控制台中,单击"报告"。
- 2 从列表框选择报告类型。

- 3 更改报告的任何"基本设置"或"高级设置"。
- 4 单击"保存过滤器"。
- 5 在"过滤器名称"文本框中,键入此报告过滤器的说明性名称。过滤器添加到 "使用保存的过滤器"列表后,只会显示该名称的前 32 个字符。
- 6 单击"确定"。
- 7 在确认对话框显示时单击"确定"。

在您保存过滤器后,该过滤器会显示在适用于相关报告和日志的"使用保存的 过滤器"列表框中。

#### 删除保存的过滤器

- 1 在"报告"选项卡上,选择报告类型。
- 2 在"使用保存的过滤器"列表框中,选择要删除的过滤器名称。
- 3 在"使用保存的过滤器"列表框旁单击"删除"图标。
- 4 在确认对话框显示时单击"是"。

## 关于重复的过滤器名称

过滤器存储部分由创建者决定,因此当两个用户创建同名过滤器时,并不会发生问题。但是,单个用户或以默认的admin帐户登录的两个不同用户不得创建同名过滤器。

如果用户创建同名过滤器,则在以下两种情况下会发生冲突:

- 两个用户在不同的站点上都以默认的 admin 帐户登录,且两个用户创建了同名 过滤器。
- 一个用户在创建一个过滤器后又登录其他站点并紧接着创建了另一个相同名称 的过滤器。

如果在站点复制之前出现了任一种情况,则用户随后会在过滤器列表中看到两个同 名的过滤器。只有一个过滤器可供使用。当出现此问题时,最佳做法是删除可用过 滤器,然后以其他名称重新创建。删除可用过滤器时,不可用的过滤器也会随之删 除。

## 打印和保存报告副本

当您生成报告后,报告会出现在新窗口中。您可以打印报告或保存报告副本。

**注意**:默认情况下,Internet Explorer 不会打印背景颜色和图像。如果禁用这个打印选项,打印出来的报告可能看起来会与当初创建的报告不同。您可以将浏览器的 设置更改为打印背景颜色和图像。

#### 打印报告副本

- 1 在"报告"窗口中,单击"打印"。
- 2 在"打印"对话框中,视需要选择所要的打印机,然后单击"打印"。

当您保存报告时,您保存的是基于报告数据库中当前数据的安全环境快照。如果稍 后再以相同的过滤器配置运行相同的报告,新报告会显示不同的数据。

#### 保存报告副本

- **1** 在"报告"窗口中,单击"保存"。
- 2 在"文件下载"对话框中,单击"保存"。
- 3 在"另存为"对话框的"保存位置"选择框中,浏览至文件要保存到的位置。
- 4 在"文件名"列表框中,视需要更改默认的文件名。
- 5 单击"保存"。

报告会以MicrosoftWeb存档、单个文件(\*.mht)的格式保存到您选定的位置。

6 在"下载完成"对话框中,单击"关闭"。

## 创建和删除调度报告

调度报告是指根据您所配置的调度自动运行的报告。调度报告会以电子邮件形式发送给收件人,因此您必须加入至少一位收件人的电子邮件地址。报告运行之后,会以.mht 文件附件形式通过电子邮件发送给您所配置的收件人。

快照报告中所显示的数据每小时都会在数据库中进行更新。调度报告会按管理员使用"运行间隔"选项所配置的时间通过电子邮件发送给报告的收件人。在Symantec Endpoint Protection 通过电子邮件发送快照报告时,报告中的数据是最近一小时内的最新数据。含某段时间内数据的其他报告会根据您针对客户端日志所配置的上传间隔在数据库中进行更新。

请参见第 251 页的"配置客户端日志设置"。

**注意**:如果您在某站点中有多个服务器共享数据库,则只有最先安装的服务器才会运行为该站点调度的报告。此默认设置可以确保站点中的所有服务器不会同时运行相同的调度扫描。若要指定不同的服务器运行调度报告,则可以在本地站点属性中配置此选项。

请参见第 205 页的"编辑站点属性"。

下列快速报告仅可作为调度报告使用:

- 客户端软件分装(快照)
- 某段时间内的联机/脱机客户端(快照)

- 某段时间内有最新策略的客户端(快照)
- 某段时间内的非遵从性客户端(快照)
- 病毒定义分装(快照)

您可以更改已调度的任何报告的设置。下次运行报告时,就会使用新的过滤器设置。您也可以创建其他调度报告,并将其关联至先前保存的报告过滤器。您可以删除单个或所有调度报告。

**注意**: 当您将保存的过滤器与调度报告关联时,请确定过滤器不含自定义日期。如果过滤器指定了自定义日期,您会在每次报告运行时获得相同的报告。

和您按需运行的报告一样,您可以打印和保存调度报告。

**注意**:在首次创建调度报告时,您必须使用默认过滤器或已保存的过滤器。在调度 报告后,您可以返回上一步,并编辑过滤器。

如需在这些过程中可以在"调度报告"选项卡上设置的选项的相关信息,请单击"更多信息"。

#### 创建调度报告

- 1 在控制台中,单击"报告"。
- 2 在"调度报告"选项卡上,单击"添加"。
- 3 在"报告名称"文本框中,键入说明性名称,并选择是否键入较长的说明。 虽然您可以将超过255个字符的文本粘贴到"说明"文本框中,但此说明中只 会保存255个字符。
- 4 如果当前不想运行此报告,请取消选中"启用此调度报告"。
- 5 从列表框选择您要调度的报告类型。
- 6 从列表框选择您要调度的特定报告名称。
- 7 从列表框选择您要使用的已保存过滤器的名称。
- 8 在"运行间隔"文本框中,选择您要通过电子邮件发送报告的时间间隔(小时数、天数、周数、月数)。然后键入选定的时间间隔值。例如,如果您要每隔一天提交报告,请选择天数,然后键入2。
- 9 在"报告调度"下的"运行间隔"文本框中,键入此报告应该通过电子邮件发送给收件人的频率。
- 10 在"在以下时间后开始"文本框中,键入您要开始运行报告的日期,或者单击 日历图标,然后选择日期。然后从列表框选择小时和分钟。

- 11 在"报告收件人"下方,键入电子邮件地址,多个地址则请以逗号分隔。 您必须先设置邮件服务器属性,电子邮件通知才会生效。
- 12 单击"确定"以保存调度报告配置。

#### 编辑用于调度报告的过滤器

- 1 在控制台中,单击"报告"。
- 2 单击"调度报告"。
- 3 在报告列表中,单击您要编辑的调度报告。
- **4** 单击"编辑过滤器"。
- 5 对过滤器进行所需的更改。
- 6 单击"保存过滤器"。
  - 若要保留原始的报告过滤器,请重命名此编辑后的过滤器。
- 7 单击"确定"。
- 8 在确认对话框显示时单击"确定"。

#### 删除调度扫描

- 1 在控制台中,单击"报告"。
- 2 在"调度报告"选项卡的报告列表中,单击您要删除的报告名称。
- 3 单击"删除"。
- 4 在确认对话框显示时单击"是"。

158 | 查看和配置报告 | **创建和删除调度报告** 

# 11

## 查看和配置日志和通知

本章节包括下列主题:

- 关于日志
- 使用监视器摘要选项卡
- 查看日志
- 保存和删除过滤器
- 日志的基本过滤设置
- 日志的高级过滤器设置
- 从日志运行命令和操作
- 关于减少发送至日志的事件量
- 导出日志数据
- 使用通知

## 关于日志

您可以使用日志查看安全产品所生成的详细事件。日志所包括的事件数据来自管理 服务器以及与这些服务器通信的所有客户端。由于报告是静态的,其所包括的详细 数据没有日志里那么多,因此某些管理员倾向于使用日志来监控其网络。

您可能想通过查看这些信息来解决网络中的安全或连接问题。这些信息也有助于调 查威胁或确认事件的历史记录。

**注意**:报告页面和日志页面通常会以安装管理服务器时所用的语言显示。若要在使用远程 Symantec Endpoint Protection Manager 控制台或浏览器时显示这些页面,必须在所使用的计算机上安装适当的字体。

您可以将某些日志事件数据导出为可用于导入电子表格应用程序的逗号分隔文件。 其他日志数据则可以导出为转储文件或导出至 Syslog 服务器。

请参见第175页的"导出日志数据"。

## 关于日志类型、内容和命令

您可以从"监视器"页查看下列类型的日志:

- 应用程序与设备控制
- 审核
- 遵从性
- 计算机状态
- 网络威胁防护
- TruScan 主动型威胁扫描
- 风险
- ∎ 扫描
- 系统

**注意:**所有这些日志都可以从"监视器"页使用"日志"选项卡访问。您可以在 "通知"选项卡上查看有关已创建通知的信息,并可以在"命令状态"选项卡上查 看有关命令状态的信息。

某些类型的日志又细分为不同类型的内容,以便于查看。例如,应用程序控制与设 备控制日志包括应用程序控制日志和设备控制日志。您也可以从某些日志运行命 令。

请参见第179页的"查看和过滤管理员通知信息"。

**注意**:如果您仅安装了 Symantec Network Access Control,则仅有一些日志包含数据;一些日志为空。审核日志、遵从性日志、计算机状态日志和系统日志都包含数据。如果您只安装了 Symantec Endpoint Protection,则遵从性日志和 Enforcer 日志为空,而其他所有日志包含数据。

表11-1说明了您可查看的不同类型的内容,以及您可以通过各个日志执行的操作。

日志类型	内容和操作
应用程序与设备控制	应用程序控制日志和设备控制日志包含有关禁止某些类型行为的事件的信息。 有以下应用程序与设备控制日志可供使用: • 应用程序控制,包括有关防篡改的信息 • 设备控制 应用程序控制日志中的信息包括如下条目: • 事件发生的时间 • 采取的操作 • 相关域和计算机 • 严重性 • 相关规则 • 调用者进程 • 目标 设备控制日志中的信息包括如下条目: • 事件发生的时间 • 事件发型 • 相关域和组 • 相关域和组 • 相关试算机 • 相关计算机 • 相关计算机 • 相关式算机 • 相关式算机 • 相关成用名
审核	审核日志包含有关策略修改活动的信息。可用信息包括事件时间和类型、修改的策略、 相关域、站点和管理员,以及说明。 此日志没有任何关联的操作。

表11-1 日志和列表

日志类型	内容和操作
遵从性	遵从性日志包含有关 Enforcer 服务器、Enforcer 客户端和 Enforcer 通信以及主机遵 从性的信息。
	如果您安装了 Symantec Network Access Control,下列遵从性日志可供使用:
	<ul> <li>Enforcer 服务器 此日志跟踪Enforcer与其管理服务器之间的通信。记录的信息包括Enforcer名称、 与管理服务器连接的时间、事件类型、站点,以及服务器名称。</li> <li>Enforcer客户端 提供有关所有Enforcer客户端连接的信息,包括对等验证信息。提供的数据包括各 个Enforcer的名称、类型、站点、远程主机和远程MAC地址,以及是否已通过、 拒绝或验证客户端。</li> <li>Enforcer通信(仅Gateway Enforcer) 提供有关通过Enforcer设备所进行的通信的某些信息。此信息包括通信的方向和时 间、使用的协议、Enforcer名称和站点。此信息还包括使用的本地端口、方向和计 数。您可以过滤已允许或已禁止的连接尝试。</li> <li>主机遵从性 此日志跟踪客户端的主机完整性检查的详细信息。可用信息包括时间、位置、操作 系统、故障原因和说明。</li> </ul>
	这些日志没有任何关联的操作。

日志类型	内容和操作
计算机状态	计算机状态日志包含有关网络客户端计算机的实时操作状态的信息。可用信息包括计 算机名和 IP 地址、上次登录时间、定义日期、受感染状态、自动防护状态、服务器、 组、域和用户名。
	您可以通过计算机状态日志执行下列操作:
	<ul> <li>扫描 此命令启动"活动扫描"、"全面扫描"或"自定义扫描"。自定义扫描选项是您 在"管理员定义的扫描"页上设置的命令扫描选项。命令使用的是"防病毒和防间 谍软件策略"中的设置,此策略将应用于选来进行扫描的客户端。</li> <li>更新内容</li> </ul>
	端进行策略、定义和软件更新。
	■ 更新内容并扫描
	此命令触发对所选择组中客户端进行策略、定义和软件更新。此命令随后将启动 "活动扫描"、"全面扫描"或"自定义扫描"。自定义扫描选项是您在"管理员 定义的扫描"页上设置的命令扫描选项。命令使用的是"防病毒和防间谍软件策 略"中的设置,此策略将应用于选来进行扫描的客户端。
	■ 取用所有扫描 此命令将取消对所选收件人进行的所有正在运行的扫描和任何排队的扫描。
	■ 重新启动客户端计算机
	此命令会重新启动所选计算机。如果用户登录,会显示重新启动警告,该警告基于 管理员为该计算机配置的重新启动选项。您可以在"客户端"页面的"策略"选项 卡中的"常规设置"对话框的"常规设置"选项卡中配置客户端重新启动选项。
	■ 后用目初防护 此命令可以为您选择的所有客户端计算机启用自动防护。
	■ 启用网络威胁防护
	此命令可以为您选择的所有客户端计算机启用网络威胁防护。
	禁用网络威胁防护 此命令可以为您选择的所有客户端计算机禁用网络威胁防护。
	您也可以从此日志清除受感染计算机状态。

日志类型	内容和操作
网络威胁防护	网络威胁防护日志包含有关对防火墙和入侵防护攻击的信息。可用信息包括拒绝服务 攻击、端口扫描,以及对可执行文件进行的更改。其中还包含有关通过防火墙的连接 (通信)以及通过的数据包的信息。这些日志还包含对计算机进行的某些操作更改, 例如检测网络应用程序以及配置软件。可用信息包括时间、事件类型和采取的操作等 条目。其他可用信息包括严重性、方向、主机名、采取的操作、IP 地址,以及相关协 议。 下列网络威胁防护日志可供使用: ■ 攻击
	<ul> <li>通信</li> <li>数据包</li> </ul>
	这些日志没有任何关联的操作。
TruScan 主动型威胁扫描	企业通过 TruScan 主动型威胁扫描日志包括主动型威胁扫描期间所检测到的威胁的相关信息。TruScan 主动型威胁扫描会使用启发式扫描查找与病毒和安全风险行为类似的任何行为。此方法可检测未知病毒和安全风险。可用信息包括发生时间、事件名称、相关计算机和用户、应用程序名称和类型以及文件名等条目。
	您可以从此日志,将检测到的进程添加到先前存在的集中式例外策略。
风险	风险日志包含有关风险事件的信息。可用的部分信息包括事件名称和时间、用户名、 计算机、风险名称、计数、源和路径名。 您可以从此日志采取下列操作:
	<ul> <li>将风险添加至集中式例外策略</li> <li>将文件添加至集中式例外策略</li> <li>将文件夹添加至集中式例外策略</li> <li>将扩展名添加至集中式例外策略</li> <li>从隔离区删除</li> </ul>
扫描	扫描日志包含有关防病毒和防间谍软件扫描活动的信息。其中提供的信息包括计算机 名、IP 地址、状态、扫描时间、持续时间和扫描结果等项目。 这些日志没有任何关联的操作。
系统	<ul> <li>系统日志包含有关事件的信息,例如服务何时启动和停止。可用信息包括事件时间和 事件类型、站点、域、相关服务器和严重性等条目。</li> <li>有以下系统日志可供使用:</li> <li>管理</li> <li>客户端服务器活动</li> <li>服务器活动</li> <li>客户端活动</li> <li>Enforcer 活动</li> </ul>
	这些日志仅有忙凹大��的探作。

日志类型	内容和操作
命令状态列表	命令状态列表包含有关您已从控制台运行的命令状态的信息。其中的信息包括运行命 令的日期、命令由谁发出,以及命令的说明。其中还包括命令的完成状态,以及命令 影响的客户端。
通知列表	通知列表包含有关通知事件的信息。这类事件包括通知的日期和时间等信息。还包括 通知是否已确认、通知由谁创建,通知主题和消息。
	这些日志没有任何关联的操作。
	<b>注意:</b> 通知日志从"监视器"页的"通知"选项卡访问,而不是从"日志"选项卡访问。
	请参见第179页的"查看和过滤管理员通知信息"。

## 使用监视器摘要选项卡

"监视器"页面上的"摘要"选项卡显示有关重要日志数据的精简摘要,让您立刻 就能了解安全状态。

您可以在"摘要"选项卡上查看下列摘要:

- 防病毒和防间谍软件防护
- 网络威胁防护
- 遵从性
- 站点状态

表11-2列出了摘要视图的内容。

表11-2 摘要视图及其内容	
摘要视图	目录
防病毒	防病毒视图包括下列信息:     TruScan 主动型威胁     风险分布     新风险     按源显示风险分布     按攻击者显示风险分布     按组显示风险分布
	<b>注意</b> :新风险是从上次数据库清除之后开始计算的,计算的时间段以在"首选项"的"主页和监视器"选项卡上配置的时间为准。 请参见第 132 页的"关于主页和监视器显示选项"。 例如,假设您的"首选项"时间范围设置为默认值,即过去 24小时。此外还假设您的数据库设置为在每周日晚间进行清除,并删除三天之前的旧风险。如果特定病毒在周一感染网络中的计算机,即会报告为新风险。如果另一台计算机在周 三感染了相同的病毒,则不会计算在内。如果相同的病毒在 下周一又感染网络中的一台计算机,则会报告为新风险。原 因是感染发生在过去24小时内,且数据库在周日清除了三天 前的旧风险条目。上次的风险检测发生在三天之前,因此已 从数据库删除。
网络威胁防护	<ul> <li>"网络威胁防护"视图包括下列信息:</li> <li>按组列出首要遭攻击目标</li> <li>攻击事件类型</li> <li>首要攻击源</li> <li>按严重性显示安全事件</li> </ul>
遵从性	<ul> <li>"遵从性"视图包括下列信息:</li> <li>■ 网络遵从性状态为失败</li> <li>■ 遵从性状态分布</li> <li>■ 遵从性失败的客户摘要</li> <li>■ 遵从性失败详细信息</li> <li>注意:如果您未安装 Symantec Network Access Control,</li> <li>"遵从性"视图不会包括任何数据。</li> </ul>

摘要视图	目录
站点状态	"站点状态"视图包括下列信息:
	■ 站点状态
	■ 按服务器显示前几个错误生成器
	■ 按客户端显示前几个错误生成器
	■ 某段时间内的复制失败
	■ 按 Enforcer 显示前几个错误生成器
	<b>注意</b> :如果您未安装 Symantec Network Access Control, "按 Enforcer 显示前几个错误生成器"视图不会包括任何数据。

如果仅安装了 Symantec Network Access Control,应该注意下列信息:

- 表11-2 中描述的"遵从性"视图包括您的主页。
- "站点状态"是"摘要"选项卡上唯一可用的视图。

您可以在"摘要"选项卡视图中单击任何饼图来查看更多详细信息。对于"网络威胁防护"下的各类"首要遭攻击目标"摘要,则可使用列表框查看按照组、子网、客户端或端口分类的摘要。

**注意**:如果仅安装了 Symantec Endpoint Protection, "遵从性"摘要视图中的图 表会是空的。如果仅安装了 Symantec Network Access Control, "摘要"选项卡 会仅包括"站点状态"视图。您可以在主页上查看"遵从性"摘要信息。

#### 更改摘要类型

- 1 在主窗口中,单击"监视器"。
- **2** 在"摘要"选项卡最上方的"摘要"类型列表框中,选择您想要查看的视图类型。

## 查看日志

可以根据所选的一系列过滤器设置从日志生成要查看的事件列表。每种日志类型和 内容类型都有您可以直接使用或者进行修改的默认过滤器配置。也可以创建并保存 新的过滤器配置。可以基于默认过滤器或之前创建的现有过滤器来创建新的过滤 器。如果保存了此过滤器配置,便可以在日后生成同样的日志视图,而不需每次都 配置设置。您可以删除不再需要的自定义过滤器配置。

请参见第170页的"保存和删除过滤器"。

**注意**: 在您查看含大量数据的日志时,如出现数据库错误,那么您可能要更改数据 库超时参数。

请参见第 255 页的"更改超时参数"。

如果收到 CGI 或终止进程错误,您最好更改其他超时参数。

如需其他超时参数的相关信息,请参见 Symantec 知识库中标题为 Reporting server does not report or shows a timeout error message when querying large amounts of data 的文章。

由于日志所包括的部分信息是定期收集而来,因此您可以刷新日志视图。若要配置 日志刷新频率,请显示该日志,然后从该日志视图右上方的"自动刷新"列表框中 选择所需选项。

**注意**:如果是使用特定日期来查看日志数据,则"自动刷新"会失去作用。其数据 始终不会发生变化。

如需每个可配置选项的说明,可在 Symantec Endpoint Protection Manager 控制 台上单击该报告类型的"更多信息"链接。"更多信息"会显示上下文关联帮助。

**注意**: 接受通配符和搜索匹配条目的过滤器选项字段不区分大小写。ASCII 星号字符是唯一可用作通配符的星号字符。

#### 查看日志

- 1 在主窗口中,单击"监视器"。
- 2 在"日志"选项卡的"日志类型"列表框中,选择您要查看的日志类型。
- 3 对于某些类型的日志,会显示"日志内容"列表框。如果显示此框,请选择您 要查看的日志内容。
- 4 在"使用保存的过滤器"列表框中,选择一个已保存的过滤器,或保留"默认"值。
- 5 从"时间范围"列表框中选择时间,或保留默认值。如果您选择"设置特定日 期",请设置您要显示哪个或哪些日期和时间之后的条目。
- 6 单击"高级设置"以限制显示的条目数。 您也可以针对所洗的日志类型设置任何其他可用的"高级设置"。
- 7 在您设好所要的视图配置后,请单击"查看日志"。 日志视图会出现在同一窗口中。

## 显示日志中的事件详细信息

您可以显示存储在日志中的事件的详细信息。

#### 显示事件详细信息

- 1 在主窗口中,单击"监视器"。
- 2 在"日志"选项卡的"日志类型"列表框中,选择您要查看的日志类型。
- **3** 对于某些类型的日志,会显示"日志内容"列表框。如果显示此框,请选择您 要查看的日志内容。
- **4** 单击"查看日志"。
- 5 单击您要查看其详细信息的事件,然后单击"详细信息"。

## 查看其他站点的日志

如果想要查看其他站点的日志,则必须从 Symantec Endpoint Protection Manager 控制台登录到位于远程站点的服务器。如果您拥有远程站点服务器的帐户,则可以 进行远程登录并查看该站点的日志。

如果您已配置复制伙伴,则可以选择将所有日志从复制伙伴复制到本地伙伴,反之 亦然。

请参见第264页的"复制日志"。

如果您选择复制日志,在默认情况下,当您查看任何日志时,会同时看见您的站点 与复制站点的信息。如果您想要看见单个站点,则必须过滤数据,将其限制在您想 要查看的位置。

**注意**:如果您选择复制日志,请确定您有充足的磁盘空间可以存储所有复制伙伴的 其他日志。

#### 查看其他站点的日志

- **1** 打开 Web 浏览器。
- 2 如下所示, 在地址文本框中键入服务器名称或 IP 地址以及端口号 9090:

#### http://192.168.1.100:9090

控制台开始下载。您登录的计算机必须已安装 Java 2 Runtime Environment (JRE)。如果没有,您会收到下载和安装提示。按照提示安装 JRE。

请参见第 26 页的"登录 Symantec Endpoint Protection Manager 控制台"。

3 在控制台登录对话框中,键入您的用户名和密码。

4 如果"服务器"文本框没有自动填写,则在其中键入服务器名称或IP地址以及端口号8443,如下所示:

http://192.168.1.100:8443

5 单击"登录"。

## 保存和删除过滤器

您可以使用"基本设置"和"高级设置"建构自定义过滤器,以更改所要查看的信息。您可以将自己的过滤器设置保存到数据库,以便日后再次生成同样的视图。保存设置时,设置会保存到数据库中。您提供给过滤器的名称会显示在适用于该类型日志和报告的"使用保存的过滤器"列表框中。

**注意**:如果您选择"过去24小时"作为日志过滤器的时间范围,则此24小时的时间范围会从您首次选择过滤器时开始算起。如果您刷新页面,并不会重置此24小时范围的开始时间。如果您先选择过滤器,然后等待查看日志,那么此时间范围也会从您选择过滤器时开始算起,而不是从您查看日志时开始算起。

如果您要确定此过去 24 小时时间范围是从现在开始算起,请先选择另一个时间范围,然后重新选择"过去 24 小时"。

#### 保存过滤器

- 1 在主窗口中,单击"监视器"。
- 2 在"日志"选项卡的"日志类型"列表框中,选择您要为其配置过滤器的日志 视图类型。
- 3 对于某些类型的日志,会显示"日志内容"列表框。如果显示此框,请选择您 要为其配置过滤器的日志内容。
- **4** 在"使用保存的过滤器"列表框中,选择您要从其开始设置的过滤器。例如, 选择默认过滤器。
- 5 在"您要使用何种过滤器设置"下方,单击"高级设置"。
- 6 更改任何设置。
- 7 单击"保存过滤器"。
- 8 在显示的对话框中,请在"过滤器名称"框中,键入您要用于此日志过滤器配置的名称。当保存后的过滤器添加到过滤器列表后,只会显示该名称的前 32 个字符。
- 9 单击"确定",新的过滤器名称便会添加到"使用保存的过滤器"列表框中。
- 10 在确认对话框显示时单击"确定"。

#### 删除保存的过滤器

- 1 在"使用保存的过滤器"列表框中,选择要删除的日志过滤器的名称。
- 2 在"使用保存的过滤器"列表框旁,单击"删除"图标。
- 3 出现请您确认是否要删除此过滤器的提示时,单击"是"。

## 关于重复的过滤器名称

过滤器存储部分由创建者决定,因此当两个用户创建同名过滤器时,并不会发生问题。但是,如果单个用户或两个用户以默认的admin帐户登录,则不应该创建同名过滤器。

如果用户创建同名过滤器,则在以下两种情况下会发生冲突:

- 两个用户在不同的站点上都以默认的 admin 帐户登录,且两个用户创建了同名 过滤器。
- 一个用户在创建过滤器后又登录其他站点并紧接着创建了相同名称的过滤器。

如果在站点复制之前出现了任一种情况,则用户随后会在过滤器列表中看到两个同 名的过滤器。只有一个过滤器可供使用。当出现此问题时,最佳做法是删除可用过 滤器,然后以其他名称重新创建。删除可用过滤器时,不可用的过滤器也会随之删 除。

## 日志的基本过滤设置

大多数日志有相同的基本设置。

表11-3说明大多数日志常用的基本设置。

表11-3 日志的基本设置

日志类型 指定要查看的日志类型。 从下列类型中进行选择: ■ 应用程序与设备控制 ■ 审核	说明	设置
<ul> <li>遵从性</li> <li>计算机状态</li> <li>网络威胁防护</li> <li>TruScan 主动型威胁扫描</li> <li>风险</li> <li>扫描</li> </ul>	指定要查看的日志类型。 从下列类型中进行选择: 回应用程序与设备控制 同核 可接 可接 以性 计算机状态 网络威胁防护 TruScan 主动型威胁扫描 风险 目描	日志类型

设置	说明
日志内容	如果有多个该类型的日志,则可以选择要查看的日志内容类型。
使用保存的过滤器	指定您要用来创建日志视图的过滤器。 可以使用默认过滤器或已命名并保存的自定义过滤器来查看 日志信息。
时间范围	指定您要在日志中查看的事件的时间范围。 请从下列时间中进行选择: <ul> <li>过去 24 小时</li> <li>过去一周</li> <li>过去一个月</li> <li>当前的月份</li> <li>过去三个月</li> <li>过去一年</li> <li>设置特定日期</li> </ul>
高级设置	每个日志都有一些特定的高级设置。单击"高级设置"和"基本设置",即可在两者之间切换。

## 日志的高级过滤器设置

高级设置可帮助您更好地控制要查看的数据。高级设置针对日志类型和内容。 如果网络中有计算机正在运行旧版 Symantec AntiVirus,则您在使用日志过滤器 时,可应用下列术语:

- 旧版服务器组按域分类
- 旧版客户端组按组分类
- 旧版父服务器按服务器分类

**注意:**您不能过滤 Symantec Client Firewall 有关入侵防护特征的旧版数据。若要 查看计算机上运行的特征版本,您可以转至计算机状态日志。选择一台安装有 Symantec Client Firewall 的计算机,然后单击"详细信息"。IDS 版本字段包含此 信息。

有关每个可配置选项的说明,您可以在 Symantec Endpoint Protection Manager 控制台上单击该类型日志的"更多信息"。"更多信息"会显示上下文关联帮助。

## 从日志运行命令和操作

您可以从计算机状态日志对选定客户端运行若干命令。

您也可以直接从 Symantec Endpoint Protection Manager 控制台的"客户端"页 面右键单击一个组来运行命令。命令和操作在客户端上的处理顺序因命令而异。无 论命令是从什么地方发出的,命令和操作的处理方式都是相同的。

如需有关运行命令时可设置选项的信息,您可以在控制台中的"日志"选项卡上单击"更多信息"查看。"更多信息"显示上下文相关帮助。

您可以从"命令状态"选项卡查看您从控制台运行的命令的状态及其详细信息。您 还可以从此选项卡取消正在运行的特定扫描。

您可以从计算机状态日志取消所有正在运行的扫描以及已经排在所选客户端的队列 中的扫描。如果您确认了此命令,表会刷新,然后您会看见取消命令已添加到命令 状态表中。

**注意**:如果您运行扫描命令,并选择"自定义扫描",则扫描会使用您在"管理员 定义的扫描"页面上配置的命令扫描设置。命令使用的是应用于所选客户端的防病 毒和防间谍软件策略中的设置。

如果您从日志运行"重新启动客户端计算机"命令,则该命令会立即发送。如果用 户登录到客户端,就会看到重新启动警告,该警告基于管理员为该客户端配置的重 新启动选项。您可以在"客户端"页面的"策略"选项卡中的"常规设置"对话框 的"常规设置"选项卡中配置客户端重新启动选项。

下列日志可允许您向集中式例外策略添加例外:

- 应用程序控制日志
- TruScan 主动型威胁扫描日志
- 风险日志

请参见第 471 页的"从日志事件创建集中式例外"。

若要从日志添加任何类型的例外,您必须已创建集中式例外策略。

请参见第465页的"配置集中式例外策略"。

您也可以从风险日志删除隔离区内的文件。

如果 Symantec Endpoint Protection 在压缩文件中检测到风险,则将隔离整个压缩 文件。然而,对于压缩文件中的每个文件,风险日志都会包含一个单独的条目。您 不能通过从风险日志使用"从隔离区删除"命令仅删除隔离区内受感染的文件。若 要成功删除风险,您必须在使用"从隔离区删除"命令之前,选择压缩文件中的所 有文件。 **注意**:若要选择压缩文件中的文件,您必须在日志视图中显示所有文件。您可以使用风险日志过滤器的"高级设置"中的"限制"选项来增加视图中的条目数。

#### 从风险日志删除隔离区中的文件

- 1 单击"监视器"。
- 2 在"日志"选项卡的"日志类型"列表框中选择"风险日志",然后单击"查 看日志"。
- 3 在日志中选择一个文件被隔离的条目。
- 4 从"操作"列表框中选择"从隔离区删除"。
- 5 单击"开始"。
- 6 在显示的对话框中,单击"删除"。
- 7 在显示的确认对话框中单击"确定"。

#### 从风险日志删除隔离区中的压缩文件

- 1 单击"监视器"。
- 2 在"日志"选项卡的"日志类型"列表框中选择"风险日志",然后单击"查 看日志"。
- 3 选择与压缩文件中所有的文件相关的条目。

您必须将压缩文件中的所有条目显示于日志视图中。您可以使用"高级设置" 下的"限制"选项来增加视图的条目数。

- 4 从"操作"列表框中选择"从隔离区删除"。
- 5 单击"开始"。
- 6 在显示的对话框中,单击"删除"。
- 7 在显示的确认对话框中单击"确定"。

#### 从计算机状态日志运行命令

- 1 单击"监视器"。
- 2 在"日志"选项卡的"日志类型"列表框中选择"计算机状态"。
- 3 单击"查看日志"。
- 4 从"操作"列表框选择一个命令。
- 5 单击"开始"。

如果您选择的命令有设置选项,则将显示一个新页面,您可以在此配置适当的 设置。

6 完成配置后,请单击"是"或"确定"。

- 7 在显示的命令确认消息框中,单击"是"。
- 8 在"消息"对话框中,单击"确定"。

如果命令未成功进入队列,您可能需要重复此过程。您可以检查服务器是否关闭。如果控制台已失去与服务器的连接,您可以注销控制台然后再重新登录来 看看是否有帮助。

#### 查看命令状态详细信息

- 1 单击"监视器"。
- 2 在"命令状态"选项卡上,从列表中选择一个命令,然后单击"详细信息"。

#### 取消正在运行的特定扫描

- 1 单击"监视器"。
- 2 在"命令状态"选项卡上,在您要取消的扫描命令的"命令"列中,单击"取 消扫描"图标。
- 3 当显示命令已成功进入队列的确认消息时,单击"确定"。

#### 取消所有正在运行的扫描和排在队列中的扫描

- 1 单击"监视器"。
- 2 在"日志"选项卡的"日志类型"列表框中选择"计算机状态"。
- 3 单击"查看日志"。
- 4 选择列表中的一台或多台计算机,然后从命令列表中选择"取消所有扫描"。
- 5 单击"开始"。
- 6 当确认对话框显示时,单击"是"以取消所选计算机的所有进行中的和排在队 列中的扫描。
- 7 当显示命令已成功进入队列的确认消息时,单击"确定"。

## 关于减少发送至日志的事件量

您可以通过配置日志处理参数来减少发送至防病毒和防间谍软件日志的事件数目。 可从"防病毒和防间谍软件策略"针对每个策略配置这些选项。

请参见第 327 页的"在防病毒和防间谍软件策略中设置日志处理参数"。

## 导出日志数据

导出日志数据的方式有数种。您可以将某些日志中的数据导出到逗号分隔的文本文件。您可以将其他日志的数据导出到 Tab 分隔的文本文件(称为转储文件),也可以将其导出到 Syslog 服务器。如果您要在集中的位置存放整个网络的所有日志,日

志数据导出将非常有用。如果您要使用第三方程序(如电子表格)组织或操作数据,日志数据导出也非常有用。您也可能想在删除日志记录之前,先导出日志数据。

将日志数据导出到 Syslog 服务器时,您必须配置 Syslog 服务器来接收这些日志。 若要将日志转发至第三方程序,您需要安装该第三方程序且连接至网络。例如,您 可以使用 Microsoft Excel 打开导出的日志文件。每个字段会显示在一个单独的列 中,每行对应一个单独的日志记录。

注意:您不能使用导出的日志数据还原数据库。

## 将日志数据导出到文本文件

将数据从日志导出到文本文件时,默认情况下,文件会置于 *drive*:\Program Files\ Symantec\Symantec Endpoint Protection Manager\data\dump 文件夹中。条目 会置于.tmp 文件中,直到所有记录都传输到文本文件为止。

如果您未安装 Symantec Network Access Control,则某些日志会不存在。

表11-4显示日志数据类型与导出的日志数据文件名的对应关系。

日志数据	文本文件名
服务器管理	scm_admin.log
服务器应用程序控制	agt_behavior.log
服务器客户端	scm_agent_act.log
服务器策略	scm_policy.log
服务器系统	scm_system.log
客户端数据包	agt_packet.log
客户端主动型威胁	agt_proactive.log
客户端风险	agt_risk.log
客户端扫描	agt_scan.log
客户端安全	agt_security.log
客户端系统	agt_system.log
客户端通信	agt_traffic.log

表 11-4 Symantec Endpoint Protection 的日志文本文件名

**注意:** 表11-4中的日志名称并非与"监视器"页面的"日志"选项卡上使用的日志 名称一一对应。

表11-5显示日志数据类型与 Enforcer 日志的导出日志数据文件名的对应关系。

表 11-5 Symantec Network Access Control 的更多日志文本文件名

日志数据	文本文件名
服务器 Enforcer 活动	scm_enforcer_act.log
Enforcer 客户端活动	enf_client_act.log
Enforcer 系统	enf_system.log
Enforcer 通信	enf_traffic.log

**注意**:导出到文本文件时,导出记录的数量可能与您在"外部日志"对话框中设置的数量不同。重新启动管理服务器时,会发生这种情况。重新启动管理服务器后, 日志条目计数会重置为0,而临时日志文件中可能已经有条目。在这种情况下,重 新启动后生成的每种类型的第一个\*.log文件包含的条目会多于指定值。后续导出 的任何日志文件则会包含正确数量的条目。

有关以下步骤中可设置选项的详细信息,您可以在 Symantec Endpoint Protection Manager 控制台上单击"帮助",以获取"常规"选项卡的说明。

#### 将日志数据导出到转储文件

- 1 在控制台中,单击"管理员"。
- 2 单击"服务器"。
- 3 单击要配置外部日志的本地站点或远程站点。
- 4 单击"配置外部日志"。
- 5 在"常规"选项卡上,选择将日志数据发送到文件的频率。
- 6 选择要处理外部日志的主日志服务器。

如果您使用的是 Microsoft SQL, 且有多个管理服务器连接至数据库,则只需要一台服务器作为主日志服务器。

- 7 选中"将日志导出到转储文件"。
- 8 若有必要,选中"限制转储文件记录",并键入您要一次发送到文本文件的条 目数。

- 9 在"日志过滤器"选项卡上,选择要发送到文本文件的所有日志。 如果您所选日志类型可选择严重性等级,您必须选中要保存的严重性等级。您 选择的所有等级都会保存。
- 10 单击"确定"。

#### 将数据导出到 Syslog 服务器

您可以配置 Symantec Endpoint Protection,将某些日志的日志数据发送到 Syslog 服务器。

注意:请记住配置 Syslog 服务器来接收日志数据。

有关以下步骤中可设置选项的详细信息,您可以在 Symantec Endpoint Protection Manager 控制台上单击"帮助",以获取"常规"选项卡的说明。

#### 将日志数据导出到 Syslog 服务器

- 1 在控制台中,单击"管理员"。
- 2 单击"服务器"。
- 3 单击您要导出日志数据的本地站点或远程站点。
- 4 单击"配置外部日志"。
- 5 在"常规"选项卡上,选择将日志数据发送到文件的频率。
- 6 选择要处理外部日志的服务器。

如果您使用的是 Microsoft SQL, 且有多个管理服务器连接到数据库,则只需要一个服务器作为主日志服务器。

- 7 选中"对 Syslog 服务器启用日志传送"。
- 8 根据需要配置下列字段:
  - Syslog 服务器:
     键入您要接收日志数据的 Syslog 服务器的 IP 地址或域名。
  - UDP 目标端口: 键入 Syslog 服务器用来侦听 Syslog 消息的目标端口,或者使用默认值。
  - 日志工具: 键入您要用于 Syslog 配置文件的日志工具数目,或者使用默认值。有效值 的范围为 0 到 23。
- **9** 在"日志过滤器"选项卡上,选择要发送到文本文件的所有日志。如果您所选 日志类型可选择严重性等级,请选中要保存的严重性等级。

10 单击"确定"。

## 将日志数据导出为逗号分隔文本文件

您可以将日志中的数据导出为逗号分隔文本文件。

#### 将日志导出为逗号分隔文本文件

- 1 在控制台中,单击"监视器"。
- 2 在"日志"选项卡上,选择您要导出的日志。
- 3 更改任何"基本设置"或"高级设置"。
- **4** 单击"查看日志"。
- 5 单击"导出"。
- 6 在显示的新窗口中, 单击"**文件**"菜单, 然后单击"另存为"。
- 7 如果提示您继续操作,请单击"是"。
- 8 在出现的"保存网页"窗口中,使用"保存位置"列表框浏览至您要将此文件 保存到的目录。
- 9 在"文件名"文本框中,键入要使用的文件名。
- 10 若要保存原始数据,请在"另存类型"列表框中,将类型更改为"文本文件 (\*.txt)"。
- 11 单击"保存"即可将数据即导出至文件。

## 使用通知

通知是指网络中发生的安全事件的相关消息。您可以配置进行多种不同类型的通知。通知中部分针对用户,部分针对管理员。

您可以配置下列通知操作,以在满足多种不同的与安全相关的条件时向管理员或其他指定用户发出警报:

- 发送电子邮件。
- 运行批处理文件或其他可执行文件。
- 在数据库中的通知日志中记录条目。

请参见第180页的"创建管理员通知"。

## 查看和过滤管理员通知信息

您能够以查看其他日志中信息的相同方式来查看通知日志中的信息。您可以过滤通 知日志,以一次只查看单个类型通知事件的相关信息。您可以过滤通知视图并保存 过滤器以供日后使用。

您可以根据下列条件过滤日志中的通知:

- 时间范围
- 确认状态
- 类型
- 创建者
- ∎ 名称

#### 查看所有通知

- 1 在控制台中,单击"监视器"。
- 在"通知"选项卡上,单击"查看通知"。
   所有类型的通知列表随即出现。

#### 过滤通知视图

- 1 在控制台中,单击"监视器"。
- 2 在"通知"选项卡的"您要使用何种过滤器设置"下,单击"高级设置"。
- 3 设置任何用以过滤的选项。

您可以使用时间范围、确认状态、通知类型、创建者或特定通知名称的任意组 合进行过滤。

**4** 单击"查看通知"。

所选类型通知的列表随即出现。

## 用于管理员通知的阈值指南

当您在配置通知类型时,某些类型会包括默认值。这些指南会根据您环境的大小提供合理的起点设置,但还可能需要另行调整。可能需要经过测试以及出错之后,才能在过多与过少通知之间找出最适合您环境的平衡点。将阈值设置为一个初始限制值,然后试行几天。看看您收到的通知是否过少,或者通知是否过多以致对您或您的网络造成困扰。

以病毒、安全风险和防火墙事件检测为例,假设您网络中的计算机数目少于100 台。此网络的合理阈值是如果在一分钟内检测到两个风险事件则配置一个通知。如 果您有100到1000台计算机,合理的阈值是在一分钟内检测五个风险事件。

您可能也想要在客户端的定义文件过期时收到警报。您可能想在各客户端的定义文件过期超过两天以上时收到通知。

## 创建管理员通知

您可以创建和配置在发生某些安全相关事件时触发的通知。

您可以配置软件采取下列通知操作:
- 将通知记录到数据库。
- 向个人发送电子邮件。

**注意**:若要发送电子邮件通知,您还必须配置邮件服务器。若要配置邮件服务器,请单击"管理员">"服务器"页面,选择一个服务器,然后单击"编辑服务器属性",再单击"邮件服务器"选项卡。

■ 运行批处理文件或其他可执行文件。

通知的默认调节器时间段是"自动"。如果触发了通知,并且触发条件继续存在,则在 60 分钟内不会再次执行您配置的通知操作。例如,假设您将通知设置为当病毒在一小时内感染五台计算机时以电子邮件方式获得通知。如果病毒继续以此速率或高于此速率感染您的计算机,则 Symantec Endpoint Protection 会每小时向您发送一次电子邮件。在感染速率变为低于每小时五台计算机之前,都会持续发送电子邮件。

您可以将软件配置为在发生多种不同类型的事件时通知您。

表11-6说明了将触发不同类型通知的不同类型事件。

通知	说明
验证失败	登录失败会触发此类型通知。您可设置要触发通知的登录失败次数和时间段。Symantec Endpoint Protection 会在该时间段内发生的登录失败次数超过您的设置值时通知您。它会报告发生的登录失败次数。
客户端列表更改	客户端更改会触发此类型通知。可触发此通知的更改类 型包括客户端的增加、移动、名称更改或删除。客户端 的非受管检测器状态、客户端模式或硬件更改也可能会 触发此通知。
客户端安全警报	您可以在遵从性、网络威胁防护、通信、数据包、设备 控制和应用程序控制安全事件中进行选择。您还可以选 择应该触发此通知的爆发类型和程度以及时间段。类型 包括发生于任何计算机上、发生于单台计算机上或发生 于多台计算机上。部分这些类型需要您同时在关联的策 略中启用日志记录。
Enforcer 关闭	如Enforcer设备脱机, 会触发此类型通知。将通知您每 个Enforcer的名称、其组以及其上次状态持续的时间。
检测到强制性或商业应用程序	当检测到存在于"商业应用程序列表"或管理员监视应 用程序列表中的应用程序时,将触发此通知。

表11-6 通知类型

通知	说明
新发现的应用程序	如发现新的应用程序, 会触发此类型通知。
检测到的新风险	如发现新的风险, 会触发此类型通知。
新软件包	如发现新的软件包下载, 会触发此类型通知。
风险爆发	可设置应触发此类型通知的新风险出现次数和类型以及 时间段。类型包括发生于任何计算机上、发生于单台计 算机上或发生于多台计算机上。
服务器运行状况	服务器运行状态(脱机、差或重要)会触发此通知。通 知中将列出服务器名称、运行状态、原因和上次状态。
单个风险事件	检测到单个风险事件时会触发此通知。通知会列出关于 风险的详细信息,包括相关用户和计算机以及 Symantec Endpoint Protection 采取的操作。
系统事件	诸如服务器和Enforcer活动、复制失败、备份和还原问题以及系统错误之类的系统事件会触发此通知。通知会列出检测到的此类事件的数目。
不受管理的计算机	如发现不受管理的计算机,会触发此通知。通知会列出 详细信息,例如每台计算机的 IP 地址、MAC 地址和操 作系统。
病毒定义过时	您可在设置通知时定义过期时间,并设置要触发此通知 而必须达到的计算机数目和计算机定义的已存在天数。

使用"通知条件"设置,您可以根据发生于任何计算机上、发生于单台计算机上或 发生于多台计算机上这三种类型来配置客户端安全警报。您还可以针对风险爆发配 置这些选项。

您最好创建一个"网络威胁防护"通知,此通知将在某通信事件匹配为防火墙规则 设置的条件时触发。

若要创建此类型通知,您必须执行下列任务:

- 在"防火墙策略规则"列表中,在您想要获取通知的规则的"记录"列中选中 "发送电子邮件警报"选项。
- 在"通知"选项卡上,配置网络威胁防护、数据包或通信事件的客户端安全警报。

请参见第 412 页的"配置网络威胁防护的通知"。

若要了解每个可配置选项的说明,可在 Symantec Endpoint Protection Manager 控制台上单击"更多信息"。"更多信息"会显示上下文关联帮助。

**注意:**您可以通过"显示通知类型"列表框过滤您创建的通知条件视图。要确保所 创建的新通知都能显示出来,请务必选中此列表框中的"所有"选项。

#### 创建通知

- 1 在控制台中,单击"监视器"。
- 2 在"通知"选项卡上,单击"通知条件"。
- 3 单击"添加",然后从显示的列表中选择您要添加的通知类型。
- 4 在显示的新窗口的"通知名称"文本框中,键入一个说明性名称。
- 5 指定您需要的过滤器选项。例如,对于某些类型的通知,可以将通知限制在特定的域、组、服务器、计算机、风险或应用程序范围内。
- 6 指定通知设置以及通知触发时要采取的操作。您可以单击"帮助"来查看所有 通知类型可用选项的说明。

如果您选择"发送电子邮件到"作为采取的操作,则电子邮件通知将取决于邮件服务器的用户名选项。通过"服务器属性"对话框为邮件服务器配置的用户 名必须符合以下格式: user@domain。如果此字段为空,通知会从 SYSTEM@computer name发送。如果报告服务器具有使用全角字符集(DBCS) 字符的名称,则您为用户名字段指定的电子邮件帐户名称必须符合以下格式: user@domain。

如果您选择"运行批处理文件或可执行文件"作为采取的操作,请键入相应文件的名称。不允许键入路径名称。要运行的批处理文件或可执行文件必须位于下面的目录:

drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\bin

7 单击"确定"。

#### 创建网络威胁防护通知

- 1 在控制台中,单击"监视器"。
- 2 在"通知"选项卡上,单击"通知条件"。
- 3 单击"添加",然后选择"客户端安全警报"。
- 4 键入此通知的名称。
- 5 如果您要将通知限制在特定的域、组、服务器、计算机范围内,请指定您需要的过滤器选项。
- 6 选择下列爆发类型之一:
  - 发生于多台计算机上
  - 发生于任何计算机上
  - 发生于单台计算机上

- 7 若要指定"网络威胁防护"活动的类型,请选中下列复选框之一:
  - 对于防火墙或入侵防护特征检测到的攻击和事件,请选中"网络威胁防护 事件"。
  - 对于已触发并记录在数据包日志中的防火墙规则,请选中"数据包事件"。
  - 对于已触发并记录在通信日志中的防火墙规则,请选中"通信事件"。
- 8 如有需要,可通过更改默认通知条件设置希望在多少分钟内发生多少次风险时 触发此通知。
- **9** 选中"发送电子邮件到",然后键入在满足条件时要通知的人员的电子邮件地址。
- 10 单击"确定"。

现在可以使用"防火墙策略规则"列表的"记录"列中的"发送电子邮件警报"选项。当此通知触发时,即发送电子邮件。

请参见第 413 页的"配置通信事件的电子邮件"。

### 关于编辑现有通知

如果您编辑现有通知的设置,其先前生成的条目会根据您的新设置在通知日志中显示消息。如果您要在通知日志视图中保留以前的通知消息,请勿编辑现有通知的设置,而是以新名称创建新通知。然后,取消选中您在"触发此通知时应该发生什么操作"下方所配置的操作,以此方式禁用现有通知。

# 使用监视器和报告来确保 网络安全

本章节包括下列主题:

- 关于使用监视器和报告来帮助确保网络安全
- 关于排除病毒和安全风险
- 查找脱机客户端

## 关于使用监视器和报告来帮助确保网络安全

报告会显示客户端和服务器的相关信息的静态快照,不过您可以调度报告使之定期 运行,以提供最新信息。从"监视器"页面访问的日志是动态的,并且会显示更具 体且更详细的信息,如计算机名和用户名。您可能需要这种详细程度的数据以准确 地确定某些问题。您可以从某些日志对组中的所有客户端运行命令,以便立即补救 问题。您可以从"命令状态"选项卡监控命令的状态。

您可以从"监视器"页面设置的通知能提供有关问题的警报。您可以使用通知触发 对问题的补救,方法是使其运行批处理文件或其他可执行文件。您可以设置在发生 特定事件或达到出现次数阈值时发出通知。

您可以使用许多不同的方式从日志和报告中获取相关信息。例如,假设您想知道网络中哪些计算机受到感染。主页会显示新感染和仍受感染的计算机数目。如果网络中发现安全问题,则当您登录Symantec Endpoint Protection Manager 控制台时,这些数目会立即让您获悉情况。

您可以使用许多不同的方式来查找有关这些计算机的更多详细信息。例如,您可以 执行下列操作:

■ 调度"受感染和有风险的计算机"快速报告使之在每天上午运行,并将其配置 为以电子邮件形式发送给自己或其他人。

#### 186 | 使用监视器和报告来确保网络安全 关于使用监视器和报告来帮助确保网络安全

- 创建一个"风险"报告过滤器,使之包含您所需的有关受感染计算机的具体详细信息,然后保存它。每当您在主页看到发生了安全问题时,就应使用该过滤器运行快速报告。您也可以创建一个使用此保存的过滤器的调度报告,以用来运行并通过电子邮件发送给您自己或其他人。
- 直接转至"风险"日志,查看感染事件。您可以使用默认过滤器或保存的过滤
   器来只显示您所需的详细信息。
- 如果需要,可自定义主页面以更改"报告收藏夹"部分中的默认报告。您可以 使用任何预定义的快速报告或使用自定义过滤器的报告。每次您查看这些报告 时它们都会运行,以便包含最新的信息。

无论您首选的方法如何,您可能都需要创建一些自定义报告和日志过滤器。您可以 定期使用自定义过滤器来监控或排除网络中的安全问题。若要自定义过滤器,您必 须先标识您要在报告或日志中查看的信息。例如,您可以运行报告以显示在一段特 定时间内感染您的网络的首要安全风险。假设您发现过去一周网络中的首要风险是 RPC.Attack,那么此报告会指出受感染的计算机数。然后您就可以使用"风险"日 志来显示受 RPC.Attack 感染的计算机的名称。"风险"日志还会显示受感染时登 录到那些计算机的用户名。

## 关于应用程序控制与设备控制报告和日志中的信息

应用程序控制与设备控制日志和报告包括有关下列事件类型的信息:

- 访问计算机实体遭到禁止
- 设备不能连接网络

计算机实体包括文件、注册表项和进程等。可用信息包括如时间和事件类型、采取 的操作、主机及涉及的规则等条目。此外,还包括涉及的调用者进程。这些日志和 报告包括有关应用程序与设备控制策略及防篡改的信息。

表12-1介绍了可从应用程序与设备控制报告和日志获取信息的常规用途。

报告或日志	常规用途
含警报次数最多的应用程序控制日 志的前几组	使用此报告可检查网络中哪些组存在的风险最严重。
首要已禁止目标	使用此报告可检查最常用来攻击您网络的是哪些文件、 进程及其他实体。
首要已禁止设备	使用此报告可找出从影响网络安全这一方面看最有问题 的设备。

#### 表 12-1 应用程序控制与设备控制快速报告和日志摘要

报告或日志	常规用途
应用程序控制日志	<ul> <li>使用此日志可查看有关下列实体的信息:</li> <li>● 针对事件所采取的操作</li> <li>● 事件所涉及的进程</li> <li>● 当应用程序访问遭禁止时从策略应用的规则名称</li> </ul>
设备控制日志	若您需要查看设备控制详细信息,如设备控制启用或禁 用设备的确切时间,请使用此日志。此日志还显示其他 信息,如计算机名、计算机位置、登录的用户以及涉及 的操作系统。

## 关于审核报告和日志中的信息

审核日志包括有关策略修改活动的信息,如事件时间和类型、策略修改、域、站 点、管理员以及说明。

默认审核快速报告称作"使用的策略"。可通过查看"使用的策略"报告来监控您 网络中正在按组使用的策略。如果您想要知道是哪个管理员更改了某个特定策略以 及更改发生在何时,您可以查看审核日志。

## 关于遵从性报告和日志中的信息

遵从性日志包括与Enforcer服务器、客户端、通信以及主机遵从性相关的信息。可用的信息包括时间和事件类型、涉及的Enforcer名称、站点和服务器等项。

**注意**:如果您未安装 Symantec Network Access Control, "遵从性"日志和报告 不会包含任何数据。

表12-2说明可从遵从性报告和日志中获取的信息的常规用途。

报告或日志	常规用途
网络遵从性状态	使用此报告可查看整体的遵从性情况,以此了解哪些客 户端没有通过主机完整性检查、没有通过验证或者已断 开。
遵从性状态	使用此报告可查看网络中已通过或未通过主机完整性检 查的客户端总计。
遵从性失败的客户摘要	使用此报告可查看控制失败事件(如防病毒、防火墙或 VPN)的常规原因。

表12-2 遵从性日志和快速报告摘要

报告或日志	常规用途
遵从性失败详细信息	使用此报告可查看有关遵从性失败的更详细信息。报告 会显示每个失败涉及的条件和规则。其中包括已部署客 户端的百分比以及部署失败的百分比。
	例如, "遵从性失败摘要"可能显示的是因防病毒软件 原因而失败的十个客户端。相比之下, "遵从性失败详 细信息"显示下列信息:
	<ul> <li>四个客户端当前未运行防病毒软件。</li> <li>西本名户端土尤其时后素软件。</li> </ul>
	<ul> <li>网门各户端木安装的病毒软件。</li> <li>四个客户端的防病毒定义已过期。</li> </ul>
按位置列出的不遵从客户端	使用此报告可查看是否某些位置的遵从性问题比其他位置多。
Enforcer 服务器日志	使用此日志可查看有关 Enforcer 遵从性事件、涉及的 Enforcer 名称、其站点和服务器的信息。
	此外,此日志还包括下列信息:
	■ 哪些 Enforcer 不能注册到其服务器
	■ 哪些 Enforcer 已成功接收下载的策略和 sylink.xml
	■ Enforcer 的服务器是否已成功接收 Enforcer 的日志
Enforcer 客户端日志	使用此日志可查看哪些客户端已通过或未通过主机完整 性检查、已通过或未通过验证,或者已与网络断开。
Enforcer 通信日志	使用此日志可查看有关通过 Enforcer 的通信的信息。
	可用信息包括:
	■ 通信的方向
	■ 通信开始和退出的时间 ● 使用的批判
	<ul> <li>● 使用的源 IP 地址和目标 IP 地址</li> </ul>
	■ 使用的端口
	■ 数据包大小(以字节为单位)
	■ 允许或禁止的连接尝试
	此日志仅适用于 Gateway Enforcer。
主机遵从性日志	使用此日志可查看有关特定遵从性事件的特定信息。这些事件包括原因、涉及的用户、涉及的操作系统名称。

## 关于计算机状态报告和日志中的信息

计算机状态日志包括有关网络中计算机实时运行状态的信息。可用的信息包括计算 机名和 IP 地址、上次登录时间、定义日期、感染状态、自动防护状态、服务器、 组、域和用户名。"计算机状态"报告的过滤器包括标准配置选项和特定于遵从性 的选项。

表12-3介绍了可从计算机状态报告和日志中获取的信息的常规用途。

报告或日志	常规用途
病毒定义分发	使用此报告可确定您网络中的所有组、域或服务器是否使用了最新的病毒定义文件版本。
未登入服务器的计算机	使用此报告可查找因尚未签入服务器而可能丢失或遗漏的计算机。
Symantec Endpoint Protection 产 品版本	使用此报告可检查您网络中使用的产品软件、病毒定 义、IPS 特征和主动型防护内容的版本。利用此信息您 可以确切找出需要更新的计算机。
人侵防护特征分布	使用此报告可确定您网络的所有组是否使用了最新的入 侵防护特征。您还可以查看哪些域或服务器已过期。
客户端清单	使用此报告可查看归入特定硬件和软件类别的计算机数 目和百分比。可用信息包括计算机的操作系统、总内 存、可用内存、总磁盘空间、可用磁盘空间和处理器类 型。例如,从"客户端清单"报告中,您也许会看到有 22%的计算机的可用磁盘空间低于1GB。
遵从性状态分布	使用此报告可查看哪些组或子网中不符合遵从性要求的 计算机所占比例最大。如果某些组的遵从性问题比其他 组多,您最好深入了解其中的原因所在。
客户端联机状态	使用此报告可查看哪些组或子网的在线客户端所占比例 最高。如果某些组或子网当前遭遇的问题比其他组或子 网多,您最好深入了解其中原因。
有最新策略的客户端	使用此报告可查看哪些组或子网未使用最新策略的计算机所占比例最大。
按组显示客户端计数	使用此报告可查看按组列出的客户端和用户总计。

表12-3 计算机状态快速报告和日志摘要

报告或日志	常规用途
安全状态摘要	使用此报告可快速查看发生下列问题的计算机总计:
	<ul> <li>自动防护已禁用</li> <li>防病毒引擎已关闭</li> <li>防篡改已关闭</li> <li>计算机需要重新启动</li> <li>计算机未通过主机完整性检查</li> <li>网络威胁防护已关闭</li> <li>如果您不采取适当措施,这些计算机可能继续存在风</li> </ul>
	险。 ————————————————————————————————————
防护内容版本	使用此报告可检查您网络中使用的主动型防护内容的版 本,以确切找出需要更新的计算机。
客户端迁移	使用此报告可查看按域、组和服务器列出的客户端的迁 移状态。您可以快速确定哪些客户端的迁移已失败或尚 未启动迁移。
某段时间内的联机/脱机客户端(快照)	使用此报告可确切找出网络连接频率不够的客户端。此 报告仅用作调度报告。
某段时间内有最新策略的客户端(快照)	使用此报告可确切找出策略更新频率不够的客户端。此 报告仅用作调度报告。
客户端软件分装(快照)	使用此报告可确切找出未部署最新软件版本的客户端。 此报告仅用作调度报告。
某段时间内的非遵从性客户端(快 照)	使用此报告可确切找出经常不能通过主机完整性检查的 客户端。此报告仅用作调度报告。
病毒定义分装 (快照)	使用此报告可检查客户端拥有的定义版本。此报告仅用作调度报告。
计算机状态日志	如需报告涵盖主题的更多详细信息,请检查"计算机状态"日志。

## 关于网络威胁防护报告和日志中的信息

网络威胁防护日志可用于跟踪计算机的活动及其与其他计算机和网络的交互情况。 它们记录有关试图通过网络连接进出计算机的通信的信息。

网络威胁防护日志包括针对防火墙的攻击的详细信息,如以下信息:

- 拒绝服务攻击
- ∎ 端口扫描

■ 对可执行文件的更改

网络威胁防护日志收集入侵防护的相关信息。此类日志还包括通过防火墙的连接 (通信)以及访问的注册表项、文件和DLL的相关信息,以及通过计算机的数据包 的相关信息。对计算机的操作更改也会记录在这些日志中。此类信息可能会包括服 务启动和停止的时间或软件被配置的时间。其他可能包括的信息类型还有如时间和 事件类型以及采取的操作等。此日志还可能包括涉及通信所使用的方向、主机名、 IP 地址和协议。若应用于事件,此类信息还会包括严重性等级。

表12-4介绍了可从网络威胁防护报告和日志中获取的信息的常规用途。

表12-4 网络威胁防护快速报告和日志摘要

报告或日志	常规用途
首要遭攻击目标	使用此报告可了解哪些组、子网、计算机或端口最常遭 受攻击。您最好根据此报告采取一定操作。例如,您可 能会发现通过VPN装上的客户端最常遭受攻击。您最好 将这些计算机归入一组,以便您应用更严格的安全策 略。
首要攻击源	使用此报告可确定哪些主机最常攻击您的网络。
首要攻击类型	使用此报告可确定最常攻击您网络的攻击类型。您可以 监控的可能攻击类型包括端口扫描、拒绝服务攻击和 MAC欺骗。
首要禁止的应用程序	可以合并使用这些报告来确定最常用来攻击您网络的应
某段时间内禁止的应用程序	用程序。您还可以查看用来攻击的这些应用程序是否已在某段时间内发生更改。
某段时间内的攻击	可以使用此报告确定您网络中最常遭受攻击的组、IP地址、操作系统和用户。还可使用它来确定最常发生的攻击类型。
按严重性显示安全事件	可以使用此报告查看您网络中安全事件的严重性摘要。
前几项通信通知	这些报告用于显示已违反您已配置为如有违反需要发送
某段时间内的通信通知	通知的防火墙规则的攻击的数目。在防火墙策略规则的 "记录"列中选中"发送电子邮件警报"选项,即可将 此数据配置为发送报告。使用"某段时间内的通信通 知"可查看这些攻击在某段时间的增减情况以及对其他 组的影响。使用它们可以看出哪些组最容易遭受经由防 火墙的攻击。
完整报告	使用此报告可以一并查看所有"网络威胁防护"快速报告中显示的信息。
通信日志	如需有关通过您防火墙的特定通信事件或通信类型的详 细信息,请使用此日志。

#### 192 | 使用监视器和报告来确保网络安全 关于使用监视器和报告来帮助确保网络安全

报告或日志	常规用途
数据包日志	如需特定数据包的详细信息,请使用此日志。您最好通 过查看数据包来深入了解报告中列出的安全事件。
攻击日志	如需发生的特定攻击的详细信息,请使用此日志。

## 关于 TruScan 主动型威胁扫描报告和日志中的信息

表 12-5 说明一些可从 TruScan 主动型威胁扫描报告和日志获取的信息种类的常规 用途。

#### 表12-5 TruScan 主动型威胁扫描快速报告和日志摘要

报告或日志	常规用途
TruScan 主动型威胁扫描检测结果 (位于"风险"报告下) 某段时间内的TruScan 主动型威胁 检测(位于"风险"报告下)	使用此报告可以查看下列信息:
	<ul> <li>标记为风险但您已将其添加到网络可接受的例外中的应用程序列表</li> <li>已检测到且已确认为风险的应用程序列表</li> <li>已检测到但其状态仍未确认为风险的应用程序列表</li> </ul>
	使用"某段时间内的TruScan 主动型威胁检测"可查看 TruScan 主动型威胁扫描检测到的威胁是否已在某段时 间内发生更改。
TruScan 主动型威胁分布(位于 "风险"报告下)	<ul> <li>此报告可用于以下目的:</li> <li>查看"商业应用程序"列表和"强制检测"列表中 有哪些应用程序最常被检测到</li> <li>查看针对检测结果采取的操作</li> <li>确定您网络中是否有特定计算机频繁受到此携带病 毒应用程序的攻击</li> <li>查看发动攻击的应用程序的详细信息</li> </ul>
TruScan 主动型威胁扫描日志	如需特定主动型威胁检测事件的详细信息,请使用此日志。此信息可能包括在检测进行时登录的用户名等。您还可以使用此日志中的命令将如文件、文件夹、扩展名和进程等合法实体添加到集中式例外策略中。当它们添加到列表后,如果某合法活动被检测为风险,也不会对此实体采取操作。

## 关于风险报告和日志中的信息

风险日志和报告包含有关管理服务器及其客户端上的风险事件的信息。

表12-6说明一些可从风险快速报告和日志中获取的信息种类的常规用途。

日志和报告类型	常规用途
受感染和有风险的计算机	使用此报告可很快确定您应该注意哪些计算机,因为它 们已受到病毒的感染或者存在安全风险。
检测操作摘要	使用此报告可了解风险检测到后已采取的操作。此信息 也会显示在 Symantec Endpoint Protection 主页上。
风险检测数量	使用此报告可了解哪些域、组或特定计算机检测到的风 险数量最大。然后,您可以深入了解网络中的某些实体 为何比其他实体存在更多风险。
网络中检测到的新风险	使用此报告可确定并跟踪新风险对您网络的影响。
前几个风险检测关联	使用此报告可了解风险与计算机、用户、域和服务器之间的关联。
风险分布摘要 某段时间内的风险分布	使用这些报告可以跟踪风险的分布情况。通过这些情况,可以确定到底是哪些特定的风险、域、组、服务器、计算机和用户出现的问题较多。您可以使用"某段时间内的风险分布"查看某段时间内这些风险的变化情况。
前几个风险的操作摘要	使用此报告可检查已针对 Symantec Endpoint Protection 在您网络中检测到的风险采取了什么操作。
通知数 某段时间内的通知数	通过这些报告提供的信息,您可以改善网络中创建及配 置通知的方式。
每周爆发	使用此报告可跟踪每周爆发的风险。
全面风险报告	使用此报告可同时查看所有分布报告和新风险报告信息。
风险日志	如需"风险"报告中任何方面的详细信息,请使用此日志。例如,您可以使用"风险"日志查看经常检测到风险的计算机上的风险详细信息。您还可以使用"风险"日志查看影响您网络的特定严重性的安全风险的详细信息。

表12-6 风险快速报告和日志摘要

## 关于扫描报告和日志中的信息

扫描日志和报告提供关于防病毒和防间谍软件扫描活动的信息。 表12-7 说明一些可从扫描快速报告和日志中获取的信息种类的常规用途。

报告或日志	常规用途
扫描统计信息直方图	如您希望使用此报告来查看客户端完成调度扫描所花时间的直方图时,请将其按扫描时间分组。您最好根据此 信息更改所调度扫描的时间。您可以根据已扫描的文件 数目过滤此报告。这些结果有助于您了解是否有任何用 户对调度扫描进行了限制,只使其扫描计算机的少数文 件。
按上次扫描时间显示计算机	使用此报告可确定哪些计算机近期尚未运行扫描。在此 报告中,您可以将要检查的时间配置为过去 24 小时或 过去一周,或者其他自定义时间段。
未扫描的计算机	使用此报告可获取在特定时间段内没有进行扫描的计算 机的列表。此报告还可以提供按特定域或组分类的计算 机 IP 地址。这些计算机可能存在风险。
扫描日志	在此日志内,您可以按扫描持续时间分类各项,以了解 您网络中哪些计算机的扫描时间最长。您可以根据此信 息,视需要自定义这些计算机的调度扫描。

#### 表12-7 扫描快速报告和日志摘要

## 关于系统报告和日志中的信息

系统日志包括有助于解答客户端疑难问题的信息。

表 12-8 说明一些可从系统快速报告和日志中获取的信息种类的常规用途。

表12-8 系统日志和系统快速报告摘要

报告或日志	常规用途
按生成错误多少排列最靠前的客户端	使用此报告可以查看哪些客户端生成的错误和警告数目 最多。您可以查看这些客户端的位置及其用户类型,检 查它们为何出现了比其他客户端更多的问题。然后,您 可以转到系统日志查看详细信息。
按生成错误多少排列最靠前的服务 器	使用此报告可以查看哪些服务器生成的错误和警告数目 最多。您可以查看这些服务器,检查它们为何与网络的 一般情形相比出现的问题要多。
按生成错误多少排列最靠前的 Enforcer	使用此报告可以查看哪些Enforcer生成的错误和警告数 目最多。您可以查看这些Enforcer,检查它们为何与网 络的一般情形相比出现的问题要多。
某段时间内的数据库复制失败	使用此报告可以查看哪些服务器或站点发生的数据库复制问题最多。报告也会说明复制失败的原因,以便您可以纠正这些问题。

报告或日志	常规用途
站点状态	使用此报告可以查看您的服务器是如何处理其客户端负 荷的。您最好根据此报告中的信息调整负荷。
管理日志	使用此日志可以查看管理相关条目,如下列活动:
	<ul> <li>登录和注销</li> <li>策略更改</li> <li>密码更改</li> <li>当证书匹配时</li> <li>复制事件</li> <li>登录相关事件</li> </ul>
	此日志可能有助于排除证书缺失、策略或导入等客户端 方面的故障。您可以分别查看与域、组、用户、计算 机、导入、软件包、复制以及其他事件相关的事件。
客户端服务器活动日志	使用此日志可以查看特定服务器上发生的所有客户端活动。
	例如,您可以使用此日志查看下列条目:
	<ul><li>■ 策略卜载是否成功或失败</li><li>■ 客户端与服务器之间的连接</li><li>■ 服务器注册</li></ul>
服务器活动日志	除了其他用途外,您可以将此日志用于以下目的:
	<ul> <li>找到复制问题所发生的位置并将其解决</li> <li>找到备份问题所发生的位置并将其解决</li> <li>找到 Radius 服务器问题所发生的位置并将其解决</li> <li>查看特定严重性等级的所有服务器事件</li> </ul>
客户端活动日志	除了其他用途外,您还可以使用此日志监控下列客户端 相关活动:
	<ul> <li>哪些客户端已遭到禁止而不能访问网络</li> <li>哪些客户端需要重新启动</li> <li>哪些客户端已安装成功或安装失败</li> <li>哪些客户端出现了服务启动与终止问题</li> <li>哪些客户端出现了规则导入问题</li> <li>哪些客户端出现了策略下载问题</li> <li>哪些客户端与服务器的连接失败</li> </ul>

报告或日志	常规用途
Enforcer 活动日志	使用此日志可以监控 Enforcer 发生的问题。在此日志 中,您可以查看管理事件、Enforcer 事件、启用事件和 策略事件。您可以根据严重性等级过滤事件。 例如,您可以使用此日志解决以下类型的问题: Enforcer 连接 策略和配置的导入与应用 Enforcer 启动、停止和暂停

**注意**:如果您没有安装 Symantec Network Access Control, Enforcer 活动日志以及其他应用到 Enforcer 之日志中的条目会为空。

## 关于排除病毒和安全风险

您可以根据网络的安全状态,每天或按照需要排除病毒感染和安全风险。首先,您 要识别并找出风险,然后决定处理它们的方式。在您补救问题之后,您可以更新 "计算机状态"日志,以表明您已对风险做出了响应。

## 标识受感染及有风险的计算机

标识受感染且存在风险的计算机是第一要务。

#### 标识受感染的计算机

1 在控制台中,单击"主页",然后查看"操作摘要"。

如果您是系统管理员,则可看到您站点内新感染和仍受感染的计算机数。如果 您是域管理员,则可看到您所管理域中的新感染和仍受感染的计算机数。仍受 感染是新感染的子集,仍受感染的数目会随着您对网络中风险的清除而减少。 如果后续扫描还将计算机报告为受感染,则计算机仍会处于受感染状态。例 如,Symantec Endpoint Protection可能只可部分清除计算机中的风险,因此 自动防护仍会检测到该风险。

- 2 在控制台中,单击"报告"。
- 3 在"报告类型"列表框中,单击"风险"。
- 4 在"选择报告"列表框中,单击"受感染和有风险的计算机"。
- 5 单击"创建报告",然后注意显示的受感染和有风险的计算机列表。

## 更改操作并重新扫描标识出的计算机

补救网络中的风险的下一个步骤就是确定计算机仍受感染或存在风险的原因。检查 针对受感染和有风险计算机上每个风险所采取的操作。所配置及采取的操作有可能 是"不操作"。如果此操作为"不操作",您应该清除计算机中的风险、将计算机 从网络中删除,或接受风险。您最好编辑应用于此计算机所属组的防病毒和防间谍 软件策略;或者针对此类别的风险或此特定风险配置其他操作。

#### 标识需要更改的操作及重新扫描标识出的计算机

- 1 在控制台中,单击"监视器"。
- 2 在"日志"选项卡中,选择"风险"日志,然后单击"查看日志"。

您可以从"风险日志事件"列中看到已发生的事件以及已采取的操作。从"风 险名称"列中,可以看到仍处于活动状态的风险的名称。从"域组用户"列中 可以查看计算机属于哪一个组。

如果因为扫描采取的操作为"不操作"而造成客户端存在风险,您可能需要更 改相应组的防病毒和防间谍软件策略。从"计算机"列中您可以看到仍存在活 动风险的计算机的名称。

请参见第334页的"配置要针对检测到的已知病毒和安全风险执行的操作"。

如果您的策略配置为使用"推模式",则在下次检测信号时,该策略会被推送 至相应组中的客户端。

请参见第 297 页的"配置推模式或拉模式来更新客户端策略和内容"。

- 3 单击"上一步"。
- 4 在"日志"选项卡中,选择"计算机状态"日志,然后单击"查看日志"。
- **5** 如果您更改了操作并推送了新策略,请选择需要使用新设置重新扫描的计算机。
- 6 从"命令"列表框中,选择"扫描",然后单击"开始"以重新扫这些描计算机。

您可以从"命令状态"选项卡监控扫描命令的状态。

### 重新启动需重新启动才能完成补救的计算机

某些计算机由于需要重新启动才能完成对病毒或安全风险的补救操作,故而可能仍 存在风险或处于受感染状态。

#### 重新启动计算机以完成补救

- 在风险日志中,选中"需要重新启动"列。
   情况可能是某些计算机中的风险已部分清除,但这些计算机仍需重新启动才能 完成补救操作。
- 2 在列表中选择需要重新启动的计算机。
- 3 在"命令"列表框中,选择"重新启动计算机",然后单击"开始"。 您可以从"命令状态"选项卡监控"重新启动计算机"命令的状态。

#### 更新定义并重新扫描

某些计算机可能会因为其定义已过期而仍存在风险。

#### 更新定义并重新扫描

- 1 对于视图中的其余计算机,选中"定义日期"列。如果有些计算机的病毒定义 已过期,请选定这些计算机。
- 2 在"命令"列表框中,选择"更新内容并扫描",然后单击"开始"。 您可以从"命令状态"选项卡监控"更新内容并扫描"命令的状态。
- 3 单击"主页",然后在"操作摘要"中查看"仍受感染"和"新感染"行中的数字。

如果数目为零,则表示您已将风险清除完毕。如果数目不为零,那么您应该要检查残留的风险。

#### 关于调查及清除残留的风险

如果仍然残留有任何风险,您可能需要做进一步的调查。有关检测到的风险的更多 信息,您可以从"扫描结果"对话框单击指向 Symantec 安全响应中心的链接。扫 描结果也可以告诉您与检测到的风险有关的进程、文件或注册表项。您可能可以创 建自定义应用程序控制策略来禁止具有攻击性的应用程序。或者,您可能需要断开 计算机与网络的连接,然后删除文件和注册表项,并手动终止进程。

### 清除可疑事件

可疑安全风险是指TruScan主动型威胁扫描检测到需要调查的情况。检测到的情况 可能是有害的,也可能是无害的。如果您确定此风险无害,可以使用集中式例外策 略将此风险排除在日后的检测范围之外。如果主动型威胁扫描不能补救风险,或者 您已经将扫描配置为忽略风险,则可能需要清除这些风险。

如果您已配置 TruScan 主动型威胁扫描 进行记录,而您调查并确定此风险有害,则可以使用集中式例外策略予以补救。可通过配置集中式例外策略来终止或隔离风险,但不能记录风险。

如果 Symantec Endpoint Protection 使用默认 TruScan 主动型威胁扫描设置检测 到此风险,则 Symantec Endpoint Protection 不能补救此风险。如果您确定此风险 有害,应手动删除此风险。删除此风险之后,便可以将该条目从风险日志中删除。

## 查找脱机客户端

您可以利用几种方式查看网络中哪些计算机处于脱机状态。 例如,您可以执行下列检查:

- 运行"计算机状态"快速报告"未登入服务器的计算机"来查看联机状态。
- 配置和运行此报告的自定义版本,以查看特定组或站点中的计算机。
- 查看"计算机状态"日志,其中包含计算机的 IP 地址以及上次登录时间。

客户端可能会出于几个原因而脱机。您可以利用几种方式来标识处于脱机状态的计 算机并针对这些问题采取补救措施。

如果您安装有 Symantec Network Access Control,则可以使用"遵从性"过滤器 选项来自定义"未登入服务器的计算机"快速报告。然后,可以使用此报告查看因 特定原因而不在网络中的计算机。接着就可以解决发现的问题。

可用来过滤的遵从性原因如下:

- 计算机的防病毒版本过期。
- 计算机的防病毒软件并未运行。
- 脚本失败。
- 计算机的位置发生了更改。

#### 查找处于脱机状态的客户端

- 1 在控制台中,单击"监视器"。
- 2 在"日志"选项卡的"日志类型"列表框中,单击"计算机状态"。
- 3 单击"高级设置"。
- 4 在"联机状态"列表框中,单击"脱机"。
- 5 单击"查看日志"。

默认情况下,将显示在过去24小时脱机的计算机列表。此列表包括每部计算 机的名称、IP地址以及上次登录其服务器的时间。您可以调整时间范围,以显 示在要查看的任何时间范围内脱机的计算机。 200 | 使用监视器和报告来确保网络安全 | 查找脱机客户端





# 高级管理任务

- 管理站点
- 管理服务器
- 管理目录服务器
- 管理电子邮件服务器
- 管理代理服务器
- 管理 RSA 服务器
- 管理服务器证书
- 管理数据库
- 复制数据
- 管理防篡改

202 |

# 13

# 管理站点

本章节包括下列主题:

- 关于站点管理
- 关于跨越不同公司站点的站点复制
- 关于在站点选用 Enforcer
- 关于远程站点
- 编辑站点属性
- 备份站点
- 删除远程站点

## 关于站点管理

Symantec Endpoint Protection 将安装的组件组织成各个站点。一个站点包括单个 或多个 Symantec Endpoint Protection Manager 及一个数据库(MS SQL 或嵌入 式)。它也可以包括一个或多个 Enforcer,各个 Enforcer 通常都位于相同的企业 位置。大型企业通常安装许多站点。所需站点数目通常与公司拥有多个实际办公场 所、独立的部门、不同子网的区域等因素有关。企业管理层及IT部门通常会负责决 定这些站点的数目和位置。

本地站点是您登录的 Symantec Endpoint Protection Manager 控制台。不过,这 不一定表示该站点实际上就在本地。此站点可以位于另一个城市。远程站点是指作 为复制伙伴链接到本地站点的站点。

您可以从任何可管理本地站点和远程站点的控制台集中管理网络安全。

对于本地站点和远程站点,您可以从特定站点执行下列任务:

■ 更改站点说明。
 请参见第 205 页的"编辑站点属性"。

- 将控制台设置为在经过一段时间后注销。
   请参见第 205 页的"编辑站点属性"。
- 清除经过一段时间还未连接的客户端。 请参见第 205 页的"编辑站点属性"。
- 设置日志阈值。
- 调度每日及每周报告。
- 配置要过滤的外部记录,并将日志发送至文件或 Syslog 服务器。
- 更改数据库名称和说明。
   请参见第 245 页的"在 Symantec Endpoint Protection Manager 控制台中编辑 数据库的名称和说明"。

从特定站点,您可以只为本地站点执行下列任务:

- 立即备份本地站点。
   请参见第 238 页的"备份 Microsoft SQL 数据库"。
   请参见第 242 页的"从控制台按需备份嵌入式数据库"。
- 更改备份调度。
   请参见第 242 页的"从 Symantec Endpoint Protection Manager 调度自动数据 库备份"。
- 删除所选服务器(仅当多个 Symantec Endpoint Protection Manager 连接至单 个 Microsoft SQL 数据库时)。
- 在同一站点中添加与复制伙伴的连接。
   请参见第 260 页的"添加和断开复制伙伴"。
- 更新服务器证书。
   请参见第 231 页的"关于服务器证书类型"。
- 查询数据库中的信息。

这些列表并非面面俱到。它们旨在让您了解在本地或远程可执行的任务类型。

您无法从远程站点执行某些任务。如果您想要安装新的站点,您需要转到已安装 Symantec Endpoint Protection Manager 或 Enforcer 的特定计算机。不过,您可 以远程登录一个站点,以执行只能在本地站点的控制台上执行的其他任务。

请参见第 26 页的"登录 Symantec Endpoint Protection Manager 控制台"。

## 关于跨越不同公司站点的站点复制

在公司安装第一个站点之后,您可以安装其他站点作为复制伙伴。您可以在安装第 二个及后续站点时添加复制伙伴。 如需如何在初始安装期间配置第一个站点的详细信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

## 关于在站点选用 Enforcer

如果您的站点需要额外的强制执行功能,您可以安装 Gateway Enforcer、LAN Enforcer 和 DHCP Enforcer。

如果要将 Enforcer 添加到现有站点,请参见《Symantec Network Access Control Enforcer 设备操作指南》。

## 关于远程站点

您可以从"服务器"选项卡查看其他站点。如果您连接至其他 Symantec Endpoint Protection Manager 控制台,您也可以编辑远程站点的服务器属性。您可以对远程站点执行下列任务:

- 删除远程站点及其复制伙伴。
- 更改远程服务器的说明。
- 更改对远程站点的控制台的访问权限。
- 设置远程站点的电子邮件服务器。
- 为远程站点调度目录服务器同步。
- 设置从远程站点的服务器到代理服务器的连接。
- 配置外部日志记录,以将日志发送到文件或 Syslog 服务器。

## 编辑站点属性

站点属性包括以下内容:

- 站点名称和站点说明
- 指定控制台超时的时间段
- 是否要删除经过一段时间未连接的客户端
- 是否要打开站点的"应用程序发现"
- 在站点上维护的最大日志大小
- 报告调度

您可以从控制台编辑本地或远程站点属性。

#### 编辑站点属性

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面的"任务"下,单击"服务器"。
- 3 在"管理员"页面的"查看"下方,展开"本地站点(站点<站点名称>)"或展 开"远程站点"。
- 4 选择您要编辑其属性的站点。
- 5 在"管理员"页面的"任务"下方,单击"编辑站点属性"。
- 6 在"常规"选项卡的"站点属性"对话框中,编辑"说明"框中的站点说明。 您最多可以使用 1024 个字符。
- 7 在"常规"选项卡的"站点属性"对话框中,从"控制台超时"列表的"5分钟"到"从不"中选择一个值。 默认值为1小时。达到"控制台超时"时间时,会自动将管理员从控制台中注销。
- 8 在"常规"选项卡的"站点属性"对话框中,选中"删除经过x天未连接的客户端"。
   您可以删除经过指定天数(1至99999)未连接的用户。默认设置是三十(30)
- 9 在"常规"选项卡的"站点属性"对话框中,选中"保持跟踪客户端所运行的 每个应用程序"。

"已知应用程序"可记录每个客户端上启动的所有应用程序,帮助管理员跟踪 客户端的网络访问及应用程序使用情况。您可以启用或禁用特定站点的"应用 程序发现"功能。如果未启用此选项,该站点不会运行应用程序的跟踪功能。 即使针对连接至指定站点的那些客户端启用应用程序跟踪功能,该功能也不会 再运行。此选项的作用如同总开关。

10 在"常规"选项卡的"站点属性"对话框中,从"选择要发送通知并运行调度 报告的服务器"列表中选择报告服务器。

仅当您使用连接至多个数据库的 Microsoft SQL 数据库,才需要使用此选项。

11 单击"确定"。

天。

## 备份站点

当您备份站点的信息时,所执行的任务与备份站点的数据库相同。 请参见第 238 页的"备份 Microsoft SQL 数据库"。 请参见第 242 页的"从控制台按需备份嵌入式数据库"。

#### 备份站点

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面的"任务"下,单击"服务器"。
- **3** 在"管理员"页面的"查看"下方,单击 localhost。
- 4 在"管理员"页面的"任务"下方,单击"编辑备份设置"。
- 5 在"本地站点的备份站点:本地站点的站点名称"对话框中,从"备份服务器" 列表选择备份服务器的名称。

默认路径名称为 Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup。

不过,您可以使用其中一个可用的备份实用程序来更改备份路径的名称。

- 6 从"要保留的备份的数目"列表选择要保留的备份的数目。 您最多可以选择保留10个备份,超出此数目之后,便会自动删除备份副本。
- 7 单击"确定"。

## 删除远程站点

当您删除公司远程站点的服务器时,您需要手动从所有的 Symantec Endpoint Protection Manager 中删除它。这样的服务器列在"远程站点"下方。从某个 Symantec Endpoint Protection Manager 控制台中卸载软件并不会使其图标从其他 控制台上的"服务器"窗格中消失。

#### 删除远程站点

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面的"任务"下,单击"服务器"。
- 3 在"管理员"页面的"查看"下方,单击"远程站点"。
- 4 在"管理员"页面的"查看"下方,展开"远程站点",然后选择计划要删除的站点。

- 5 单击"删除远程站点"。 在"删除远程站点"对话框中,会提示您确认删除远程站点: 解除远程站点也会删除此站点 参与的所有复制伙伴关系。 您是否确定要删除此站点?
- 6 单击"是",删除远程站点。 您可以添加复制伙伴,重新添加已删除的远程站点。

## 管理服务器

本章节包括下列主题:

- 关于服务器管理
- 关于服务器和第三方密码
- 启动和停止管理服务器服务
- 授权或拒绝远程 Symantec Endpoint Protection Manager 控制台的访问
- 删除所选服务器
- 导出和导入服务器设置

## 关于服务器管理

您可以使用 Symantec Endpoint Protection Manager 控制台的"管理员"页面集 中管理所有类型的服务器。

"管理员"页面的"查看服务器"下方会列出下列组:

- 本地站点 本地站点上的控制台、数据库、复制伙伴(例如其数据库会进行复制的其他控制台),以及可选 Enforcer
- 远程站点

任何远程站点上的控制台、数据库、复制伙伴(例如其数据库会进行复制的其他 Symantec Endpoint Protection Manager),以及可选 Enforcer

## 关于服务器和第三方密码

您可以创建连接的所有服务器,都需要在 Symantec Endpoint Protection Manager 中配置第三方密码。第三方密码会自动保存在您最初安装 Symantec Endpoint Protection Manager 时所创建的数据库中。 通常系统会在配置下列类型服务器时提示您提供第三方密码:

- 电子邮件服务器
- 目录服务器
- RSA 服务器
- 代理服务器

## 启动和停止管理服务器服务

安装 Symantec Endpoint Protection Manager 时,服务器配置助手的最后一个步骤会提供 Symantec Endpoint Protection Manager 控制台复选框(默认为已选择)。如果您使此复选框保持选中,则控制台会自动启动。

管理服务器会作为自动服务运行。如果软件未自动启动,您可以从"开始"菜单的 "管理工具"中使用"服务"加以启动(或在以后停止)。

**注意**:如果您停止管理服务器服务,则客户端就不能再与之连接。如果客户端需要 与管理服务器通信才能连接至网络,则在重新启动管理服务器服务之前会拒绝这些 客户端访问。

例如,客户端必须与管理服务器通信才能通过主机完整性检查。

#### 启动管理服务器服务

◆ 从命令提示符键入:

net start semsrv

#### 停止管理服务器服务

♦ 从命令提示符键入:

net stop semsrv

您也可以重新启动控制台来自动启动服务。

# 授权或拒绝远程 Symantec Endpoint Protection Manager 控制台的访问

您可以通过授权或拒绝访问安装远程控制台的计算机来确保主控制台的安全。默认 情况下允许访问所有控制台。管理员可以从本地或从网络中的任何一台计算机远程 登录到主控制台。 除了全局授权或拒绝访问之外,您也可以用IP地址指定例外。如果您选择授权访问 所有远程控制台,则例外列表会自动拒绝访问。相反地,如果您拒绝访问所有远程 控制台,则会自动授权访问所有例外。

当您创建例外时,指定的计算机必须具有静态IP地址。您也可以指定子网掩码,针 对计算机组创建例外。例如,您可能希望允许访问您管理的所有区域。但是,您可 能要拒绝对公共区域中的控制台的访问。

#### 授权或拒绝访问远程控制台

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,选择您要更改其控制台访问权限的服务器。
- 3 在"任务"下方,单击"编辑服务器属性"。
- 4 在"常规"选项卡中,单击"已授权访问"或"已拒绝访问"。
- 5 如果您要指定计算机IP地址,将其设为此控制台访问权限的例外,请单击"添加"。

添加的计算机会成为授权访问的例外,会拒绝访问这些计算机。如果您选择 "已拒绝访问",您指定的计算机会是唯一能够进行访问的计算机。针对一台 计算机或一组计算机创建例外。

- 6 在"拒绝控制台访问"对话框中,单击下列选项之一:
  - 单台计算机

对于单台计算机,键入其 IP 地址。

■ 计算机组

对于多台计算机,键入组的 IP 地址和子网掩码。

7 单击"确定"。

此时计算机会出现在例外列表中。对于每个 IP 地址和掩码,将显示其权限状态。

如果您将"已授予访问"更改为"已拒绝访问"或反之,则所有的例外也会一 并更改。如果您已创建例外以拒绝访问,则这些例外会更改为允许访问。

8 单击"全部编辑",更改显示在例外列表中的计算机 IP 地址或主机名称。

"IP地址编辑器"随即出现。"IP地址编辑器"是一种文本编辑器,可以编辑 IP 地址和子网掩码。

- 9 单击"确定"。
- 10 将例外添加至列表或编辑列表完成后,请单击"确定"。

## 删除所选服务器

您可能已卸载多个 Symantec Endpoint Protection Manager 的安装。但是,它们可能仍显示在 Symantec Endpoint Protection Manager 控制台中。在这种情况下,您必须删除连接。

这种情况最常出现在使用 Microsoft SQL 数据库,且有多个 Symantec Endpoint Protection Manager 连接至此数据库时。如果卸载某个 Symantec Endpoint Protection Manager,它仍然会显示在其他控制台上。您需要手动删除不再连接的服务器。

#### 删除所选服务器

**1** 停止 Symantec Endpoint Protection Manager 服务。

请参见第 210 页的"启动和停止管理服务器服务"。

- 2 在控制台中,单击"管理员"。
- 3 在"管理员"页面中,单击"服务器"。
- 4 在"查看服务器"下方,展开"本地站点(站点名称)"并单击您要删除的 Symantec Endpoint Protection Manager。
- 5 单击"删除所选服务器"。
- 6 单击"是",确认您要删除所选服务器。

## 导出和导入服务器设置

您可能要导出或导入 Symantec Endpoint Protection Manager 的设置。设置会导出为.xml 格式的文件。

#### 导出服务器设置

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,展开"本地站点(站点<站点名称>)",然后选择您要导出的管理服务器。
- 3 单击"导出服务器属性"。
- 4 选择保存文件的位置,并指定文件名。
- 5 单击"导出"。

#### 导入服务器设置

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,展开"本地站点(站点<站点名称>)",然后选择您要导入设置的管理服务器。

- 3 单击"导入服务器属性"。
- 4 选择要导入的文件, 然后单击"导入"。
- 5 单击"**是**",确认导入。

214 | 管理服务器 **导出和导入服务器设置** 

# 15

# 管理目录服务器

本章节包括下列主题:

- 关于目录服务器的管理
- 添加目录服务器
- 同步目录服务器和 Symantec Endpoint Protection Manager 之间的用户帐户
- 关于从 LDAP 目录服务器导入用户和计算机帐户信息
- 在LDAP 目录服务器上搜索用户
- 从 LDAP 目录服务器搜索结果列表导入用户
- 关于组织单位和 LDAP 服务器

## 关于目录服务器的管理

在与任何目录服务器进行通信之前,都需要对 Symantec Endpoint Protection Manager进行相应配置。您需要在目录服务器和管理服务器之间建立连接。如果您没有建立连接,便不能从 Active Directory 或 LDAP 目录服务器导入用户,也不能与它们进行同步。

## 添加目录服务器

对于 Active Directory 服务器,您不能过滤用户。对于 LDAP 服务器,您可以在导 人数据之前过滤用户。因此,如果需要过滤数据,您可能希望添加具有 LDAP 兼容 性的 Active Directory 服务器作为 LDAP 服务器。

添加目录服务器之后,您可能会想要设置同步处理。

请参见第216页的"同步目录服务器和 Symantec Endpoint Protection Manager 之间的用户帐户"。

#### 添加目录服务器

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,选择您要添加目录服务器的管理服务器。
- 3 在"任务"下方,单击"编辑服务器属性"。
- 4 在"<站点名称>的服务器属性"对话框的"目录服务器"选项卡中,单击"添 加"。
- 5 在"添加目录服务器"对话框的"名称"字段中,键入您要添加的目录服务器 的名称。
- 在"添加目录服务器"对话框中,选中 Active Directory 或 LDAP 作为服务 器类型。
- 7 在"添加目录服务器"对话框的"服务器IP地址或名称"框中,键入服务器的 IP地址、主机名或域名。

必须键入要添加的目录服务器的 IP 地址、主机名称或域名。

8 如果添加 LDAP 服务器,请在"LDAP 端口"框中,键入 LDAP 服务器的端口 号。

如果添加 Active Directory 服务器,则不能更改这些值。 默认端口设置为 389。

- 9 如果添加 LDAP 服务器,请在 LDAP BaseDN 框中键入 LDAP BaseDN。
- 10 在"用户名"框中,键入授权的目录服务器帐户的用户名。
- 11 在"密码"框中,键入目录服务器帐户的密码。
- 12 如果您要使用安全套接字层 (SSL) 连接至目录服务器,请选中"使用安全连接"。

如果未选中此选项,则使用常规未加密连接。

13 单击"确定"。

## 同步目录服务器和 Symantec Endpoint Protection Manager 之间的用户帐户

您可以配置目录服务器以使用 Symantec Endpoint Protection Manager 导入和同步用户。您必须已经添加目录服务器,之后才能同步用户相关信息。

#### 同步目录服务器和 Symantec Endpoint Protection Manager 之间的用户帐户

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,选择您要添加目录服务器的管理服务器。
管理目录服务器 | 217 关于从 LDAP 目录服务器导入用户和计算机帐户信息 |

- 3 在"任务"下方,单击"编辑服务器属性"。
- 4 在"服务器属性"对话框中,单击"目录服务器"选项卡。
- 5 如果尚未选中"与目录服务器同步",请选中。 此选项为默认设置。
- 6 若要设置调度来指定您要将管理服务器与目录服务器同步的频率,请执行下列 任一操作:
  - 若要每 24 小时自动同步,请单击"自动调度"。 默认设置是调度为每 86400 秒进行同步。您也可以通过编辑 tomcat\etc\ conf.properties 文件来自定义时间间隔。
  - 若要指定所需同步的频率,请单击"同步间隔"并指定小时数。
- 7 单击"确定"。

# 关于从 LDAP 目录服务器导入用户和计算机帐户信息

管理员可以使用 LDAP 协议从 LDAP 目录服务器导入用户及计算机帐户的相关信息。

如果您计划导入有关用户和帐户的信息,则必须先建立Symantec Endpoint Protection Manager 和目录服务器之间建立连接。

请参见第 215 页的"添加目录服务器"。

然后您可以搜索并导入有关用户和帐户的信息,方法是完成下列任务:

- 搜索 LDAP 服务器中的用户。 请参见第 217 页的"在 LDAP 目录服务器上搜索用户"。
- 导入有关用户帐户的信息。 请参见第 220 页的"从 LDAP 目录服务器搜索结果列表导入用户"。

## 在 LDAP 目录服务器上搜索用户

将用户信息导入管理服务器时,需要在 LDAP 服务器上搜索用户。

#### 在 LDAP 目录服务器上搜索用户

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择要导入用户的组。
- 3 在"任务"下,单击"导入 Active Directory 或 LDAP 用户"。
- **4** 在"导入 Active Directory 或 LDAP 用户"对话框的"服务器"框中,键入 IP 地址或主机名。

- 5 在"导入 Active Directory 或 LDAP 用户"对话框的"服务器端口"框中,键入 LDAP 服务器或 Active Directory 服务器的端口号。
  默认的端口号为 389。
- 6 如果您要使用安全套接字层 (SSL) 与目录服务器连接,请单击"使用安全连接"。

如果未选中此选项,则会使用未加密的连接。

7 单击"列出用户",以列出用户。 您也可以在"LDAP 搜索基础"框中键入 LDAP 查询来查找要导入的用户名。 您可以指定搜索选项,例如"属性=值"对。多个属性必须使用逗号隔开。

CN	CommonName
DC	DomainComponent
L	LocalityName
ST	StateOrProvinceName
0	OrganizationName
OU	OrganizationalUnitName
С	CountryName
STREET	StreetAddress

并非所有 LDAP 服务器都支持所有选项。例如, Microsoft Active Directory 不 支持 O。

您指定"属性=值"对的顺序很重要,因为它指示了 LDAP 目录层次结构中条目的位置。

如果在安装目录服务器期间,您指定了 DNS 类型的域名(例如 itsupport.sygate.com),则可以查询目录服务器,因为 itsupport 是典型的 NT NetBIOS 域名。

若要查询 Active Directory 服务器,请按照下列顺序指定 LDAP 搜索基础:

CN=Users, DC=itsupport, DC=sygate, DC=com

可以在搜索基础中使用通配符或正则表达式。例如:

CN=a\*, CN=Users, DC=itsupport, DC=sygate, DC=com

此查询会返回以字母 a 开头的所有用户名。

下面的例子表示您可能要执行结构目录搜索的组织,例如:

mycorp.com -> engineering.mycorp.com or sales.mycorp.com

您可以指定任一选项,作为要搜索 LDAP 目录的开始位置。

o=mycorp.com or o=engineering.mycorp.com

您可以在 LDAP 搜索字符串中,使用 > 或 < 来指定逻辑比较。

如果 LDAP 查询返回 1,000 个以上的结果,则该查询可能失败。因此,请确保 设置搜索基础,以便报告的用户数少于 1,000。

- 8 在"授权帐户"框中,键入LDAP用户帐户的名称。
- 9 在"密码"框中,键入LDAP用户帐户的密码。
- 10 单击"列出用户",显示 LDAP 服务器上的用户列表。 如果选中"只显示未添加到任何组的用户",则只会显示尚未添加的用户。

## 从 LDAP 目录服务器搜索结果列表导入用户

您也可以从 LDAP 服务器搜索结果列表导入用户。

#### 从 LDAP 目录服务器搜索结果列表导入用户

- 1 在控制台中,单击"客户端"。
- 2 在"组列表"树中,选择要从LDAP 服务器添加用户的目标组。
  若要添加所有用户,请单击"全部添加",或者从列表选择特定用户,然后单击"添加"。
- 3 单击字段名称,按该列进行排序。 您可以按字段对搜索结果进行升序或降序排序。
- 4 从"LDAP 用户列表"区域选择一或多位用户。 您可以使用标准 Windows 选择键(例如 Ctrl 键)选择非连续的用户。
- 5 单击"添加",新用户的名称就会显示在组树中。
- 6 根据需要,重复此过程,将用户添加到其他组,直到将所有新用户添加到适当 的组中。
- 7 单击"关闭"。

# 关于组织单位和 LDAP 服务器

Symantec Endpoint Protection Manager 可从 Active Directory 或 LDAP 服务器自动同步组织单位 (OU) 中的用户、计算机和整个组结构。导入后,您便可以将策略分配给创建的组。您不能在 Symantec Endpoint Protection Manager 控制台中修改导入的组织单位。如果您仍然需要添加、删除或修改它们,则必须在 LDAP 服务器上执行这些任务。如果您启用同步,则 Symantec Endpoint Protection Manager 会自动保持与目录服务器上所实现的结构同步。

您也可以在控制台上创建组,然后将用户从OU复制到这些组。管理服务器组和OU 中可能会有相同的用户。在这种情况下,组的优先级会高于OU的优先级。因此, 组的策略会应用于用户或计算机。

## 从 Active Directory 服务器或 LDAP 目录服务器导入组织单位

如果要导入组织单位或容器,则 Symantec Endpoint Protection Manager 必须已 连接到 LDAP 服务器。

请参见第 215 页的"添加目录服务器"。

您不能从"导入组织单位"对话框过滤任何结果。如果要过滤用户,就必须在将 LDAP 服务器添加到管理服务器时执行此操作。在两个地方都不能过滤 Active Directory 服务器。

根据用户人数,此进程可能需要些时间。您不能将组织单位放入多个组树中。

#### 从 LDAP 服务器导入组织单位

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择要添加组织单位或容器的组。
- 3 在"任务"下,单击"导入组织单位或容器"。
- 4 选择域。
- 5 选择组织单位。
- 6 单击"确定"。

#### 关于同步组织单位

与 LDAP 服务器及 Active Directory 集成和同步是 Symantec Endpoint Protection Manager 的选用功能。您可以从其他服务器导入组织单位,然后设置自动与其他服务器同步导入的 OU。

您在 LDAP 服务器上所做的任何更改不会立即显示在之前导入管理服务器的组织单位中。延迟的时间视同步处理频率而定。您可以通过在控制台上编辑服务器属性来 设置同步频率。

即使您已执行下列任务,用户的名称仍会出现在控制台上的组中:

- 将用户从组织单位复制至组
- 随后从 LDAP 服务器删除该用户

只有 LDAP 服务器与组织单位之间才会发生同步。

222 | 管理目录服务器 | **关于组织单位和 LDAP 服务器** 

# 管理电子邮件服务器

本章节包括下列主题:

- 关于管理电子邮件服务器
- 建立 Symantec Endpoint Protection Manager 和电子邮件服务器之间的通信

16

# 关于管理电子邮件服务器

如果您的网络支持电子邮件服务器,那么在建立 Symantec Endpoint Protection Manager 与电子邮件服务器之间的通信后,可能会需要执行下列工作:

- 设置要发送给管理员的安全事件的自动电子邮件通知
- 设置要发送给客户端的安全事件的自动电子邮件通知

只有在 Symantec Endpoint Protection Manager 与网络中至少一台电子邮件服务 器建立连接之后,才会发送自动电子邮件通知。

请参见第 413 页的"配置通信事件的电子邮件"。

# 建立 Symantec Endpoint Protection Manager 和电子 邮件服务器之间的通信

如果要使用电子邮件通知,您需要在 Symantec Endpoint Protection Manager 上 配置电子邮件服务器。

#### 建立 Symantec Endpoint Protection Manager 和电子邮件服务器之间的通信

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,选择您要建立与电子邮件服务器连接的管理服务器。
- 3 在"任务"下方,单击"编辑服务器属性"。
- 4 在"服务器属性"对话框中,单击"邮件服务器"选项卡。

- 5 在"服务器地址"文本框中,键入电子邮件服务器的IP地址、主机名或域名。
- 6 在"用户名"文本框中,键入帐户在电子邮件服务器上的用户名。

只有在电子邮件服务器需要验证时,才需要添加用户名。

7 在"服务器属性"对话框的"密码"文本框中,键入帐户在电子邮件服务器上的密码。

只有在电子邮件服务器需要验证时,才需要添加密码。

8 单击"确定"。

# 管理代理服务器

本章节包括下列主题:

- 关于代理服务器
- 设置 HTTP 代理服务器和 Symantec Endpoint Protection Manager 之间的连接
- 设置 FTP 代理服务器与 Symantec Endpoint Protection Manager 之间的连接

# 关于代理服务器

您可以使用 HTTP 代理和 FTP 代理服务器来帮助管理 LiveUpdates。

在 Symantec Endpoint Protection Manager 与下列服务器类型之间,您可以创建 连接类型:

- HTTP 代理服务器
- FTP 代理服务器

# 设置HTTP代理服务器和Symantec Endpoint Protection Manager 之间的连接

如果企业网络支持HTTP代理服务器,您需要将HTTP代理服务器连接至Symantec Endpoint Protection Manager。您可以使用HTTP代理服务器自动下载LiveUpdate 内容。

#### 设置 HTTP 代理服务器

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,选择您要将HTTP代理服务器连接到的管理服务器。
- 3 在"任务"下方,单击"编辑服务器属性"。
- 4 在"服务器属性"对话框中,单击"代理服务器"选项卡。

- 5 在 "HTTP 代理设置"下方,从 "代理使用"列表中选择 "使用自定义代理设置"。
- 6 在"服务器地址"字段中,键入HTTP代理服务器的IP地址。 有效的IP地址或服务器名称最多可有 256 个字符。
- 7 在"端口"字段中,键入代理服务器的端口号。 有效的端口号范围为0-65535。
- 8 选中"需要验证,才能通过代理服务器连接"。
- 9 在"用户名"字段中,键入代理服务器的用户名。
- 10 在"密码"字段中,键入您要连接到的代理服务器的密码。
- 11 单击"确定"。

# 设置FTP代理服务器与SymantecEndpointProtection Manager 之间的连接

如果您在公司网络中支持FTP代理服务器,就需要将该FTP代理服务器与Symantec Endpoint Protection Manager 连接。您可以使用 HTTP 代理服务器自动下载 LiveUpdate 内容。

设置 FTP 代理服务器与 Symantec Endpoint Protection Manager 之间的连接

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下,选择要将 FTP 代理服务器连接到的管理服务器。
- 3 在"任务"下方,单击"编辑服务器属性"。
- 4 在"服务器属性"对话框中,单击"代理服务器"选项卡。
- 5 在 "FTP 代理设置"下,从代理使用列表中选择"使用自定义代理设置"。
- 6 在"服务器地址"字段中,键入FTP代理服务器的IP地址。 IP地址或服务器名称最多可包含256个字符。
- 7 在"端口"字段中,键入代理服务器的端口号。 有效的端口号范围为0-65535。
- 8 单击"确定"。

# 管理 RSA 服务器

本章节包括下列主题:

- 关于将 RSA SecurID 与 Symantec Endpoint Protection Manager 配合使用的前 提条件
- 将 Symantec Endpoint Protection Manager 配置为使用 RSA SecurID 验证
- 为 Symantec Endpoint Protection Manager 管理员指定 SecurID 验证
- 配置管理服务器以支持 HTTPS 通信

# 关于将 RSA SecurID 与 Symantec Endpoint Protection Manager 配合使用的前提条件

如果您要使用 RSA SecurID 验证使用 Symantec Endpoint Protection Manager 的 管理员,则需要运行 RSA 安装向导来启用加密验证。

在运行向导之前,请确保:

- RSA ACE 服务器已安装好
- 安装 Symantec Endpoint Protection Manager 的计算机已在 RSA ACE 服务器 上注册为有效主机
- 为同一主机创建节点密码文件
- RSA ACE 服务器的 sdconf.rec 文件可以在网络上访问
- 同步后的 SecurID 卡或密钥卡已分配给 Symantec Endpoint Protection Manager 帐户。此登录名称必须已在 RSA ACE 服务器上激活
- 管理员有可用的 RSA PIN 或密码

Symantec 支持下列 RSA 登录类型:

■ RSA SecurID 令牌(非软件 RSA 令牌)

- RSA SecurID 卡
- RSA 键区卡(非 RSA 智能卡)

若要以 RSA SecurID 登录 Symantec Endpoint Protection Manager,管理员需具 备登录名、令牌(硬件)和 PIN 号码。

# 将 Symantec Endpoint Protection Manager 配置为使用 RSA SecurID 验证

如果您的企业网络包括 RSA 服务器,则需要在安装 Symantec Endpoint Protection Manager 的计算机上安装 RSA ACE Agent 软件,并将其配置为 SecurID 验证客户端。Symantec Endpoint Protection Manager 也称为管理服务器。

#### 在 Symantec Endpoint Protection Manager 上配置 RSA SecurID 验证

- 在已安装 Symantec Endpoint Protection Manager 的同一台计算机上安装 RSA ACE Agent 软件。您可以从 RSA Authentication Agent 光盘运行 Windows .msi 文件来安装软件。
- 2 从 RSA ACE 服务器将 nodesecret.rec、sdconf.rec 和 agent\_nsload.exe 文件 复制到安装 Symantec Endpoint Protection Manager 的计算机上。
- 3 在命令提示符处,键入以下命令:

#### agent\_nsload -f nodesecret.rec -p nodesecret 文件的密码

- 4 在控制台中,单击"管理员",再单击"服务器"。
- 5 在"查看服务器"下方,选择您要连接至 RSA 服务器的管理服务器。
- 6 在"任务"下方,单击"配置 SecurID 验证"。
- 7 在"欢迎使用配置 SecurID 验证向导"面板中,单击"下一步"。
- 8 在"配置 SecurID 验证向导"的"条件"面板中,阅读先决条件,以满足所有要求。
- 9 单击"下一步"。
- 10 在"配置SecurID验证向导"的"上载RSA文件"面板中,浏览查找sdconf.rec 文件所在的文件夹。

您也可以键入路径名称。

- 11 单击"下一步"。
- 12 单击"测试",测试您的配置。
- 13 在"测试配置"对话框中, 键入SecurID的用户名和密码, 然后单击"测试"。 现在已成功验证。

# 为 Symantec Endpoint Protection Manager 管理员指 定 SecurID 验证

您可以指定管理员必须先通过 SecurID 进行验证, 然后才能登录到管理控制台。

您可以创建新的管理员或修改现有管理员的设置。下面的过程说明了如何为新管理 员指定验证方式。

请参见第63页的"添加管理员帐户"。

#### 为 Symantec Endpoint Protection Manager 管理员创建 SecurID 验证

- 1 在控制台中,单击"管理员",然后单击"管理员"。
- 2 在"任务"下方,单击"添加管理员"。
- 3 在"添加管理员"对话框中,键入您之前为 RSA ACE 客户端配置的用户名。
- 4 在"验证类型"旁边,单击"更改"。
- 5 在"管理员验证"对话框中,选择"RSASecurID验证",然后单击"确定"。
- 6 在"添加管理员"对话框中,单击"确定"。

# 配置管理服务器以支持 HTTPS 通信

如果您计划在客户端、Symantec Endpoint Protection Manager 和可选 Enforcer 之间使用 HTTPS 通信和 SSL 验证,则需要添加 SSL 证书。您需要将 SSL 证书添加 到 Microsoft 的 Internet Information Server (IIS)。

您需要按此顺序完成下列任务:

- 生成或购买 SSL 证书。
- 将证书添加到已与 Symantec Endpoint Protection Manager 安装于同一台计算 机上的 IIS 服务器。
- 配置管理服务器列表以支持 HTTPS 通信。

#### 将证书添加到 IIS 服务器

- 1 单击"开始">"程序">"管理工具">"Internet信息服务(IIS)管理器"。
- **2** 在"本地计算机"下方,选择"网站"下方的 Symantec Web Server。
- 3 右键单击 Symantec Web Server, 然后选择"属性"。
- 4 在"目录安全性"选项卡中,单击"服务器证书"启动"Web 服务器证书向导"。

- 5 按照向导的步骤,创建或导入服务器证书。 有关详细信息,请参见 IIS 联机帮助。
- 6 在"网站"选项卡中,指定 SSL 端口的端口号(默认为 443)。

# 19

# 管理服务器证书

本章节包括下列主题:

- 关于服务器证书类型
- 更新服务器证书
- 备份服务器证书
- 找出 Keystore 密码

# 关于服务器证书类型

数字证书是验证及加密机密数据的业界标准。如果您要在信息通过网络中的路由器 时避免读取该信息,就需要对数据加密。因此,您需要使用了HTTPS协议的数字 证书。

在此安全过程中,服务器会使用服务器证书自我标识及验证。Symantec使用HTTPS 协议在网络中的所有服务器、客户端和可选的 Enforcer 之间进行通信。

您也必须在管理服务器上启用加密,以便服务器使用服务器证书来标识并验证自 己。如果没有启用此选项,那么数字证书的安装不会起作用。

Symantec Endpoint Protection Manager 支持下列类型的证书:

■ JKS Keystore 文件 (.jks)

名为 keytool.exe 的 Java 工具会生成 Keystore 文件。Symantec 仅支持 Java 密 钥标准 (JKS) 格式。Java 加密扩展 (JCEKS) 格式需要有特定版本的 Java 运行时 环境 (JRE)。Symantec Endpoint Protection Manager 仅支持使用与 Symantec Endpoint Protection Manager 上 Java 开发工具包 (JDK) 相同版本所生成的 JCEKS Keystore 文件。

该 Keystore 必须包括证书及私钥。Keystore 密码必须与密钥密码相同。它通常 是从 Internet Information Services (IIS) 导出的。

■ PKCS12 Keystore 文件 (.pfx 或 .p12)

 证书和私钥文件(DER 或 PEM 格式)
 Symantec 支持 DER 或 PEM 格式的未加密证书和私钥,不支持 PKCS8 加密的 私钥文件。

为安全起见,您可能会想要备份证书的相关信息。如果管理服务器损坏,或是您忘记了 Keystore 密码,便可以轻松地检索该密码。

有关设置服务器证书的相关信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

# 更新服务器证书

您可以使用"更新服务器证书向导",引导您完成更新证书的进程。

#### 更新 JKS 服务器证书

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,单击您要为其更新服务器证书的管理服务器。
- 3 在"任务"下,单击"管理服务器证书"。
- 4 在"欢迎使用管理服务器证书向导"窗格中,单击"下一步"。
- 5 在"管理服务器证书"面板中,单击"更新服务器证书",然后单击"下一步"。
- 6 在"更新服务器证书"面板中,单击"JKS keystore 文件 (.jks)",然后单击 "下一步"。
- 7 在 "JKS Keystore" 面板中,单击 "浏览" 找到管理服务器上的 JKS Keystore 文件 (.jks),或在文本字段中键人此文件的路径名称,然后单击"打开"。
- **8** 在"Keystore 密码"文本框中键入 Keystore 密码。
- 9 在"Keystore 密码"的文本字段中再次键入 Keystore 密码, 然后单击"下一步"。
- 10 在"管理服务器证书向导已完成"面板中,单击"完成"。
  - 在"管理服务器证书向导已完成"面板中,会出现消息,指明是否成功添加了 服务器证书。

您必须注销然后重新启动管理服务器才能使证书生效。

#### 更新 PKCS12 服务器证书

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,单击您要为其更新服务器证书的管理服务器。
- 3 在"任务"下,单击"管理服务器证书"。
- 4 在"欢迎使用管理服务器证书向导"窗格中,单击"下一步"。

- 5 在"管理服务器证书"面板中,单击"更新服务器证书",然后单击"下一步"。
- 6 在"更新服务器证书"面板中,单击"PKCS12keystore文件(.pfx和.p12)", 然后单击"下一步"。
- 7 在 "PKCS12 Keystore" 面板中,单击"浏览"找到管理服务器上的 PKCS12 Keystore 文件(.pfx 和.p12),或在文本字段中键入此文件的路径名称,然后单击"打开"。
- 8 在 "PKCS12 Keystore" 面板中的 "Keystore 密码" 文本框中键入 Keystore 密码, 然后单击 "下一步"。
- 9 在"管理服务器证书向导已完成"面板中,单击"完成"。

在"管理服务器证书向导已完成"面板中,会出现消息,指明是否成功添加了 服务器证书。

您必须注销然后重新启动管理服务器才能使证书生效。

#### 更新未加密服务器证书和私钥(DER 或 PEM 格式)

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,单击您要为其更新服务器证书的管理服务器。
- 3 在"任务"下,单击"管理服务器证书"。
- 4 在"欢迎使用管理服务器证书向导"窗格中,单击"下一步"。
- 5 在"管理服务器证书"面板中,单击"更新服务器证书",然后单击"下一步"。
- 6 在"更新服务器证书"面板中,单击"证书和私钥文件(DER或PEM格式)", 然后单击"下一步"。
- 7 在"证书文件"面板中,单击"浏览"找出管理服务器上的证书(DER和PEM 格式),或在"证书路径"文本框中键入此文件的路径名称,然后单击"打 开"。
- 8 在"管理服务器证书向导已完成"面板中,单击"完成"。
  在"管理服务器证书向导已完成"面板中,会出现消息,指明是否成功添加了服务器证书。

您必须注销然后重新启动管理服务器才能使证书生效。

## 备份服务器证书

为防管理服务器损坏,您必须备份私钥以及代表证书的文件。

#### 备份服务器证书

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,单击要备份服务器证书的管理服务器。
- 3 在"任务"下,单击"管理服务器证书"。
- 4 在"欢迎使用管理服务器证书向导"窗格中,单击"下一步"。
- 5 在"管理服务器证书"面板中,单击"备份服务器证书",然后单击"下一步"。
- 6 在"备份服务器证书"面板中,键入路径名,或单击"浏览",以找出要将私 钥备份到的文件夹,然后单击"打开"。

请注意,管理服务器证书会备份到相同的文件夹中。

初始安装期间,会备份 JKS Keystore 文件。此外也会备份名称为 server\_*timestamp*.xml 的文件。JKS Keystore文件包括服务器的私钥和公钥 对,以及自我签名证书。

- 7 在"备份服务器证书"面板中,单击"下一步"。
- 8 在"管理服务器证书"屏幕中,单击"完成"。

## 找出 Keystore 密码

发生灾难时,您可能需要找出 Keystore 密码。

有关灾难恢复的详细信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

#### 找出关键字密码

1 打开 Windows 资源管理器,然后找出备份证书文件的文件夹。

Symantec Endpoint Protection Manager 默认会将证书备份于 *install\_directory*:\ Program Files\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup 目录下。

**2** 打开 server\_*timestamp*.xml 文件, 然后找出 Keystore 密码。

# 管理数据库

本章节包括下列主题:

- 关于数据库的管理
- 备份 Microsoft SQL 数据库
- 从控制台按需备份嵌入式数据库
- 从 Symantec Endpoint Protection Manager 调度自动数据库备份
- 还原数据库
- 在 Symantec Endpoint Protection Manager 控制台中编辑数据库的名称和说明
- 重新配置 Microsoft SQL 数据库
- 重新配置嵌入式数据库
- 关于管理日志数据

# 关于数据库的管理

Symantec Endpoint Protection 和 Symantec Network Access Control 支持 Microsoft SQL 或嵌入式数据库。嵌入式数据库通常用于 1000 台或 1000 台以下连接至 Symantec Endpoint Protection Manager 控制台的客户端的组织。更大的组织通常 使用 Microsoft SQL Server 数据库。

如果您安装某个嵌入式数据库,则 Symantec Endpoint Protection Manager 会自动安装该数据库。如果贵公司环境已支持 Microsoft SQL Server,则您可能希望利用现有的硬件和软件。Microsoft SQL Server 通常可支持较大数目的客户端。

数据库包含有关安全和强制执行策略的信息。此外,所有配置设置、关于攻击的数据、日志和报告也都会包含在数据库中。因此,您可以监控网络上的安全威胁。

数据库中的信息会存储在表中,表也称为数据库架构。数据库架构供管理员进行专 门报告之用。

#### 关于数据库命名惯例

Microsoft SQL 数据库会使用与嵌入式数据库不同的命名惯例。

您可以将 Microsoft SQL 数据库安装在装有 Symantec Endpoint Protection Manager 的同一台计算机上,也可以安装在另一台计算机上。在任何一种情况下,Microsoft SQL 数据库都会与安装 Microsoft SQL 数据库服务器的计算机保持相同的名称。

您可以将管理服务器和 Microsoft SQL 数据库安装在同一个名为 PolicyMgrCorp 的 计算机上。此数据库会与安装它的计算机使用相同的名称。数据库名称会显示在 "管理员"页面"查看"下的树中。它也会在"数据库管理"窗格中显示为Microsoft SOL 数据库的数据库地址。

如果您使用嵌入式数据库,数据库的名称会始终为 localhost。

名称 localhost 会显示在"管理员"页面的"查看"下方。它也会在"数据库管理" 窗格中显示为嵌入式数据库的数据库地址。

#### 关于管理服务器配置向导与 Symantec Database Tools

您可以从 Symantec Endpoint Protection Manager 控制台中备份、调度和编辑特 定的数据库设置,例如数据库名称。不过,若要还原和重新配置数据库,就必须使 用管理服务器配置向导和 Symantec Database Backup and Restore 实用程序。

您可以使用管理服务器配置向导来重新配置 Microsoft SQL 数据库和嵌入式数据库的所有设置。

请参见第 237 页的"关于重新配置数据库"。

您可以使用 Symantec Database Tools 实用程序备份、还原及重新配置 Microsoft SQL 数据库和嵌入式数据库的所有设置。

请参见第 236 页的"关于数据库备份"。

#### 关于数据库备份

当您备份数据库时,将创建数据库的单独副本。要定期备份数据库的原因有很多。 因为数据库大小会随着时间增加,所以您需要定期备份数据库。在维护生产数据库

时,备份数据库及删除数据库中未使用的空间是必要的步骤。

若发生数据损坏或硬盘故障等灾难,可以还原数据库的最新快照。如果要获取数据 库的完好副本,您必须恢复到故障发生前的时间点。恢复过程中,部分数据可能需 要重新输入数据库。不过,主要结构和大部分数据会通过使用最近的备份得以保 留。 您可以从 Symantec Endpoint Protection Manager 控制台或使用 Symantec Database Backup and Restore 实用程序备份数据库。Symantec Database Backup and Restore 实用程序会在安装期间自动安装。

您可用下列方式进行备份:

- 仅限 Microsoft SQL 数据库 您可以使用 Microsoft SQL Server Enterprise Manager 设置含自动备份的维护 计划。
- 嵌入或 Microsoft SQL 数据库 您可以从控制台执行按需备份,还可以调度要进行的自动备份。

备份最好存储在单独的磁盘驱动器上。建议您定期备份该磁盘驱动器。

请参见第 238 页的"备份 Microsoft SQL 数据库"。

请参见第 242 页的"从控制台按需备份嵌入式数据库"。

#### 关于重新配置数据库

因下列原因,您可以重新配置 Microsoft SQL 数据库或嵌入式数据库:在多种不同 情况下您必须重新配置数据库:

- 数据库服务器的 IP 地址或主机名称已更改。
- 用来连接到 Symantec Endpoint Protection Manager 的数据库服务器端口已更 改。
- 数据库的名称已更改。

**注意**: 您也可以更改 Symantec Endpoint Protection Manager 中的数据库名称。

请参见第 245 页的"在 Symantec Endpoint Protection Manager 控制台中编辑 数据库的名称和说明"。

- Q限 Microsoft SQL:负责数据库的用户的名称已更改。如果您在数据库服务器 上更改其用户名,Symantec Endpoint Protection Manager 控制台将不能再连 接到此数据库服务器。
- 负责数据库的用户的密码已更改。您可以修改负责数据库服务器的用户的密码。 如果修改密码,则管理服务器将不能再连接到数据库服务器。
- Q限 Microsoft SQL: SQL 客户端路径已更改。默认位于 C:\Program Files\ Microsoft SQL Server\80\Tools\Binn 的 SQL 客户端 bin 文件夹已更改。 如果在 Microsoft SQL 数据库服务器上更改了 SQL 客户端路径,则控制台将不 能再连接到此数据库服务器。
- 将嵌入式数据库升级为 Microsoft SQL 数据库。

请参见第 245 页的"重新配置 Microsoft SQL 数据库"。

请参见第 247 页的"重新配置嵌入式数据库"。

请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安 装指南》。本指南提供如何从嵌入式数据库升级为 Microsoft SQL 数据库的相关信 息。

# 备份 Microsoft SQL 数据库

您可以从 Symantec Endpoint Protection Manager 控制台或 Symantec Database Backup and Restore 实用程序执行 Microsoft SQL 数据库的按需备份。安装 Symantec Endpoint Protection Manager 期间, 会自动安装 Symantec Database Backup and Restore 实用程序。您也可以使用 Microsoft SQL Server 软件随附的数据库维护计 划向导备份 Microsoft SQL 数据库。Microsoft SQL 数据库维护计划向导也可以帮 助您设置备份调度及其他维护任务。

请参见第 238 页的"从 Symantec Endpoint Protection Manager 控制台按需备份 Microsoft SQL 数据库"。

请参见第 239 页的"使用数据库维护向导备份 Microsoft SQL 数据库"。

请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安 装指南》。本指南提供如何使用 Symantec Database Backup and Restore 实用程序 备份 Microsoft SQL 数据库的相关信息。

# 从 Symantec Endpoint Protection Manager 控制台按需备份 Microsoft SQL 数据库

此控制台包含站点备份,可用于备份数据库及日后还原数据库。此外,您可以在 Microsoft SQL Server 代理上设置维护计划。

下列过程包括推荐的设置。

您可能需要使用其他设置,具体取决于下列条件:

- 您组织的规模。
- 保留的供备份用的磁盘空间大小。
- 任何需遵循的公司准则。

从 Symantec Endpoint Protection Manager 控制台按需备份 Microsoft SQL 数据库

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下,单击代表 Microsoft SQL 数据库的图标。

3 在"任务"下,单击"立即备份站点"。

此方法可备份所有的站点数据,包括数据库。您可以在备份期间和备份之后, 检查系统日志以及备份文件夹的状态。

4 单击"关闭"。

#### 使用数据库维护向导备份 Microsoft SQL 数据库

Microsoft SQL Server Enterprise Manager 提供了一个用于帮助设置数据库维护计 划的向导。您可以使用数据库维护向导来管理数据库及调度 Microsoft SQL 数据库 的自动备份。

注意:确认 SQL Server 代理已启动。

若要运行数据库维护计划向导,您需要 Sysadmin 访问权限。

参见 Microsoft SQL Server 文档,了解有关如何维护 Microsoft SQL Server 数据库 的详细信息。

#### 使用 Microsoft SQL Sever 2000 Enterprise Manager 中的数据库维护向导备份 Microsoft SQL 数据库

- 在 SQL Server Enterprise Manager 上,单击"程序">Microsoft SQL Server
  "企业管理器"。
- 2 展开服务器名称,其中"服务器名称"是安装数据库的服务器名称。
- **3** 双击"管理"文件夹。

如果 SQL Server 代理已启动,图标旁会出现绿色箭头。如果未启动,请选择 SQL Server 代理并单击鼠标右键,然后选择 "启动"来启动 SQL Server Service Manager。

- **4** 展开"数据库"。
- 5 右键单击 sem5 并选择"所有任务" > "维护计划"。
- 6 在"欢迎使用数据库维护计划向导"屏幕上,单击"下一步"。
- 7 在"选择数据库"屏幕上,选择"以下数据库:"并选中旁边的 sem5来备份数 据库。然后单击"下一步"。
- 8 在"更新数据优化信息"屏幕上,选择"从数据库文件中删除未使用的空间"。
- 9 在"增长超过:"文本框中,键入1024或适当的最大大小(具体取决于您组织的大小)。

如果数据库超过指定大小,会自动删除未使用的空间。

**10** 在"收缩后保留的可用空间"文本框中,选择**"20%的数据空间"**或者选择适 合公司需要的其他数量。 **11** 数据会每周进行优化,并且会指定可接受的默认值。如果您要更改调度,可单击"更改"。

在出现的"编辑重复执行的作业计划"对话框中,指定要从数据库删除未使用 空间的频率及时间,然后单击"确定"。

- 12 在完成优化设置后,单击"下一步"。
- **13** 在"数据库完整性检查"屏幕上,单击"下一步"而不设置此选项,因为 Symantec Endpoint Protection Manager 将维护数据库完整性。
- 14 在"指定数据库备份计划"屏幕上,选中"作为维护计划的一部分来备份数据 库"和"完成时验证备份的完整性"。
- 15 选择用来存储备份的介质。
- 16 单击"更改"以修改备份调度。
- 17 在"编辑重复执行的作业计划"对话框中,在"执行"后面单击"每天"。选择数据库需要备份的频率。建议选择"每1天"。
- 18 选中"启用调度"。
- 19 设置您要进行备份的时间。您还可以选择开始日期和结束日期,必要时也可选择"无结束日期",然后单击"确定"。
- 20 单击"下一步"。
- 21 在"指定备份磁盘目录"屏幕上,单击"使用默认备份目录"(默认路径为 \MSSQL\BACKUP)或"使用此目录"以选择备份目录。
- 22 选择您要复制文件的目标目录。

目录必须位于与数据库所在的相同计算机上。您需要将备份导向至其他磁盘驱动器。

- 23 选中"为每个数据库都创建一个子目录"。
- 24 单击"删除文件,如果其保留时间超过",然后指定时间间隔,超过此时间间 隔的旧备份将自动移除或删除。

请确认您有足够的磁盘空间可存储所指定时间间隔之内的备份,然后单击"下 一步"。

25 按如下所示说明进行操作:

如果您在配置数据库服务器期间选择了自 继续步骤 41。 动维护 Sem5 数据库

如果"恢复模式"对话框显示"简单" 继续步骤 41。

如果"恢复模式"对话框显示"完整" 继续步骤 26。

- 26 在"指定事务日志备份计划"屏幕,选中"作为维护计划的一部分来备份数据 库事务日志"。
- 27 选择用来存储备份的介质。
- 28 单击"更改"以修改备份事务日志的调度。

会出现"编辑重复执行的作业计划"对话框。

事务日志的最大大小在默认情况下会设置为8GB。如果事务日志达到最大大小,将不再有任何作用,而数据库可能会损坏。(您可以在 SQL Server Enterprise Manager 更改事务日志的最大大小。)

29 在"执行"后面单击"每天"。

选择事务日志需要备份的频率。建议选择"每1天"。务必选中"启用调度"。

- 30 选择进行备份的频率。 建议使用默认选项"每4小时执行"。
- 31 选择开始日期与结束日期,必要时选择"无结束日期",然后单击"确定"。
- 32 单击"下一步"。
- **33** 在"指定备份磁盘目录"屏幕上,单击"使用默认备份目录"或"使用此目 录"来选择备份目录。

默认路径为\MSSQL\BACKUP。

- 34 选择您要复制文件的目标目录。
- 35 选中"为每个数据库都创建一个子目录"。
- 36 单击"删除文件,如果其保留时间超过:"
- 37 指定时间间隔,超过此时间间隔的旧备份将自动移除或删除。 请确认您有足够的磁盘空间可存储所指定时间间隔之内的备份,然后单击"下 一步"。
- **38** 在"要生成的报表"屏幕上,选中**"将报告写入目录中的文本文件"**。 指定要生成报告的文本文件的完整路径及名称。
- 39 选中"删除文本报告文件,如果其保留时间超过",并将其设置为4周。
- **40** 选中"将电子邮件报表发送到操作员",并指定通过SQL邮件将生成的报告投 递给哪一位系统管理员。如果电子邮件操作员不可用,则选择"新建操作员", 然后单击"下一步"。
- 41 在"维护计划历史记录"屏幕中,单击"下一步"。 您应该使用维护计划历史记录的默认设置,除非您需要更改设置。

- 42 在"正在完成数据库维护计划历史记录"屏幕上,键入维护计划的名称,如 SQL Database Maintenance,然后单击"完成"。
- 43 在计划完成时,查看计划创建成功的消息,然后单击"确定"。

# 从控制台按需备份嵌入式数据库

您可以从控制台按需备份嵌入式数据库。

请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安 装指南》。该指南提供有关如何使用 Symantec Database Backup and Restore 实用 程序备份嵌入式数据库的信息。

#### 从控制台备份嵌入式数据库

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下,单击代表嵌入式数据库的图标。
- 3 在"任务"下,单击"立即备份站点"。

此方法可备份所有站点数据,包括数据库。您可以在备份期间和备份之后,检 查系统日志以及备份文件夹的状态。

- 4 "备份"消息出现时,单击"是"。
- 5 单击"关闭"。

# 从 Symantec Endpoint Protection Manager 调度自动 数据库备份

您可以在 Symantec Endpoint Protection Manager 中创建 Microsoft SQL 和嵌入式 数据库两者的自动备份调度。

您可以在 Symantec Endpoint Protection Manager 中按需备份数据库,或设置调 度来自动备份 Microsoft SQL 和嵌入式数据库。不过,您也可以使用 Microsoft SQL Server 的数据库维护向导来设置 Microsoft SQL 数据库的自动备份调度。此外,您 也可以使用 Symantec Database Backup and Restore 实用程序来备份 Microsoft SQL 数据库或嵌入式数据库。

请参见第 238 页的"从 Symantec Endpoint Protection Manager 控制台按需备份 Microsoft SQL 数据库"。

请参见第 242 页的"从控制台按需备份嵌入式数据库"。

请参见第 239 页的"使用数据库维护向导备份 Microsoft SQL 数据库"。

请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安 装指南》。本指南提供如何使用 Symantec Database Backup and Restore 实用程序 备份 Microsoft SQL 数据库的相关信息。

#### 从控制台备份嵌入式数据库

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下,单击表示 Microsoft SQL 或嵌入式数据库且要更改其备份设置的图标。
- 3 在"任务"下方,单击"编辑备份设置"。
- 4 在"本地站点的备份站点"对话框中,单击"调度备份"。
- 5 选择"每小时"、"每日"或"每周",然后指定下列选项之一,从而指定备 份频率:
  - 若选择"每小时",则请在"开始时间"框中指定要在每个整点的几分进 行备份。
  - 若选择"每日",请在"开始时间"框中指定要在每日的什么时间进行备份。
  - 若选择"每周",则请在"开始时间"框中指定要在几点几分进行备份。
  - 如果选择"每周",请指定"每周的",以指出应在星期几执行备份。
- 6 单击"确定"。

在调度的时间,备份会自动执行,并将备份文件置于带有备份执行日期的.zip 文件中。备份文件会存储于在指定为服务器数据根目录的路径中创建的备份文 件夹中。

例如,在 2007 年 8 月 1 日 9:46 AM 创建的备份文件便命名为 2007-Aug-01\_09-46-13-AM.zip。

## 还原数据库

如果数据库不再正常工作,那么如果您先前已经备份该数据库,则可以将其还原。

#### 还原数据库

- 1 找出您具有的最新备份文件。这个文件的格式为.zip并标记有日期。文件存储 在指定为服务器数据根目录的路径中创建的备份文件夹中。
- 2 使用下列策略之一设置要还原数据库的计算机
  - 使用另一台计算机 如果先前计算机上的硬件出现故障,您需要将操作系统和SymantecEndpoint Protection Manager 安装在新计算机上。即使您使用新数据替换数据库, 仍须在安装完成之后配置数据库。

- 使用同一台计算机 如果硬件与 Symantec Endpoint Protection Manager 能够正常工作,即可 用同一台计算机还原数据库。如果遇到问题,可能需要卸载 Symantec Endpoint Protection Manager 并重新安装它,再配置数据库,然后还原数 据。
- 3 注销 Symantec Endpoint Protection Manager 控制台。
- 4 选择"开始">"程序">"管理工具">"服务"来停止 Symantec Endpoint Protection Manager 服务。
- **5** 找到 Symantec Endpoint Protection Manager 服务, 然后单击鼠标右键选择 "停止"。
- 6 选择"开始">"程序">Symantec Endpoint Protection Manager>"数据 库备份及还原"。
- 7 单击"还原",再在显示的消息上单击"是"。
- 8 在"正在还原数据库"对话框中,从列表中选择要使用的备份。
- 9 单击"确定"。

数据库还原需要几分钟的时间。完成任务所需的时间会视数据库的大小、用户人数、复制伙伴以及其他条件而定。

10 数据库还原一旦完成,会出现以下消息:

成功还原数据库。

- 11 单击"退出"。
- 12 如果是在其他计算机上还原数据库,请单击"开始">"程序">Symantec Endpoint Protection Manager,因为您需要删除旧的数据库服务器。如果不 是,您已经完成数据库的还原。
- 13 登录控制台。
- 14 单击"管理员"。
- 15 单击"服务器"。
- 16 在"管理员"页面的"任务"下方,右键单击旧数据库服务器,再选择"删除"。
- 17 视需要重新配置其他条件,例如用户名和密码。

请参见第 245 页的"重新配置 Microsoft SQL 数据库"。

# 在 Symantec Endpoint Protection Manager 控制台中 编辑数据库的名称和说明

您可以编辑本地或远程数据库的名称及说明。

您也可以使用"管理服务器配置向导"来编辑数据库的名称。

请参见第 245 页的"重新配置 Microsoft SQL 数据库"。

#### 编辑数据库的名称和说明

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,展开"本地站点"。
- 3 选择本地数据库, 或展开"远程站点", 选择要编辑属性的远程站点数据库。
- 4 在"任务"下方,单击"编辑数据库属性"。
- 5 在"数据库属性"对话框的"名称"字段中,编辑数据库名称。
- 6 在"数据库属性"对话框的"说明"字段中,编辑数据库说明。
- 7 单击"确定"。

## 重新配置 Microsoft SQL 数据库

您需要使用"管理服务器配置向导"来重新配置 Microsoft SQL 数据库。 请参见第 237 页的"关于重新配置数据库"。

#### 重新配置 Microsoft SQL 数据库

- **1** 通过依次选择 "开始" > "所有程序" > "管理工具" > "服务" 来停止 Symantec Endpoint Protection Manager 服务。
- **2** 找到 Symantec Endpoint Protection Manager, 然后右键单击以选择"停止"。
- 3 单击"开始">"所有程序">Symantec Endpoint Protection Manager>"管理服务器配置向导"。
- 4 在"欢迎使用管理服务器配置向导"屏幕中,单击"重新配置管理服务器"。
- 5 单击"下一步"开始重新配置。
- **6** 在"服务器名"框中,编辑安装 Symantec Endpoint Protection Manager 的 计算机名称。
- 7 在"服务器端口"框中,编辑 Symantec Endpoint Protection Manager 监听的 HTTPS 端口号。

默认的端口号为8443。

8 编辑服务器数据文件夹的位置,或浏览到数据文件所在的根文件夹。 根文件夹包括备份、复制和其他 Symantec Endpoint Protection Manager 文件。

默认路径名称为 C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data。

- 9 单击"下一步"。
- 10 单击 Microsoft SQL Server。
- 11 单击"下一步"。
- 12 如适用,请在"数据库服务器"框中,键入数据库服务器的名称。

键入 SQL Server Enterprise Manager (SEM) 服务器保存应用程序数据的数据 库服务器 IP 地址或主机名称。

- 在 "SQL Server 端口" 框中, 键入 SQL 服务器端口号。
  默认的端口号为 1433。
- 14 在"数据库名称"框中键入数据库的名称。 存储应用程序数据的 Microsoft SOL 数据库的名称。
- 15 在"用户"框中键入用户名。 此名称表示负责数据库的用户。
- 16 在"密码"字段中键入密码。

这是数据库用户的密码。此字段不能为空。

17 在 "SQL 客户端路径" 中键入 SQL 客户端路径名称。

默认情况下, SQL 客户端 bin 文件夹含有 bcp.exe 文件。例如, C:\Program Files\Microsoft SQL Server\80\Tools\Binn。

bcp.exe 文件必须位于安装 Symantec Endpoint Protection Manager 的同一台 计算机上。此文件为 SQL Server 客户端软件包的一部分。您还必须在管理服 务器配置向导中正确指定 Microsoft SQL 客户端路径名称。如果未正确指定路 径名称或从未安装 Microsoft SQL 客户端软件包,则无法重新配置数据库。

18 单击"下一步"。

数据库便会创建。此过程只需数分钟。如果 Symantec Endpoint Protection Manager 服务仍在运行中,则在这段时间内会显示数据库消息。

**19** 您可以选择"启动 Symantec Endpoint Protection Manager"和"启动管理控制台"。

这些选项在默认情况下处于选中状态。

20 单击"完成"。

此时即完成数据库的重新配置。如果使启动选项保持选中状态,则会出现控制 台登录屏幕。

# 重新配置嵌入式数据库

您必须使用 Symantec 管理服务器配置向导来重新配置数据库。

请参见第 237 页的"关于重新配置数据库"。

#### 重新配置嵌入式数据库

- 1 选择"开始">"程序">"管理工具">"服务"来停止 Symantec Endpoint Protection Manager 服务。
- 2 找到 Symantec Endpoint Protection Manager, 然后右键单击以选择"停止"。
- 3 单击"开始">"程序">Symantec Endpoint Protection Manager>"管理 服务器配置向导"。
- 4 在"欢迎使用管理服务器配置向导"屏幕中,单击"重新配置管理服务器"。
- 5 单击"下一步"开始重新配置。
- **6** 在"服务器名"框中,编辑安装 Symantec Endpoint Protection Manager 的 计算机名称。
- **7** 在"服务器端口"框中,编辑 Symantec Endpoint Protection Manager 监听的 HTTPS 端口号。

默认的端口号为8443。

8 编辑服务器数据文件夹的位置,或浏览到数据文件所在的根文件夹。

根文件夹包括备份、复制和其他 Symantec Endpoint Protection Manager 文件。

默认路径名称为 C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data。

- 9 单击"下一步"。
- 10 单击"嵌入式数据库"。
- 11 单击"下一步"。
- 12 在"数据库服务器端口"框中,键入服务器端口号。 默认的端口号为 2638。

13 在"密码"框中键入密码。

此字段不能为空。

- 14 在"确认密码"框中再次键入密码。
- 15 单击"下一步"。

创建数据库可能需要几分钟时间。如果 Symantec Endpoint Protection Manager 服务仍在运行中,则在这段时间内会显示数据库消息。

16 您可以选择"启动 Symantec Endpoint Protection Manager"和"启动管理控 制台"。

这些选项在默认情况下处于选中状态。

17 单击"完成"。

此时即完成数据库的重新配置。如果使启动选项保持选中状态,则会出现控制 台登录屏幕。

# 关于管理日志数据

您可以配置多个选项来管理存储在数据库中的日志。

#### 关于日志数据和存储区

从所有日志上载到 Symantec Endpoint Protection Manager 控制台的数据都会存储在控制台数据库中。

来自下列类型日志的数据会存储在数据库的两个表中:

- 应用程序与设备控制日志
- 审核日志
- Enforcer 日志
- 网络威胁防护日志
- 系统日志

来自其他日志的数据会存储在单个表中。

您可以设置日志选项,以管理存储在两个表中的数据库日志。

请参见第 250 页的"为站点中的服务器配置日志设置"。

您可以使用站点属性中的数据库维护选项管理包括来自其他日志数据的单个表。您 可以设置会影响存储在单个表中的数据的数据库维护选项。

请参见第 254 页的"配置日志的数据库维护选项"。

至于存储在两个表中的日志,其中一个表(表A)是当前的日志表。新的日志条目 会写人这个表。当到达日志阈值或过期日期时,新的日志条目会存储在第二个表 (表B)中。在表B到达阈值或到达"到期时间"字段中指定的天数之前,数据都 会保留在表A内。到达以上指定时间后,表A会彻底清除,并将新条目保存在表 A。表B中的信息会一直保留到切换发生为止。表的切换(也称为从数据库清除日 志)会自动发生。切换时间取决于您在站点属性中设置的日志设置。不论清除是自 动或手动进行的,过程都是相同的。

如果您更倾向于在进行例行数据库维护时手动清除日志,则可以在备份数据库后执行清除。

如果您允许自动清除,而又不常进行数据库备份,则可能会丢失部分日志数据。如 果您定期在执行数据库备份后执行手动日志清除,则可以确保所有日志数据的完好 保留。如果您必须将日志保留一段较长的时间(例如一年),这种程序就极为有 用。

**注意**:从数据库手动清除日志数据中介绍的手动操作程序不会影响保存在数据库内 单个表中的日志数据。

#### 从数据库手动清除日志数据

您可以手动清除日志,但此为可选过程,您并非一定要执行。

#### 从数据库手动清除日志数据

 为避免备份前自动进行数据库清除,可以将站点属性上的日志设置增大至最大 值。

请参见第 250 页的"为站点中的服务器配置日志设置"。

- 2 在适当的时候运行备份。
- **3** 在安装 Symantec Endpoint Protection Manager 的计算机上打开 Web 浏览器,并键入下列 URL:

#### https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action =SweepLogs

执行此任务后,所有类型日志的条目都会保存在备用数据库数据表中。在下一次清除开始之前,原始表都不会被清除。

- **4** 要清空所有条目,而仅保留最新条目,请再次执行清除。原始表也会清除,然 后会再次存储条目。
- 5 请记得将站点属性的日志设置恢复为您首选的值。

## 来自旧版客户端的日志数据

Symantec Endpoint Protection 报告功能使用临时文件夹(即 drive:\Symantec\ Symantec Endpoint Protection Manager\Inetpub\Reporting\Temp)来实现多个 目的。有些管理员可能想要调度自己的自动化任务,定期清理此临时文件夹。如果 要这样做,请确保不会删除LegacyOptions.inc文件(如果有)。如果删除此文件, 将会失去来自旧版 Symantec AntiVirus 客户端日志的传入数据。

## 为站点中的服务器配置日志设置

为了有助于控制磁盘空间的使用,您可以配置可以在站点服务器的日志上保留的条 目数。您也可以配置这些条目保留的天数。您可以为不同的站点配置不同的设置。

**注意:** "监视器"页面中 Symantec Endpoint Protection Manager 控制台"日志" 选项卡上的日志信息会以逻辑组的形式呈现,以此方便您的查看。"站点属性"的 "日志设置"选项卡上的日志名称会与日志内容一一对应,而不会和"监视器"页 面中"日志"选项卡上的日志类型对应。

如需每个配置选项的说明,可在控制台上单击该报告类型的"更多信息"链接。 "更多信息"会显示上下文关联帮助。

#### 为站点中的服务器配置日志设置

- 1 在控制台中,单击"管理员"。
- 2 单击左下角的"服务器"。
- 3 选择要配置的站点。
- 4 在"任务"下方,单击"编辑站点属性"。
- 5 在"日志设置"选项卡上,为每个类型的日志设置可以保留的条目数和这些条 目可以保留的天数。

您可以设置管理服务器日志、客户端日志和 Enforcer 日志的大小。

6 单击"确定"。

#### 关于配置事件汇总

在 Symantec Endpoint Protection Manager 控制台的两个位置中,您可以配置客 户端日志的事件聚合。

表 20-1 说明在何处配置客户端事件汇总,以及设置所代表的意义。

表 20-1	客户端事件汇总

位置	说明
在"策略"页面上,依次选择"防 病毒和防间谍软件策略"、"其 他"、"日志处理"选项卡	在这个位置可配置风险事件的汇总。默认汇总时间为5 分钟。事件第一次发生时会立即记录。后续若发生相同 事件,则会汇总起来,客户端会每5分钟记录一次出现 次数。
在"客户端"页面上,依次选择 "策略"页面、"客户端日志设 置"	在这个位置可配置网络威胁防护事件的汇总。所有事件 在汇总为单个事件并上传至控制台之前,在客户端上保 留的时间长度都为一个调节器周期。调节器周期有助于 将事件减少至可管理的数量。默认调节器周期设置为 "自动"。.调节器空闲期间用于决定前后两个日志条目 必须间隔的时间,只有在此时间过后下一发生的事件才 能视为新的条目。默认调节器空闲时间为10秒。

请参见第 327 页的"在防病毒和防间谍软件策略中设置日志处理参数"。

请参见第 251 页的"配置客户端日志设置"。

#### 配置客户端日志设置

如果您安装了 Symantec Endpoint Protection,就可以配置一些客户端日志选项。 您可以配置日志中要保留的条目数,以及每个条目保留在客户端上的天数。 您可以为下列客户端日志配置设置:

- 控制
- ∎ 数据包
- 风险
- 安全性
- 系统
- ∎ 通信

如果您安装了 Symantec Network Access Control,您就可以启用和禁用记录,并 可以将 Enforcer 日志发送到管理服务器。您可以配置日志条目数和条目保留在客户 端上的天数。

有关 Enforcer 日志的详细信息,请参见《Symantec Network Access Control Enforcer 操作指南》。

对于安全性、风险和通信日志,您还可以配置用于事件汇总的调节器时间段和调节 器闲置时间段。

您可以配置是否要将每种类型的客户端日志上载到服务器,以及上载的大小上限。

如果您选择不上载客户端日志,则会有以下结果:

- 您不能从 Symantec Endpoint Protection Manager 控制台使用"监控"窗格中的"日志"选项卡查看客户端日志数据。
- 您不能在备份数据库时备份客户端日志。
- 您不能将客户端日志数据导出至文件或集中式日志服务器。

#### 配置客户端日志设置

- 1 在控制台上,单击"客户端"。
- 2 在"策略"选项卡的"与位置无关的策略与设置"下方,单击"设置"下的 "客户端日志设置"。
- 3 在"用于 <组名称>的客户端日志设置"对话框中,设置最大文件大小和保留 日志条目的天数。
- 4 对任何要让客户端转发至服务器的日志选中"上载到管理服务器"。
- 5 对于安全日志和通信日志,设置调节器时间段和调节器闲置时间段。 这些设置会决定网络威胁防护事件汇总的频率。
- 6 设置客户端一次上载到管理器的最大条目数。
- 7 单击"确定"。

#### 关于配置防病毒和防间谍软件策略的客户端日志处理选项

您可以配置下列防病毒和防间谍软件策略的日志处理选项:

- 哪些防病毒和防间谍软件事件将从客户端转发到服务器上的防病毒和防间谍软件防护日志
- 防病毒和防间谍软件防护日志中的事件要保留在服务器上多长时间
- 将汇总事件从客户端上传到服务器的频率

请参见第 327 页的"在防病毒和防间谍软件策略中设置日志处理参数"。

#### 备份站点日志

在配置 Symantec Endpoint Protection 来备份日志数据之前不会备份日志数据。如 果不备份日志,则备份期间只会保存日志配置选项。您可以使用备份还原数据库, 但数据库中的日志在还原之后将不会有任何数据。

此配置选项与本地站点的其他备份选项位于"管理员"页面的"服务器"页面上。 您最多可以选择保留十个版本的站点备份。如果选择保留多个版本,则应确保有足够的磁盘空间来存放所有数据。
#### 备份站点日志

- 1 在控制台上,单击"管理员"。
- 2 选择数据库服务器。
- 3 在"任务"下方,单击"编辑备份设置"。
- 4 在"备份设置"组框中,选中"备份日志"。
- 5 单击"确定"。

#### 关于上传大量客户端日志数据

如果您有许多客户端,可能会生成大量的客户端日志数据。 请考虑是否要使用下列配置来减少数据量:

- 只将部分客户端日志上传到服务器。
  请参见第 251 页的"配置客户端日志设置"。
- 过滤掉重要性较低的风险事件和系统事件,减少转发到服务器的数据。
  请参见第 327 页的"在防病毒和防间谍软件策略中设置日志处理参数"。

如果您仍打算将非常大量的客户端日志数据上传到服务器,则必须考虑下列因素:

- 网络中的客户端数目
- 检测信号频率,这会控制客户端日志多久上传一次到服务器
- 在日志数据插入数据库之前,存储日志数据的目录空间

若您配置将大量客户端日志数据频繁上传到服务器,可能会导致空间不足问题。如果您必须上传大量客户端日志数据,可能就需要调整某些默认值以避免发生空间不足的问题。当您部署到客户端时,请监控服务器上日志插入目录的空间,并视需要调整这些值。日志转换成.dat文件并写入数据库的默认目录为*drive*.\Program Files\ Symantec\Symantec Endpoint Protection Manager\data\inbox\log。进行安装时,会要求您选择服务器数据文件夹,服务器数据目录的位置就是在那时设置的。 您可以从"开始"菜单运行"管理服务器配置向导",视需要更改此目录。\inbox\log 目录会自动添加到您设置的目录。

客户端日志上传的频率是在"客户端"页面的"策略"页面的"通信设置"下配置的。默认频率为每五分钟上传日志一次。

若要调整控制服务器上可用空间的值,您必须在注册表中更改这些值。需要更改的 注册表项位于服务器上的 HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\ Symantec Endpoint Protection\SEPM 中。

表 20-2 列出注册表项及其默认值,并对其作用进行了说明。

值名称	默认与说明
MaxInboxSpace	MaxInboxSpace 指定分配给目录的空间,日志档案会在 此目录中转换成.dat 文件,之后再存储到数据库。 默认值为 200 MB。
MinDataFreeSpace	MinDataFreeSpace指定此目录应保持可用的最小空间。 此键可确保使用同一个目录的其他应用程序有足够的运 行空间,而不会对性能造成负面影响。 默认值为0。
IntervalOfInboxSpaceChecking	IntervalOfInboxSpaceChecking 指定 Symantec Endpoint Protection 在检查完收件箱中可供日志数据使用的空间 之后,应等待多久再进行下次检查。 默认值为 30 秒。

#### 表 20-2 包括日志上传设置的注册表项

## 关于管理数据库中的日志事件

数据库会接收持续生成的条目,并将这些条目存储到日志文件中。您必须管理存储 在数据库中的数据,这样存储的数据才不会耗尽所有可用的磁盘空间。数据过多 时,会造成运行数据库的计算机崩溃。

您应该了解默认的数据库维护设置,并在数据库所用的磁盘空间不断增加时更改这 些设置。如果风险活动极多,您可能需要删除一些数据才能为服务器保留一定的可 用磁盘空间。

#### 配置日志的数据库维护选项

管理员可以为存储在日志中的数据配置数据库维护选项。通过数据库维护选项,您 可指定压缩设置及数据的保留时间,从而可以管理数据库的大小。

如需特定数据库维护选项的相关信息,请参见"'站点名称'的站点属性"对话框的 "数据库"选项卡中的上下文相关帮助。

#### 配置日志的数据库维护选项

- 1 在控制台上,单击"管理员"。
- 2 选择站点。
- 3 在"任务"下方,单击"编辑站点属性"。
- 4 在"数据库"选项卡上,设置风险事件的保留天数。

若要继续保留超过您对风险事件所设置阈值的风险感染事件子集,请选中"不 要删除感染事件"复选框。

- 5 设置您要将发现相同风险的事件压缩为单个事件的频率。
- 6 设置已压缩事件的保留天数。

此值包括事件压缩之前已保留的时间。例如,假设您指定要删除保留时间超过 十天的压缩事件,并指定要压缩保留时间超过七天的事件。在此情况下,事件 在压缩后三天便会删除。

- 7 设置已确认和未确认通知的保留天数。
- 8 设置扫描事件的保留天数。
- 9 设置从控制台运行的命令及其相关命令状态信息保留的天数。经过此时间之 后,Symantec Endpoint Protection 不会再将这些命令分发至其指定的收件 人。
- **10** 如果您要删除未使用的病毒定义及含有 EICAR 为病毒名称的病毒事件,请选中 相应复选框。

EICAR测试病毒是欧洲计算机防病毒研究协会(European Institute for Computer Anti-Virus Research, EICAR)所开发的文本文件,该测试病毒为测试大多数的防病毒软件提供了一种简单而又安全的方式。您可以从EICAR网站下载此文件。您可以使用它来确认 Symantec Endpoint Protection 防病毒部分的工作情况。

11 单击"确定"。

## 关于使用 Interactive SQL 实用程序搭配嵌入式数据库

如果您选择将嵌入式数据库与 Symantec Endpoint Protection 或 Symantec Network Access Control 搭配使用,请注意下列信息。当您运行名为 Interactive SQL (dbisqlc.exe) 的数据库应用程序时,它会禁止数据插入嵌入式数据库。如果使用这个应用程序一段时间,.dat文件会累积在 *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\inbox\log 目录中。为避免.dat 文件累积,并要重新开始将数据插入数据库,请关闭该应用程序。

#### 更改超时参数

如果查看含有大量数据的报告或日志时数据库出现错误,您可以进行下列更改:

- 更改 Microsoft SQL Server 连接超时
- 更改 Microsoft SQL Server 命令超时

这些值的报告默认设置如下:

- 连接超时时间为 300 秒 (5分钟)
- 命令超时时间为 300 秒(5分钟)

如果收到 CGI 或终止进程错误,您最好更改其他超时参数。请参见 Symantec 知识 库中标题为 Reporting server does not report or shows a timeout error message when querying large amounts of data 的文章。

#### 更改超时参数

- **1** 打开 Reporter.php 文件,此文件位于 \Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Resources 目录下。
- 2 使用任何文本编辑器将下列设置添加到文件中:
  - \$CommandTimeout =*xxxx*
  - **\$ConnectionTimeout = xxxx** 超时值使用秒为单位。如果您将相应值指定为零,或将相应字段保留为空, 则会使用默认值。

## 关于在 64 位计算机上还原损坏的客户端系统日志

如果 64 位客户端上的系统日志发生损坏,则可能会在 Symantec Endpoint Protection Manager 控制台上的系统日志中看到未指定的错误消息。客户端上的日志损坏时,您便不能查看其中的数据,且数据不会上传至控制台。此情况可能会影响控制台"计算机状态"、"风险"及"扫描"日志与报告中的数据。

若要更正此情况,您可以删除客户端上损坏的日志文件以及 serialize.dat 文件。这些文件位于客户端的 Drive:\Documents and Settings\All Users\Application Data\ Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\*date*.Log 中。删除这些文件之后,系统会重新创建日志文件,并开始正确记录日志条目。

# 21

## 复制数据

本章节包括下列主题:

- 关于数据的复制
- 关于复制的影响
- 添加和断开复制伙伴
- 调度自动和按需复制
- 复制客户端软件包
- 复制日志

## 关于数据的复制

复制是在数据库之间共享信息的过程,可确保内容一致。您可以使用复制,增加可 供客户端使用的数据库服务器数量,藉此降低每台服务器的负载。复制通常在初始 化安装期间设置。

有关如何在初始化安装期间设置数据复制的详细信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

复制伙伴是具有一台数据库服务器的另一个站点,也会连接至您指定为主要站点或本地站点的站点。一个站点可视其需要有不限数目的复制伙伴。所有的复制伙伴会共享公共的授权密钥。每当调度 Symantec Endpoint Protection Manager 来复制数据时,您在任何复制伙伴上所做的更改都会复制到所有其他复制伙伴。

例如,您可能会想要在主要办公室设置一个站点(站点1)和第二个站点(站点2)。站点2是属于第一个站点的复制伙伴。站点1及站点2上的数据库会根据您设置的同步处理调度进行重新同步。如果在站点1上进行了更改,在运行复制之后,该更改会自动显示在站点2上。如果在站点2上进行了更改,在运行复制之后,该更改会自动显示在站点1上。您也可以安装第三个站点(站点3),以便从站点1或站点2复制数据。第三个站点是另外两个站点的复制伙伴。

站点 1 站点 2 Symantec Symantec Endpoint Endpoint Protection Manager Protection Manager MS SQL MS SQL 数据库 数据库 复制 站点 3 复制 Symantec Endpoint Protection Manager MS SQL 数据库

图 21-1 说明如何将本地站点的数据复制到其他两个站点。

#### 图 21-1 站点复制伙伴

复制伙伴在"管理员"页面上列出。选择树中的复制伙伴,即可显示关于伙伴的信息。所有站点通常具有相同类型的数据库。不过您可以使用不同类型的数据库来设置站点之间的复制。此外,您也可以设置嵌入式数据库和 MS SQL 数据库之间的复制。

如果您使用嵌入式数据库,则因为配置要求只能连接一个 Symantec Endpoint Protection Manager。如果使用 MS SQL 数据库,则可以连接多个 Symantec Endpoint Protection Manager 或共享一个数据库。只有第一个 Symantec Endpoint Protection Manager 需要设置为复制伙伴。

所有设置为复制伙伴的站点都可以视为位于相同站点场中。一开始,您可以安装第 一个站点,然后安装第二个站点作为复制伙伴。第三个站点安装后可设置为连接到 前两个站点中的一个。您可以根据需要将任意数目的站点添加到站点场。

您可以删除复制伙伴,以停止复制。您可以稍后重新添加复制伙伴,让数据库保持 一致。但是,某些更改可能相互冲突。

请参见第 259 页的"关于复制的设置"。

您可以在初始安装期间或在稍后的时间设置数据复制。当您在初始安装期间设置复制时,也可以设置复制伙伴之间同步处理的调度。

## 关于复制的影响

如果管理员同时对每一个复制站点进行更改,则可能会丢失某些更改。如果在两个站点上更改了相同设置而发生了冲突,那么复制时生效的将是最后所做的更改。

例如,站点1(纽约)复制站点2(东京),而站点2复制站点3(伦敦)。您希望 连接至纽约网络的客户端也连接至纽约的Symantec Endpoint Protection Manager。 但是,您不希望客户端连接至东京或伦敦的Symantec Endpoint Protection Manager。

#### 关于复制的设置

在设置复制时,客户端通信设置也会一并复制。因此,您需要按照下列方式确认, 通信设置对于站点场中的所有站点都正确无误:

- 创建常规通信设置,以便客户端根据连接类型进行连接。例如,针对站点场中的所有站点,您可以使用 symantec.com 之类的通用 DNS 名称。只要客户端进行连接,DNS 服务器便会解析名称,并且将客户端连接至本地的 Symantec Endpoint Protection Manager。
- 通过将组分配至站点来创建特定的通信设置,以便组中的所有客户端均连接至指定的 Symantec Endpoint Protection Manager。
  例如,您可以在站点1上为客户端创建两个组、为站点2创建两个不同的组,并为站点3上创建另外两个组。可以在组级别应用通信设置,以便客户端连接至指定的 Symantec Endpoint Protection Manager。

您可能希望为管理组的位置设置而设置指导方针。这些指导方针有助于避免在相同位置发生冲突。这也有助于避免位于不同站点的任何组发生冲突。

## 复制期间如何合并更改

在进行复制之后,站点1上的数据库及站点2上的数据库会彼此相同。只有服务器 的计算机标识信息会不同。

如果管理员更改站点场中所有站点上的设置,则可能会发生冲突。例如,站点1和 站点2的管理员都添加相同名称的组。若要解决此冲突,则复制之后两个组将同时 存在。不过,其中一个使用波浪号~加数字1(~1)重命名。

如果两个站点都添加了一个称为 Sales 的组,在复制之后您会在两个站点看见两个组。一个组称为 Sales,另一个为 Sales 1。当同名的策略添加到两个站点的相同位置时,就会发生重复的情况。

如果在不同的站点创建了同名的重复网络适配器,则会加上波浪号与数字1(-1)。 这两个符号会加到其中一个名称中。

如果在两个站点上更改不同的设置,更改会在复制后合并。例如,如果您在站点1 上更改"客户端安全设置",并且在站点2上更改"密码保护",两组更改在复制 后都会显示。如果可能,两个站点的更改会合并。

如果在两个站点添加策略,新的策略会在复制后出现在两个站点上。如果在两个不 同的站点更改相同的策略,则会发生冲突。如果在多个站点上更改了策略,则最后 一次更新的所有更改会在复制后会保持下来。

如果复制被调度为每小时发生一次,并且您在以下时间执行下列任务:

- 在下午 2:00 编辑站点 1 上的 AvAsPolicy1。
- 在下午 2:30 编辑站点 2 上的同一个策略。

那么在下午 3:00 运行复制并且复制完成后,只有在站点 2 上所做的更改会保持下来。

如果其中一个复制伙伴脱机,则远程站点可能仍会将状态指示为联机。

## 添加和断开复制伙伴

如果要与其他站点进行数据复制,则您可能已在初始安装期间完成此设置。如果您 在初始安装期间没有设置复制,则可以现在通过添加复制伙伴来设置。当将多个站 点设置为复制伙伴时,这些站点称作站点场。您可以将任何站点作为复制伙伴添加 到站点场。

若需更多信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

您也可以将先前删除的复制伙伴再次添加为复制伙伴。

开始前,需要备妥以下信息:

■ 您要设置成为复制伙伴的 Symantec Endpoint Protection Manager 的 IP 地址或 主机名称。

您要连接的 Symantec Endpoint Protection Manager 必须之前已为复制伙伴。
 Symantec Endpoint Protection Manager 也可以是相同站点场上其他站点的伙伴。

#### 添加复制伙伴

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,选择一个站点。
- 3 在"任务"下,单击"添加复制伙伴"。
- 4 在"添加复制伙伴向导"中,单击"下一步"。
- 5 键入您要设置成为复制伙伴的 Symantec Endpoint Protection Manager 的 IP 地址及主机名称。
- 6 键入已安装 Symantec Endpoint Protection Manager 的远程服务器的端口号。 远程服务器端口的默认设置为 8443。
- 7 键入管理员的用户名和密码。
- 8 单击"下一步"。
- 9 在"调度复制"窗格中,执行下列操作之一以指定两个伙伴之间的复制调度:
  - 选中"自动复制"。 这可在两个站点之间定期进行自动复制。此选项为默认设置。因此您不能 设置自定义复制调度。
  - 取消选中"自动复制"。 您现在可以设置自定义复制调度:
    - 在"复制频率"选择每小时、每日或每周。
    - 在"每周的"列表中选择要在星期几运行复制,以设置每周调度。
- 10 单击"下一步"。
- 11 在"复制日志文件和客户端软件包"窗格中,根据您是否需要复制日志选中或 取消选中相应选项。

默认设置为取消选中。

- 12 在"添加复制伙伴"对话中,执行下列其中一个操作:
  - 如果数据库已在复制伙伴站点上还原,单击"是"。
    您必须在每个复制伙伴站点上还原数据库,才能继续升级或还原数据库。
  - 如果未还原数据库,单击"否"。然后还原数据库并重新开始此过程。

- 13 单击"下一步"。
- 14 单击"完成"。

复制伙伴站点会添加到"管理员"页面的"复制伙伴"下面。

#### 断开复制伙伴的连接

删除复制伙伴只会断开复制伙伴与 Symantec Endpoint Protection Manager 的连接。这不会删除站点。如果需要,可稍后通过添加复制伙伴重新添加站点。

#### 从复制进程删除数据库

- 1 在控制台中,单击"管理员"。
- 2 在"管理员"页面的"查看服务器"下方,单击"复制伙伴"。
- 3 展开"复制伙伴",并选择要与其断开的伙伴。
- 4 在"管理员"页面的"任务"窗格下方,单击"删除复制伙伴"。
- 5 在询问是否要删除复制伙伴时,键入"是"。

## 调度自动和按需复制

您可以自动或按需调度复制。您也可以指定调度复制的频率。

#### 按需复制数据

复制通常会根据安装期间您在添加复制伙伴时设置的调度进行。较小 ID 号码的站 点会先启动调度的复制。有时候,您可能希望复制立即进行。

#### 调度按需复制

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下,展开"复制伙伴",然后选择您要立即复制其数据库的 伙伴。
- **3** 在"任务"下,单击"立即复制"。

4 询问您确定要立即开始一次复制时,请单击"是"。 下列消息随即出现:

已调度复制。 如需调度复制事件结果的详细信息, 请在数分钟的延迟之后, 检查服务器系统日志。延迟时间视管理服务器负载、 复制的更改量, 以及通信通道带宽而定。

5 单击"确定"。此时会立即复制数据库。

如果在多台服务器上使用一个 Microsoft SQL 数据库,则只能从该站点上的第 一台服务器开始复制。如果尝试从第二台服务器立即复制,则会出现下面的消 息:

只有站点的第一个服务器可以执行复制。 请登录到服务器:<第一个服务器名称> 启动 复制。

#### 更改复制频率

复制通常会根据您在初始化安装期间添加复制伙伴时设置的调度进行。较小 ID 号码的站点会先启动调度的复制。当复制伙伴创建之后,您可以更改复制调度。当您更改某个复制伙伴上的调度时,等到下一次复制之后,两端复制伙伴上的调度都会相同。

#### 更改复制频率

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下,单击"复制伙伴"。
- 3 在"任务"下,单击"编辑复制伙伴"。
- 4 在"编辑复制伙伴"对话框中,执行下列操作之一,以指定两个伙伴之间的复 制调度:
  - 选中"自动复制"。 这可在两个站点之间定期进行自动复制。此选项为默认设置。因此您不能 设置自定义复制调度。
  - 取消选中"自动复制"。 您现在可以设置自定义复制调度。
    - 在"复制频率"选择每小时、每日或每周。

■ 在"每周的"列表中选择要在星期几运行复制,以设置每周调度。

5 单击"确定"。

## 复制客户端软件包

您可以选择在本地站点和远程站点的复制伙伴之间复制或复制客户端软件包。您可 能会想将客户端软件包的最新版本从本地站点复制到远程站点。接着远程站点的管 理员便可部署客户端软件包。

若需如何在站点创建和部署客户端安装软件包的相关信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 安装指南》。

如果您决定复制客户端软件包,可能会复制大量的数据。如果复制许多软件包,数据可能会多达5GB。Symantec Endpoint Protection和 Symantec Network Access Control 32 位及 64 位安装软件包可能需要多达 500 MB 磁盘空间。

有关磁盘存储要求的详细信息,请参见《Symantec Endpoint Protection及Symantec Network Access Control 安装指南》。

#### 在复制伙伴之间复制客户端软件包

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下,单击"复制伙伴"。
- 3 展开"复制伙伴",并选择要复制客户端软件包的复制伙伴。
- 4 在"任务"下,单击"编辑复制伙伴属性"。
- 5 在"复制伙伴属性"对话框的"伙伴"下,单击"在本地站点和伙伴站点之间 复制客户端软件包"。
- 6 单击"确定"。

## 复制日志

您可以指定复制某复制伙伴的日志,还可以指定复制其数据库。在添加复制伙伴, 或者编辑复制伙伴属性时,您可以指定复制日志。如果您计划复制日志,请确保您 有足够的磁盘空间可以存储所有复制伙伴计算机上的其他日志。

请参见第169页的"查看其他站点的日志"。

#### 在两个复制伙伴之间复制日志

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下,单击"复制伙伴"。
- 3 展开"复制伙伴",并选择要开始生成复制日志的复制伙伴。
- 4 在"管理员"页面的"任务"下方,单击"编辑复制伙伴属性"。

- 6 单击"确定"。
- 5 在"复制伙伴属性"对话框的"伙伴"下,单击"将日志从本地站点复制到此 伙伴站点"或"将日志从此伙伴站点复制到本地站点"。

266 | 复制数据 | **复制日志** 



本章节包括下列主题:

- 关于防篡改
- 配置防篡改

## 关于防篡改

防篡改功能可为服务器和客户端上运行的 Symantec 应用程序提供实时保护。该功能可防止蠕虫、特洛伊木马、病毒和安全风险之类的非 Symantec 进程感染 Symantec 进程。您可以将软件配置为禁止或记录尝试修改 Symantec 进程的操作。

**注意**:如果您使用可检测并防御不需要的广告软件和间谍软件的第三方安全风险扫描程序,这些扫描程序通常会影响 Symantec 进程。如果您在运行这类扫描程序的同时启用防篡改功能,则防篡改功能会生成大量的通知和日志条目。最佳做法是始终启用防篡改功能。如果生成的事件数目过大,请使用日志过滤功能。

当客户端安装为非受管客户端时,防篡改功能具有下列默认值:

- 启用防篡改功能。
- 当防篡改功能检测到篡改企图时,它将禁止该尝试并记录该事件。
- 防篡改功能会在检测到篡改企图时向用户发送默认消息。

当客户端安装为受管客户端时,防篡改功能具有下列默认值:

- 启用防篡改功能。
- 当防篡改功能检测到篡改企图时,它将仅记录该事件。
- 当防篡改功能检测到篡改企图时,它不会向用户发送消息。

**注意**:如果您启用有关 Symantec Endpoint Protection 检测到篡改企图的通知,关于 Windows 进程的通知以及关于 Symantec 进程的通知都将发送至受感染的计算机。

## 配置防篡改

您可以启用和禁用防篡改,并配置检测到篡改企图时所要采取的操作。您也可以配 置此功能以通知用户其检测到篡改企图。

初次使用 Symantec Endpoint Protection 时,若您每周监控一次日志,最好使用操作"仅记录事件"。在没有发现误报可以放心的情况下,就可以将防篡改设置为"禁止它并记录事件"。

您也可以配置当 Symantec Endpoint Protection 检测到篡改企图时将在客户端上显示的消息。默认情况下,当软件检测到篡改企图时会显示通知消息。

您可以创建既包含文本又包含变量的消息。变量会以可标识攻击特性的数值填入。 如果使用变量,则必须按照它显示的样子键入。

表 22-1 说明了您在配置消息时可以使用的变量。

字段	说明
[ActionTaken]	防篡改功能为响应攻击而执行的操作。
[ActorProcessID]	攻击 Symantec 应用程序的进程的 ID 号。
[ActorProcessName]	攻击 Symantec 应用程序的进程的名称。
[Computer]	受攻击的计算机的名称。
[DateFound]	攻击发生的日期。
[EntityType]	进程攻击的目标的类型。
[Filename]	攻击受保护进程的文件的名称。
[Location]	保护其免遭篡改的计算机硬件或软件 区域。对于"防篡改" 消息,这个字段是 Symantec 应用程序。
[PathAndFilename]	攻击受保护进程的文件的完整路径和名称。
[SystemEvent]	发生的篡改企图的类型。
[TargetPathname]	进程攻击的目标的位置。
[TargetProcessID]	进程攻击的目标的进程 ID。

字段	说明
[TargetTerminalSession ID]	发生事件的终端会话的 ID。
[User]	发生攻击时已登录的用户的名称。

#### 启用或禁用防篡改

- 1 在控制台中,单击"客户端"。
- 2 在"策略"选项卡的"设置"下方,单击"常规设置"。
- 3 在"防篡改"选项卡上,选中或取消选中"防止 Symantec 安全软件被篡改或 关闭"。
- 4 如果您不希望用户能更改此设置,请单击锁定图标。
- 5 单击"确定"。

#### 配置基本防篡改设置

- 1 在控制台中,单击"客户端"。
- 2 在"策略"选项卡的"设置"下方,单击"常规设置"。
- 3 在"防篡改"选项卡的列表框中,选择下列操作之一:
  - 若要禁止并记录未授权活动,请单击"禁止它并记录事件"。
  - 若要记录未授权活动,但仍允许活动进行,请单击"Q记录事件"。
- 4 如果您不希望用户能更改此设置,请单击锁定图标。
- 5 单击"确定"。

#### 启用和自定义防篡改通知消息

- 1 在控制台中,单击"客户端"。
- 2 在"策略"选项卡的"设置"下方,单击"常规设置"。
- 3 在"防篡改"选项卡上,单击"检测到篡改时显示通知消息"。
- 4 如果要修改默认消息,则可以在文本字段框中键入其他文本以及删除文本。 如果使用变量,则必须按照它显示的样子键入。
- 5 如果您不希望用户能更改此设置,请单击锁定图标。
- 6 单击"确定"。







# 常规策略管理任务

- 管理组的位置
- 使用策略
- 设置已知应用程序

272 |

# 23

# 管理组的位置

本章节包括下列主题:

- 关于组的位置
- 启用客户端的策略自动分配
- 使用向导添加位置
- 不使用向导添加位置
- 分配默认位置
- 编辑组位置的名称和说明
- 删除组的位置

## 关于组的位置

用户尝试连接到公司网络的位置不同,需要的策略和设置通常也不同。因此,您可以为用户所属的每个组创建不同的位置或配置文件。

您可能想为下列类型的客户端计算机添加位置:

- 无线网络办公室中
- 非无线网络办公室内
- 远程位置(在远程公司机构工作)
- VPN(从外部位置进入的VPN)

您可以根据适合该位置的特定条件,自定义每个位置的策略和设置。

例如,默认位置的策略可能不像 VPN 或 Home 位置的策略那么严格。当用户受公司防火墙保护时,将使用与默认位置关联的策略。

设置所有需要管理的组后,您就可以添加位置。如果您的安全策略要求,则每个组 可以有不同的位置。

如果添加位置,则会应用于您创建此位置的组,以及从此父组继承的任何子组。因此,您希望应用于所有最终用户的位置或许应该在"我的公司"组级别创建。特定 于特定组的位置可以在子组级别创建。

例如,在大部分的公司中,所有用户皆需要让默认位置自动添加"我的公司"组。 但是,并非所有最终用户都需要 VPN 连接。需要 VPN 连接的最终用户可以组成一 个组,称为 Telecommuter。VPN 位置会添加到 Telecommuter 组,也会添加到继 承的办公室位置。该组的成员便可以使用与 Office 或 VPN 位置关联的策略。

您也可以根据位置,配置管理服务器与客户端之间的通信设置。

请参见第114页的"配置位置的通信设置"。

#### 关于位置和位置感测

员工经常需要从多个位置连接到网络。您可以基于网络连接类型(例如无线、以太 网或VPN),以及网络连接的位置(例如家中、网咖或办公室)来改善和分配单独 的安全策略。Symantec 可避免自动运行进程时将组织暴露在黑客威胁之中。

如果您要保护网络,则需要设置条件来触发此自动切换或位置感测。您必须将最佳 的安全策略自动应用至客户端或服务器。最佳的安全策略通常取决于用户连接的位 置。

您可以针对每个组的位置添加一组条件,以便自动为用户环境选择正确的安全策略。这些条件以信息为基础,例如,发起网络访问请求时采用的计算机网络设置。 IP 地址、MAC 地址或目录服务器的地址也可作为条件。

如果您更改控制台中的安全策略,则管理服务器会更新客户端的策略,或者客户端 会下载策略。如果当前的位置在更新后失效,客户端将切换到其他有效的位置,或 者使用默认的位置。

#### 关于规划位置

开始将位置添加到组之前,需要考虑您的环境所需的安全策略类型。您也必须判断 定义每个位置的条件。

您应考虑下列问题:

- 用户从什么位置进行连接? 考虑需要创建哪些位置,以及如何标记每一个位置。例如,用户可能在办公室、 从家里、从客户站点或从其他远程站点(例如旅行时所住的旅馆)进行连接。 大型站点可能需要其他合格的位置。
- 应该为每个位置设置位置感测吗?
- 如果使用位置感测,您想如何识别位置?

您可以根据 IP 地址、WINS、DHCP 或 DNS 服务器地址、网络连接和其他条件 来识别位置。

- 如果通过网络连接标识位置,使用哪种类型的连接?
  例如,网络连接可能是与 Symantec Endpoint Protection Manager、拨号网络或特定品牌的 VPN 服务器的连接。
- 是否要此位置连接的客户端使用特定的控制类型(例如服务器控制、混合控制 或客户端控制)?
- 是否要在每个位置进行主机完整性检查?或者是否要随时跳过此操作(例如未 连接至 Symantec Endpoint Protection Manager 时)?
- 每个位置应该允许哪些应用程序和服务?
- 是否要此位置和组中的其他位置使用相同通信设置,或者使用不同的通信设置? 您可以为一个位置设置唯一的通信设置。

## 关于组的默认位置

如果发生下列情形之一,会使用默认位置:

- 多个位置中有一个符合位置条件,且最后一个位置不符合位置条件。
- 您正在使用位置感测,而所有位置都不满足条件。
- 位置在策略中已重命名或更改。客户端在收到新策略时会恢复为默认位置。

Symantec Endpoint Protection Manager 最初安装后,仅设置了默认位置,称为 Default。此时,每个组的默认位置都为 Default。稍后添加其他位置之后,可以更 改此默认位置。每个组都必须有一个默认位置。

您可能更希望将 Home 或 Road 等位置指定为默认位置。

## 启用客户端的策略自动分配

您可以控制分配到客户端的策略,具体取决于客户端连接的位置。因此,您应该启 用位置感测。

#### 启用客户端的策略自动分配

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择要实现自动位置切换的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 对于尚未从父组继承策略和设置的组,您只能修改与位置无关的设置。
- 4 在"与位置无关的策略与设置"下,单击"常规设置"。

5 在"常规设置"对话框中,在"常规设置"选项卡的"位置设置"下,选中 "记住上次的位置"。

默认情况下, 启用此选项。客户端起初会分配至与客户端上次网络连接的源位 置相关联的策略。

- 如果在客户端计算机连接至网络时选中了"记住上次的位置",则一开始 会给客户端分配一个策略。此策略与上次使用的位置关联。如果启用了位 置感测,则客户端会在几秒后自动切换至适当的策略。与特定位置关联的 策略会确定客户端的网络连接。如果禁用了位置感测,即使客户端是在服 务器的控制下,用户仍可手动切换至任意位置。如果启用隔离位置,客户 端可能会在几秒后切换至隔离策略。
- 如果在客户端连接至网络时未选中"记住上次的位置",则一开始会给客户端分配与默认位置关联的策略。该客户端将不能连接到上次使用的位置。如果启用了位置感测,则客户端会在几秒后自动切换至适当的策略。与特定位置关联的策略会确定客户端的网络连接。如果禁用了位置感测,即使客户端是在服务器的控制下,用户仍可手动切换至任意位置。如果启用隔离位置,客户端可能会在几秒后切换至隔离策略。
- 6 选中"启用位置感测"。

默认情况下,位置感测已启用。会自动给客户端分配与用户尝试连接至网络的 位置关联的策略。

7 单击"确定"。

## 使用向导添加位置

您可以使用向导向组中添加位置。每个位置都可拥有其自己的一组策略和设置。您 可以设置条件,以便在满足条件时触发客户端以切换到使用不同安全设置的新位 置。应用的最佳安全策略通常会根据客户端连接到网络时的位置而定。启用位置感 测,可确保在必要时将最严格的安全策略分配给客户端。

#### 使用向导添加位置

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择要为其添加一个或多个位置的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您只能向没有从父组继承策略的组添加位置。
- 4 在"任务"下,单击"添加位置"。
- 5 在"欢迎使用添加位置向导"面板中,单击"下一步"。
- 6 在"指定位置名称"面板中,键入新位置的名称和说明,然后单击"下一步"。

7 在"指定条件"面板中,选择客户端从一个位置切换到另一个位置的下列任一条件:

无特定条件 选择此选项,以便客户端可以在有多个位置可用时选择 此位置。

IP 地址范围 选择此选项,以便客户端可以在其IP 地址包括在指定范 围内时选择此位置。您必须同时指定开始IP 地址和结束 IP 地址。

子网地址和子网掩码 选择此选项,以便客户端可以在其子网掩码和子网地址 已指定时选择此位置。

DNS 服务器 选择此选项,以便客户端可以在连接到指定的DNS 服务 器时选择此位置。

- 客户端可以解析主机名 选择此选项,以便客户端可以在连接到指定的域名及 DNS 解析地址时选择此位置。
- 客户端可以连接到管理服务器 选择此选项,以便客户端可以在连接到指定的管理服务 器时选择此位置。

网络连接类型 选择此选项,以便客户端可以在连接到指定的网络连接 类型时选择此位置。使用下列任一连接时,客户端会切 换到此位置:

- 任何网络
- 拨号网络
- 以太网
- 无线
- Check Point VPN-1
- Cisco VPN
- Microsoft PPTP VPN
- Juniper NetScreen VPN
- Nortel Contivity VPN
- SafeNet SoftRemote VPN
- Aventail SSL VPN
- Juniper SSL VPN
- 8 单击"下一步"。
- 9 在"添加位置向导完成"面板中,单击"完成"。

## 不使用向导添加位置

您可以不使用向导,将位置及其关联策略和设置添加到组。

请参见第 276 页的"使用向导添加位置"。

#### 不使用向导添加位置

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择要为其添加一个或多个位置的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您仅能为不是从上层组继承策略的组添加位置。
- 4 在"客户端"页面的"任务"下方,单击"管理位置"。
- 5 在"管理位置"对话框的"位置"下,单击"添加"。
- 6 在"新添加位置"对话框中,键入新位置的名称和说明,然后单击"确定"。
- 7 在"管理位置"对话框中的"符合以下条件时切换到该位置"旁,单击"添加"。
- 8 在"指定位置条件"对话框的"类型"下拉列表中,选择并定义条件。 如果客户端计算机有指定的条件,便会切换到该位置。
- 9 单击"确定"。
- 10 若要添加其他条件,请在"符合以下条件时切换到该位置"旁单击"添加", 然后选择"AND关系的条件"或"OR关系的条件"。
- **11** 重复步骤 8 到步骤 9。
- 12 单击"确定"。

## 分配默认位置

每次创建新组时,Symantec Endpoint Protection Manager 控制台都会自动创建名为 Default 的默认位置。您可以将其他位置指定为默认位置。

#### 分配默认位置

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,单击要为其分配其他默认位置的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名> 继承策略和设置"。
- **4** 在"任务"下,单击"管理位置"。
- 5 在"管理位置"对话框中的"位置"下,选择要作为默认位置的位置。

- 6 在"说明"下,选中"如果发生冲突则设置此位置为默认位置"。 在为组分配其他位置前,默认位置始终是 Default 位置。
- 7 单击"确定"。

## 编辑组位置的名称和说明

您可以编辑组级别的位置名称和说明。

#### 编辑组位置的名称和说明

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"窗格的"查看客户端"下,单击您要编辑其名称和说明的组。
- 3 在"策略"选项卡的"任务"窗格下,单击"管理位置"。
- 4 在"位置名称"文本框中,编辑位置名称。
- 5 在"说明"名称文本框中,编辑位置说明。
- 6 单击"确定"。

## 删除组的位置

您可能需要删除不再适用的组位置。

#### 删除位置

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择内含要删除位置的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您只能从不继承父组策略的组删除位置。
- 4 在"客户端"页面的"任务"下,单击"管理位置"。
- 5 在"管理位置"对话框的"位置"下,选择要删除的位置,然后单击"删除"。 您不能删除已设为默认位置的位置。
- 6 在"确认删除"对话框中,单击"是"。

280 | 管理组的位置 | **删除组的位置** 

# 24

## 使用策略

本章节包括下列主题:

- 关于策略
- 关于共享和非共享策略
- 关于添加策略
- 编辑策略
- 分配共享策略
- 撤回策略
- 删除策略
- 导出策略
- 导入策略
- 关于复制策略
- 在策略页面中复制共享策略
- 在客户端页面中复制共享或非共享策略
- 粘贴策略
- 复制和粘贴组策略
- 替换策略
- 将共享策略转换为非共享策略
- 将共享策略的副本转换为非共享策略
- 关于更新客户端的策略

■ 配置推模式或拉模式来更新客户端策略和内容

## 关于策略

可以使用不同类型的安全策略来管理网络安全性。许多策略是在安装期间自动创建 的。可以使用默认策略,也可以自定义策略以符合特定环境的需要。

表24-1列出了不同类型的策略。它还说明了在初始安装期间是否创建默认策略,并 且包含对每种类型的策略的说明。

表 24-1 Symantec Endpoint Protection Manager 策略

策略名称	默认策略	说明
防病毒和防间谍软件	是	定义防病毒和防间谍软件威胁扫描 设置,包括如何处理检测到的进 程。
防火墙	是	定义允许和禁止通信的防火墙规则,并指定智能通信过滤、通信和 对等验证的设置。
人侵防护	是	定义入侵防护特征的例外,并指定 诸如活动响应之类的入侵防护设 置。
主机完整性	是	帮助定义、还原及强制执行客户端 的安全,以确保企业网络和数据安 全无虞。
应用程序与设备控制	是	防范应用程序访问系统资源,管理 可连接到计算机的外围设备。
LiveUpdate	是	指定客户端为检查有无更新而必须 联系的计算机,以及定义客户端必 须按何种频率检查有无更新的调 度。
集中式例外	否	指定您要应用的特定策略功能的例 外。

您可以对所有策略执行下列任务:

∎ 添加

如果您在"策略"页面中添加或编辑共享策略,则还必须将这些策略分配给组 或位置。否则这些策略不会生效。

■ 编辑

- 删除
- 分配
- 替换
- 复制和粘贴
- 导入和导出

除防病毒和防间谍软件策略以及 LiveUpdate 设置策略外,可以撤回任何类型的策略。

## 关于共享和非共享策略

策略可以为共享策略,也可以为非共享策略。共享策略应用于任何组和位置。如果 创建共享策略,则可以在所有使用相应策略的组和位置轻松将其编辑和替换。您可 以拥有多个共享策略。

您可以在 My Company 组级别或更低级别应用共享策略,而子组能够继承策略。

非共享策略应用于组中的特定位置。每个策略只能应用至一个位置。针对已经存在 的特定位置您可能需要特定的策略。在这种情况下,您可以为该位置创建一个唯一 的策略。

您可以将一个策略应用于一个组或位置,或者也可将多个安全策略分别应用于组中 的每个位置。例如,一个组已经被分配了多个位置。当用户身在办公室或家中时, 可能需要从不同位置连接至企业网络。所以,您可能需要将具有各自的规则集和设 置的不同策略应用于每个位置。

您可以给每个用户或计算机组应用不同的策略。远程用户通常会使用DSL及ISDN, 因此您可能需要VPN连接。其他远程用户可能要使用拨号来连接至企业网络。在办 公室工作的员工通常是使用以太网连接,但是,销售及市场组可能也会使用无线连 接。针对这些组连接至企业网络时所处的位置,每个组可能需要有自己的防火墙策 略。

对于在大多数员工工作站上安装的非验证应用程序,您可能要实现限制性策略以保 护企业网络免受攻击。您的 IT 组可能需要访问其他应用程序。因此相较于常规员 工,IT 组的安全策略限制可能要少些。在这种状况下,您可以为 IT 组创建不同的 防火墙策略。

当您在创建新策略时,通常会编辑一个默认策略。默认策略通常包括默认规则和安 全设置。

## 关于添加策略

您可以添加策略成为共享策略或非共享策略。

您通常会在"策略"页面的"策略"选项卡上添加组和位置共享的任何策略。不 过,如果添加的策略不是组之间共享的策略,而只应用到特定位置,请在"客户 端"页面中添加。

如果决定要在"客户端"页面中添加策略,可以使用下列任何方法添加新策略:

- 以现有策略为基础来创建新策略。
- 创建新策略。
- 从先前导出的策略导入策略。

请参见第 284 页的"添加共享策略"。

请参见第 285 页的"在客户端页面中使用向导添加非共享策略"。

#### 添加共享策略

您通常是在"策略"页面而非"客户端"页面添加共享策略。位置与组可以共享相同的策略。当您完成添加共享策略后,您还必须分配该共享策略。

您可以从"客户端"页面添加非共享策略。

请参见第 285 页的"在客户端页面中使用向导添加非共享策略"。

#### 在策略页面添加共享策略

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下,选择任一策略类型。
- 3 在"任务"下,单击"添加<策略类型>策略"。
- 4 在"<策略类型>策略"页上的"概述"窗格中,键入策略的名称和说明。
- 5 选中"启用此策略"(如果尚未选中)。
- 6 在"概述"窗格中,选择下列视图之一:

树视图 任何已分配到组和位置的策略都会以图标显示。

列表视图 任何已分配到组和位置的策略都会以列表显示。

- 7 若要配置策略,请在"查看策略"下单击策略类型,如"防病毒和防间谍软件防护"。
- 8 配置完此策略后,单击"确定"。
- 9 在"分配策略"对话框中,执行下列任务之一:
  - 若要立即将策略分配给组或位置,请单击"是",然后跳至步骤 10。
  - 若要稍后将策略分配给组或位置,请单击"**否**"。 请参见第 289 页的"分配共享策略"。

必须将策略分配给组或位置,否则客户端计算机不会接收策略。

- 10 在"分配<策略类型>策略"对话框中,选中要应用策略的组和位置。
- 11 单击"分配"。
- 12 若要确认,请单击"是"。

#### 在客户端页面中使用向导添加非共享策略

您可以在"客户端"页面中添加非共享或共享策略。

您可以在"策略"页面中添加共享策略

请参见第 284 页的"添加共享策略"。

#### 在客户端页面中使用向导添加非共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,找出要将策略添加到的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您必须禁用此组的继承。如果没有取消选中继承,就不能添加策略。
- 4 在"特定于位置的策略与设置"下方,向下滚动至位置。
- 5 在"位置限定的策略"的右侧,单击"添加策略"。 如果已有共享或位置限定的策略存在,就不会出现在"为<位置名称>添加策略"向导中。

6 在"为<位置名称>添加策略"向导中,选择要添加的策略类型,然后单击"下 一步"。

如果不存在任何策略,您只能添加位置限定的策略。只有当不存在特定类型策略时,"添加策略"才会出现。

7 选择下列任一选项:

使用现有的共享策略	从相同类型的共享策略创建非共享策略。如 果您编辑此策略,则所有使用此策略的位置 中的此策略都会随之更改。
	请参见第287页的"在客户端页面中从现有策 略添加新的非共享策略"。
创建新策略	创建非共享策略。
	请参见第286页的"在客户端页面中添加新的 非共享策略"。
从策略文件导入策略	从先前导出的.dat格式文件创建非共享策略。
	请参见第287页的"在客户端页面中从先前导

出的策略文件添加新的非共享策略"。

#### 在客户端页面中添加新的非共享策略

如果您在"客户端"页面中创建非共享策略,该策略只会应用到特定位置。 请参见第 285 页的"在客户端页面中使用向导添加非共享策略"。

#### 在客户端页面中添加新的非共享策略

- 在"为<位置名称>添加策略"向导中,选择要添加的策略类型,然后单击"下 一步"。
- 2 单击"创建新策略",然后单击"下一步"。

- 3 在"<策略类型>策略概述"窗格中,键入策略的名称和描述。
- 4 若要配置策略,请在"查看策略"下,单击下列任一类型的策略:

防病毒和防间谍软件	请参见第 313 页的"关于使用防病毒和防间谍软件策略"。
防火墙	请参见第 369 页的"关于使用防火墙策略"。
入侵防护	请参见第 389 页的"关于使用入侵防护策略"。
应用程序与设备控制	请参见第 437 页的"关于使用应用程序与设备控制策略"。
主机完整性	请参见第 479 页的"关于使用主机完整性策略"。
LiveUpdate	请参见第 89页的"关于 LiveUpdate 策略"。
集中式例外	请参见第 464 页的"关于使用集中式例外策略"。

#### 在客户端页面中从现有策略添加新的非共享策略

在客户端页面中,您可以从现有策略添加新的非共享策略。 请参见第 285 页的"在客户端页面中使用向导添加非共享策略"。

#### 在客户端页面中从现有策略添加新的非共享策略

- 在"为<位置名称>添加策略"向导中,选择要添加的策略类型,然后单击"下 一步"。
- 2 单击"使用现有的共享策略",然后单击"下一步"。
- 3 在"添加策略"对话框的"策略"下拉列表中,选择现有的策略。
- 4 单击"确定"。

#### 在客户端页面中从先前导出的策略文件添加新的非共享策略

在客户端页面中,您可以从先前导出的策略文件添加新的非共享策略。 请参见第 285 页的"在客户端页面中使用向导添加非共享策略"。

#### 在客户端页面中从先前导出的策略文件添加新的非共享策略

- 在"为<位置名称>添加策略"向导中,选择要添加的策略类型,然后单击"下 一步"。
- 2 单击"从策略文件导入策略",然后单击"下一步"。

3 在"导入策略"对话框中,浏览以找出先前导出的.dat 文件。

4 单击"导入"。

## 编辑策略

您可以在"策略"页面的"策略"选项卡以及在"客户端"页面中编辑共享策略。 但在"客户端"页面中只能编辑非共享策略。

位置与组可以共享相同的策略。您必须先编辑共享策略然后才能对其进行分配。 您可以在"客户端"页面中编辑非共享策略和共享策略。

#### 在策略页面中编辑共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下,单击策略类型。
- 3 在 "<策略类型>策略" 窗格中,选择要编辑的特定策略。
- **4** 在"任务"下,选择"编辑策略"。
- 5 必要时,在"<策略类型>策略概述"窗格中编辑策略的名称和说明。
- 6 若要编辑策略,请针对下列策略单击任一个"<策略类型>策略"页面:

#### 在客户端页面中编辑非共享或共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,选择要编辑策略的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您必须禁用此组的继承。如果没有取消选中继承,就不能编辑策略。
- 4 在"特定于位置的策略与设置"下,滚动查找要编辑其策略的位置名称。
- 5 找出要编辑的特定于位置的策略。
- 6 在所选策略右侧,单击"任务",然后单击"编辑策略"。
- 7 执行下列操作之一:
  - 若要编辑非共享策略,请转至步骤8。
  - 若要编辑共享策略,请在"编辑策略"对话框中单击"编辑共享",以便 编辑所有位置中的该策略。
- 8 您可以单击要编辑的策略类型的相应链接。
# 分配共享策略

在"策略"页面中创建共享策略之后,您必须将其分配给一个或多个组以及一个或 多个位置。未分配的策略不会下载到组和位置中的客户端计算机。如果您在添加策 略时未分配策略,则可以稍后将其分配给组和位置。您也可以将策略重新分配给其 他组或位置。

#### 分配共享策略

1 创建共享策略。

请参见第 284 页的"添加共享策略"。

- 2 在"策略"页面的"查看策略"下,选择要分配的策略类型。
- 3 在 "<策略类型>策略" 窗格中,选择要分配的特定策略。
- 4 在"策略"页面的"任务"下,单击"分配策略"。
- 5 在"分配 <策略类型>策略"对话框中,选中要向其分配策略的组和位置。
- 6 单击"分配"。
- 7 单击"是"以确认您要分配该策略。

# 撤回策略

在某些情况下,您可能会想要从组或位置撤回策略。例如,某个特定组可能在您采 用新策略后发生问题。撤回策略时,策略会自动从您指定的组和位置中撤回。但 是,策略仍会留在数据库中。

您可以在"策略"页面撤回所有策略,除了以下策略:

- 防病毒和防间谍软件
- LiveUpdate

**注意**:删除策略前,您必须从所有组和位置撤回该策略。您不能从位置和组撤回防病毒和防间谍软件策略,也不能撤回 LiveUpdate 策略。您只能以其他防病毒和防间谍软件策略或 LiveUpdate 策略加以替换。

#### 在策略页面撤回共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下,单击您要撤回的策略类型。
- 3 在 "<策略类型>策略" 窗格中,单击要撤回的特定策略。
- 4 在"策略"页面的"任务"下,单击"撤回策略"。
- 5 在"撤回策略"对话框中,选中要从其中撤回策略的组和位置。

- 6 单击"撤回"。
- 7 当系统提示您确认是否要从组和位置撤回策略时,单击"是"。

#### 在客户端页面中撤回共享或非共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,选择您要从中撤回策略的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您必须禁用此组的继承。如果没有取消选中继承,则不能撤回策略。
- 4 在"特定于位置的策略与设置"下,滚动查找要从中撤回策略的位置的名称。
- 5 找出您要从该位置撤回的策略。
- 6 单击"任务",然后单击"撤回策略"。
- 7 在"撤回策略"对话框中,单击"是"。

# 删除策略

您也许需要删除一个应用于组和位置的策略。例如,企业指导方针有所更改,要求 实行不同策略。当添加新的企业组时,您可能需要删除旧组及其关联策略。

您可能需要删除共享或非共享的策略。随着新组和位置的加入,您可能需要删除旧 策略。

若是删除非共享的策略,使用同一命令即可撤回并删除相应策略。

**注意**:您必须先将相应的策略从其所分配至的组或位置撤回,才可以将其删除。您 不能撤回防病毒和防间谍软件策略,或者 LiveUpdate 策略。而是必须先使用其他 防间谍软件策略或 LiveUpdate 策略来进行相应替换。接着,您才可以删除原始的 防间谍软件策略或 LiveUpdate 策略。每个组和位置都必须至少包含一个防间谍软 件策略和一个 LiveUpdate 策略。

#### 在策略页面中删除共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,选择要删除的策略类型。 策略可能已经或可能尚未分配到一或多个组和一或多个位置。
- 3 在 "<策略类型>策略" 窗格中,单击要导出的特定策略。
- 4 在"策略"页面的"任务"下方,单击"删除策略"。
- 5 当提示您确认删除所选策略时,单击"是"。

#### 在"客户端"页面中删除非共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,选择要删除策略的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您必须禁用此组的继承。如果没有取消选中继承,就不能删除策略。
- 4 在"特定于位置的策略与设置"下,滚动查找要删除其策略的位置名称。
- 5 找出要删除的特定于位置的策略。
- 6 在所选策略的右方,单击"任务",然后单击"撤回策略"。 当您撤回策略时,也会一并删除策略。您不能将防病毒和防间谍软件策略或 LiveUpdate 策略从任何位置删除。您仅可以其他策略替换该策略。
- 7 单击"是"。

# 导出策略

您可以将现有策略导出为.dat 文件。例如,可能需要导出策略以在其他站点使用。 在其他站点上,必须使用原始站点中的.dat 文件来导入策略。所有与策略关联的设 置都会自动导出。

您可以导出共享或非共享策略。

#### 在策略页面中导出共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击要导出的策略的类型。
- 3 在 "<策略类型>策略" 窗格中,选择要导出的特定策略。
- 4 在"策略"页面的"任务"下方,单击"导出策略"。
- 5 在"导出策略"对话框中,找出要导出策略文件的文件夹,然后单击"导出"。

#### 在客户端页面中导出共享或非共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,选择要导出策略的组。
- 3 在"策略"选项卡中,取消选中"从父组<组名>继承策略和设置"。 您必须禁用此组的继承。如果没有取消选中继承,就不能导出策略。
- 4 在"特定于位置的策略与设置"下,滚动查找要导出其策略的位置名称。
- 5 找出要导出的特定于位置的策略。
- 6 在策略的右边单击"任务",然后单击"导出策略"。

7 在"导出策略"对话框中,浏览到您要将策略导出至的目标文件夹。

8 在"导出策略"对话框中,单击"导出"。

# 导入策略

您可以导入策略文件,然后将它应用于组,或只应用于位置。导入文件的格式为.dat。

您可以在"客户端"页面中导入特定位置的共享或非共享策略。

请参见第287页的"在客户端页面中从先前导出的策略文件添加新的非共享策略"。

#### 在策略页面中导入共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下,单击要导入的策略类型。
- 3 在"<策略类型>策略"窗格中,单击要导入的策略。
- 4 在"策略"页面的"任务"下方,单击"导入 <策略类型>策略"。
- 5 在"导入策略"对话框中,浏览至要导入的策略,然后单击"导入"。

# 关于复制策略

在您开始自定义任何策略前,您最好复制相应的策略。复制策略之后,必须指执行 粘贴操作.

请参见第 293 页的"粘贴策略"。

# 在策略页面中复制共享策略

您可以在"策略"页面中复制共享策略。

您也可以在"客户端"页面上复制共享策略。

请参见第 293 页的"在客户端页面中复制共享或非共享策略"。

#### 在策略页面中复制共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下,单击要复制的策略类型。
- 3 在"<策略类型>策略"窗格中,单击要复制的特定策略。
- 4 在"策略"页面的"任务"下,单击"复制策略"。

- 5 在"复制策略"对话框中,选中"不要再显示此消息"。 选中此选项后,就不会再显示有关此过程的通知。该消息会指出策略已经复制 到剪贴板,可以执行粘贴操作。
- 6 单击"确定"。

# 在客户端页面中复制共享或非共享策略

您可以在"客户端"页面中复制共享或非共享策略。不过,您必须接着在"客户端"页中粘贴策略。

您也可以在"策略"页面中复制共享策略。

请参见第 292 页的"在策略页面中复制共享策略"。

#### 在客户端页面中复制共享或非共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择要为其复制策略的组。
- **3** 在"策略"选项卡的"特定于位置的策略与设置"下,滚动查找要复制其中策略的位置名称。
- 4 找到该位置中要复制的特定策略。
- 5 在策略的右侧,单击"任务",然后单击"复制"。
- 6 在"复制策略"对话框中,选中"不要再显示此消息"。

选中此选项后,就不会再显示有关此过程的通知。该消息会指出策略已经复制 到剪贴板,可以执行粘贴操作。

7 单击"确定"。

# 粘贴策略

您必须先复制策略,才能粘贴策略。

对于共享策略,在粘贴策略后,该策略会显示在右侧窗格中。"的副本"三个字会 加在策略名称的结尾,以标记这是策略副本。然后,您可以编辑策略副本的名称。 请参见第 292 页的"关于复制策略"。

#### 在策略页面中粘贴共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下方,单击要粘贴的策略类型。

- 3 在"<策略类型>策略"窗格中,选择要粘贴的特定策略。
- 4 在"策略"页面的"任务"下方,单击"粘贴策略"。

#### 在客户端页面中粘贴共享或非共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,选择要粘贴策略的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您必须禁用此组的继承。如果没有取消选中继承,就不能粘贴策略。
- 4 在"特定于位置的策略与设置"下,滚动查找要粘贴其策略的位置名称。
- 5 找出您在该位置中要粘贴的特定策略。
- 6 在策略的右侧,单击"任务",然后单击"粘贴"。
- 7 当系统提示您是否覆盖现有策略时,单击"是"。

# 复制和粘贴组策略

您可以复制分配给一个组的组设置、位置和策略,并贴至另一个组。新复制的设置、位置和策略会覆盖贴入组现有的策略设置。

#### 复制和粘贴组策略

- 1 在控制台中,单击"客户端"。
- 2 单击要复制其中策略的组。
- 3 在"任务"下方,单击"复制组策略"。
- 4 单击要将策略复制到的组。
- 5 在"任务"下方,单击"粘贴组策略"。
- 6 在确认对话框中单击"是"。

# 替换策略

您可能需要以其他共享策略替换某个共享策略。您可以替换所有位置或某一位置的 共享策略。

当您替换所有位置的策略时,管理服务器只会针对有该策略的位置替换策略。例如,假设 Sales 组在其四个位置的其中三个位置使用销售策略。如果要用市场策略 替换销售策略,则只有这三个位置会收到市场策略。

您可能需要某一组客户端使用相同的设置,不论各客户端的位置在哪里。在这种状况下,您可以使用共享策略替换非共享策略。用共享策略替换非共享策略时,请分别针对每个位置进行。

#### 替换所有位置的共享策略

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"查看策略"下,单击要替换的策略类型。
- 3 在"<策略类型>策略"窗格中,单击相应策略。
- 4 在"策略"页面的"任务"下,单击"替换策略"。
- 5 在"替换<策略类型>策略"对话框的"新<策略类型>策略"下拉列表中,选择要替换旧策略的共享策略。
- 6 选择要替换其现有策略的组和位置。
- 7 单击"替换"。
- 8 当系统提示您确认是否替换组和位置的策略时,单击"是"。

#### 替换一个位置的共享策略或非共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,选择您要替换策略的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您必须禁用此组的继承。如果不取消选中继承,则不能替换策略。
- 4 在"特定于位置的策略与设置"下,滚动鼠标查找包含相应策略的位置。
- 5 在要替换的策略旁边,单击"任务",然后单击"替换策略"。
- 6 在"替换策略"对话框的"新策略"下拉列表中,选择替代策略。
- 7 单击"确定"。

# 将共享策略转换为非共享策略

当现有共享策略不再应用于所有组或所有位置时,您最好将此策略转换为非共享策略。

完成转换时,转换后具有新名称的策略会出现在"特定于位置的策略与设置"下 方。

#### 将共享策略转换为非共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,选择您要转换其策略的组。
- 3 在与上一步骤中所选组关联的窗格中,单击"策略"。
- 4 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 如果没有取消选中继承,就不能导出任何策略。

- 5 在"特定于位置的策略与设置"下,滚动查找要转换其中策略的位置的名称。
- 6 找出您要从该位置转换的特定策略。
- 7 单击"任务",然后单击"转换为非共享策略"。
- 8 在"概述"对话框中,编辑策略的名称与说明。
- 9 单击"确定"。

# 将共享策略的副本转换为非共享策略

您可以复制共享策略的内容,并使用该内容创建非共享策略。通过使用副本,可以 更改一个位置的共享策略内容,而不影响所有其他位置。副本会覆盖现有的非共享 策略。

#### 将共享策略的副本转换为非共享策略

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下方,选择您要替换策略的组。
- 3 在"策略"选项卡中,取消选中"从父组 <组名>继承策略和设置"。 您必须禁用此组的继承。如果不取消选中继承,则不能替换策略。
- 4 在"特定于位置的策略与设置"下,滚动鼠标查找包含相应策略的位置。
- 5 在要替换的策略旁边,单击"任务",然后单击"编辑策略"。
- 6 在"编辑策略"对话框中,单击"使用副本创建非共享策略"。
- 7 编辑策略。

请参见第 288 页的"编辑策略"。

8 配置完此策略后,单击"确定"。

# 关于更新客户端的策略

配置管理服务器的策略时,必须先将更新策略下载到客户端。在控制台中,您可以 配置客户端使用下列两种更新方法中的一种:

- 拉模式 客户端会根据检测信号设置的频率,定期连接至 Symantec Endpoint Protection Manager。客户端会在连接时检查管理服务器的状态。
- 推模式 客户端会和管理服务器创建持续的HTTP连接。每当管理服务器状态发 生更改时,就会立刻通知客户端。

无论使用哪一种模式,客户端都会根据管理服务器的状态更改来采取相应的操作。 由于持续连接的关系,推模式需要较大的网络带宽;大多数情况下,您应将客户端 设置为拉模式。

检测信号为客户端计算机上载诸如日志条目等数据和下载策略的频率检测信号为各 客户端用来与 Symantec Endpoint Protection Manager 进行通信的协议。客户端 启动后会立刻出现首次检测信号。依照您所设置的检测信号频率会出现下次检测信 号。

检测信号频率是决定 Symantec Endpoint Protection Manager 可支持的客户端数 的重要因素。如果您将检测信号频率设为 30 分钟或 30 分钟以下,那么 Symantec Endpoint Protection Manager 可支持的客户端总数就会受到限制。如果部署的客 户端数为 1,000 或 1,000 以上,应该将检测信号频率设置为可满足公司安全要求的 最长时间。例如,如果您想要每天更新安全策略并收集日志,检测信号频率就要设 为 24 小时。请咨询 Symantec Professional Services 以及 Symantec Enterprise Support,以获取您的网络环境所需的正确配置、硬件及网络体系结构。

# 配置推模式或拉模式来更新客户端策略和内容

您可以指定是由管理服务器将策略推送至客户端,还是由客户端从管理服务器提取 策略。默认设置为推模式。如果您选择拉模式,则依默认客户端每隔五分钟就会连 接到管理服务器,但您可以更改此默认的检测信号时间间隔。

您可以设置组或位置的模式。

#### 配置组的推模式或拉模式

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择您要指定推模式或拉模式策略的组。
- 3 在"客户端"页面上,单击"策略"选项卡。
- 4 在"策略"选项卡上,取消选中"从父组 <组名称> 继承策略和设置"。
- 5 在"与位置无关的策略与设置"窗格的"设置"下,单击"通信设置"。
- 6 在"用于 <组名称> 的通信设置"对话框的"下载"下,确认已选中"从管理 服务器下载策略和内容"。
- 7 执行下列操作之一:
  - 单击"推模式"。
  - 单击"拉模式",然后在"检测信号时间间隔"下,设置分钟数或小时数。

8 单击"确定"。

#### 指定位置的推模式或拉模式

- 1 在控制台中,单击"客户端"。
- 2 在"客户端"页面的"查看客户端"下,选择您要指定推模式或拉模式策略的组。
- 3 在"客户端"页面上,单击"策略"选项卡。
- 4 在"策略"选项卡上,取消选中"从父组 <组名称> 继承策略和设置"。
- 5 在"特定于位置的策略与设置"下,在待修改位置的"特定于位置的策略"下 方,展开"特定于位置的设置"。
- 6 在"特定于位置的设置"下,单击"通信设置"右侧的"任务">"编辑设置",然后取消选中"使用组通信设置"。
- 7 在"通信设置"的右侧,单击"本地-推"或"本地-拉"。
- 8 执行下列操作之一:
  - 単击"推模式"。
  - 单击"拉模式",然后在"检测信号时间间隔"下,设置分钟数或小时数。
- 9 单击"确定"。

# 25

# 设置已知应用程序

本章节包括下列主题:

- 关于已知应用程序
- 启用已知应用程序
- 搜索应用程序

# 关于已知应用程序

客户端会监控每台计算机上运行的应用程序和服务,并收集相关信息。您可以配置 客户端,使其将信息收集在列表中并将该列表发送至管理服务器。应用程序及其特 性的列表称为已知应用程序。

您可以使用此信息找到用户运行的应用程序。您也可以视需要使用有关应用程序的 下列各方面信息:

- 防火墙策略
- 应用程序与设备控制策略
- TruScan 主动型威胁扫描
- 主机完整性策略
- 网络应用程序监控
- 文件指纹列表

控制台包括查询工具,可供您搜索应用程序列表。搜索条件可以应用程序或计算机 为基础。例如,您可以找出每台客户端计算机使用的 Internet Explorer 版本。 **注意**:在某些国家/地区,当地法律可能不允许在某些情况下使用已知应用程序工 具,例如,当员工在家里使用公司笔记本电脑登录您的办公室网络时,从笔记本电 脑获取应用程序使用信息。在您使用此工具之前,请确认当地法律允许您将此工具 用于您的用途。如果不允许,请按照指示禁用此工具。

注意:客户端不会记录有关 Symantec Network Access Control 客户端运行的应用 程序的信息。如果您只安装了 Symantec Network Access Control,则控制台不提 供已知应用程序功能。如果您将 Symantec Network Access Control 和 Symantec Endpoint Protection 集成在一起,则可以将已知应用程序工具与主机完整性策略配 合使用。您必须在客户端上安装网络威胁防护模块和应用程序与设备控制模块,此 功能才会正常工作。

# 启用已知应用程序

您可以为整个站点、站点中的组或组中的位置启用已知应用程序。默认情况下,已 为站点、组和位置启用已知应用程序功能。请先为每个站点启用已知应用程序,然 后可以选择是否为特定组和位置启用已知应用程序。

若要启用已知应用程序,必须完成下列任务:

- 为站点启用已知应用程序。 您必须为站点启用已知应用程序,才能对特定组或位置使用该工具。
- 使客户端能按组或位置将已知应用程序发送给管理服务器。

您可以设置组或位置中的每个客户端运行应用程序时向您的电子邮件地址发送的通 知。

请参见第180页的"创建管理员通知"。

您可以为本地站点或远程站点内的管理服务器设置已知应用程序。

#### 为站点启用已知应用程序

- 1 在控制台中,单击"管理员",再单击"服务器"。
- 2 在"查看服务器"下方,执行下列操作之一:
  - 单击 "本地站点(站点 <站点名称>)"。
  - 展开"远程站点",然后单击"(站点 <站点名称>)"。
- 3 在"任务"下方,单击"编辑站点属性"。
- 4 在"'站点名称'的站点属性"对话框的"常规"选项卡上,选中"保持跟踪客 户端所运行的每个应用程序"。
- 5 单击"确定"。

在您启用站点从客户端收集已知应用程序列表的功能后,您可以使客户端按照组或 位置将此列表发送至服务器。

注意:您只能修改不是从父组继承策略和设置的子组的设置。

#### 将已知应用程序列表发送至管理服务器

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择一个组。
- 3 在"策略"选项卡上,单击"通信设置"。
- 4 在"用于 <组名称>的通信设置"对话框中,确保选中"获知在客户端计算机 上运行的应用程序"。
- 5 单击"确定"。

#### 将已知应用程序发送至某一位置的管理服务器

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择一个组。
- 3 在"特定于位置的策略与设置"下,选择位置,然后展开"特定于位置的设置"。
- 4 在"通信设置"右边,单击"任务",然后取消选中"使用组通信设置"。 选中此设置能让您创建一个位置设置,而不是组设置。
- 5 单击"任务",然后单击"编辑设置"。
- 6 在"用于 <位置名称> 的通信设置"对话框中,选中"获知在客户端计算机上 运行的应用程序"。
- 7 单击"确定"。

# 搜索应用程序

当管理服务器收到来自客户端的应用程序列表之后,您可以查询有关这些应用程序 的详细信息。例如,您可以查找所有使用未经授权的应用程序的客户端计算机。然 后您就可以创建防火墙规则来禁止此客户端计算机上的应用程序。或者,您可能希 望升级所有客户端计算机,以使用最新版的 Microsoft Word。

您可以使用下列方式搜索应用程序:

- 按应用程序。 您可以将搜索范围限制为搜索特定应用程序或应用程序详细信息,例如其名称、 文件指纹、路径、大小、版本或上次修改时间。
- 按客户端或客户端计算机。

您可以搜索特定用户或特定客户端计算机运行的应用程序。例如,您可以根据 计算机的 IP 地址进行搜索。

您也可以直接在"防火墙策略"内搜索要添加到防火墙规则的应用程序名称。

请参见第 410 页的"将应用程序添加到规则"。

有关您可以从"搜索字段"中选择的客户端的信息是在添加客户端时从客户端收集的。

请参见第52页的"查看客户端的属性"。

#### 搜索应用程序

- 1 在控制台中,单击"策略"。
- 2 在"策略"页面的"任务"下方,单击"搜索应用程序"。
- 3 在"搜索应用程序"对话框的"搜索应用程序于"字段右侧,单击"浏览"。
- 4 在"选择组或位置"对话框中,选择您要查看其应用程序的客户端组,然后单击"确定"。

您一次只能指定一个组。

- 5 确保选中了"搜索子组"。
- 6 执行下列操作之一:
  - 若要按用户或计算机信息进行搜索,请单击"基于客户端/计算机信息"。
  - 若要按应用程序进行搜索,请单击"基于应用程序"。
- 7 单击"搜索字段"下的空单元格,然后从列表中选择搜索条件。

"搜索字段"单元格会显示所选选项的条件。有关这些条件的详细信息,请单击"帮助"。

- 8 单击"比较运算符"下的空单元格,然后选择其中一个运算符。
- 9 单击"值"下的空单元格,然后选择或键入值。

根据您在"搜索字段"单元格中所选的条件,"值"单元格可能会使用下拉列 表提供格式或值。

10 若要添加其他搜索条件,请单击第二行,然后在"搜索字段"、"比较运算 符"和"值"单元格中输入信息。

如果您输入多行搜索条件,则查询将尝试匹配所有条件。

- 11 单击"搜索"。
- 12 在"查询结果"表中,执行下列任一任务:
  - 单击滚动箭头以查看其他行和列。
  - 单击"上一页"和"下一页"以查看其他屏幕的信息。

- 选择某行,然后单击"查看详细信息"以查看有关应用程序的其他信息。 除非您将结果导出至文件,否则不会保存结果。
- 13 若要删除查询结果,请单击"全部清除"。
- 14 单击"关闭"。

# 保存应用程序搜索的结果

在运行查询之后,您可以将结果保存到文本文件或逗号分隔文件中。查询工具会导 出查询的所有结果,而不是选定行。

#### 保存应用程序搜索的结果

- 搜索有关应用程序或客户端计算机的详细信息。
   请参见第 301 页的"搜索应用程序"。
- 2 在"搜索应用程序"对话框的"查询结果"下方,单击"导出"。
- **3** 在"导出结果"对话框中,键入包含您要导出的应用程序详细信息和客户端计 算机详细信息的页码。
- 4 选择或键入要用来保存导出文件的路径名和文件名,然后单击"导出"。
- 5 若要确认,请单击"确定"。
- 6 如果已完成应用程序的搜索,请单击"关闭"。

304 | 设置已知应用程序 | **搜索应用程序** 





# 配置防病毒和防间谍软件防 护

- 基本防病毒和防间谍软件策略设置
- 配置自动防护
- 使用管理员定义的扫描

# 26

# 基本防病毒和防间谍软件 策略设置

本章节包括下列主题:

- 防病毒和防间谍软件防护基础篇
- 关于使用防病毒和防间谍软件策略
- 关于病毒和安全风险
- 关于扫描
- 关于针对扫描检测到的病毒与安全风险所采取的操作
- 在防病毒和防间谍软件策略中设置日志处理参数
- 关于客户端与防病毒和防间谍软件交互的选项
- 更改扫描映射网络驱动器所需的密码
- 指定 Windows 安全中心与 Symantec Endpoint Protection 客户端的交互方式
- 在定义过期或丢失时显示警告
- 指定出现在防病毒和防间谍软件错误通知中的 URL
- 指定浏览器主页的 URL
- 配置应用于防病毒和防间谍软件扫描的选项
- 将有关扫描的信息提交给 Symantec
- 管理已隔离的文件

# 防病毒和防间谍软件防护基础篇

您可通过执行下列操作为安全网络中的计算机提供防病毒和防间谍软件防护:

- 创建响应病毒和安全风险的计划。
- 在控制台主页面查看网络状态。
- 从控制台运行相应命令以打开自动防护、启动按需扫描,或更新定义。
- 使用防病毒和防间谍软件策略修改客户端计算机的自动防护与扫描设置。

# 关于创建计划以响应病毒和安全风险

若要有效响应病毒和安全风险的爆发,需要一个可以快速有效响应的计划。您应该 创建爆发响应计划,并定义处理可疑文件的操作。

表 26-1 概述了创建病毒和安全风险爆发计划所需的任务。

任务	说明
确保病毒定义文件是最新的。	确认受感染的计算机都有最新的病毒定义文件。您可以 运行报告,检查客户端计算机是否有最新的定义。 若要更新定义,请执行下列任何操作:
	<ul> <li>应用 LiveUpdate 策略。 请参见第 89 页的"关于 LiveUpdate 策略"。</li> <li>对组或"客户端"选项卡中列出的所选计算机运行 "更新内容"命令。</li> <li>对某计算机状态或风险日志中列出的所选计算机运行 "更新内容"命令。</li> </ul>
绘制网络拓朴图。	准备网络拓朴图,以便在将客户端计算机重新连接至本 地网络前,有系统地按区段隔离并清除计算机。 您的图应该包括下列信息:
	<ul><li>■ 客户端计算机名称和地址</li><li>■ 网络协议</li><li>■ 共享资源</li></ul>

表 26-1 示例计划

#### 基本防病毒和防间谍软件策略设置 | 309 防病毒和防间谍软件防护基础篇 |

任务	说明
了解安全解决方案。	您应该了解您的网络拓朴以及您网络中的客户端实现。 此外,还应该了解您的网络中所用的任何其他安全产品 的实现。
	请考虑下列问题:
	哪些安全程序保护网络服务器和工作站?
	<ul> <li>■ 更新定义的调度为何?</li> <li>■ 工资等道系列攻土时、左照此转代式注意本取更美。</li> </ul>
	<ul> <li>■ 正常省道受到攻击时,有哪些替代方法可获取更易?</li> <li>■ 哪些日志文件可用来跟踪网络上的病毒?</li> </ul>
制定备份计划。	如果发生严重的病毒感染,您可能需要还原客户端计算机。请确保您有还原重要计算机的适当备份计划。
隔离受感染的计算机。	蠕虫之类的混合型威胁不需要通过用户交互,即可通过 共享资源传播。感染计算机蠕虫后做出响应时,中断受 感染计算机与网络的连接来隔离计算机可能非常重要。
识别风险。	管理控制台报告和日志可以充分说明网络上存在的风险。 您可以使用Symantec安全响应中心的"病毒大全",对 在报告或日志中识别的特定风险做进一步了解。在某些 情况下,您可以找到处理风险的附加说明。
响应未知风险。	当发生下列情况时,应到 Symantec 安全响应中心 Web 站点查看最新信息:
	<ul><li>■ 不能通过检查日志和报告来识别可疑文件。</li><li>■ 最新的病毒定义文件不能清除可疑文件。</li></ul>
	在 Web 站点上,您可以找到有关可疑文件的最新信息。 请查看 Latest Virus Threats(最新病毒威胁)和 Security Advisories(安全建议)。
	http://www.symantec.com/region/cn/avcenter

# 如何获取详细信息

您可以搜索在线 Symantec 知识库获取详细信息。知识库包括此手册发行时尚未提供的详细信息。

#### http://www.symantec.com/region/cn/avcenter

您也可以查看 Symantec 安全响应中心网页获取有关病毒和安全风险的最新信息。

http://www.symantec.com/zh/cn/enterprise/security\_response/

# 关于查看网络的防病毒和防间谍软件状态

您可以从控制台主页快速查看安全网络的状态。状态摘要会显示安全网络中有多少 计算机禁用了防病毒和防间谍软件防护。操作摘要则会显示客户端对检测到的病毒 和安全风险执行的操作。主页中还包括整个网络的病毒定义分发。

请参见第 123 页的"关于 Symantec Endpoint Protection 主页"。

您也可以运行报告和查看日志。

请参见第185页的"关于使用监视器和报告来帮助确保网络安全"。

# 关于运行防病毒和防间谍软件防护的命令

您可以从控制台的"客户端"页中快速运行命令,也可以使用"监视器"页的计算 机状态日志快速运行命令。

#### 关于手动启用自动防护

默认情况下,默认防病毒和防间谍软件策略会启用自动防护。如果客户端计算机用 户禁用自动防护,您可以从控制台立即重新启用。

您可以在"客户端"页面的控制台,选择要对其启用自动防护的计算机,也可以从 "监视器"页面生成的日志中启用自动防护。

请参见第346页的"启用文件系统自动防护"。

#### 关于运行按需扫描

设置防病毒和防间谍软件策略时,可以包括调度扫描。但是,您可能需要在客户端 计算机上手动运行扫描。

您可以在"客户端"页面的控制台上选择要对其运行按需扫描的计算机,也可以从 "监视器"页面生成的日志运行按需扫描。

您可以运行活动扫描、全面扫描或自定义扫描。如果您选择运行自定义扫描,客户 端会使用您在防病毒和防间谍软件策略中配置的按需扫描设置。

请参见第362页的"运行按需扫描"。

### 关于防病毒和防间谍软件策略

"防病毒和防间谍软件策略"包括下列类型的选项:

- 自动防护扫描
- 管理员定义的扫描(调度和按需扫描)
- TruScan 主动型威胁扫描
- 隔离选项

- 提交选项
- 其他参数

当您安装 Symantec Endpoint Protection 时,控制台的策略列表中会显示若干防病 毒和防间谍软件策略。您可以修改这些预先配置的策略之一,也可以创建新的策略。

注意: 防病毒和防间谍软件策略包含针对 TruScan 主动型威胁扫描的配置。

请参见第316页的"关于扫描"。

# 关于预先配置的防病毒和防间谍软件策略

有下列预先配置的防病毒和防间谍软件策略可供使用:

- 防病毒和防间谍软件策略
- 防病毒和防间谍软件策略 高安全性
- 防病毒和防间谍软件策略 高性能

高安全性策略是所有预先配置的防病毒和防间谍软件策略中最严格的。您应该注 意,它可能会影响其他应用程序的性能。

高性能策略与高安全性策略相比,可提供更佳的性能,但不提供相同的保护。它主 要依靠文件系统自动防护来扫描具有所选文件扩展名的文件,以检测威胁。

默认防病毒和防间谍软件策略包括下列重要设置:

- 文件系统自动防护在计算机启动时加载,对所有文件都是启用的。
- Internet 电子邮件、Microsoft Outlook 和 Lotus Notes 自动防护对所有文件都 是启用的。
- 文件系统自动防护网络扫描会启用。
- TruScan 主动型威胁扫描已启用,且每小时运行一次。
- 新的定义到达时 ActiveScan 不会自动运行。
- 调度扫描每周运行一次,且扫描优化设置为"最佳应用程序性能"。

"高性能策略"包括下列重要设置:

- 文件系统自动防护在 Symantec Endpoint Protection 启动时加载,且对具有所 选扩展名的文件启用。
- 文件系统自动防护网络扫描会禁用。
- Internet 电子邮件、Microsoft Outlook 和 Lotus Notes 自动防护会禁用。
- 主动型威胁扫描会启用,且每6小时运行一次。

- 312 | 基本防病毒和防间谍软件策略设置 | 防病毒和防间谍软件防护基础篇
  - 新的定义到达时 ActiveScan 不会自动运行。
  - 调度扫描每月运行一次,且扫描优化设置为"最佳应用程序性能"。
     "高安全性策略"包括下列重要设置:
  - 文件系统自动防护在计算机启动时加载,对所有文件都是启用的。
  - Internet 电子邮件、Microsoft Outlook 和 Lotus Notes 自动防护对所有文件都 是启用的。
  - 文件系统自动防护网络扫描会启用。
  - 主动型威胁扫描会启用,且每小时、每次有新的进程启动时都会运行一次。
  - 新的定义到达时 ActiveScan 会自动运行。
  - 调度扫描每周运行一次,且扫描优化设置为"平衡"。

# 关于锁定"防病毒和防间谍软件策略"中的设置

您可以锁定"防病毒和防间谍软件策略"中的某些设置。锁定设置时,用户就不能 在使用该策略的客户端计算机上更改设置。

## 关于旧版客户端的防病毒和防间谍软件策略

如果您的环境中包含多种旧版客户端,则"防病毒和防间谍软件策略"可能会包含 不能应用的设置。您可能需要针对旧版客户端配置并管理个别的"防病毒和防间谍 软件策略"。

# 关于处理可疑文件的默认设置

当 Symantec Endpoint Protection 客户端识别出怀疑受病毒感染的文件时,它将使用默认的"防病毒和防间谍软件策略"执行下列操作:

- 客户端尝试修复文件。
- 如果使用当前的定义集不能修复文件,则客户端将把受感染的文件移到本地隔 离区中。此外,客户端会创建此风险事件的日志条目。客户端会将数据转发到 管理服务器。您可以从控制台查看日志数据。

您可以执行下列额外操作以完成您的病毒处理策略:

- 配置报告功能以在发现病毒时进行通知。
   请参见第 179 页的"使用通知"。
- 定义取决于病毒类型的各种修复操作。例如,您可以配置客户端自动修复宏病毒。然后,您可以配置客户端在检测到程序文件时采取其他操作。
- 对于客户端不能修复的文件指定备份操作。
   请参见第 334 页的"配置要针对检测到的已知病毒和安全风险执行的操作"。

配置本地隔离区,以将受感染的文件转发到中央隔离服务器。您可以配置"中央隔离"尝试进行修复。当"中央隔离"尝试进行修复时,会使用自己的病毒定义集。"中央隔离"定义可能比本地计算机上的定义新。您还可以使受感染文件的样本自动转发至 Symantec 安全响应中心进行分析。如需详细信息,请参见《Symantec 中央隔离区管理指南》。

# 关于使用策略管理隔离区项目

客户端检测到已知病毒时,会将受感染的文件放到客户端计算机的本地隔离区中。 客户端也可能隔离主动型威胁扫描检测到的项目。您可以在设置应用于客户端的防 病毒和防间谍软件策略时配置隔离区设置。

您可指定下列条目:

- 本地隔离区目录路径
- 客户端是否手动将隔离项目提交至 Symantec 安全响应中心
- 客户端是否自动将隔离项目提交至中央隔离服务器
- 新病毒定义到达时本地隔离区应如何进行补救

请参见第 339 页的"管理已隔离的文件"。

您也可以从控制台的风险日志中删除客户端计算机上的隔离项目。

请参见第185页的"关于使用监视器和报告来帮助确保网络安全"。

# 关于使用防病毒和防间谍软件策略

您可以通过创建和修改其他类型的策略的类似方式创建与编辑防病毒和防间谍软件策略。您可以分配、撤回、替换、复制、导出、导入或删除防病毒和防间谍软件策略。

您通常可将一个策略分配至安全网络中的多个组。如果对特定位置有特定要求,您 可以创建一个非共享、位置限定的策略。

对于本章所涉及的过程,我们是在假定您对策略配置的基本概念熟悉的情况下进行 介绍的。

请参见第 282 页的"关于策略"。

# 关于病毒和安全风险

"防病毒和防间谍软件策略"会扫描病毒和安全风险;安全风险包括间谍软件、广告软件和其他会导致计算机或网络有风险的文件等等。防病毒和防间谍软件扫描会检测内核级的Rootkit。Rootkit是任何试图在计算机操作系统中藏匿自身并可用于恶意目的的程序。

默认的"防病毒和防间谍软件策略"会执行下列操作:

- 检测、消除和修复病毒、蠕虫、特洛伊木马和混合型威胁的负面影响。
- 检测、消除和修复广告软件、拨号程序、黑客工具、玩笑程序、远程访问程序、 间谍软件、跟踪软件等的负面影响。

表 26-2 说明了客户端软件可扫描的风险类型。

表 26-2 病毒和安全风险

风险	说明
病毒	在运行时将其自身的副本附加到其他计算机 程序或文档的程序或代码。当受感染的程序 运行时,附加的病毒程序会激活,并将自己 附加到其他程序和文档中。当用户打开含有 宏病毒的文档时,就会激活附加的病毒程序, 并将自己附加到其他程序或文档中。
	病毒通常造成一定的负载,如在特定的日期 显示一则消息。有些病毒会专门损坏数据。 这些病毒会损坏程序、删除文件或重新格式 化磁盘。
恶意的 Internet Bot	在 Internet 上运行自动化任务的具有恶意企 图的程序。
	Bot可用来对计算机执行自动攻击,或从Web 站点收集信息。
蠕虫	自我复制但不会感染其他程序的程序。有些 蠕虫通过在磁盘间自我复制来进行传播,而 另外一些蠕虫只在内存中进行复制,从而降 低计算机的速度。
特洛伊木马	将自己隐藏在诸如游戏或实用程序之类的无 害程序中的恶意程序。
混合型威胁	将病毒、蠕虫、特洛伊木马和恶意代码的特征与服务器和 Internet 漏洞结合以启动、传送和传播攻击的威胁。混合型威胁利用多种方法和技术迅速传播,导致破坏波及整个网络。

风险	说明
广告软件	通过 Internet 秘密收集个人信息并将其中继回另一计算机的独立程序或附加程序。广告软件可以跟踪浏览习惯以进行广告宣传,还可以发送广告宣传内容。
	广告软件可以在用户不知情的情况下,从Web 站点(通常以共享软件或免费软件的形式) 下载或通过电子邮件或即时消息程序感染。 通常,用户在接受软件程序的最终用户授权 许可协议时会不知不觉地下载广告软件。
拨号程序	这类程序通常会在用户未许可或不知情的状况下,利用计算机通过 Internet 拨号到 900 号码或 FTP 站点。通常,拨打这些号码会产 生费用。
黑客工具	黑客用来对用户计算机进行未经授权的访问 的程序。例如,一种黑客工具是击键记录程 序,它跟踪并记录各次击键并将此信息发送 给黑客。然后,黑客可以执行端口扫描或漏 洞扫描。黑客工具还可用于创建病毒。
玩笑程序	以幽默或令人恐惧的方式改变或中断计算机 操作的程序。例如,可以从 Web 站点、电子 邮件或即时消息程序下载的程序。它可以在 用户尝试删除它时使回收站远离鼠标,或者 使鼠标单击造成相反的结果。
其他	这是不符合病毒、特洛伊木马、蠕虫或其他 安全风险类别严格定义的任何其他安全风险。
远程访问程序	可通过 Internet 从其他计算机进行访问以便 获取信息或者攻击或修改用户计算机的程序。 例如,在用户自己不知情的情况下,用户可 能安装某个程序,或其他进程可能安装某个 程序。该程序可在修改或不修改原始远程访 问程序的情况下用于恶意目的。
间谍软件	可以秘密监控系统活动并检测密码及其他保 密信息,然后将信息中继回另一计算机的独 立程序。
	间谍软件可以在用户不知情的情况下,从Web 站点(通常以共享软件或免费软件的形式) 下载或通过电子邮件和即时消息程序感染。 通常,用户在接受软件程序的最终用户授权 许可协议时会不知不觉地下载间谍软件。

风险	说明
跟踪软件	跟踪用户在 Internet 上的路径并向目标系统 发送信息的独立应用程序或附加应用程序。 例如,此类应用程序可以从 Web 站点、电子 邮件或即时消息程序下载。然后,它可以获 取与用户行为相关的保密信息。

默认情况下,自动防护在运行时会扫描病毒、特洛伊木马、蠕虫和安全风险。

诸如 Back Orifice 之类的某些风险在早期客户端软件版本中被视为病毒。这些风险 会继续被视为病毒,以便客户端软件能够针对旧计算机提供防护。

# 关于扫描

您可以在"防病毒和防间谍软件策略"中包括下列类型的扫描:

- 防病毒和防间谍软件扫描
  - 自动防护扫描
  - 管理员定义的扫描
- TruScan 主动型威胁扫描

默认情况下,所有防病毒和防间谍软件扫描都会检测病毒和安全风险,例如广告软件和间谍软件;这类扫描会隔离病毒和安全风险,然后消除或修复它们的负面影响。自动防护扫描和管理员定义的扫描会检测已知的病毒和安全风险。主动型威胁 扫描会通过扫描潜在恶意行为来检测未知病毒和安全风险。

**注意**:在某些情况下,您可能会无意中安装了一个包含安全风险(如广告软件或间 谍软件)的应用程序。如果 Symantec 确定禁止该风险并不会损害计算机,则客户 端软件就会禁止该风险。如果禁止风险可能会使计算机处于不稳定状态,则客户端 软件会等应用程序安装完毕后再隔离风险。然后修复该风险的负面影响。

# 关于自动防护扫描

自动防护扫描包括下列类型的扫描:

- 文件系统自动防护扫描
- Lotus Notes 和 Outlook (MAPI 和 Internet )的自动防护电子邮件附件扫描
- 针对使用POP3或SMTP通信协议的Internet电子邮件与附件的自动防护扫描; Internet 电子邮件的自动防护扫描还包括出站电子邮件启发式扫描

**注意**:由于性能原因,服务器操作系统不支持 POP3 的 Internet 电子邮件自动防护。请不要在 Microsoft Exchange 服务器上安装 Microsoft Outlook 自动防护。

自动防护会持续扫描从计算机读取或写入计算机的文件和电子邮件数据是否有病毒 或安全风险;病毒和安全风险可能包括间谍软件或广告软件。

您可以将自动防护配置为仅扫描选择的文件扩展名。当它扫描选择的扩展名时,即 使病毒更改了文件的扩展名,自动防护也能确定文件的类型。

配置自动防护设置时,若要针对病毒与安全风险强制执行公司的安全策略,您可在 客户端上锁定自动防护选项。用户不能更改您锁定的选项。

默认情况下,自动防护已启用。您可以在控制台的"客户端"选项卡下查看自动防护状态,也可以通过生成显示计算机状态的报告和日志进行查看。还可以直接在客户端上查看自动防护状态。

自动防护扫描会扫描下列应用程序的电子邮件附件:

- Lotus Notes 4.5x、4.6、5.0 和 6.x
- Microsoft Outlook 98/2000/2002/2003/2007 (MAPI 和 Internet )

如果通过 MAPI 或 Microsoft Exchange 客户端使用 Microsoft Outlook,且已为电 子邮件启用自动防护,则附件会立即下载到运行此电子邮件客户端的计算机上。当 用户打开邮件时,便会扫描附件。如果您通过速度较慢的连接下载大型附件,则会 影响邮件性能。对于经常收到大型附件的用户,您可能想禁用此功能。

**注意**: 当您执行客户端软件安装时,如果计算机上已安装 Lotus Notes 或 Microsoft Outlook,则客户端软件会检测到该电子邮件应用程序。接着客户端会安装正确的自动防护电子邮件类型。如果您在执行手动安装时选择完整安装,则会安装两个类型。

如果电子邮件程序不是支持的数据格式之一,则可以在文件系统上启用自动防护来 保护您的网络。如果用户在 Novell GroupWise 电子邮件系统上收到附件受感染的 邮件,则当用户打开附件时,自动防护就会检测到病毒。这是因为大部分的电子邮 件程序会在用户从电子邮件程序启动附件时,将该附件保存到临时目录。如果您在 文件系统上启用自动防护,则自动防护会在附件写入临时目录时检测到病毒。如果 用户尝试将受感染的附件保存到本地驱动器或网络驱动器,则自动防护也会检测到 病毒。

### 关于自动防护检测持续下载同样的安全风险的进程

如果自动防护检测到某个进程不断将安全风险下载到客户端计算机,便会显示通知 并记录检测。(自动防护必须配置为发送通知。)如果进程持续下载同一安全风 险,则用户计算机上会多次显示通知,且自动防护会记录多个事件。为避免多次通 知和记录多个事件,自动防护会在检测到此安全风险三次后,自动停止发送关于该 安全风险的通知。此外,自动防护在检测到同一事件三次后,也会停止记录该事件。

在某些情况下,自动防护不会停止发送安全风险的通知,也不会停止记录安全风险 事件。

在下列任一情况下,自动防护会不断发送通知并记录事件:

- 您或客户端计算机的用户禁用安全风险的安装禁止功能(默认为启用)。
- 对进程下载的安全风险类型所采取的操作含有"不操作"的操作时。

### 关于自动排除文件和文件夹

客户端软件会自动检测某些第三方应用程序和 Symantec 产品是否存在。检测到它 们后,客户端软件会为这些文件和文件夹创建排除项。客户端会将这些文件和文件 夹排除在所有防病毒和防间谍软件扫描范围之外。

客户端软件会自动为以下项目创建排除项:

- Microsoft Exchange
- Active Directory 域控制器
- 某些 Symantec 产品

**注意:**若要查看客户端在 32 位计算机上创建的排除项,您可以检查 HKEY\_LOCAL\_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions 注册表的内容。切勿直接编辑这个注册表。在 64 位计 算机上,请查看 HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions 中的内容。

客户端不会将系统临时文件夹排除在扫描范围之外,因为这样会给计算机带来极大的安全漏洞。

您可以使用集中式例外来配置其他任何排除项。

有关使用集中式例外的信息,请参见第465页的"配置集中式例外策略"。

#### 关于自动排除 Microsoft Exchange Server 的文件和文件夹

如果在已安装 Symantec Endpoint Protection 客户端的计算机上还安装有 Microsoft Exchange Server,客户端软件会自动检测到 Microsoft Exchange。当客户端软件 检测到 Microsoft Exchange Server 时,会创建适当的文件和文件夹排除项,而文 件系统自动防护和所有其他扫描会排除这些项。Microsoft Exchange Server 可包括 群集服务器。客户端软件会定期检查相应 Microsoft Exchange 文件和文件夹位置是 否有所变化。如果您在已安装客户端软件的计算机上安装 Microsoft Exchange,则

在客户端检查有无变化时会创建排除项。客户端会排除相应的文件和文件夹;如果 某单个文件移出了所排除的文件夹,此文件仍然在排除范围之内。

客户端软件可为下列版本的MicrosoftExchange服务器创建文件和文件夹扫描排除项:

- Exchange 5.5
- Exchange 6.0
- Exchange 2000
- Exchange 2003
- Exchange 2007
- Exchange 2007 SP1

对于 Exchange 2007,请参见用户文档了解其与防病毒软件的兼容性。在少数情况下,可能需要为某些 Exchange 2007 文件夹手动创建扫描排除项。例如,在群集环境中,您可能需要创建一些排除项。

有关详细信息,请参见 Symantec 知识库中的 Preventing Symantec Endpoint Protection 11.0 from scanning the Microsoft Exchange 2007 directory structure (防止 Symantec Endpoint Protection 11.0 扫描 Microsoft Exchange 2007 目录结 构),网址为:

http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007072619121148

#### 关于自动排除 Symantec 产品中的文件和文件夹

在检测到某些 Symantec 产品时,客户端会为这些产品创建适当的文件和文件夹扫 描排除项。

客户端会为下列 Symantec 产品创建排除项:

- Symantec Mail Security 4.0/4.5/4.6/5.0/6.0 for Microsoft Exchange
- Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange
- Norton AntiVirus 2.x for Microsoft Exchange
- Symantec Endpoint Protection Manager 嵌入式数据库和日志

#### 关于自动排除 Active Directory 文件和文件夹

客户端软件会为 Active Directory 域控制器数据库、日志和工作文件创建文件和文件夹排除项。客户端会监控安装在客户端计算机上的应用程序。如果软件检测到客户端计算机上安装有 Active Directory,便会自动创建排除项。

## 如果客户端电子邮件应用程序使用单个收件箱

Outlook Express、Eudora、Mozilla 和 Netscape 都是将所有电子邮件存储在单个 文件的应用程序。如果客户端计算机使用的是任何使用单个收件箱的电子邮件应用 程序,您应该创建集中式例外以将收件箱文件排除在外。例外会应用于所有防病毒 和防间谍软件扫描,也会应用于自动防护。

只要满足以下两个条件,Symantec Endpoint Protection 客户端会隔离整个收件 箱,用户便不能访问电子邮件:

- 客户端运行按需扫描或调度扫描时,在收件箱文件中检测出病毒。
- 为此病毒配置的操作是"隔离"。

Symantec 通常不建议您将某些文件排除在扫描范围之外。若将收件箱文件排除在 扫描范围之外,便不能隔离收件箱;但是,如果客户端在用户打开电子邮件时检测 出病毒,客户端可以将该邮件安全隔离或删除。

# 关于管理员定义的扫描

管理员定义的扫描是一种防病毒和防间谍软件扫描,可检测已知的病毒和安全风 险。为了达到最完备的防护,您应该为客户端计算机调度不定期的扫描。自动防护 扫描读入和读出计算机的文件和电子邮件,与之不同的是,管理员定义的扫描则是 检测病毒和安全风险。管理员定义的扫描会通过检查所有文件和进程(或部分文件 和进程)来检测病毒和安全风险。管理员定义的扫描也可扫描内存和加载点。

可以在设置防病毒和防间谍软件策略时配置管理员定义的扫描。

管理员定义的扫描包括以下类型的扫描:

- 调度扫描
- 按需扫描

常规而言,您最好每周运行一次全面的调度扫描,每天运行一次活动扫描。默认情况下,Symantec Endpoint Protection 客户端会在每次客户端计算机启动时运行活动扫描。

#### 关于调度扫描

您可以将扫描调度在特定时间运行。用户也可以从客户端计算机为他们的计算机调度扫描,但是他们不能更改或禁用您为他们的计算机调度的扫描。客户端软件一次 会运行一个调度扫描。如果将一个以上的扫描调度在同一时间进行,则它们会依次 运行。

调度扫描的设置和自动防护扫描设置类似,但是这两种扫描必须分别配置。您配置 的集中式例外可应用于所有类型的防病毒和防间谍软件扫描。

如果计算机在某一调度扫描期间为关闭状态,除非计算机已配置为运行错过的扫描 事件,否则此扫描不会运行。 调度扫描会检查文件是否带有病毒和安全风险,例如,间谍软件和广告软件。 表 26-3 介绍了调度扫描的类型。

表 26-3 调度扫描的类型

类型	说明
活动扫描	非常快速地扫描系统内存以及计算机上的所有常见病毒和 安全风险位置。此类型扫描的扫描范围包括所有在内存中 运行的进程、重要的注册表文件,以及 config.sys 和 windows.ini之类的文件,还包括一些重要的操作系统文件 夹。
全面扫描	扫描整个计算机中是否有病毒和安全风险,包括引导扇区 和系统内存。
自定义扫描	扫描针对病毒和安全风险而选择的文件和文件夹。

## 关于按需扫描

您可以通过从控制台运行按需扫描来检查选定客户端计算机上的选定文件和文件 夹。按需扫描可为对网络区域或本地硬盘驱动器的扫描立即提供扫描结果。您可以 从控制台的"客户端"选项卡运行这类扫描。也可以从控制台的"监视器"选项卡 运行这类扫描。

请参见第362页的"运行按需扫描"。

请参见第 173 页的"从日志运行命令和操作"。

默认按需扫描可扫描所有的文件和文件夹。您可以在防病毒和防间谍软件策略中更 改按需扫描的设置。在此策略中,您可以指定要扫描的文件扩展名和文件夹。从 "显视器"页面运行按需扫描时,扫描会按照策略中配置的设置扫描客户端。

请参见第 361 页的"配置按需扫描选项"。

# 关于 TruScan 主动型威胁扫描

TruScan 主动型威胁扫描会使用启发式扫描查找与病毒和安全风险行为类似的行为。防病毒和防间谍软件扫描是检测已知的病毒和安全风险,而主动型威胁扫描则 是检测未知的病毒和安全风险。

**注意**:由于主动型威胁扫描会检查客户端计算机上活动的进程,因此此类型扫描会 影响系统性能。 默认情况下,客户端软件会运行主动型威胁扫描。您可以在防病毒和防间谍软件策 略中启用或禁用主动型威胁扫描。如果您未锁定此设置,则客户端计算机的用户可 以启用或禁用此类型的扫描。

虽然防病毒和防间谍软件策略包括主动型威胁扫描的设置,但是此类型扫描设置的 配置方式有别于防病毒和防间谍软件扫描设置。

请参见第 419 页的"关于 TruScan 主动型威胁扫描"。

# 关于更新定义文件之后的扫描

如果自动防护已激活,客户端软件会立即使用更新后的定义文件开始扫描。

若定义文件已更新,客户端软件会尝试修复存储在隔离区中的文件,并扫描活动的 进程。

主动型威胁扫描检测到的已隔离文件会加以扫描,以此检查这些文件是否有当前认定的病毒或安全风险。客户端扫描主动型威胁扫描隔离项目的方式与客户端扫描其他类型扫描隔离的项目相似。对于隔离的检测项目,客户端软件会完成补救操作,并清除任何负面影响。如果该主动型威胁检测项目已列入 Symantec 白名单,则客户端软件会还原该检测项目,并将其从隔离区中删除;但不会重新启动该进程。

# 关于扫描选定扩展名或文件夹

对于各种类型的防病毒和防间谍软件扫描与自动防护,您可以按照扩展名选择要包括的文件。对于管理员定义的扫描,您也可以按照文件夹选择要包括的文件。例如,您可以指定调度扫描只扫描某些扩展名,而自动防护扫描所有扩展名。

当您选择用于扫描的文件扩展名或文件夹时,可以选择要扫描的多个扩展名或文件 夹。任何未选的扩展名或文件夹都不会包括在扫描范围之内。

在"文件扩展名"对话框中,您可以快速添加所有常见程序或所有常见文件的扩展 名,也可以自行添加扩展名。自行添加扩展名时,扩展名长度不可超过四个字符。

在"编辑文件夹"对话框中,请选择Windows文件夹,而不选择绝对文件夹路径。 在安全网络的客户端计算机上,这些文件夹可能使用不同的路径。您可以选择下列 任一文件夹:

- COMMON\_APPDATA
- COMMON\_DESKTOPDIRECTORY
- COMMON\_DOCUMENTS
- COMMON\_PROGRAMS
- COMMON\_STARTUP
- PROGRAM\_FILES
- PROGRAM\_FILES\_COMMON

- SYSTEM
- WINDOWS

如果只扫描选定文件扩展名或文件夹,可以改善扫描性能。例如,如果您要复制一 个大型文件夹,且此文件夹不在所选扫描文件夹列表中,则复制过程可以快速进 行,因为此文件夹的内容已排除在扫描范围之外。

您可以按照扩展名或目录类型将某些文件排除在扫描范围之外。您可以通过配置包括排除项的集中式例外策略来将某些文件排除在扫描范围之外。策略中若有指定排除项,则每次客户端使用该策略运行任何防病毒和防间谍软件扫描时,都会排除这些项。

请参见第465页的"配置集中式例外策略"。

建议扫描的文件扩展名

扫描所选扩展名时,客户端软件不会通过读取文件头来确定文件类型。扫描所选扩 展名时,客户端只扫描具有您指定的扩展名的文件。

警告:由于客户端软件会将某些文件和文件夹排除在扫描范围之外,因此它不会保 护这些排除的文件和文件夹免遭病毒和安全风险的攻击。

文件扩展名	说明
СНМ	Microsoft Windows 的 HTML 编译帮助文件
386	驱动程序
ACM	驱动程序; 音频压缩管理器
ACV	驱动程序; 音频压缩或解压缩管理器
ADT	ADT 文件; 传真
AX	AX 文件
BAT	批处理文件
BTM	批处理文件
BIN	二进制
CLA	Java 类
CMD	命令文件
СОМ	可执行文件

表 26-4 说明了建议扫描的扩展名。

表 26-4

文件扩展名	说明
CPL	Microsoft Windows的 Applet 控制面板
CSC	Corel 脚本
CSH	UNIX Shell 脚本
DLL	动态链接库
DOC	Microsoft Word
DOT	Microsoft Word
DRV	驱动程序
EXE	可执行文件
HLP	帮助文件
НТА	HTML 应用程序
НТМ	HTML
HTML	HTML
HTT	HTML
INF	安装脚本
INI	初始化文件
JPEG	图形文件
JPG	图形文件
JS	JavaScript
JSE	以 JavaScript 编码的程序
JTD	Ichitaro
MDB	Microsoft Access
MP?	Microsoft Project
MSO	Microsoft Office 2000
OBD	Microsoft Office 活页夹
OBT	Microsoft Office 活页夹
OCX	链接和嵌入自定义控件的 Microsoft 对象
文件扩展名	说明
-------	--
OV?	Overlay 文件
PDF	Adobe 可移植文档格式
PIF	程序信息文件
PL	PERL 程序源代码 (UNIX)
РМ	演示管理器位图
РОТ	Microsoft PowerPoint
РРТ	Microsoft PowerPoint
PPS	Microsoft PowerPoint
RTF	RTF 文档
SCR	传真、屏幕保护程序、快照或 Farview 或 Microsoft Windows 的脚本
SH	Shell 脚本 (UNIX)
SHB	Corel Show Background 文件
SHS	Shell 片断文件
SMM	Lotus AmiPro
SYS	设备驱动程序
VBE	VESA BIOS (核心函数)
VBS	VBScript
VSD	Microsoft Office Visio
VSS	Microsoft Office Visio
VST	Microsoft Office Visio
VXD	虚拟设备驱动程序
WSF	Windows 脚本文件
WSH	Windows Script Host 设置文件
XL?	Microsoft Excel
XL??	Microsoft Excel

文件扩展名	说明
ACCD?	Microsoft Office Access
DOC?	Microsoft Office Word
DOT?	Microsoft Office Word
PP?	Microsoft Office PowerPoint
PP??	Microsoft Office PowerPoint

# 关于排除指定的文件及文件夹

公司的安全策略可能允取您的计算机保留某些安全风险。您可以将客户端配置为将这些风险排除在所有防病毒和防间谍软件扫描的范围之外。

您可以将指定文件和文件夹排除在自动防护和管理员定义的扫描范围之外。例如, 您可以排除 C:\Temp\Install 路径或包含可允许的安全风险的文件夹。您可以排除 会触发误报警报的文件。例如,如果您先前使用其他病毒扫描程序清除受感染的文 件,程序可能没有完全删除病毒代码。该文件可能是无害的,但是禁用的病毒代码 可能会造成客户端软件记录误报。如果您不确定文件是否受到感染,请向Symantec 技术支持咨询。

创建排除项后,该排除项将应用于您运行的所有防病毒和防间谍软件扫描类型。您 可以创建属于集中式例外的排除项。

请参见第465页的"配置集中式例外策略"。

# 关于针对扫描检测到的病毒与安全风险所采取的操作

许多相同的扫描选项适用于不同的扫描类型。当您配置按需、调度或自动防护扫描 时,可以指定客户端软件发现病毒与安全风险时要采取的第一个与第二个操作。

您可以分别指定客户端发现下列类型风险时所采取的第一个与第二个操作:

- 宏病毒
- 非宏病毒
- 所有安全风险(广告软件、间谍软件、玩笑程序、拨号工具、黑客工具、远程 访问程序、跟踪软件等等)
- 个别类别的安全风险,例如间谍软件
- 为特定的安全风险实例自定义操作

默认情况下,Symantec Endpoint Protection 客户端会先尝试清除受病毒感染的文件。

如果客户端软件不能清除文件,就会执行下列操作:

- 将文件移至受感染计算机上的隔离区
- 拒绝访问文件
- 记录事件

默认情况下,客户端会将受安全风险感染的任何文件移至受感染计算机上的隔离 区。客户端也会尝试消除或修复风险的负面影响。默认情况下,隔离区包含所有客 户端已执行操作的记录。必要时,计算机可以回到客户端尝试消除和修复操作之前 所存在的状态。

如果不能隔离与修复安全风险,则第二个操作会将风险记录下来。

对于 TruScan 主动型威胁扫描检测结果,会根据您是使用 Symantec 管理的默认值 还是选择自行设置操作来决定具体操作。您可以在"防病毒和防间谍软件策略"的 一个单独部分中配置主动型威胁扫描的操作。

请参见第 427 页的"指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级别"。

# 在防病毒和防间谍软件策略中设置日志处理参数

您可以在"防病毒和防间谍软件策略"中包括日志处理参数。默认情况下,客户端 始终会将某些类型的事件发送至管理服务器(例如,"已停止扫描"或"已开始扫 描")。您可以选择是否发送其他类型的事件(例如,"文件未扫描")。

客户端发送至管理服务器的事件会影响报告和日志中的信息。您应该决定要将哪个 类型的信息转发至管理服务器。如果只选择某些类型的事件,则可减小日志的大小 和报告涵盖的信息量。

您也可以配置客户端保留日志条目的时间长短。此选项不会影响客户端发送至管理 控制台的任何事件。您可以使用此选项来减少客户端计算机上的实际日志大小。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 设置"防病毒和防间谍软件策略"的日志处理参数

- 1 在"防病毒和防间谍软件策略"页面上,单击"其他"。
- 2 在"日志处理"选项卡的"防病毒和防间谍软件日志事件过滤"下方,选择您 要转发至管理服务器的事件。
- 3 在"日志保留"下方,选择客户端删除日志行的频率。
- 4 在"日志事件汇总"下方,选择将汇总事件发送至服务器的频率。
- 5 完成此策略的配置后,单击"确定"。

# 关于客户端与防病毒和防间谍软件交互的选项

您可以在策略中配置用于控制客户端用户体验的特定参数。 您可以执行下列操作之一:

- 配置调度扫描的扫描进度选项。
- 设置客户端的扫描选项。
- 更改扫描映射驱动器所需的密码。
- 指定 Windows 安全中心与 Symantec Endpoint Protection 客户端的交互方式。
- 在定义过时或丢失时显示警告。
- 指定要在防病毒和防间谍软件错误通知中显示的 URL。
- 指定安全风险尝试更改 URL 时重定向 Internet 浏览器的 URL。

您可以在受感染计算机上显示并自定义警告消息。例如,如果用户的计算机上安装 间谍软件程序,您可以通知他们已经违反公司策略。您可以在通知中加入用户必须 立即卸载应用程序的消息。

注意:您也可以锁定策略设置,以使用户不能更改设置。

# 更改扫描映射网络驱动器所需的密码

在可以扫描映射的网络驱动器之前,客户端计算机上的 Symantec Endpoint Protection 会要求用户提供密码。默认情况下,此密码设为 symantec。

注意:如果用户扫描网络驱动器,该扫描可能会影响客户端计算机的性能。

有关以下步骤中所使用选项的详细信息,您可以单击"帮助"。

#### 更改扫描映射驱动器所需的密码

- 1 在"防病毒和防间谍软件策略"页面上,单击"其他"。
- 2 在"其他"选项卡的"扫描网络驱动器"下方,选中"扫描映射网络驱动器前 请求键入密码"。
- 3 单击"更改密码"。
- 4 在"配置密码"对话框中键入新密码,并再次键入密码以进行确认。
- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

# 指定 Windows 安全中心与 Symantec Endpoint Protection 客户端的交互方式

如果您使用 Windows XP Service Pack 2 或 Windows Vista 的 Windows 安全中心,则可以使用"防病毒和防间谍软件策略"在客户端计算机上设置下列选项:

- 定义文件经过多长时间后, Windows 安全中心将其视为过期。
- Windows 安全中心是否在主机计算机上显示 Symantec 产品的防病毒警报。

**注意**:不管 Windows 安全中心是处于启用状态还是禁用状态,您都可以随时在管理控制台中看到 Symantec 产品的状态。

# 将Symantec Endpoint Protection 客户端配置为禁用 Windows 安全中 心

您可以配置客户端软件在哪些情况下禁用 Windows 安全中心。

#### 配置 Symantec Endpoint Protection 禁用 Windows 安全中心

- 1 在"防病毒和防间谍软件策略"页面上,单击"其他"。
- **2** 单击"其他"选项卡。
- 3 在 Windows 安全中心下方的"禁用 Windows 安全中心"下拉列表中,选择下 列选项之一:

从不	永不禁用 Windows 安全中心。
一次	只禁用一次 Windows 安全中心。如果用户重新启用它,客户端软件将不再禁用它。
始终	始终禁用Windows安全中心。如果用户重新启用它,客户端软件 会立即再次禁用它。
还原	只有在 Symantec Endpoint Protection 禁用 Windows 安全中心的 情况下才予以重新启用。

4 单击"确定"。

# 配置在主机计算机上显示 Symantec Endpoint Protection 警报

您可以将 Windows 安全中心配置为显示来自 Symantec Endpoint Protection 客户 端的警报。

#### 配置在主机计算机上显示警报

- 1 在"防病毒和防间谍软件策略"页面上,单击"其他"。
- **2** 单击"其他"选项卡。
- 3 在 "Windows 安全中心"下方的 "显示 Windows 安全中心内的防病毒警报" 下拉菜单中,选择下列选项之一:

禁用	Windows 安全中心不会在 Windows 通知区域中 显示这些警报。
启用	Windows 安全中心会在 Windows 通知区域中显示这些警报。
使用现有设置	Windows 安全中心会使用现有的设置来显示这些 警报。

**4** 单击"确定"。

# 配置定义的过期时间

默认情况下,Windows 安全中心会将 Symantec 定义的有效期设为 30 天。您可以 在 Windows Installer 运行安装期间,更改定义的有效天数。您也可以在"防病毒 和防间谍软件策略"中更改设置。

在客户端计算机上, Symantec Endpoint Protection 客户端每 15 分钟检查一次, 以比较过期时间、定义的日期和当前日期。通常情况下,因为定义常常是自动更新 的,所以不会向 Windows 安全中心报告过期状态。如果您手动更新定义,则可能 需要等 15 分钟才会在 Windows 安全中心中看到正确的状态。

#### 配置定义的过期时间

- 1 在"防病毒和防间谍软件策略"页面上,单击"其他"。
- **2** 单击"其他"选项卡。
- 3 在"Windows 安全中心"下方的"定义过期时,显示 Windows 安全中心消息"之下,键人天数。您也可以使用向上或向下箭头选择病毒和安全风险定义的有效天数。

值的范围为1到30。

4 完成此策略的配置后,单击"确定"。

# 在定义过期或丢失时显示警告

您可以显示并自定义病毒与安全风险定义过期或丢失时,在客户端计算机上出现的 警告消息。如果您并未调度自动更新,您可能会想要警告用户。如果您允许用户关 闭 LiveUpdate,您可能也会想要警告用户。

#### 显示有关定义的警告

- 1 在"防病毒和防间谍软件策略"页面上,单击"其他"。
- 2 在"通知"选项卡的"操作"下方,选择下列选项之一,或两项全选:
  - 当定义过期时显示消息
  - Symantec Endpoint Protection 在没有病毒定义的情况下运行时显示警告
- 3 针对过期的病毒与安全风险定义,设置定义过期几天后出现警告。
- 4 针对丢失的病毒与安全风险定义,设置在出现警告前,Symantec Endpoint Protection 必须运行的补救尝试次数。
- 5 在每个所选中的选项上,单击"警告",然后自定义默认消息。
- 6 在警告对话框中单击"确定"。
- 7 完成此策略的配置后,单击"确定"。

# 指定出现在防病毒和防间谍软件错误通知中的 URL

在极少数情况下,用户可能会看到客户端计算机上出现错误。例如,客户端计算机 可能会在扫描过程中出现缓冲区溢出或解压缩问题。

您可以指定导向 Symantec 支持网站的 URL 或指定自定义 URL。例如,您可能想 指定内部网站。

注意: URL 也会出现在所发生错误的客户端计算机的系统事件日志中。

#### 指定出现在防病毒和防间谍软件错误通知中的 URL

- 1 在"防病毒和防间谍软件策略"页面上,单击"其他"。
- 2 在"通知"选项卡上,选中"显示错误消息并在其中显示指向解决方案的 URL"。
- 3 选择下列选项之一:
  - 显示指向 Symantec 技术支持知识库文章的 URL
  - 显示自定义 URL
- 4 如果您要自定义消息,请单击"自定义错误消息"。

- 5 输入要添加的自定义文本,再单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

# 指定浏览器主页的 URL

您可以指定当 Symantec Endpoint Protection 客户端修复拦截浏览器主页的安全风 险时要作为主页的 URL。

#### 指定浏览器主页的 URL

- 1 在"防病毒和防间谍软件策略"页面上,单击"其他"。
- 2 在"其他"选项卡的"Internet 浏览器防护"下方,键入 URL。
- 3 完成此策略的配置后,单击"确定"。

# 配置应用于防病毒和防间谍软件扫描的选项

某些扫描选项是所有防病毒和防间谍软件扫描公用的。防病毒和防间谍软件扫描包括自动防护扫描和管理员定义的扫描。 策略包括下列选项:

- 配置所选文件扩展名或文件夹的扫描
- 配置安全风险的集中式例外
- 配置对检测到的已知病毒和安全风险执行的操作
- 管理在受感染计算机上显示的通知消息
- 在受感染的计算机上自定义并显示通知
- 在受感染的电子邮件中添加警告
- 通知受感染电子邮件的发件人
- 通知受感染电子邮件的用户

有关主动型威胁扫描的操作和通知的信息将在另一节中进行说明。

请参见第 429 页的"配置 TruScan 主动型威胁扫描的通知"。

#### 配置所选文件扩展名的扫描

如果只扫描具有所选扩展名的文件,则 Symantec Endpoint Protection 客户端会更快地完成扫描。虽然只扫描所选扩展名对计算机的防护程度较低,但在只扫描所选 扩展名时,可以选择病毒通常攻击的文件类型。扫描所选扩展名时,扫描会更加有效,且使用的计算机资源也较少。

您可以配置要扫描的扩展名,在下列要求之间获取平衡:

- 网络所需的防护程度
- 提供防护所需的时间和资源数量

例如,您可能想只扫描具有很可能包含病毒或其他风险的扩展名的文件。当您只扫 描特定扩展名时,具有其他扩展名的所有文件会自动从扫描中排除。将文件从扫描 中排除时,就会减少运行扫描所需的计算机资源数量。

警告: 当您选择要扫描的扩展名时, 任何其他扩展名就不会防御病毒和安全风险。

有关以下步骤中所使用选项的详细信息,您可以单击"帮助"。

#### 只将具有特定扩展名的文件加入自动防护或管理员定义的扫描

- 1 在"扫描详细信息"选项卡的"文件类型"下,单击"只扫描选择的扩展名"。
- **2** 单击"选择扩展名"。
- 3 在"文件扩展名"对话框中,您可以执行下列任何操作:
  - 若要添加您自己的扩展名, 请键入扩展名, 再单击"添加"。
  - 若要删除任何扩展名,请选择扩展名,再单击"删除"。
  - 若要将列表恢复为默认设置,请单击"使用默认值"。
  - 若要添加所有程序扩展名,请单击"添加公用程序"。
  - 若要添加所有文档扩展名,请单击"添加公用文档"。
- 4 完成此策略的配置后,单击"确定"。

#### 配置选定文件夹的扫描

您可以配置选定文件夹,以运行某些管理员定义的扫描。这些管理员定义的扫描包括自定义调度扫描和按需扫描。您不能配置选定文件夹进行自动防护。 请参见第 322 页的"关于扫描选定扩展名或文件夹"。 可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置选定文件夹的扫描

- 1 在"防病毒和防间谍软件策略"页面上,单击"管理员定义的扫描"。
- 2 在"扫描"选项卡上,执行下列操作之一:
  - 単击"添加"。
  - 在"调度扫描"下,选择现有扫描,再单击"编辑"。
  - 在"管理员按需扫描"下,单击"编辑"。

- 3 在"扫描详细信息"选项卡的"扫描类型"下拉列表中,单击"自定义扫描"。 按需扫描预先设置为"自定义扫描"。
- 4 在"扫描"下,单击"编辑文件夹"。
- 5 在"编辑文件夹"对话框中,单击"扫描选定文件夹",然后在文件夹列表中,选中要进行此扫描的所有文件夹。

"选定的文件夹"字段将显示您的所有选择。

- 6 单击"确定",直至返回"管理员定义的扫描"页面。
- 7 完成此策略的配置后,单击"确定"。

#### 关于安全风险的例外

如果您要在网络保留任何安全风险,则这些风险在客户端计算机上检测到时,您可以将其忽略。

若用户对某项安全风险配置了自定义操作,但您已指定忽略该项安全风险,则用户 的自定义操作将不会采用。

**注意**: 当您将某安全风险添加到例外列表后, Symantec Endpoint Protection 客户 端将不再记录任何与此安全风险有关的事件。不过即使该风险已列入例外列表, 您 仍可以配置客户端记录该风险。不论是否记录该风险,当计算机出现该风险时, 用 户都不会收到任何通知。

您可以使用集中式例外策略来配置例外。

请参见第465页的"配置集中式例外策略"。

## 配置要针对检测到的已知病毒和安全风险执行的操作

使用这些操作可指定当防病毒和防间谍软件扫描检测到已知病毒或安全风险时,客 户端该如何响应。这些操作适用于自动防护扫描和管理员定义的扫描。您可以针对 主动型威胁扫描分别配置操作。

请参见第 419 页的"关于 TruScan 主动型威胁扫描"。

通过这些操作可设置客户端软件在检测到已知病毒或安全风险时该如何响应。可以 指定第一个操作,并可以指定当第一个操作不能执行时要执行的第二个操作。 Symantec Endpoint Protection 客户端在发现病毒或诸如广告软件或间谍软件之类 的安全风险时,会采取这些操作。病毒和安全风险的类型列于层次结构中。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

**注意**:对于安全风险,请审慎使用删除操作。某些情况下,删除安全风险会导致应用程序丧失功能。

**警告:**如果将客户端软件配置为删除安全风险影响的文件,则不能再还原这些文件。

若要备份安全风险影响的文件,请将客户端软件配置为隔离文件。

#### 配置要针对检测到的已知病毒和安全风险执行的操作

- 在"操作"选项卡的"检测"下方,选择病毒或安全风险类型。
   在默认情况下,每个安全风险子类别都会自动配置为使用整个安全风险类别所 设置的操作。
- 2 若要将安全风险类别的特定实例配置为使用其他操作,请选中"覆盖为安全风险配置的操作",然后只为该类别设置操作。
- 3 在"操作目的"下方,选择客户端软件在检测到该类病毒或安全风险时要采取的第一个与第二个操作。
  您可以锁定操作,以使用户不能在使用此策略的客户端计算机上更改操作。
  对于安全风险,请审慎使用删除操作。某些情况下,删除安全风险会导致应用程序丧失功能。
- **4** 对于每个要设置操作的(病毒与安全风险)类别,重复步骤 **3**。
- 5 完成此策略的配置后,单击"确定"。

# 关于受感染计算机上的通知消息

可以使自定义通知消息在当管理员定义的扫描或自动防护发现病毒或安全风险时显示在受感染的计算机上。这些通知可以向用户发出警报以使用户查看其最近在客户端计算机上的活动。例如,用户可能因下载应用程序或查看网页而导致感染间谍软件。

**注意**:运行客户端的操作系统语言可能不能转译病毒名称中的某些字符。如果操作系统不能转译某些字符,这些字符会在通知中显示为问号。例如,某些Unicode病毒名称可能含有全角字符。在运行客户端的英语操作系统计算机上,这些字符会显示为问号。

对于电子邮件的自动防护扫描,还可以配置下列选项:

- 在受感染的电子邮件中添加警告
- 通知受感染电子邮件的发件人

■ 就受感染的电子邮件通知用户。

请参见第 353 页的"配置自动防护的通知选项"。

有关主动型威胁扫描结果的通知是单独配置的。

请参见第 429 页的"配置 TruScan 主动型威胁扫描的通知"。

# 在受感染的计算机上自定义并显示通知

您可以创建发现病毒或安全风险时在受感染计算机上显示的自定义消息。您可以通过直接在消息字段输入来添加或修改文本。

当您运行远程扫描时,您可以通过在受感染计算机屏幕上显示消息将问题通知用 户。在自定义警告消息时,您可以将像风险名称、受感染文件的名称、风险状态这 样的信息纳入其中。警告消息看起来可能类似以下示例:

#### 扫描类型:调度扫描

```
事件: 发现风险
安全风险名称: Stoned-C
文件: C:\Autoexec.bat
位置: C:
计算机: ACCTG-2
用户: JSmith
采取的操作:已清除
```

表 26-5 介绍了可用于通知消息的变量字段。

表 26-5 通知消息变量

字段	说明
SecurityRiskName	发现的病毒或安全风险的名称。
ActionTaken	为应对检测到的病毒或安全风险而采取的操作。
	此操作可以是已配置的第一操作或第二操作。
Status	文件的状态: "受感染"、"未感染"或"已删除"。
	该消息变量在默认情况下不使用。若要显示此信息,请手动将此变量添 加到消息。
Filename	病毒或安全风险感染的文件的名称。
PathAndFilename	病毒或安全风险感染的文件的完整路径和名称。
Location	病毒或安全风险所在计算机上的驱动器。
Computer	病毒或安全风险所在的计算机名。

字段	说明
User	出现病毒或安全风险时已登录的用户的名称。
Event	事件的类型,如"发现风险"。
LoggedBy	检测到病毒或安全风险的扫描类型。
DateFound	发现病毒或安全风险的日期。
StorageName	应用程序的受影响区域,例如,文件系统自动防护或Lotus Notes 自动防护。
ActionDescription	为应对检测到的病毒或安全风险而采取的操作的完整说明。

#### 在受感染计算机上显示通知消息

- 1 在"防病毒和防间谍软件策略"页上,单击下列选项之一:
  - 管理员定义的扫描
  - 文件系统自动防护
  - Internet 电子邮件自动防护
  - Microsoft Outlook 自动防护
  - Lotus Notes 自动防护
- 2 如果您在"扫描"选项卡上选择"管理员定义的扫描",请单击"添加"或 "编辑"。
- **3** 在"通知"选项卡上,选中"**在受感染的计算机上显示通知消息"**,然后修改 通知消息的正文。
- 4 单击"确定"。

# 将有关扫描的信息提交给 Symantec

您可以指定将有关主动型威胁扫描检测的信息、自动防护或扫描检测的信息自动发送给 Symantec 安全响应中心。

客户端提交的信息可帮助Symantec判定检测出的威胁是否存在误报。如果Symantec确定威胁确实存在,就会生成用以解决威胁的特征。特征会包括在定义的更新版本中。对于 TruScan 主动型威胁检测, Symantec 可更新允许或不允许的进程列表。

- 当客户端发送有关进程的信息时,该信息包括下列项目:
- 可执行文件的路径
- 可执行文件

- 内部状态信息
- 有关涉及威胁的文件和注册表加载点的信息
- 主动型威胁扫描使用的内容版本

能够标识客户端计算机的任何个人信息都不会提交。

有关检测率的信息可帮助 Symantec 优化病毒定义更新。检测率会显示大部分都是 由客户检测到的病毒和安全风险。Symantec安全响应中心可删除未检测到的特征, 并且将分段病毒定义列表提供给需要它的客户。分段列表可提升防病毒和防间谍软 件扫描的性能。

当主动型威胁扫描检测到目标后,客户端软件会检查是否已发送有关该进程的信息。如果信息已发送,客户端就不会再次发送该信息。

**注意**:当主动型威胁扫描检测到商业应用程序列表上的项目后,有关这些检测结果 的信息不会转发给 Symantec 安全响应中心。

当您启用进程的提交时,由主动型威胁扫描隔离的项目会更新。项目更新后,"隔离区"窗口会显示已提交给 Symantec 安全响应中心的样本。提交具有其他操作类型的检测结果后,客户端软件不会通知用户,并且管理控制台不会提供指示。其他操作类型包括"记录"或"终止"。

您可以将"隔离区"样本提交给 Symantec。

请参见第 342 页的"将已隔离的项目提交至 Symantec"。

#### 关于提交调节

客户端能否提交样本至 Symantec 将取决于下列信息:

- 提交数据控制文件的日期
- 允许发送提交的计算机百分比

Symantec 会发布提交控制数据 (SCD) 文件,并将其包括在 LiveUpdate 软件包中。 每个 Symantec 产品都有其各自的 SCD 文件。

此文件可控制以下设置:

- 一天内客户端可提交的次数
- 客户端软件重试提交时可等候的时间长度
- 提交失败后重试的次数
- Symantec 安全响应中心服务器接收提交的 IP 地址

如果SCD文件已过期,则客户端会停止提交。如果某客户端计算机已有7天未检索 LiveUpdate,则 Symantec 会认为该 SCD 文件已过期。 如果客户端停止了传输提交,则客户端软件不会收集提交信息并稍后发送。客户端 再次开始传输提交时,只会发送在提交重新开始之后发生的事件信息。

管理员也可以配置允许发送提交的计算机百分比。各个客户端计算机可决定是否应 该提交信息。客户端计算机会在1至100之间随机选择一个数字。如果该数字小于 或等于该计算机策略中设置的百分比,计算机就会提交信息。如果该数字大于配置 的百分比,计算机就不会提交信息。

#### 配置提交选项

提交默认为启用。您可以在"防病毒和防间谍软件策略"页面的"提交"选项卡上 启用或禁用提交。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 指定是否发送 TruScan 主动型威胁扫描检测到的进程相关信息

- 1 在"防病毒和防间谍软件策略"页面上,单击"提交"。
- 2 在 "TruScan 主动型威胁扫描"下,选中或取消选中 "允许客户端计算机提交 扫描检测到的进程"。
- 3 如果选中此参数,您就可以更改允许提交进程信息的客户端计算机百分比。
- 4 如果您已启用提交,可使用向上箭头或向下箭头选择百分比,也可在文本框中 键入所需值。
- 5 完成此策略的配置后,单击"确定"。

#### 指定是否发送自动防护和手动扫描检测率的相关信息

- 1 在"防病毒和防间谍软件策略"页面上,单击"提交"。
- 2 在"检测率"下,选中或取消选中"允许客户端计算机提交威胁检测率"。 如果选中此参数,您就可以更改允许提交检测率的客户端计算机百分比。
- 3 完成此策略的配置后,单击"确定"。

# 管理已隔离的文件

管理已隔离的文件包括下列各项操作:

- 指定本地隔离区目录
- 将已隔离的项目提交至 Symantec
- 配置新定义到达时要采取的操作

# 关于隔离区设置

您可以使用防病毒和防间谍软件策略配置客户端的隔离区设置。

隔离区设置管理是病毒爆发策略的重要部分。

# 指定本地隔离区目录

如果您不想使用默认的隔离区目录来存储客户端计算机上的已隔离文件,您可以另 外指定一个本地目录。您可以使用路径扩展,方法是在输入路径时使用百分比符 号。例如,您可以输入%COMMON\_APPDATA%。不允许使用相对路径。 本软件支持下列扩展参数:

%COMMON_APPDATA%	此路径通常是 C:\Documents and Settings\ All Users\Application Data
%PROGRAM_FILES%	此路径通常是 C:\Program Files
%PROGRAM_FILES_COMMON%	此路径通常是 C:\Program Files\Common
%COMMON_PROGRAMS%	此路径通常是 C:\Documents and Settings\ All Users\Start Menu\Programs
%COMMON_STARTUP%	此路径通常是 C:\Documents and Settings\ All Users\Start Menu\Programs\Startup
%COMMON_DESKTOPDIRECTORY%	此路径通常是 C:\Documents and Settings\ All Users\Desktop
%COMMON_DOCUMENT%	此路径通常是 C:\Documents and Settings\ All Users\Documents
%SYSTEM%	此路径通常是 C:\Windows\System32
%WINDOWS%	此路径通常是 C:\Windows

#### 指定本地隔离区目录

- 1 在"防病毒和防间谍软件策略"页面上,单击"隔离"。
- 2 在"其他"选项卡的"本地隔离区选项"下方,单击"指定隔离区目录"。
- 3 在文本框中,输入客户端计算机上的本地目录名称。您可以使用路径扩展,方法是在输入路径时使用百分比符号。例如,您可以输入 %COMMON APPDATA%,但不允许相对路径。
- 4 完成此策略的配置后,单击"确定"。

# 配置自动清除选项

客户端软件扫描到可疑文件时,会将该文件放到受感染计算机的本地隔离区文件夹中。隔离区清理功能会自动将隔离区中超过指定保存期限的文件删除。当隔离区中 存储文件的目录到达特定大小时,隔离区清理功能会自动删除其中的文件。 您可以使用防病毒和防间谍软件策略来配置这些选项。您可以分别配置已修复、已 备份和已隔离文件的保留天数。您也可以设置目录的大小上限,当超过此大小时, 便将文件自动从客户端计算机中删除。

您可以使用其中一个设置,也可以同时使用两者。如果设置两种类型的限制,则会 首先删除超过所设保存期限的所有文件。如果目录的大小仍大于您所设置的大小限 制,则会逐一删除最旧的文件。系统会一直删除文件,直到目录大小低于所设限制 为止。默认情况下,不启用这些选项。

#### 配置自动清除选项

- 1 在"防病毒和防间谍软件策略"页面上,单击"隔离"。
- 2 在"清理"选项卡的"已修复的文件"下方,选中或取消选中"启用修复文件 的自动删除"。
- 3 在"在以下天数后删除"框中,键入时间间隔值或单击箭头来选择时间间隔, 以天为单位。
- 4 选中"删除最旧的文件,将目录大小限制在",然后以 MB 为单位键入目录大小上限。默认设置为 50 MB。
- 5 在"备份文件"下方,选中或取消选中"启用备份文件的自动删除"。
- 6 在"以下之后删除"框,输入时间间隔或单击箭头来选择时间间隔,以天为单位。
- 7 选中"删除最旧的文件,将目录大小限制在",然后以 MB 为单位键入目录大小上限。默认值为 50 MB。
- 8 在"隔离的文件"下方,选中或取消选中"启用无法修复的隔离文件的自动删除"。
- 9 在"在以下天数后删除"框中,键入时间间隔值或单击箭头来选择时间间隔, 以天为单位。
- 10 选中"删除最旧的文件,将目录大小限制在",然后以 MB 为单位键入目录大小上限。默认值为 50 MB。
- 11 完成此策略的配置后,单击"确定"。

#### 将隔离项目提交至中央隔离服务器

您可以将隔离区内的项目从本地隔离区转发至中央隔离服务器。如果您在安全网络 中使用了中央隔离服务器,则应该将客户端配置为转发项目。中央隔离服务器可以 将此类信息转发至 Symantec 安全响应中心。客户端提交的信息可帮助 Symantec 判定检测出的威胁是否存在误报。

**注意**: 只有防病毒和防间谍软件扫描检测到的隔离项目才能发送至"中央隔离服务器"。无法发送主动型威胁扫描检测到的隔离项目。

#### 启用隔离项目到隔离服务器的提交

- 1 在"防病毒和防间谍软件策略"页面上,单击"提交"。
- 2 在"隔离的项"下,选中"允许客户端计算机自动将隔离项发送至隔离服务器"。
- 3 输入隔离服务器的名称。
- 4 输入要使用的端口号,然后选择重试连接的秒数。
- 5 配置完此策略设置后,单击"确定"。

## 将已隔离的项目提交至 Symantec

您可以通过启用客户端软件,允许用户将受感染或可疑的文件以及相关的负面影响 提交至Symantec安全响应中心,以进行进一步的分析。用户提交信息后,Symantec 便可根据此信息改善其检测功能,并进行相应修复。

提交至 Symantec 安全响应中心的文件将为 Symantec Corporation 所有。在某些 情况下,这些文件可能会与防病毒社区共享。Symantec 共享文件时,会使用业界 标准的加密技术并可能不对数据具名,以此保护内容的完整性与您的隐私权。

在某些状况下,Symantec可能拒绝文件。例如,若文件看来未受感染,Symantec可能拒绝文件。如果您想要让用户可以重新提交所选文件,则您可以启用文件的重新提交。用户一天可重新提交文件一次。

#### 启用隔离项目至 Symantec 的提交

- 1 在"防病毒和防间谍软件策略"页面上,单击"提交"。
- 2 在"隔离的项"下方,选中"允许客户端计算机手动将隔离项发送至Symantec 安全响应中心"。
- 3 完成此策略的配置后,单击"确定"。

#### 配置新定义到达时要采取的操作

您可以配置新定义到达客户端计算机时应采取的操作。默认情况下,客户端会重新 扫描隔离区内的项目,并自动以静默方式修复和还原项目。一般而言,您应该始终 使用此设置。

#### 配置新定义的操作

- 1 在"防病毒和防间谍软件策略"页面上,单击"隔离"。
- 2 在"常规"选项卡的"当新的病毒定义到达时"下,单击下列选项之一:
  - 自动静默地修复和还原隔离中的文件
  - 静默地修复隔离中的文件,但不还原
  - 提示用户

- 不执行任何操作
- 3 完成此策略的配置后,单击"确定"。

344 | 基本防病毒和防间谍软件策略设置 | 管理已隔离的文件

# 27

# 配置自动防护

本章节包括下列主题:

- 关于配置自动防护
- 关于自动防护的类型
- 启用文件系统自动防护
- 配置文件系统自动防护
- 配置 Internet 电子邮件自动防护
- 配置 Microsoft Outlook 自动防护
- 配置 Lotus Notes 自动防护
- 配置自动防护的通知选项

# 关于配置自动防护

设置防病毒和防间谍软件策略时,也可以配置自动防护设置。您也可以手动启用客 户端组或特定计算机和用户的自动防护。

您可以锁定或解除锁定防病毒和防间谍软件策略中的许多自动防护选项。当您锁定 选项时,客户端计算机上的用户不能更改该选项。默认情况下,解除锁定各选项。

有些自动防护选项类似于其他防病毒和防间谍软件扫描的选项。

请参见第 332 页的"配置应用于防病毒和防间谍软件扫描的选项"。

# 关于自动防护的类型

自动防护可保护文件系统以及客户端所收到的电子邮件附件。 您可以配置以下类型的自动防护:

- 文件系统自动防护
- Internet 电子邮件自动防护
- Microsoft Outlook 自动防护
- Lotus Notes 自动防护

默认会启用所有类型的自动防护。如果您的客户端计算机运行有其他电子邮件安全 产品,例如 Symantec Mail Security,就可能不需要启用电子邮件自动防护。

请参见第 316 页的"关于自动防护扫描"。

# 启用文件系统自动防护

自动防护设置包括在您要应用于客户端计算机的防病毒和防间谍软件策略中。默认 情况下,"文件系统自动防护"启用。您可以锁定此设置,从而使客户端计算机上 的用户不能禁用文件系统自动防护。若要允许用户更改本设置,或是禁用了文件系 统自动防护,则您可能需要从控制台启用自动防护。

您可以使用控制台中的"客户端"选项卡来启用"文件系统自动防护"。您也可以 从计算机状态日志手动启用"文件系统自动防护"。

请参见第173页的"从日志运行命令和操作"。

如果您要禁用"自动防护",您必须在应用于该组的"防病毒和防间谍软件策略" 中禁用此设置。

#### 启用文件系统自动防护

- 在控制台,单击"客户端",然后在"查看客户端"中,选择包括您要为其启 用"自动防护"的计算机的组。
- 2 在右窗格中,选择"客户端"选项卡。
- 3 执行下列操作之一:
  - 在左窗格的"查看客户端"中,右键单击您要为其启用"自动防护"的组。
  - 在右窗格的"客户端"选项卡中,选择您要为其启用"自动防护"的计算 机和用户,然后右键单击选择。
- 4 单击下列其中一项命令:
  - "对组运行命令">"启用自动防护"
  - "对客户端运行命令" > "启用自动防护"
- 5 在显示的消息框中,单击"确定"。

如果要启用或禁用电子邮件的"自动防护",必须在"防病毒和防间谍软件策略"中包括此设置。

# 配置文件系统自动防护

将文件系统自动防护配置为防病毒和防间谍软件策略的一部分时,所配置的设置会 定义自动防护及其关联功能的行为方式。您可以指定是要扫描软驱、网络驱动器还 是两者都要扫描。

**注意**:您配置自动防护选项时,可以单击自动防护设置旁的锁定图标。使用此策略 的客户端计算机上的用户不能更改锁定的设置。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置文件系统自动防护

- 1 在"防病毒和防间谍软件策略"页面上,单击"**文件系统自动防护"**。
- 2 在"扫描详细信息"选项卡上,选中或取消选中"启用文件系统自动防护"。
- 3 在"扫描"下的"文件类型"下,单击下列选项之一:
  - 扫描所有文件
  - 只扫描选择的扩展名

请参见第 332 页的"配置所选文件扩展名的扫描"。

4 在"附加选项"下,选中或取消选中"扫描安全风险"和"禁止安装安全风险"。

请参见第 348 页的"关于自动防护安全风险扫描与禁止"。

- **5** 在"网络设置"下,选中或取消选中"网络",以启用或禁用网络文件的自动 防护扫描。
- 6 如果选中"网络",请单击"网络设置"。
- 7 在"网络设置"对话框中,执行下列任何操作:
  - 启用或禁用自动防护以信任运行自动防护的远程计算机上的文件。
  - 配置自动防护扫描的网络高速缓存选项。
- 8 单击"确定"。
- 9 在"软盘设置"下,选中或取消选中"访问软盘时检查其是否有引导型病毒"。
- **10** 如果您选中"访问软盘时检查其是否有引导型病毒",可设置找到启动病毒时 您要采取的操作。您可以从引导记录清除病毒、记录病毒或保留病毒。
- 11 在"操作"选项卡上,设置任意选项。 请参见第 334 页的"配置要针对检测到的已知病毒和安全风险执行的操作"。 您也可以设置"文件系统自动防护"的补救选项。

- 在"通知"选项卡上,设置任何通知选项。
   请参见第 353 页的"配置自动防护的通知选项"。
- 13 在"高级"选项卡上,设置下列任何选项:
  - 启动和关机
  - 重新加载选项
- 14 在"附加选项"下,单击"文件高速缓存"或"风险跟踪程序"。
- 15 配置文件高速缓存或风险跟踪程序设置,然后单击"确定"。
- 16 完成此策略的配置后,单击"确定"。

#### 关于自动防护安全风险扫描与禁止

在默认情况下,自动防护会执行下列操作:

- 扫描安全风险,如广告软件或间谍软件
- 隔离受感染的文件
- 删除或修复安全风险带来的负面影响

如果禁止安装安全风险不会影响计算机的稳定性,则在默认情况下,自动防护还会 禁止此类安装。如果 Symantec 判定禁止安全风险可能会损及计算机稳定性,则自 动防护会允许安装该风险。自动防护也会立即采取对该风险所配置的操作。

但有时候,您可能暂时需要禁用自动防护中的安全风险扫描,然后再重新启用。此 外,您还可能需要禁用禁止安全风险功能,以控制自动防护对特定安全风险做出响 应的时间。

**注意**:您不能禁用其他扫描类型的安全风险扫描。然而,您可以将 Symantec Endpoint Protection 配置为忽略安全风险,而仅记录该检测事件。您也可以通过将 特定风险添加到集中式例外列表,从所有类型的扫描全局排除这些风险。

请参见第463页的"关于集中式例外策略"。

#### 配置高级扫描和监控选项

您可以配置文件和进程自动防护扫描的高级扫描和监控选项。这些选项包括扫描文 件的时间,以及启发式扫描设置。

自动防护的启发式扫描与主动型威胁扫描不同。自动防护的启发式扫描会扫描文件 是否有恶意行为,而主动型威胁扫描则会检查运行中的进程是否有恶意行为。

请参见第 419 页的"关于 TruScan 主动型威胁扫描"。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置高级扫描和监控选项

- 1 在"防病毒和防间谍软件策略"页面上,单击"文件系统自动防护"。
- 2 在"扫描详细信息"选项卡的"扫描"下,单击"高级扫描和监控"。
- 3 在"扫描文件条件"下,指定触发扫描的活动。
- 4 在 "Bloodhound(TM)检测设置"下,选中或取消选中 "启用Bloodhound(TM) 病毒检测"。

您还可以更改防护级别。

- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

#### 关于风险跟踪程序

风险跟踪程序会标识客户端计算机上的网络共享型病毒感染源。

自动防护检测到感染时,会将信息发送到 Symantec Endpoint Protection 主服务 Rtvscan。Rtvscan 会确定感染来自本地还是远程。

如果感染来自远程计算机,则Rtvscan 会执行下列操作:

- 查找并记录计算机的 NetBIOS 计算机名及其 IP 地址。
- 查找并记录发送时登录计算机的用户。
- 在"风险属性"对话框中显示此信息。

默认情况下, Rtvscan 每秒轮询一次网络会话, 然后将此信息缓存为远程计算机次 要源列表。此信息会最大程度地提高风险跟踪程序成功识别受感染的远程计算机的 频率。例如, 在 Rtvscan 能够记录网络会话之前, 风险可能已经关闭网络共享。然 后, 风险跟踪程序会使用次要源列表, 尝试识别远程计算机。您可以在"自动防护 高级选项"对话框中配置此信息。

风险跟踪程序信息会出现在"风险属性"对话框中,而且仅适用于受感染文件所导致的风险条目。当风险跟踪程序确定感染由本地主机活动导致时,会将源列为本地 主机。

发生下列情形时,风险跟踪程序会将源列为未知:

- 无法识别远程计算机。
- 文件共享的已验证用户涉及多台计算机。当用户 ID 与多个网络会话关联时,会发生此情形。例如,多台计算机可能使用相同的服务器用户 ID 登录文件共享服务器。

您可以记录当前感染本地计算机的多台远程计算机完整列表。请在本地客户端计算机上,将HKEY\_LOCAL\_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\ProductControl\Debug 字符串值设为 THREATTRACER X。 THREATTRACER 值会启用调试输出,而 X 可确保只显示风险跟踪程序的调试输 出。您还可以添加一个L来确保记录存储到 <SAV\_Program\_Folder>\vpdebug.log 日志文件中。若要确保调试窗口不出现,请添加 XW。

若要试验此功能,请使用可从以下 URL 找到的 Eicar.com 病毒测试文件:

#### www.eicar.org

风险跟踪程序还包括禁止源计算机的IP地址的选项。若要使此选项生效,您必须在 防火墙策略中设置相应的选项,以启用此类型的自动禁止。

#### 关于文件高速缓存

文件系统自动防护使用文件高速缓存,以记住上次扫描时未感染的文件。在启动过 程中会保留文件高速缓存。如果客户端计算机关闭后重新启动,文件系统自动防护 会记住未感染的文件,而不会扫描这些文件。

在下列情况下, 文件系统自动防护会重新扫描文件:

- 客户端计算机下载了新的定义。
- 自动防护检测出文件可能在自动防护未运行时发生了更改。

如果您始终通过自动防护扫描各个文件,可禁用文件高速缓存。如果禁用文件高速 缓存,可能会影响客户端计算机的性能。

您也可以设置下列参数:

- 文件高速缓存大小 默认高速缓存大小为每卷 10,000 个文件。如果您要通过文件系统自动防护重新 扫描更多或更少的文件,可以更改高速缓存大小。
- 加载新定义时,是否通过自动防护重新扫描高速缓存 您可能需要禁用此参数,以改善文件系统自动防护的性能。

# 配置 Internet 电子邮件自动防护

Internet 电子邮件自动防护可同时防护安全套接字层 (SSL) 上使用 POP3 或 SMTP 通信协议的传入电子邮件和传出电子邮件。启用 Internet 电子邮件自动防护时,客 户端软件会扫描电子邮件本文以及其中的任何附件。

您可以启用自动防护来支持处理使用 POP3 和 SMTP 连接的加密电子邮件。自动防 护会检测安全连接,而不扫描加密的邮件。即使 Internet 电子邮件自动防护不扫描 加密的邮件,它仍能保护计算机不受附件中的病毒和安全风险侵袭。

文件系统自动防护在您将电子邮件附件保存到硬盘驱动器时扫描附件。

**注意:** 64 位计算机不支持 Internet 电子邮件自动防护。Internet 电子邮件自动防护也不支持在服务器操作系统上扫描 POP3 电子邮件。

Symantec Endpoint Protection 客户端还提供出站电子邮件启发式扫描。启发式扫描使用"Bloodhound 病毒检测"来识别传出邮件中可能包含的风险。当客户端扫描传出电子邮件时,这种扫描有助于防止风险散播。这些风险包括可能利用电子邮件客户端复制和散播到网络的蠕虫。

电子邮件扫描不支持以下电子邮件客户端:

- IMAP 客户端
- AOL 客户端
- 基于 HTTP 的电子邮件,例如 Hotmail 和 Yahoo!邮件

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置 Internet 电子邮件自动防护

- 1 在"防病毒和防间谍软件策略"页面上,单击"Internet电子邮件自动防护"。
- 2 在"扫描详细信息"选项卡上,选中或取消选中"启用Internet电子邮件自动 防护"。
- 3 在"扫描"下的"文件类型"下,单击下列选项之一:
  - 扫描所有文件
  - 只扫描选择的扩展名

请参见第 332 页的"配置所选文件扩展名的扫描"。

- 4 选中或取消选中"扫描压缩文件中的文件"。
- 5 单击"确定"。
- 6 在"操作"选项卡上,设置任意选项。 请参见第 334 页的"配置要针对检测到的已知病毒和安全风险执行的操作"。
- 7 单击"确定"。
- 8 在"通知"选项卡上的"电子邮件通知"下,选中或取消选中下列任何选项:
  - 在电子邮件消息中插入警告
  - 向发件人发送电子邮件
  - 向其他人发送电子邮件

请参见第353页的"配置自动防护的通知选项"。

- 9 单击"确定"。
- **10** 在 "高级" 选项卡的"加密连接"下,启用或禁用加密的 POP3 或 SMTP 连 接。
- 11 在"启发式群发邮件蠕虫检测"下,选中或取消选中"启发式出站蠕虫检测"。
- 12 完成此策略的配置后,单击"确定"。

# 配置 Microsoft Outlook 自动防护

默认情况下,自动防护会扫描 Microsoft Outlook 电子邮件附件。您可以自定义扫描设置。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置 Microsoft Outlook 自动防护

- 1 在"防病毒和防间谍软件策略"页面上,单击"Microsoft Outlook 自动防 护"。
- 2 在"扫描详细信息"选项卡上,选中或取消选中"启用 Microsoft Outlook 自 动防护"。
- 3 在"扫描"下的"文件类型"下,单击下列选项之一:
  - 扫描所有文件
  - 只扫描选择的扩展名

请参见第 332 页的"配置所选文件扩展名的扫描"。

- 4 选中或取消选中"扫描压缩文件中的文件"。
- 5 在"操作"选项卡上,设置任意选项。

请参见第334页的"配置要针对检测到的已知病毒和安全风险执行的操作"。

- 6 在"通知"选项卡上,选中或取消选中下列任意选项:
  - 在电子邮件消息中插入警告
  - 向发件人发送电子邮件
  - 向其他人发送电子邮件

请参见第 353 页的"配置自动防护的通知选项"。

7 完成此策略的配置后,单击"确定"。

# 配置 Lotus Notes 自动防护

默认情况下,自动防护会扫描LotusNotes电子邮件附件。您可以自定义扫描设置。 可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置 Lotus Notes 自动防护

- 1 在"防病毒和防间谍软件策略"页面上,单击"Lotus Notes 自动防护"。
- 2 在"扫描详细信息"选项卡上,选中或取消选中"启用 Lotus Notes 自动防护"。
- 3 在"扫描"下的"文件类型"下,单击下列选项之一:

- 扫描所有文件
- 只扫描选择的扩展名

请参见第 332 页的"配置所选文件扩展名的扫描"。

- 4 选中或取消选中"扫描压缩文件中的文件"。
- 5 在"操作"选项卡上,设置任意选项。 请参见第334页的"配置要针对检测到的已知病毒和安全风险执行的操作"。
- 6 在"通知"选项卡上,选中或取消选中下列任意选项:
  - 在电子邮件消息中插入警告
  - 向发件人发送电子邮件
  - 向其他人发送电子邮件

请参见第 353 页的"配置自动防护的通知选项"。

7 配置完策略设置后,单击"确定"。

# 配置自动防护的通知选项

默认情况下, "文件系统自动防护"扫描的结果会显示在受感染的计算机上。您可 以配置"防病毒和防间谍软件策略",以便不在客户端计算机上显示结果。 您可以自定义"自动防护"在检测时要显示在客户端计算机上的通知消息。 请参见第 336 页的"在受感染的计算机上自定义并显示通知"。 对于支持的电子邮件软件,您还可以配置自动防护执行下列操作:

- 在电子邮件中添加有关受感染计算机的警告。
- 通知受感染电子邮件的发件人。
- 就受感染的电子邮件通知其他人。

您可以自定义要发送以通知用户的电子邮件。

**注意**: 配置选项来通知发件人和其他人有关受感染的电子邮件时,请务必谨慎。受 感染电子邮件的地址可能是具有欺骗性的地址。如果发送通知,则可能会生成垃圾 邮件,并造成网络通信增加。

对于通知消息和电子邮件而言,可自定义的变量字段稍有不同。可以自定义消息正 文和感染信息字段中的信息。

表 27-1 说明您可以自定义消息正文的信息类型。

#### 表 27-1 电子邮件正文字段

字段	说明
User	出现病毒或安全风险时已登录的用户的名称。
DateFound	发现病毒或安全风险的日期。
EmailSender	发送带有受感染附件电子邮件的电子邮件地址。
EmailRecipientList	将带有受感染附件的电子邮件发送到的地址列表。

表 27-2 说明您可以自定义感染字段的信息类型。

#### 表 27-2 感染信息字段

字段	说明
SecurityRiskName	发现的病毒或安全风险的名称。
ActionTaken	为应对检测到的病毒或安全风险而采取的操作。此操作可以是已配置的第一个操作或第二个操作。
Status	文件的状态: "受感染"、"未感染"或"已删除"。
	该消息变量在默认情况下不使用。若要显示此信息,请手 动将此变量添加到消息。
Filename	病毒或安全风险感染的文件的名称。
PathAndFilename	病毒或安全风险感染的文件的完整路径和名称。
Computer	病毒或安全风险所在的计算机名。
User	出现病毒或安全风险时已登录的用户的名称。
DateFound	发现病毒或安全风险的日期。
OriginalAttachmentName	包含病毒或安全风险的附件的名称。
StorageName	应用程序受影响的区域。例如,存放区名称可能是"文件系统自动防护"或"Lotus Notes 自动防护"。

# 在受感染的计算机上显示自动防护结果

如果要让用户可以看到文件和进程的自动防护扫描结果,则可在受感染的计算机上显示结果。如果不想在客户端计算机上显示结果,也可以禁用显示。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 在受感染的计算机上显示自动防护结果

- 1 在"防病毒和防间谍软件策略"页面上,单击"文件系统自动防护"。
- 2 在"通知"选项卡上,选中或取消选中"受感染的计算机上显示自动防护结果 对话框"。
- 3 配置完策略设置后,单击"确定"。

#### 在受感染的电子邮件中添加警告

对于支持的电子邮件软件,您可以配置自动防护以自动将警告插入受感染电子邮件的正文。如果 Symantec Endpoint Protection 客户端不能清除消息中的病毒,警告消息就非常重要。如果已移动、删除或重命名受感染的附件或者未对其进行任何操作,则此警告也很重要。警告消息会告诉您发现了哪种病毒,并说明已采取的操作。

可以将下列文本附加到与受感染附件关联的电子邮件的顶部:

Symantec Endpoint Protection 发现来自 [EmailSender] 的附件中有安全风险。 对于每个受感染的文件,还会将下列信息添加到电子邮件中:

- 附件的名称
- 风险的名称
- 采取的操作
- 文件的感染状态

您可以自定义邮件的主题和正文。

此电子邮件包含名为 EmailSender 的字段。您可以自定义此默认消息。

收件人看到的消息如下所示:

Symantec Endpoint Protection 在来自 John.Smith@mycompany.com 的附件中发现安全风可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 在受感染的电子邮件中添加电子邮件警告

- 1 在"防病毒和防间谍软件策略"页上,单击下列选项之一:
  - Internet 电子邮件自动防护。
  - Microsoft Outlook 自动防护。
  - Lotus Notes 自动防护。
- 2 在"通知"选项卡的"电子邮件通知"下方,选中"在电子邮件消息中插入警告"。
- 3 单击"警告",然后执行下列操作之一:

- 单击"确定"以接受默认消息。
- 自定义警告消息。
- 4 完成此策略的配置后,单击"确定"。

# 通知受感染电子邮件消息的发件人

对于支持的电子邮件软件,您可以配置自动防护以自动给附件受感染的电子邮件发 件人回复。

**注意**: 配置选项来通知发件人有关受感染的电子邮件时,请务必谨慎。受感染电子 邮件的地址可能是具有欺骗性的地址。如果发送通知,则可能会生成垃圾邮件,并 造成网络通信增加。

您也可以配置自动防护以发送具有下列主题的默认回复电子邮件:

在邮件 [EmailSubject] 中发现安全风险

消息正文用于通知发件人受感染的附件:

Symantec Endpoint Protection 在您 ([EmailSender]) 发送至 [EmailRecipientList] 的附件中发现安全风险。

对于每个受感染的文件,还会将下列信息添加到电子邮件中:

- 附件的名称
- 风险的名称
- 采取的操作
- 文件的感染状态

您也可以自定义这个消息。

#### 通知受感染电子邮件的发件人

- 1 在"防病毒和防间谍软件策略"页上,单击下列选项之一:
  - Internet 电子邮件自动防护。
  - Microsoft Outlook 自动防护。
  - Lotus Notes 自动防护。
- 2 在"通知"选项卡的"电子邮件通知"下方,选中"向发件人发送电子邮件"。
- 3 单击"发件人"。
- **4** 在"向发件人发送电子邮件"对话框中,在"消息"选项卡的"消息文本"下 方,执行下列操作之一:
  - 单击"确定"以接受默认消息。

■ 键入要在每个消息中显示的主题行、消息正文以及感染信息,然后单击"**确** 定"。

您可以单击"帮助"以获取有关消息中可用的变量的信息。

- 5 仅针对"Internet 电子邮件自动防护",在"电子邮件服务器"选项卡上,键 入下列信息:
  - 邮件服务器名称和端口
  - 用户名和密码
  - 电子邮件的反向路径
- 6 完成此策略的配置后,单击"确定"。

# 就受感染的电子邮件消息通知其他人

对于支持的电子邮件软件,您可以配置自动防护以在打开包含受感染附件的电子邮 件时通知其他人。

**注意**: 配置选项来通知其他人有关受感染的电子邮件时,请务必谨慎。受感染电子邮件的地址可能是具有欺骗性的地址。如果发送通知,则可能会生成垃圾邮件,并 造成网络通信增加。

您可以使用下列主题,将电子邮件发送给其他用户:

在邮件 [EmailSubject] 中发现安全风险

邮件正文包括有关受感染附件的发件人的信息:

Symantec Endpoint Protection 发现来自 [EmailSender] 的附件中有安全风险。 对于每个受感染的文件,还会将下列信息添加到电子邮件中:

- 附件的名称
- 风险的名称
- 采取的操作
- 文件的感染状态

您也可以自定义这个消息。

#### 就受感染的电子邮件通知其他人

- 1 在"防病毒和防间谍软件策略"页上,单击下列选项之一:
  - Internet 电子邮件自动防护。
  - Microsoft Outlook 自动防护。

■ Lotus Notes 自动防护。

- 2 在"通知"选项卡的"电子邮件通知"下方,选中"向其他人发送电子邮件"。
- 3 单击"其他人"。
- 4 在"向其他人发送电子邮件"对话框的"其他人"选项卡上,提供一个或多个 接收通知的电子邮件地址。
- **5** 单击"消息"选项卡,键入要在每个消息中显示的主题行、消息正文以及感染 信息。

您可以单击"帮助"以获取有关消息中可用的变量的信息。

- 6 仅针对"Internet 电子邮件自动防护",在"电子邮件服务器"选项卡上,键 入下列信息:
  - 邮件服务器名称和端口
  - 用户名和密码
  - 电子邮件的反向路径
- 7 单击"确定"。
- 8 完成此策略的配置后,单击"确定"。

# 配置 Internet 电子邮件自动防护扫描的进度通知

您可以启用或禁用 Internet 电子邮件自动防护扫描的进度指示条选项。 您可以配置下列选项:

- 是否在发送电子邮件时在客户端计算机上显示进度窗口。
- 是否在通知区域中显示图标以指示电子邮件的传输状态。

默认情况下会启用这两个选项。

#### 配置进度通知

- 1 在"防病毒和防间谍软件策略"页面上,单击"Internet电子邮件自动防护"。
- 2 在"通知"选项卡的"进度通知"下,选中或取消选中下列选项:
  - 发送电子邮件时显示进度指示条。
  - 显示通知区域图标。
- 3 完成此策略的配置后,单击"确定"。

# 使用管理员定义的扫描

本章节包括下列主题:

- 关于使用管理员定义的扫描
- 添加调度扫描到防病毒和防间谍软件策略
- 配置按需扫描选项
- 运行按需扫描
- 配置管理员定义的扫描的扫描进度选项
- 设置管理员定义的扫描的高级选项

# 关于使用管理员定义的扫描

管理员定义的扫描包括防病毒和防间谍软件调度扫描和按需扫描。设置防病毒和防 间谍软件策略时,也可以配置这些扫描类型的选项。

您可以使用调度扫描与按需扫描,增强自动防护所提供的防护。自动防护会在您读 写文件时,提供防护。调度扫描与按需扫描则可以扫描客户端计算机存储的所有文 件。还可以防护客户端计算机的内存、装载点,及其他重要位置。

**注意**:对于受管理客户端,Symantec Endpoint Protection 提供默认调度扫描,扫描客户端计算机中所有的文件、文件夹及位置。

管理员定义的扫描的某些选项类似于"自动防护"扫描选项。这些类似选项包括检测操作以及您指定的通知。

请参见第 332 页的"配置应用于防病毒和防间谍软件扫描的选项"。

# 添加调度扫描到防病毒和防间谍软件策略

您可以在设置防病毒和防间谍软件策略时配置调度扫描。

调度扫描设置可以保存为模板。您可使用任何保存为模板的扫描创建不同的防病毒 和防间谍软件策略。配置多个防病毒和防间谍软件策略时,可以利用扫描模板节省 时间。默认情况下,策略中会包括调度扫描模板。默认调度扫描可扫描所有的文件 和目录。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 添加调度扫描至防病毒和防间谍软件策略

- 1 在"防病毒和防间谍软件策略"页面上,单击"管理员定义的扫描"。
- 2 在"扫描"选项卡的"调度扫描"下,单击"添加"。
- 3 在"添加调度扫描"对话框中,单击"创建新的调度扫描"。
- 4 单击"确定"。
- 5 在"添加调度扫描"对话框的"扫描详细信息"选项卡中,输入此调度扫描的 名称和说明。
- 6 单击"活动扫描"、"全面扫描"或"自定义扫描"。
- 7 如果您选择了"自定义",则可以在"扫描"下指定要扫描的目录。
- 8 在"文件类型"下,单击"扫描所有文件"或"只扫描选择的扩展名"。
   请参见第 332 页的"配置所选文件扩展名的扫描"。
- 9 在"选中以下以增强扫描"下,选中或取消选中"内存"、"常见感染位置" 或"最常见病毒和安全风险位置"。
- 10 单击"高级扫描选项"。
- 11 设置用于压缩文件、存储迁移或性能优化的各选项。
- 12 单击"确定"以保存此扫描的高级扫描选项。
- 13 在"调度"选项卡的"扫描调度"下,设置扫描运行的频率和时间。
- 14 在"操作"选项卡上,设置任意选项。

请参见第 334 页的"配置要针对检测到的已知病毒和安全风险执行的操作"。 您还可以针对扫描设置补救选项。

- 15 在"通知"选项卡上,设置任意选项。 请参见第 335 页的"关于受感染计算机上的通知消息"。
- 16 若要将此扫描保存为模板,请选中"副本另存为调度扫描模板"。
- 17 单击"确定"。
#### 从模板添加调度扫描

- 1 在"防病毒和防间谍软件策略"页面上,单击"管理员定义的扫描"。
- 2 在"扫描"选项卡的"调度扫描"下,单击"添加"。
- 3 在"添加调度扫描"对话框中,单击"从调度扫描模板创建调度扫描"。
- 4 选择此策略要使用的扫描模板。
- 5 单击"确定"。

## 配置按需扫描选项

您可以配置要按需运行的自定义扫描的选项。您可以从"客户端"页面手动运行按 需扫描,也可以从管理控制台的"监视器"页面运行按需扫描。

您不能配置扫描选项的扫描名称或说明。每次您从客户端计算机上的管理控制台运 行自定义按需扫描时,客户端都会使用这些选项。

注意:您可以按需运行活动扫描或全面扫描。

请参见第 320 页的"关于管理员定义的扫描"。

按需扫描的设置类似于调度扫描。

请参见第 360 页的"添加调度扫描到防病毒和防间谍软件策略"。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置按需扫描的设置

- 1 在"防病毒和防间谍软件策略"页面上,单击"管理员定义的扫描"。
- 2 在"扫描"选项卡的"管理员按需扫描"下方,单击"编辑"。
- 3 在"编辑管理员按需扫描"对话框的"扫描详细信息"选项卡上,单击"扫描"下的"编辑文件夹"。

默认情况下,会扫描所有的文件夹。

- 4 在"编辑文件夹"对话框中,选择您所要的文件夹,再单击"确定"。
- 5 在"编辑管理员按需扫描"对话框的"文件类型"下,单击"扫描所有文件" 或"只扫描选择的扩展名"。

请参见第 322 页的"关于扫描选定扩展名或文件夹"。

- 6 在"选中以下以增强扫描"下,选中或取消选中"内存"、"常见感染位置" 或"最常见病毒和安全风险位置"。
- 7 单击"高级扫描选项"。

- 8 设置用于压缩文件、存储迁移或性能优化的各选项。
- 9 单击"确定"以保存此扫描的高级选项。
- 10 在"操作"选项卡上,设置任意选项。 请参见第 334 页的"配置要针对检测到的已知病毒和安全风险执行的操作"。 您还可以针对扫描设置补救选项。
- 在"通知"选项卡上,设置任意选项。
   请参见第 335 页的"关于受感染计算机上的通知消息"。
- 12 单击"确定"。

## 运行按需扫描

您可以从管理控制台远程运行扫描。可以从控制台的"客户端"选项卡运行扫描, 也可以从在"监视器"选项卡上生成的计算机状态日志中运行扫描。

请参见第 173 页的"从日志运行命令和操作"。

您可以运行活动扫描、全面扫描或自定义按需扫描。自定义扫描使用防病毒和防间 谍软件策略中配置的按需扫描设置。

默认情况下,会对下列类型的项目进行扫描:

- 所有目录
- 所有文件类型
- 内存
- 常见感染位置
- 最常见病毒和安全风险位置

请参见第361页的"配置按需扫描选项"。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

**注意**:如果您在运行按需扫描的客户端计算机上发出重新启动的命令,扫描会停止,且客户端计算机将重新启动。扫描并不会重新启动。

#### 对组运行按需扫描

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下方,右键单击包括您要扫描的计算机的组。
- **3** 单击"对组运行命令">"扫描"。

- **4** 在"选择扫描类型"对话框中,选择"活动扫描"、"全面扫描"或"自定义 扫描"。
- 5 单击"确定"。
- 6 在显示的消息框中,单击"是"。
- 7 在显示的确认消息框中,单击"确定"。

#### 对计算机或用户运行按需扫描

- 1 在控制台中,单击"客户端"。
- 2 在右窗格的"客户端"下方,选择您要为之运行扫描的计算机和用户。
- 3 右键单击选定内容,再单击"对客户端运行命令">"扫描"。
- 4 在显示的消息框中,单击"是"。
- 5 在"选择扫描类型"对话框中,选择"活动扫描"、"全面扫描"或"自定义 扫描"。
- 6 单击"确定"。
- 7 在显示的确认消息框中,单击"确定"。

## 配置管理员定义的扫描的扫描进度选项

您可以配置是否在客户端计算机上显示"扫描结果"对话框。如果您允许此对话框 显示在客户端计算机上,用户就能暂停或推迟管理员定义的扫描。

您可以允许用户完全停止扫描。您也可以配置用户如何暂停或推迟扫描的选项。 您可以允许用户执行下列扫描操作:

暂停	用户暂停扫描时, "扫描结果"对话框仍保持打开状态, 等候用户继续或中止扫描。如果关闭计算机,则不会继续 运行暂停的扫描。
延缓	用户延缓调度扫描时,可以选择将扫描推迟一小时或三小时。您可以配置延缓的次数。在用户延缓扫描时,"扫描结果"对话框关闭,而当推迟期结束并且扫描恢复时,该 对话框会重新出现。
停止	用户停止扫描时,扫描通常会立即停止。如果用户停止扫 描的同时,客户端软件正在扫描压缩文件,则扫描不会马 上停止。在这种情况下,扫描在压缩文件扫描完毕后停止。 停止的扫描则不会重新启动。

暂停的扫描在经过一段指定的时间间隔后会自动重新启动。 可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置管理员定义的扫描的扫描进度选项

- 1 在"防病毒和防间谍软件策略"页面上,单击"管理员定义的扫描"。
- 2 在"高级"选项卡的"扫描进度选项"下方,单击"显示扫描进度"或"如果 检测到风险,则显示扫描进度"。
- 3 若要在扫描完成后自动关闭扫描进度指示条,请选中"完成时关闭扫描进度窗口"。
- 4 选中"允许用户停止扫描"。
- 5 单击"暂停选项"。
- 6 在"暂停扫描选项"对话框中,执行下列操作之一:
  - 若要限制用户可以暂停扫描的时间,请选中"限制扫描暂停的时间",然 后键入分钟数。范围是3至180。
  - 若要限制用户可以推迟(或延缓)扫描的次数,请在"延缓机会的最大次数"框中,键入1至8之间的数字。
  - 默认情况下,用户可将扫描推迟1小时。若要将此限制更改为3小时,请 选中"允许用户延缓扫描3小时"。
- 7 单击"确定"。

## 设置管理员定义的扫描的高级选项

您可以设置调度扫描和按需扫描的高级选项。

有关以下步骤中所使用选项的详细信息,您可以单击"帮助"。

#### 设置管理员定义的扫描的高级选项

- 1 在"防病毒和防间谍软件策略"页面上,单击"管理员定义的扫描"。
- 2 在"高级"选项卡的"调度扫描"下方,选中或取消选中下列选项:
  - 用电池供电时延迟调度扫描
  - 扫描创建者未登录时,允许运行用户定义的调度扫描
- 3 在"启动和触发扫描"下方,选中或取消选中下列选项:
  - 用户登录时运行启动扫描
  - 允许用户修改启动扫描
  - 新的定义到达时运行"活动扫描"
- 4 单击"确定"。





# 配置网络威胁防护

- 基本网络威胁防护设置
- 配置入侵防护
- 自定义网络威胁防护

# 基本网络威胁防护设置

本章节包括下列主题:

- 关于网络威胁防护与网络攻击
- 关于防火墙
- 关于使用防火墙策略
- 关于防火墙规则
- 添加空白规则
- 使用向导添加规则
- 添加继承自父组的规则
- 导入和导出规则
- 复制并粘贴规则
- 更改规则的顺序
- 启用与禁用规则
- 启用智能通信过滤
- 启用通信与隐藏设置
- 配置对等验证

## 关于网络威胁防护与网络攻击

计算机传输信息的途径会被网络攻击利用。客户端可以通过监控进出计算机的信息 以及禁止攻击尝试来保护您的计算机。 信息以数据包的形式在Internet上传输。每个数据包都包含一个标头,其中包含以下信息:发送计算机、目标接收者、应如何处理数据包中的数据以及接收数据包的 端口。

端口是一种通道,用来将来自Internet上的信息流分为若干由单个应用程序处理的 单独路径。Internet应用程序在计算机上运行时会侦听一个或多个端口,并接受发 送到这些端口的信息。

网络攻击会利用特定Internet程序的弱点。攻击者会使用工具,将包含恶意程序代码的数据包发送到特定端口。如果容易受到此攻击危害的某个应用程序监听该端口,攻击者就可以通过代码访问、禁用甚至控制计算机。攻击所用的编程代码可能包含在一个或多个数据包中。

可以使用网络威胁防护的默认设置来安装客户端。在大多数情况下,您无须更改这 些设置。将这些设置保留原样通常不会有问题。不过,如果您对网络有深入的了 解,则可以对客户端防火墙进行诸多更改,以完善客户端计算机的防护功能。

## Symantec Endpoint Protection 如何防止计算机受到网络攻击

Symantec Endpoint Protection 客户端具有下列可保护组织内的计算机不受入侵攻 击的工具:

防火墙	监控所有Internet通信并创建防护,以禁止或限制查看计算机上 信息的尝试。
入侵防护	分析所有入站信息和出站信息,检查是否出现攻击常见的数据模式。
	请参见第 387 页的"关于入侵防护系统"。

## 关于防火墙

Symantec Endpoint Protection 防火墙是一种软件,可在计算机与 Internet 之间设一道屏障。防火墙可防止未授权的用户访问连接到 Internet 的计算机和网络。它会检测可能的黑客攻击,保护个人信息,以及消除不必要的网络通信源。



所有进入或离开专用网络的信息都必须通过防火墙,防火墙会检查这些信息数据 包,禁止不满足指定安全条件的数据包。防火墙检查信息数据包的方式是使用防火 墙策略。防火墙策略由一个或多个协同工作的规则组成,可允许或禁止用户访问网 络。只有授权的通信可以通过。防火墙策略会定义授权的通信。

防火墙在后台工作。您可以确定用户与客户端交互的程度,即允许或禁止其配置防 火墙规则和防火墙设置。客户端可能只会通知用户有新的网络连接和可能的问题, 或者用户可以完全访问客户端的用户界面。

请参见第 370 页的"关于防火墙规则"。

## 关于使用防火墙策略

Symantec Endpoint Protection Manager包括默认防火墙策略,提供办公室环境所需的防火墙规则和防火墙设置。办公室环境通常处于企业防火墙、边界数据包过滤器或防病毒服务器的保护之下。因此与使用有限边界保护的大多数家用环境相比较而言,办公室环境通常更为安全。

当您首次安装控制台时,它会自动将默认防火墙策略添加到每个组中。每当您添加 新位置时,控制台会自动将防火墙策略复制到默认位置。

如果默认的防护并不适合,您可以自定义每个位置的防火墙策略,例如主站点或客户站点。如果您不想使用默认防火墙策略,可以对其进行编辑或用其他共享策略替换。

防火墙策略包括下列元素:

防火墙规则 防火墙规则是策略组件,可控制防火墙以何种方式保护计算 机免受恶意传入通信和应用程序的攻击。企业通过会自动根 据这些规则检查所有传入和传出的数据包,并且根据规则中 指定的信息允许或禁止数据包。

智能通信过滤器 允许大部分网络所需的特定通信类型,例如 DHCP、DNS 和 WINS 通信。

请参见第 384 页的"启用智能通信过滤"。

通信与隐藏设置 检测和禁止来自特定驱动程序、协议和其他源的通信。 请参见第 385 页的"启用通信与隐藏设置"。

对等验证设置 禁止远程计算机到客户端计算机的连接,直到客户端计算机 验证了该远程计算机。

请参见第 385 页的"配置对等验证"。

您可以将位置设为客户端控制或混合控制,以使用户可自定义防火墙策略。

请参见第400页的"针对混合控制配置网络威胁防护设置"。

您可以用创建和修改其他类型的策略的类似方式创建和编辑防火墙策略。您可以分 配、撤消、替换、复制、导出、导入或删除防火墙策略。

您通常可将一个策略分配至安全网络中的多个组。如果对特定位置有特定要求,您 可以创建一个非共享、位置限定的策略。

如要使用策略,您应熟悉策略配置的基本概念。

请参见第 282 页的"关于策略"。

## 关于防火墙规则

防火墙规则控制客户端如何保护客户端计算机不受恶意入站通信及出站通信的侵袭。防火墙自动根据这些规则检查所有入站及出站的数据包。然后,防火墙根据规则中指定的信息允许或禁止数据包。当计算机试图连接另一台计算机时,防火墙会将连接类型与其防火墙规则列表进行比较。

#### 关于防火墙规则的各部分

一般情况下,防火墙规则可规定允许或拒绝网络连接的条件。您可以使用下列条件 来定义防火墙规则:

- 触发器 应用程序、主机、协议和网络适配器 时间 防火墙评估规则时,所有触发器都必须为 True,才会出现完全匹配的 情况。如果与当前数据包有关的任何一个触发器不为 True,防火墙就无法 应用规则。您可以将各项触发器定义结合起来,形成更复杂的规则,例如 标识与特定目标地址相关的特定协议。
- 条件 调度和屏幕保护程序状态

条件参数不会规定网络连接的某个方面。相反,条件参数决定规则的实际 状态。您可以定义调度或标识屏幕保护程序的状态,从而指示何时将规则视 为活动或不活动状态。条件参数是可选的,如果没有定义,则不会有任何 作用。防火墙不会评估未处于活动状态的规则。

操作 允许或禁止,以及记入日志或不记入日志

操作参数会指定防火墙成功匹配规则时所采取的操作。如果规则匹配且是针 对接收的数据包选择的,则防火墙会执行所有操作。防火墙可以允许或禁止 数据包,以及记录或不记录数据包。如果防火墙允许通信,则会让规则指定 的通信访问网络。如果防火墙禁止通信,则会禁止规则指定的通信,不让此 通信访问网络。

一个合并了所有条件的规则,可能会允许每天早上9点至下午5点在远程端口80 上提交给 IP 地址 192.58.74.0 的通信。

## 关于应用程序触发器

如果应用程序是您在允许通信规则中定义的唯一触发器,则防火墙会允许应用程序 执行任何网络操作。重要的是应用程序,而不是应用程序执行的网络操作。例如, 假设您允许 Internet Explorer,而且未定义任何其他触发器。用户可以访问使用 HTTP、HTTPS、FTP、Gopher 及 Web 浏览器所支持的任何其他协议的远程站点。 您可以定义其他触发器来规定允许与哪些特定网络协议和主机的通信。

以应用程序为基础的规则可能不太容易进行疑难解答,因为应用程序可能使用有多种协议。例如,如果防火墙先处理允许Internet Explorer 的规则,再处理禁止FTP的规则,用户仍可以与FTP通信。用户可以在浏览器中输入使用FTP的URL,例如ftp://ftp.symantec.com。

请不要使用应用程序规则来控制网络级别的通信。例如,如果用户使用其他Web浏览器,禁止或限制使用 Internet Explorer 的规则就不会起作用。其他Web 浏览器所生成的通信还是会与Internet Explorer 规则以外的所有其他规则比较。规则配置为禁止某些应用程序发送和接收通信时,以应用程序为基础的规则更为有效。

**注意:**如果 Trend Micro PC-cillin IS 2007 与 Symantec Endpoint Protection 客户 端安装在同一台电脑上,则针对特定Web浏览器的防火墙规则将不会起作用。Trend Micro PC-cillin 会将 Web 通信提交至其自己的代理软件。在 Trend Micro PC-cillin 中,您必须禁用 Web 站点访问控制和数据威胁防护选项。

#### 关于主机触发器

定义主机触发器时,您可以指定位于所指定网络连接两端的主机。 通常,表示主机之间关系的方式是将主机称为网络连接的源或目标。 您可以使用下列任一方式定义主机关系:

源/目标 主机是源还是目标取决于通信的方向。有时候可能本地客户端计 算机是源,而有时候则可能远程计算机是源。源与目标关系较常用于网络型防火墙。

本地/远程 本地主机一定是本地客户端计算机,而远程主机一定是位于网络 其他位置的远程计算机。主机关系的这种表示与通信方向无关。 本地与远程关系较常用于主机型防火墙,而且比较容易查看通信。

图 29-1 以通信方向说明源和目标的关系。

图 29-1 源主机与目标主机



图 29-2 以通信方向说明本地主机与远程主机的关系。



您可以定义多个源主机和多个目标主机。您在连接两端所定义的主机可使用 OR 语 句评估。所选主机之间的关系则可使用 AND 语句评估。

例如,假设有个规则定义了单个本地主机和多个远程主机。当防火墙检查数据包时,本地主机必须匹配相关的 IP 地址。不过,地址的另一端则可匹配任何远程主机。例如,您可以定义规则来允许本地主机与 symantec.com、yahoo.com 或 google.com 之间的 HTTP 通信。这个规则的作用等于单独定义三个规则。

请参见第 403 页的"添加主机和主机组至规则"。

## 关于网络服务触发器

网络触发器会根据所指定的网络通信,标识产生作用的一个或多个网络协议。 您可以定义以下类型的协议:

ТСР	端口或端口范围
UDP	端口或端口范围
ICMP	类型和代码
IP	协议编号(IP 类型) 例如:类型 1 = ICMP、类型 6 = TCP、类型 17 = UDP
以太网	以太网帧类型 例如: 类型0x0800=IPv4, 类型=0x8BDD=IPv6, 类型0x8137 = IPX

定义TCP型或UDP型服务触发器时,您可以标识指定网络连接两端的端口。通常,端口称为网络连接的源或目标。

您可以使用下列任一方式定义网络服务关系:

源/目标 源端口和目标端口取决于通信方向。有一种情况是,本地客户端 计算机可能会拥有源端口;而另一种情况是远程计算机可能拥有 源端口。

本地/远程 本地主机计算机始终拥有本地端口,而远程计算机始终拥有远程 端口。此端口关系的说明与通信方向无关。

定义协议时,便会指定通信方向。

您可以定义多个协议。例如,规则可能包括 ICMP、IP 和 TCP 协议。规则会说明多 种类型的连接,这些可能是已标识客户端计算机之间的连接,也可能是应用程序所 使用的连接。

#### 关于网络适配器触发器

如果您定义了网络适配器触发器,则规则只会与使用指定适配器类型传送或接收的 通信有关。

您可以指定下列其中一种类型的适配器:

- 以太网
- 无线
- 拨号
- 任何 VPN
- 特定厂商的虚拟适配器

当您定义特定类型的适配器时,请将适配器的使用方式列入考虑范围。例如,如果规则允许以太网适配器的出站HTTP通信,则已安装的所有同类型适配器都会允许HTTP通过。唯一的例外是同时指定了本地主机地址。客户端计算机可能使用多NIC的服务器和工作站来桥接两个或两个以上网络段。若要控制特定适配器的相关通信,就必须使用每个段的地址方案,而不是适配器本身。

#### 关于规则处理顺序

防火墙规则依序安排,从最高优先级到最低优先级,或者按照"规则"列表中从上 到下的顺序。防火墙会依此顺序检查规则。如果第一项规则未指示如何处理数据 包,则防火墙就会检查第二项规则来获取有关如何处理数据包的信息。此过程会一 直进行下去,直到发现匹配的规则为止。防火墙发现匹配的规则之后,会采取该规 则指定的操作,不再检查优先级较低的后续规则。例如,如果先列出的规则禁止所 有通信,而其后的规则允许所有通信,则客户端会禁止所有通信。

#### 表 29-1 处理防火墙规则、IPS 特征及各项设置的顺序

优先级	设 <u>置</u>
第一	自定义 IPS 特征
第二	人侵防护设置、通信设置及隐藏设置
第三	智能通信过滤器
第四	防火墙规则
第五	端口扫描检查
第六	通过 LiveUpdate 下载的 IPS 特征

"规则"列表内有条蓝色分隔线。在下列情况中,分隔线会设置各项规则的优先级:

- 子组继承父组的规则。
- 客户端设置为混合控制。防火墙同时处理服务器规则和客户端规则。

```
图 29-3
```

```
规则列表
```



#### 关于继承的规则

防火墙会处理"规则"列表中继承的防火墙规则,其方式如下:

- 在蓝色分隔线之上,策略继承的规则优先级高于您创建的规则。
- 在蓝色分隔线之下,您创建的规则优先级高于策略继承的规则。

图 29-4 显示当子组从父组继承规则时, "规则"列表如何对规则进行排序。此例 中, "销售"组为父组。"欧洲销售"组继承自"销售"组。



请参见第 381 页的"添加继承自父组的规则"。

#### 关于服务器规则和客户端规则

规则可分为服务器规则或客户端规则。服务器规则是您在 Symantec Endpoint Protection Manager 控制台中创建的规则,也是下载至 Symantec Endpoint Protection 客户端的规则。客户端规则是用户在客户端上创建的规则。

表29-2说明以下两者之间的关系,客户端用户控制等级以及用户与防火墙规则的交互。

表 29-2 用户控制级别和规则状态

用户控制级别	用户交互
服务器控制	客户端接收到服务器规则,但用户不能查看这些规则。用户不能 创建客户端规则。
混合控制	客户端接收服务器规则。用户可以创建客户端规则,这些规则会 与服务器规则以及客户端安全设置合并。
客户端控制	客户端不接收服务器规则。用户可以创建客户端规则。您不能查 看客户端规则。

请参见第103页的"配置用户界面设置"。

对于混合控制的客户端,防火墙会以特定顺序处理服务器规则和客户端规则。 表 29-3 列出了防火墙处理服务器规则、客户端规则及客户端设置的顺序。

表 29-3 服务器

服务器规则和客户端规则的处理优先级

优先级	规则类型或设置
第一	高优先级的服务器规则("规则"列表中蓝线以上的规则)
第二	客户端规则
第三	低优先级的服务器规则("规则"列表中蓝线以下的规则)
	在客户端上, 蓝线以下的服务器规则会在客户端规则之后处理。
第四	客户端安全设置
第五	客户端应用程序特定设置

在客户端上,用户可以修改客户端规则或安全设置,但用户不能修改服务器规则。

警告:如果客户端为混合控制,则用户可以创建允许所有通信的客户端规则。此规则会覆盖蓝线以下的所有服务器规则。

请参见第 383 页的"更改规则的顺序"。

## 关于状态检查

防火墙会使用状态检查,此进程可跟踪有关当前连接的信息,例如源与目标 IP 地址、端口和应用程序。客户端在检查防火墙规则之前,会使用此连接信息决定通信的方向。

例如,如果某个防火墙规则允许客户端连接到Web服务器,则防火墙将记录该连接 信息。当服务器回复时,防火墙会发现期望Web服务器对客户端的响应,并且不检 查规则库就可允许Web服务器通信流向发起客户端。在防火墙记录连接之前,规则 必须允许初始的出站通信。

有了状态检查,您就可以简化规则库,因为不必为通常仅从一个方向发起的通信创 建允许双向通信的规则。通常单向发起的客户端通信包括Telnet(端口23)、HTTP (端口80)及HTTPS(端口443)。客户端会发起此出站通信,所以您只需为这 些协议创建一个允许出站通信的规则。防火墙允许返回通信。

通过只配置出站规则,您可以使用下列方式增加客户端安全:

- 降低规则库的复杂程度。
- 消除蠕虫或其他恶意程序在配置为仅用于出站通信的端口上连接到客户端的可能性。对于不是由客户端发起的客户端通信,还可以仅配置入站规则。

状态检查支持定向 TCP 通信的所有规则。状态检查不支持过滤 ICMP 通信的规则。 对于 ICMP 通信,必要时您必须创建允许双向通信的规则。例如,如果您希望客户 端使用 ping 命令并接收回复,则必须创建允许双向 ICMP 通信的规则。 由于防火墙在本质上是状态式的,因此您只需创建起始连接的规则,而无需创建特 定数据包的特性。一旦允许连接,就暗示着允许作为该连接主要部分的所有数据 包。

#### 关于 UDP 连接

对于 UDP 通信,客户端分析第一个 UDP 数据报,并将对初始数据报所执行的操作 应用于当前程序会话的所有后续 UDP 数据报。相同计算机之间的入站或出站通信 将被视为 UDP 连接的一部分。

对于状态 UDP 通信,当创建 UDP 连接时,即允许入站 UDP 通信,即使防火墙规则禁止此通信。例如,如果某个规则禁止特定应用程序的入站 UDP 通信,但您选择允许出站 UDP 数据报,则在当前的应用程序会话中将允许所有入站 UDP 通信。对于无状态 UDP,您必须创建允许入站 UDP 通信响应的防火墙规则。

若应用程序关闭端口, UDP 会话会在 40 秒后超时。

## 添加空白规则

当您创建新的防火墙策略时,策略会包括几个默认规则。默认规则可为办公室环境 提供基本防护。如果您需要其他防火墙规则,可以添加它们。 您可以使用下列方式添加规则:

- 将空白规则添加到列表, 然后手动配置该规则。
- 运行防火墙规则向导。
   请参见第 380 页的"使用向导添加规则"。

为了简化规则库管理,请尽可能在规则中同时指定人站和出站通信。您无需创建通 信(如HTTP)的人站规则。Symantec Endpoint Protection 客户端会对 TCP 通信 使用状态检查,因此不需要规则来过滤客户端发起的返回通信。

请参见第377页的"关于状态检查"。

#### 添加空白规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡的"规则"列表下,单击"添加空白规则"。
- 4 在"名称"文本框中,键入规则的名称。
- 5 在"严重性"字段中,单击下拉列表,然后选择下列选项之一:
  - 重要
  - 主要

- 次要
- 信息
- 6 右键单击"应用程序"字段,再单击"编辑",然后在"应用程序列表"对话框中定义应用程序。

请参见第 410 页的"将应用程序添加到规则"。

- 7 单击"确定",再单击"确定"。
- 8 右键单击"主机"字段,再单击"编辑",然后在"主机列表"中定义主机。 请参见第 403 页的"添加主机和主机组至规则"。
- 9 单击"确定",再单击"确定"。
- 10 右键单击"时间"字段,再单击"编辑",然后设置调度。 请参见第 411 页的"添加调度至规则"。
- 11 单击"确定",再单击"确定"。
- 12 右键单击"服务"字段,再单击"编辑",添加或配置自定义网络服务。 请参见第 405 页的"添加网络服务至规则"。
- 13 单击"确定"。
- 14 右键单击"适配器"字段,再选择下列一个或多个项目:
  - 所有适配器
  - 任何 VPN
  - 拨号
  - 以太网
  - 无线
  - 更多适配器
     您可以从特定供应商适配器的列表添加和选择

请参见第408页的"添加网络适配器"。

- 15 右键单击"屏幕保护程序"字段,再选择要屏幕保护程序处于哪一种状态:
  - 开
  - 关
  - 任意
- 16 右键单击"操作"字段,再选择通信符合规则时要防火墙采取的操作:
  - 允许
  - ∎ 禁止

■ 询问

- 17 右键单击"记录"字段,再选择通信符合规则时要防火墙采取的一个或多个记录操作:
  - 写入通信日志
  - 写入数据包日志
  - 发送电子邮件警报 请参见第 413 页的"配置通信事件的电子邮件"。

"创建位置"字段不可编辑。如果策略是共享的,该字段会显示"共享"。如 果策略不是共享的,该字段会显示非共享策略分配给的组的名称。

- 18 右键单击"说明"字段,再单击"编辑"。
- 19 在"输入说明"对话框中,键入规则的可选说明,再单击"确定"。
- 20 添加完规则后,执行下列操作之一:
  - 添加其他规则。
  - 添加智能通信过滤设置或通信与隐藏设置。
     请参见第 384 页的 "启用智能通信过滤"。
     请参见第 385 页的 "启用通信与隐藏设置"。
  - 配置完策略后,单击"确定"。
- 21 如果系统显示提示,请将策略分配到某个位置。 请参见第 289 页的"分配共享策略"。

## 使用向导添加规则

使用添加防火墙规则向导可创建下列任一类型的规则:

- 应用程序规则 基于尝试使用网络资源的特定运行进程的规则。
- 主机规则 基于网络连接端点的规则
- 服务规则 基于网络连接使用的协议的规则

您可能需要指定两个或两个以上的条件来说明特定的网络通信,例如来自特定主机 的特定协议。添加规则后必须对其进行配置,因为添加防火墙规则向导不会配置具 有多个条件的新规则。

当您开始熟悉规则的定义和处理方式后,就可以添加空白规则,然后视需要配置各 个字段。空白规则会允许所有通信。

请参见第 378 页的"添加空白规则"。

#### 使用向导添加规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡的"规则"列表下方,单击"添加规则"。
- 4 在添加防火墙规则向导中,单击"下一步"。
- 5 在"选择规则类型"面板中,选择其中一种规则类型。
- 6 单击"下一步"。
- 7 在每个面板输入数据,以创建所选类型的规则。
- 8 若为应用程序和主机规则,请单击"添加更多"来添加其他应用程序和服务。
- **9** 完成后,单击"完成"。
- 10 在"规则"列表中,右键单击任何字段编辑规则。
- 11 完成策略配置后,单击"确定"。

## 添加继承自父组的规则

您可以通过只从父组继承规则来添加规则。若要从父组继承规则,子组的策略必须 是非共享策略。

注意:如果组的所有策略都是从父组继承来的,则此选项将不可用。

请参见第44页的"关于组从其他组继承位置及策略"。

继承的规则会自动启用。子组的策略只能继承父组中启用的防火墙规则。当您已继 承规则时,可以禁用这些规则,但不能加以修改。将新规则添加到父组的策略中 时,新规则会自动添加到继承策略中。

当继承的规则显示在"规则"列表上时,会加上紫色阴影。在蓝字那行上面,继承 的规则会添加到您创建的规则上面。在蓝字那行下面,继承的规则会添加到您创建 的规则下面。

防火墙策略也会继承默认规则,因此子组的防火墙策略可能会有两组默认规则。您 可能要删除其中一组默认规则。

若要删除继承的规则,可以取消继承它们,而非删除它们。您必须删除所有继承的 规则,而不是所选规则。

#### 添加继承自父组的规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡的"规则"列表上方,选中"从父组继承防火墙规则"。 若要删除继承的规则,请取消选中"从父组继承防火墙规则"。
- 4 单击"确定"。

## 导入和导出规则

您可以从其他防火墙策略导出和导入防火墙规则和设置,如此就无需重新创建它 们。例如,您可将一个策略的部分规则集导入另一个策略。若要导入规则,您必须 先将规则导出至.dat 文件并有权访问该文件。

规则会以其在父策略所列的顺序添加,以蓝线为准。您可以稍后更改其处理顺序。

#### 导出规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"列表中,选择要导出的规则并右键单击该规则,再单击"导出"。
- 4 在"导出策略"对话框中,找到要保存.dat文件的目录,键入文件名,然后单击"导出"。

#### 导入规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 右键单击"规则"列表,再单击"导入"。
- 4 在"导入策略"对话框中,找到包含要导入的防火墙规则的.dat 文件,然后单击"导入"。
- 5 在"输入"对话框中,键入策略的新名称,然后单击"确定"。
- 6 单击"确定"。

## 复制并粘贴规则

您可以在相同策略或不同策略之间复制和粘贴规则。

#### 复制和粘贴规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡上,右键单击要复制的规则,再单击"复制规则"。
- 4 右键单击要粘贴规则的行,再单击"粘贴规则"。
- 5 单击"确定"。

## 更改规则的顺序

防火墙会由上而下处理防火墙规则列表。您可以通过更改防火墙规则的顺序,确定 防火墙处理防火墙规则的方式。更改顺序时,只会影响当前所选位置的顺序。

#### 更改规则的顺序

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则",再选择要移动的规则。
- 3 执行下列操作之一:
  - 若要让此规则优先于前面的规则处理,请单击"上移"。
  - 若要让此规则在其下面的规则之后进行处理,请单击"下移"。
- **4** 单击"确定"。

## 启用与禁用规则

规则必须启用,防火墙才能处理这些规则。如果需要允许对某计算机或应用程序进 行特定访问,则可以禁用防火墙规则。禁用共享策略时,所有位置都会禁用该规 则;禁用特定于位置的策略时,只有一个位置会禁用该规则。所有继承策略也都会 禁用该规则。

#### 启用和禁用防火墙规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。

- 3 在"规则"选项卡中,选择想要启用或禁用的规则,然后选中或取消选中"启用"列的复选框。
- 4 单击"确定"。

## 启用智能通信过滤

使用智能通信过滤器可在某些网络服务之间进行通信,以便不必定义明确允许这些服务的规则。可以启用"智能通信过滤器"以允许大多数网络上的DHCP、DNS和WINS通信。使用智能通信过滤器可对已配置为使用DHCP、DNS和WINS的网络连接进行出站请求和入站回复。

使用这些过滤器可使 DHCP、DNS 或 WINS 客户端接收来自服务器的 IP 地址,同时保护客户端不受来自网络的攻击。

- 当客户端向服务器发送请求时,客户端会等待五秒以允许入站响应。
- 如果客户端没有向服务器发送请求,则每个过滤器均不允许传送数据包。

使用智能过滤器可在发送请求时允许传送数据包。但不会禁止数据包。防火墙规则可允许或禁止数据包。

**注意**:若要在混合控制中配置这些设置,您还必须在"客户端用户界面混合控制设置"对话框中启用这些设置。

请参见第103页的"关于混合控制"。

#### 启用智能通信过滤

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页上单击"智能通信过滤"。
- 3 如果尚未选中,请选中下列任一复选框:
  - 启用智能 DHCP
  - 启用智能 DNS
  - 启用智能 WINS

有关这些选项的详细信息,请单击"帮助"。

- 4 单击"确定"。
- 5 如果系统显示提示,请将策略分配到某个位置。 请参见第 289 页的"分配共享策略"。

## 启用通信与隐藏设置

您可以启用各种通信设置和隐藏网页浏览设置,保护客户端不受特定类型的网络攻击。您可以启用通信设置,检测和禁止通过驱动程序、NetBIOS和令牌环进行通信的通信。您也可以配置设置,检测使用多种隐藏攻击方法的通信。您还可以控制不匹配任何防火墙规则的IP通信行为。在防火墙完成特定操作后,控制权就会移交给多个组件。每个组件都设计为用来执行不同类型的数据包分析。

**注意**:若要在混合控制中配置这些设置,您还必须在"客户端用户界面混合控制设置"对话框中启用这些设置。

请参见第103页的"关于混合控制"。

#### 启用通信与隐藏设置

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"通信与隐藏设置"。
- 3 如果没有选中复选框,请在"通信设置"和"隐藏设置"组框中选中任何一个 复选框。

有关这些选项的详细信息,请单击"帮助"。

- 4 单击"确定"。
- 5 如果系统显示提示,请将策略分配到某个位置。 请参见第 289 页的"分配共享策略"。

## 配置对等验证

使用对等验证,远程客户端计算机(对等方)可连接到同一公司网络中的另一台客 户端计算机(验证者)。验证者会暂时禁止来自远程计算机的入站 TCP 和 UDP 通 信,直到远程计算机通过主机完整性检查。

主机完整性检查验证远程计算机的下列特性:

- Symantec Endpoint Protection 和 Symantec Network Access Control 都已安 装在远程计算机上。
- 远程计算机符合主机完整性策略的要求。

如果远程计算机通过主机完整性检查,即允许其连接到验证者。

如果远程计算机未通过主机完整性检查,验证者将继续禁止该远程计算机。您可以 指定被禁止的远程计算机重新尝试连接到验证者的重试时间间隔。也可以指定始终 允许某些远程计算机,即使这些计算机不能通过主机完整性检查。如果未对远程计 算机启用主机完整性检查,则视为远程计算机通过主机完整性检查。

对等验证信息显示在"Enforcer客户端遵从性"日志和"网络威胁防护通信"日志中。

注意: 对等验证适用于服务器控制和混合控制模式, 但不适用于客户端控制模式。

警告:请不要为与管理服务器安装于同一台计算机上的客户端启用对等验证。否则,如果远程计算机未通过主机完整性检查,管理服务器将无法将策略下载至该远 程计算机。

#### 配置对等验证

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"对等验证设置"。
- 3 在"对等验证设置"窗格上,选中"启用对等验证"。
- 4 配置页面上所列出的每个值。 有关这些选项的详细信息,请单击"帮助"。
- 5 若要允许远程计算机在未经验证的情况下连接至客户端计算机,请选中"从验 证范围中排除主机",然后单击"排除主机"。 客户端计算机将允许到"主机列表"中所列计算机的通信。
- 6 在"排除主机"对话框中,单击"添加"以添加无须验证的远程计算机。
- 7 在"主机"对话框中,通过 IP 地址、IP 范围或子网定义主机,然后单击"确定"。
- 8 在"排除主机"对话框中,单击"确定"。
- 9 配置完此策略后,单击"确定"。
- 如果系统显示提示,请将策略分配到某个位置。
   请参见第 289 页的"分配共享策略"。

# 30

## 配置入侵防护

本章节包括下列主题:

- 关于入侵防护系统
- 配置入侵防护
- 创建自定义 IPS 特征

## 关于入侵防护系统

入侵防护系统 (IPS) 是 Symantec Endpoint Protection 客户端在防火墙后的第二层 防护。IPS是一种在已安装客户端并启用入侵防护系统的计算机上运行的网络系统。 如果检测到已知攻击,会自动以一或多种入侵防护方法禁止攻击。

入侵防护系统扫描网络中每个进出计算机的数据包来检测攻击特征。攻击特征是这 样一个数据包序列:该序列可标识攻击者利用操作系统或程序的已知漏洞的企图。

如果信息匹配已知的攻击,则 IPS 会自动舍弃数据包。IPS 还可以将与发送数据的 计算机之间的连接断开一段指定时间。此功能称为"活动响应",会保护网络上的 计算机不受任何方式的影响。

客户端包括下列可识别攻击特征的 IPS 引擎类型。

Symantec IPS 特征	Symantec IPS 特征使用可扫描多个数据包的流式引擎。 Symantec IPS 特征可拦截会话层的网络数据并捕获在应用程 序及网络堆栈间传递的 消息段。
自定义 IPS 特征	自定义 IPS 特征使用一个数据包式的引擎分别扫描每个数据 包。

入侵防护系统将检测到的攻击记录在安全日志中。您可以启用自定义 IPS 特征将检测到的攻击记录在数据包日志中。

## 关于 Symantec IPS 特征

Symantec IPS 会使用下列两种方法检查数据包。它分别扫描每个数据包,查找不符 合规范以及会使 TCP/IP 堆栈崩溃的模式。它也会将数据包视为信息流进行监控。 它通过查找向特定服务发出的利用或破坏系统的命令进行监控。IPS 可以记住以前 数据包中的全部或部分模式列表,并且可以将该信息应用于后续数据包检查。

IPS依赖一个包含大量攻击特征的列表来检测和禁止可疑的网络活动。Symantec安全响应中心团队提供已知威胁列表,您可以使用SymantecLiveUpdate在客户端上更新此列表。您可以将特征下载至控制台,然后使用LiveUpdate内容策略将它们下载至客户端。默认情况下,SymantecIPS引擎及相关IPS特征集会安装在客户端上。

请参见第 90 页的"配置 LiveUpdate 内容策略"。

您也可以更改 Symantec IPS 特征的行为。

请参见第 390 页的"更改 Symantec IPS 特征的行为"。

## 关于自定义 IPS 特征

客户端还包含支持数据包式特征的 IPS 引擎。流式及数据包式的引擎都会检测攻击 TCP/IP 堆栈、操作系统组件及应用程序层的网络数据中的特征。然而,数据包式特 征检测到 TCP/IP 堆栈中攻击的速度会比流式特征快。

数据包式引擎不会检测跨越多个数据包的特征。数据包式 IPS 引擎受到的限制比较多,因为它不能缓冲部分匹配项,并且只能扫描单个数据包负载。

数据包式特征可检查单个数据包是否匹配规则。规则是根据各种条件(如端口、协议、源或目标 IP 地址、TCP 标志号码或者应用程序)制定的。例如,自定义特征可监控收到的信息数据包中是否有 GET / cgi-bin/phf? 中的字符串 phf,该字符串表示 CGI 程序攻击。每个数据包都会经过评估,看是否具有该特定模式。如果通信数据包匹配规则,客户端就会允许或禁止此数据包,并选择性地在数据包日志中记录该事件。

一个自定义 IPS 特征包含以下部分:

- 说明性名称
   名称和说明会显示在安全日志中,也可以显示在数据包日志中,但不要求必须
   显示在数据包日志中。
- 可选说明
- 严重性 如果安全日志中的事件触发特征,则提供该事件的严重性等级。
- ∎ 通信方向
- 内容 内容即语法。请使用下面的标准语法:

rule protocol-type, [protocol-options,] [ip-protocol options,]
msg, content...

- rule protocol-type, [protocol-options,] [ip-protocol option,] = 通信说明
- msg = 安全日志中显示的文本字符串。
- content = 与数据包中的负载部分进行比对以确定是否可能匹配的字符串。
- 可选应用程序

您可以提供触发相应特征的应用程序名称,但不要求必须提供。提供应用程序 名称后,IPS引擎就可以只匹配指定应用程序的特征,而不是全部应用程序的特 征。通过提供应用程序名称,还可以帮助减少其他应用程序可能产生的误报。

事件触发特征时要采取的操作。 触发特征时,会允许或禁止通信,并将这一操作记录在安全日志中。如果严重 性很高,您应禁止通信。如果您只想监视通信,则允许通信。您可以将事件写 入数据包日志,但并不要求必须这样做。数据包日志用来转储事务数据包。

由于特征是以正则表达式和字符串匹配为基础的,所以可能会造成误报。自定义特征在尝试匹配数据包时,会使用这两个条件来搜索字符串。

客户端默认不包括自定义特征。您可创建自定义 IPS 特征。

请参见第 393 页的"创建自定义 IPS 特征"。

## 配置入侵防护

默认的 IPS 设置可防护客户端计算机不受各种威胁攻击。您可以自定义网络的默认 设置。您可以使用下列一种或多种方式自定义 IPS 设置:

- 启用入侵防护设置。
- 更改特定攻击特征的行为。
- 从扫描中排除特定计算机。
- 自动禁止攻击计算机。
- 启用入侵防护通知。
   请参见第 412 页的"配置网络威胁防护的通知"。
- 创建自定义 IPS 特征。
   请参见第 393 页的"创建自定义 IPS 特征"。

## 关于使用入侵防护策略

除自定义 IPS 特征和入侵防护通知外,当您配置入侵防护时,就会同时创建入侵防护策略。针对自定义 IPS 特征,您可以创建自定义 IPS 库。

您可以用创建和修改其他类型策略的类似方式创建与编辑入侵防护策略。您可以分 配、撤回、替换、复制、导出、导入或删除入侵防护策略或自定义入侵防护库。 您通常可将一个策略分配至安全网络中的多个组。如果对特定位置有特定要求,您 可以创建一个非共享、位置限定的策略。

对于本章所涉及的过程,我们是在假定您对策略配置的基本概念熟悉的情况下进行 介绍的。

请参见第 282 页的"关于策略"。

## 启用入侵防护设置

根据您选择的入侵防护技术,您可以在客户端上禁止某些类型的攻击。

您必须先启用入侵防护设置,才能启用 Symantec IPS 特征引擎或自定义 IPS 特征 引擎。如果没有启用此设置,客户端会忽略可能的攻击特征。

**注意**:若要在混合控制中配置这些设置,您还必须在"客户端用户界面混合控制设置"对话框中启用这些设置。

请参见第400页的"针对混合控制配置网络威胁防护设置"。

有关这些选项的详细信息,请单击"帮助"。

#### 启用入侵防护设置

- 在控制台中,打开"入侵防护策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"入侵防护策略"页面上,单击"设置"。
- 3 在"设置"页面上,选中下列适用的复选框:
  - 启用入侵防护
  - 启用拒绝服务检测
  - 启用端口扫描检测
- 4 配置完此策略后,单击"确定"。 请参见第 392 页的"设置排除的计算机列表"。

## 更改 Symantec IPS 特征的行为

基于下列原因,您可能想更改 Symantec IPS 特征的默认行为:

 减少误报的可能性。在某些状况下,无害的网络活动可能看似攻击特征。如果 您收到重复出现的可能攻击警告,而且您知道这些攻击是由安全的行为所触发, 您可以排除匹配这些无害活动的攻击特征。 ■ 减少客户端检查的攻击特征数以降低资源消耗。但是,您必须确保该攻击特征 不会构成威胁,才能将其排除禁止。

您可以更改 IPS 识别到攻击特征时客户端采取的操作。您也可以更改客户端是否将 事件记录在安全日志中。

注意:若要更改您创建或导入的自定义 IPS 特征的行为,您可以直接编辑该特征。

#### 更改 Symantec IPS 特征的行为

- 在控制台中,打开"入侵防护策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"入侵防护策略"页面上,单击"例外"。
- **3** 在"例外"页面上,单击"添加"。
- 4 在"添加入侵防护例外"对话框中,执行下列操作之一以过滤特征:
  - 若要显示特定类别的特征,请从"显示类别"下拉列表中选择选项。
  - 若要显示按特定严重性分类的特征,请从"显示严重性"下拉列表中选择 选项。
- 5 选择一个或多个 IPS 特征。

若要为所有特征设置相同行为,请单击"全选"。

- 6 单击"下一步"。
- 7 在"特征操作"对话框中,将操作从"禁止"更改为"允许",或者从"允许"更改为"禁止"。
- 8 可选择下列其中一种方式更改记录操作:
  - 将"记录通信"更改为"不记录通信"。
  - 将"不记录通信"更改为"记录通信"。
- 9 单击"确定"。

如果您要删除例外,并且将特征的行为恢复成原始行为,请选择此特征并单击 "**删除"**。

- 10 单击"确定"。
- 11 如果您想要更改其他特征的行为,请重复步骤3至10。
- 12 配置完此策略后,单击"确定"。

#### 删除例外

- 在控制台中,打开"入侵防护策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"入侵防护策略"页面上,单击"例外"。
- **3** 在"例外"窗格上,选择想要删除的例外,然后单击"删除"。
- 4 当请求您确认删除时,请单击"是"。

#### 禁止攻击计算机

当 Symantec Endpoint Protection 客户端检测到网络攻击时,它会自动禁止连接以确保客户端计算机的安全。客户端会启动活动响应,自动禁止特定期间内进出攻击 计算机的全部通信。攻击计算机的 IP 地址会针对单个位置而禁止。

攻击者的IP地址会记录在安全日志中。在客户端控制下,用户可以通过停止安全日 志中的活动响应,取消禁止攻击。

如果您将客户端设置为混合控制,则可以指定客户端上是否提供该设置供用户启用。如果未提供该设置,就必须在"客户端用户界面混合控制设置"对话框中启用 它。

请参见第400页的"针对混合控制配置网络威胁防护设置"。

更新的 IPS 特征、更新的拒绝服务特征、端口扫描以及 MAC 欺骗也会触发活动响应。

#### 禁止攻击计算机

- 在控制台中,打开"入侵防护策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"入侵防护策略"页面上,单击"设置"。
- 3 在"设置"页面上,选中"自动禁止攻击者的 IP 地址"。
- 4 在"禁止 IP 地址的秒数...秒"文本框中,指定要禁止可能攻击者的秒数。 输入从1秒到 999,999 秒的数字。
- 5 配置完此策略后,单击"确定"。

#### 设置排除的计算机列表

Symantec Endpoint Protection 客户端可能会将某些常规的 Internet 活动定义为攻击。例如,某些Internet 服务提供商会扫描计算机的端口,以确保您遵守其服务协议。或者,您可以将内部网络的某些计算机设置为测试用途。

您可以设置计算机列表,对于这些计算机,客户端不会匹配攻击特征、检查是否有端口扫描或拒绝服务攻击。客户端会允许这些主机的所有入站通信和出站通信,不论防火墙规则和设置或 IPS 特征为何。

**注意**:您也可以设置计算机列表,在 IPS 特征未检测到攻击的情况下允许这些计算 机的所有入站通信和出站通信。在此情况下,您可以创建允许所有主机的防火墙规则。

#### 设置排除的计算机列表

- 在控制台中,打开"入侵防护策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"入侵防护策略"页面上,单击"设置"。
- 3 选中"启用排除主机"(如果尚未选中),然后单击"排除主机"。
- 4 在"排除主机"对话框中,单击"添加"。
- 5 在"主机"对话框的下拉列表中,选择下列其中一种主机类型:
  - IP 地址
  - IP 范围
  - ∎ 子网
- 6 输入与所选主机类型关联的适当信息。

有关这些选项的详细信息,请单击"帮助"。

- 7 单击"确定"。
- 8 重复4和7,以向排除的计算机列表添加更多设备和计算机。
- 9 若要编辑或删除任何排除主机,请选择某一行,再单击"编辑"或"删除"。
- 10 单击"确定"。
- 11 配置完此策略后,单击"确定"。

## 创建自定义 IPS 特征

您可以自行编写特征,以标识特定入侵,并减少特征导致误报的可能性。您向自定 义特征添加的信息越多,特征就越有效。

创建自定义库时,可以将特征编为特征组,以方便管理。必须向自定义特征库添加 至少一个特征组,才能将特征添加到特征组。您可以在组之间和库之间复制和粘贴 特征。 警告:在编写入侵防护特征之前,您必须熟悉TCP、UDP或ICMP协议。格式不正确的特征可能会损坏自定义IPS库以及客户端的完整性。

若要创建自定义 IPS 特征,您必须完成下列步骤:

- 创建自定义 IPS 库。
- 添加特征。

#### 创建自定义 IPS 库

- 1 在控制台中,单击"策略",再单击"入侵防护"。
- 2 在"任务"下,单击"添加自定义入侵防护特征"。
- 3 在"自定义入侵防护特征"对话框中,键入库的名称和可选说明。

"NetBIOS组"是特征组示例,其中有一个示例特征。您可以编辑现有组或添加新组。

- 4 若要添加新组,请在"特征"选项卡的"特征组"列表下,单击"添加"。
- 5 在"入侵防护特征组"对话框中,键入组名和可选说明,再单击"确定"。 默认情况下,组已启用。如果启用特征组,则该组内的所有特征会自动启用。 若要保留组以供参考,但要禁用它,请取消选中"启用此组"。
- 6 添加自定义特征。

#### 添加自定义特征

- **1** 创建自定义 IPS 库。
- 2 在"特征"选项卡的"此组的特征"下,单击"添加"。
- 3 在"添加特征"对话框中,键入特征的名称和可选说明。
- 4 在"严重性"下拉列表中,选择严重性等级。 匹配特征条件的事件将记录为此严重性等级。
- 5 在"方向"下拉列表中,指定要特征检查的通信方向。
- 6 在"内容"字段中,键入特征的语法。 有关语法的详细信息,可以单击"帮助"。
- 7 如果您要应用程序触发特征,请单击"添加"。
- 8 在"添加应用程序"对话框中,键入应用程序的文件名和可选说明。 例如,若要添加应用程序 Microsoft Internet Explorer,请将文件名键入为 iexplore或iexplore.exe。如果不指定文件名,任何应用程序都可以触发特征。

9 单击"确定"。

默认情况下,将启用已添加的应用程序。如果要禁用应用程序以便稍后再启 用,请取消选中"已启用"列的复选框。

- 10 在"操作"组框中,选择特征检测到事件时要客户端采取的操作:
  - 禁止 标识并禁止事件或攻击,并将其记录在安全日志中
  - 允许 标识并允许事件或攻击,并将其记录在安全日志中
- 11 若要在数据包日志中记录事件或攻击,请选中"写入数据包日志"。
- 12 单击"确定"。

默认情况下,将启用已添加的特征。如果要禁用特征以便稍后再启用,请取消选中"已启用"列的复选框。

- 13 若要将其他特征添加到特征组,请重复步骤2到12。 若要编辑或删除特征,请选择该特征,然后单击"编辑"或"删除"。
- 14 完成配置此库后,单击"确定"。
- 15 如果系统发出相应提示,请将自定义 IPS 特征分配给组。 请参见第 289 页的"分配共享策略"。 您也可以将多个自定义 IPS 库分配给组。 请参见第 395 页的"将多个自定义 IPS 库分配给组"。

#### 将多个自定义 IPS 库分配给组

创建自定义IPS库后,可将它分配给组而非个别位置。然后您可以将其他自定义IPS 库分配给该组。

#### 将多个自定义 IPS 库分配给组

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择要为其分配自定义特征的组。
- 3 在"策略"选项卡的"与位置无关的策略与设置"下,单击"自定义入侵防 护"。
- 4 在"用于 <组名> 的自定义入侵防护"对话框中,针对要分配给该组的每个自 定义 IPS 库,选中"已启用"列的复选框。
- 5 单击"确定"。

## 更改特征的顺序

自定义特征的 IPS 引擎会按照特征列表中的特征列举顺序来检查特征。每个数据包 只会触发一个特征。当某个特征与人站或出站通信数据包匹配时, IPS 引擎就会停 止检查其他特征。因此, IPS 引擎会以正确的顺序执行特征。您可以在特征列表中 更改特征的顺序。如果有多个匹配的特征,则必须将优先级较高的特征转至上方。 例如,如果您添加一个特征组来禁止目标端口 80 的双向 TCP 通信,则可以添加下 列特征:

- 禁止端口 80 的所有通信
- 允许端口 80 的所有通信

如果"禁止所有通信"特征列在前面,则"允许所有通信"特征永不会应用。如果 "允许所有通信"特征列在前面,则"禁止所有通信"特征永不会应用,且会始终 允许所有 HTTP 通信。

#### 更改特征的顺序

- 1 打开自定义 IPS 库。
- 2 添加或编辑特征。

请参见第 394 页的"添加自定义特征"。

- **3** 在"特征"选项卡的"此组的特征"表中,选择要移动的特征,然后执行下列 操作之一:
  - 若要先处理此特征再处理其上面的特征,请单击"上移"。
  - 若要在处理此特征前先处理其下面的特征,请单击"下移"。
- 4 配置完此库后,单击"确定"。

#### 复制并粘贴特征

您可以在同一特征组中,在不同的特征组之间或在不同的特征库之间复制和粘贴特征。例如,您可能会发现将特征添加到了错误的特征组中。或者,您想拥有两个几 乎相同的特征。

#### 复制并粘贴特征

- 1 打开自定义 IPS 库。
- 2 在"自定义入侵防护特征"对话框中,在"特征"选项卡的"此组的特征"表中,右键单击要复制的特征,再单击"复制"。
- 3 右键单击特征列表, 然后单击"粘贴"。
- 4 配置完此库后,单击"确定"。
### 定义特征的变量

添加自定义 IPS 特征时,可以使用变量来代表特征中的可变数据。如果数据更改, 您可以编辑变量,而无需编辑整个库中的特征。

您必须先定义特征的变量,然后才能使用变量。然后,您可以在自定义特征库的任 意特征中使用您在该库中定义的变量。

您可以复制并粘贴现有示例变量的内容,作为创建内容的起始基础。

#### 定义变量

- 1 创建自定义 IPS 库。
- 2 在"自定义入侵防护特征"对话框中,单击"变量"选项卡。
- 3 单击"添加"。
- 4 在"添加变量"对话框中,键入变量的名称和可选说明。
- 5 添加变量值的内容字符串,最多 255 个字符。 键入变量内容字符串时,应遵循的语法规则与键入特征内容值时所遵循的语法规则相同。
- 6 单击"确定"。

变量添加到表后,您就可以将该变量用于此自定义库中的任何特征。

#### 使用特征的变量

- 在"特征"选项卡上,添加或编辑特征。
   请参见第 394 页的"添加自定义特征"。
- 2 在"添加特征"或"编辑特征"对话框中,在"内容"字段键入变量名称,名称之前加上货币符号(\$)。

例如,若要创建名为HTTP的变量,用来指定HTTP端口,请键入:

#### \$HTTP

- 3 单击"确定"。
- 4 配置完此库后,单击"确定"。

398 | 配置入侵防护 | **创建自定义 IPS 特征** 

# 31

# 自定义网络威胁防护

本章节包括下列主题:

- 启用和禁用网络威胁防护
- 针对混合控制配置网络威胁防护设置
- 添加主机和主机组
- 编辑和删除主机组
- 添加主机和主机组至规则
- 添加网络服务
- 编辑和删除自定义网络服务
- 添加网络服务至规则
- 启动网络文件和打印机共享
- 添加网络适配器
- 添加网络适配器至规则
- 编辑和删除自定义网络适配器
- 将应用程序添加到规则
- 添加调度至规则
- 配置网络威胁防护的通知
- 设置网络应用程序监控

## 启用和禁用网络威胁防护

默认情况下, "网络威胁防护"为启用。您可能希望在选定的计算机上禁用"网络 威胁防护"。例如,若您想在客户端计算机上安装补丁程序,就必须禁用其"网络 威胁防护",否则客户端计算机会强制防火墙禁止安装。

如果网络威胁防护禁用,出现下列情况时,它会自动启用:

- 用户关闭客户端计算机,然后重新启动。
- 客户端位置从服务器控制更改为客户端控制。
- 您将客户端配置为在一段特定时间后启用防护。
- 启用防护的新安全策略已下载至客户端。

您也可以从计算机状态日志手动启用"网络威胁防护"。

请参见第 173 页的"从日志运行命令和操作"。

您还可以授予客户端计算机用户启用或禁用防护的权限。不过,您可以覆盖客户端 的设置。或者,您也可以禁用客户端的防护,即使用户已经启用防护。您也可以启 用客户端的防护,即使用户已经禁用防护。

请参见第103页的"配置用户界面设置"。

#### 启用与禁用组的"网络威胁防护"

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端",选择您要为其启用或禁用防护的组。
- 3 执行下列操作之一:
  - 若要启用或禁用对组中所有计算机与用户的防护,请右键单击组,再单击 "对组运行命令",然后单击"启用网络威胁防护"或"禁用网络威胁防 护"。
  - 若要启用或禁用组中某些计算机与用户的防护,请在"客户端"选项卡上选择用户或计算机。然后右键单击选项,再单击"对客户端运行命令">"启用网络威胁防护"或"禁用网络威胁防护"。
- 4 若要确认操作,请单击"是"。
- 5 单击"确定"。

## 针对混合控制配置网络威胁防护设置

您可以设置客户端以使用户对于其可以配置哪些网络威胁防护设置不具有控制能力、具有完全控制能力或具有有限控制能力。当您配置客户端时,请依据下列指导 方针:

- 如果您将客户端设置为服务器控制,则用户不能创建任何防火墙规则,也不能 启用防火墙设置和入侵防护设置。
- 如果您将客户端设置为客户端控制,则用户可以创建防火墙规则,也可以启用 所有防火墙设置和入侵防护设置。
- 如果您将客户端设置为混合控制,则用户可以创建防火墙规则,而您可以决定 用户可启用哪些防火墙设置和入侵防护设置。

请参见第 103 页的"配置用户界面设置"。

#### 针对混合控制配置网络威胁防护设置

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下,选择具有您要修改的用户控制级别的组。
- 3 在"策略"选项卡的"特定于位置的策略与设置"下方,展开某位置下方的"特定于位置的设置"。
- 4 在"客户端用户界面控制设置"的右侧,单击"任务">"编辑设置"。
- 5 在"控制模式设置"对话框中,单击"混合控制",然后单击"自定义"。
- 6 在"客户端/服务器控制设置"选项卡的"防火墙策略"类别和"入侵防护策略"类别下方,执行下列操作之一:
  - 若要让用户可以配置客户端设置,请单击"客户端"。
  - 若要配置客户端设置,请单击"服务器"。
- 7 单击"确定"。
- 8 单击"确定"。
- 9 对于您设置为"服务器"的每个防火墙设置和入侵防护设置,在"防火墙策略"或"入侵防护策略"中启用或禁用此设置。

请参见第 384 页的"启用智能通信过滤"。 请参见第 385 页的"启用通信与隐藏设置"。 请参见第 389 页的"配置入侵防护"。

## 添加主机和主机组

主机组是DNS域名、DNS 主机名称、IP 地址、IP 范围、MAC 地址或子网的集合, 它们使用一个名称组成一组。主机组的目的是为了不必重复键入主机地址和名称。 例如,您可以将多个 IP 地址一次一个添加到防火墙规则中。或者,可以将多个 IP 地址添加到一个主机组,然后将该组添加到防火墙规则。

合并主机组时,必须说明组的使用位置。如果您以后决定删除主机组,必须先从引 用此组的所有规则中删除主机组。 添加主机组时,该主机组将出现在"主机列表"的底端。您可以从防火墙规则的 "主机"字段中访问"主机列表"。

请参见第 372 页的"关于主机触发器"。

#### 创建主机组

- 1 在控制台中,单击"策略"。
- 2 展开"策略组件",然后单击"主机组"。
- **3** 在"任务"下,单击"添加主机组"。
- 4 在"主机组"对话框中键入名称,然后单击"添加"。
- 5 在"主机"对话框的"类型"下拉列表中,选择下列其中一种主机:
  - DNS 域
  - DNS 主机
  - IP 地址
  - IP 范围
  - MAC 地址
  - ∎ 子网
- 6 键入每种主机类型的适当信息。
- 7 单击"确定"。
- 8 根据需要添加其他主机。
- 9 单击"确定"。

## 编辑和删除主机组

您可以编辑或删除任何您添加的自定义主机组。您不能编辑或删除默认的主机组。 在删除自定义主机组之前,您必须从所有引用此组的规则中删除此主机组。您所编 辑的设置在所有引用此组的规则中都会更改。

#### 编辑主机组

- 1 在控制台中, 单击"策略" > "策略组件" > "主机组"。
- 2 在"主机组"窗格中,选择要编辑的主机组。
- **3** 在"任务"下,单击"编辑主机组"。
- 4 在"主机组"对话框中,选择性地编辑组名,选择主机,然后单击"编辑"。 若要从组中删除主机,请单击"删除",再单击"是"。
- 5 在"主机"对话框中,更改主机类型或编辑主机设置。

- 6 单击"确定"。
- 7 单击"确定"。

#### 删除主机组

- **1** 在控制台中,单击"策略">"策略组件">"主机组"。
- 2 在"主机组"窗格中,选择您要删除的主机组。
- 3 在"任务"下,单击"删除主机组"。
- 4 当请求您确认时,请单击"删除"。

## 添加主机和主机组至规则

若要禁止特定服务器接收或提交的通信,请以IP地址而不是以域名或主机名来禁止 通信。否则,用户还是可以访问与此主机名对应的IP地址。

#### 添加主机和主机组至规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡的"规则"列表中,选择要编辑的规则,右键单击"主机" 字段,再单击"编辑"。
- 4 在"主机列表"对话框中,执行下列操作之一:
  - 单击"源/目标"。
  - 单击"本地/远程"。
- 5 在"源/目标"或"本地/远程"表中,运行下列任务之一:
  - 若要启用通过"策略组件"列表添加的主机组,请跳至步骤10。
     请参见第401页的"添加主机和主机组"。
  - 若只要在所选规则添加主机,请单击"添加"。
- 6 在"主机"对话框中,从"类型"下拉列表选择主机类型,然后输入各主机类型的适当信息。

若需此对话框其他选项的详细信息,请单击"帮助"。

- 7 单击"确定"。
- 8 根据需要添加其他主机。

- **9** 在"主机列表"对话框中,针对要触发防火墙规则的主机或主机组,确定"已 启用"栏中的复选框已选中。
- 10 单击"确定"回到"规则"列表。

## 添加网络服务

网络服务可让网络计算机发送和接收邮件,共享文件以及打印。网络服务会使用一个或多个协议或端口,传递特定类型的通信。例如,HTTP服务会通过TCP协议使用端口 80 和 443。您可以创建允许或禁止网络服务的防火墙规则。

使用网络服务列表,就无需在每次创建规则时重复键入协议和端口。您可以从常用 网络服务的默认列表选择网络服务,然后将该网络服务添加到防火墙规则。您也可 以将网络服务添加到默认列表。

注意: IPv4 和 IPv6 是两种用于 Internet 的网络层协议。防火墙会拦阻来自 IPv4 的攻击,但不会拦阻来自 IPv6 的攻击。如果您在运行 Microsoft Vista 的计算机上 安装客户端,则"规则"列表会包括数项禁止 IPv6 以太网协议类型的默认规则。如果删除这些默认规则,则必须创建禁止 IPv6 的规则。

如果您要允许或禁止的网络服务不在默认列表中,则可以添加该服务。您需要熟悉 服务所使用的协议类型和端口。

若要添加可从任何防火墙规则访问的自定义网络服务,请通过"策略组件"列表添加。

#### 将自定义网络服务添加到默认列表

- 1 在控制台中,单击"策略"。
- 2 展开"策略组件",然后单击"网络服务"。
- 3 在"任务"下,单击"添加网络服务"。
- 4 在"网络服务"对话框中,键入服务的名称,再单击"添加"。
- 5 从"协议"下拉列表中,选择下列其中一种协议:
  - TCP
  - UDP
  - ICMP
  - IP
  - 以太网

根据您选择的协议的不同,选项会有所变化。有关详细信息,可以单击"帮助"。

- 6 填好相应字段,再单击"确定"。
- 7 根据需要添加一个或多个附加协议。
- 8 单击"确定"。

您就可以将服务添加到任何防火墙规则。

## 编辑和删除自定义网络服务

您可以编辑或删除任何您添加的自定义网络服务。您不能编辑或删除默认的网络服务。在删除自定义网络服务之前,您必须从所有引用此服务的规则中删除此服务。

#### 编辑自定义网络服务

- 1 在控制台中,单击"策略">"策略组件">"网络服务"。
- 2 在"网络服务"窗格中,选择要编辑的服务。
- 3 在"任务"下,单击"编辑网络服务"。
- 4 在"网络服务"对话框中,更改服务名称,或选择协议,然后单击"编辑"。
- 5 更改协议设置。

有关此对话框中其他选项的信息,请单击"帮助"。

- 6 单击"确定"。
- 7 单击"确定"。

#### 删除自定义网络服务

- 1 在控制台中,单击"策略">"策略组件">"网络服务"。
- 2 在"网络服务"窗格中,选择要删除的服务。
- 3 在"任务"下,单击"删除网络服务"。
- 4 当请求您确认时,请单击"是"。

## 添加网络服务至规则

您可以通过防火墙规则添加自定义网络服务。不过,该网络服务不会添加到默认列 表。您不能从任何其他规则访问自定义适配器。

#### 添加网络服务至规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。

- **3** 在"规则"选项卡的"规则"列表中,选择要编辑的规则,右键单击"服务" 字段,再单击"编辑"。
- 4 在"服务列表"对话框中,针对要触发规则的每项服务,选中其旁边的"启 用"复选框。
- 5 若只要为所选规则添加其他服务,请单击"添加"。
- 6 在"协议"对话框中,从"协议"下拉列表选择协议。
- 7 填入适当的字段。

有关这些选项的详细信息,请单击"帮助"。

- 8 单击"确定"。
- 9 单击"确定"。
- 10 单击"确定"。

## 启动网络文件和打印机共享

您可以让客户端在本地网络中共享其文件,或通过浏览查找本地网络中的共享文件 和打印机。为防止网络攻击,您可能需要禁用网络文件和打印机共享。

您可以通过添加防火墙规则来启用网络文件和打印共享。防火墙规则允许访问端口 以浏览和共享文件及打印机。您需要先创建一个防火墙规则,使客户端可以共享其 文件。接着再创建第二个防火墙规则,使客户端可以通过浏览查找其他文件和打印 机。

如果客户端处于客户端控制或混合控制模式,则客户端用户可以通过在网络威胁防 护中配置这些设置来自动启用它们。在混合控制模式下,指定这种类型的通信的服 务器防火墙规则可以覆盖这些设置。在服务器控制模式下,这些设置在客户端上不 可用。

有关详细信息,请参见《Symantec Endpoint Protection 及 Symantec Network Access Control 客户端指南》。

#### 让客户端通过浏览查找文件和打印机

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"名称"栏中添加为空规则,然后键入规则的名称。 请参见第 378 页的"添加空白规则"。
- 4 右键单击"服务"字段,再单击"编辑"。
- 5 在"服务列表"对话框中,单击"添加"。

- 6 在"协议"对话框中的"协议"下拉列表中,单击 TCP,然后单击"本地/远程"。
- **7** 在"远程端口"下拉列表中,键入 88,135,139,445
- 8 单击"确定"。
- 9 在"服务列表"对话框中,单击"添加"。
- 10 在"协议"对话框中的"协议"下拉列表中,单击 UDP。
- 11 在"本地端口"下拉列表中,键入137,138
- 12 在"远程端口"下拉列表中,键入88
- 13 单击"确定"。
- 14 在"服务列表"对话框中,确保两项服务均已启用,然后单击"确定"。
- 15 在"规则"选项卡上,确保"操作"字段设为"允许"。
- 16 配置完策略后,单击"确定"。
- 17 如果系统显示提示,请将策略分配到某个位置。 请参见第 289 页的"分配共享策略"。

#### 让其他计算机能够浏览客户端上的文件

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"名称"栏中添加为空规则,然后键入规则的名称。 请参见第 378 页的"添加空白规则"。
- 4 右键单击"服务"字段,再单击"编辑"。
- 5 在"服务列表"对话框中,单击"添加"。
- 6 在"协议"对话框中的"协议"下拉列表中,单击TCP,然后单击"本地/远程"。
- 7 在"本地端口"下拉列表中,键入88,135,139,445
- 8 单击"确定"。
- 9 在"服务列表"对话框中,单击"添加"。
- 10 在"协议"对话框中的"协议"下拉列表中,单击 UDP。
- 11 在"本地端口"下拉列表中, 键入 88, 137, 138
- 12 单击"确定"。
- 13 在"服务列表"对话框中,确保两项服务均已启用,然后单击"确定"。

14 在"规则"选项卡上,确保"操作"字段设为"允许"。

- 15 配置完策略后,单击"确定"。
- 16 如果系统显示提示,请将策略分配到某个位置。 请参见第 289 页的"分配共享策略"。

## 添加网络适配器

您可以对每个网络适配器分别应用不同的防火墙规则。例如,您可能想要在办公室 禁止经过 VPN 的通信,但在家里不想这么做。

您可以从所有防火墙策略和规则共享的默认列表选择网络适配器。"策略组件"列表的默认列表中包括最常见的适配器。常见的适配器包括 VPN、以太网、无线、Cisco、Nortel和Enterasys 适配器。使用默认列表,您就无须为每个创建的规则重新键入每个网络适配器。

注意: 客户端不会过滤或检测来自 PDA (个人数字助理) 设备的网络通信。

#### 将自定义网络适配器添加到默认列表

- 1 在控制台中,单击"策略">"策略组件">"网络适配器"。
- 2 在"任务"下,单击"添加网络适配器"。
- 3 在"网络适配器"对话框中的"适配器类型"下拉列表中,选择适配器。
- 4 在"适配器名称"字段中,键入说明(可选)。
- 5 在"适配器标识"文本框中,键入适配器品牌名称,须区分大小写。 若要查找适配器的品牌名称,请打开客户端的命令行,然后键入下列文本: ipconfig/all。
- 6 单击"确定"。

接着,您就可以将适配器添加到任何防火墙规则。

## 添加网络适配器至规则

您可以通过防火墙规则添加自定义网络适配器。不过,该适配器不会添加到共享列 表。您不能从任何其他规则访问自定义适配器。

#### 添加网络适配器至规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡的"规则"列表中,选择要编辑的规则,右键单击"适配器"字段,再单击"更多适配器"。
- 4 在"网络适配器"对话框中,执行下列操作之一:
  - 若要触发任何适配器(包括未列出的适配器)的规则,请单击"应用规则 到所有适配器",然后转至步骤8。
  - 若要触发所选适配器的规则,请单击"应用规则到下列适配器",再针对 要触发规则的每个适配器,选中"已启用"复选框。
- 5 若只要为所选规则添加自定义适配器,请单击"添加"。
- 6 在"网络适配器"对话框中,选择适配器类型,然后在"适配器标识"文本字 段中输入适配器的品牌名称。
- 7 单击"确定"。
- 8 单击"确定"。
- 9 单击"确定"。

### 编辑和删除自定义网络适配器

您可以编辑或删除任何您添加的自定义网络适配器。您不能编辑或删除默认网络适 配器。在删除自定义适配器之前,您必须从所有引用此适配器的规则中删除此适配 器。您所编辑的设置在引用此适配器的所有规则中都会更改。

#### 编辑自定义网络适配器

- 1 在控制台中,单击"策略"。
- 2 在"策略组件"下,单击"网络配接器"。
- 3 在"网络适配器"窗格中,选择要编辑的自定义适配器。
- 4 在"任务"下,单击"编辑网络适配器"。
- 5 在"网络适配器"对话框中,编辑适配器类型、名称或适配器标识文本。
- 6 单击"确定"。

#### 删除自定义网络适配器

- 1 在控制台中,单击"策略"。
- 2 在"策略组件"下,单击"网络配接器"。

- 3 在"网络适配器"窗格中,选择要删除的自定义适配器。
- 4 在"任务"下,单击"删除网络适配器"。
- 5 当请求您确认时,请单击"是"。

## 将应用程序添加到规则

您可以定义有关客户端运行的应用程序的信息,并将此信息加入到防火墙规则中。 例如,您可能想要允许使用旧版的 Microsoft Word。

您可以使用下列方式定义应用程序:

- 可以通过手动键入信息,定义应用程序的特性。如果信息不足,则可以搜索已 知应用程序列表。
- 可以通过搜索已知应用程序列表,定义应用程序的特性。已知应用程序列表中的应用程序是您网络中的客户端计算机运行的应用程序。

#### 定义应用程序

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡的"规则"列表中,右键单击"应用程序"字段,再单击 "编辑"。
- 4 在"应用程序列表"对话框中,单击"添加"。
- 5 在"添加应用程序"对话框中,输入下列一个或多个字段:
  - 路径及文件名
  - ∎ 说明
  - 大小(以字节为单位)
  - 应用程序上次更改的日期
  - 文件指纹
- 6 单击"确定"。
- 7 单击"确定"。

#### 从已知应用程序列表中搜索应用程序

- 1 在"防火墙策略"页面上,单击"规则"。
- 2 在"规则"选项卡上选择规则,右键单击"应用程序"字段,再单击"编辑"。
- 3 在"应用程序列表"对话框中,单击"添加自"。

4 在"搜索应用程序"对话框中搜索应用程序。

请参见第 301 页的"搜索应用程序"。

- 5 若要将应用程序添加到"应用程序"列表,请在"查询结果"表下方选择应用 程序,单击"添加",再单击"确定"。
- 6 单击"关闭"。
- 7 单击"确定"。

## 添加调度至规则

您可以设置启用或禁用规则的时间。

#### 添加调度至规则

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡上,选择要编辑的规则,右键单击"时间"字段,再单击 "编辑"。
- 4 在"调度列表"对话框中,单击"添加"。
- 5 在"添加调度"对话框中,配置要启用或禁用规则的开始时间和结束时间。
- 6 在"月"下拉列表中,选择"全部"或特定月份。
- 7 选中下列复选框之一:
  - ∎ 每天
  - 周末
  - 工作日
  - 指定天 如果选中"指定天",请选中所列出的一个或多个日期。
- 8 单击"确定"。
- 9 在"调度列表"中,执行下列操作之一:
  - 若要使规则在这段时间保持启用状态,请取消选中"任何时间,除了"栏 的复选框。
  - 若要使规则在这段时间保持禁用状态,请选中"任何时间,除了"栏的复 选框。
- 10 单击"确定"。

## 配置网络威胁防护的通知

默认情况下,当客户端检测到各种"网络威胁防护"事件时,客户端计算机将显示 通知。您可以启用其中的某些通知。启用的通知会显示一条标准消息。您可以在标 准消息中加入自定义的文本。

表 31-1 显示了您可以启用和配置的事件类型。

表 31-1 网络威胁防护通知

通知类型	通知类型	说明
当客户端禁止应用程序时在 计算机上显示通知	防火墙	客户端的防火墙规则禁止了某应用程序。您可 以启用或禁用此通知,并可在通知中添加其他 文本。
在按照防火墙规则执行的操 作为"询问"时要显示的其 他文本	防火墙	客户端上的应用程序尝试访问网络。此通知始 终为启用,不可禁用。
显示入侵防护通知	入侵防护	客户端检测到入侵防护攻击。您可以在客户端 处于服务器控制或混合控制状态时启用或禁用 此通知。

#### 配置防火墙通知

1 在控制台中,打开"防火墙策略"。

请参见第288页的"编辑策略"。

- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"通知"选项卡上,选中"当客户端禁止应用程序时在计算机上显示通知"。
- 4 若要向规则操作设置为"询问"时所显示的标准消息中添加自定义文本,请选 中"在按照防火墙规则执行的操作为'询问'时要显示的其他文本"。
- 5 对任一项通知单击"设置其他文本"。
- 6 在"输入其他文本"对话框中,键入您希望通知显示的其他文本,再单击"确 定"。
- 7 配置完此策略后,单击"确定"。

#### 配置入侵防护通知

- 1 在控制台中,单击"客户端",然后在"查看客户端"中选择一个组。
- 2 在"策略"选项卡的"特定于位置的策略与设置"下方,展开某位置下方的"特定于位置的设置"。
- 3 在"客户端用户界面控制设置"的右侧,单击"任务",然后再单击"编辑设置"。

- 4 在 "<组名称> 的客户端用户界面控制设置"对话框中,单击"混合控制"或 "服务器控制"。
- 5 在"混合控制"或"服务器控制"旁,单击"自定义"。

如果您单击"混合控制",在"客户端/服务器控制设置"选项卡的"显示/隐 藏入侵防护通知"旁,单击"服务器"。然后单击"客户端用户界面设置"选 项卡。

- 6 在"客户端用户界面设置"对话框或选项卡中,单击"显示入侵防护通知"。
- 7 若要在通知出现时启用蜂鸣声,请单击"通知用户时使用音效"。
- 8 在"显示通知的秒数"文本字段中,键入您希望显示通知的秒数。
- 9 若要在显示的标准通知中添加文本,请单击"其他文本"。
- 10 在"其他文本"对话框中,键入您希望通知显示的其他文本,再单击"确定"。
- 11 单击"确定"。
- 12 单击"确定"。

#### 配置通信事件的电子邮件

您可以将 Symantec Endpoint Protection Manager 配置为每当防火墙检测到违规、 攻击或事件时向您发送电子邮件。例如,您可能想在客户端禁止来自特定 IP 地址的 通信时收到通知。

#### 配置通信事件的电子邮件

- 在控制台中,打开"防火墙策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"防火墙策略"页面上,单击"规则"。
- 3 在"规则"选项卡上选择规则,右键单击"记录"字段,然后执行下列操作:
  - 若要在触发防火墙规则时发送电子邮件,请选中"发送电子邮件警报"。
  - 若要在触发防火墙规则时生成日志事件,请选中"写入通信日志"和"写入数据包日志"。
- 4 配置完此策略后,单击"确定"。
- 5 配置安全警报。

请参见第180页的"创建管理员通知"。

6 配置邮件服务器。

请参见第 223 页的"建立 Symantec Endpoint Protection Manager 和电子邮件 服务器之间的通信"。

## 设置网络应用程序监控

您可以配置客户端检测和监控客户端计算机上运行的任何网络应用程序。网络应用 程序可发送和接收通信。客户端会检测应用程序的内容是否更改。

应用程序内容更改的原因如下:

- 应用程序遭受特洛伊木马攻击。
- 应用程序已更新为新版本或使用更新进行了更新。

如果您怀疑某一应用程序受到了特洛伊木马攻击,可以使用网络应用程序监控将客 户端配置为禁止此应用程序。您也可以将客户端配置为询问用户是允许还是禁止此 应用程序。

网络应用程序监控会将应用程序的行为记录在安全日志中。如果应用程序的内容修 改太过频繁,应用程序可能是受到了特洛伊木马的攻击,这样客户端计算机就会处 于不安全的状态。如果应用程序的内容修改并不是经常性的,则可能是安装了补丁 程序,客户端计算机应处于安全状态。您可以使用这些信息创建防火墙规则来允许 或禁止应用程序。

您可以将应用程序添加到列表,设置客户端不监控它们。您最好将认为不会受到特 洛伊木马攻击但经常会有自动补丁程序更新的应用程序排除在监控范围之外。

如果您认为客户端计算机有防病毒和防间谍软件防护的防护即已足够,则最好禁用 网络应用程序监控。同时您最好将询问用户允许或禁止网络应用程序的通知数减至 最少。

#### 设置网络应用程序监控

- 1 在控制台中,单击"客户端"。
- 2 在"查看客户端"下方选择组后,再单击"策略"。
- 3 在"策略"选项卡的"与位置无关的策略与设置"下方,单击"网络应用程序 监控"。
- 4 在"用于 <组名称> 的网络应用程序监控"对话框中,单击"启用网络应用程 序监控"。
- 5 在"**检测到应用程序更改时**"下拉式列表中,选择防火墙要对客户端上运行的 应用程序采取的操作:
  - 询问 询问用户是允许还是禁止应用程序。
  - 禁止通信 禁止应用程序使其不能运行。
  - 允许并记录
     允许应用程序运行,并将信息记录在安全日志中。
     防火墙只会对修改过的应用程序采取此操作。

- 6 如果选择"询问",请单击"附加文本"。
- 7 在"附加文本"对话框中,输入要出现在标准消息下方的文本,再单击"确定"。
- 8 若要将某一应用程序排除在监控范围之外,请在"未受监控的应用程序列表" 下方,执行下列操作之一:
  - 若要手动定义应用程序,请单击"添加",填入一个或多个字段,再单击 "确定"。
  - 若要从已知应用程序列表定义应用程序,请单击"添加自"。
     请参见第 301 页的"搜索应用程序"。
     已知应用程序功能必须启用。
     请参见第 300 页的"启用已知应用程序"。

已知应用程序列表可监控网络和非网络应用程序。您只能从已知应用程序列表 选择网络应用程序。将应用程序添加到"未受监控的应用程序列表"之后,您 可以启用、禁用、编辑或删除它们。

- 9 若要启用或禁用应用程序,选中"已启用"栏的复选框。
- 10 单击"确定"。

416 | 自定义网络威胁防护 | **设置网络应用程序监控** 





## 配置主动型威胁防护

- 配置 TruScan 主动型威胁扫描
- 配置应用程序与设备控制
- 自定义应用程序与设备控制策略

# 32

## 配置 TruScan 主动型威胁 扫描

本章节包括下列主题:

- 关于 TruScan 主动型威胁扫描
- 关于使用 Symantec 默认设置
- 关于 TruScan 主动型威胁扫描所检测的进程
- 关于管理 TruScan 主动型威胁扫描检测的误报
- 关于 TruScan 主动型威胁扫描忽略的进程
- TruScan 主动型威胁扫描如何与隔离区配合工作
- TruScan 主动型威胁扫描如何与集中式例外配合工作
- 了解 TruScan 主动型威胁检测
- 配置 TruScan 主动型威胁扫描频率
- 配置 TruScan 主动型威胁扫描的通知

## 关于 TruScan 主动型威胁扫描

TruScan 主动型威胁扫描可为计算机提供更高级别的防护。主动型威胁扫描可弥补现有防病毒、防间谍软件、入侵防护以及防火墙防护技术的不足之处。

防病毒和防间谍软件扫描大多依赖特征来检测已知威胁。主动型威胁检测则可使用 启发方式检测未知的威胁。启发式进程扫描会分析应用程序或进程的行为。此种扫 描将确定进程是否具有威胁(如特洛伊木马、蠕虫或击键记录程序)的特性。这种 防护有时被称为零时差攻击防护。 **注意**: 自动防护还会使用名为 Bloodhound 的启发式方式来检测文件中是否有可疑 行为。主动型威胁扫描则是检测活动进程中的可疑行为。

您可以在防病毒和防间谍软件策略中设置主动型威胁扫描。其中许多设置都可以锁 定,以防客户端计算机上的用户更改设置。

您可以配置下列设置:

- 要扫描的威胁类型
- 主动型威胁扫描的运行频率
- 检测到主动型威胁时,客户端计算机上是否要显示通知

启用"扫描特洛伊木马和蠕虫"和"扫描击键记录程序"设置时,会启用"TruScan 主动型威胁扫描"。如果禁用其中一项设置,Symantec Endpoint Protection 客户 端中的"状态"页面上,"主动型威胁防护"会显示为禁用。

主动型威胁扫描默认为启用。

**注意**:由于主动型威胁扫描会分析应用程序和进程是否有异常行为,因此可能会影 响计算机的性能。

## 关于使用 Symantec 默认设置

您可以决定要如何管理主动型威胁检测。您可以使用 Symantec 默认设置,或者指 定敏感级别和检测操作。

如果您选择让 Symantec 管理检测,客户端软件会决定操作和敏感级别。客户端计 算机上运行的扫描引擎会决定默认设置。如果您选择自行管理检测,可以设置单个 检测操作和特定敏感级别。

为将误报检测减至最少,Symantec 建议在刚开始时使用 Symantec 管理的默认设置。一段时间过后,您可以观察客户端检测到的误报数目。如果数目很少,您可以 逐步调整主动型威胁扫描设置。例如,对于特洛伊木马和蠕虫检测,您可以将敏感 度滑块调得比默认值高些。在设置新配置之后,您可以再观察主动型威胁扫描的运 行结果。

请参见第 425 页的"了解 TruScan 主动型威胁检测"。

请参见第 427 页的"指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级别"。

## 关于 TruScan 主动型威胁扫描所检测的进程

主动型威胁扫描会检测行为与特洛伊木马、蠕虫或击键记录程序类似的进程。通 常,这些进程所表现出的行为类型可能会受到威胁的利用,例如打开用户计算机上 的端口。

您可以配置某些类型的主动型威胁扫描设置。您可以启用或禁用对行为疑似特洛伊 木马、蠕虫或击键记录程序等进程的检测。例如,您可能想检测行为疑似特洛伊木 马和蠕虫的进程,但是不想检测行为疑似击键记录程序应用程序的进程。

Symantec 提供了可能会遭恶意利用的商业应用程序的列表。列表包括一些会记录 用户击键的商业应用程序,还包括可远程控制客户端计算机的应用程序。您最好了 解客户端计算机是否安装了这些类型的应用程序。默认情况下,主动型威胁扫描会 检测这些应用程序,并记录相关事件。您可以指定不同的补救操作。

您可以配置客户端在检测到各种特定类型的商业应用程序时应采取的补救操作类型。这些检测对象包括监控或记录用户的击键情况,或者远程控制用户计算机的商业应用程序。如果扫描检测出商业击键记录程序或商业远程控制程序,客户端会采取策略中设置的操作。您也可以允许用户控制操作。

主动型威胁扫描还会检测行为疑似广告软件和间谍软件的进程。您不能配置主动型 威胁扫描处理这些类型的检测的方式。如果主动型威胁扫描检测到广告软件或间谍 软件,而您要允许这些软件出现在客户端计算机上,则您必须创建集中式例外。

请参见第465页的"配置集中式例外策略"。

表 32-1 说明主动型威胁扫描所检测的进程。

进程类型	说明
特洛伊木马和蠕虫	表现出类似特洛伊木马或蠕虫的特征的进程。
	主动型威胁扫描会使用启发式扫描,查找疑似特洛伊木马或蠕虫的进程。这些进程可能是也可能不是威胁。
击键记录程序	呈现击键记录程序特性的进程。
	主动型威胁扫描会检测商业击键记录程序,但也会检测呈现击键 记录程序行为的任何未知进程。击键记录程序是捕获用户的击键 过程的击键记录应用程序。这些应用程序可用来收集密码信息和 其他重要信息。这些不一定是威胁。
商业应用程序	可能用于恶意用途的已知商业应用程序。
	主动型威胁扫描会检测各种类型的商业应用程序。您可以配置两 种类型的操作:击键记录程序和远程控制程序。

表32-1

TruScan 主动型威胁扫描所检测的进程

进程类型	说明
广告软件和间谍软件	呈现广告软件和间谍软件特性的进程
	主动型威胁扫描会使用启发式扫描,检测疑似广告软件和间谍软件的未知进程。这些进程可能是也可能不是风险。

您可以通过配置客户端软件设置是否将主动型威胁检测的信息提交至 Symantec。 您可以将此设置包含在防病毒和防间谍软件策略内。

请参见第 337 页的"将有关扫描的信息提交给 Symantec"。

## 关于管理 TruScan 主动型威胁扫描检测的误报

TruScan 主动型威胁扫描有时会返回误报。主动型威胁扫描会查找有可疑行为的应 用程序和进程,而不是查找已知的病毒或安全风险。由于其本身的特性,这些扫描 通常会标记不需要检测的项目。

对于特洛伊木马、蠕虫或击键记录程序的检测结果,您可以选择使用 Symantec 指 定的默认操作和敏感级别。您也可以选择自行管理检测操作和敏感级别。如果您自 行管理设置,则您检测的结果可能会有许多误报。如果您要管理操作和敏感级别, 应该注意这对安全网络的影响。

**注意**:如果您更改了敏感级别,检测结果总数也会更改。如果您更改了敏感级别,可能会减少主动型威胁扫描生成的误报数。Symantec的建议是,如果您要更改敏感级别,应逐步更改,并监控结果。

如果主动型威胁扫描检测到您认为不是问题的进程,您可以创建例外。某进程创建 为例外后,便可确保日后扫描时不会标记该进程。客户端计算机的用户也可以创建 例外。如果用户定义的例外和管理员定义的例外发生冲突,会优先采用管理员定义 的例外。

请参见第465页的"配置集中式例外策略"。

表 32-2 简述了创建管理误报的计划的各项任务。

表 32-2 官埕 医 推 的 计 划		
任务	说明	
确保由 Symantec 管理 特洛伊木马、蠕虫和击 键记录程序的检测。	防病毒和防间谍软件策略包括Symantec管理的设置。默认情况下, 启用此设置。启用此设置后,Symantec会决定检测到这些类型的 进程后应采取的操作。Symantec也会决定扫描的敏感级别。	
	由 Symantec 管理检测时,主动型威胁扫描会根据扫描对检测结果的判断执行相应操作。	
	扫描会对检测结果执行下列其中一项操作:	
	<ul> <li>■ 隔离区 若检测结果很有可能确实是威胁,扫描会执行此操作。</li> <li>■ 仅记录 若检测结果可能是误报,扫描会执行此操作。</li> </ul>	
	<b>注意:</b> 如果检测操作是由您管理,则请选择其中一个操作。您所选择的操作会始终用于相应的检测类型。如果您将操作设置为"隔离",客户端会隔离相应检测类型的所有项目。	
确保 Symantec 内容是 最新的。	确认生成误报的计算机具有最新的 Symantec 内容。最新的内容应 包括 Symantec 已判定为已知误报的进程的相关信息。主动型威胁 扫描不会检测这些已知误报。	
	您可以在控制台中运行一个报告,以检查哪些计算机在运行最新版 本的内容。	
	请参见第185页的"关于使用监视器和报告来帮助确保网络安全"。	
	若要更新内容,可以执行下列任一操作:	
	<ul> <li>应用 LiveUpdate 策略。 请参见第 89 页的"关于 LiveUpdate 策略"。</li> <li>为"客户端"选项卡中列出的选定计算机运行"更新"命令。</li> <li>为计算机状态或风险日志中列出的选定计算机运行"更新"命令。</li> </ul>	
确保提交已启用。	提交设置是防病毒和防间谍软件策略的一部分。	
	确保客户端计算机已配置为自动将主动型威胁扫描检测到的进程相关信息发送至Symantec安全响应中心。默认情况下,启用此设置。	
	请参见第 337 页的"将有关扫描的信息提交给 Symantec"。	
针对发现的误报创建例 外。	您可以创建一个策略来将针对所发现误报的例外包括在内。例如, 您可能会在安全网络中运行某个进程或应用程序,您知道该进程可 在您的环境中安全运行。如果TruScan主动型威胁扫描检测出该进 程,您可以创建例外,以便日后扫描不会检测该进程。	
	请参见第465页的"配置集中式例外策略"。	

表 32-2 管理误报的计划

## 关于 TruScan 主动型威胁扫描忽略的进程

TruScan 主动型威胁扫描允许特定进程,使这些进程免于扫描。Symantec 设有此 进程列表。Symantec 通常会将已知是误报的应用程序填入此列表。安全网络中的 客户端计算机会在下载新内容时定期收到此列表的更新。客户端计算机可使用几种 方式下载内容。管理服务器可发送更新的内容。您或您的用户也可在客户端计算机 上运行 LiveUpdate。

TruScan 主动型威胁扫描会忽略某些进程。这些进程可能包括 Symantec 没有足够 相关信息的应用程序或加载其他模块的应用程序。

您也可以指定 TruScan 主动型威胁扫描忽略某些进程。您可以通过创建集中式例外,指定主动型威胁扫描忽略特定进程。

客户端计算机上的用户也可以为主动型威胁扫描创建例外。如果管理员定义的例外 与用户定义的例外发生冲突,主动型威胁扫描只会应用管理员定义的例外。扫描时 会忽略用户的例外。

请参见第 424 页的"TruScan 主动型威胁扫描如何与集中式例外配合工作"。

## TruScan 主动型威胁扫描如何与隔离区配合工作

您可以配置主动型威胁扫描来隔离检测到的项目,客户端计算机上的用户可还原隔 离的条目。Symantec Endpoint Protection 客户端还可以自动还原已隔离的项目。

当客户端收到新定义时,会重新扫描隔离的条目。如果隔离的项目被视为是恶意 的,客户端会记录该事件。

客户端计算机会定期收到 Symantec 定义的已知正常的进程和应用程序列表更新。 当客户端计算机收到新列表时,就会根据最新的列表检查隔离的项目。如果最新的 列表允许任何隔离的项目,客户端会自动还原这些项目。

此外,管理员或用户还可以为主动型威胁检测创建例外。当最新的例外允许隔离的 项目时,客户端会还原这些项目。

用户可以在客户端的"查看隔离区"页面上查看隔离的项目。

客户端不会将主动型威胁扫描隔离的项目提交到中央隔离服务器。用户可以自动或 手动将本地隔离区中的项目提交到 Symantec 安全响应中心。

请参见第 342 页的"将已隔离的项目提交至 Symantec"。

## TruScan 主动型威胁扫描如何与集中式例外配合工作

您可以自行创建例外列表,以供 Symantec Endpoint Protection 客户端在运行主动 型威胁扫描时进行检查。创建这些列表的方式是创建例外。例外可指定主动型威胁 扫描检测的进程,以及检测到指定的进程时要采取的操作。您创建的例外进程不能 包括在 Symantec 定义的已知进程和应用程序列表中。 例如,您可能想创建例外来执行下列任何操作:

- 忽略特定商业击键记录程序
- 隔离不想在客户端计算机上运行的特定应用程序
- 允许特定远程控制应用程序运行

为避免例外之间发生冲突, 主动型威胁扫描使用以下优先顺序:

- Symantec 定义的例外
- 管理员定义的例外
- 用户定义的例外

Symantec 定义的列表始终优先于管理员定义的例外。管理员定义的例外始终优先于用户定义的例外。

您可以使用集中式例外策略,将检测操作设置为"忽略",以指定允许检测到的已 知进程。您也可以创建集中式例外,将操作设置为"隔离"或"终止",以指定不 允许特定进程。

管理员可以创建集中式例外,指定要主动型威胁扫描检测的文件名,从而强制执行 主动型威胁检测。当主动型威胁扫描检测到该文件时,客户端会记录此实例。因为 文件名并不是唯一的,所以可能会有多个进程使用相同的文件名。您可以使用强制 检测来帮助创建例外,以忽略、隔离或终止特定进程。

当客户端计算机上的主动型威胁扫描记录检测到的进程时,该进程会加入已知进程 列表。当您创建主动型威胁扫描的例外时,就可以从列表中选择进程。您可以设置 对检测到的进程执行特定的操作。您也可以使用控制台中"监视器"选项卡下的主 动型检测日志来创建例外。

请参见第465页的"配置集中式例外策略"。

请参见第167页的"查看日志"。

用户可以在客户端计算机上通过下列其中一种方法创建例外:

- 查看隔离区列表
- 扫描结果对话框
- 集中式例外

管理员可以锁定例外列表,以便用户不能创建任何例外。如果用户在管理员锁定列 表之前就创建了例外,则用户创建的例外会处于禁用状态。

## 了解 TruScan 主动型威胁检测

当 TruScan 主动型威胁扫描检测到标记为可能为恶意程序的进程时,其中有些进程 通常是合法进程。有些检测不能提供足够信息,因此不能将其归类为威胁或误报; 这些进程被视为"未知"。 主动型威胁扫描会在扫描运行时,检查活动进程的行为。扫描引擎会检查特定的行为,例如启用端口或捕获击键。如果某项进程表现出了这类行为,且达到一定程度,扫描会将该进程标记为潜在威胁。如果进程在扫描时未显示可疑行为,则扫描不会标记该进程。

默认情况下,主动型威胁扫描会检测疑似特洛伊木马、蠕虫或击键记录程序的进程。您可以在防病毒和防间谍软件策略中启用或禁用这些检测类型。

**注意**: 主动型威胁扫描设置不会影响防病毒和防间谍软件扫描, 因为扫描是使用特征检测已知风险。客户端会先检测已知的风险。

客户端将使用 Symantec 默认设置来判断应对检测到的项采取何种操作。如果扫描 引擎判断项目无须补救,客户端会记录该项检测。如果扫描引擎判断相应项目需要 补救,客户端会隔离该项目。

**注意**: Windows 服务器操作系统或 64 位 Windows XP Professional 当前不支持"扫描特洛伊木马和蠕虫"和"扫描击键记录程序"选项。.您可以为服务器操作系统上运行的客户端修改防病毒和防间谍软件策略中的这些选项,但是扫描并不会运行。 在服务器操作系统的客户端用户界面中,扫描选项会显示为不可用。如果您在策略中启用扫描选项,则这些选项会选中,但不可用。

Symantec 默认设置还用来决定主动型威胁扫描的灵敏度。灵敏度等级愈高,标记的进程愈多。灵敏度等级愈低,标记的进程愈少。灵敏度等级不指示检测的确定程度。也不会影响误报检测率。灵敏度等级愈高,扫描检测到的误报和实报愈多。

您应该使用 Symantec 默认设置来帮助尽量减少检测到的误报数。

您可以禁用 Symantec 定义的默认设置。禁用 Symantec 默认设置后,您可以针对 检测到的特洛伊木马、蠕虫或击键记录程序配置操作和敏感级别。在客户端用户界 面上,显示的默认设置将不是 Symantec 的默认设置。而是您手动管理检测时所使 用的默认设置。

对于商业应用程序,您可以指定主动型威胁扫描进行检测时客户端可采取的操作。 您可以为商业击键记录程序检测和商业远程控制应用程序检测分别指定不同的操 作。

**注意**:如果防病毒和防间谍软件策略中的相关设置未锁定,则客户端计算机上的用 户可以修改主动型威胁扫描设置。在客户端计算机上,TruScan 主动型威胁扫描设 置会显示在"主动型威胁防护"下。

#### 指定 TruScan 主动型威胁扫描检测的进程类型

TruScan 主动型威胁扫描默认会检测特洛伊木马、蠕虫和击键记录程序。您可以禁用对特洛伊木马、蠕虫和击键记录程序的检测。

您可以单击"帮助"来了解有关扫描的进程类型选项的详细信息。

#### 指定 TruScan 主动型威胁扫描检测的进程类型

- 1 在"防病毒和防间谍软件策略"页面上,单击"TruScan主动型威胁扫描"。
- 2 在"扫描详细信息"选项卡的"正在扫描"中,选中或取消选中"扫描特洛伊 木马和蠕虫"和"扫描击键记录程序"。
- 3 单击"确定"。

#### 指定检测特洛伊木马、蠕虫和击键记录程序的操作和敏感级别

TruScan 主动型威胁扫描不同于防病毒和防间谍软件扫描。防病毒和防间谍软件扫描会查找已知风险。主动型威胁扫描则根据特定类型进程或应用程序的行为查找未知的风险。这种扫描会检测任何类似特洛伊木马、蠕虫或击键记录程序的行为。

如果让 Symantec 管理检测,则对于正确的结果,检测操作为"隔离",而对于误报的结果,检测操作为"仅记录"。

如果您自行管理检测,则可以配置检测操作。主动型威胁扫描进行检测时,始终都 会使用该操作。例如,您可以指定 Symantec Endpoint Protection 客户端记录检测 到的行为类似特洛伊木马和蠕虫的进程。当客户端检测到进程时,不会予以隔离, 而是仅记录事件。

您可以配置敏感级别。当您设置较高的敏感级别时,主动型威胁扫描会提高检测率 (实报率和误报率)。

**注意**:如果启用这些设置,可能会生成高误报率。您应该清楚安全网络中运行的进程类型。

您可以单击"帮助"以了解扫描的操作和敏感度选项的详细信息。

#### 指定对特洛伊木马、蠕虫或击键记录程序的操作和敏感度

- 1 在"防病毒和防间谍软件策略"页面上,单击"TruScan主动型威胁扫描"。
- 2 在"扫描详细信息"选项卡的"正在扫描"下,确保选中"扫描特洛伊木马和 蠕虫"和"扫描击键记录程序"。
- 3 针对各风险类型,取消选中"使用 Symantec 定义的默认值"。

- 4 针对任一风险类型,将操作设置为"记录"、"终止"或"隔离"。 如果操作设置为"隔离"或"终止",且您启用了通知,则会发送通知。(默认情况下,通知已启用)。请审慎使用"终止"操作。在某些情况下,这可能会导致应用程序不能工作。
- 5 执行下列操作之一:
  - 左右移动滑块,以分别降低或提高敏感度。
  - 单击"低"或"高"。
- 6 单击"确定"。

#### 指定检测到商业应用程序时应采取的操作

您可以更改在TruScan主动型威胁扫描检测到结果时所要采取的操作。如果您将操 作设置为"忽略",主动型威胁扫描会忽略商业应用程序。

有关以下步骤中所使用选项的详细信息,您可以单击"帮助"。

#### 指定检测到商业应用程序时应采取的操作

- 1 在"防病毒和防间谍软件策略"页面上,单击"TruScan主动型威胁扫描"。
- 2 在"扫描详细信息"选项卡的"正在检测商业应用程序"下,将操作设置为 "忽略"、"记录"、"终止"或"隔离"。
- 3 单击"确定"。

## 配置 TruScan 主动型威胁扫描频率

您可以配置TruScan主动型威胁扫描的运行频率,方法是在"防病毒和防间谍软件 策略"中添加相应设置。

注意: 更改主动型威胁扫描的频率可能会影响客户端计算机的性能。

您可以单击"帮助"来了解有关扫描频率选项的详细信息。

#### 配置主动型威胁扫描频率

- 1 在"防病毒和防间谍软件策略"页面上,单击"TruScan主动型威胁扫描"。
- 2 在"扫描频率"选项卡的"扫描频率"下方,设置下列选项之一:
  - 使用默认扫描频率 扫描引擎软件会确定扫描频率。此选项为默认设置。
  - 使用自定义扫描频率

如果启用此选项,则可以指定客户端在检测到新进程时立即进行扫描。您也可以配置扫描频率时间。

3 单击"确定"。

## 配置 TruScan 主动型威胁扫描的通知

默认情况下,只要TruScan主动型威胁扫描检测到进程,就会向客户端计算机发送 通知。如果不希望通知用户,则可以禁用通知。

通知的目的是警报用户,告知主动型威胁扫描检测到进程,让用户采取补救措施。 用户可以使用通知对话框,针对检测到的进程采取补救措施。若主动型威胁扫描检 测到的进程不需要补救,Symantec Endpoint Protection 客户端会记录检测事件, 但不会发送通知。

**注意**:如果您设置检测使用 Symantec 默认设置,则只有在客户端建议补救进程时 才会发送通知。

用户也可以通过查看威胁日志并选择操作来补救检测到的进程。

您可以创建集中式例外来排除进程不受检测;客户端计算机上的用户也可以创建例 外。

请参见第463页的"关于集中式例外策略"。

您可以单击"帮助"以获取有关扫描的通知选项的详细信息。

#### 配置 TruScan 主动型威胁扫描的通知

- 1 在"防病毒和防间谍软件策略"页面上,单击"TruScan主动型威胁扫描"。
- 2 在"通知"选项卡上,选中或取消选中下列选项:
  - 检测到时显示消息。
  - 终止进程前提示。
  - 停止服务前提示。
- 3 单击"确定"。

430 | 配置 TruScan 主动型威胁扫描 | 配置 TruScan 主动型威胁扫描的通知

# 33

## 配置应用程序与设备控制

本章节包括下列主题:

- 关于应用程序与设备控制
- 关于应用程序与设备控制策略的结构
- 关于应用程序控制
- 关于设备控制
- 关于使用应用程序与设备控制策略
- 启用默认的应用程序控制规则集
- 创建应用程序与设备控制策略
- 配置应用程序与设备控制策略的应用程序控制
- 为应用程序与设备控制策略配置设备控制

## 关于应用程序与设备控制

基于下列原因,您可能需要使用应用程序和设备控制:

- 避免恶意软件拦截客户端计算机上的应用程序
- 避免不慎删除客户端计算机的数据
- 限制可在客户端计算机上运行的应用程序
- 将计算机受周边设备安全威胁感染的可能性降至最低

使用"应用程序与设备控制策略",可在客户端计算机上实现应用程序与设备控制。

应用程序与设备控制策略对客户端计算机提供下列类型的防护:

- 由应用程序控制监控客户端计算机上的 Windows API 调用,并控制客户端文件、文件夹、注册表项和进程的访问。 它可保护系统资源免受应用程序的侵害。
- 由设备控制管理可附加到计算机的周边设备。

创建新的"应用程序与设备控制策略"时,可以定义这两种防护类型。您也可以选择先添加应用程序控制或设备控制,然后再添加另一种防护。

组中的每个位置只能应用一个应用程序与设备控制策略。如果您要实现两种类型的 防护,您必须在相同的策略中定义应用程序控制与设备控制。

**注意**:本章中的信息仅适用于 32 位的客户端计算机。应用程序与设备控制策略不 适用于 64 位的客户端计算机。

## 关于应用程序与设备控制策略的结构

"应用程序与设备控制策略"的应用程序控制部分会包括多个规则集,而每个规则 集都会包括一项或多项规则。您可以配置规则集的属性,以及各项规则的属性、条 件和操作。

规则控制会尝试访问 Symantec Endpoint Protection 监控的计算机实体,例如文件 或注册表值。您可以将这些不同类型的尝试配置为条件。对于各项条件,您可以配 置匹配条件时要采取的操作。您可以配置规则只应用于某些应用程序,也可以配置 规则排除操作应用于其他应用程序。

请参见第 434 页的"关于应用程序控制规则属性"。

请参见第 435 页的"关于应用程序控制规则条件"。

请参见第 435 页的"关于应用程序控制规则条件属性"。

请参见第 436 页的"关于应用程序控制规则条件操作"。

设备控制包括禁止的设备列表及不禁止的设备列表。您可以添加到这两份列表,并 管理其中的内容。

图 33-1 说明应用程序和设备控制组件,以及它们彼此之间的关系。


### 关于应用程序控制

应用程序控制可监视和控制应用程序的行为。您可以禁止或允许访问指定的注册表项、文件和文件夹。您也可以禁止或允许应用程序启动或终止其他进程。您可以定义允许哪些应用程序运行,而哪些应用程序不可通过不正常进程予以终止。您可以定义哪些应用程序可以调用动态链接库 (DLL)。

警告:应用程序控制是高级的安全功能,只能由有经验的管理员进行配置。

使用定义您如何控制应用程序的规则集,可实现应用程序控制。应用程序控制是允 许或禁止操作的一组控制。您可以在策略中创建所需数量的规则集。您也可以使用 各规则集的"已启用"选项,配置哪些规则集随时启用。 您可以依照下列方式,使用应用程序控制来保护客户端计算机:

■ 保护特定注册表项和值。

- 保护目录,例如\WINDOWS\system 目录。
- 防止用户改变配置文件。
- 保护重要的程序文件,例如安装客户端的 Symantec 主目录。
- 保护特定进程,或排除进程而不予以保护。
- 控制 DLL 的访问。

### 关于测试模式

创建应用程序控制规则集时,您会在默认模式中创建,也就是"测试"(仅记录) 模式。"测试"模式可以先测试规则,然后再予以启用。在"测试"模式中,不会 应用任何操作,但是会按照已应用来记录您配置的操作。使用"测试"模式,可以 将策略分配到组和位置,并生成客户端"控制"日志。您可以检查客户端控制日志 中有无错误,然后针对规则进行必要的更正。在策略工作合乎预期之后,您便可以 将模式更改为"生产"模式,运行应用程序控制规则集。

最佳实践条件是在"测试"模式中运行全部规则集一段时间,然后再切换到"生产"模式。由于不能全盘预测规则的全部可能详细信息,这种做法可以减少会发生的潜在问题。

请参见第446页的"更改应用程序控制规则集的模式"。

### 关于应用程序控制规则集和规则

规则集包括规则及其条件。规则是一组应用于一项或多项指定进程的条件和操作。 最佳实践条件是创建一个规则集,包括允许、禁止和监控一项指定任务的所有操 作。按照此条件进行,有助于规则有条不紊。例如,假设您要禁止写入全部可移动 磁盘的尝试,并且要禁止应用程序篡改特定应用程序。若要达成这些目标,您应该 创建两个不同的规则集。您不应该以一个规则集创建达成这些目标的全部必要规 则。

您可以将规则应用于一个或多个应用程序,以定义监控的应用程序。规则包括条件。这些条件会监控在规则中,针对指定操作定义的一个或多个应用程序。条件定 义您允许或不允许应用程序进行的条目。条件也包括观察到条件中指定的操作时要 采取的操作。

**注意**:请注意,操作一律应用于规则中定义的进程,而不应用于条件中定义的进程。

### 关于应用程序控制规则属性

您可以配置规则的下列属性:

■ 名称

- 描述(可选)
- 启用或禁用规则
- 应应用规则的应用程序列表
- 不应应用规则的应用程序列表(可选)

### 关于应用程序控制规则条件

条件是允许或拒绝应用程序的操作。

表 33-1说明可针对规则配置的应用程序控制规则条件。

### 表 33-1 规则条件的类型

条件	说明
注册表访问尝试	允许或禁止访问客户端计算机的注册表设置。
	您可以允许或禁止访问指定的注册表项、值和数据。
文件和文件夹访问尝试	允许或禁止访问客户端计算机上指定的文件或文件夹。
	您可以将文件和文件夹的监控限制在特定的驱动器类型。
启动进程尝试	允许或禁止在客户端计算机启动进程。
终止进程尝试	允许或禁止在客户端计算机中终止进程。
	例如,您可能需要阻止特定的应用程序被停止。此条件会搜 索尝试终止指定应用程序的应用程序。
	<b>注意</b> :此条件会防止其他应用程序或过程终止进程。这不会防止以退出应用程序的正常方式终止应用程序,例如单击"文件"菜单的"退出"。
加载 DLL 尝试	允许或禁止在客户端计算机加载 DLL。
	您可以定义要防止或允许加载到应用程序中的 DLL 文件。您可以使用特定的文件名、通配符、指纹列表和正则表达式。您也可以将 DLL 的监控限制在从特定驱动器类型启动的 DLL。

### 关于应用程序控制规则条件属性

您可以配置规则条件的下列属性:

- 名称
- 描述(可选)
- 启用或禁用规则条件
- 应针对条件监控的计算机实体列表

■ 应排除在针对条件监控以外的计算机实体列表(可选)

### 关于应用程序控制规则条件操作

您可以配置匹配条件时将采取的某些操作。 出现应用程序尝试进行的状况时,可配置下列操作:

- 继续处理其他规则。
- 允许应用程序访问实体。
- 禁止应用程序访问实体。
- 终止应用程序进程。

例如,您可以配置一组操作,在进程尝试读取受监控实体时运行。您可以配置不同 组的操作,在相同进程尝试创建、删除或写入受监控实体时执行。您可以针对任何 所需数量的进程分别配置操作。

您也可以配置应用程序控制记录尝试状况,并且在发生尝试状况时向用户显示自定 义消息。

**警告:**务必谨慎使用"终止进程"操作,因为在规则中使用此操作,可能不会产生预期效果。这会终止执行已配置操作的进程,而非用户当前启动的进程。

例如,假设您要在任何进程启动 Winword.exe 时即终止 Winword.exe。您决定创 建规则,并且以"启动进程尝试"条件和"终止进程"操作配置此规则。您将条件 应用于 Winword.exe,并且将规则应用于全部的进程。某人可能预期此规则终止 Winword.exe,但是包括此配置的规则不会生成如此的效果。如果您尝试从 Windows 资源管理器启动 Winword.exe,包括此配置的规则会终止 Explorer.exe,而非 Winword.exe。

### 关于设备控制

使用设备控制可管理外围设备对客户端计算机的访问。通过设备控制,管理员可以 对能够访问计算机的设备进行更多控制。您可以构建被禁止访问计算机的设备列表 和允许访问计算机的设备列表。虽然设备可能实际连接到计算机,但仍可拒绝此设 备访问该计算机。您可以禁止或允许 USB、红外线、FireWire 和 SCSI 设备,以及 串行端口和并行端口。您也可以允许将其他设备类型(例如 USB硬盘驱动器)排除 在禁止范围之外。您也可以选择使用 Windows GUID 或设备 ID 定义设备控制。您 可以通过构建硬件设备列表来实现设备控制。

表33-2列出了端口和设备配置组合示例,以及每个组合对尝试访问客户端计算机的 设备产生的影响。

配置	结果
端口禁止+设备排除	设备可使用
端口排除+设备禁止	设备不可用
	注意:不要禁止键盘。

表 33-2 端口和设备配置组合

例如,您可以决定禁止所有端口,但不能禁止USB鼠标,以便其可连接到客户端计 算机。在此情形下,虽然USB鼠标使用的端口被禁止,鼠标却仍可以在客户端计算 机上使用。

### 关于使用应用程序与设备控制策略

创建与编辑"应用程序与设备控制策略"的方式与创建和修改其他类型 Symantec Endpoint Protection 策略的方式相同。您可以分配、撤回、替换、复制、导出、导入或删除应用程序与设备控制策略。

如果默认的应用程序与设备控制策略未提供您需要的防护,另外仍有下列选择:

- 编辑默认策略。
- 创建自定义策略。

请参见第 439 页的"配置应用程序与设备控制策略的应用程序控制"。

管理服务器上默认有应用程序与设备控制策略。不过,客户端上默认禁用应用程序 与设备控制策略驱动程序。若要启用驱动程序,必须启用现有规则,或在策略中新 建并启用新规则。将策略下载至客户端计算机后,系统会发出通知请求用户重新启 动客户端计算机。用户必须重新启动客户端,才能启用策略以保护客户端计算机。

如果您撤回或禁用应用程序与设备控制策略,则会禁用该驱动程序,从而客户端不 会受到保护。若要再次启用防护,用户必须再次重新启动客户端计算机。

警告:应用程序与设备控制策略是一个功能强大的工具,使用它可为您的环境创建 自定义的强制执行策略。不过,配置错误可能会禁用计算机或服务器。实现应用程 序与设备控制策略时,客户端计算机可能会失败,或者与 Symantec Endpoint Protection Manager 的通信可能被禁止。如果发生此类故障,可能不能从远程配置 客户端计算机。您可能只能从本地还原客户端计算机。Symantec 建议您在部署策 略之前,先以测试模式使用策略。然后,就可以从控制日志检查有无错误。

应用程序与设备控制事件记录在客户端控制日志中。在控制台上,您可以从应用程 序控制日志和设备控制日志中查看这些信息。 您通常可将一个策略分配至安全网络中的多个组。如果对特定位置有特定要求,您 可以创建一个非共享、位置限定的策略。

请参见第 282 页的"关于策略"。

### 启用默认的应用程序控制规则集

应用程序与设备控制策略的应用程序控制部分由应用程序控制规则集组成。每一个 应用程序控制规则集都由一个或多个规则组成。默认应用程序控制规则集随Symantec Endpoint Protection Manager 一起安装。默认的规则集在安装时处于禁用状态。

**注意**:请不要编辑默认的应用程序控制规则集。如果默认规则集和控制设置不能满 足需要,可改为创建新的应用程序控制规则集来满足需要。

如果要使用应用程序与设备控制策略中的默认规则集,必须启用它们。

#### 启用默认的应用程序控制规则集

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下,单击"应用程序与设备控制"。
- 3 在"应用程序与设备控制策略"窗格中,单击您要向其添加默认应用程序控制规则集的策略。
- 4 在"任务"下,选择"编辑策略"。
- 5 在"应用程序与设备控制策略"窗格中,单击"应用程序控制"。
- 6 若要查看默认应用程序控制规则集中的设置,请单击"规则集"下的名称,然 后单击"编辑"。

一定不要做任何更改。

- 7 查看完规则及其条件设置后,请单击"取消"。
- 8 选中您要启用的每个规则集旁边的复选框。
- 9 单击"确定"。

### 创建应用程序与设备控制策略

您可以创建新的应用程序与设备控制策略。创建新策略之后,您可以创建一或多个 应用程序控制规则集,或硬件设备控制列表,或两者都创建。

您不应该创建只包括设备控制或应用程序控制的策略。如果您要实现应用程序控制 和设备控制,则"应用程序与设备控制策略"必须同时包括两者。您一次只能为组 或位置分配一个"应用程序与设备控制策略"。

### 创建和分配应用程序与设备控制策略

- 1 在 Symantec Endpoint Protection Manager 控制台中, 单击"策略"。
- 2 在"查看策略"下,单击"应用程序与设备控制"。
- 3 在"任务"之下,单击"添加应用程序和设备控制策略"。
- 4 在"概述"窗格的"策略名称"字段中,键入新应用程序及设备控制策略的名称。

新策略的默认名称为"新应用程序及设备控制策略"。

- 5 在"描述"字段中,键入新策略的描述。 此为选填信息;仅供参考之用。
- 6 如果不需要立即实现策略,请取消选中"启用此策略"。 新策略默认为启用。
- 7 单击"确定"。

### 配置应用程序与设备控制策略的应用程序控制

若要配置应用程序控制,您需要完成下列任务:

- 创建新应用程序控制规则集。
- 将一项或多项规则添加到规则集。
- 将一项或多项条件添加到规则。
- 配置匹配条件时要采取的操作。
- 将条件应用于实体,
- 或者排除让条件应用于实体。
- 将规则应用于进程,
- 或者排除让规则应用于进程。
- 启用规则。
- 启用规则集。

### 创建新的应用程序控制规则集并向该集添加新规则

一个新的应用程序规则集包含一个或多个由管理员定义的规则。每个规则集和每个规则都具有属性。每个规则还可以包含一项或多项条件,用以监视应用程序及其对 指定的文件、文件夹、注册表项和进程的访问。 您可以创建多个规则并将这些规则添加到单个应用程序控制规则集中。可创建任意 数量的规则和规则集来实现所需的防护。可以根据需要从规则列表中删除规则以及 更改规则在规则集层次结构中的位置。还可以启用和禁用规则集或集内的各个规 则。

规则的列出顺序对应用程序控制的正常工作很重要。应用程序控制规则在工作原理 上与大多数基于网络的防火墙规则相似,因为两者都使用首个规则匹配功能。当有 多个规则中的条件得到满足时,除非为最上方的规则配置的操作为"继续处理其他 规则",否则仅应用最上方的规则。

配置规则时应考虑规则的顺序及其条件,以免出现意想不到的结果。请考虑下面的 情况:假如一位管理员希望防止所有用户在USB驱动器上移动、复制和创建文件。 此管理员已经有一个规则,此规则的条件是允许对名为 Test.doc 的文件进行写访 问。管理员向这个现有的规则集添加第二个条件,以禁止所有 USB驱动器。在这种 情况中,用户仍然能够在 USB 驱动器上创建和修改 Test.doc 文件。由于在此规则 中允许对 Test.doc 进行写访问的条件在禁止对 USB驱动器进行写访问的条件之前, 因此在列表中禁止对 USB驱动器进行写访问的条件前面的条件得到满足时,不会处 理禁止对 USB 驱动器进行写访问的条件。

您可以查看默认规则集的结构,看看它们是如何构造的。

警告:只有高级管理员才应创建应用程序控制规则集。

如果应用程序与控制策略中使用的规则集中出现配置错误,可能会造成计算机或服务器无法运行。客户端计算机可能会出故障,或者其与 Symantec Endpoint Protection Manager 的通信可能受阻。

#### 创建新规则集并向其添加规则

- 创建一个新的应用程序与设备控制策略。
   请参见第 284 页的"添加共享策略"。
- 2 在"应用程序控制"窗格中,单击"添加"。
- 3 在"添加应用程序控制规则集"对话框中,如果不想将有关此规则集的事件记入日志,请取消选中"启用记录"。 记录在默认情况下是启用的。
- 4 在"规则集名称"文本框中,更改此规则集的默认名称。
- 5 在"说明"字段中, 键入说明。
- 6 在"规则名称"文本框中更改规则的默认名称,然后键入对规则的说明。
- 7 如果不想立即启用此新规则,请取消选中"启用此规则"。

- 8 若要添加另一规则,请单击"添加",再单击"添加规则"。
- 9 单击"确定"。

创建规则集和规则后,应定义该规则应应用到的应用程序。如有必要,还应定 义应排除在该规则应用范围之外的任何应用程序。然后,就可以向该规则添加 条件,并配置在满足这些条件时要采取的操作。

### 将条件添加到规则

将规则应用于至少一项应用程序后,您可以添加或配置规则的条件。条件具有属性 和操作。条件的属性会指定条件搜索的条目。其操作会定义匹配条件时发生的状况。

### 将条件添加到规则

- 1 在"应用程序控制"窗格中,单击已创建的规则集,然后单击"编辑"。
- 2 在"编辑应用程序控制规则集"对话框中,单击要将条件添加到的规则。
- 3 在"条件"列表下,单击"添加",然后单击"添加条件"。
- 4 选择下列其中一项条件:
  - 注册表访问尝试
  - 文件和文件夹访问尝试
  - 启动进程尝试
  - 终止进程尝试
  - 加载 DLL 尝试

如果需要,您可以在规则中添加、配置和删除条件。

### 配置规则的条件属性

条件属性包括名称、说明以及启用或禁用条件。此外,条件属性包括对实体应用条件,也可以包括将某些实体排除在条件应用范围之外。

**注意**:将条件应用于特定文件夹中全部的实体时,最佳方法是使用 folder\_name\\* 或 folder\_name\\*\\*。一个星号即包括指定文件夹中的全部文件和文件夹。使用 folder\_name\\*\\*可包括指定文件夹中所的各个文件和文件夹,以及各个子文件夹中 的各个文件和文件夹。

#### 配置条件属性

- 1 在"编辑应用程序控制规则集"对话框中,单击要应用的条件。
- 2 必要时,可以更改"名称"文本框中的默认名称,也可以选择添加说明。

- 3 如果您要立即启用此条件,请选中"启用此条件"。
- 4 在"应用于下列实体"(其中 <实体> 表示进程、注册表项、文件和文件夹、 DLL 等)的右侧,单击"添加"。
- 5 在"添加实体定义"对话框中,配置下列其中一组选项:
  - 对于"注册表访问尝试",键人注册表项名称及其值名和数据。单击"使用通配符匹配(支持\*和?)"或"使用正则表达式匹配"。
  - 对于"文件和文件夹访问尝试",键入文件或文件夹的名称。
    单击"使用通配符匹配(支持\*和?)"或"使用正则表达式匹配"。
    如果有需要,选中特定驱动器类型来匹配在上面运行的文件和文件夹。
    如果有需要,选中"只匹配以下设备 ID 类型上的文件",然后在文本字段
    中键入设备 ID 类型,或单击"选择",从"设备选择"对话框的列表中选择设备 ID 类型,从而仅匹配在该 ID 类型的设备上运行的进程。
  - 对于"启动进程尝试",键入进程名称。
    单击"使用通配符匹配(支持\*和?)"或"使用正则表达式匹配"。
    如果有需要,选中特定驱动器类型来匹配在上面运行的进程。
    如果有需要,选中"只匹配在以下设备 ID 类型上运行的进程",然后在文本字段中键入设备 ID 类型,或单击"选择",从"设备选择"对话框的列表中选择设备 ID 类型,从而仅匹配在该 ID 类型的设备上运行的进程。
    如果有需要,选中"选项",以根据文件指纹匹配进程,并且只匹配具有指定参数的进程。您可以选择要完全匹配参数,或使用正则表达式匹配。
  - 对于"终止进程尝试"或"加载 DLL 尝试",键入进程名称。
    单击"使用通配符匹配(支持\*和?)"或"使用正则表达式匹配"。
    如果有需要,选中特定驱动器类型来匹配在上面运行的进程。
    如果有需要,选中"只匹配在以下设备 ID 类型上运行的进程",然后在文本字段中键入设备 ID 类型,或单击"选择",从"设备选择"对话框的列表中选择设备 ID 类型,从而仅匹配在该 ID 类型的设备上运行的进程。
    果有需要,单击"选项",以根据文件指纹匹配进程。
- 6 单击"确定"。
- 7 在"请勿将此规则应用于下列进程"窗格的右侧,单击"添加",然后根据需要重复此配置。

用于排除的选项与用于包括的选项相同。

- 8 单击适当的控件来进行选择,并在文本框中输入所有必要信息。
- 9 单击"确定"。

设置条件的属性后,您需要配置匹配条件时采取的操作。

### 配置匹配条件时要采取的操作

下列操作可供全部的条件使用:

继续处理其他规则	允许您只记录事件,然后继续处理列表中其他的规则
	对于其他所有操作,在匹配第一项条件后,客户端计算 机会停止处理规则。
允许访问	允许操作继续进行
禁止访问	阻止操作进行
终止进程	删除进行请求的应用程序

**注意:**最佳实践条件是使用"拒绝访问"操作防止条件发生,而非使用"终止进程"操作。只有在高级配置中,才应该使用"终止进程"操作。

#### 配置匹配条件时要采取的操作

- 1 在"编辑应用程序控制规则集"对话框中,单击要配置操作的条件。
- 2 在"操作"选项卡上,运行下列其中一项操作:
  - 对于"启动进程尝试"条件和"终止进程尝试"条件,请单击下列其中一 个选项:继续处理其他规则、允许访问、拒绝访问或终止进程。
  - 对于 "DLL访问尝试"条件,单击下列其中一个选项:继续处理其他规则、 允许访问、拒绝访问或终止进程。
  - 对于"注册表访问尝试"条件和"文件和文件夹访问尝试"条件,您可以 配置两组操作。其中一组会在出现读取尝试时应用,另一组会在出现创建、 删除或写入尝试时应用。 在"读取尝试"下,单击下列其中一个选项:继续处理其他规则、允许访问、拒绝访问或终止进程。
- 3 如果需要,选中"启用记录",然后选择要分配至所记录实体的严重性等级。
- 4 必要时,选中"通知用户",然后键入要让用户看见的文本属性。
- 5 重复步骤2至4,针对"创建、删除或写入尝试"配置相同的选项。
- 6 单击"确定"。

### 将规则应用于特定应用程序以及将应用程序排除在规则的应用范围外

您可以将规则应用于应用程序,也可以将应用程序排除在规则的操作范围之外。您 可以指定一份包含规则应用至的应用程序的列表(包括)。您还可以指定另一份包 含规则不应用至的应用程序的列表(排除)。若要将规则应用于特定应用程序,您可以在"将此规则应用于下列进程"文本字段中定义该应用程序。 如果您要将规则应用于一组特定应用程序以外的其他所有应用程序,您可以使用下列设置:

- 在"将此规则应用于下列进程"文本框中,针对所有进程定义通配符(\*)。
- 在"请勿将此规则应用于下列进程"文本框中,列出需要排除的应用程序。
   您可以在各份列表中定义所需数量的应用程序。

**注意**: 各项规则都必须至少在"应用此规则至下列进程"文本框中列有一项应用程 序。

将应用程序添加到规则时,您可以使用下列方式指定应用程序:

- 进程名称
- ∎ 通配符
- 正则表达式
- 文件指纹
- 从中启动应用程序的驱动器的类型。
- 设备 ID

#### 将规则应用到特定应用程序

- 1 在"编辑应用程序控制规则集"对话框中,单击要应用的规则。
- 2 如果您要将一个应用程序配置为规则应用的对象,则在"将此规则应用于下列 进程"右侧,单击"添加"。
- 3 在"添加进程定义"对话框中,配置以下项:
  - 键入要求其匹配此规则的应用程序的名称。
  - 单击"使用通配符匹配(支持\*和?)"或"使用正则表达式比对",以匹配 名称。
  - 如果有需要,选中对其上进程进行匹配的特定驱动器类型。
  - 如果有需要,选中"只匹配在以下设备 ID 类型上运行的进程",然后在文本字段中键入设备 ID 类型,或单击"选择",从"设备选择"对话框的列表中选择设备 ID 类型,从而仅匹配在该 ID 类型的设备上运行的进程。
  - 如果有需要,可选中"选项",以便根据文件指纹匹配进程,以及只匹配 具有指定参数的进程。您可以选择要完全匹配参数,或使用正则表达式匹 配。

4 单击"确定"。

您可以重复步骤2至4以添加所需数量的应用程序。

5 如果您要配置一个或多个应用程序排除在规则应用范围之外,则在"请勿将此规则应用于下列进程"右侧,单击"添加"。

如果需要,可重复此配置过程排除多个应用程序。将规则应用于特定应用程序 时,如果您定义要排除的应用程序,也会出现相同的选项。

6 定义应用程序完毕时,单击"确定"。

### 更改应用程序控制规则集的应用顺序

您可以控制应用程序控制规则集的应用顺序。您也可以控制规则集内个别规则的应用顺序。

### 更改应用程序控制规则集的应用顺序

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"窗格中,单击"应用程序与设备控制"。
- 3 单击要编辑的策略。
- 4 在"任务"下,选择"编辑策略"。
- 5 单击"应用程序控制"。
- 6 单击要移动的应用程序控制规则集。
- 7 单击"上移"或"下移",更改其在列表中的优先级。
- 8 针对要重新安排优先级的各个规则集,重复前两项步骤。
- 9 单击"确定"。

### 在应用程序与设备控制策略中禁用应用程序控制规则集和个别规则

您可能需要在不撤回或删除整个"应用程序与设备控制策略"的情况下,禁用其中 特定的应用程序控制规则集。

#### 在应用程序与设备控制策略中禁用应用程序控制规则集

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下,单击"应用程序与设备控制"。
- 3 单击要禁用其中规则集的策略。
- 4 在"任务"下,选择"编辑策略"。
- 5 单击"应用程序控制"。

- 6 针对要禁用的规则集,取消选中旁边的复选框。
- 7 单击"确定"。

您现在已经禁用一个规则集,并没有禁用整个策略。

### 禁用应用程序与设备控制策略中的个别规则

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下,单击"应用程序与设备控制"。
- 3 单击要禁用其中规则的策略。
- 4 在"任务"下,选择"编辑策略"。
- 5 单击"应用程序控制"。
- 6 单击要禁用其中规则的规则集,然后单击"编辑"。
- 7 在"规则"下的规则列表中,单击要禁用的规则。
- 8 在"属性"选项卡上,取消选中"启用此规则"。
- 9 在"编辑应用程序控制规则集"对话框中,单击"确定"。
- 10 单击"确定"。

您现在已经禁用一个子规则,并没有禁用整个策略或规则集。

### 更改应用程序控制规则集的模式

第一次创建应用程序控制规则集时,可以在"测试"模式下创建。测试策略内的规则集后,可以将模式更改为"生产"模式。

#### 更改应用程序控制规则集的模式

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下,单击"应用程序与设备控制"。
- 3 单击包括所需更改应用程序控制规则集的策略。
- 4 单击"编辑策略"。
- 5 单击"应用程序控制"。
- 6 单击要更改的规则集。
- 7 在"测试/正式"下,单击对应的下拉列表箭头显示模式列表。
- 8 单击新模式。
- 9 单击"确定"。

### 为应用程序与设备控制策略配置设备控制

使用设备控制可管理硬件设备。您可以随时修改此列表。 请参见第 449 页的"关于硬件设备"。

### 添加设备控制

- 1 在"应用程序与设备控制策略"窗格中,单击"设备控制"。
- 2 在"禁止的设备"下,单击"添加"。
- 3 查看硬件设备列表,然后单击要禁止其访问客户端计算机的所有设备。
- 4 单击"确定"。
- 5 在"不禁止的设备"下,单击"添加"。
- 6 查看硬件设备列表,然后单击要将其排除在禁止访问客户端计算机范围之外的 所有设备。
- 7 如果不想将设备控制信息记入日志,请取消选中"记录禁止的设备"。 默认情况下会将这些信息记入日志。
- 8 如果要通知用户,请选中"当设备被禁止时提示用户"。 如果您启用了通知,请单击"指定消息文本",然后键入您希望用户看到的文本。
- 9 单击"确定"。

448 | 配置应用程序与设备控制

为应用程序与设备控制策略配置设备控制

# 34

## 自定义应用程序与设备控 制策略

本章节包括下列主题:

- 关于硬件设备
- 获取类 ID 或设备 ID
- 将硬件设备添加至硬件设备列表
- 编辑硬件设备列表中的硬件设备
- 关于授权使用应用程序、补丁程序和实用程序
- 创建及导入文件指纹列表
- 关于系统锁定
- 设置系统锁定

### 关于硬件设备

可以使用默认的硬件设备列表将供应商特定的设备添加至"应用程序与设备控制策略"。使用硬件设备列表,您就不必在每次从规则添加设备时重新键入设备。

有两个数值用来标识硬件设备:设备 ID 与类 ID。您可以使用这两个值中的任意一个来标识"硬件设备"列表中的设备。

Symantec Endpoint Protection Manager 控制台包括必要时可禁止的设备列表以及可排除在禁止范围之外的设备列表。管理员可以在列表中添加设备、删除设备或编辑设备。

### 注意:您既不能编辑默认设备,也不能删除默认设备。

#### 

### 关于类 ID

类 ID 是指 Windows GUID。每种设备类型都有与之关联的类和 ClassGuid。 ClassGuid 是一个十六进制值,其格式如下:

{0000000-0000-0000-0000-000000000000}}

### 关于设备 ID

设备 ID 是设备专有的 ID。设备可以具有特定的设备 ID,也可以具有更为通用的 ID。例如,您可以指定使用同一个设备 ID 的所有 USB 设备,也可以选择一个特定 的可移动 USB 磁盘驱动器。要添加设备时您必须使用设备 ID。

下面是一个设备 ID 示例:

{IDE\CDROMHL-DT-ST\_RW/DVD\_GCC-4242N\_\_\_\_\_0201\_\_\_\_ \5&3CCF215&0&0.0.0}

### 获取类 ID 或设备 ID

可以使用 Symantec DevViewer 工具获取类 ID 或设备 ID。还可以使用 Windows 设备管理器获取类 ID。

### 使用 DevViewer 工具获取类 ID 或设备 ID

- 1 在产品的第3张光盘上,找到\TOOLS\NOSUPPORT\DEVVIEWER 目录,然 后将 DevViewer.exe 工具下载到客户端计算机。
- 2 在客户端计算机上,运行 DevViewer.exe。
- 3 展开"设备"树并找到需要其设备 ID 或 GUID 的设备。
- 4 在右侧窗格中,右键单击设备 ID (以[设备 ID] 开头),然后单击"复制设备 ID"。
- 5 单击"退出"。
- 6 在管理服务器上,将设备 ID 粘贴到硬件设备列表中。

### 从控制面板获取设备 ID

- 1 在 Windows 任务栏上, 单击"开始" > "设置" > "控制面板" > "系统"。
- 2 在"硬件"选项卡上,单击"设备管理器"。
- 3 在"设备管理器"列表中,双击相应设备。
- 4 在该设备的"属性"对话框的"详细信息"选项卡中,选择"设备 ID"。 默认情况下,设备 ID 是第一个显示的值。

- 5 按 Ctrl+C 复制 ID 字符串。
- 6 单击"确定"或"取消"。

请参见第 451 页的"将硬件设备添加至硬件设备列表"。

### 将硬件设备添加至硬件设备列表

在获取了某个硬件设备的类 ID 或设备 ID 之后,您即可以将该硬件设备添加至默认的硬件设备列表。随后,您可以从"应用程序与设备控制策略"的设备控制部分访问此默认列表。

### 将硬件设备添加至硬件设备列表

- 1 在控制台中,单击"策略"。
- 2 在"策略组件"下,单击"硬件设备"。
- 3 在"任务"下,单击"添加硬件设备"。
- 4 输入要添加的设备的名称。

根据惯例,类 ID 和设备 ID 都用大括号括起来。

- 5 选择"类ID"或"设备ID",然后粘贴从Windows设备管理器或DevViewer 工具复制的ID。
- 6 可以使用通配符来定义一组设备 ID。例如,可以使用以下字符串: \*IDE\CDROM\*。

请参见第 450 页的"获取类 ID 或设备 ID"。

7 单击"确定"。

### 编辑硬件设备列表中的硬件设备

您可以编辑任何添加到列表中的硬件设备。列出的默认设备不能加以编辑。

#### 编辑硬件设备列表中的硬件设备

- 1 在控制台中,单击"策略"。
- 2 在"策略组件"下,单击"硬件设备"。
- 3 在硬件设备列表中,单击您要编辑的硬件设备。
- 4 单击"编辑硬件设备"。
- 5 编辑设备名称、类 ID 或设备 ID。

### 6 单击"确定"。

更新后的设备信息会显示在"标识"列表中。

### 关于授权使用应用程序、补丁程序和实用程序

Symantec Endpoint Protection Manager 可让您保护客户端计算机免于受未批准的 应用程序攻击。保护方式有两种。首先,您可以使用文件指纹来识别可在客户端计 算机上运行的已批准应用程序、补丁程序和实用程序。接着,您可以决定当未批准 的应用程序尝试访问客户端计算机时要采取的操作。如果启用系统锁定,您可以将 Symantec Endpoint Protection Manager 配置为仅记录未批准的应用程序,或配置 为使用系统锁定保护受未经许可程序攻击的客户端计算机。

若要使用系统锁定,请先为您的环境中每种类型的客户端创建文件指纹列表。文件 指纹列表是针对该客户端计算机批准的应用程序列表。然后,将每个文件指纹添加 到 Symantec Endpoint Protection Manager 的文件指纹列表。最后,再配置未批 准的应用程序尝试访问该计算机时要采取的操作。

例如,为您的环境中每种类型的客户端创建文件指纹列表。假设您的环境中有 Windows Vista 32 位、Windows Vista 64 位以及 Windows XP SP2 客户端。对环 境中存在的这三种客户端类型的每一种类型映像运行 Checksum.exe 文件。 Checksum.exe 会为各客户端类型的所有应用程序生成文件指纹,并将其放入文件 指纹列表中。在此例中,您最终会得到三个文件指纹:每个映像一个。

接下来,使用 Symantec Endpoint Protection 创建文件指纹列表,将您生成的三个 文件指纹中的每一个添加到该列表:每个客户端类型一个文件指纹列表。然后,您 会定义未批准的应用程序尝试访问客户端计算机时,Symantec Endpoint Protection 要采取什么操作。您可以禁用系统锁定并允许应用程序访问。您可以选择仅记录未 批准的应用程序。为得到最大的保护,您可以在未授权的应用程序正尝试访问的客 户端计算机上启用系统锁定。

### 创建及导入文件指纹列表

客户端计算机映像的文件指纹列表包括该客户端计算机中各应用程序的校验和列表,以及这些应用程序的完整文件路径。您可以检查各个映像是否包括批准供您公司使用的所有可执行文件。若要创建文件指纹列表,请使用随 Symantec Endpoint Protection 安装于客户端计算机上的实用程序 Checksum.exe。可以对您的环境中的各个计算机映像运行本命令,以创建其文件指纹列表。文件 Checksum.exe 位于下列位置:

### C:\Program Files\Symantec\Symantec Endpoint Protection

您可以从命令提示运行这个工具。Checksum.exe 会创建一个文本文件,其中包括该计算机上所有可执行文件列表及其对应校验和。

您可以使用 Symantec Endpoint Protection Manager 将各个客户端计算机类型的 文件指纹列表导入至主文件指纹列表中。您可以使用 Symantec Endpoint Protection Manager 来管理文件指纹列表。文件指纹列表包括所有客户端计算机的已批准文 件。您也可以为您要批准的各个文件添加文件指纹。

### 创建文件指纹列表

您可以使用 Checksum.exe 来创建文件指纹列表。文件指纹列表会对各个文件及驻 留在客户端计算机映像中的对应校验和进行命名。此工具随客户端上的 Symantec Endpoint Protection 一起提供。

### 创建文件指纹列表

- **1** 转至要为其创建文件指纹列表的映像所在的计算机。计算机必须已经安装 Symantec Endpoint Protection 客户端软件。
- 2 打开命令提示窗口。
- 3 导航至包含 Checksum.exe 文件的目录。默认情况下,该文件位于以下位置:

C:\Program Files\Symantec\Symantec Endpoint Protection

4 键入以下命令:

checksum.exe *outputfile* <**驱动器**>

其中的 outputfile 是文本文件名称,包括指定驱动器上所有可执行文件的校验和。输出文件为文本文件 (outputfile.txt)。

您可以使用下列语法示例:

checksum.exe cdrive.txt c:\

此命令会创建名称为 cdrive.txt 的文件。文件将包括在其运行的客户端计算机 C 驱动器中找到的所有可执行文件和 DLL 的校验和和文件路径。

### Checksum.exe 输出示例

下列为在计算机映像上运行的 Checksum.exe 输出文件的示例。各行格式为 checksum\_of\_the\_file 空格 full\_pathname\_of\_the\_exe\_or\_DLL。

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll
77e4ff0b73bc0aeaaf39bf0c8104231f c:\dell\pnp\m\co\HSF_UNXT.sys
f59ed5a43b988a18ef582bb07b2327a7 c:\dell\pnp\m\co\HSF_DF.sys
60e1604729a15ef4a3b05f298427b3b1 c:\dell\pnp\m\co\HSF_DF.sys
4f3ef8d2183f927300ac864d63dd1532 c:\dell\pnp\m\co\HXFSetup.exe
dcd15d648779f59808b50f1a9cc3698d c:\dell\pnp\m\co\MDMXSDK.sys
0a7782b5f8bf65d12e50f506cad6d840 c:\dell\pnp\mgmt\drac2wdm.sys
9a6d7bb226861f6e9b151d22b977750d c:\dell\pnp\mgmt\racser.sys
d97e4c330e3c940ee42f6a95aec41147 c:\dell\pnp\n\bc\b57xp32.sys
```

### 编辑文件指纹列表

您无法直接编辑现有的文件指纹列表。首先,您可以使用另一个计算机映像,运行 Checksum.exe 创建新的文件指纹列表。然后即可将 Symantec Endpoint Protection Manager 的现有文件指纹列表与客户端映像的新文件指纹列表合并。

### 编辑文件指纹列表

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下方,展开"策略组件",然后单击"文件指纹列表"。
- 3 在"文件指纹列表"窗格中,在要编辑的指纹列表上单击鼠标右键。
- 4 单击"编辑"。
- 5 在编辑文件指纹向导中,单击"下一步"。
- 6 单击"将指纹文件附加到该文件指纹",将新文件添加到现有的文件,然后单击"下一步"。
- 7 单击"浏览"找出文件,或在文本框中键入文件指纹列表的完整路径。
- 8 单击"下一步"。
- 9 单击"关闭"。
- 10 单击"完成"。

### 将文件指纹列表导入共享策略

您可以用导人文件的方式,将文件指纹列表添加到共享策略。列表必须已经创建。 请参见第 453 页的"创建文件指纹列表"。

### 将文件指纹列表导入共享策略

- **1** 在控制台中,单击"策略"。
- 2 在"查看策略"下方,展开"策略组件",然后单击"文件指纹列表"。
- 3 在"任务"下,单击"添加文件指纹列表"。
- 4 在"欢迎使用添加文件指纹向导"窗格中,单击"下一步"。
- 5 在"新文件指纹的相关信息"面板的"名称"文本框中,键入要添加的指纹列 表名称。
- 6 在"新文件指纹的相关信息"面板的"说明"文本框中,键入要添加的指纹列 表说明。

此步骤是可选的。

- 7 单击"下一步"。
- 8 在"创建文件指纹"面板中,单击"通过导入指纹文件创建文件指纹"。

- 9 单击"下一步"。
- 10 单击"浏览"找出文件,或在文本框中键入文件指纹列表的完整路径。
- 11 单击"下一步"。
- 12 单击"关闭"。
- 13 单击"完成"。

新的列表会出现在右侧的"文件指纹列表"中。

### 合并共享策略中的文件指纹列表

您可以将共享策略中的多个文件指纹列表合并。开始这项任务之前,必须已经添加 要合并的列表。

请参见第454页的"将文件指纹列表导入共享策略"。

#### 合并共享策略中的文件指纹列表

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下方,展开"策略组件",然后单击"文件指纹列表"。
- **3** 在"欢迎使用添加文件指纹向导"窗格中,单击"下一步"。
- 4 在"新文件指纹的相关信息"面板的"名称"文本框中,键入要添加的合并指 纹列表名称。
- 5 在"新文件指纹的相关信息"面板的"说明"文本框中,键入要添加的合并指 纹列表说明。

此步骤是可选的。

- 6 单击"下一步"。
- 7 在"创建文件指纹"面板中,单击"通过组合多个现有文件指纹创建文件指 纹"。

只有在共享策略中已有文件指纹列表时,此选项才可用。

- 8 单击"下一步"。
- 9 选择您要合并的指纹列表。
- 10 单击"下一步"。
- 11 单击"关闭"。

### 12 单击"完成"。

合并的指纹列表会出现在右侧的"文件指纹列表"中。

### 删除文件指纹列表

您可以删除任何不再需要的文件指纹列表。请先确保在组级别不再需要相应的文件指纹列表,然后再将此列表从共享策略中删除。

### 删除文件指纹列表

- 1 在控制台中,单击"策略"。
- 2 在"查看策略"下方,展开"策略组件",然后单击"文件指纹列表"。
- 3 在"文件指纹列表"窗格中,选择您要删除的文件指纹列表。
- 4 在"任务"下方,单击"删除列表"。
- 5 单击"是"确认。

文件指纹列表便会从 Symantec Endpoint Protection Manager 中删除,但仍 会保留在计算机上您先前从其导入列表的位置中。

### 关于系统锁定

系统锁定是一项防护设置,可用来控制可在客户端计算机上运行的应用程序。您可 以创建一个文件指纹列表,其中包含授权在贵公司使用的所有应用程序的校验和及 位置。客户端软件包括 Checksum.exe 工具,此工具可用来创建文件指纹列表。系 统锁定的优点是,无论用户是否连接到网络都能够强制执行它。

使用系统锁定可禁止几乎所有试图运行或自我加载到现有应用程序中的特洛伊木马、间谍软件或恶意软件。例如,您可以防止这些文件加载到 Internet Explorer。系统锁定可确保系统保持在已知且可信的状态。

在客户端计算机上运行的应用程序可能包括下列可执行文件:

- exe
- .com
- .dll
- .0CX

Symantec 建议您在下列阶段实现系统锁定:

获取核准的软件映像	创建软件映像,其中包括用户可以在其计算机上使用 的所有应用程序。使用此映像创建文件指纹列表。
记录未批准的应用程序	启用系统锁定,记录未包括在文件指纹列表中的应用 程序。接下来您可以调整文件指纹,以包括用户所需 的应用程序。在禁止未核准的应用程序之前,您可以 给用户适当的警告。

添加允许的应用程序 添加您希望允许使用的可执行文件(即使这些文件未 包括在文件指纹列表中)。 启用系统锁定 强制执行系统锁定,并禁止未批准的应用程序。

您可以选择定义当用户使用的应用程序受到禁止时将向用户显示的自定义消息。

### 系统锁定先决条件

在启用系统锁定之前,必须先满足下列先决条件:

创建文件指纹列表	您必须先创建包括所允许应用程序的文件指纹列表。 可从用户计算机上定期安装的企业映像创建此列表。 您可在运行客户端的计算机上创建此列表。
添加一个或多个文件指纹列表	创建指纹列表之后,需将它们添加到管理器。
合并文件指纹列表	可以合并多个文件指纹列表。例如,可以对公司里的 不同组使用不同的映像。
按照下列步骤实现系统锁定:	
设置并测试系统锁定	在您禁止未批准的可执行文件之前,可先添加一个或 多个文件指纹列表。添加应始终允许的应用程序,并 将结果记录在"控制"日志中。
检查未批准的应用程序列表	测试系统锁定数天之后,可以查看未批准的应用程序 的列表。此列表会显示组中用户运行的未批准应用程 序。您可以决定是否添加更多应用程序至文件指纹或 允许的列表中。

启用系统锁定

接下来,您可以启用系统锁定,禁止不在文件指纹列 表中的应用程序。

### 设置系统锁定

若要设置系统锁定,请遵照下面包含两个步骤的过程操作:

步骤1,监控客户端计算机运行的应用程序。 在此步骤中,您可以在未批准的应用程序列表中跟踪这些应用程序。未批准的 应用程序列表包括客户端运行,但不在已批准应用程序的文件指纹列表中的应 用程序。客户端不会禁止未批准的应用程序。在禁止这些应用程序之前,您可 以跟踪客户端用于参考的应用程序。您还可以测试是否有任何应用程序出现在 未批准的应用程序列表中。如果运行测试,则状态会指出已运行的时间,以及 是否发生了异常。请在测试模式下长时间运行系统锁定,直到发现客户端计算 机运行哪些未批准的应用程序。然后启用系统锁定。

步骤 2, 启用系统锁定。 在测试模式下长时间运行系统锁定,直到发现了运行哪些未批准的应用程序之 后,请启用下列设置:

批准使用这些不在已批准应用程 将应用程序添加到已批准的应用程序列表,或将它们添 序之列的应用程序 加到您创建文件指纹的映像。

通知用户 您可以通知用户他/她已失去对计算机的访问权限。您 也可以告知用户,指定的应用程序可以在您指出的某个 未来日期使用。然后,您可以在那一天启用系统锁定。

继续记录未批准应用程序的使 无须采取任何操作。 用。

注意:您还可以创建防火墙规则,以允许客户端上已批准的应用程序。

### 设置系统锁定

- 1 在控制台上,单击"客户端"。
- 2 在"查看客户端"下,找出要设置系统锁定的组。
- 3 在"策略"选项卡上,单击"系统锁定"。
- 4 在"用于 <组名称> 的系统锁定"对话框中,单击"步骤1:仅记录未批准应用程序"(如果要在测试模式下启用此防护)。
  此选项会记录客户端当前正在运行的未批准的网络应用程序。
- 5 单击"步骤 2:启用系统锁定"(如果要启用此防护)。此步骤会禁止客户端试 图运行的未批准应用程序。
- 6 在"批准的应用程序"下,选择要用作已批准的可执行文件列表的文件指纹列 表。

请参见第 454 页的"编辑文件指纹列表"。

- 7 如果要添加其他文件指纹列表,请单击"添加",再单击列表名称,然后单击 "确定",以添加其他文件指纹列表。
- 8 对于您希望在客户端禁止前先测试的应用程序,请选中"删除前测试"。
- 9 若要查看未批准的应用程序列表,请单击"查看未批准的应用程序"。

在 "未批准的应用程序"对话框中,审查应用程序。这个列表包括应用程序运 行的时间、计算机的主机名称、客户端的用户名,以及可执行文件的文件名等 信息。 10 确定处理未批准应用程序的方式。

您可以将要允许的应用程序的名称添加到批准的应用程序列表。您可以在下次 创建文件指纹时,将相应可执行文件添加至计算机映像。

- 11 单击"关闭"。
- 12 若要指定始终允许的可执行文件(即使未包括在文件指纹列表中),请在"文件名"列表下单击"添加"。
- **13** 在"添加文件定义"对话框中,指定可执行文件(.exe 或.dll)的完整路径名称。

可以使用常规字符串或正则表达式语法来指定名称。名称可以包括通配符(\* 代表任意字符,?代表单个字符)。名称还可以包括环境变量,例如 %ProgramFiles%(代表 Program Files 目录的位置)或 %windir%(代表 Windows 安装目录的位置)。

- 14 保留"使用通配符匹配(支持\*和?)"的默认选中状态,或者单击"使用正则表达式匹配"(如果您在文件名中改用正则表达式)。
- 15 如果希望仅在文件在特定类型的驱动器上执行时允许该文件,请单击"只匹配 以下驱动器类型上的文件"。

然后取消选中您不希望包含的驱动器类型。默认情况下已选择所有驱动器类型。

- 16 如果要按设备 ID 类型匹配,请选中"只匹配以下设备 ID 类型上的文件",然 后单击"选择"。
- 17 在列表中单击所需的设备,然后单击"确定"。
- 18 单击"确定"。
- **19** 若要在客户端禁止应用程序时在客户端计算机上显示消息,请选中"禁止应用 程序时通知用户"。
- 20 若要写入自定义消息,请单击"通知",键入消息,然后单击"确定"。
- 21 单击"确定"。

460 | 自定义应用程序与设备控制策略 | **设置系统锁定** 





# 配置集中式例外

■ 配置集中式例外策略

462 |

# 35

## 配置集中式例外策略

本章节包括下列主题:

- 关于集中式例外策略
- 配置集中式例外策略
- 配置集中式例外的客户端限制
- 从日志事件创建集中式例外

### 关于集中式例外策略

集中式例外策略包括下列类型扫描的例外:

- 防病毒和防间谍软件扫描
- TruScan 主动型威胁扫描
- 防篡改扫描

**注意**:防病毒和防间谍软件扫描包括所有的自动防护扫描、调度扫描、按需扫描,或用户定义的扫描。

通常,例外是指您希望客户端软件不要扫描的风险或进程。如果在客户端计算机上 使用例外,可能会缩短扫描时间。扫描时间缩短后,客户端计算机的系统性能就会 提高。

对于TruScan主动型威胁扫描,您可能还想让客户端软件检测在默认情况下不会检测的特定进程。您可以创建一个例外以强制进行检测。当检测结果出现在已检测到的进程列表中时,您可以再创建一个例外来指定针对该检测到的进程的操作。

**注意**:对于防病毒和防间谍软件扫描或防篡改,您可以使用集中式例外来指定要排除在扫描范围之外的特定项目。不过,如果是主动型威胁扫描,则可使用集中式例外指定针对检测到的进程执行的操作,或进行强制检测。

创建集中式例外策略时,例外会应用于使用该策略的客户端计算机上该类型的所有 扫描。可以在同一策略中包括所有的例外。

不同于其他策略, Symantec Endpoint Protection Manager 控制台中不包含默认的 集中式例外策略。您必须创建新策略。可以从"策略"页面创建集中式例外策略, 也可以从管理控制台的"客户端"页面创建集中式例外策略。

可以利用管理控制台中的日志,将例外添加到集中式例外策略。您必须先创建集中 式例外策略,然后才能使用该功能来创建例外。

请参见第471页的"从日志事件创建集中式例外"。

### 关于使用集中式例外策略

您可以使用与创建和修改其他类型策略类似的方式,创建和编辑集中式例外策略。 您可以分配、撤消、替换、复制、导出、导入或删除集中式例外策略。

您通常可将一个策略分配至安全网络中的多个组。如果对特定位置有特定要求,您 可以创建一个非共享、位置限定的策略。

若要使用集中式例外策略,您必须熟悉策略配置的基本知识。

请参见第 282 页的"关于策略"。

### 关于防病毒和防间谍软件扫描的集中式例外

您可能想将特定的安全风险排除在防病毒和防间谍软件扫描范围之外。您可能还想 将特定文件、文件夹或文件扩展名排除在扫描范围之外。

将一个安全风险排除在扫描范围之外后,扫描会忽略该风险。您可以将例外配置为 让扫描记录此检测结果。任何一种情况下,客户端软件都不会在检测到指定的安全 风险时通知用户。将某些文件、文件夹或扩展名排除在扫描范围之外后,扫描会忽 略这些文件、文件夹或扩展名。

**注意**:集中式例外适用于所有防病毒和防间谍软件扫描。您不能针对不同的扫描类型创建不同的例外。例如,您可能要创建一个集中式例外以排除特定的文件扩展名。这样,客户端软件就会将此扩展名排除在自动防护扫描及所有管理员定义的扫描与用户定义的扫描之外。管理员定义的扫描与用户定义的扫描包括调度扫描与按需扫描。

### 关于 TruScan 主动型威胁扫描的集中式例外

您可能想将特定进程排除在主动型威胁扫描范围之外。您需要确定要排除的进程可 在安全网络中的客户端计算机上安全运行。若要排除检测到的进程,您必须将相应 检测操作设置为"忽略"。

您还可以通过创建集中式例外来指定不允许的特定进程。若要指定不允许的进程, 您必须将相应检测操作设置为"隔离"或"终止"。

您可以通过创建指定文件名的集中式例外,强制进行主动型威胁检测。当主动型威胁扫描检测到该文件时,客户端会记录此实例。因为文件名并不是唯一的,所以可能会有多个进程使用相同的文件名。您可以使用强制检测帮助您创建例外,以隔离 或终止与该文件关联的进程。

请参见第 424 页的"TruScan 主动型威胁扫描如何与集中式例外配合工作"。

### 关于防篡改的集中式例外

防篡改可保护客户端计算机不受那些篡改 Symantec 进程和内部对象的进程的攻击。 当防篡改检测到一个可能会修改 Symantec 配置设置或 Windows 注册表值的进程 时,就会加以禁止。您可能需要允许应用程序修改 Symantec 设置。您可能想要停 止客户端计算机上特定注册表区域或特定文件的防篡改功能。

在某些情况下,防篡改可能会禁止屏幕读取器或某些其他辅助技术应用程序。您可 以创建集中式例外,以便应用程序可在客户端计算机上运行。

### 关于客户端与集中式例外的交互

管理员定义的例外始终优先于用户定义的例外。在客户端计算机上,用户可以查看 管理员定义的例外列表,但是不能更改它们。用户还可以查看其创建的任何例外。

默认情况下,客户端计算机上的用户拥有有限的集中式例外配置权限。

默认情况下,用户受到下列限制:

- 用户不能创建例外来强制进行主动型威胁扫描的检测。用户不能从检测到的进程列表中进行选择来创建主动型威胁扫描的例外。但是,用户可以在客户端计算机上选择文件来创建主动型威胁扫描的例外。
- 用户不能创建防篡改的任何例外。

您可以限制客户端计算机上的用户,让他们不能创建防病毒和防间谍软件扫描或主 动型威胁扫描的例外。

请参见第 470 页的"配置集中式例外的客户端限制"。

### 配置集中式例外策略

配置集中式例外策略的方式与配置其他类型策略的方式类似。

可以单击"帮助"获取以下步骤中所用选项的详细信息。

#### 配置集中式例外策略

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 在"集中式例外"下,单击"添加",然后执行下列任何操作:
  - 单击"安全风险例外",然后添加想要在策略中包括的安全风险例外。 请参见第 466 页的"配置防病毒和防间谍软件扫描的集中式例外"。
  - 单击"TruScan 主动型威胁扫描例外",然后添加要在策略中包含的主动型威胁扫描例外。
     请参见第 468 页的"配置 TruScan 主动型威胁扫描的集中式例外"。
  - 单击"防篡改例外",然后添加想要纳入该策略中的防篡改扫描例外。 请参见第 470 页的"配置防篡改的集中式例外"。
- 3 重复步骤2添加更多例外。
- 4 完成此策略的配置后,单击"确定"。

### 配置防病毒和防间谍软件扫描的集中式例外

您可以创建已知安全风险、文件、文件夹或扩展名的例外。这些例外应用于使用该 策略的客户端计算机上运行的所有防病毒和防间谍软件扫描。

有关以下步骤中所使用选项的详细信息,您可以单击"帮助"。

### 配置防病毒和防间谍软件扫描的集中式例外

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 在"集中式例外"下,单击"添加">"安全风险例外",然后执行下列操作 之一:
  - 单击"已知风险",然后配置例外。 请参见第 467 页的"配置已知安全风险的集中式例外"。
  - 单击"文件",然后配置例外。
     请参见第 467 页的"配置文件的集中式例外"。
  - 单击"文件夹",然后配置例外。
     请参见第 467 页的"配置文件夹的集中式例外"。
  - 单击"扩展名",然后配置例外。 请参见第 468 页的"配置文件扩展名的集中式例外"。
- 3 单击"确定"。
- 4 完成此策略的配置后,单击"确定"。

### 配置已知安全风险的集中式例外

客户端软件检测到的安全风险会显示于"已知安全风险例外"对话框中。

已知安全风险列表包括有关风险严重性的信息。

您可以单击"帮助",获取有关已知安全风险的集中式例外选项的详细信息。

### 配置已知安全风险的集中式例外

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 在"集中式例外"下,单击"添加">"安全风险例外">"已知风险"。
- **3** 在"已知安全风险例外"对话框中,选择想从防病毒和防间谍软件扫描中排除的一个或多个安全风险。
- **4** 如果想要记录检测事件,选中"检测到安全风险时记录"。

如果未选中此选项,客户端在检测到所选风险时会将其忽略。客户端也因此不 会记录检测事件。

- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

### 配置文件的集中式例外

您可以分别添加文件的例外。如果想创建多个文件的例外,请重复此过程。

#### 配置文件的集中式例外

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 在"集中式例外"下,单击"添加">"安全风险例外">"文件"。
- 3 如果要限制例外,请在"安全风险文件例外"下的"前缀变量"下拉框中,选择一个文件位置。

如果您要将例外应用于客户端计算机上任何位置的文件,请单击[NONE]。

- 4 在"文件"文本框中,键入文件的名称。 包括文件的任何路径信息。
- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

### 配置文件夹的集中式例外

您可以分别添加单个文件夹的例外。如果想创建多个文件夹的例外,请重复此过 程。

#### 配置文件夹的集中式例外

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 在"集中式例外"下,单击"添加">"安全风险例外">"文件夹"。
- 3 如果要限制例外,请在"安全风险文件夹例外"下的"前缀变量"下拉框中,选择一个文件夹位置。 如果您要将例外应用于客户端计算机上任何位置的文件,请单击[NONE]。
- 4 在"文件夹"文本框中,键入文件夹的名称。 包括文件夹的任何路径信息。
- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

### 配置文件扩展名的集中式例外

可以将多个文件扩展名添加到例外。在创建例外之后,您不能为相同的策略创建其 他扩展名例外。您必须编辑现有的例外。

**注意**: 您一次只能添加一个扩展名。如果您在"添加"文本框中输入多个扩展名, 则策略会将这些条目当成一个扩展名。

#### 配置文件扩展名的集中式例外

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 在"集中式例外"下,单击"添加">"安全风险例外">"扩展名"。
- 3 在文本框中,键入要排除的扩展名,然后单击"添加"。
- 4 重复步骤3将更多扩展名添加至例外。
- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

### 配置 TruScan 主动型威胁扫描的集中式例外

您可以通过配置例外将检测到的进程从未来的主动型威胁扫描范围中排除。您还可 以强制主动型威胁扫描检测特定进程。

### 配置 TruScan 主动型威胁扫描的集中式例外

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 单击"添加">"TruScan 主动型威胁扫描例外",然后执行下列操作之一:
  - 单击"已检测到的进程"。
请参见第 469 页的"为已检测到的进程配置集中式例外"。

- 单击"进程"。 请参见第469页的"通过配置例外强制TruScan主动型威胁扫描检测进程"。
- 3 单击"确定"。
- 4 完成此策略的配置后,单击"确定"。

#### 为已检测到的进程配置集中式例外

您可以为 TruScan 主动型威胁扫描检测到的进程创建例外。

当您要创建已检测到进程的例外时,您可以从检测列表中选择。管理控制台会将客 户端在安全网络中记录的检测信息填充到列表中。

如果网络中的客户端计算机尚未运行检测,检测列表则为空。

您可以强制主动型威胁扫描检测特定进程。当主动型威胁扫描检测到此进程,且管 理控制台接收到相应事件时,该进程会出现在检测到的进程列表中。

请参见第 469 页的"通过配置例外强制 TruScan 主动型威胁扫描检测进程"。

#### 为已检测到的进程配置集中式例外

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 单击"添加">"TruScan 主动型威胁扫描例外">"已检测到的进程"。
- 3 选择要为其创建例外的进程。
- **4** 在"操作"下拉框中,选择"忽略"、"终止"、"隔离"或"仅记录"。
- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

#### 通过配置例外强制 TruScan 主动型威胁扫描检测进程

您可以通过配置例外来强制主动型威胁扫描检测某个进程。在主动型威胁扫描当前 不检测特定进程时,您可以配置此类型的例外。

在以后运行扫描并检测到指定的进程后,您可以再创建一个例外来处理该进程。

请参见第 469 页的"为已检测到的进程配置集中式例外"。

#### 通过配置例外强制 TruScan 主动型威胁扫描检测进程

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 单击"添加">"TruScan 主动型威胁扫描例外">"进程"。

3 在对话框中键入进程名称。

例如,您可以键入如下所示的可执行文件名称:

#### foo.exe

- 4 单击"确定"。
- 5 完成此策略的配置后,单击"确定"。

## 配置防篡改的集中式例外

您还可以配置防篡改的集中式例外。您需要知道与您要允许的应用程序相关联的文件名。

例如,防篡改可能会禁止辅助技术应用程序,例如屏幕读取器。您需要知道与辅助 技术应用程序相关联的文件的名称。然后,您就可以创建例外,以允许应用程序运 行。

#### 配置防篡改的集中式例外

- 1 在"集中式例外策略"页面,单击"集中式例外"。
- 2 单击"添加">"防篡改例外"。
- 3 如果要限制例外,请在"防篡改例外"对话框的"前缀变量"下拉框中,选择 一个文件位置。
- 4 在"文件"文本框中,键入文件的名称。 包括文件的任何路径信息。
- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

## 配置集中式例外的客户端限制

您可以通过配置限制措施使客户端计算机上的用户不能创建防病毒和防间谍软件扫 描或TruScan主动型威胁扫描的例外。默认情况下,允许用户配置例外。用户对主 动型威胁扫描只拥有有限的配置权限。

有关以下步骤中所使用选项的详细信息,您可以单击"帮助"。

注意:不管限制设置如何,客户端计算机上的用户永远不能创建防篡改例外。

#### 配置集中式例外的客户端限制

- 1 在"集中式例外策略"页面,单击"客户端限制"。
- 2 在"客户端限制"下,选中或取消选中"安全风险例外"和"TruScan主动型 威胁扫描例外"。
- 3 完成此策略的配置后,单击"确定"。

## 从日志事件创建集中式例外

您可以从防病毒和防间谍软件扫描或主动型威胁扫描的日志事件创建集中式例外。您不能从防篡改的日志事件创建例外。

当您从日志事件创建异常错误时,您可以将风险、文件、文件夹、扩展名或进程添加到"集中式例外策略"。可在创建例外时指定集中式例外策略。

请参见第159页的"关于日志"。

#### 从日志事件创建集中式例外

- 1 在"监视器"选项卡上,单击"日志"选项卡。
- 2 在"日志类型"下拉列表中,选择下列其中一个选项:
  - 风险
  - TruScan 主动型威胁扫描
  - 应用程序与设备控制
- 3 如果您选择"应用程序与设备控制",则可以从"日志内容"列表框中选择 "应用程序控制"。
- **4** 单击"查看日志"。
- 5 按照相关说明,为所选的日志类型添加集中式例外。 请参见第 471 页的"添加风险事件的集中式例外"。 请参见第 472 页的"添加 TruScan 主动型威胁扫描事件的集中式例外"。 请参见第 472 页的"添加防篡改事件的集中式例外"。

## 添加风险事件的集中式例外

您可以添加风险事件的集中式例外。

#### 添加风险事件的集中式例外

- 1 在"风险日志"页面中,选择要为其添加集中式例外的一个或多个事件。
- 2 在"操作"旁,选择下列其中一个选项:

- 将风险添加至集中式例外策略
- 将文件添加至集中式例外策略
- 将文件夹添加至集中式例外策略
- 将扩展名添加至集中式例外策略
- 3 单击"开始"。
- 4 在对话框中,您可以删除与事件关联的任何风险、文件、文件夹或扩展名。如 果删除项目,则该项目就不会包括在例外中。 如果没有项目显示在风险、文件、文件夹或扩展名列表中,您就不能创建例 外。
- 5 对于安全风险,如果您要客户端软件记录检测,请选中"检测到安全风险时记录"。
- 6 选择应该使用此例外的所有集中式例外策略。
- 7 单击"确定"。

## 添加 TruScan 主动型威胁扫描事件的集中式例外

您可以添加主动型威胁扫描事件的集中式例外。

#### 添加 TruScan 主动型威胁扫描事件的集中式例外

- 1 在 "TruScan 主动型威胁扫描日志"页面上,选择要为其添加集中式例外的一 个或多个事件。
- 2 在"操作"旁边,选择"将进程添加至集中式例外策略"。
- 3 单击"开始"。
- 4 在对话框中的"响应"下拉列表中,选择进程的检测操作。 或者,还可以删除不希望包括在例外中的任何进程。
- 5 选择应该包括此例外的集中式例外策略。
- 6 单击"确定"。

## 添加防篡改事件的集中式例外

您可以添加防篡改事件的集中式例外。防篡改功能必须已经禁止您想要允许的应用 程序。在防篡改禁止应用程序之后,客户端计算机会记录该事件,并将其发送到管 理服务器。您就可以使用该日志事件来创建例外。

#### 添加防篡改事件的集中式例外

 在"应用程序与设备控制日志"页面上,选择要添加集中式例外的一个或多个 事件。

例如,您可以选择应用于想要运行的辅助技术应用程序的一个或多个事件。

- 2 在"操作"旁边,选择"将文件添加至集中式例外策略"。
- 3 单击"开始"。
- 4 若要删除不想在例外中包括的文件,请选择该文件并单击"删除"。 重复此步骤,删除更多文件。
- 5 选择应该包括此例外的集中式例外策略。
- 6 单击"确定"。

474 | 配置集中式例外策略 从日志事件创建集中式例外





## 配置主机完整性以实现端点 策略遵从

- 基本主机完整性设置
- 添加自定义要求

476 |

# 36

# 基本主机完整性设置

本章节包括下列主题:

- 主机完整性强制执行的工作方式
- 关于使用主机完整性策略
- 关于主机完整性要求
- 添加主机完整性要求
- 启用和禁用主机完整性要求
- 更改主机完整性要求的顺序
- 从模板添加主机完整性要求
- 关于主机完整性检查的设置
- 在要求不满足时允许主机完整性检查通过
- 配置主机完整性检查的通知
- 关于主机完整性补救
- 指定客户端等候补救的时间长度
- 允许用户推迟或取消主机完整性补救
- 在用户未登录时隐藏补救

## 主机完整性强制执行的工作方式

可以通过设置主机完整性策略来确保与网络连接的客户端计算机运行所需的应用程 序和数据文件。运行主机完整性检查的客户端会实现您设置的主机完整性策略设 置。客户端通过自行采取操作来强制执行这些策略,例如下载补丁程序或启动某个 程序。 "主机完整性"检查期间,客户端会依照"主机完整性"策略设置的请求进行。它 会检查注册表项、活动应用程序、文件的日期与大小以及其他可能的参数,以便确 定所需软件是否存在。

当客户端发现计算机上尚未安装所需软件时,它会自动在安全日志中生成一个条 目。如果在客户端上启用了用户通知,则用户计算机上会显示一条消息。

如果计算机上未安装所需软件,可设置客户端以静默方式连接到补救服务器。接着 可从服务器下载和安装必要的软件。软件可能包括软件补丁程序、纠正程序、病毒 定义的更新等。客户端可让用户选择是要立即下载还是要推迟下载。安装软件后, 计算机才能连接到企业网络。

客户端也可以检测防病毒应用程序是否过期。如果防病毒应用程序的版本比系统管 理员指定的版本旧,则客户端将不能连接到企业网络。客户端需要安装最新版的防 病毒应用程序,才能连接。

"主机完整性策略"包括的设置,可决定客户端计算机上客户端运行"主机完整 性"检查的频率。客户端计算机可通过 Symantec Enforcer 连接网络。您可以将主 机完整性策略设置为客户端只在 Enforcer 提示其运行主机完整性检查才运行该项检 查。Enforcer 会验证以下条件:客户端是否正在运行,客户端的策略是否最新,以 及在允许访问网络之前是否已通过主机完整性检查。

客户端每次收到新的安全策略时,就会立即运行主机完整性检查。可以将客户端设 置为自动下载并安装最新的安全策略。如果策略更新失败,则会生成一个安全日志 条目。如果在客户端上启用了用户通知,则用户计算机上会显示一条消息。

在设置主机完整性强制执行的要求时,您可以考虑下列示例:

- 客户端运行最新的防病毒软件。
- 仅当客户端尝试通过 Enforcer 连接到网络时,才执行主机完整性检查。
- 检查触发在客户端上以静默方式执行的操作。

您也可以使用 Enforcer 强制执行这些策略。Enforcer 是作为客户端连接到网络的 媒介的软件应用程序或可选硬件设备。本文所显示的大多数示例中均使用了 Enforcer。

Enforcer 会自动执行下列操作:

- 验证用户的计算机上是否已安装客户端
- 提示客户端检索更新的安全策略(如果有)

然后, Enforcer 会提示客户端运行主机完整性检查。

客户端首先会验证是否已安装最新的防病毒软件且已运行。如果该软件已安装但未运行,则客户端会以静默方式启动防病毒应用程序。若未安装,客户端会从主机完整性要求中指定的 URL 下载该软件。然后,客户端会安装并启动该软件。

下一步,客户端会验证防病毒特征文件是否是最新的。如果防病毒文件不是最新的,则客户端会以静默方式检索并安装更新的防病毒文件。

客户端现在会再次运行主机完整性检查,并会通过检查。. Enforcer 会收到结果,并允许客户端访问企业网络。在此例中,必须满足以下要求:

用于进行主机完整性更新的文件服务器已安装最新的文件。客户端必须从文件服务器获取更新的应用程序。您可以设置一个或多个连接到企业网络的补救服务器。用户可以从补救服务器复制或自动下载任何必要应用程序所需的补丁程序与修补程序。

如果补救服务器失败,则主机完整性补救也会失败。客户端尝试利用 Enforcer 连接时,如果"主机完整性"失败,则 Enforcer 会禁止客户端。控制台包括这 样一项功能:即使主机完整性检查失败也允许该检查通过。在这种情况下, Enforcer 不会禁止客户端。有关失败的主机完整性检查的信息会记录在客户端 的安全日志中。

您必须配置管理服务器,安全策略的更新才会自动发送到运行客户端的任何计算机。

若针对主机完整性策略定义的参数不成功,则Enforcer 会禁止客户端连接至网络。 客户端会出现以下消息:

Symantec Enforcer 已禁止来自客户端的所有通信。 规则: {要求的名称} 失败。

如果Enforcer禁止客户端,则客户端会尝试进行恢复。如果主机完整性策略设置为 在允许客户端连接到网络之前更新文件,则会通知用户需要进行更新。更新期间会 显示更新进度指示条。如果用户断开与企业网络的连接,则该进程会再次启动。

## 关于使用主机完整性策略

您可以使用与创建和修改其他类型策略类似的方式,创建和编辑主机完整性策略。 您可以分配、撤回、替换、复制、导出、导入或删除主机完整性策略。

您通常可将一个策略分配至安全网络中的多个组。如果对特定位置有特定要求,您 可以创建一个非共享、位置限定的策略。

若要使用主机完整性策略,您必须熟悉策略配置的基本知识。

请参见第 282 页的"关于策略"。

#### 关于隔离策略

"隔离策略"是运行"主机完整性"检查的 Symantec Network Access Control 客 户端策略。如果没有达到主机完整性策略要求,客户端会尝试补救。如果补救失 败,客户端会自动切换到隔离策略。"隔离策略"可以是"防病毒和防间谍软件策 略"、"防火墙策略"、"入侵防护策略"、"LiveUpdate策略"或"应用程序与 设备控制策略"。您可以设置"隔离策略",并将该策略分配至位置。

## 关于主机完整性要求

规划主机完整性要求时,必须考虑以下问题:

- 您需要什么软件(应用程序、文件、补丁程序等)来保证企业的安全?
- 如果未满足要求,会发生什么情况?例如:
  - 客户端会连接到服务器并还原软件以满足要求。
  - 即使未满足要求也可以通过主机完整性检查。
  - 主机完整性检查会失败并会禁止网络访问。
  - 会显示消息通知用户接下来要执行的操作。

更加细致地考虑以下各个方面:

- 在每个用户的计算机连接网络时,它们分别需要哪些防病毒应用程序、反间谍 软件应用程序、防火墙应用程序、补丁程序或更新?通常为每种类型的软件创 建一个单独的要求。使用预定义的主机完整性要求可以轻松地设置这些常用要求。
- 可以授予用户选择要在其计算机上运行的防火墙、防间谍软件或防病毒应用程序的权限。使用预定义要求可以指定某个特定的应用程序或整个受支持的应用程序列表是可接受的。您可以创建包括您公司可接受的应用程序的自定义要求。
- 如何处理才能还原用户的计算机以满足要求?正常情况下,您需要设置具有所需软件的补救服务器。配置要求时,必须指定可供客户端从中下载并安装所需软件的 URL。
- 一些补丁程序要求用户重新启动计算机。更新按照特定顺序完成,以便在用户 必须重新启动之前应用所有更新。作为主机完整性策略的一部分,您可以设置 检查要求和尝试补救的顺序。
- 还应考虑当未满足要求并且无法还原时会发生什么情况。对于每个要求,您可以选择即使未满足该要求也允许主机完整性检查通过。主机完整性策略通常也允许您配置消息。如果主机完整性检查失败,或在前一次检查中失败而在本次检查中通过,则客户端会向用户显示这些消息。您可能要在这些消息中为用户添加其他说明。另外,可以设置当主机完整性检查失败时要激活的隔离策略。
- 可以通过将类似的应用程序包括在一个自定义要求中来简化对所需应用程序的 管理。例如,诸如 Internet Explorer 和 Netscape Navigator 之类的 Internet 浏 览器都可包括在同一个要求中。
- 作为自定义要求的一部分,您可以指定在不符合要求时是否允许主机完整性检查通过。当对一个脚本中检查多少个条件进行规划时,请记住,此设置会作为一个整体应用于自定义要求脚本。设置的这一特点可能会影响您是希望创建多个较小的自定义要求,还是创建一个包含多个步骤的较长要求。

您会发现,设置一个描述您公司的主机完整性强制执行要求的电子表格是相当有用 的。

主机完整性策略包括下列要求类型:

- 预定义的要求包括最常见的主机完整性检查类型,并且可让您选择下列类型:
  - 防病毒要求
  - 防间谍软件要求
  - 防火墙要求
  - 补丁程序要求
  - Service Pack 要求
- 可使用自定义要求编辑器定义的自定义要求。
   请参见第 499 页的"编写自定义要求脚本"。
- 主机完整性要求模板,这些模板通过 Symantec Enterprise Protection 联机订购 服务进行更新。
   请参见第 483 页的"从模板添加主机完整性要求"。

添加新要求时,可以选择一种预定义的要求类型。随即会出现一个对话框,显示一 组预定义设置,可供您配置。如果预定义设置不符合您的要求,则可以创建自定义 要求。

## 添加主机完整性要求

主机完整性策略用于设置客户端计算机上防火墙、防病毒软件、防间谍软件、补丁 程序、Service Pack或其他必需应用程序的要求。

每个主机完整性策略都包括要求和常规设置。这些要求指定以下项:

- 应检查的条件
- 客户端为响应条件应采取的操作(如下载和安装)

指定"主机完整性"要求时,可以从以下类型选择:预定义、自定义或模板要求。 可通过主机完整性策略 LiveUpdate 服务获得模板要求。您可以在策略之间对要求 进行复制粘贴和导出导入。

通过常规设置可配置客户端运行主机完整性检查的时间和频率,并配置补救选项和 通知。

可以创建新的共享或非共享的主机完整性策略。创建新策略后,可以添加预定义的 要求和/或自定义的要求。

#### 添加主机完整性要求

- 在控制台中,打开"主机完整性策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"主机完整性策略"页面中,单击"要求"。
- 3 在"要求"页面中,通过选择以下选项之一,决定主机完整性检查应何时在客户端上运行:

- 4 单击"添加"。
- 5 在"添加要求"对话框中,选择下列任一要求类型:
  - 防病毒要求
  - 防间谍软件要求
  - 防火墙要求
  - 补丁程序要求
  - Service Pack 要求
  - 自定义要求
- 6 单击"确定"。
- 7 配置要求设置。请参见第 480 页的"关于主机完整性要求"。
- 8 在"高级设置"页上,配置主机完整性检查、补救和通知的设置。 有关详细信息,可以单击"帮助"。 请参见第 484 页的"关于主机完整性检查的设置"。

- 9 配置完此策略后,单击"确定"。
- 10 将策略分配给组或位置。

请参见第 289 页的"分配共享策略"。

## 启用和禁用主机完整性要求

创建主机完整性策略要求时,可以创建要求供未来使用。您必须先禁用这些要求, 等到有需要时再启用。测试主机完整性策略时,可以暂时禁用要求。

#### 启用与禁用主机完整性要求

- 在控制台中,打开"主机完整性策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"主机完整性策略"页面中,单击"要求"。
- 3 在"要求"页面上选择要求,然后运行下列其中一项任务:
  - 若要启用要求,请选中所选择要求的"启用"复选框。
  - 若要禁用要求,请取消选中所选择要求的"启用"复选框。
- 4 配置完此策略后,单击"确定"。

## 更改主机完整性要求的顺序

您可以更改要求的位置。更改位置时,可以确定要求的执行顺序。如果下载请求在 安装后重新启动的软件,此位置会很重要。您可以设置顺序,以确保请求重新启动 以进行补救的要求最后执行。

#### 更改主机完整性要求的顺序

- 在控制台中,打开"主机完整性策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"主机完整性"页面中,单击"要求"。
- 3 在"要求"列表中,选择要移动的要求,然后单击"上移"或"下移"。
- 4 配置完此策略后,单击"确定"。

## 从模板添加主机完整性要求

联机订购服务可提供主机完整性模板。

可以导入最新模板并在为主机完整性策略制定自定义要求时使用这些模板。您可以 根据需要选择任意数量的要求。您可以选择要求直接使用,或根据环境需要加以修 改。

如果您的订阅已过期,已导入的要求仍然可以使用。但不能再导入最新的更新。

如果您是第二次导人要求,而且已存在相同名称的要求,则导人的要求不会覆盖现 有的要求。相反,导人的要求将在"要求"表上其名称的旁边显示一个2字。

#### 从模板添加主机完整性要求

- 在控制台中,打开"主机完整性策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"主机完整性"页面中,单击"要求"。
- **3** 在"要求"页上,单击"模板"。
- 4 在"主机完整性联机更新"对话框中,展开"模板",然后选择模板类别。
- 5 在要添加的每个模板旁边,单击"添加"。
- 6 单击"导入"。
- 7 配置完此策略后,单击"确定"。

## 关于主机完整性检查的设置

设置主机完整性策略时,有多种设置可供选择。设置将会决定主机完整性检查的执 行方式,以及结果的处理方式。

如果更改了主机完整性策略,则在下一次检测信号时会将其下载到客户端。然后, 客户端会运行主机完整性检查。

如果用户要切换至具有不同主机完整性策略的位置,而此时正在运行主机完整性检查,则客户端会停止此项检查。如果策略要求,此停止操作还会包括补救尝试。如 果新位置中的补救服务器连接不可用,则用户会收到超时消息。检查完成后,客户 端会丢弃结果。接着,客户端会根据位置的新策略,立即运行新的主机完整性检 查。

如果新位置使用相同的策略,则客户端会保留所有的主机完整性计时器设置。仅当 策略设置需要时,客户端才会运行新主机完整性检查。

表 36-1 显示主机完整性检查的设置。

#### 表 36-1 主机完整性检查设置

设置	说明
主机完整性检查时间间隔	指定主机完整性检查的频率。

设置	说明
检查结果保留时间	设置主机完整性检查结果保留的时间
	您可以设置客户端保留前一次主机完整性检查 结果的时间。即使用户采取的操作通常会导致 运行新的主机完整性检查,但客户端仍会保留 前一次的检查结果。例如,用户可能下载新软 件或更改位置。
检查要求一次失败后继续检查	指定客户端在检查要求一次失败后继续检查。 直到失败的要求还原之后客户端才会停止主机 完整性检查。
	客户端根据主机完整性策略中指定的顺序检查 主机完整性要求。
	如果启用此设置,则即使主机完整性检查未通 过也可以尝试其他补救操作(如果需要)。
	即使要求不满足,也可允许主机完整性检查通 过。此设置可在各要求类型的"要求"对话框 中找到。可以为每项要求分别应用此设置。

## 在要求不满足时允许主机完整性检查通过

除了在主机完整性策略中启用或禁用要求来决定客户端是否运行要求脚本之外,还 可以让客户端运行要求脚本并记录结果,但忽略结果。可以让主机完整性检查在不 论要求是否满足的情况下都通过。即使不满足要求条件,也认为符合要求。

对于特定要求,可启用对话框中的"即使这项要求不满足,也允许主机完整性检查 通过"。如果要将此设置应用于所有要求,则必须对每个要求分别启用此设置。默 认情况下,此设置处于禁用状态。

如果启用即使要求不满足也允许主机完整性检查通过的设置,则在事件发生时,客户端窗口中会显示以下消息:

主机完整性检查未通过但却报告为已通过

#### 在要求不满足时允许主机完整性检查通过

- 在控制台中,打开"主机完整性策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"主机完整性"页面中,单击"要求"。
- **3** 在"要求"页面中,单击"添加",然后添加预定义的要求或自定义要求,并 且单击"确定"。

- 4 在要求的对话框上,选中"即使这项要求不满足,也允许主机完整性检查通过"。
- 5 单击"确定"。
- 6 完成此策略的配置后,单击"确定"。

## 配置主机完整性检查的通知

客户端运行主机完整性检查时,您可以配置发生下列状况时将出现的通知:

- 主机完整性检查未通过。
- 主机完整性检查未通过后再次检查通过。

主机完整性检查的结果会出现在客户端的安全日志中。这些信息会上载至管理服务器"监视器"页面的遵从日志中。

客户端的安全日志包括多个窗格。如果您选择主机完整性检查事件类型,左下方窗 格会列出各个要求是已通过还是未通过。右下方窗格会列出要求的条件。您可将客 户端配置为禁止信息在右下方窗格中出现。虽然进行疑难解答时可能需要这项信 息,但是您可能不希望用户查看这类信息。例如,您可能写入了指定注册表值或文 件名称的自定义要求。安全日志仍会记录详细信息。

您也可以启用通知,以便用户可选择立即下载软件或推迟进行补救。

请参见第 488 页的"允许用户推迟或取消主机完整性补救"。

#### 配置主机完整性检查的通知

- 在控制台中,打开"主机完整性策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"主机完整性"页面上,单击"高级设置"。
- **3** 在"高级设置"页面的"通知"下,若要显示详细的要求信息,请选中"显示 详细主机完整性日志记录"。

客户端的安全日志右下方窗格会显示主机完整性要求的完整信息。

- 4 选中以下任意选项:
  - 主机完整性检查未通过时显示通知消息.
  - 主机完整性检查未通过后再次检查通过时显示通知消息.
- 5 若要添加自定义消息,请单击"设置更多文本",键入最多不超过512个字符的附加文本,然后单击"确定"。
- 6 如果即使用户未登录,也要显示任一一项通知,请取消选中"用户必须先登录,然后才会出现应用程序和主机完整性通知"。
- 7 完成策略配置后,单击"确定"。

## 关于主机完整性补救

如果客户端主机完整性检查显示不符合主机完整性要求,则客户端可以尝试还原必要的文件以符合要求。然后客户端计算机需要通过主机完整性检查。客户端会下载、安装文件,或者启动所需的应用程序。在设置主机完整性策略时,可以指定在补救过程中要执行的操作。不仅可以指定客户端在何处下载补救文件,而且还可以指定如何实施补救过程。

您可以允许用户取消正在下载的软件。您还可以设置允许用户推迟下载的次数以及 时间长短。除了您已禁用取消补救的要求外,此设置应用于策略中的所有其他类型 的要求。用户只能够取消预定义的要求。

## 关于为满足主机完整性而还原应用程序和文件

为满足要求而设置补救时,可以指定要下载和安装的安装软件包或文件的位置。指 定安装软件包或文件的下载位置时,可以使用以下任一种格式:

#### UNC \\servername\sharename\dirname\filename

如果目标客户端禁用"网上邻居"浏览,则UNC还原不可用。如果使用UNC 路径进行补救,请确保没有禁用"网上邻居"浏览功能。

- FTP FTP://ftp.ourftp.ourcompany.com/folder/filename
- HTTP HTTP://www.ourcompany.com/folder/filename

安装软件包或文件将始终下载到临时目录。任何相对路径都会参照此目录。如果存在 TMP 环境变量,则会用 TMP 环境变量对临时目录进行定义;否则,将用 TEMP 环境变量(如果存在)对其进行定义。默认目录为 Windows 目录。

对于文件执行,当前工作目录始终设置为 Windows 临时目录。在执行前环境变量 会被替换掉。Windows 目录路径将替换命令 %windir%。

可以使用%1(默认设置)来执行在"下载URL"字段中指定的文件。%1变量代表最后下载的文件。

在下载、安装或执行用于还原要求的命令之后,客户端会始终重新测试要求。此 外,客户端还会记录结果,即通过或未通过。

## 主机完整性补救和 Enforcer 设置

设置主机完整性要求时,可以指定在不符合主机完整性要求时,客户端应通过连接 到补救服务器来使用所需的任何信息更新客户端计算机。如果将此类要求应用于通 过Enforcer连接到网络的客户端,则需要确保在禁止客户端进行常规网络访问的同 时允许其访问补救服务器。否则,客户端将不能还原主机完整性,因而仍不符合主 机完整性要求。 完成此任务的方式视 Enforcer 的类型而定。下面的列表给出了几个例子:

- 对于 Gateway Enforcer,可以配置 Gateway Enforcer,使之将补救服务器识别 为可信的内部 IP 地址。
- 对于 DHCP Enforcer,可以在 DHCP 服务器上设置隔离区网络配置以允许访问 补救服务器。
- 对于 LAN Enforcer,如果使用具有动态 VLAN 功能的交换机,则可以设置一个可访问补救服务器的 VLAN。

## 指定客户端等候补救的时间长度

您可以指定客户端在尝试再次安装和启动补救下载之前可等候的时间。不论您指定 的时间长度为何,只要启动新的主机完整性检查,客户端就会再次尝试补救客户端 计算机。

#### 指定客户端等候补救的时间长度

- 在控制台中,打开"主机完整性策略"。
   请参见第 288 页的"编辑策略"。
- 2 在"主机完整性策略"页面中,单击"要求"。
- 3 在"要求"页面中,单击"添加",然后添加预定义的要求,再单击"确定"。
- 4 在各个预定义要求的对话框中,选中"如果尚未在客户端安装 <要求名称>则 进行安装"。
- **5** 选中"下载安装软件包"。

针对防病毒要求,选中"下载安装软件包"。

- **6** 选中指定如下载失败尝试再次下载之前等待的时间。
- 7 指定等候的分钟、小时或天数。
- 8 配置完此策略后,单击"确定"。

## 允许用户推迟或取消主机完整性补救

如果有要求指定补救操作,您可以允许用户取消补救。您也可以允许用户将补救推 迟到更为合适的时间。补救操作的例子包括安装应用程序或更新特征文件。您可以 在可以取消补救的次数和用户可以推迟补救的时间长短上设置限制。设置的限制决 定了需要补救时客户端显示的消息窗口上用户可以使用的选项。您也可以向消息窗 口添加文本。

最短和最长时间设置决定了消息窗口中可用选项的范围。不符合某项要求时,系统 会为用户显示消息窗口。该范围以列表形式显示在消息中"以后提醒我"图标的旁 边。 如果用户所选的推迟时间比主机完整性检查的时间间隔短,则用户的选择会被覆盖。客户端再一次运行主机完整性检查前,消息窗口都不会显示。如果用户选择了在5分钟后提醒,但主机完整性检查是每30分钟运行一次,则补救消息窗口会等到30分钟后才显示。因此,为避免用户混淆,可能需要同步处理最短时间设置与主机完整性检查频率设置。

如果用户推迟补救,则客户端会记录事件。主机完整性会显示为失败,原因是不符合要求。用户可以随时在客户端用户界面手动运行新的主机完整性检查。

如果用户推迟了补救操作,且在推迟期间,客户端收到更新的策略,则可用于补救的时间长度将重置为指定的最长时间。

#### 允许用户推迟运行主机完整性矫正

1 在控制台中, 打开"主机完整性策略"。

请参见第 288 页的"编辑策略"。

- 2 在"主机完整性策略"页面中,单击"高级设置"。
- **3** 在"高级设置"页面的"补救对话框选项"下,设置用户可将补救推迟多久的 最短和最长时间限制。
- 4 键入用户可取消补救的次数上限。
- 5 若要在客户端计算机上添加自定义消息,请单击"设置更多文本"。

如果用户单击"详细信息"选项,则您键入的消息将显示在客户端的补救窗口 中。如果没有指定其他文本,则当用户单击"详细信息"时,在"详细信息" 区域会重复显示默认的窗口文本。

- 6 在"输入更多文本"对话框中,键入最多不超过512个字符的自定义消息,然 后单击"确定"。
- 7 配置完此策略后,单击"确定"。

#### 允许用户取消主机完整性补救

1 在控制台中,打开"主机完整性策略"。

请参见第288页的"编辑策略"。

- 2 在"主机完整性策略"页面中,单击"要求"。
- 3 在"要求"页面中,单击"添加",然后添加预定义的要求,再单击"确定"。
- 4 在各个预定义要求的对话框中,选中"如果尚未在客户端安装 <要求名称>则 进行安装"。
- 5 选中"下载安装软件包"。

针对防病毒要求,选中"下载安装软件包"。

- 6 选中"允许用户取消下载主机完整性补救"。
- 7 配置完此策略后,单击"确定"。

## 在用户未登录时隐藏补救

默认情况下,不论用户是否登录,主机完整性补救都会运行。客户端能随时利用操 作系统更新或必要的安全软件补救客户端计算机。然而,当补救运行本地应用程序 或已下载的应用程序时,即使用户未登录,仍可运行应用程序。例如,安装软件包 可能会启动Internet Explorer,用户可以从Internet Explorer中运行命令提示或其 他程序。基于安全考虑,在用户登录客户端前,您可能不想让任何应用程序或通知 出现。

当您编写使用"运行程序"功能的自定义要求时,可以绕过此问题。"运行程序"功能会启动使用已登录用户环境的程序。

请参见第 504 页的"运行程序"。

#### 在用户未登录时隐藏补救

1 在控制台中,打开"主机完整性策略"。

请参见第 288 页的"编辑策略"。

- 2 在"主机完整性"页面上,单击"高级设置"。
- 3 在"高级设置"页面的"通知"下,确认已选中"用户必须先登录,然后才会 出现应用程序和主机完整性通知"。
- 4 完成策略配置后,单击"确定"。

# 37

# 添加自定义要求

本章节包括下列主题:

- 关于自定义要求
- 关于条件
- 关于功能
- 关于自定义要求逻辑
- 编写自定义要求脚本
- 显示消息对话框
- 下载文件
- 生成日志消息
- 运行程序
- 运行脚本
- 设置文件的时间戳
- 指定脚本的等待时间

## 关于自定义要求

自定义要求会检查客户端计算机是否具备管理员所选择或定义的任何条件。您可以 撰写自定义要求来纠正任何已识别出的遵从问题。

您可以使用预定义的选定内容及字段来创建复杂或简单的要求脚本。

创建自定义要求时,可以使用预定义要求对话框中的字段及列表。然而,自定义要 求会为您提供更大的灵活性。在自定义要求中,您可以添加预定义应用程序列表中 不包括的应用程序。您也可以通过单独添加每个应用程序来创建预定义列表的子集。

## 关于条件

条件是自定义要求脚本中,可能执行以检测遵循问题的检查操作。 您可以选择以下类别的条件:

- 防病毒检查
- 防间谍软件检查
- 防火墙检查
- 文件检查和操作
- 注册表检查和操作
- 实用程序

您可以将条件指定为存在或不存在(NOT)。您可以使用 AND 或 OR 关键字,添加多 个条件语句。

## 关于防病毒的条件

对于自定义要求,您可以指定要作为IF-THEN条件语句的一部分进行检查的防病毒应用程序和特征文件信息。

可以检查下列条件:

- 防病毒产品已安装
- 防病毒产品已在运行
- 防病毒特征文件已更新至最新

在作为自定义要求的一部分检查应用程序和特征文件时,可以指定与创建预定义要求时相同的信息。选项名称可能会略有不同。

如果您选择"任何病毒产品"选项,则下拉式列表上的任何应用程序都符合要求。 通过使用 OR 关键词选择每个应用程序,可以纳入一个应用程序子集。

在指定特征文件信息时,可以选择一个或两个选项来检查特征文件是否为最新。如果选择两个选项,则必须满足以下两个条件才能满足要求:

- 选择"检查特征文件是否少于"并输入天数。日期在指定的天数之前的文件为 过期文件。
- 选择"检查特征文件的日期为"再选择"之前"、"之后"、"等于"或"不等于",然后指定一个日期(mm/dd/yyyy)。您也可以指定小时及分钟;默认为00:00。特征文件期限由该文件的最后修改日期确定。

## 关于防间谍软件的条件

对于自定义主机完整性要求,您可以指定要作为IF-THEN条件语句的一部分进行检查的防间谍软件应用程序和特征文件信息。

可以检查下列条件:

- 已安装防间谍软件
- 正在运行防间谍软件
- 防病毒特征文件已更新至最新

在作为自定义要求的一部分检查应用程序和特征文件时,可以指定与创建预定义要求时相同的信息。选项名称可能会略有不同。

如果您选择"任何防间谍软件产品"选项,则下拉式列表上的任何应用程序都匹配 要求。

在指定特征文件信息时,可以选择一个或两个选项来检查特征文件是否为最新。如果您选择两个选项,则下列两项条件必须都满足,才能满足要求:

- 选择"检查特征文件是否少于"并输入天数。
   日期在指定的天数之前的文件为过期文件。
- 选择"检查特征文件的日期为"再选择"之前"、"之后"、"等于"或"不等于",然后指定一个日期(mm/dd/yyyy)。您也可以指定小时及分钟;默认为00:00。特征文件期限由该文件的最后修改日期确定。

## 关于防火墙的条件

对于自定义主机完整性要求,您可以指定要作为IF-THEN条件语句的一部分进行检查的防火墙应用程序。

可以检查下列条件:

- 防火墙已安装
- 防火墙正在运行

如果您要选择下拉式列表中的任意应用程序,您可以选择"任何防火墙产品"。通过使用 OR 关键词选择每个应用程序,可以纳入应用程序的子集。

## 关于文件的条件

对于自定义主机完整性要求,可以将检查应用程序或文件作为IF-THEN条件语句的 一部分。

您可以在自定义主机完整性要求中指定下列检查文件信息的选项:

文件:比较文件使用期限	指定天数或星期数, 然后选择"大于"或 "小于"。
文件:比较文件日期	指定mm/dd/yyyy格式的日期。也可以指定 小时与分钟。默认时间为 00:00。您可以选 择"等于"、"不等于"、"之前"或"之 后"。
文件:比较文件大小	指定字节数。可以选择"等于"、"不等 于"、"小于"或"大于"。
文件:比较文件版本	指定 <b>x.x.x</b> 格式的文件版本,其中x表示从 0到65535的一个十进制数。可以选择"等 于"、"不等于"、"小于"或"大于"。
文件: 文件存在	指定要检查的文件的名称。
文件:文件指纹等于	通常使用"搜索应用程序"选择一个应用程 序来获取此信息。
指定一个十六进制数 (最多 32 位数)	选择某个选项时,对话框上会显示附加字 段。您需要为每个选项指定文件名与路径, 并输入其他必要信息。
文件:文件下载完成	您可以将文件从指定位置下载到指定目录。 如果需要验证才能通过HTTP访问文件位 置,则可以指定用户名和密码。

您可以使用系统变量、注册表值或结合使用这两者来指定文件名和路径。在选择其 中一个文件选项时,对话框将显示输入文件名和路径的方法示例。

您可以使用"搜索应用程序"功能,找到以前记录的应用程序。当您在自定义要求 脚本中指定文件选项时,借助"搜索应用程序"选项,可以访问和"搜索应用程 序"工具相同的搜索工具。您可以浏览在管理服务器上定义的组,以过滤应用程 序,输入搜索查询以及将结果导出到文件。

使用系统环境变量或注册表值来搜索:

使用系统环境变量

若要指定位于WINDIR环境变量中指 定的目录下名为cmd.exe的文件,请 键入以下命令:

%WINDIR%\cmd.exe

使用注册表值

使用组合注册表值与系统环境变量

#### 若要将值 HEY\_LOPL\_MCHINE\Software\Synartec\\AppBath 读取为文件 sem.exe 的路径,请键入 以下命令:

#HKEY\_LOCAL\_MACHINE\
Software\Symantec\AppPath#\
sem.exe

请利用以下示例来使用组合注册表值 与系统环境变量:%SYSTEMDIR%\ #HKEY\_LOCAL\_MACHINE\ Software\Symantec\AppPath#.

## 关于操作系统的条件

对于自定义主机完整性要求,您可以指定要作为IF-THEN条件语句的一部分进行检查的操作系统信息。选择某个选项时,对话框上会显示附加字段。

实用程序:操作系统是	指定操作系统。如果要更新补丁程序,则需选择需 要该补丁程序的确切版本。可以使用 OR 关键词来 指定多种操作系统。
实用程序:操作系统语言是	此函数用于检测客户端操作系统的语言版本。如果 "自定义要求"对话框中未列出语言版本,则可以 通过在"语言标识符"字段中键入语言标识符来添 加语言。若要添加多个标识符,请使用逗点来分隔 各个ID,如0405,0813。有关标识符列表,请参见 "语言标识符"表。
补丁程序:将当前Service Pack与指定版 本相比较	键入要检查的 Service Pack 的编号,例如 1a。编 号不得超过两个字符。可以检查下列条件:等于、 不等于、小于或大于。
	数字加上字母会视为大于只有数字本身;例如, Service Pack 编号 6a 会视为大于 6。请确保一次 应用一个补丁程序。
补丁程序:已安装补丁程序	键入要检查的补丁程序名称,例如: KB12345。只能在此字段中键入数字和字母。

请确保补丁程序名称或 Service Pack 编号与操作系统的正确版本相匹配。如果指定的操作系统与补丁程序或 Service Pack 不匹配,则不符合要求。

## 关于注册表的条件

对于自定义主机完整性要求,您可以指定要作为IF-THEN条件语句的一部分进行检查的注册表设置。也可以指定更改注册表值的方法。只有HKEY\_LOCAL\_MACHINE、HKEY\_CLASSES\_ROOT和HKEY\_CURRENT\_CONFIG 是所支持的注册表设置。

可以使用以下选项检查注册表设置:

注册表:注册表项已存在	指定注册表项的名称以检查它是否存在。
注册表: 注册表值等于	指定注册表项的名称和值名称并指定将值与哪些数 据进行比较。
注册表: 注册表值已存在	指定注册表项的名称以检查它是否具有指定的值名 称。
注册表:设置注册表值	指定要为指定项分配的值;如果项不存在,将创建 该项。此选项将替换现有值,不管它是否具有相同 类型;换句话说,如果现有值为DWORD值,但您 指定了字符串值,则会用字符串值替换DWORD。
注册表:增加注册表 DWORD 值	指定DWORD值。可以使用此选项进行计数,例如 允许未修补的计算机最多符合要求 n 次。

指定注册表项时,务必考虑以下几点:

- 项名称不得超过255个字符。
- 如果注册表项末尾含有反斜线(),则视为注册表项。例如: HKEY\_LOCAL\_MACHINE\SOFTWARE\
- 如果注册表项末尾没有反斜线,则视为注册表名称。例如: HKEY\_LOCAL\_MACHINE\SOFTWARE\ActiveTouch

指定注册表值时,务必考虑以下几点:

- 值名称不得超过 255 个字符。
- 可以检查 DWORD(十进制)、二进制(十六进制)或字符串值。
- 对于 DWORD 值,可以检查该值是否小于、等于、不等于或大于指定的值。
- 对于字符串值,可以检查值数据是否等于或包含给定的字符串。如果希望字符 串比较区分大小写,请选中"匹配大小写"复选框。
- 对于二进制值,可以检查值数据是否等于或包含一组给定的二进制数据。以十 六进制字节来表示数据。如果指定"值包含",则还可以指定此数据的偏移。 如果偏移保留为空,则会搜索给定二进制数据的值。十六进制编辑框中允许的 值为0到9以及a到f。

以下是注册表值示例:

DWORD 12345(十进制)

二进制 31 AF BF 69 74 A3 69(十六进制)

字符串 ef4adf4a9d933b747361157b8ce7a22f

## 关于功能

您可以使用功能, 定义条件表达式经评估为真或假时执行的操作。

自定义要求条件会检查特定防病毒产品的安装,但是不能配置为安装产品以作为补救操作。撰写自定义要求时,必须明确定义使用功能语句执行的补救操作。

功能会出现在 THEN 和 ELSE 语句中,也可能出现在自定义要求脚本的末尾。若要 达成需要的补救结果,您可能需要指定多个功能。每一个功能会执行特定的任务, 例如下载文件或可执行文件。您不会定义个别功能提供特定的补救操作,例如安装 特定的防病毒产品。若要下载特定的防病毒产品,您必须使用常规的下载功能。

表 37-1 显示自定义要求脚本中的下列功能:

表 37-1 自定义要求功能

函数	说明
下载文件	将 URL 或 UNC 引用的文件下载至客户端计算机。如果使用 URL,则同时支持 HTTP 和 FTP。
设置注册表值 增加注册表 DWORD 值	创建指定的注册表项,然后设置或增加注册表项中包括的注册表值。
记录消息	指定要添加到客户端安全日志和注册表的自定义消息。
运行程序	执行已常驻于客户端计算机的程序。您可以指定程序是否在用户登录时运行。
运行脚本	在客户端计算机上运行自定义脚本。您可以使用内置的文本 编辑器,创建脚本内容。脚本可能是批处理文件、INI文件, 或 Windows 识别的任何可执行文件格式。此外,脚本可能 只包括要提供给其他程序的参数。
设置时间戳	在客户端计算机的指定文件上标记当前时间和日期。
显示消息对话框	以"确定"按钮在客户端计算机上显示消息对话窗口。A可 指定默认超时。
等待	将自定义要求脚本的执行暂停一段时间。

## 关于自定义要求逻辑

您可以使用类似脚本的逻辑撰写自定义要求。这些规则使用来自于预定义条件和操作列表的IF..THEN..ELSE逻辑。

## 关于 RETURN 语句

您可以添加 RETURN 语句,以指定要求的整体"主机完整性"结果。RETURN 语句包括 PASS 关键字和 FAIL 关键字。所有自定义要求的末尾都必须包括 RETURN 语句。

与预定义要求不同,自定义要求必须明确指定"主机完整性"检查的结果。在某些 状况下,将一组条件评估为真,视为自定义要求通过"主机完整性"评估。在其他 状况下,您可能需要使相同的评估视为未通过"主机完整性"评估。

## 关于 IF、THEN 和 ENDIF 语句

您可以使用一个或多个 IF、THEN 和 ENDIF 语句,定义自定义要求的主要逻辑结构。IF、THEN 和 ENDIF 语句定义检查特定条件的结构 (IF),以及评估这些条件为 真时采取的操作 (THEN)。

您可以使用嵌套的 IF、THEN 和 ENDIF 语句,以形成较复杂的自定义要求。评估 另一项条件前,如果某项条件必须为真,您就必须使用嵌套 IF、THEN 和 ENDIF 语句。

## 关于 ELSE 语句

IF、THEN和ENDIF语句仅限于一组条件,以及评估条件为真时执行的一组操作。 在许多状况下,您可能需要指定一个或多个要采取的操作,以执行想要的补救操 作。您可以添加ELSE语句,确认每当指定的条件判定不成立时,所要采取的操作。

## 关于 NOT 关键字

您可以使用NOT关键字反转特定条件的逻辑评估。将条件添加自定义要求脚本后,可以右键单击条件,然后选择"切换成NOT",以反转条件的逻辑。使用NOT关键字不会更改IF语句的整体真假评估。这只会反转特定条件的真假状态。

## 关于 AND、OR 关键字

您可以在 IF、THEN 或 ENDIF 语句中指定多项条件,然而,这必须添加额外的关键字才能进行。在任何 IF 语句中,您可以添加 AND 和/或 OR 关键字,以逻辑方式 使多项条件相关联。条件的逻辑关联会直接影响 IF 语句的整体真假评估。如果您在 IF 语句中使用 AND 关键字, IF 语句中全部的条件都必须评估为真,才能使 IF 语句 为真。如果您使用 OR 关键字,则只要 IF 语句中任一项条件为真, IF 语句即为真。

指定多项条件时,您必须解读条件的逻辑关联,以预测评估为真或为假。自定义要 求脚本不会以括号格式显示表达式,而会以嵌套关键字和节点显示。.第一个表达式 的开头一律是第一项指定的条件,只要使用相同的逻辑运算符关键字,表达式就会 持续运算。例如,您可以使用 OR 关键字,使三项不同的条件相关联。只要您使用 OR 关键字,全部的条件就会包括在相同的逻辑表达式中。

## 编写自定义要求脚本

若要创建自定义要求,需要向脚本中添加一条或多条 IF..THEN.. 语句。运行脚本时,主机完整性检查会查找IF节点下所列的条件。然后,将根据该条件执行 THEN 节点下所列的操作。最后返回结果(通过或未通过)。

脚本会在左窗格中显示一个树结构, 而在右窗格中显示条件或函数下拉列表。

作为自定义要求的一部分,您可以指定在不符合要求时是否允许主机完整性检查通 过。当对一个脚本中检查多少个不同的条件进行规划时,请记住,此设置会作为整 体应用于自定义要求脚本。这可能会影响您是希望创建多个较小的自定义要求,还 是创建一个含有多个步骤的较长要求。

#### 编写自定义要求脚本

1 添加自定义要求。

请参见第 481 页的"添加主机完整性要求"。

2 在"自定义要求"对话框中,键入要求的名称。

该要求名称就会显示在客户端计算机中。通过此名称,用户会知道要求已通过 还是已失败,或者系统提示其下载软件。

- 3 若要添加条件,请在"自定义的要求脚本"下,单击"添加",然后单击 IF.THEN..。
- 4 通过突出显示 IF 节点下面的空条件,在右窗格中选择一个条件。 主机完整性检查会在客户端计算机上查找该条件。
- 5 在"选择条件"下拉列表中,指定所需的其他信息。
- 6 在"自定义的要求脚本"下,单击 THEN,然后单击"添加"。 THEN 语句提供了条件为 True 时应当执行的操作。
- 7 单击以下任意选项:
  - IF..THEN 使用嵌套的 IF..THEN.. 语句提供其他条件或操作。 请参见第 500 页的"添加 IF THEN 语句"。
  - 函数 使用函数来定义补救操作。

请参见第 497 页的"关于功能"。

Return

使用返回语句来指定条件的评估结果是通过还是失败。每个自定义要求必须以通过或失败语句结束。

- 注释
   使用注释来解释所添加的条件、函数或语句的功能。
   请参见第 501 页的"添加注释"。
- 8 在右窗格中,定义已添加的条件。

有关这些选项的详细信息,请单击"帮助"。

- 9 若要添加更多的嵌套语句、条件或函数,请在"自定义的要求脚本"下,右键 单击节点,然后单击"添加"。
- 10 根据需要重复步骤7至8。
- 11 若要在无论结果如何的情况下都通过主机完整性检查,请选中"即使这项要求 不满足,也允许主机完整性检查通过"。
- 12 配置完此要求后,单击"确定"。

## 添加 IF THEN 语句

IF..THEN 语句定义检查特定条件 (IF) 的结构,以及这些条件评估为 true (THEN) 时 采取的操作。

#### 添加 IF THEN 语句

- 编写自定义要求脚本。
   请参见第 499 页的"编写自定义要求脚本"。
- 2 在"自定义的要求脚本"下,选择下列其中一项:
  - 若要添加第一个 IF THEN 语句,请选择顶级节点。
  - 要在与现有语句相同的级别上添加 IF THEN 语句,请选择 END IF。
  - 要添加嵌套的 IF THEN 语句,请选择要在其下添加该语句的行。
- 3 单击"添加"。
- 4 单击 IF..THEN。

## 在 IF 及 IF NOT 语句之间切换

您可能需要切换检查条件是否存在。

#### 在 IF 及 IF NOT 语句之间更改

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

2 右键单击相应的条件, 然后单击"切换成 NOT"。

## 添加 ELSE 语句

您可以添加 ELSE 语句,确认每当指定的条件判定不成立时,所要采取的操作。

#### 添加 ELSE 语句

- 编写自定义要求脚本。
   请参见第 499 页的"编写自定义要求脚本"。
- 2 在"自定义的要求脚本"下,单击 THEN。
- 3 单击"添加",然后单击 ELSE。

## 添加注释

添加语句(例如IFTHEN语句)时,可以添加注释。使用注释可以解释代码某部分 要执行的操作。注释仅作参考之用。

#### 添加注释

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- 2 在"自定义的要求脚本"下,选择已添加的任何语句,然后单击"添加"。
- 3 单击"注释"。
- 4 单击"//在此处插入语句",然后在右侧窗格的"备注"文本字段中,输入您的注释。

### 复制和粘贴IF语句、条件、函数和注释

您可以在自定义要求内或之间复制并粘贴语句或整个IFTHEN节点。如果您要将这 些项移动至脚本的其他部分,或重复该功能,您可能需要复制和粘贴这些条目。

#### 复制和粘贴 IF 语句

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- 2 在"自定义的要求脚本"下,在相应的脚本项上单击鼠标右键,然后单击"复制"。
- 3 在为空的语句行上单击鼠标右键,然后单击"粘贴"

#### 删除语句、条件或函数

您可以在任何时候删除语句、条件或函数。如果IF节点下只有一个条件语句,则删 除该语句也会删除整个IF THEN 语句。

#### 删除语句、条件或函数

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- 2 在"自定义的要求脚本"下,选择要删除的要求项。
- 3 单击"删除"。
- 4 若请求您确认删除,请单击"是"。

## 显示消息对话框

在自定义主机完整性要求中,您可以指定函数或条件以便为客户端创建一个显示给 用户的消息框。如果用户单击"确定"或"是",此函数或条件就会返回true,否 则会返回 false。

#### 显示消息对话框

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- 2 在"自定义要求"对话框的"自定义的要求脚本"下,选择要在其中添加函数 的节点。
- 3 单击"添加",然后单击"函数"。
- 4 单击"实用程序:显示消息对话框"。

若要插入条件,请选择 IF...Then,接着选择适当的分支,然后选择"实用程 序:消息对话框返回值等于"。

- 5 键入消息框的标题(最长 64 个字符)。
- 6 键入消息框的文本(最长 480 个字符)。

- 7 选择下列图标之一进行显示:"信息"、"问题"、"警告"或"错误"。 图标与文本都会显示。
- 8 选择对话框中显示的按钮集:
  - ∎ 确定
  - 确定并取消
  - 是和否
- 9 为每个按钮集都选择默认按钮。
- 10 若要在无用户交互的状态超过特定时间后关闭消息框并返回默认值,请选中 "达到最长等待时间后关闭消息框要执行的操作",并指定等待时间。 时间值必须大于 0。

下载文件

对于自定义要求,您可以指定必须下载某个文件到客户端计算机。

#### 下载文件

- 编写自定义要求脚本。
   请参见第 499 页的"编写自定义要求脚本"。
- **2** 在"自定义要求"对话框的"自定义的要求脚本"下,选择要在其中添加函数的节点。
- 3 单击"添加",然后单击"函数"。
- 4 单击"文件:下载文件"。
- **5** 输入所下载文件的 URL 位置,以及要将文件下载至的客户端计算机文件夹。 您可以指定 URL 或 UNC 位置。如果使用 URL,可支持 HTTP 和 FTP。
- 6 请选中"显示下载进程对话框",这样用户便可检查文件下载到客户端计算机 的进度。
- 7 如果要让用户能够取消文件下载,请选中"允许用户取消此要求的主机完整 性"。

如果在不适合的时间下载文件,用户可能会丢失工作。

## 生成日志消息

在自定义主机完整性要求中,您可以指定一个记录操作相关消息的函数。此函数可 将指定消息字符串插入客户端安全日志中。该消息会显示在安全日志的详细信息区 域。

#### 生成日志消息

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- 2 在"自定义要求"对话框的"自定义的要求脚本"下,选择要在其中添加函数 的节点。
- 3 单击"添加",然后单击"函数"。
- 4 单击"实用程序:记录消息"。
- 5 在"严重性类型"下拉式列表中,选择下列其中一种日志严重性类型:信息、 主要、次要或重要。
- 6 键入最长为 512 个字符的消息。

## 运行程序

对于自定义主机完整性要求,您可以指定一个让客户端启动程序的函数。

#### 运行程序

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- 2 在"自定义要求"对话框的"自定义的要求脚本"下,选择要在其中添加函数的节点。
- 3 单击"添加",然后单击"函数"。
- 4 单击"实用程序:运行程序"。
- 5 在"执行命令"文本字段中,键入运行脚本的命令。

在执行前环境变量会被替换掉。例如, %windir% 将被替换为 Windows 目录路 径。可以使用 %1 变量执行最后下载的文件。

- 6 在"运行程序"下方,选择下列其中一个选项:
  - 在系统环境中
  - 在登录用户环境中 该执行命令必须包括完整的文件路径,以显示登录的用户。如果没有用户 登录,则结果将失败。
- 7 若要指定允许该执行命令完成的时间,请选择下列其中一个选项:
  - 不等待 如果成功执行,此操作就会返回 true,但它不会等到执行完成。
    - 等到执行完成
- 输入最长时间 输入以秒为单位的时间。如果执行命令没有在指定的时间内完成,则会终 止文件执行。
- 8 此外,您也可以取消选中"显示新进程窗口"。

## 运行脚本

在自定义主机完整性要求中,您可以指定一个使客户端运行脚本的函数。您可以使用脚本语言,如JScript或VBScript,这些语言可通过 Microsoft Windows Script Host运行。

#### 运行脚本

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- **2** 在"自定义要求"对话框的"自定义的要求脚本"下,选择要在其中添加函数的节点。
- 3 单击"添加",然后单击"函数"。
- 4 单击"实用程序:运行脚本"。
- 5 输入脚本的文件名,例如 myscript.js。
- 6 键入脚本的内容。
- 7 在"执行命令"文本字段中,键入运行脚本的命令。

使用%F指定脚本文件名。将在系统环境中执行该脚本。

- 8 若要指定允许该执行命令完成的时间,请选择下列其中一个选项:
  - 不等待 如果成功执行,此操作就会返回 true,但它不会等到执行完成。
  - 等到执行完成
  - 输入最长时间 输入以秒为单位的时间。如果执行命令没有在指定的时间内完成,则会终止文件执行。
- 9 此外,您也可以取消选中"在运行完成或终止之后,删除临时文件"。 如果选中了"不等待",此选项将禁用,因而不可用。
- 10 此外,您也可以取消选中"显示新进程窗口"。

# 设置文件的时间戳

在自定义要求中,您可以通过指定"设置时间戳"函数来创建注册表设置以存储当前的日期和时间。然后可以使用"检查时间戳"条件来确定自创建该时间戳以来, 是否已经过指定的时间长度。

举一个例子:如果您已设置以较短的间隔(如2分钟)运行主机完整性检查,但想 要指定以较长的间隔(如一天)执行操作。在这种情况下,当客户端收到新的配置 文件或用户手动运行主机完整性检查时,将删除存储的时间值。

#### 设置文件的时间戳

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- 2 在"自定义要求"对话框的"自定义的要求脚本"下,选择要在其中添加函数 的节点。
- 3 单击"添加",然后单击"函数"。
- 4 单击"实用程序:设置时间戳"。
- 5 对于将存储日期和时间信息的注册表设置,键入最长为256个字符的名称。

#### 比较当前时间和存储的时间值:

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- 2 在"自定义要求"对话框的"自定义的要求脚本"下,选择要在其中添加条件的节点。
- 3 单击"添加",再按 IF..THEN..。
- 4 单击"实用程序:检查时间戳"。
- 5 键入您之前为保存的时间注册表设置输入的名称。
- 6 以分钟、小时、天或周为单位指定时间长度。

如果指定的时间长度已过或者注册表设置值为空,则"设置时间戳"函数将返回 true 值。

# 指定脚本的等待时间

在自定义主机完整性要求中,您可通过指定相应的函数来使自定义要求脚本等待一 段指定的时间后再运行。

#### 指定脚本的等待时间

1 编写自定义要求脚本。

请参见第 499 页的"编写自定义要求脚本"。

- **2** 在"自定义要求"对话框的"自定义的要求脚本"下,选择要在其中添加函数的节点。
- 3 单击"添加",然后单击"函数"。
- **4** 单击"实用程序:等待"。
- 5 键入要等待的秒数。

508 | 添加自定义要求 | **指定脚本的等待时间** 



本附录包括下列主题:

■ 客户端服务

# 客户端服务

您可以从客户端计算机上的命令行对客户端服务使用smc命令直接操作客户端。您 最好在远程运行参数的脚本中使用此命令。例如,如果您需要停止客户端以在多个 客户端上安装应用程序,便可以先停止再重新启动每项客户端服务。

附录

除了 smc -start 参数之外,客户端服务必须运行,您才能使用命令行参数。命令 行参数不区分大小写。

表 A-1 介绍了如果用户是任何 Windows 用户组的成员,您可以运行的参数。

参数	说明
smc -checkinstallation	检查 smc 客户端服务是否已安装。
	返回 0、-3
smc -checkrunning	检查 smc 客户端服务是否正在运行。
	返回 0、-4
smc -dismissgui	关闭 Symantec Endpoint Protection 或 Symantec Network Access Control 客户端用户界面,包括通知区域图标。
	客户端仍会运行并继续保护客户端计算机。
	返回 0

表 A-1 所有 Windows 成员都可以使用的参数

参数	说明
smc -exportlog	将日志的全部内容导出为.txt文件。
	若要导出日志,请使用下列语法:
	smc -exportlog <i>log_type 0 -1 output_file</i>
	其中:
	log_type 是:
	■ 0 = 系统日志
	■ 1 = 安全日志
	■ 2 = 通信日志 ■ 2 = 数据句日志
	■ 5 - <del>奴</del> 始也日心 ■ 4 = 控制日志
	例如,您可以键入下列语法:
	<pre>smc -exportlog 2 0 -1 c:\temp\TrafficLog</pre>
	其中: ○ 为文件的开头
	-1 为文件的结尾
	仅可导出控制日志、数据包日志、安全日志、系统日志和通信 日志。
	output_file是您分配给导出后文件的路径名称和文件名称。
	返回 0、-2、-5
smc -runhi	如果已安装 Symantec Network Access Control,则运行主机完整性检查。
	返回 0
smc -showgui	显示 Symantec Endpoint Protection 或 Symantec Network Access Control 客户端用户界面。
	返回 0
smc -updateconfig	检查管理服务器上的配置文件是否比客户端上的配置文件更新。 配置文件包括管理服务器上的所有设置,例如策略、组、日志设 置、安全设置以及用户界面设置。
	如果客户端配置文件过期, updateconfig 会下载最新的配置文件,并替换现有的配置文件,也就是 serdef.dat。
	返回 0

只有在满足下列条件时,才能运行表A-2中的参数:

■ 客户端运行 Windows 2003/XP/Vista 或 Windows Server 2008, 且用户为 Windows 管理员组的成员。

■ 客户端运行 Windows 2003/XP, 且用户为超级用户组的成员。

如果客户端运行的是 Windows Vista, 且启用了"用户帐户控制",则用户会自动同时成为管理员组和用户组的成员。若要使用下列参数,用户必须仅为管理员组的成员。

参数	说明
smc -exportconfig	将客户端的配置文件导出至.xml文件。配置文件包括管理服务器 上的所有设置,例如策略、组、日志设置、安全设置以及用户界 面设置。
	您必须指定路径名称和文件名。例如,您可以输入下列命令:
	smc -exportconfig C:\My Documents\MyCompanyprofile.xml
	返回 0、-1、-5、-6
smc -importconfig	将客户端的当前配置文件的内容替换为导入的配置文件。客户端 必须运行才能导入配置文件的内容。
	您必须指定路径名称和文件名。例如,您可以输入下列命令:
	smc -importconfig C:\My Documents\MyCompanyprofile.xml。
	返回 0、-1、-5、-6
smc -exportadvrule	将客户端的防火墙规则导出为.sar文件。导出的规则只能够导入 至处于客户端控制模式或混合模式的非受管客户端或受管客户端。 处于服务器控制模式的受管客户端会忽略这些规则。
	您必须指定路径名称和文件名。例如,您可以输入下列命令:
	smc -exportadvrule C:\myrules.sar
	返回 0、-1、-5、-6

参数	说明
smc -importadvrule	将导入的防火墙规则添加到客户端现有的防火墙规则列表。这些 规则不会覆盖现有的规则。客户端会同时列出现有规则和导入的 规则,即使每个规则的名称和参数都相同也同样如此。
	您只能将防火墙规则导入至处于客户端控制模式或混合模式的非 受管客户端或受管客户端。处于服务器控制模式的受管客户端会 忽略这些规则。
	若要导入防火墙规则,请导入.sar 文件。例如,您可以输入下列 命令:
	smc -importadvrule C:\myrules.sar
	导入规则之后,系统日志会添加一个条目。
	返回 0、-1、-5、-6
smc -start	启动 Symantec Endpoint Protection 或 Symantec Network Access Control 客户端服务。
	返回 0、-1
smc -stop	停止 Symantec Endpoint Protection 或 Symantec Network Access Control 客户端服务,并从内存卸载。
	返回 0、-1

当您导入配置文件和防火墙规则时,请注意遵守下列规则:

- 您不能直接从映射网络驱动器导入配置文件或防火墙规则文件。
- 客户端不支持 UNC (通用命名约定)路径。

## 错误代码

表 A-3 显示必要参数无效或丢失时 smc 命令返回的错误代码。

表A-3	Smc 错误代码
错误代码	说明
0	命令成功。
-1	用户不属于 Windows 管理员组或 Windows 超级用户组。如果客户端 运行 Windows Vista,则用户不是 Windows 管理员组的成员。
-2	参数无效。 您键人的参数可能错误,或者在参数后方附加了不正确的参数。
-3	未安装 smc 客户端服务。

错误代码	说明
-4	未运行 smc 客户端服务。
-5	输入文件无效。 例如, importconfig、exportconfig、updateconfig、 importadv、exportadvrule、与exportlog参数需要正确的路径 名与文件名
-6	输入文件不存在。 例如, importconfig、updateconfig与 importadvrule 参数需要正确的路径名、配置文件名 (.xml) 或防火墙规则文件名 (.sar)。

## 在客户端有密码防护时键入参数

如果您或其他用户都可以停止客户端服务,或者导入或导出配置文件,则可以在客户端上设置密码保护。如果客户端使用下列参数进行了密码保护,则您必须键入相应的密码:

-stop 客户端会在您或用户停止客户端之前,请求输入密码。

-importconfig 客户端会在您导入配置文件之前,请求输入密码。

-exportconfig 客户端会在您导出配置文件之前,请求输入密码。

请参见第105页的"使用密码保护客户端"。

注意:密码不得超过15个字符。

#### 在客户端有密码防护时键入参数

- 1 在客户端计算机的任务栏, 单击"开始" > "运行"。
- 2 在"运行"对话框中,键入 cmd。

```
3 在 Windows MS-DOS 提示符下,键人下列任一参数:
smc -parameter-p password
smc -p password -parameter
其中:
parameter 为 -stop、-importconfig 或 -exportconfig。
password 是您在控制台中指定的密码。
例如,您可以键人下列任一语法:
smc -exportconfig c:\profile.xml -p password 或
smc -p password-exportconfig c:\profile.xml
4 关闭命令提示符。
```



# 关于客户端和服务器通信 设置

本附录包括下列主题:

■ 关于客户端和服务器通信设置

# 关于客户端和服务器通信设置

客户端与服务器之间的通信设置以及其他客户端设置存储在客户端计算机的文件 中。

表B-1	客户端文件
文件名	说明
SerDef.dat	依照位置存储通信设置的加密文件。每当用户更改位置时,系统便会读取 SerDef.dat 文件并将适用该新位置的通信设置应用到 客户端。
sylink.xml	存储全局通信设置。此文件仅供内部使用,不可以编辑。其中包括 Symantec Endpoint Protection Manager 的设置。如果 编辑此文件, 则大部分的设置会由客户端下次连接的管理服务器的设置所覆盖。
SerState.dat	存储用户界面相关信息的加密文件,例如客户端的屏幕大小、是否显示 网络威胁防护的客户端控制台,以及是否显示 Windows 服务。客户端 启动时,会读取此文件并回到停止前的相同用户界面状态。

516 | 关于客户端和服务器通信设置 | 关于客户端和服务器通信设置



#### 符号

{first-level index term} 92

#### A

Active Directory 服务器 导入用户信息 42 过滤 215 Active Directory 域控制器 自动排除 319 安全风险 313 另请参见风险 操作 312 关于操作 326 进程持续下载 318 配置操作 334 扫描时忽略 334 安全响应中心网站 Symantec Endpoint Protection 从主页访问 129 按需扫描 高级选项 364 配置 361 扫描进度选项 363 运行 362

#### В

Bot 314 报告 155 *另请参见* 调度报告 Symantec Endpoint Protection 主页 123 Symantec Network Access Control 主页 130 保存 154 保存配置设置 153 打印 154 风险 145, 192 概述 119 过去 24 小时过滤器 134

基础篇 118 计算机状态 142,189 快速 140 类型 119 配置过滤器 119 日志 159 扫描 147,193 删除配置设置 153 设备控制 141 审核 141,187 网络威胁防护 144,191 系统 148.194 应用程序控制 141 应用程序与设备控制 186 重要须知 149 主动型威胁防护 192 主页首选项 132 遵从性 141,187 报告收藏夹 Symantec Endpoint Protection 自定义 128 备份 Microsoft SQL 数据库, 从控制台 238 控制台的嵌入式数据库 242 使用 Microsoft SQL 向导备份 Microsoft SQL 数 据库 239 数据库 236 病毒 313-314 操作 312 关于操作 326 配置操作 334 病毒爆发计划 308 拨号程序 315 补救 主机完整性 487 等待时间 488 推迟 488 文件 487 应用程序 487 部署 使用查找非受管计算机 75

#### С

CGI 错误 数据库 256 ClassGuid 450 操作系统的条件 主机完整性要求 495 测试模式 434,446 策略 LiveUpdate 89 编辑 288 编辑共享 策略页面 288 撤回 289 导出共享 策略页面 291 导入 292 导入策略文件 512 非共享 283 分配共享 289 共享 283 关于 282 继承 44 默认 282 删除非共享 291 删除共享 290 添加非共享 从已导出 287 客户端页面 285-286 添加共享 策略页面 284 从现有共享 287 查找非受管计算机客户端部署工具 75 招时参数 数据库 255 撤回 策略 289 触发器 防火墙规则 371 网络服务 373 网络适配器 374 应用程序 371 主机 372

#### D

Default 组 41 DER 和 PEM 格式 232 DHCP 通信 384 DNS 通信 384 打印共享 406 代理服务器 FTP 225 **HTTP 225** 当前域 61 导出 策略 291 防火墙规则 382 管理服务器列表 113 客户端安装软件包 73 导入 LDAP 目录服务器搜索返回的用户信息 220 策略 292 策略文件 限制 512 防火墙规则 382 限制 512 来自 LDAP 服务器的用户信息 217 主机完整性策略要求 模板及 483 组织单位 221 等待洗项 主机完整性补救 488 第三方 密码 209 第三方内容分发 对受管客户端 95 非受管客户端的注册表项要求 97 关于 95 使用 LiveUpdate 策略启用 95 用于非受管客户端 97 电子邮件 350,357 另请参见 Internet 电子邮件自动防护 另请参见受感染电子邮件 防火墙规则 413 调度 按需备份 Microsoft SQL 数据库 238 按需嵌入式数据库备份 242 使用数据库维护向导按需备份 Microsoft SQL 数 据库 239 添加到规则 411 自动数据库备份 242 调度报告 155 另请参见 报告 创建 156 关于 155 删除 157 修改 156 调度扫描 320 另请参见扫描

保存为模板 360 高级选项 364 关于 320 扫描进度选项 363 添加到策略 360 定义文件 更新之后扫描 322 配置新定义的操作 342 显示过期或丢失 331 对等验证 385

#### Ε

ELSE 语句 501 Enforcer 还原主机完整性 487

## F

FTP 代理服务器 225 防病毒和防间谍软件策略 调度扫描 360 高安全性策略 312 高性能策略 311 关于 311 管理客户端交互 328 旧版客户端 312 默认策略 311 设置 Windows 安全中心选项 329 设置日志处理 327 使用 313 锁定设置 312 提交洗项 337 防病毒和防间谍软件防护 基础篇 308 锁定和解除锁定功能 100 防病毒洗项 主机完整性要求 492 防篡改 管理 267 集中式例外 465,470 锁定和解除锁定功能 100 消息 268 防火墙 关于 368 通信设置 385 通知 412 主机完整性要求 493 防火墙策略 关于 369

防火墙规则 部分 370 操作 371 处理顺序 374 更改 383 触发器 371 导出 382 导入 382 限制 512 电子邮件 413 调度 添加 411 服务器 376 复制 383 更改顺序 383 关于 370, 376 继承 375,381 禁用 383 客户端 376 列表 375 启用 383 添加 使用空白规则 378 使用向导 380 条件 371 网络服务 编辑和删除 405 添加 404-405 网络服务触发器 373 网络适配器 编辑和删除 409 添加 408 网络适配器触发器 374 应用程序 371 添加 410 粘贴 383 主机 372 主机组 编辑和删除 402 创建 401 添加 403 防火墙规则向导 380 防火墙日志和报告. 请参见网络威胁防护 防间谍软件选项 主机完整性要求 493 访问权限 64 非共享策略. 请参见策略 非受管客户端 使用第三方工具分发更新 97

风险 314 另请参见安全风险 报告 145,192 检测 314 排除 196 日志 164.192 从隔离区删除文件 173 风险跟踪程序 349 禁止 IP 地址 350 服务 编辑和删除 405 添加 404 添加到规则 405 服务器 FTP 代理 225 HTTP 代理 225 管理 209 规则 376 目录 215 日志 250 添加目录服务器 216 服务器控制 101 服务器设置 导出和导入 212 辅助技术 创建集中式例外 465, 470, 472 父组. 请参见继承 复制 LiveUpdate 和 87 按需调度 262 断开复制伙伴的连接 262 概述 257 客户端软件包 264 频率 263 日志 264 设置 安装后 257 初始 257 示例 259 示例图 258 数据合并 260 添加复制伙伴 260 通信设置 259

#### G

GUID 作为设备控制 436 隔离区 本地目录 340

关于 313 管理项目 313 将项目发送至 Symantec 342 将项目转发至中央隔离服务器 341 清除洗项 340 删除文件 173 设置 339 跟踪软件 316 功能 等待 506 记录消息 503 设置时间戳 506 下载文件 503 显示消息对话框 502 运行程序 504 运行脚本 505 攻击 禁止 367,392 特征 387 共享策略. 请参见策略 共享文件和打印机 406 挂锁图标 100 管理 域 61 管理的设置 锁定和解除锁定 100 在客户端上配置 99 管理服务器 编辑 111 管理服务器列表 编辑 111 导出和导入 113 分配给组和位置 110 服务器优先级 112 复制 113 关于 108 默认列表 108 替换 113 添加 109 显示分配的组和位置 110 粘贴 113 指定给组 108 管理服务器配置向导 236 管理员 登录失败后锁定帐户 67 访问权限 64 更改密码 68 关于 62 类型 62

切换类型 66 删除 69 添加 63 验证 67 重命名 68 管理员定义的扫描 359 *另请参见* 按需扫描 *另请参见* 调度扫描 广告软件 315 规则.*请参见* 防火墙规则 规则优先级 应用程序与设备控制策略 445 过滤器 保存在日志中 170 用户和计算机 53

#### Η

HTTP 代理服务器 225 HTTP 协议 109 HTTPS 协议 109 黑客工具 315 汇总 250 混合控制 102 关于 103 配置网络威胁防护设置 400 混合型威胁 314 活动响应 设置 392

## I

ICMP 通信 377 IF THEN 语句 500 IF 条件语句 502 Internet Bot 314 Internet 电子邮件自动防护 350 IPS 例外 390 **IPS** 特征 Symantec 更改行为 390 关于 388 例外 390 自定义 变量 397 创建 393 复制并粘贴 396 更改顺序 396 关于 388 将库分配给组 395

库 394-395 生成库 394 IPS 引擎 387 流式 388 数据包式 388 IPv4 404 IPv6 404

#### J

JKS Keystore 文件 231 集中式例外 463 另请参见集中式例外策略 TruScan 主动型威胁扫描事件 472 防篡改 465.470 防篡改事件 472 风险事件 471 辅助技术应用程序 470,472 扩展名 468 强制 TruScan 检测 469 文件 467 文件夹 467 已检测到的进程 469 已知安全风险 467 针对 TruScan 主动型威胁扫描 465,468 针对防病毒和防间谍软件扫描 464 主动型威胁扫描 424 集中式例外策略 463 另请参见集中式例外 TruScan 主动型威胁扫描的例外 468 从日志事件创建例外 471 防病毒和防间谍软件扫描的例外 466 客户端交互 465 客户端限制 470 配置 466 使用 464 计算机 搜索 54 计算机模式 45 计算机状态 报告 142,189 杳看 51 日志 163,189 继承 策略 44 覆盖 44 防火墙规则 375,381 启用 44 位置 覆盖 44

继承的策略 移动组的方式 43 加密 231 间谍软件 315 检测率 将信息发送到 Symantec 338 检查. 请参见状态检查 将威胁信息发送到 Symantec 337 禁止 客户端添加至组 49 禁止攻击计算机 392 警告消息 示例 336 添加到受感染的电子邮件中 355 在受感染的计算机上显示 336 旧版客户端 防病毒和防间谍软件策略 312

#### Κ

考虑事项 切换模式 47 可疑文件 312 客户端 264 另请参见复制 定义 45 更新 第三方分发工具 95 智能更新程序 94 规则 376 控制日志 437 密码保护 105 命令 509 软件包复制 264 删除升级软件包 77 脱机 199 用户界面 访问 99 配置 100-101,103 客户端安装软件包 导出 73 关于 71 配置 72 收集用户信息 73 添加 76 添加更新 76 客户端的类型 45 客户端计算机 模式 45 客户端控制 101

客户端类型 45 客户端数据 搜索 54 客户端状态 查看 51 空白规则 378 控制级别 101 控制台 增加超时时间段 205 库. *请参见* IPS 特征 快速报告 创建 153 基本过滤器设置 151 扩展名 扫描选定 332

### L

LDAP 目录服务器 导入 用户信息来源 217.220 组织单位 221 过滤 215 搜索用户 217 LDAP 协议 217 LiveUpdate LiveUpdate 管理员 82 MSI和MSP文件 87 策略 关于 89 配置 89-90 第三方分发选项 82 分发内容 81 更新定义与内容 80 **更新类型 80** 关于更新内容 81 内容修订 85 配置内容策略 90 配置设置策略 89 配置下载更新的站点 87 配置组更新提供者 93 使用第三方分发工具而非 95 使用复制 87 特征及定义 80 智能更新程序 94 类ID 关于 449 例外 463 另请参见集中式例外 IPS 特征 390

零时差攻击 419

#### Μ

Microsoft Exchange 服务器 自动排除 319 Microsoft SQL 管理数据库 235 MSI 文件 87 MSP 文件 87 My Company 组 41 密码 第三方 209 密码保护 参数 513 更改密码 328 客户端 105 扫描映射的驱动器 328 密码更改 管理员 68 命令 从日志运行 173 客户端 509 通过控制台在客户端上运行 56 模板 用于调度扫描 360 模式 446 客户端计算机 45 默认策略 282 目录服务器 关于 215 添加 216 同步 216 内容 不是最新版的修订 86 分发方法 81-82 关于存储修订 85 客户端与管理服务器的更新 81 使用默认管理服务器更新客户端 86 随机进行 86

#### Ρ

PC-cillin 371 PKCS12 Keystore 文件 231 排除. *请参见* 集中式例外 自动创建 318 排除主机 392 屏幕读取器 防篡改禁止的应用程序 465

## Q

其他风险类别 315 取消 主机完整性补救 488

#### R

Rootkit 313 RSA SecurID 验证前提条件 67 RSA 服务器 配置 SecurID 验证 228 与 Symantec Endpoint Protection Manager 配合 使用 227 日志 159,187 TruScan 主动型威胁扫描 164, 192 保存过滤器配置 170 查看 167 从数据库清除 249 存储区 248 导出数据 176 风险 164,192 从隔离区删除文件 173 服务器 配置大小 250 复制 169 关于 121 管理 254 过滤 170 过去 24 小时过滤器 170 计算机状态 163,189 客户端 配置大小 251 客户端控制日志 437 类型 160 扫描 164,193 删除配置设置 171 审核 161 事件详细信息 169 数据库错误 168 数据库维护 选项 254 刷新 168 通知 165 网络威胁防护 164,191 系统 164,194 应用程序与设备控制 161,186 远程查看 169 远程访问 169 运行命令从 173

遵从性 162,187 蠕虫 314 入侵防护 关于 368,387 禁止攻击计算机 392 配置 389 启用 390 通知 412 在指定的计算机上禁用 392

#### S

SecurID 验证 为管理员指定 229 在管理服务器上配置 228 smc 命令 关于 509 Symantec Database Backup and Restore 实用程序 236 Symantec Endpoint Protection Manager 删除 多重安装 212 自动服务启动 210 Symantec 安全响应中心 309 提交 338 Symantec 产品 自动排除 319 扫描 320 另请参见调度扫描 按需运行 362 报告 147.193 防病毒和防间谍软件 332 集中式例外 464 关于 316 管理员定义的扫描的高级选项 364 建议的文件扩展名 323 将文件排除在扫描范围之外 326 日志 164.193 扫描进度选项 363 停止 363 选择要扫描的文件及文件夹 322 延缓 363 在客户端上显示警告消息 336 暂停 363 指定操作 326 自动防护 316 删除 管理员 69 设备 ID 450 关于 449 作为设备控制 436

设备级别控制 报告 141 应用程序与设备控制 436 设置 防火墙 369.385 网络威胁防护 400 审核 报告 141 日志 161 升级客户端 76 升级一个或多个组中的客户端 77 生产模式 434,446 事件 关于 120 汇总 250-251 数据库维护 选项 254 事件日志 167 过去 24 小时过滤器 134,170 适配器. 请参见 网络适配器 收集用户信息 73 手动扫描. 请参见按需扫描 首诜项 报告 132 受感染的计算机 显示自动防护结果于 354 受感染电子邮件 將警告添加到 355 通知发件人 356 通知其他人 357 受限管理员 关于 63 配置访问权限 65 属性 组 43 数据库 CGI 错误 256 Microsoft SQL bcp.exe 文件 246 命名惯例 236 Symantec Database Backup and Restore 实用程 序 236 备份 236 自动 242 编辑 名称 245 说明 245 错误 255 大小 236

调度自动备份 242 更改超时参数 255 管理 235 管理服务器配置向导 236 还原 步骤 243 嵌入式 命名惯例 236 维护 254 终止进程错误 256 重新配置 237 Microsoft SQL 245 嵌入式 247 搜索 组、用户和计算机 54 搜索应用程序 自定义要求 494 锁定 挂锁图标 100 在"防病毒和防间谍软件策略"中 312 锁定和解除锁定设置 客户端 100

#### Т

TCP 通信 377 Trend Micro PC-cillin 371 TruScan 将信息发送到 Symantec 337 TruScan 主动型威胁扫描 Symantec 默认设置 420 操作 427 隔离区 424 管理检测 425 忽略进程 424 集中式例外 424, 465, 468 检测进程 421 进程 427 敏感级别 427 默认设置 420 频率 428 强制检测 425,469 日志 164, 192 商业应用程序 428 通知 429 误报 422 特洛伊木马 314,414 特征. 请参见 IPS 特征 特征的变量 397

提交 338 发送至中央隔离服务器 341 将项目发送至 Symantec 342 将信息发送到 Symantec 337 配置洗项 339 添加 管理员 63 添加组 42 通信 启用智能通信 384 设置 385 通信设置 客户端和服务器 515 通知 TruScan 主动型威胁扫描 429 日志 165 网络威胁防护 412 主机完整性检查 486 自动防护选项 353 通知消息 针对防病毒和防间谍软件扫描 335 同步 目录服务器 216 组织单位 221 图标 挂锁 100 脱机客户端 199

#### U

UDP 通信 378 URL 出现在错误通知 331 指定浏览器主页 332

#### W

Windows GUID 类 ID 450 Windows 安全中心 329 定义的过期时间 330 禁用 329 警报 329 WINS 通信 384 外部记录 176 玩笑程序 315 网络服务 编辑 405 触发器 373 删除 405

添加到规则 405 添加到默认列表 404 网络适配器 编辑和删除 409 触发器 374 添加到规则 408 添加到默认列表 408 网络体系结构选项 更新的第三方管理 82 网络威胁防护 报告 144,191 创建通知 412 概述 367 禁用 400 启用 400 日志 164,191 针对混合控制配置 400 网络应用程序监控 414 威胁 192.367 另请参见网络威胁防护 另请参见主动型威胁防护 混合型 314 位置继承 44 文件 共享 406 为满足主机完整性而还原 487 主机完整性要求中的选项 493 自扫描排除 326 文件高速缓存 文件系统自动防护 350 文件夹 扫描选定 333 文件系统自动防护. 请参见 自动防护 文件指纹 452 误报 389.422 最大程度地最少 393

#### Х

XML 服务器设置 212 系统 报告 148, 194 日志 164, 194 系统管理员 关于 62 系统锁定 启用 457 显示用户和计算机属性 52 协议
HTTP 109
HTTPS 109,231
LDAP 217
编辑和删除 405
添加 404
添加到规则 405
虚拟机
随机进行同时内容下载 87

## Y

验证 对等 385 针对管理员 67 证书 231 移动 组 43 移动用户和计算机 关于 50 疑难解答 使用查找非受管计算机 75 已知应用程序 410 另请参见应用程序 保存搜索结果 303 关于 299 列表 410 启用 300-301 搜索 301 隐藏设置 385 应用程序 410 另请参见已知应用程序 定义 410 监控网络应用程序 414 授权 456 搜索 301.410 添加到规则 410 为满足主机完整性而还原 487 主机完整性要求中的选项 493 应用程序触发器 防火墙规则 371 应用程序级别控制 433 应用程序控制 配置 439 应用程序控制规则集 模式 434,446 设置优先级 445 应用程序与设备控制 报告 141,186 规则 435

日志 161, 186, 437 应用程序与设备控制策略 37 创建 438 规则 禁用 445 优先级 445 结构 432 控制类型 431 使用 437 用户 搜索 54 添加到组 46 用户和计算机 过滤 53 用户和计算机属性 显示 52 用户界面 关于 99 配置 100-101,103 用户控制级别 101 用户模式 45 用户信息 收集 73 域 当前 61 添加 61 域管理员 62 远程访问程序 315 远程控制台 授予访问 210

#### Ζ

证书 JKS Keystore 文件 231 PKCS12 Keystore 文件 231 服务器 231 更新 232 数字 231 证书和私钥文件(DER 或 PEM 格式) 232 知识库 309 智能通信过滤 384 终止进程错误 数据库 256 重命名 管理员 68 组 43 重新配置 Microsoft SQL 数据库 245 嵌入式数据库 247

数据库 237 重新启动命令 56 主动型威胁防护 419 报告 192 关于 37 主动型威胁扫描. 请参见 TruScan 主动型威胁扫描 主机 本地/远程 372 从入侵防护排除 392 添加到规则 403 源/目标 372 主机触发器 防火墙规则 372 主机完整性 关于 38 主机完整性策略 创建 481 共享 481 关于 481 还原主机完整性 487-488 Enforcer 设置 487 推迟 488 使用 479 要求 定义 480 即使条件不满足仍通过 485 类型 481 模板 483 排序 483 启用和禁用 **483** 示例 478 自定义要求 编写 499 操作系统的条件 495 等待洗项 506 防病毒的条件 492 防火墙的条件 493 防间谍软件的条件 493 关于 491 日志消息 503 设置时间戳 506 文件洗项 493 下载文件 503 消息框 502 运行程序 504 运行脚本 505 注册表选项 496 自我强制执行 477

主机完整性检查 策略更改 484 记录详细信息 486 强制通过 485 设置 484 通知 486 主机组 编辑 402 创建 401 删除 402 添加到规则 403 主页 Symantec Endpoint Protection 安全响应中心链接 129 关于 123 使用 124 自定义 128 Symantec Network Access Control 关于 130 使用 130 注册表选项 主机完整性要求 496 状态 客户端与计算机 51 状态检查 创建通信规则 377 关于 377 自定义要求 AND、OR 关键字 498 ELSE 语句 498, 501 IF、THEN、ENDIF 语句 498 NOT 关键字 498 RETURN 语句 498 编写 499 复制语句 501 功能 497 关于 491 删除语句 502 条件 492 注释 501 自动防护 Lotus Notes 352 Microsoft Outlook 352 安全风险扫描与禁止 348 高级扫描和监控选项 348 类型 345 配置 345 配置进度通知 358 配置通知选项 353

扫描 316 适用于 Internet 电子邮件 350 文件高速缓存 350 在受感染的计算机上显示结果 354 针对文件系统 配置 347 启用 346 自动排除 Microsoft Exchange Server 的 319 关于 318 为 Active Directory 域控制器 319 为 Symantec 产品 319 组 定义 40 分配管理服务器列表 110 禁止 49 默认 41 搜索 54 添加 42 添加计算机 46 移动 43 在客户端安装软件包中 41 指定管理服务器列表 108 重命名 43 组更新提供者 端口和通信 93 在"设置策略"中配置 93 组继承. 请参见继承 组结构 关于 40 组属性 查看 43 组织单位 导入 42,221 同步 221 遵从性 报告 141,187 日志 162,187