

Symantec™ Data Loss Prevention 管理指南

11.6 版



Symantec Data Loss Prevention 管理指南

本书所述软件按授权许可协议提供，使用时必须遵循许可协议的条款。

文档版本：11.6

法律声明

Copyright © 2012 Symantec Corporation. © 2012 年 Symantec Corporation 版权所有。All rights reserved. 保留所有权利。

Symantec、Symantec 徽标是 Symantec Corporation 或其附属机构在美国和其他国家/地区的商标或注册商标。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源或免费软件许可所规定的任何权利或义务。有关第三方程序的更多信息，请参见本 Symantec 产品附带的“第三方许可证协议”文档。

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，不得以任何形式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，除非此类免责声明的范围在法律上视为无效。Symantec Corporation（赛门铁克公司）不对任何与性能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
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

技术支持

Symantec 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编写我们的联机知识库文章。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
- 升级保证可保证软件顺利升级
- 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：

<http://www.symantec.com/zh/cn/support/index.jsp>

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：

<http://www.symantec.com/zh/cn/support/index.jsp>

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。而且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：

https://licensing.symantec.com/acctmgmt/index.jsp?localeStr=zh_CN

客户服务

可从以下网站获得客户服务信息：

<http://www.symantec.com/zh/cn/support/index.jsp>

客户服务可帮助您解决一些非技术性问题，例如以下几类问题：

- 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
- 有关升级保障和维护合同的信息
- Symantec 采购计划的相关信息
- 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：

国家/地区	销售热线	电子邮件
中国大陆	800 810 8826	China-Sales@symantec.com
中国台湾	0080 1611 391	Taiwan-Sales@symantec.com
中国香港特别行政区	800 963 421	HongKong-Sales@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：

安全托管服务	托管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：

<http://www.symantec.com/zh/cn>

目录

技术支持	3
部分 1 快速入门	39
第 1 章 Symantec Data Loss Prevention 简介	41
关于 Symantec Data Loss Prevention	41
关于 Enforce 平台	43
关于 Network Monitor 和 Prevent	44
关于 Network Discover	45
关于 Network Protect	45
关于 Endpoint Discover	46
关于 Endpoint Prevent	46
关于 Symantec Data Loss Prevention for Mobile	47
关于 Symantec Enterprise Vault 数据分类服务	47
第 2 章 快速了解如何管理 Symantec Data Loss Prevention	49
关于 Symantec Data Loss Prevention 管理	49
关于 Enforce Server 管理控制台	50
登录和注销 Enforce Server 管理控制台	51
关于 Administrator 帐户	51
执行初始设置任务	52
更改 Administrator 密码	52
为 Administrator 添加电子邮件帐户	53
编辑用户配置文件	54
更改密码	56
第 3 章 使用语言和区域设置	57
关于字符集、语言和区域设置支持	57
支持的检测语言	58
使用国际字符	60
关于 Symantec Data Loss Prevention 语言包	61
关于区域设置	61
在 Enforce Server 管理控制台上使用非英文语言	62

使用 Language Pack Utility	63
部分 2 管理 Enforce Server 平台	67
第 4 章 管理 Enforce Server 服务和设置	69
关于 Enforce Server 服务	69
关于在 Windows 上启动和停止服务	70
在 Windows 上启动 Enforce Server	70
在 Windows 上停止 Enforce Server	70
在 Windows 上启动检测服务器	71
在 Windows 上停止检测服务器	71
在单层 Windows 安装上启动服务	72
在单层 Windows 安装上停止服务	72
在 Linux 上启动和停止服务	73
在 Linux 上启动 Enforce Server	73
在 Linux 上停止 Enforce Server	74
在 Linux 上启动检测服务器	74
在 Linux 上停止检测服务器	74
在单层 Linux 安装上启动服务	75
在 Linux 单层安装上停止服务	75
第 5 章 管理角色和用户	77
关于基于角色的访问控制	77
关于对用户进行身份验证	78
关于配置角色和用户	81
关于建议的组织角色	82
解决方案软件包包括的角色	83
配置角色	85
配置用户帐户	91
配置密码强制实施设置	95
重置管理员密码	95
管理和添加角色	96
管理和添加用户	97
集成 Active Directory 以进行用户身份验证	97
创建 Active Directory 集成的配置文件	98
验证 Active Directory 连接	100
为 Active Directory 身份验证配置 Enforce Server	101
关于配置证书身份验证	102
为 Enforce Server 管理控制台配置证书身份验证	104
将证书颁发机构 (CA) 证书添加到 Tomcat 信任存储区	105

将常见名称 (CN) 值映射到 Symantec Data Loss Prevention 用户帐户	108
关于证书吊销检查	108
排除证书身份验证故障	113
禁用密码身份验证和基于表单的登录	114
第 6 章 连接到组目录	115
关于连接到目录组服务器	486
配置目录服务器连接	116
计划目录服务器索引编制	118
第 7 章 管理存储的凭据	121
关于凭据存储	121
将新凭据添加到凭据存储中	121
配置端点凭据	122
管理凭据存储中的凭据	123
第 8 章 管理系统事件和消息	125
关于系统事件	125
系统事件报告	126
使用保存的系统报告	128
服务器事件详细信息	129
配置触发事件的阈值	130
关于系统事件响应	132
启用 Syslog 服务器	134
关于系统警报	135
配置 Enforce Server 以发送电子邮件警报	135
配置系统警报	136
关于日志查看	138
系统事件代码和消息	138
第 9 章 添加新的产品模块	151
安装新的许可证文件	151
关于系统升级	152
第 10 章 集成 Enforce 与 Symantec Protection Center (SPC)	153
关于 Symantec Protection Center (SPC)	153
关于 Enforce Server 与 SPC 集成	154
Enforce Server 与 SPC 集成的注意事项和要求	154

将 Enforce Server 与 SPC 集成	155
第 11 章 将 Symantec Data Loss Prevention 服务器迁移到 64 位操作系统	163
将 Symantec Data Loss Prevention 服务器从 32 位操作系统迁移到 64 位操作系统	163
将 Enforce Server 迁移到 64 位操作系统	165
将检测服务器迁移到 64 位操作系统	168
部分 3 管理检测服务器	171
第 12 章 安装和管理检测服务器	173
关于管理 Symantec Data Loss Prevention 服务器	173
启用高级进程控制	174
服务器控件	175
服务器配置 - 基本	176
Network Monitor Server - 基本配置	177
Network Prevent for Email Server - 基本配置	179
Network Prevent for Web Server - 基本配置	182
Network Discover Server 和 Network Protect - 基本配置	184
Endpoint Server - 基本配置	185
分类服务器 - 基本配置	186
服务器配置 - 高级	187
添加检测服务器	187
删除服务器	189
将 SSL 证书导入到 Enforce Server 或发现服务器	190
关于系统概述屏幕	191
服务器状态概述	191
最近的错误和警告事件列表	193
“服务器详细信息”屏幕	194
高级服务器设置	195
高级代理设置	218
第 13 章 管理日志文件	233
关于日志文件	233
操作日志文件	234
调试日志文件	236
日志收集和配置屏幕	240
配置服务器日志记录行为	240
收集服务器日志和配置文件	244
关于日志事件代码	248

第 14 章

Network and Mobile Prevent for Web 操作日志文件和事件代码	248
Network and Mobile Prevent for Web 访问日志文件和字段	250
Network and Mobile Prevent for Web 协议调试日志文件	252
Network Prevent for Email 日志级别	252
Network Prevent for Email 操作日志代码	253
Network Prevent for Email 产生的响应和代码	256
使用 Symantec Data Loss Prevention 实用程序序	259
关于 Symantec Data Loss Prevention 实用程序	259
关于端点实用程序	260
关于环境检查实用程序	261
在 Windows 上运行环境检查实用程序	262
在 Linux 上运行环境检查实用程序	262
关于环境检查实用程序输出	263
关于 DBPasswordChanger	263
DBPasswordChanger 语法	264
使用 DBPasswordChanger 的示例	264
关于 sslkeytool 实用程序和服务器证书	264
关于 sslkeytool 命令行选项	265
使用 sslkeytool 生成新的 Enforce Server 证书和检测服务器证书	266
使用 sslkeytool 添加新的检测服务器证书	268
验证服务器证书用法	269
关于 SQL 预索引器	269
SQL 预索引器命令功能和选项	270
排除预索引错误	271
关于远程 EDM 索引器	272
远程 EDM 索引器的系统要求	272
使用远程 EDM 索引器	272
安装远程 EDM 索引器	273
从命令行进行安装（适用于 Linux）	274
创建 EDM 配置文件以便远程编制索引	275
远程 EDM 索引器命令选项	277
复制和使用生成的索引文件	278
疑难解答索引作业	278
在 Windows 平台上卸载远程索引器	279
在 Linux 平台上卸载远程索引器	279

部分 4	实施策略检测	281
第 15 章	检测数据丢失	283
	策略检测简介	283
	关于可检测的内容	283
	关于可检测的文件属性	284
	关于可监控的协议	284
	关于可检测的端点事件	284
	关于可检测的身份	285
	关于可检测的语言	285
	可用检测技术	285
	关于确切数据匹配	286
	关于索引文档匹配	287
	关于向量机学习	287
	关于指定内容匹配	288
	关于目录组匹配	288
	关于自定义检测	289
	检测规则简介	290
	内容匹配条件	290
	文件属性匹配条件	291
	网络协议匹配	292
	端点匹配条件	293
	组（身份）匹配条件	293
	关于可以匹配的邮件组件	294
	关于规则严重性	295
	关于规则例外	296
	关于复合匹配条件	297
	关于检测服务器策略执行	297
	实施策略检测	299
	关于制定数据泄露防护策略	299
	关于策略检测的制定	300
	关于获得精确检测结果	300
	关于要避免的常见检测问题	301
	关于使用适当的检测方法	302
	关于使用例外缩小检测范围	303
	关于使用复合规则进行精确检测	303
第 16 章	策略创建	305
	关于策略	305
	关于策略组件	306
	关于系统定义的策略模板	308

关于解决方案软件包	308
关于策略组	309
关于策略部署	310
关于策略创建权限	310
关于策略模板导入和导出	311
关于数据配置文件	312
关于用户组	314
实施策略	314
策略最佳做法	315
第 17 章 基于模板创建策略	317
从模板创建策略	317
“美国监管执法”策略模板	319
“英国与国际监管执法”策略模板	321
“客户和员工数据保护”策略模板	322
“机密的或分类的数据保护”策略模板	323
“网络安全执法”策略模板	324
“可接受使用执法”策略模板	325
选择确切数据配置文件	326
选择索引文档配置文件	327
第 18 章 配置策略	329
添加新的策略或策略模板	329
配置策略	330
将规则添加至策略中	332
配置策略规则	334
定义规则严重性	337
配置匹配计数	337
选择匹配的组件	339
向策略中添加例外	340
配置策略例外	342
配置复合匹配条件	344
第 19 章 管理策略	347
管理和添加策略	347
创建和修改策略组	349
管理和添加策略组	350
导入策略模板	351
将策略检测导出为模板	351
将 10 版数据标识符或关键字策略导入 11 版系统	352
向策略添加自动响应规则	352

关于删除策略和策略组	353
第 20 章 使用确切数据匹配来检测内容	355
关于实施确切数据匹配	356
实施确切数据匹配	356
关于数据所有者例外	357
关于字段映射	358
关于索引调度	358
配置确切数据匹配计数	359
管理并添加确切数据配置文件	359
创建确切数据源文件	361
迁移旧有数据所有者例外配置	362
为编制索引准备确切数据源文件	363
将确切数据源文件上传到 Enforce Server	364
创建和修改确切数据配置文件	365
映射确切数据配置文件字段	369
调度确切数据配置文件索引编制	371
配置“内容匹配确切数据”条件	372
EDM 最佳做法	374
第 21 章 使用索引文档匹配来检测内容	377
关于实施索引文档匹配	377
管理并添加已编制索引的文档配置文件	378
配置“内容匹配文档签名”条件	380
实施索引文档匹配	382
准备文档源以便编制索引	382
将内容排除（加入白名单）在检测范围之外	383
创建和修改索引文档配置文件	384
根据文件名和大小过滤文档	386
计划文档配置文件的索引编制	388
使用 WebDAV 创建远程 SharePoint 文件的索引	391
关于使用 WebDAV 对 SharePoint 文档远程 IDM 编制索引	391
使用 WebDAV 创建远程 SharePoint 文件的索引	391
针对 IIS 启用 WebDAV	392
故障排除	393
IDM 最佳做法	394
第 22 章 使用向量机学习来检测内容	395
实施向量机学习 (VML)	396
关于培训的内容	397
创建新的 VML 配置文件	398

结合使用“当前配置文件”选项卡与“临时工作区”选项卡	399
上传培训的示例文档	399
培训 VML 配置文件	401
调整内存分配	403
关于培训的基本准确百分比率	404
管理培训集文档	405
管理 VML 配置文件	406
更改 VML 配置文件的名称和说明	408
配置 VML 策略规则	408
关于在策略中使用被拒绝的 VML 配置文件	410
配置 VML 策略例外	410
关于相似度阈值和相似度评分	411
调整相似度阈值	412
第 23 章 使用数据标识符检测内容	413
关于数据标识符	414
可用的系统数据标识符	415
关于数据标识符宽度	417
关于可选验证器	418
关于数据标识符的跨组件匹配	419
关于修改数据标识符	419
关于数据标识符模式	420
关于数据标识符的模式语言限制	420
关于验证器	421
关于自定义数据标识符	423
关于数据规范化程序	424
关于数据标识符配置	424
关于数据标识符的唯一匹配项计数	426
关于更改随机化美国 SSN	427
管理和添加数据标识符	428
配置“内容匹配数据标识符”条件	428
选择系统数据标识符宽度	430
配置可选验证器	433
对数据标识符进行唯一匹配项计数	436
修改和创建数据标识符	437
在修改系统数据标识符之前手动克隆它	438
编辑所需的验证器输入	438
实施自定义数据标识符	439
实施模式以匹配数据	440
选择所需的数据验证器	441
实施自定义脚本验证器	442
数据标识符最佳做法	442

第 24 章	使用关键字匹配检测内容	445
	关于实施关键字匹配	445
	关于关键字邻近匹配	446
	关键字匹配示例	446
	关键字语法要求	448
	配置“内容匹配关键字”条件	448
	关键字匹配最佳做法	451
第 25 章	使用正则表达式检测内容	453
	关于正则表达式匹配	453
	配置“内容匹配正则表达式”条件	453
	关于编写正则表达式	454
	正则表达式检测最佳做法	456
第 26 章	检测文件属性	457
	关于实施文件属性匹配	457
	关于文件类型检测	458
	关于自定义文件类型识别	458
	关于文件大小检测	459
	关于文件名检测	459
	使用表达式模式来匹配文件名	459
	配置“邮件附件类型或文件类型匹配”条件	460
	配置“邮件附件大小或文件大小匹配”条件	461
	配置“邮件附件名或文件名匹配”条件	462
	启用自定义文件类型检测	463
	配置自定义文件类型签名条件	463
	文件属性检测最佳做法	464
第 27 章	检测网络事件	467
	关于对网络进行的协议监控	465
	配置用于网络检测的“协议监控”条件	466
第 28 章	检测移动事件	467
	关于移动的协议监控	467
	配置移动监测的协议监控条件	467
第 29 章	检测端点事件	469
	关于进行端点事件检测	469
	关于端点协议、目标和应用程序检测	470

关于端点设备检测	470
关于端点位置检测	471
配置端点监控条件参数	471
收集端点设备 ID	473
管理及添加端点设备	474
创建及修改端点设备配置	474
配置“端点设备类或 ID”条件	476
配置“端点位置”条件	476
端点检测最佳做法	477
第 30 章 检测所述身份	479
关于指定身份匹配	479
配置“发送者/用户匹配模式”条件	480
配置“接受者匹配模式”条件	482
指定身份匹配最佳做法	483
第 31 章 检测已同步的身份	485
关于实施同步的目录组匹配	485
关于连接到目录组服务器	486
创建或修改用户组	487
配置“发送者/用户基于目录服务器匹配用户组”条件	488
配置“接受者基于目录服务器匹配用户组”条件	489
同步的 DGM 最佳做法	490
第 32 章 检测已配置的身份	491
关于实施配置的目录组匹配	491
为 DGM 创建确切数据配置文件	492
配置“发送者/用户匹配来自确切数据配置文件的目录”条件	493
配置“接受者匹配来自确切数据配置文件的目录”条件	493
配置的 DGM 的最佳做法	494
第 33 章 检测国际内容	495
关于实施非英语语言检测	495
国际策略模板	495
使用国际系统数据标识符的查找关键字	497
第 34 章 文件格式	499
可提取其内容的文件格式	499
可提取其内容的文字处理文件格式	500
可提取其内容的演示文稿文件格式	501

可提取其内容的电子表格文件格式	502
可提取其内容的封装文件格式	503
可提取其内容的文本和标记文件格式	504
可提取其内容的电子邮件文件格式	505
可提取其内容的计算机辅助设计文件格式	505
可提取其内容的图形文件格式	505
可提取其内容的数据库文件格式	506
可提取其内容的其他文件格式	506
可识别的文件类型	506
第 35 章 数据标识符	521
ABA 汇款路径号码数据标识符	522
ABA 汇款路径号码大宽度	523
ABA 汇款路径号码中宽度	523
ABA 汇款路径号码小宽度	524
澳大利亚医疗号码数据标识符	525
澳大利亚税务号码数据标识符	525
荷兰税号数据标识符	526
加拿大社会保险号码数据标识符	526
加拿大社会保险号大宽度	527
加拿大社会保险号中宽度	527
加拿大社会保险号小宽度	528
意大利税号数据标识符	529
信用卡磁条数据数据标识符	529
信用卡号数据标识符	532
信用卡号大宽度	532
信用卡号中宽度	533
信用卡号小宽度	535
CUSIP 号码数据标识符	538
CUSIP 号码大宽度	538
CUSIP 号码中宽度	538
CUSIP 号码小宽度	539
驾驶执照号码 - 加利福尼亚州数据标识符	540
驾驶执照号码 - 加利福尼亚州大宽度	540
驾驶执照号码 - 加利福尼亚州中宽度	540
驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州数据标识符	541
驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州大宽度	541
驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州中宽度	542
驾驶执照号码 - 伊利诺斯州数据标识符	543
驾驶执照号码 - 伊利诺斯州大宽度	543
驾驶执照号码 - 伊利诺斯州中宽度	543
驾驶执照号码 - 新泽西州数据标识符	544

驾驶执照号码 - 新泽西州大宽度	544
驾驶执照号码 - 新泽西州中宽度	545
驾驶执照号码 - 纽约州数据标识符	545
驾驶执照号码 - 纽约州大宽度	545
驾驶执照号码 - 纽约州中宽度	546
法国国家统计局代码数据标识符	546
香港特别行政区 ID 数据标识符	547
IBAN 中部数据标识符	548
IBAN 东部数据标识符	549
IBAN 西部数据标识符	552
IP 地址数据标识符	554
IP 地址大宽度	554
IP 地址中宽度	555
IP 地址小宽度	555
国家药品代码 (NDC) 数据标识符	556
国家药品代码 (NDC) 大宽度	556
国家药品代码 (NDC) 中宽度	557
国家药品代码 (NDC) 小宽度	558
中华人民共和国 ID 数据标识符	558
新加坡 NRIC 数据标识符	559
韩国居民登记号码数据标识符	559
韩国居民登记号码大宽度	560
韩国居民登记号码中宽度	560
西班牙 DNI ID 数据标识符	561
SWIFT 代码数据标识符	561
SWIFT 代码大宽度	561
SWIFT 代码小宽度	562
瑞士 AHV 号码数据标识符	563
中国台湾 ID 数据标识符	563
英国驾照号数据标识符	564
英国驾照号大宽度	564
英国驾照号中宽度	564
英国驾照号小宽度	565
英国选民登记号数据标识符	566
英国国民保健服务 (NHS) 号数据标识符	567
英国国民保健服务 (NHS) 号中宽度	567
英国国民保健服务 (NHS) 号小宽度	568
英国国家保险号码数据标识符	569
英国国家保险号码大宽度	569
英国国家保险号码中宽度	569
英国国家保险号码小宽度	570
英国护照号数据标识符	571
英国护照号大宽度	571

英国护照号中宽度	571
英国护照号小宽度	572
英国税号数据标识符	573
英国税号大宽度	573
英国税号中宽度	573
英国税号小宽度	574
美国个人纳税识别号 (ITIN) 数据标识符	574
美国个人纳税识别号 (ITIN) 大宽度	575
美国个人纳税识别号 (ITIN) 中宽度	575
美国个人纳税识别号 (ITIN) 小宽度	576
美国社会安全号 (SSN) 数据标识符	577
美国社会安全号 (SSN) 大宽度	577
美国社会安全号 (SSN) 中宽度	578
美国社会安全号 (SSN) 小宽度	579
美国 SSN - 随机化自定义数据标识符 (DI)	580
创建“美国 SSN - 随机化”自定义 DI	581
使用美国 SSN - 随机化自定义 DI 的建议	582
第 36 章 策略模板	585
Caldicott 报告策略模板	587
加拿大社会保险号策略模板	589
CAN-SPAM 法案策略模板	589
常见间谍软件上传站点策略模板	591
竞争对手通信策略模板	591
机密文档策略模板	591
信用卡号策略模板	592
客户数据保护策略模板	593
1998 年数据保护法案（英国）策略模板	594
数据保护规定（欧盟）策略模板	596
国防信息系统 (DMS) 的常规服务分类策略模板	597
设计文档策略模板	598
员工数据保护策略模板	599
加密数据策略模板	600
出口管理条例 (EAR) 策略模板	600
FACTA 2003（红色标记规则）策略模板	602
金融信息策略模板	605
禁止访问的网站策略模板	605
赌博策略模板	606
“金融服务法案”策略模板	606
HIPAA 和 HITECH（包括 PHI）策略模板	608
1998 年人权法策略模板	612
非法药品策略模板	612

个人纳税识别号 (ITIN) 策略模板	613
国际武器贸易条例 (ITAR) 策略模板	613
媒体文件策略模板	614
并购协议策略模板	615
NASD 规则 2711 以及 NYSE 规则 351 和 472 策略模板	616
NASD 规则 3010 和 NYSE 规则 342 策略模板	618
NERC 电气设备安全指导策略模板	619
网络图策略模板	620
网络安全策略模板	621
攻击性语言策略模板	621
外国资产管制办公室 (OFAC) 策略模板	622
OMB 备忘录 06-16 和 FIPS 199 条例策略模板	623
密码文件策略模板	625
支付卡行业 (PCI) 数据安全标准策略模板	625
PIPEDA 策略模板	626
价格信息策略模板	628
项目数据策略模板	629
专有媒体文件策略模板	629
出版文档策略模板	630
种族歧视语言策略模板	630
受限文件策略模板	631
受限接受者策略模板	631
简历策略模板	631
萨班斯-奥克斯利法案策略模板	632
SEC 公平披露规则策略模板	634
下流语言策略模板	636
源代码策略模板	637
州数据隐私策略模板	637
SWIFT 代码策略模板	641
Symantec DLP 感知与避免策略模板	641
英国驾照号策略模板	642
英国选民登记号策略模板	642
英国国民保健服务 (NHS) 号策略模板	642
英国国家保险号码策略模板	643
英国护照号策略模板	643
英国税号策略模板	644
美国情报控制标记 (CAPCO) 和 DCID 1/7 策略模板	644
美国社会安全号策略模板	645
暴力与武器策略模板	646
Webmail 策略模板	646
Yahoo 留言板活动策略模板	647
端口 80 上的 Yahoo 和 MSN Messenger 策略模板	648

部分 5	配置策略响应	651
第 37 章	响应策略违规	653
	关于响应规则	653
	关于响应规则操作	654
	所有检测服务器的响应规则	655
	端点检测的响应规则	656
	Network and Mobile Prevent for Web 检测的响应规则	657
	Network Protect 检测的响应规则	658
	分类服务器的响应规则	658
	关于响应规则执行类型	659
	关于“自动”响应规则	659
	关于智能响应规则	660
	关于响应规则条件	661
	关于响应规则操作的执行优先级	662
	关于响应规则创建权限	664
	实施响应规则	664
	响应规则最佳做法	665
第 38 章	配置和管理响应规则	667
	管理响应规则	667
	添加新的响应规则	668
	配置响应规则	669
	关于配置智能响应规则	670
	配置响应规则条件	670
	配置响应规则操作	671
	修改响应规则排序	673
	关于删除响应规则	674
第 39 章	响应规则条件	675
	配置“端点位置”响应条件	675
	配置“端点设备”响应条件	676
	配置“事件类型”响应条件	677
	配置“事件匹配数”响应条件	678
	配置“协议或端点监视”响应条件	679
	配置“严重性”响应条件	681
第 40 章	响应规则操作	683
	配置“添加注释”操作	684
	配置“限制事件数据保留”操作	684

保留端点事件的数据	685
丢弃网络事件的数据	686
配置“记录到 Syslog 服务器”操作	686
配置“发送电子邮件通知”操作	687
配置服务器 FlexResponse 操作	689
配置“设置属性”操作	690
配置“设置状态”操作	691
配置“Endpoint: FlexResponse”操作	692
配置“Endpoint Discover: 隔离文件”操作	693
配置“Endpoint Prevent: 阻止”操作	694
配置“Endpoint Prevent: 通知”操作	697
配置 Endpoint Prevent: 用户取消操作	699
配置“Network and Mobile Prevent for Web: 阻止 FTP 请求”操作	701
配置“Network and Mobile Prevent for Web: 阻止 HTTP/S”操作	702
配置“Network Prevent: 阻止 SMTP 邮件”操作	703
配置“Network Prevent: 修改 SMTP 邮件”操作	704
配置“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”操作	706
配置“Network Protect: 复制文件”操作	707
配置“Network Protect: 隔离文件”操作	708
部分 6 补救和管理事件	711
第 41 章 补救事件	713
关于事件补救	713
补救事件	715
执行智能响应规则	716
事件补救操作命令	717
响应操作变量	718
Monitor 和 Prevent 事件变量	718
移动事件变量	719
发现事件变量	720
第 42 章 补救网络事件	723
网络事件列表	723
网络事件列表 - 操作	725
网络事件列表 - 列	726
网络事件快照	727
网络事件快照 - 标题和导航	728
网络事件快照 - 常规信息	728
网络事件快照 - 匹配项	730

网络事件快照 - 属性	731
网络摘要报告	731
第 43 章 补救端点事件	733
端点事件列表	733
端点事件快照	736
关于 Endpoint Prevent 响应规则的报告	740
端点事件目标或协议特定的信息	741
端点事件摘要报告	743
配置 Endpoint Server 文件过滤器	744
第 44 章 补救移动事件	747
Mobile Prevent 事件报告	747
Mobile Prevent 事件快照	748
Mobile Prevent 事件列表	748
Mobile Prevent 事件列表 - 操作	750
Mobile Prevent 事件列表 - 列	750
Mobile Prevent 事件快照 - 标题和导航	752
Mobile Prevent 事件快照 - 常规信息	752
Mobile Prevent 事件快照 - 匹配项	754
Mobile Prevent 事件快照 - 属性	754
Mobile Prevent 摘要报告	755
第 45 章 补救发现事件	757
关于 Network Discover 的报告	961
关于 Network Discover 的事件报告	962
发现事件报告	759
发现事件快照	760
解决 Firefox 浏览器中的链接访问问题	762
发现事件列表	763
Network Discover 事件操作	763
Network Discover 事件条目	765
发现摘要报告	767
第 46 章 使用分类事件	769
分类事件列表	769
分类事件快照	770
分类事件摘要报告	772

第 47 章 管理和报告事件 773

关于 Symantec Data Loss Prevention 报告	775
关于使用报告的策略	776
设置报告首选项	777
关于事件报告	777
关于控制板报告和执行摘要	779
查看控制板	780
创建控制板报告	780
配置控制板报告	782
选择要包括在控制板中的报告	783
关于摘要报告	783
查看摘要报告	784
创建摘要报告	784
查看事件	785
关于自定义报告和控制板	786
使用 IT Analytics 管理事件	788
过滤报告	788
保存自定义事件报告	789
调度自定义事件报告	789
事件和系统报告的交付日程表选项	791
控制板报告的交付日程表选项	793
使用日期工具调度报告	795
编辑自定义控制板和报告	795
导出事件报告	795
Network Monitor 的导出字段	796
Network Discover 的导出字段	797
Mobile Prevent for Web 的导出字段	798
Endpoint Discover 的导出字段	798
删除事件	799
删除自定义控制板和报告	800
常见事件报告功能	801
事件报告中的页面导航	801
事件报告过滤器和摘要选项	802
通过电子邮件发送事件报告	803
打印事件报告	804
事件快照历史记录选项卡	804
事件快照属性部分	804
事件快照关联选项卡	805
事件快照策略部分	805
事件快照匹配项部分	806
事件快照访问信息部分	806
自定义事件快照页面	807

关于报告的过滤器和摘要选项	807
报告的常规过滤器	808
事件报告的摘要选项	811
报告的高级过滤器选项	815
第 48 章 存档事件	823
关于事件存档	823
存档事件	824
还原存档的事件	824
禁止存档事件	825
删除存档的事件	825
第 49 章 使用事件数据	827
关于事件状态属性	827
配置状态属性和值	829
配置状态组	829
导出 Web 存档	830
导出 Web 存档 - 创建存档	831
导出 Web 存档 - 所有最近事件	832
关于自定义属性	833
关于使用自定义属性	834
如何填充自定义属性	835
配置自定义属性	835
手动设置自定义属性的值	836
第 50 章 实施查找插件	837
关于查找插件	837
查找插件的类型	838
关于查找参数	840
关于插件部署	841
关于插件链接	841
关于升级查找插件	842
实施和测试查找插件	842
管理和配置查找插件	843
创建新的查找插件	845
选择查找参数	846
启用查找插件	850
链接查找插件	850
重新加载查找插件	851
排除查找插件故障	851
配置查找插件的详细记录	852

配置高级插件属性	853
配置 CSV 查找插件	854
创建 CSV 文件的要求	855
指定 CSV 文件路径	856
选择 CSV 文件分隔符	856
选择 CSV 文件字符集	857
将属性和参数键映射至 CSV 字段	857
CSV 属性映射示例	858
测试 CSV 查找插件并进行故障排除	859
CSV 查找插件教程	860
配置 LDAP 查找插件	862
LDAP 服务器连接的要求	863
将属性映射到 LDAP 数据	863
LDAP 的属性映射示例	864
测试和故障排除 LDAP 查找插件	865
LDAP 查找插件教程	865
配置脚本查找插件	867
编写脚本查找插件	868
指定脚本命令	869
指定参数	869
启用 stdin 和 stdout 选项	870
对脚本启用事件协议过滤	870
启用和加密脚本凭据	871
链接多个脚本查找插件	872
脚本查找插件教程	873
脚本示例	874
配置迁移的自定义（旧版）查找插件	876

部分 7

第 51 章

监视和防止网络中的数据丢失	879
---------------------	-----

实施 Network Monitor	881
实施 Network Monitor	881
选择网络数据包捕获方法	883
关于数据包捕获软件的安装和配置	884
在 Windows 平台上安装 WinPcap	884
更新 Endace 卡驱动程序	885
安装和更新 Napatech 网络适配器和驱动程序软件	885
配置 Network Monitor Server	886
对 Network Monitor 启用 GET 处理	888
为 Network Monitor 创建策略	888
测试 Network Monitor	889

第 52 章	实施 Network Prevent for Email	891
	实施 Network Prevent for Email	891
	关于邮件传输代理 (MTA) 集成	893
	针对反射或转发模式配置 Network Prevent for Email Server	893
	将 Linux IP 表配置为从受限端口重新路由流量	898
	指定一个或多个上游邮件传输代理 (MTA)	899
	为 Network Prevent for Email 创建策略	900
	关于策略违规数据标头	901
	启用策略违规数据标头	902
	测试 Network Prevent for Email	902
第 53 章	实施 Network Prevent for Web	905
	实施 Network Prevent for Web	905
	Network Prevent 授权许可	907
	配置 Network Prevent for Web Server	907
	关于代理服务器配置	910
	代理服务器与 Network Prevent for Web 的兼容性	910
	配置请求与响应模式服务	912
	指定一个或多个代理服务器	913
	为 Network Prevent for Web 启用 GET 处理	914
	为 Network Prevent for Web 创建策略	914
	测试 Network Prevent for Web	916
	Network Prevent for Web Server 的故障排除信息	916
部分 8	发现机密数据的存储位置	917
第 54 章	关于 Network Discover	919
	关于 Network Discover	919
	Network Discover 的工作原理	921
第 55 章	设置和配置 Network Discover	923
	设置和配置 Network Discover	923
	修改 Network Discover Server 配置	924
	关于 Linux Network Discover Server	926
	添加新的 Network Discover 目标	926
	编辑现有的 Network Discover 目标	927
第 56 章	Network Discover 扫描目标配置选项	929
	Network Discover 扫描目标配置选项	929
	为 Network Discover 目标配置必填字段	930

调度 Network Discover 扫描	931
为 Network Discover 扫描的内容提供密码身份验证	933
加密配置文件中的密码	934
设置发现过滤器以在扫描中包括或排除项目	935
按项目大小过滤发现目标	937
根据上次访问或修改日期过滤发现目标	938
使用 Network Discover 扫描限制优化资源	940
创建未受保护的敏感数据的位置的库存	941
第 57 章 管理 Network Discover 目标扫描	943
管理 Network Discover 目标扫描	943
管理 Network Discover 目标	944
关于 Network Discover 扫描目标列表	944
使用 Network Discover 扫描目标	945
删除 Network Discover 扫描目标	946
管理 Network Discover 扫描历史记录	946
关于 Network Discover 扫描历史记录	947
使用 Network Discover 扫描历史记录	949
删除 Network Discover 扫描	949
关于 Network Discover 扫描详细信息	950
使用 Network Discover 扫描详细信息	952
管理 Network Discover 服务器	952
查看 Network Discover 服务器状态	953
关于 Network Discover 扫描优化	953
关于增量扫描和差异扫描之间的区别	955
关于增量扫描	956
使用增量扫描来扫描新的或修改过的项	957
关于管理增量扫描	957
使用差异扫描来扫描新的或修改过的项	958
配置 Network Discover 目标的并行扫描	958
第 58 章 管理 Network Discover 事件报告	961
关于 Network Discover 的报告	961
关于 Network Discover 的事件报告	962
第 59 章 使用服务器 FlexResponse 插件补救事件	965
关于服务器 FlexResponse 平台	965
使用服务器 FlexResponse 自定义插件补救事件	967
部署服务器 FlexResponse 插件	968
将服务器 FlexResponse 插件添加到插件属性文件	968
创建用于配置服务器 FlexResponse 插件的属性文件	970

查找事件进行手动补救	973
使用服务器 FlexResponse 插件的操作手动补救事件	973
验证事件响应操作的结果	974
对服务器 FlexResponse 插件进行故障排除	975
部署 Python Script Bridge 服务器 FlexResponse 插件	976
安装 Python Script Bridge 插件	977
为您的 Python 插件配置 Python Script Bridge 插件	978
配置多个 Python Script Bridge 插件	980
Python Script Bridge 的属性文件	980
为 Python Script Bridge FlexResponse 插件创建响应规则	983
第 60 章 设置文件共享扫描	985
设置文件系统扫描	985
支持的文件系统目标	986
自动发现开放文件共享	987
排除内部 DFS 文件夹	987
配置 Microsoft Outlook 个人文件夹 (.pst 文件) 扫描	988
配置与运行文件系统的扫描	988
优化文件系统目标扫描	991
为文件共享配置 Network Protect	992
第 61 章 设置 Lotus Notes 数据库扫描	995
设置 Lotus Notes 数据库扫描	995
支持的 Lotus Notes 目标	996
配置与运行 Lotus Notes 扫描	997
配置 Windows 服务器上的 Lotus Notes 本机模式配置扫描选项	999
配置 Lotus Notes DIIOP 模式配置扫描选项	1000
在 Linux 服务器上配置 Lotus Notes 本机模式扫描配置选项	1002
第 62 章 设置 SQL 数据库扫描	1003
设置 SQL 数据库扫描	1003
支持的 SQL 数据库目标	1004
配置并运行 SQL 数据库扫描	1004
为 SQL 数据库目标安装 JDBC 驱动程序	1007
SQL 数据库扫描配置属性	1008
第 63 章 设置 SharePoint 服务器扫描	1011
设置 SharePoint 服务器扫描	1011
关于 SharePoint 服务器扫描	1012
支持的 SharePoint 服务器目标	1014
SharePoint 2007 和 2010 扫描的访问权限	1014

关于备用访问映射集合	1015
配置和运行 SharePoint 服务器扫描	1015
在服务器场的 Web 前端上安装 SharePoint 解决方案	1018
将 SharePoint 扫描设置为使用 Kerberos 身份验证	1020
排除 SharePoint 扫描故障	1021
第 64 章 设置 Exchange Server 扫描	1023
使用 Exchange Web 存储连接器设置 Exchange 2003 和 2007 存储库 的扫描	1023
关于 Exchange 2003 和 2007 服务器扫描	1024
支持的 Exchange Server Web 存储连接器目标	1025
提供扫描所有邮箱和公用文件夹的访问权限	1026
配置 Exchange 2003 和 2007 服务器扫描	1026
Exchange 2003 和 2007 扫描的配置和使用案例示例	1030
解答 Exchange 2003 和 2007 扫描的疑难	1031
设置使用 Exchange Web 服务扫描 Exchange 2007 SP2 和 2010 存储 库	1032
关于 Exchange 2007 SP2 和 2010 服务器扫描	1033
支持的 Exchange Server Web 服务连接器目标	1033
配置 Exchange 2007 SP2 和 2010 服务器扫描	1034
Exchange 2007 SP2 和 2010 扫描的配置示例和使用情况	1037
故障排除 Exchange 2007 SP2 和 2010 扫描问题	1038
第 65 章 关于 Network Discover 扫描程序	1041
Network Discover 扫描程序的工作原理	1041
排除扫描程序故障	1042
扫描程序进程	1043
扫描程序安装目录结构	1044
扫描程序配置文件	1045
扫描程序控制器配置选项	1046
第 66 章 设置文件系统扫描	1049
设置文件系统扫描	1049
支持的文件系统扫描程序目标	1050
安装文件系统扫描程序	1051
启动文件系统扫描	1053
从命令行以静默方式安装文件系统扫描程序	1054
文件系统扫描程序的配置选项	1055
扫描 Windows 计算机上的 C 驱动器的配置示例	1056
在 UNIX 上扫描 /usr 目录的配置示例	1056
使用包括过滤器进行扫描的配置示例	1057

使用排除过滤器进行扫描的配置示例	1057
使用包括和排除过滤器进行扫描的配置示例	1058
使用日期过滤进行扫描的配置示例	1058
使用文件大小过滤进行扫描的配置示例	1059
在 UNIX 系统中跳过符号链接的扫描的配置示例	1059
第 67 章 设置 Microsoft Exchange Server 扫描	1061
设置 Microsoft Exchange Server 扫描	1061
支持的 Exchange 扫描程序目标	1062
检查 Exchange 邮箱存储权限	1063
安装 Exchange 扫描程序	1064
Exchange 扫描程序的配置选项	1066
对配置文件名进行配置	1069
配置 DNMailbox 的设置	1069
启动 Microsoft Exchange 扫描	1069
扫描 Exchange 存档公用文件夹的配置示例	1071
扫描 Exchange 收件箱的配置示例	1071
扫描其他用户收件箱的配置示例	1072
扫描所有 Exchange 邮箱的配置示例	1072
第 68 章 设置 SharePoint 2007 服务器扫描	1075
设置 SharePoint 2007 服务器扫描	1075
支持的 SharePoint 扫描程序目标	1076
SharePoint 2007 扫描的访问权限	1077
安装 SharePoint 2007 扫描程序	1078
启动 SharePoint 2007 扫描	1079
SharePoint 2007 扫描程序的配置选项	1081
扫描特定站点集合的配置示例	1082
扫描特定网站的配置示例	1082
扫描 Web 应用程序中所有网站的配置示例	1082
扫描服务器上所有 Web 应用程序中所有网站的配置示例	1083
调度 SharePoint 2007 扫描	1083
第 69 章 设置 SharePoint 2003 服务器扫描	1085
设置 SharePoint 2003 服务器扫描	1085
安装 SharePoint 2003 扫描程序	1086
启动 SharePoint 2003 扫描	1088
SharePoint 2003 扫描程序的配置选项	1089
扫描所有 SharePoint 2003 站点的配置示例	1090
扫描一个 SharePoint 2003 站点的配置示例	1091

第 70 章	设置 Web 服务器扫描	1093
	设置 Web 服务器扫描	1093
	支持的 Web 服务器（扫描程序）目标	1094
	安装 Web 服务器扫描程序	1094
	启动 Web 服务器扫描	1096
	Web 服务器扫描程序的配置选项	1097
	不使用身份验证的网站扫描的配置示例	1100
	使用基本身份验证的网站扫描的配置示例	1100
	使用基于表单的身份验证的网站扫描配置示例	1100
	使用 NTLM 的网站扫描的配置示例	1101
	网站扫描的 URL 过滤示例	1101
	网站扫描的日期过滤示例	1102
第 71 章	设置 Documentum 存储库扫描	1103
	设置 Documentum 存储库扫描	1103
	支持的 Documentum（扫描程序）目标	1104
	安装 Documentum 扫描程序	1104
	启动 Documentum 扫描	1106
	Documentum 扫描程序的配置选项	1107
	扫描 Documentum 存储库中所有文档的配置示例	1109
第 72 章	设置 Livelink 存储库扫描	1111
	设置 Livelink 存储库扫描	1111
	持的 Livelink 扫描程序目标	1112
	为 SQL Server 创建 ODBC 数据源	1112
	安装 Livelink 扫描程序	1113
	启动 Livelink 扫描	1115
	Livelink 扫描程序的配置选项	1116
	扫描 Livelink 数据库的配置示例	1117
第 73 章	为自定义扫描目标设置 Web 服务	1119
	为自定义扫描目标设置 Web 服务	1119
	关于设置 Web 服务定义语言（WSDL）	1120
	Web 服务 Java 客户端的示例	1120
	Web 服务示例的示例 Java 代码	1121

部分 9	发现和防止端点计算机上的数据丢失	1125
第 74 章	使用 Endpoint Discover 和 Endpoint Prevent	1127
	关于 Endpoint Discover 和 Endpoint Prevent	1127
	Endpoint Discover 的工作原理	1128
	Endpoint Prevent 的工作原理	1128
	关于 Endpoint Server	1129
	关于 Symantec DLP Agent	1129
	关于 Endpoint Prevent 监视	1130
	关于可移动存储监控	1130
	关于 CD/DVD 监视	1131
	关于打印/传真监视	1132
	关于剪贴板监视	1132
	关于应用程序监控	1133
	关于网络共享监视	1133
	关于端点网络监视	1133
	关于 Endpoint Discover 监视	1135
	关于目标 Endpoint Discover 扫描	1136
	关于端点计算机的策略	1136
	关于为 Endpoint Prevent 创建策略	1137
	关于 Endpoint Server 的监视策略与响应规则	1138
	关于规则结果缓存 (RRC)	1140
	关于端点报告	1140
第 75 章	实施 Endpoint Discover	1143
	如何实施 Endpoint Discover	1143
	为 Endpoint Discover 创建策略组	1144
	为 Endpoint Discover 创建策略	1144
	为 Endpoint Discover 添加规则	1145
	设置对 Endpoint Discover 目标的扫描	1146
	Endpoint Discover 目标的配置选项	1147
	配置 Endpoint Discover 扫描超时设置	1149
第 76 章	实施 Endpoint Prevent	1151
	如何实施 Endpoint Prevent	1151
	设置端点位置	1152
	关于不同区域设置中的 Endpoint Prevent 响应规则	1153

第 77 章	使用代理配置	1155
	关于代理配置	1155
	关于克隆代理配置	1156
	添加代理配置	1156
	将代理配置应用于 Endpoint Server	1161
第 78 章	使用 Endpoint FlexResponse	1163
	关于 Endpoint FlexResponse	1163
	部署 Endpoint FlexResponse	1164
	关于在端点计算机上部署 Endpoint FlexResponse 插件	1165
	使用静默安装过程部署 Endpoint FlexResponse 插件	1166
	关于 Endpoint FlexResponse 实用程序	1167
	使用 Endpoint FlexResponse 实用程序部署 Endpoint FlexResponse 插件	1169
	在 Enforce Server 上启用 Endpoint FlexResponse	1169
	使用 Endpoint FlexResponse 实用程序卸载 Endpoint FlexResponse 插件	1170
	从特定端点计算机中检索 Endpoint FlexResponse 插件	1170
	从端点计算机中检索 Endpoint FlexResponse 插件列表	1171
第 79 章	实施 Symantec DLP Agent	1173
	关于 Symantec Management Console	1173
	克隆广告与程序	1174
	使用计算机发现	1174
	安装 Symantec Management Agent	1175
	关于 Symantec Management Console 报告	1176
	关于 Symantec Management Console 代理任务	1176
	创建用户任务	1177
	关于 Symantec DLP Agent 安装	1178
	Symantec DLP Agent 的已安装内容	1178
	关于 Symantec DLP Agent 的安装前步骤	1180
	关于 Symantec DLP Agent 安全	1181
	关于监视程序服务	1183
	关于 Endpoint Server 冗余	1183
	关于 AgentInstall.msi 软件包	1184
	关于卸载密码	1185
	使用 Symantec Management Console 安装 Symantec DLP Agent	1187
	使用无人参与安装方法安装 Symantec DLP Agent	1188
	手动安装 Symantec DLP Agent	1189

第 80 章	管理 Symantec DLP Agent	1193
	关于 Symantec DLP Agent 管理	1193
	使用代理概述屏幕	1193
	代理管理事件屏幕	1198
	关于 Symantec DLP Agent 删除	1200
	关于端点代理日志	1204
	设置端点代理的日志级别	1204
第 81 章	关于应用程序监控	1207
	关于应用程序监控	1207
	添加应用程序	1208
第 82 章	使用 Endpoint Server 工具	1211
	关于端点工具	1211
	在 Windows 7 或 Vista 上使用端点工具	1212
	关于 endpointkeytool 实用程序	1212
	关闭代理和监视程序服务	1214
	检测代理访问的数据库文件	1215
	查看扩展日志文件	1215
	关于设备 ID 实用程序	1216
	使用密码生成工具创建密码	1218
部分 10	监视和防止移动设备上的数据丢失	1219
第 83 章	Symantec Data Loss Prevention for Mobile 简介	1221
	Symantec Data Loss Prevention for Mobile 的工作方式	1221
	Mobile Prevent 的部署选项	1223
	关于将 Mobile Prevent 部署为单机解决方案	1223
	关于将 Mobile Prevent 与 Network Prevent 一起部署	1225
	关于 Mobile Prevent 的数字证书	1227
	关于 VPN 服务器和按需 VPN	1228
	关于 Microsoft Exchange ActiveSync	1228
	忽略 Microsoft Exchange ActiveSync 监控	1229
	关于移动设备管理	1230
第 84 章	实施 Mobile Prevent (Web)	1231
	实施 Mobile Prevent	1231
	配置 Mobile Prevent for Web Server	1232

配置 VPN 配置文件	1235
关于代理服务器配置	1236
指定一个或多个代理服务器	1238
为 Mobile Prevent 启用 GET 处理	1239
创建 Mobile Prevent 的策略	1239
针对安全银行业务配置 Mobile Prevent	1241
测试 Mobile Prevent	1241
索引	1243

1

部分

快速入门

- 1. Symantec Data Loss Prevention 简介
- 2. 快速了解如何管理 Symantec Data Loss Prevention
- 3. 使用语言和区域设置

Symantec Data Loss Prevention 简介

本章节包括下列主题：

- [关于 Symantec Data Loss Prevention](#)
- [关于 Enforce 平台](#)
- [关于 Network Monitor 和 Prevent](#)
- [关于 Network Discover](#)
- [关于 Network Protect](#)
- [关于 Endpoint Discover](#)
- [关于 Endpoint Prevent](#)
- [关于 Symantec Data Loss Prevention for Mobile](#)
- [关于 Symantec Enterprise Vault 数据分类服务](#)

关于 Symantec Data Loss Prevention

Symantec Data Loss Prevention 允许您：

- 发现并找到文件和 Web 服务器、数据库、移动设备以及端点（台式机和便携式计算机系统）中的机密信息
- 通过隔离保护机密信息
- 监视网络流量以防止传输机密数据
- 监视并防止在移动设备上进行的机密数据传输。
- 监视敏感数据在端点计算机上的使用

- 防止机密数据传输到外部
- 自动强制数据安全与加密策略

Symantec Data Loss Prevention 包括以下组件：

- Enforce Server
请参见第 43 页的“[关于 Enforce 平台](#)”。
请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。
请参见第 50 页的“[关于 Enforce Server 管理控制台](#)”。
- Network Discover
请参见第 45 页的“[关于 Network Discover](#)”。
- Network Protect
请参见第 45 页的“[关于 Network Protect](#)”。
- Network Monitor
- Network Prevent
- Mobile Prevent for Web
请参见第 47 页的“[关于 Symantec Data Loss Prevention for Mobile](#)”。
- Endpoint Discover
请参见第 46 页的“[关于 Endpoint Discover](#)”。
请参见第 1127 页的“[关于 Endpoint Discover 和 Endpoint Prevent](#)”。
- Endpoint Prevent
请参见第 46 页的“[关于 Endpoint Prevent](#)”。
- Symantec Enterprise Vault 数据分类
请参见第 47 页的“[关于 Symantec Enterprise Vault 数据分类服务](#)”。

Discover、Protect、Monitor、Mobile 和 Prevent 模块可作为独立产品来部署，也可组合起来部署。不管部署哪些独立产品，始终会提供 Enforce Server 来进行集中管理。请注意，Network Protect 模块需要 Network Discover 模块。

每个产品模块与相应的检测服务器相关联：

- Network Discover Server 在范围广泛的企业数据存储库中查找遭到暴露的机密数据，存储库类型包括：
 - 文件服务器
 - 数据库
 - Microsoft SharePoint
 - Lotus Notes
 - EMC Documentum

- Livelink
- Microsoft Exchange
- Web 服务器
- 其他数据存储库

如果您获得 NetworkProtect 的许可证，此服务器也可如策略中所指定的那样来复制与隔离文件服务器上的敏感数据。

请参见第 45 页的“[关于 Network Discover](#)”。

- Network Monitor Server 监视网络上的流量。
请参见第 44 页的“[关于 Network Monitor 和 Prevent](#)”。
- Network Prevent for Email Server 阻止包括敏感数据的电子邮件。
请参见第 891 页的“[实施 Network Prevent for Email](#)”。
- Network Prevent for Web Server 阻止包括敏感数据的 HTTP 发布与 FTP 传输。
请参见第 905 页的“[实施 Network Prevent for Web](#)”。
- Mobile Prevent for Web Server 监视并阻止通过移动设备进行的包含敏感数据的 HTTP/S 和 FTP 传输。
请参见第 1231 页的“[实施 Mobile Prevent](#)”。
- Endpoint Server 监视并防止机密数据在端点计算机上的误用。
请参见第 1127 页的“[关于 Endpoint Discover 和 Endpoint Prevent](#)”。

Symantec Data Loss Prevention 的分布式体系结构允许组织执行以下操作：

- 执行集中式管理与报告。
- 只需集中管理数据安全策略一次，部署即刻遍布整个 Symantec Data Loss Prevention 套件。
- 根据您组织的规模扩展数据丢失防护。

关于 Enforce 平台

Symantec Data Loss Prevention Enforce Server 是中央管理平台，可允许您定义、部署和强制执行数据泄漏防护和安全策略。Enforce Server 管理控制台提供一个基于 Web 的集中式界面，以便部署检测服务器、创建策略、补救事件和管理系统。

请参见第 41 页的“[关于 Symantec Data Loss Prevention](#)”。

Enforce 平台为您提供以下功能：

- 建立并部署准确的数据泄露防护策略。您可以选择各种检测技术、定义规则，并指定要包括在数据丢失防护策略中的操作。使用提供的法规和最佳做法策略模板，可满足法规遵从性要求、数据保护要求以及可接受使用要求，并应付特定的威胁。

请参见第 305 页的“[关于策略](#)”。

请参见第 283 页的“[策略检测简介](#)”。

- 自动部署和强制执行数据泄露防护策略。您可自动运行通知、补救工作流程、阻止与加密的策略强制选项。
- 衡量风险降低并阐明遵从。Enforce Server 的报告功能允许您创建可执行报告，这些报告可识别风险随时间降低的趋势。您也可以创建遵从性报告，以符合法规要求。
 - 请参见第 775 页的“[关于 Symantec Data Loss Prevention 报告](#)”。
 - 请参见第 777 页的“[关于事件报告](#)”。
- 能够进行快速补救。您可以根据事件严重性，使用详细的事件报告以及工作流程自动化，将整个补救进程自动化。使用以角色为基础的访问控制，个别业务单元及部门能够查看并补救与其业务或员工相关的事件。
 - 请参见第 713 页的“[关于事件补救](#)”。
 - 请参见第 715 页的“[补救事件](#)”。
- 保护员工隐私。您可以使用 Enforce Server 来查看事件，而不会泄露发送者的身份或邮件内容。通过此方式，跨国公司即可符合对于监视欧盟员工以及跨国传输个人数据方面的法律要求。
 - 请参见第 77 页的“[关于基于角色的访问控制](#)”。

关于 Network Monitor 和 Prevent

Symantec Data Loss Prevention 网络数据监视与保护产品包括：

■ Network Monitor

Network Monitor 会捕获和分析网络上的流量。它会通过指定的协议检测机密数据和重要流量元数据。例如，SMTP、FTP、HTTP 和各种 IM 协议。您可以对 Network Monitor Server 进行配置以监视自定义协议并使用各种过滤器（按协议）滤除低风险流量。

请参见第 881 页的“[实施 Network Monitor](#)”。

■ Network Prevent for Email

Network Prevent for Email 与标准 MTA 和托管电子邮件服务集成以提供内联 SMTP 电子邮件管理。部署在内联 Network Prevent for Email Server 上的策略会指导下一跳邮件服务器阻止、重新路由或标记电子邮件。这些阻止取决于特定内容和其他消息属性。必要时可以使用 TLS 来保护 MTA 与 Network Prevent for Email Server 之间的通信。

实施 Network Monitor、查看其捕获的事件并相应优化策略，然后再实施 Network Prevent for Email。

请参见第 891 页的“[实施 Network Prevent for Email](#)”。

请参见《Symantec Data Loss Prevention MTA 集成指南（适用于 Network Prevent for Email）》。

■ Network Prevent for Web

为了内联活动 Web 请求管理，Network Prevent for Web 集成了 HTTP、HTTPS 或 FTP 代理服务器。此集成会使用 Internet 内容修改协议 (ICAP)。Network Prevent for Web Server 会检测 HTTP、HTTPS 或 FTP 内容中的机密数据。进行检测时，它会使代理依管理策略的规定拒绝请求或删除 HTML 内容。

请参见第 905 页的“[实施 Network Prevent for Web](#)”。

关于 Network Discover

Network Discover 可以高速扫描网络文件共享文件夹、Web 内容服务器、数据库、文档存储库和端点系统，以检测是否有暴露的数据和文档。Network Discover 可让公司准确了解暴露机密数据的位置，并可协助显著降低数据丢失的风险。

Network Discover 可让组织具备以下能力：

- 精确指出未受保护的机密数据。Network Discover 可帮助组织准确找出其网络上存储的具有风险的数据。然后您可以通知共享文件服务器的拥有者保护这些数据。
- 减少机密数据的扩散。Network Discover 可帮助组织检测敏感信息在公司内的扩散情况，降低数据丢失的风险。
- 自动化调查与审核。Network Discover 简化了数据安全调查与遵从审核。它通过让用户自动扫描机密数据并查看访问控制与加密策略，来完成此任务。
- 在事件补救期间，Symantec Data Insight 可帮助组织解决由于不完整或不准确的元数据或跟踪信息所导致的识别信息的数据所有者和责任方的问题。
请参见《[Symantec Data Loss Prevention Data Insight 操作指南](#)》。
- 要提高补救 Network Discover 事件的灵活性，请使用 FlexResponse 应用程序编程接口 (API) 或可用的 FlexResponse 插件。
有关插件的列表，请参见 *Symantec Data Loss Prevention FlexResponse Platform Developers Guide* (《Symantec Data Loss Prevention FlexResponse 平台开发人员指南》) 或联系 Symantec 专业服务。

请参见第 41 页的“[关于 Symantec Data Loss Prevention](#)”。

请参见第 919 页的“[关于 Network Discover](#)”。

关于 Network Protect

Network Protect 通过从网络服务器或台式机的开放文件共享文件夹中，删除暴露的机密数据、知识产权和机密信息，以降低您的风险。请注意，没有单独的 Network Protect Server，Network Protect 产品模块会将保护功能添加至 Network Discover Server。

Network Protect 可让组织具备以下能力：

- 隔离暴露的文件。Network Protect 可自动将那些违反策略的文件移动至隔离区域，该区域会重新创建源文件结构以方便查找。（可选）Symantec Data Loss Prevention 可以在违规文件的原始位置放置标记文本文件。该标记文件会说明隔离原始文件的原因与位置。
- 复制暴露的或可疑的文件。Network Protect 可自动将那些违反策略的文件复制到隔离区域。隔离区域可重新创建源文件结构以方便查找，并将原始文件保留在原来的位置。
- 隔离文件还原。Network Protect 可以轻松将已隔离的文件还原至其原始位置或新位置。
- 执行访问控制和加密策略。Network Protect 可预先确保员工遵从现有的访问控制与加密策略。

请参见第 41 页的“[关于 Symantec Data Loss Prevention](#)”。

请参见第 992 页的“[为文件共享配置 Network Protect](#)”。

关于 Endpoint Discover

Endpoint Discover 会检测台式或便携式端点计算机上的敏感数据。它至少包括一个 Endpoint Server 和至少一个在端点计算机上运行的 Symantec DLP Agent。您可以将多个 Symantec DLP Agent 连接到单个 Endpoint Server。Symantec DLP Agent：

- 检测端点文件系统中的敏感数据。
- 收集该活动的数据。
- 将事件发送至 Endpoint Server。
- 如有必要，将数据发送至相关联的 Endpoint Server 以进行分析。

请参见第 1127 页的“[关于 Endpoint Discover 和 Endpoint Prevent](#)”。

请参见第 41 页的“[关于 Symantec Data Loss Prevention](#)”。

关于 Endpoint Prevent

Endpoint Prevent 检测并防止敏感数据从台式或便携式端点计算机移出。它至少包括一个 Endpoint Server 和在连接至该 Endpoint Server 的端点系统上运行的所有 Symantec DLP Agent。您可以将多个 Symantec DLP Agent 连接至单个 Endpoint Server。Endpoint Prevent 会检测以下数据传输形式：

- 应用程序监控
- CD/DVD
- 剪贴板

- 电子邮件/SMTP
- eSATA 可移动驱动器
- FTP
- HTTP/HTTPS
- IM
- 网络共享
- 打印机/传真
- USB 可移动介质设备

请参见第 1127 页的“[关于 Endpoint Discover 和 Endpoint Prevent](#)”。

请参见第 41 页的“[关于 Symantec Data Loss Prevention](#)”。

关于 Symantec Data Loss Prevention for Mobile

Symantec Data Loss Prevention for Mobile (以后称为 Mobile Prevent) 监控来自移动设备的电子邮件、Web 和应用程序通信，以防从组织内发出敏感信息。与企业网络的连接建立后，所有网络流量都会发送至 Mobile Prevent for Web Server 进行分析。这样既可保护组织的敏感信息，同时又使移动设备用户可访问 Facebook、Dropbox 和 Twitter 等站点和应用程序。

利用 Mobile Prevent 可执行下列活动：

- 监视移动设备上通过 HTTP、HTTPS 或 FTP 流量外泄的机密信息。
- 阻止移动设备上通过 HTTP、HTTPS 或 FTP 流量外泄的机密信息。
- 补救源自移动设备的事件。

请参见第 1230 页的“[关于移动设备管理](#)”。

请参见第 1231 页的“[实施 Mobile Prevent](#)”。

请参见第 41 页的“[关于 Symantec Data Loss Prevention](#)”。

关于 Symantec Enterprise Vault 数据分类服务

Symantec Enterprise Vault 数据分类服务使用 Symantec Data Loss Prevention 检测技术自动对在 Symantec Enterprise Vault for Microsoft Exchange 中管理的 Microsoft Exchange 邮件进行分类。Discovery Accelerator 和 Compliance Accelerator (与 Enterprise Vault 数据分类服务解决方案分开提供) 在搜索或审核期间使用分类标记对邮件进行过滤。

Symantec Enterprise Vault 数据分类服务解决方案使用以下组件：

- Symantec Enterprise Vault for Microsoft Exchange - 为 Microsoft Exchange 邮件的存档提供框架。
- Enterprise Vault 数据分类过滤器 – 与 Symantec Enterprise Vault for Microsoft Exchange 一起工作，将 Exchange 邮件发布到分类服务器，并接收来自分类服务器的邮件分类结果。然后，Symantec Enterprise Vault for Microsoft Exchange 根据分类结果删除邮件或对邮件进行存档和分类。
- 分类服务器 – 分类服务器是一种新的 Symantec Data Loss Prevention 检测服务器，它从 Enterprise Vault 数据分类过滤器接收邮件，并将策略应用于邮件以生成分类结果。分类服务器可以使用任何可用的 Symantec Data Loss Prevention 检测技术（包括 EDM、IDM 和 DCM）评估 Exchange 邮件。该服务器也可以使用特定于分类的新检测规则来基于邮件属性（MAPI 属性）评估 Exchange 邮件。
分类服务器的安装和注册方式与其他 Symantec Data Loss Prevention 检测服务器相同。有关更多信息，请参见《Symantec Data Loss Prevention 安装指南》。
- 分类策略 – 不是生成 Symantec Data Loss Prevention 事件，分类策略使用“对 **Enterprise Vault 内容进行分类**”响应规则操作来生成分类结果，并将该结果返回到 Enterprise Vault 数据分类过滤器。响应规则配置指示分类结果应通知 Enterprise Vault 对邮件进行存档还是删除邮件。对于已存档的邮件，响应规则还指定应分配给邮件的保留类别和分类标记。该规则还确定 Enterprise Vault for Microsoft Exchange 是否应在遵从性审阅中包含已存档的邮件，还是应将这些邮件排除以供进一步审阅。对于未存档的邮件，该响应规则指定 Enterprise Vault for Microsoft Exchange 删除这些邮件时应使用的方法。

注意：分类服务器仅用于 Symantec Enterprise Vault 数据分类服务解决方案，该解决方案独立于 Symantec Data Loss Prevention 进行授权。您必须配置 Enterprise Vault Exchange 代理过滤器和分类服务器，使其相互通信。有关更多信息，请参见 *Symantec Enterprise Vault Data Classification Services Implementation Guide*（《Symantec Enterprise Vault 数据分类服务操作指南》）。

使用用于配置 Symantec Data Loss Prevention 策略的相同 Enforce Server 管理控制台页面来配置分类策略。不过，仅当您已获得分类服务器使用授权时，MAPI 检测规则和分类响应操作才适用。

快速了解如何管理 Symantec Data Loss Prevention

本章节包括下列主题：

- [关于 Symantec Data Loss Prevention 管理](#)
- [关于 Enforce Server 管理控制台](#)
- [登录和注销 Enforce Server 管理控制台](#)
- [关于 Administrator 帐户](#)
- [执行初始设置任务](#)
- [更改 Administrator 密码](#)
- [为 Administrator 添加电子邮件帐户](#)
- [编辑用户配置文件](#)
- [更改密码](#)

关于 Symantec Data Loss Prevention 管理

Symantec Data Loss Prevention 系统由一个 Enforce Server 和一个或多个检测服务器组成。

Enforce Server 存储所有系统配置、策略、保存的报告以及其他 Symantec Data Loss Prevention 信息并管理所有活动。

从通过 Firefox 或 Internet Explorer Web 浏览器访问的 Enforce Server 管理控制台执行系统管理。您登录后即会显示 Enforce 控制台。

请参见第 50 页的“[关于 Enforce Server 管理控制台](#)”。

在首次完成《Symantec Data Loss Prevention 安装指南》中的安装步骤后，必须执行初始配置任务以启动并运行 Symantec Data Loss Prevention。您必须执行这些基本任务，系统才能开始监视网络上的数据。

请参见第 52 页的“[执行初始设置任务](#)”。

关于 Enforce Server 管理控制台

您可以通过 Enforce Server 管理控制台管理 Symantec Data Loss Prevention 系统。

管理员用户可以看到并访问管理控制台的所有组件。其他用户只能看到其角色被授予访问权限的组件。当前登录的用户帐户会出现在屏幕的右上方。

当您第一次登录管理控制台时，会显示“主页”屏幕。要导航整个系统，请从四个菜单群集（“主页”、“事件”、“策略”和“系统”）之一中选择项目。要访问联机帮助，请单击屏幕右上方的“帮助”。

下列导航和操作图标位于管理控制台的右上方：

表 2-1 管理控制台导航和操作图标

图标	说明
	返回上一个屏幕。Symantec 建议您使用此“上一步”按钮而非浏览器的“上一步”按钮。使用浏览器的“上一步”按钮可能会导致预想不到的行为，因此建议不要使用。
	屏幕刷新。Symantec 建议您使用此“刷新”按钮而非浏览器的“重新加载”或“刷新”按钮。使用浏览器的按钮可能会导致预想不到的行为，因此建议不要使用。
	将当前报告发送到打印机。如果不能将当前屏幕内容发送到打印机，则此图标不可用。
	将当前报告通过电子邮件发送到一个或多个接受者。如果当前屏幕内容不能通过电子邮件发送，则此图标不可用。

请参见第 51 页的“[登录和注销 Enforce Server 管理控制台](#)”。

登录和注销 Enforce Server 管理控制台

如果您分配有多个角色，您一次只能以一个角色登录。在登录时必须指定角色名和用户名。

登录到 Enforce Server

- 1 在 Enforce Server 主机上，打开浏览器并导航至服务器的 URL（由 Symantec Data Loss Prevention 管理员提供）。
- 2 在 Symantec Data Loss Prevention 登录屏幕上的“**登录名**”字段中输入用户名。对于管理员角色，该用户名始终是Administrator。具有多个角色的用户应以role\user格式（例如，ReportViewer\bsmith）指定角色名和用户名。如果没有这样做，Symantec Data Loss Prevention会在用户登录时为其分配一个角色。
请参见第 85 页的“[配置角色](#)”。
- 3 在“**密码**”字段中，键入密码。对于首次登录的管理员，该密码是您在安装期间创建的密码。
有关安装详细信息，请参见相应的《Symantec Data Loss Prevention 安装指南》。
- 4 单击“**登录**”。

此时将出现 Enforce Server 管理控制台。管理员可以访问管理控制台的所有部分，但是其他用户只能看到为该特定角色授权的那些部分。

注销 Enforce Server

- 1 单击屏幕右上方的“**注销**”。
- 2 单击“**确定**”进行确认。

Symantec Data Loss Prevention 会显示确认注销成功的消息。

请参见第 54 页的“[编辑用户配置文件](#)”。

关于 Administrator 帐户

Symantec Data Loss Prevention 系统预配置有一个永久帐户：Administrator。请注意，名称要区分大小写，并且不能更改。该帐户的密码是在安装期间配置的。

有关更多信息，请参考《Symantec Data Loss Prevention 安装指南》。

只有Administrator 帐户才可以看到并修改Administrator 帐户。因为Administrator 始终对系统的每个部分都有访问权限，所以“角色”选项不出现在“[配置管理员](#)”屏幕上。

请参见第 52 页的“[更改 Administrator 密码](#)”。

请参见第 53 页的“[为 Administrator 添加电子邮件帐户](#)”。

执行初始设置任务

在首次完成《Symantec Data Loss Prevention 安装指南》中的安装步骤后，必须执行初始配置任务以启动并运行 Symantec Data Loss Prevention。您必须执行这些基本任务，系统才能开始监视网络上的数据。

- 将 Administrator 密码更改为只有您知道的唯一密码，并为 Administrator 用户帐户添加电子邮件地址，以便您可以收到各种系统事件通知。
请参见第 51 页的“[关于 Administrator 帐户](#)”。
- 添加并配置检测服务器。
请参见第 187 页的“[添加检测服务器](#)”。
请参见第 176 页的“[服务器配置 - 基本](#)”。
- 除 Symantec Data Loss Prevention 解决方案软件包提供的用户帐户之外，您可以根据需要添加任意用户帐户。
- 查看随 Symantec Data Loss Prevention 解决方案软件包提供的策略模板，自行熟悉其内容和数据要求。根据需要修订策略或创建新策略。
- 添加您计划与策略进行关联的数据配置文件。
并非始终需要数据配置文件。仅在您有权使用数据配置文件，且打算在策略中使用数据配置文件时，才需要执行此步骤。

更改 Administrator 密码

安装过程中，您为 Administrator 帐户创建了一个常规密码。首次登录时，应将该密码更改为具有唯一性和保密性的密码。

有关更多信息，请参见《Symantec Data Loss Prevention 安装指南》。

密码区分大小写，并且必须至少包含八个字符。

请注意，您可以将 Symantec Data Loss Prevention 配置为要求强密码。强密码经过专门设计，不容易被破解。在“系统”>“设置”>“常规”>“配置”屏幕上配置密码策略。

密码到期后，Symantec Data Loss Prevention 会在下次登录时显示“密码更新”窗口。显示“密码更新”窗口时，请键入旧密码，然后键入新密码并进行确认。

请参见第 91 页的“[配置用户帐户](#)”。

更改 Administrator 密码

- 1 用 Administrator 帐户登录。
- 2 采取以下其中一个操作：

■ 单击管理控制台右上角的“配置文件”。

■ 转至“系统”>“用户管理”>“用户”，单击 Administrator。

将显示“配置管理员”屏幕。

3 在“配置管理员”屏幕上：

■ 在“旧密码”字段中输入当前（旧）密码。

■ 在“新密码”字段中输入新密码。

■ 在“重新输入新密码”字段中重新输入新密码。两次输入的新密码必须相同。

请注意，密码区分大小写。

4 单击“保存”。

请参见第 51 页的“[关于 Administrator 帐户](#)”。

请参见第 50 页的“[关于 Enforce Server 管理控制台](#)”。

请参见第 191 页的“[关于系统概述屏幕](#)”。

为 Administrator 添加电子邮件帐户

您可以指定用于接收与管理员帐户相关的邮件的电子邮件地址。

添加或更改 Administrator 的电子邮件帐户

1 转至“系统”>“用户管理”>“用户”，单击 Administrator。

2 在显示的“编辑配置文件”屏幕上的“旧密码”字段中键入 Administrator 帐户的密码。

3 在“电子邮件地址”字段中键入新的（或更改后的）Administrator 帐户的电子邮件地址。

电子邮件地址必须包括完全限定的域名。例如：my_name@acme.com。

4 单击“保存”。

请参见第 51 页的“[关于 Administrator 帐户](#)”。

请参见第 50 页的“[关于 Enforce Server 管理控制台](#)”。

请参见第 191 页的“[关于系统概述屏幕](#)”。

编辑用户配置文件

系统用户可以使用“配置文件”屏幕配置其配置文件密码、电子邮件地址和语言。

用户还可以在“配置文件”屏幕中指定其报告首选项。

要显示“配置文件”屏幕，请单击 Enforce Server 管理控制台右上角的“配置文件”。

“配置文件”屏幕分为以下几部分：

- **常规**。使用该部分可更改密码、指定电子邮件地址以及选择语言首选项。
- **报告首选项**。使用该部分可指定首选文本编码、CSV 分隔符和 XML 导出首选项。
- **角色**。该部分显示您的角色。请注意，该部分不向管理员显示，因为管理员具有执行所有角色的权限。

“常规”部分：

更改密码

- 1 在“旧密码”字段中输入当前有效的密码。
- 2 在“新密码”字段中输入新密码。
- 3 在“重新输入新密码”字段中重新输入新密码。
- 4 单击“保存”。

下次登录时必须使用新密码。

请参见第 56 页的“[更改密码](#)”。

指定新的个人电子邮件地址

- 1 在“旧密码”字段中输入当前有效的密码。
- 2 在“电子邮件地址”字段中输入您的个人电子邮件地址。
- 3 单击“保存”。

Symantec Data Loss Prevention 的各个用户都可以选择他们要使用的可用语言和区域设置。

选择个人使用的语言

- 1 在 Enforce Server 管理控制台上，单击屏幕右上角的“配置文件”。
此时将显示您的配置文件。
- 2 在屏幕的“常规”部分，在“旧密码”字段中输入密码。

3 单击所选语言旁边的选项。

4 单击“保存”。

Enforce Server 管理控制台将会以新的语言重新显示。

选择语言配置文件对策略违规检测没有任何影响。不管选择哪种配置文件语言，都会对以任意支持语言编写的所有内容执行检测。

请参见第 57 页的[“关于字符集、语言和区域设置支持”](#)。

可供使用的语言是在安装产品时确定的，之后可以为 Symantec Data Loss Prevention 添加语言包。选择其他语言的效果如下：

■ 仅区域设置。如果选择的语言具有“无法翻译”通知，则日期和数字会以适合该语言的格式显示。报告和列表会按照该语言进行排序。但是管理控制台中的菜单、标签、屏幕和帮助系统没有翻译，仍采用英语。

请参见第 61 页的[“关于区域设置”](#)。

■ 已翻译。所选语言可能不会显示“无法翻译”通知。在这种情况下，除了数字和日期格式以及排序顺序之外，管理控制台菜单、标签、屏幕，某些情况下甚至包括帮助系统，也都翻译成所选语言。

请参见第 61 页的[“关于 Symantec Data Loss Prevention 语言包”](#)。

“报告首选项”部分：

选择文本编码

1 在“旧密码”字段中输入当前有效的密码。

2 选择文本编码选项：

■ 使用浏览器默认编码。选中此框可指定文本文件使用与浏览器相同的编码。

■ 下拉菜单。单击下拉菜单中的一个编码选项将其选中。

3 单击“保存”。

新文本编码将应用于 CSV 导出文件。此编码使您能够选择与 CSV 应用程序所期望的编码相匹配的文本编码。

选择 CSV 分隔符

1 在“旧密码”字段中输入当前有效的密码。

2 从下拉菜单中选择一种分隔符。

3 单击“保存”。

新分隔符将应用于下一个导出的逗号分隔值 (CSV) 列表。

请参见第 777 页的[“关于事件报告”](#)。

请参见第 795 页的[“导出事件报告”](#)。

选择 XML 导出详细信息

- 1 在“旧密码”字段中输入当前有效的密码。
- 2 在**XML导出中包括事件违规信息**。如果选中此框，则导出到 XML 的报告会在每个事件快照中包括突出显示的匹配项。
- 3 在**XML导出中包括事件历史记录**。如果选中此框，则导出到 XML 的报告会包括每个事件快照的“历史记录”选项卡中包含的事件历史记录数据。
- 4 单击“保存”。

所选设置将应用于下一个导出到 XML 的报告。

如果两个框均未选中，则导出的 XML 报告仅包含基本的事件信息。

请参见第 777 页的[“关于事件报告”](#)。

请参见第 795 页的[“导出事件报告”](#)。

更改密码

密码到期后，系统会在您下次尝试登录时要求您指定一个新密码。如果系统要求您更改密码，会显示“密码更新”窗口。

从“密码更新”窗口更改密码

- 1 在“密码更新”窗口的“旧密码”字段中输入旧密码。
- 2 在“密码更新”窗口的“新密码”字段中输入新密码。
- 3 在“密码更新”窗口的“重新输入新密码”字段中重新输入新密码。

下次登录时必须使用新密码。

您还可以从“配置文件”屏幕随时更改您的密码。

请参见第 54 页的[“编辑用户配置文件”](#)。

请参见第 51 页的[“关于 Administrator 帐户”](#)。

请参见第 51 页的[“登录和注销 Enforce Server 管理控制台”](#)。

使用语言和区域设置

本章节包括下列主题：

- [关于字符集、语言和区域设置支持](#)
- [支持的检测语言](#)
- [使用国际字符](#)
- [关于 Symantec Data Loss Prevention 语言包](#)
- [关于区域设置](#)
- [在 Enforce Server 管理控制台上使用非英文语言](#)
- [使用 Language Pack Utility](#)

关于字符集、语言和区域设置支持

Symantec Data Loss Prevention 通过提供大量的语言和本地化选项完全支持国际部署：

- 跨多种语言的策略创建和违规检测。
受支持语言可用于关键字、数据标识符、正则表达式、确切数据配置文件(EDM)和文档配置文件(IDM)。
请参见第 58 页的[表 3-1](#)。
- Windows 操作系统的本地化版本和多语言用户界面(MUI)版本上的操作。
- 国际字符集。要查看并使用国际字符集，您查看 Enforce Server 管理控制台时所处的系统必须有相应的功能。
请参见第 60 页的[“使用国际字符”](#)。
- 基于区域设置的日期和数字格式，以及列表和报告的排序顺序。
请参见第 61 页的[“关于区域设置”](#)。

- 本地化的用户界面 (UI) 和帮助系统。Symantec Data Loss Prevention 的语言包为 Enforce Server 管理控制台提供了特定的语言版本。它们可能还提供特定语言版本的联机帮助系统。

注意：这些语言包是在产品初始安装后单独添加的。

- 本地化的产品文档。

支持的检测语言

Symantec Data Loss Prevention 支持检测很多语言。可以将策略定义为准确检测和报告在这些语言的内容中发现的违规。

表 3-1 Symantec Data Loss Prevention 支持的语言

语言	9.x 版	10.0 版	10.5 版	11.0、11.1.x、 11.5、11.6 版
阿拉伯语		支持	支持	支持
葡萄牙语（巴西）		支持	支持	支持
繁体中文	支持	支持	支持	支持
简体中文	支持	支持	支持	支持
捷克语		支持	支持	支持
丹麦语	支持	支持	支持	支持
荷兰语	支持	支持	支持	支持
英语	支持	支持	支持	支持
芬兰语	支持	支持	支持	支持
法语	支持	支持	支持	支持
德语	支持	支持	支持	支持
希腊语		支持	支持	支持
希伯来语	支持	支持	支持	支持
匈牙利语		支持	支持	支持
意大利语	支持	支持	支持	支持

语言	9.x 版	10.0 版	10.5 版	11.0、11.1.x、 11.5、11.6 版
日语	支持	支持	支持	支持
韩语	支持	支持	支持	支持
挪威语	支持	支持	支持	支持
波兰语		支持	支持	支持
葡萄牙语	支持	支持	支持	支持
罗马尼亚语		支持	支持	支持
俄语	支持	支持	支持	支持
西班牙语	支持	支持	支持	支持
瑞典语	支持	支持	支持	支持
土耳其语		支持*	支持*	支持*

*不能将 Symantec Data Loss Prevention 安装在本地化为土耳其语的 Windows 操作系统上，也不能将土耳其语作为备用区域设置。

有关特定语言的其他信息，请参见《Symantec Data Loss Prevention 版本说明》。
此支持并未隐含以下功能：

- 以非英语语言提供的技术支持。原因是 Symantec Data Loss Prevention 支持一种特定语言并不意味着用该语言提供技术支持。
- 本地化管理用户界面 (UI) 和文档。支持某种语言并不意味着 UI 或产品文档已本地化为该语言。不过即使 UI 没有本地化，用户定义的 UI 部分（如端点上的弹出式通知消息）依然可以通过在 UI 中输入相应文本来本地化为任意语言。
- 本地化内容。关键字用在产品的多个区域，包括策略模板和数据标识符。支持某种语言并不意味着这些关键字已翻译成该语言。然而，用户可通过 Enforce Server 管理控制台以新语言添加关键字。
- 新文件类型、协议、应用程序或编码。支持某种语言并不意味着支持该语言或区域可能已流行的任何新文件类型、协议、应用程序或编码，但产品已支持的新文件类型、协议、应用程序或编码除外。
- 特定于语言的规范化。一个规范化的示例就是将字符的重音版本和非重音版本视为相同。产品已执行了一些规范化，包括标准 Unicode 规范化，这应该涵盖绝大多数情况。但是，这并不意味着包括所有潜在的规范化。

- 特定于区域的规范化和验证。例如产品具有北美电话号码格式的意识，这将允许产品将号码的不同版本视为相同，并用EDM源文件识别无效的号码。支持某种语言并不意味着支持该语言或区域的此种功能。

这些排除的类别中的项目在特定于语言或区域的基础上被跟踪为个别产品改进。请联系 Symantec 支持部门，以获取语言相关改进的更多信息，以及未列出的语言的计划。

请参见第 57 页的“[关于字符集、语言和区域设置支持](#)”。

使用国际字符

在 Symantec Data Loss Prevention 中，可以基于以下内容使用各种语言：

- 查看 Enforce Server 管理控制台的计算机上安装的基于操作系统的字符集
- 浏览器的功能

例如，关于俄语数据扫描的事件报告将包含西里尔字符。要查看该报告，用于访问 Enforce Server 管理控制台的计算机和浏览器必须能够显示这些字符。以下是一些常规指南：

- 如果用于访问 Enforce Server 管理控制台的计算机具有本地化为特定语言的操作系统，您应能够查看并使用支持该语言的字符集。
- 如果用于访问管理控制台的计算机的操作系统没有本地化为特定语言，则可能需要添加附加的语言支持。将此附加的语言支持添加到您用于访问管理控制台的计算机，而不是 Enforce Server。
 - 在 Windows 系统上，可以使用“控制面板”>“区域和语言选项”>“语言”（选项卡）-“附加的语言支持”添加附加的语言支持，以添加某些字符集的字体。
 - 可能还需要设置浏览器以配合使用要查看和输入的字符。

注意：Enforce Server 管理控制台支持 UTF-8 编码的数据。

- 在 Windows 系统上，可能也需要使用“控制面板”>“区域和语言选项”下的“语言”-“附加的语言支持”选项卡来添加某些字符集的字体。

有关特定语言的已知问题，请参见《Symantec Data Loss Prevention 版本说明》。

请参见第 57 页的“[关于字符集、语言和区域设置支持](#)”。

关于 Symantec Data Loss Prevention 语言包

在基于 Windows 的系统上，Symantec Data Loss Prevention 的语言包可以将产品本地化为特定语言。将语言包添加 Symantec Data Loss Prevention 之后，管理员可将其指定为系统范围的默认值。如果管理员已添加了多个语言包以供使用，各个用户可以选择各自要使用的语言。

请参见第 62 页的“[在 Enforce Server 管理控制台上使用非英文语言](#)”。

选择语言包后，结果如下：

- Enforce Server 的“配置”屏幕中的管理员和最终用户均可以使用其区域设置。
- Enforce Server 的屏幕、菜单项、命令和消息均以该语言显示。
- Symantec Data Loss Prevention 帮助系统可能会以该语言显示。

Symantec Data Loss Prevention 的语言包可从 [Symantec File Connect](#) 获取。

小心：在安装新版本的 Symantec Data Loss Prevention 时，将删除已安装的所有语言包。对于新的 Symantec Data Loss Prevention 本地化版本，必须升级到新版本的语言包。

请参见第 61 页的“[关于区域设置](#)”。

请参见第 57 页的“[关于字符集、语言和区域设置支持](#)”。

关于区域设置

区域设置提供下列功能：

- 以适合该区域设置的格式显示日期和数字。
- 根据区域设置的规则，对基于文本列（如“策略名称”或“文件所有者”）的列表和报告按字母顺序进行排序。

区域设置随语言包一起安装。

管理员也可以配置附加区域设置以供各个用户使用。该附加区域设置只需受所需的 Java 版本的支持。

有关这些区域设置的列表，请参见

<http://java.sun.com/j2se/version/docs/guide/intl/locale.doc.html>，其中 *version* 为当前所支持的 Java 版本。

除土耳其以外，可以使用列为“完全支持的区域设置”或“提供但未经测试的区域设置”的任何区域设置。英语是默认的区域设置，所以不需要单独选择。

如《Symantec Data Loss Prevention 安装指南》中所述，可以在安装产品时指定区域设置，也可以日后使用 Language Pack Utility 配置区域设置。

请参见第 62 页的“[在 Enforce Server 管理控制台上使用非英文语言](#)”。

请参见第 57 页的“[关于字符集、语言和区域设置支持](#)”。

在 Enforce Server 管理控制台上使用非英文语言

区域设置和语言的使用由下列角色通过 Enforce Server 管理控制台指定：

- Symantec Data Loss Prevention 管理员。将某种可用语言指定为系统范围的默认语言并设置区域设置。
- 各 Symantec Data Loss Prevention 用户。选择要使用的可用区域设置。

注意：添加多个语言包可能会对 Enforce Server 的性能略有影响，具体取决于存在的语言和自定义的数量。出现这种情况的原因是必须为每种语言另行建立和维护一组索引。

警告：请不要修改 Oracle 数据库的 NLS_LANGUAGE 和 NLS_TERRITORY 设置。

请参见第 61 页的“[关于 Symantec Data Loss Prevention 语言包](#)”。

请参见第 61 页的“[关于区域设置](#)”。

Symantec Data Loss Prevention 管理员可以指定将哪种可用语言用作默认系统范围的语言。

选择所有用户的默认语言

- 1 在 Enforce Server 上，转至“系统”>“设置”>“常规”，然后单击“配置”。
将显示“编辑常规设置”屏幕。
- 2 滚动至“编辑常规设置”屏幕的“语言”部分，然后单击您要用作系统范围的默认语言旁边的按钮。
- 3 单击“保存”。

各 Symantec Data Loss Prevention 用户可以通过更新其配置文件来选择要使用的可用语言和区域设置。

请参见第 54 页的“[编辑用户配置文件](#)”。

管理员可以使用 Language Pack Utility 更新可用语言。

请参见第 63 页的“[使用 Language Pack Utility](#)”。

请参见第 57 页的“[关于字符集、语言和区域设置支持](#)”。

注意：如果 Enforce Server 在 Linux 主机上运行，您必须使用 Linux Package Manager 应用程序在主机上安装语言字体。语言字体包以 fonts-<语言名称> 开头。例如，fonts-japanese-0.20061016-4.el5.noarch

使用 Language Pack Utility

要使某特定区域设置可用于 Symantec Data Loss Prevention，请通过 Language Pack Utility 添加语言包。

请从命令行运行 Language Pack Utility。其可执行文件 LanguagePackUtility.exe 驻留于 \Vontu\Protect\bin 目录中。

要使用 Language Pack Utility，您必须具有所有 \Vontu 文件夹和子文件夹的“读取”、“写入”和“执行”权限。

要显示该实用程序的帮助（例如有效选项及其标志的列表），请输入不带任何标志的 LanguagePackUtility。

注意：运行 Language Pack Utility 会导致 VontuManager 和 VontuIncidentPersister 服务停止约 20 秒。登录到 Enforce Server 管理控制台的任何用户均将自动注销。当其更新完成后，该实用程序会自动重新启动上述服务，用户可以重新登录到管理控制台。

可以从 Symantec [File Connect](#) 获取 Symantec Data Loss Prevention 语言包。

添加语言包 (Windows)

- 1 建议当前使用 Enforce Server 管理控制台的任何其他用户务必保存各自的工作信息并进行注销。
- 2 运行 Language Pack Utility，其 -a 标志后跟该语言包的 ZIP 文件的名称。输入：

LanguagePackUtility -a *filename*

其中 *filename* 是语言包 ZIP 文件的完全限定路径和名称。

例如，如果日语语言包 ZIP 文件存储在 c:\temp 中，请通过输入下列内容将其添加：

LanguagePackUtility -a c:\temp\Symantec_DLP_10.5_Lang_Pack-JP.zip

要在同一会话期间添加多个语言包，请指定多个文件名（以空格分隔），例如：

**LanguagePackUtility -a
c:\temp\Symantec_DLP_10.5_Lang_Pack-TW.zip
Symantec_DLP_10.5_Lang_Pack-CS.zip**

- 3 登录到 Enforce Server 管理控制台，并在“编辑常规设置”屏幕上确认新的语言选项是否可用。为此，请转到“系统”>“设置”>“常规”>“配置”>“编辑常规设置”。

添加语言包 (Linux)

- 1 建议当前使用 Enforce Server 管理控制台的任何其他用户务必保存各自的工作信息并进行注销。

- 2 打开到 Enforce Server 主机的终端会话，然后通过运行以下命令切换到 DLP 系统帐户：

su - DLP 系统帐户

- 3 运行下列命令：

DLP_home/Protect/bin/LanguagePackUtility -a <语言包 zip 文件的路径>

- 4 登录到 Enforce Server 管理控制台，并在“编辑常规设置”屏幕上确认新的语言选项是否可用。为此，请转到“系统”>“设置”>“常规”>“配置”>“编辑常规设置”。

删除语言包

- 1 建议当前使用 Enforce Server 管理控制台的任何用户务必保存各自的工作信息并进行注销。
- 2 运行 Language Pack Utility，其 -r 标志后跟要删除的语言包的 Java 区域设置代码。输入：

LanguagePackUtility -r *locale*

其中，*locale* 是一个与 Symantec Data Loss Prevention 语言包相对应的有效 Java 区域设置代码。

例如，要删除法语语言包，请输入：

LanguagePackUtility -r fr_FR

要在同一会话期间删除多个语言包，请指定多个文件名，以空格分隔。

- 3 登录到 Enforce Server 管理控制台，并在“编辑常规设置”屏幕上确认该语言包是否不再可用。为此，请转到“系统”>“设置”>“常规”>“配置”>“编辑常规设置”。

删除语言包会有下列影响：

- 用户不可以再选择单独使用已删除语言包的区域设置。

注意：如果某语言包的区域设置受运行 Symantec Data Loss Prevention 所需的 Java 版本支持，则管理员稍后可将该区域设置指定为备用区域设置，供任何需要的用户使用。

- 区域设置会恢复为管理员所配置的系统范围的默认值。
- 如果删除的语言是系统范围的默认区域设置，则系统区域设置会恢复为英语。

更改或添加区域设置

- 1 建议当前使用 Enforce Server 管理控制台的任何用户务必保存各自的工作信息并进行注销。
- 2 运行 Language Pack Utility，其 -c 标志后跟要更改或添加的区域设置的 Java 区域设置代码。请输入：

LanguagePackUtility -c *locale*

其中 *locale* 是一个可被 Java 识别的有效区域设置代码，例如表示葡萄牙语的 pt_PT。

例如，要将区域设置更改为葡萄牙语（巴西），请输入：

LanguagePackUtility -c pt_BR

- 3 登录到 Enforce Server 管理控制台，并在“编辑常规设置”屏幕上确认新的备用区域设置目前是否可用。为此，请转到“系统”>“设置”>“常规”>“配置”>“编辑常规设置”。

如果您指定了没有语言包的区域设置，则区域设置名称旁会显示“翻译不可用”。这意味着格式和排序顺序适用于该区域设置，但没有转换 Enforce Server 管理控制台屏幕和联机帮助。

注意：管理员仅可以为用户提供一种不基于先前安装的 Symantec Data Loss Prevention 语言包的附加区域设置。

请参见第 57 页的“[关于字符集、语言和区域设置支持](#)”。

2

部分

管理 Enforce Server 平台

- 4. 管理 Enforce Server 服务和设置
- 5. 管理角色和用户
- 6. 连接到组目录
- 7. 管理存储的凭据
- 8. 管理系统事件和消息
- 9. 添加新的产品模块
- 10. 集成 Enforce 与 Symantec Protection Center (SPC)
- 11. 将 Symantec Data Loss Prevention 服务器迁移到 64 位操作系统

管理 Enforce Server 服务和设置

本章节包括下列主题：

- [关于 Enforce Server 服务](#)
- [关于在 Windows 上启动和停止服务](#)
- [在 Linux 上启动和停止服务](#)

关于 Enforce Server 服务

可能需要定期停止和启动 Symantec Data Loss Prevention 服务。本节提供了每项服务以及如何在支持的平台上启动和停止这些服务的简要说明。

下表中说明了 Enforce Server 的 Symantec Data Loss Prevention 服务：

表 4-1 Enforce Server 上的服务

服务名称	说明
Vontu Manager	为 Symantec Data Loss Prevention 提供集中式报告与管理服务。
Vontu Monitor Controller	控制检测服务器（监视器）。
Vontu Notifier	提供数据库通知。
Vontu Incident Persister	将事件写入数据库。
Vontu Update	安装 Symantec Data Loss Prevention 系统更新。此服务仅在系统更新与升级期间运行。

请参见第 70 页的“[关于在 Windows 上启动和停止服务](#)”。

关于在 Windows 上启动和停止服务

启动和停止服务的过程会视安装配置以及是 Enforce Server 还是检测服务器而有所不同。

- 请参见第 70 页的“[在 Windows 上启动 Enforce Server](#)”。
- 请参见第 70 页的“[在 Windows 上停止 Enforce Server](#)”。
- 请参见第 71 页的“[在 Windows 上启动检测服务器](#)”。
- 请参见第 71 页的“[在 Windows 上停止检测服务器](#)”。
- 请参见第 72 页的“[在单层 Windows 安装上启动服务](#)”。
- 请参见第 72 页的“[在单层 Windows 安装上停止服务](#)”。

在 Windows 上启动 Enforce Server

使用以下过程，在 Windows Enforce Server 上启动 Symantec Data Loss Prevention 服务。

在 Windows Enforce Server 上启动 Symantec Data Loss Prevention 服务

- 1 在托管 Enforce Server 的计算机上，导航至“开始”>“所有程序”>“管理工具”>“服务”，打开 Windows 的“服务”菜单。
- 2 启动其他 Symantec Data Loss Prevention 服务之前，请先启动 Vontu Notifier 服务。
- 3 启动其余的 Symantec Data Loss Prevention 服务，包括：
 - Vontu Manager
 - Vontu Incident Persister
 - Vontu Update
 - Vontu Monitor Controller

请参见第 70 页的“[在 Windows 上停止 Enforce Server](#)”。

在 Windows 上停止 Enforce Server

使用以下过程，在 Windows Enforce Server 上停止 Symantec Data Loss Prevention 服务。

在 Windows Enforce Server 上停止 Symantec Data Loss Prevention 服务

- 1 在托管 Enforce Server 的计算机上，导航至“开始”>“所有程序”>“管理工具”>“服务”，打开 Windows 的“服务”菜单。
- 2 从“服务”菜单中，停止所有运行中的 Symantec Data Loss Prevention 服务，其中可能包括：
 - Vontu Update
 - Vontu Incident Persister
 - Vontu Manager
 - Vontu Monitor Controller
 - Vontu Notifier

请参见第 70 页的“[在 Windows 上启动 Enforce Server](#)”。

在 Windows 上启动检测服务器

在 Windows 检测服务器上启动 Symantec Data Loss Prevention 服务

- 1 在托管检测服务器的计算机上，导航至“开始”>“所有程序”>“管理工具”>“服务”，打开 Windows 的“服务”菜单。
- 2 启动 Symantec Data Loss Prevention 服务，其中可能包括：
 - Vontu Monitor
 - Vontu Update

请参见第 71 页的“[在 Windows 上停止检测服务器](#)”。

在 Windows 上停止检测服务器

使用以下过程，在 Windows 检测服务器上停止 Symantec Data Loss Prevention 服务。

在 Windows 检测服务器上停止 Symantec Data Loss Prevention 服务

- 1 在托管检测服务器的计算机上，导航至“开始”>“所有程序”>“管理工具”>“服务”，打开 Windows 的“服务”菜单。
- 2 从“服务”菜单中，停止所有运行中的 Symantec Data Loss Prevention 服务，其中可能包括：
 - Vontu Update
 - Vontu Monitor

请参见第 71 页的“[在 Windows 上启动检测服务器](#)”。

在单层 Windows 安装上启动服务

使用以下过程，在 Windows 中的单层安装上启动 Symantec Data Loss Prevention 服务。

在 Windows 中的单层安装上启动 Symantec Data Loss Prevention 服务

- 1 在托管 Symantec Data Loss Prevention 服务器应用程序的计算机上，导航至“开始” > “所有程序” > “管理工具” > “服务”，打开 Windows 的“服务”菜单。
- 2 启动其他 Symantec Data Loss Prevention 服务之前，请先启动 Vontu Notifier 服务。
- 3 启动其余的 Symantec Data Loss Prevention 服务，其中可能包括：
 - Vontu Manager
 - Vontu Monitor
 - Vontu Incident Persister
 - Vontu Update
 - Vontu Monitor Controller

请参见第 72 页的“[在单层 Windows 安装上停止服务](#)”。

在单层 Windows 安装上停止服务

使用以下过程，对 Windows 上的单层安装停止 Symantec Data Loss Prevention 服务。

在单层 Windows 安装上停止 Symantec Data Loss Prevention 服务

- 1 在托管 Symantec Data Loss Prevention 服务器应用程序的计算机上，导航至“开始” > “所有程序” > “管理工具” > “服务”，打开 Windows 的“服务”菜单。
- 2 从“服务”菜单中，停止所有运行中的 Symantec Data Loss Prevention 服务，其中可能包括：
 - Vontu Update
 - Vontu Incident Persister
 - Vontu Manager
 - Vontu Monitor Controller
 - Vontu Notifier

■ Vontu Monitor

请参见第 72 页的“[在单层 Windows 安装上启动服务](#)”。

在 Linux 上启动和停止服务

启动和停止服务的过程会视安装配置以及是 Enforce Server 还是检测服务器而有所不同。

- 请参见第 73 页的“[在 Linux 上启动 Enforce Server](#)”。
- 请参见第 74 页的“[在 Linux 上停止 Enforce Server](#)”。
- 请参见第 74 页的“[在 Linux 上启动检测服务器](#)”。
- 请参见第 74 页的“[在 Linux 上停止检测服务器](#)”。
- 请参见第 75 页的“[在单层 Linux 安装上启动服务](#)”。
- 请参见第 75 页的“[在 Linux 单层安装上停止服务](#)”。

在 Linux 上启动 Enforce Server

使用以下过程，在 Linux Enforce Server 上启动 Symantec Data Loss Prevention 服务。

在 Linux Enforce Server 上启动 Symantec Data Loss Prevention 服务

- 1 在托管 Enforce Server 的计算机上，以根用户身份登录。
- 2 将目录更改为 /opt/SymantecDLP/Protect/bin。
- 3 在启动其他 Symantec Data Loss Prevention 服务之前，如果要启动 Vontu Notifier 服务，请输入：

```
./VontuNotifier.sh start
```

- 4 要启动其余的 Symantec Data Loss Prevention 服务，请输入：

```
./VontuManager.sh start
./VontuIncidentPersister.sh start
./VontuUpdate.sh start
./VontuMonitorController.sh start
```

请参见第 74 页的“[在 Linux 上停止 Enforce Server](#)”。

在 Linux 上停止 Enforce Server

使用以下过程，在 Linux Enforce Server 上停止 Symantec Data Loss Prevention 服务。

在 Linux Enforce Server 上停止 Symantec Data Loss Prevention 服务

- 1 在托管数据库的计算机上，以根用户身份登录。
- 2 将目录更改为 /opt/SymantecDLP/Protect/bin。
- 3 要停止所有运行中的 Symantec Data Loss Prevention 服务，请输入：

```
./VontuUpdate.sh stop  
./VontuIncidentPersister.sh stop  
./VontuManager.sh stop  
./VontuMonitorController.sh stop  
./VontuNotifier.sh stop
```

请参见第 73 页的“[在 Linux 上启动 Enforce Server](#)”。

在 Linux 上启动检测服务器

使用以下过程，在 Linux 检测服务器上启动 Symantec Data Loss Prevention 服务。

在 Linux 检测服务器上启动 Symantec Data Loss Prevention 服务

- 1 在托管 Enforce Server 的计算机上，以根用户身份登录。
- 2 将目录更改为 /opt/SymantecDLP/Protect/bin。
- 3 要启动 Symantec Data Loss Prevention 服务，请输入：

```
./VontuMonitor.sh start  
./VontuUpdate.sh start
```

请参见第 74 页的“[在 Linux 上停止检测服务器](#)”。

在 Linux 上停止检测服务器

使用以下过程，在 Linux 检测服务器上停止 Symantec Data Loss Prevention 服务。

在 Linux 检测服务器上停止 Symantec Data Loss Prevention 服务

- 1 在托管数据库的计算机上，以根用户身份登录。
- 2 将目录更改为 /opt/SymantecDLP/Protect/bin。
- 3 要停止所有运行中的 Symantec Data Loss Prevention 服务，请输入：

```
./VontuUpdate.sh stop  
./VontuMonitor.sh stop
```

请参见第 74 页的“[在 Linux 上启动检测服务器](#)”。

在单层 Linux 安装上启动服务

使用以下过程，在 Linux 中的单层安装上启动 Symantec Data Loss Prevention 服务。

在 Linux 中的单层安装上启动 Symantec Data Loss Prevention 服务

- 1 在托管 Symantec Data Loss Prevention 服务器应用程序的计算机上，以根用户身份登录。
- 2 将目录更改为 /opt/SymantecDLP/Protect/bin。
- 3 在启动其他 Symantec Data Loss Prevention 服务之前，如果要启动 Vontu Notifier 服务，请输入：

```
./VontuNotifier.sh start
```

- 4 要启动其余的 Symantec Data Loss Prevention 服务，请输入：

```
./VontuManager.sh start  
./VontuMonitor.sh start  
./VontuIncidentPersister.sh start  
./VontuUpdate.sh start  
./VontuMonitorController.sh start
```

请参见第 75 页的“[在 Linux 单层安装上停止服务](#)”。

在 Linux 单层安装上停止服务

使用以下过程，对 Linux 上的单层安装停止 Symantec Data Loss Prevention 服务。

在 Linux 的单层安装上停止 Symantec Data Loss Prevention 服务

- 1 在托管 Symantec Data Loss Prevention 服务器的计算机上，以根用户身份登录。
- 2 将目录更改为 /opt/SymantecDLP/Protect/bin。
- 3 要停止所有运行中的 Symantec Data Loss Prevention 服务，请输入：

```
./VontuUpdate.sh stop
./VontuIncidentPersister.sh stop
./VontuManager.sh stop
./VontuMonitor.sh stop
./VontuMonitorController.sh stop
./VontuNotifier.sh stop
```

请参见第 75 页的“[在单层 Linux 安装上启动服务](#)”。

管理角色和用户

本章节包括下列主题：

- 关于基于角色的访问控制
- 关于对用户进行身份验证
- 关于配置角色和用户
- 关于建议的组织角色
- 解决方案软件包包括的角色
- 配置角色
- 配置用户帐户
- 配置密码强制实施设置
- 重置管理员密码
- 管理和添加角色
- 管理和添加用户
- 集成 Active Directory 以进行用户身份验证
- 关于配置证书身份验证

关于基于角色的访问控制

Symantec Data Loss Prevention 提供基于角色的访问控制，以管理用户访问产品特性和功能的方式。例如，角色可能允许用户查看报告，但是却禁止用户创建策略或删除事件。或者，角色可能允许用户创建策略响应规则，但不能创建检测规则。

角色确定用户在 Enforce Server 管理控制台中可看到的内容和执行的操作。例如，“报告”角色是包括在大多数 Symantec Data Loss Prevention 解决方案软件包中

的特定角色。在“报告”角色中的用户可以查看事件、创建策略，还可以配置发现目标（如果运行的是发现服务器）。但是，“报告”角色中的用户不能创建确切数据或文档配置文件。此外，“报告”角色中的用户不能执行系统管理任务。若用户以“报告”角色登录到系统，Enforce Server 管理控制台中的“管理”>“数据配置文件”和“系统”>“用户管理”模块对此用户不可见。

您可以将多个角色分配给一个用户。具有多个角色的成员允许用户在系统中执行不同种类的工作。例如，您授予信息安全管理員用户（信息安全管理員）成员两个角色：ISR（信息安全第一层响应人员）和ISM（信息安全管理員）。信息安全管理員可以第一层响应人员（ISR）或管理员（ISM）的身份（根据要执行的任务）进行登录。“信息安全管理員”只会看到适合运行这些任务的Enforce Server 组件。

您还可以将角色和策略组结合起来，以限制用户可以配置的策略和检测服务器。例如，您可以使角色与“欧洲办公室”策略组生成关联。则此角色被授予访问那些专为“欧洲办公室”设计的策略的权限。

请参见第 310 页的“[关于策略部署](#)”。

被分配给多个角色的用户在登录时必须指定所需的角色。例如，您分配给名为User01 的用户两个角色：“报告”和“系统管理”。如果 User01 登录系统以进行管理，则该用户应使用以下语法登录：**Login:System Admin\User01**

请参见第 51 页的“[登录和注销 Enforce Server 管理控制台](#)”。

在安装时创建的用户 Administrator 可以访问系统的每个部分，因此他不是任何访问控制角色的成员。

请参见第 51 页的“[关于 Administrator 帐户](#)”。

关于对用户进行身份验证

Symantec Data Loss Prevention 提供以下选项，用于让用户向 Enforce Server 管理控制台进行身份验证：

表 5-1 Enforce Server 身份验证机制

身份验证机制	登录机制	说明
密码身份验证	基于表单的登录	<p>使用密码身份验证时，Enforce Server 管理控制台通过确定提供的用户名和密码组合是否匹配 Enforce Server 配置中的活动用户帐户来对每个用户进行身份验证。如果已为活动用户帐户分配有效的角色，则其会通过身份验证。</p> <p>在使用此身份验证机制时，用户将其凭据输入至 Enforce Server 管理控制台的登录页面并通过 HTTPS 连接将其提交到托管该管理控制台的 Tomcat 容器。</p> <p>使用密码身份验证时，必须在 Enforce Server 管理控制台中为每个用户帐户直接配置用户名和密码。还必须确保每个用户帐户至少已分配一个角色。</p> <p>请参见第 97 页的“管理和添加用户”。</p>
Active Directory 身份验证	基于表单的登录	<p>使用 Microsoft Active Directory 身份验证时，Enforce Server 管理控制台首先通过评估提供的用户名来确定该名称是否存在于已配置的 Active Directory 服务器中。如果该用户名存在于 Active Directory 中，则会针对 Active Directory 密码来评估提供的用户密码。将忽略 Enforce Server 配置中配置的任何密码。</p> <p>使用 Active Directory 身份验证时，必须在 Enforce Server 管理控制台中为每个 Active Directory 用户配置用户帐户。不必输入 Active Directory 用户帐户的密码。在系统中创建了用户帐户后，可以切换至 Active Directory 身份验证。但是，在切换后，只有与 Active Directory 用户名匹配的现有用户名仍然有效。</p> <p>注意：管理员用户可以使用安装期间创建的 Enforce Server 系统帐户密码登录到 Enforce Server 管理控制台。</p> <p>请参见第 100 页的“验证 Active Directory 连接”。</p>

身份验证机制	登录机制	说明
SPC 身份验证	SPC 控制台的单一登录	<p>可以选择将 Enforce Server 与单个 Symantec Protection Center (SPC) 实例集成。使用 SPC 集成，用户首先登录到 SPC 控制台，然后可以从 SPC 界面内访问 Enforce Server 管理控制台。当用户请求管理控制台选项时，SPC 控制台通过信任连接传递 Enforce Server 管理控制台用户的用户名或用户名和角色。SPC 管理员可以将所有 SPC 用户映射到单个 Enforce Server 用户帐户，也可以将不同的 SPC 用户映射到不同的 Enforce Server 用户帐户。</p> <p>管理控制台会对源自已注册 SPC 实例的请求进行身份验证。它还会验证请求的 Enforce Server 用户帐户是否处于活动状态以及在 Enforce Server 配置中是否具有有效的角色。如果将 SPC 配置为使用特定用户名和角色组合登录，Enforce Server 将会验证请求的角色是否已分配给活动用户帐户。</p> <p>要使用集成了 SPC 的单一登录，必须首先在 Enforce Server 上启用 SPC 身份验证并将 SPC 实例注册到 Enforce Server 管理控制台。然后将每个 SPC 用户映射到 Enforce Server 配置中的一个用户帐户。也可以将多个 SPC 用户映射到单个 Enforce Server 用户帐户。还可以指定 Enforce Server 用户帐户和角色组合，或接受分配给 Enforce Server 配置中的帐户的默认角色。</p> <p>请参见第 154 页的“关于 Enforce Server 与 SPC 集成”。</p> <p>请参见第 97 页的“管理和添加用户”。</p>

身份验证机制	登录机制	说明
证书身份验证	公钥基础架构(PKI)的单一登录	<p>通过证书身份验证，用户可以使用公钥基础架构 (PKI) 所生成的 X.509 客户端证书自动登录到 Enforce Server 管理控制台。要使用基于证书的单一登录，必须首先在 Enforce Server 中启用证书身份验证。</p> <p>请参见第 104 页的“为 Enforce Server 管理控制台配置证书身份验证”。</p> <p>在客户端的浏览器与 Enforce Server 管理控制台执行 SSL 握手时，必须将客户端证书传递给 Enforce Server。例如，您可能将智能卡读卡器和中间件与浏览器结合使用来自动向 Enforce Server 提供证书。或者，从证书颁发机构获取 X.509 证书并将其上传到已配置为将证书发送到 Enforce Server 的浏览器。</p> <p>当用户访问 Enforce Server 管理控制台时，PKI 自动将用户的证书传递到托管该管理控制台的 Tomcat 容器。Tomcat 容器使用您在 Tomcat 信任存储区中配置的证书颁发机构验证客户端证书。</p> <p>请参见第 105 页的“将证书颁发机构 (CA) 证书添加到 Tomcat 信任存储区”。</p> <p>Enforce Server 管理控制台使用经过验证的证书确定该证书是否已被取消。</p> <p>请参见第 108 页的“关于证书吊销检查”。</p> <p>如果证书有效且未被取消，则 Enforce Server 会使用该证书中的常见名称 (CN) 确定是否将该 CN 映射到具有 Enforce Server 配置中的角色的活动用户帐户。对于要使用基于证书的单一登录访问 Enforce Server 管理控制台的每个用户，必须在 Enforce Server 中创建用于定义相应用户的 CN 值的用户帐户。还必须将一个或多个有效角色分配给该用户帐户。</p> <p>请参见第 97 页的“管理和添加用户”。</p>

当您安装 Enforce Server 时，安装程序会提示您选择要使用的身份验证机制。密码身份验证是与 Symantec Data Loss Prevention 结合使用的默认机制，即使您使用 SPC 身份验证或证书身份验证，也可以使用密码身份验证。如果您使用证书身份验证，可以选择禁用密码身份验证，以依赖您的 PKI 对 Enforce Server 管理控制台进行所有访问。

如果从较早版本的 Symantec Data Loss Prevention 升级，则可以手工启用 SPC 身份验证或证书身份验证。

关于配置角色和用户

安装 Enforce Server 时，需要创建一个对所有角色都具有访问权限的默认管理员用户。如果已将解决方案软件包导入到 Enforce Server，则此解决方案软件包包括了现成可用的多个角色和用户。

请参见第 51 页的“[关于 Administrator 帐户](#)”。

可能需要将角色和用户添加到 Enforce Server。添加角色和用户时，请注意以下规范：

- 了解商务用户与组织的信息安全要求和流程所需的角色。
请参见第 82 页的“[关于建议的组织角色](#)”。
- 查看安装解决方案软件包时所创建的角色。您或许可以将部分角色（或修改后的版本）用于组织中的用户。
请参见第 83 页的“[解决方案软件包包括的角色](#)”。
- 如有必要，请修改解决方案软件包角色，也可以创建任何所需的新角色。
请参见第 85 页的“[配置角色](#)”。
- 创建用户并将每个用户分配给一个或多个角色。
请参见第 91 页的“[配置用户帐户](#)”。
- 管理角色和用户，并删除那些不使用的角色和用户。
请参见第 96 页的“[管理和添加角色](#)”。
请参见第 97 页的“[管理和添加用户](#)”。

关于建议的组织角色

要确定对组织最有用的角色，请查看业务流程和安全要求。

大部分企业和组织在实施 Symantec Data Loss Prevention 系统时发现以下角色很重要：

■ 系统管理员

此角色提供对 Enforce Server 管理控制台中的“系统”模块及相关菜单选项的访问权限。此角色中的用户可以监控和管理 Enforce Server 和检测服务器。此角色中的用户还可以部署检测服务器和运行 Network Discover 扫描。但是，此角色中的用户无法查看详细的事件信息或创建策略。所有解决方案软件包都会创建具有系统管理员权限的“系统管理”角色。

■ 用户管理员

此角色授予用户管理用户和角色的权限。通常该角色不授予任何其他访问权限。由于可能存在滥用权限的现象，因此，我们建议将此角色最多分配给组织中的两个人（主要和候选）。

■ 策略管理员

此角色授予用户管理策略和响应规则的权限。通常该角色不授予任何其他访问权限。由于可能存在滥用权限的现象，因此，我们建议将此角色最多分配给组织中的两个人（主要和候选）。

■ 策略作者

此角色提供对 Enforce Server 管理控制台中的“策略”模块及相关菜单选项的访问权限。该角色适合信息安全管理員跟踪事件并对风险趋势做出响应。信息安全管理員可以创建新策略或修改现有策略，以防止数据丢失。所有解决方案软件包都会创建具有策略创建权限的“信息安全管理員”(ISM) 角色。

■ 事件响应人员

此角色提供对 Enforce Server 管理控制台中的“事件”模块及相关菜单选项的访问权限。此角色中的用户可以跟踪和补救事件。企业通常至少具有两个事件响应人员角色，提供两层权限，分别是查看和响应事件。

第一层响应人员可以查看常规事件信息，但是无法访问事件详细信息（如发送者和接受者身份）。另外，第一层响应人员还可以执行一些事件补救工作，例如上报事件或通知特定公司策略的违规者。第二层响应人员可能是可查看事件详细信息和编辑自定义属性的上报响应人员。第三层响应人员可能是可创建响应规则、策略和策略组的调查响应人员。

所有解决方案软件包都会创建“信息安全响应人员”(ISR) 角色。此角色充当第一层响应人员。可以使用 ISM（信息安全管理員）角色提供第二层响应人员的访问权限。

贵企业可能需要这些角色的变体，以及其他一些角色。有关这些角色及其他可能的角色的更多信息，请参见随解决方案软件包导入的角色的说明。

请参见第 83 页的[“解决方案软件包包括的角色”](#)。

解决方案软件包包括的角色

由 Symantec Data Loss Prevention 提供的多种解决方案软件包在安装时都会创建角色和用户。对于所有解决方案软件包，有一组标准的角色和用户。你会发现这些角色和用户有一些差异，具体取决于所导入的解决方案软件包。

下表概述了“金融服务解决方案软件包”角色。这些角色与其他 Symantec Data Loss Prevention 解决方案中的角色基本相同。

请参见第 83 页的[表 5-2](#)。

表 5-2 金融服务解决方案软件包角色

角色名称	说明
Compliance	合规主管： <ul style="list-style-type: none">■ 此角色中的用户可以查看、补救和删除事件，查找属性，也可以编辑所有的自定义属性。■ 此综合角色为用户提供用于确保遵守各项法规制度的权限。此角色还允许用户制订业务单元(BU)层级的风险降低策略，并查看事件趋势和风险计分卡。

角色名称	说明
Exec	<p>主管：</p> <ul style="list-style-type: none"> ■ 此角色中的用户可以查看、补救和删除事件，查找属性，也可以查看所有的自定义属性。 ■ 此角色为用户提供用于防止数据大幅丢失风险的访问权限。此角色中的用户还可以查看风险趋势、绩效标准及事件控制板。
HRM	<p>人力资源经理：</p> <ul style="list-style-type: none"> ■ 此角色中的用户可以查看、补救和删除事件，查找属性，也可以编辑所有的自定义属性。 ■ 此角色为用户提供用于响应与员工违规相关的安全事件的访问权限。
Investigator	<p>事件调查员：</p> <ul style="list-style-type: none"> ■ 此角色中的用户可以查看、补救和删除事件，查找属性，也可以编辑所有的自定义属性。 ■ 此角色为用户提供用于调查事件的详细情况的访问权限（包括转发事件进行讨论）。此角色中的用户还可以调查特定员工。
ISM	<p>信息安全管理员：</p> <ul style="list-style-type: none"> ■ 此角色中的用户可以查看、补救和删除事件。他们可以查看属性、编辑所有自定义属性、创建所有策略和策略组，也可以创建响应规则。 ■ 此角色为用户提供第二层事件响应权限。用户可以在信息安全小组内管理提报的事件。
ISR	<p>信息安全响应人员：</p> <ul style="list-style-type: none"> ■ 此角色中的用户可以查看、补救和删除事件，查看属性，还可以查看、编辑某些自定义属性。他们没有发送者或接受者的详细身份信息的访问权限。 ■ 此角色为用户提供第一层事件响应权限。用户可以查看策略事件，查找中断的业务流程以及将扩展补救小组支持登记到补救事件。
Report	<p>报告和策略创建：</p> <ul style="list-style-type: none"> ■ 此角色中的用户可以查看和补救事件，还可以创建所有的策略和策略组。他们不能访问事件详细信息。 ■ 此角色为策略创建和数据丢失风险管理提供一个角色。
Sys Admin	<p>系统管理员：</p> <ul style="list-style-type: none"> ■ 此角色中的用户可以管理系统和系统用户，也可以查看事件。他们不能访问事件详细信息。

配置角色

每个 Symantec Data Loss Prevention 用户分配有一个或多个角色，这些角色定义他们在系统内的权限。用户角色决定系统管理权限、策略创建权限以及事件访问权限等。如果用户是具有多个角色的成员，该用户在登录时必须指定角色，例如，登录名: Sys Admin/sysadmin01。

请参见第 77 页的“[关于基于角色的访问控制](#)”。

请参见第 81 页的“[关于配置角色和用户](#)”。

配置角色

1 导航至“系统”>“用户管理”>“角色”屏幕。

2 单击“添加角色”。

将出现“配置角色”屏幕，其中显示以下选项卡：“常规”、“事件访问”、“策略管理”和“用户”。

3 在“常规”选项卡中：

- 输入角色的唯一“名称”。名称字段区分大小写，且字符数不得超过 30 个。输入的名称应该简短且具有自述性。“说明”字段用于为角色名称加注释以及更详细地解释其用途。角色名称和说明显示在“角色列表”屏幕上。

- 在“用户权限”部分，为角色授予用户权限。

“系统”权限：

用户管理“超级用户”选择“用户管理”选项可使用户在 Enforce Server 中创建其他用户

服务器管理

选择“服务器管理”选项可让用户执行下列功能：

- 配置检测服务器。
- 创建并管理确切数据匹配(EDM)、索引文档匹配(IDM)和向量机学习(VML)的数据配置文件。
- 配置和分配事件属性。
- 配置系统设置。
- 配置响应规则。
- 创建策略组。
- 配置识别协议。
- 查看系统事件和流量报告。

Symantec Protection Center 注册 选择“**Symantec Protection Center 注册**”选项可允许用户将 Symantec Data Loss Prevention 与 Symantec Protection Center (SPC) 集成。

请参见第 153 页的“[关于 Symantec Protection Center \(SPC\)](#)”。

- 在“事件”部分，为此角色的用户授予下列事件权限：这些设置应用于系统中的所有事件报告，包括“执行摘要”、“事件摘要”、“事件列表”以及“事件快照”。

查看 选择“查看”选项可使此角色的用户查看策略违规事件。

可以选择各种“操作”和“显示属性”选项来自定义事件查看访问，如下所示：

- 默认情况下，针对所有类型的事件，“查看”选项均已启用（已选择）：“网络事件”、“发现事件”、“端点事件”、“移动事件”和“分类事件”。
- 要限制仅对某些事件类型的查看访问，请选择（突出显示）要授权此角色查看的事件类型。（按住 Ctrl 键可选择多项。）如果角色不允许用户查看部分事件报告，选项替换为“未经授权”或空白。

注意：如果取消某个角色的事件查看权限，系统会删除该角色所有依赖此取消权限的已保存报告。例如，如果取消（取消选择）查看网络事件的权限，系统会删除保存的与该角色相关的所有网络事件报告。

操作	在下列“操作”中进行选择，以自定义发生事件时用户可以执行的操作：
	■ 补救事件 此权限可让用户更改事件的状态或严重性、设置数据所有者、将注释添加到事件历史记录、设置“不存档”和“允许存档”选项，以及执行响应规则操作。此外，如果您要使用“事件报告”和“更新 API”，选择此权限可补救位置和状态属性。
	■ 要执行的智能响应规则 您可以根据每个角色，指定要执行的智能响应规则。已配置的智能响应规则会列在左侧的“可用”列中。若要按照该角色的用户来公开要执行的智能响应规则，请选择它并单击箭头，将它添加到右侧列中。使用 Ctrl 键可选择多个规则。
	注意： 在 Symantec Data Loss Prevention 11.6 版之前，智能响应规则不需要基于角色的访问控制即可执行。如果升级到 Symantec Data Loss Prevention 11.6 版，则会自动启用现有的智能响应规则以便执行（它们应显示在右侧列中）。新的响应规则必须启用才能执行。
	■ 执行属性查找 让用户从外部源查找事件属性并填入其值以进行事件补救。
	■ 删除事件 允许用户删除事件。
	■ 存档事件 可让用户存档事件。
	■ 还原已存档事件 可让用户还原先前存档的事件。
	■ 导出 Web 存档 允许用户导出系统根据事件的 Web 存档编辑的报告。
	■ XML 导出 允许用户以 XML 格式导出事件报告。
	■ 通过电子邮件以 CSV 附件发送事件报告 允许用户将包含以逗号分隔的事件详细信息列表的报告作为电子邮件附件发送。

事件报告和更新 API 从下列用户权限中选择，以便针对使用事件报告和更新 API 或过时报告 API 的 Web 服务客户端启用访问权：

■ 事件报告

让 Web 服务客户端提取事件详细信息。

■ 事件更新

启用 Web 服务客户端来更新事件详细信息。（不适用于使用弃用报告 API 的客户端）。

有关更多详细信息，请参阅 *Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide*（《Symantec Data Loss Prevention 事件报告和更新 API 开发指南》）。

显示属性

在下列“显示属性”中进行选择，自定义出现在策略违规的“事件数”视图中的属性，相应角色的用户可以查看这些属性。

“共享”属性是所有事件类型的通用属性：

■ 匹配项

违反策略的邮件的突出显示的文本显示在“事件快照”屏幕的“匹配项”选项卡中。

■ 历史记录

事件历史记录。

■ 正文

邮件的正文。

■ 附件

任何附件或文件的名称。

■ 发送者

邮件发送者。

■ 接受者

邮件接受者。

■ 主题

邮件的主题。

■ 原始邮件

控制是否可以查看导致策略违规事件的原始邮件。

注意：要正确查看附件，必须同时选中“附件”和“原始邮件”选项。

“端点”属性是特定于端点事件的属性：

■ 用户名

端点用户的名称。

■ 计算机名称

安装端点代理的计算机的名称。

“发现”属性是特定于发现事件的属性：

■ 文件所有者

被扫描文件的所有者的名称。

■ 位置

被扫描文件的位置。

自定义属性

“自定义属性”列表包括系统管理员配置的所有自定义属性（如果有）。

- 如果希望用户能够查看所有自定义属性值，选择“全部查看”。
- 如果希望用户能够编辑所有自定义属性值，选择“全部编辑”。
- 若要受限用户对某些自定义属性的权限，请清除“全部查看”和“全部编辑”复选框，然后针对您要将其设置为可视或可编辑的每个自定义属性，选择其“查看”和/或“编辑”复选框。

注意：对任何自定义属性选择“编辑”后，会自动选中“查看”复选框（以灰显表示）。如果希望此角色的用户能够查看所有自定义属性值，请选择“全部查看”。

- 在“文件夹/资源报告”部分中，您可以将下列权限授予此角色的用户：

文件夹风险报告

此权限可让用户查看“文件夹风险报告”。请参阅《Symantec Data Loss Prevention Data Insight 操作指南》

注意：该权限仅适用于 Symantec Data Loss Prevention Data Insight 许可证。

- 4 在“事件访问”选项卡中，对此角色的用户可以查看的事件类型配置任何条件（过滤器）。

注意：必须选择“常规”选项卡上的“查看”选项，这样“事件访问”选项卡上的设置才能生效。

添加事件访问条件：

- 单击“添加条件”。
- 就象写句子一样，从左到右选择条件类型及其参数。（请注意，条件中的第一个下拉列表包含系统提供的按字母顺序排列的条件，这些条件与所有自定义属性相关。）
例如，从第一个下拉列表中选择“策略组”，从第二个下拉列表中选择“为任一”，然后从最后一个列表框中选择“默认策略组”。这些设置会限制用户只能查看默认策略组检测到的那些事件。

- 5 在“策略管理”选项卡中，为角色选择下列策略权限之一：

■ 创建策略

此角色权限允许用户在选择的策略组中添加、编辑和删除策略。

它也允许用户修改系统数据标识符和创建自定义数据标识符。

它还允许用户创建和修改用户组。

此权限不允许用户创建和管理数据配置文件。此活动需要 Enforce Server 管理员权限。

■ 发现扫描控制

可让此角色的用户创建发现目标、运行扫描以及查看发现服务器。

■ 凭据管理

允许用户创建和修改系统所需的凭据，以便访问目标系统和执行发现扫描。

■ 策略组

仅当该角色的用户需要访问所有现有策略组以及未来将要创建的任意策略组时，才要选中“**所有策略组**”。

否则，可以选择单个策略组或“**默认策略组**”。

注意：这些选项不会授予创建、修改或删除策略组的权限。只有其角色包括“服务器管理”权限的用户才能使用策略组。

■ 创建响应规则

可让此角色的用户创建、编辑和删除响应规则。

注意：除非选择“**创建响应规则**”选项，否则用户无法编辑或创建策略补救的响应规则。

注意：阻止用户创建响应规则不会阻止其执行响应规则。例如，不具备响应规则创建权限的用户仍可以从事件列表或事件快照中执行智能响应规则。

- 6 在“**用户**”选项卡中，选择要为其分配此角色的任何用户。如果尚未配置任何用户，可以在创建用户之后为其分配角色。
- 7 单击“**保存**”将新创建的角色保存到 Enforce Server 数据库。

配置用户帐户

用户帐户供用户登录系统并执行任务。用户帐户所属的角色限制用户在系统中可以执行的操作。

配置用户帐户：

- 1 在Enforce Server管理控制台中，选择“系统”>“用户管理”>“用户”创建新的用户帐户或重新配置现有的用户帐户。或者，单击“配置文件”重新配置当前登录的用户帐户。
- 2 单击“添加用户”添加新用户，或单击现有用户的名称修改该用户的配置。
- 3 在“名称”字段中输入新用户帐户的名称。
 - 用户帐户名称的长度必须在8至30个字符之间，区分大小写，不能包含反斜杠(\)。
 - 如果使用证书身份验证，“名称”字段值不必与用户的常见名称(CN)匹配。但是，可以选择对“名称”和“常见名称(CN)”使用同一值，这样便能够轻松地找到特定CN的配置。Enforce Server管理控制台仅在已配置用户列表中显示“名称”字段值。
 - 如果使用Active Directory身份验证，用户帐户名称必须与Active Directory用户帐户名称匹配。请注意，尽管Active Directory用户名不区分大小写，但所有的Symantec Data Loss Prevention用户名是区分大小写的。Active Directory用户登录到Enforce Server管理控制台时，需要输入区分大小写的帐户名称。
请参见第97页的[“集成Active Directory以进行用户身份验证”](#)。

4 配置“配置用户”页的“身份验证”部分，如下所示：

选项	说明
使用密码身份验证	<p>选择此选项可使用密码身份验证并允许用户使用 Enforce Server 管理控制台登录页面登录。如果用户帐户将用于报告 API Web 服务客户端，则此选项是必需的。</p> <p>如果选择此选项，还需要在“密码”字段和“重新输入密码”字段中输入用户密码。密码长度必须至少为八个字符，且区分大小写。出于安全考虑，会对密码进行模糊处理，每个字符都显示为星号。</p> <p>如果您配置高级密码设置，用户必须指定强密码。此外，密码可能会在特定日期过期，用户必须定期定义新密码。</p> <p>请参见第 95 页的“配置密码强制实施设置”。</p> <p>即使同时还使用 SPC 身份验证或证书身份验证，您也可以选择密码身份验证。如果使用证书身份验证，您可以选择禁止从 Enforce Server 管理控制台登录页面登录。</p> <p>请参见第 114 页的“禁用密码身份验证和基于表单的登录”。</p> <p>Symantec Data Loss Prevention 使用密码身份验证来对所有报告 API 客户端进行身份验证。如果将 Symantec Data Loss Prevention 配置为使用证书身份验证，则用于访问报告 API Web 服务的任何用户帐户都必须具有有效密码。请参见《Symantec Data Loss Prevention 报告 API 开发人员指南》。</p> <p>注意：如果您配置 Active Directory 与 Enforce Server 集成，则用户可以使用其 Active Directory 密码进行身份验证。在这种情况下，“密码”字段不出现在“用户”屏幕中。</p> <p>请参见第 97 页的“集成 Active Directory 以进行用户身份验证”。</p>
使用证书身份验证	<p>选择此选项可使用证书身份验证，允许用户使用单独私钥基础架构 (PKI) 生成的证书自动执行单一登录。仅当在 Symantec Data Loss Prevention 安装期间配置了证书身份验证，或手动配置了对证书身份验证的支持时，此选项才可用。</p> <p>请参见第 78 页的“关于对用户进行身份验证”。</p> <p>请参见第 102 页的“关于配置证书身份验证”。</p> <p>如果选择此选项，必须在“常见名称(CN)”字段中为用户指定常见名称(CN)值。此 CN 值会出现在用户证书（由 PKI 生成）的“主题”字段。常见名称通常使用 <i>first_name last_name identification_number</i> 格式。</p> <p>Enforce Server 使用 CN 值将证书映射到该用户帐户。如果已经过身份验证的证书包含指定的 CN 值，则在用户登录时会应用该用户帐户的所有其他属性（如默认角色和报告首选项）。</p> <p>注意：您不能在多个 Enforce Server 用户帐户中指定同一“常见名称(CN)”值。</p>

选项	说明
帐户被禁用	<p>选择此选项可锁定用户，使其不能登录 Enforce Server 管理控制台。无论使用哪种身份验证机制，该选项都会禁止用户帐户进行访问。</p> <p>出于安全原因，登录尝试连续失败一定次数后，系统会自动禁用该帐户并锁定该用户。在这种情况下，“帐户被禁用”选项处于选中状态。要重新启用该用户帐户并允许该用户登录系统，请通过取消选中此选项清除它。</p>
5	(可选) 在页面的“常规”部分输入用户的“电子邮件地址”并为其选择一种“语言”。“语言”的选择取决于您已安装的语言包。
6	在“用户”屏幕的“报告首选项”部分中，您可以指定此用户接收事件报告的方式的首选项，包括“文本文件编码”和“CSV 分隔符”。
	如果角色授予您“ XML 导出 ”的权限，您可以选择在 XML 导出中包含事件违规和事件历史记录。
7	在“角色”部分中，选择用于为此用户分配数据和事件访问权限的角色。 必须为用户至少分配一个角色，才能访问 Enforce Server 管理控制台。 请参见第 85 页的“ 配置角色 ”。
8	选择要在登录时分配给此用户的“默认角色”。 如果用户登录时未要求使用任何特定角色，将应用此默认角色。 例如，如果用户通过证书身份验证使用单一登录或使用登录页面，Enforce Server 管理控制台将使用默认角色。使用 SPC 身份验证，可以在登录时指定要请求的确切角色，此情况下会忽略默认角色。
<hr/> <p>注意：通过单击“配置文件”并从“默认角色”菜单中选择不同的选项，各用户均可以更改其默认角色。下次登录时，将应用新的默认角色。</p> <hr/>	
	请参见第 78 页的“ 关于对用户进行身份验证 ”。
9	单击“保存”保存用户配置。
<hr/> <p>注意：保存新用户后，不能再对用户名进行编辑。</p> <hr/>	
10	根据需要管理用户和角色。 请参见第 96 页的“ 管理和添加角色 ”。 请参见第 97 页的“ 管理和添加用户 ”。

配置密码强制实施设置

在“系统”>“设置”>“常规”屏幕上，可要求用户使用强密码。强密码必须至少包含八个字符、一个数字和一个大写字母。强密码不能在一行中有两个以上重复的字符。如果启用强密码，则会对整个系统生效。没有强密码的现有用户必须在下次登录时更新其配置文件。

还可以要求用户定期更改密码。在指定间隔到期的情况下，系统会强制用户使用新密码。

如果使用 Active Directory 身份验证，则这些密码设置只适用于管理员密码。所有其他用户帐户密码都从 Active Directory 获得。

请参见第 97 页的“[集成 Active Directory 以进行用户身份验证](#)”。

配置高级身份验证设置

- 1 转至“系统”>“设置”>“常规”，然后单击“配置”。
- 2 如果要求强密码，请转至“密码强制实施”部分，并选择“要求强密码”。
- 3 要设置密码的有效期，请在“密码轮转周期”字段键入一个数字（代表天数）。要让密码永远有效，则键入 0（零的字符）。

重置管理员密码

Symantec Data Loss Prevention 提供了 AdminPasswordReset 实用程序来重置管理员密码。如果密码丢失，将无法恢复，但是可以使用该实用程序分配一个新的密码。如果禁用了证书身份验证机制但尚未定义管理员帐户的密码，也可以使用此实用程序。

要使用 AdminPasswordReset 实用程序，您必须指定 Enforce Server 数据库的密码。请使用以下过程重置密码。

重置基于表单的登录的管理员密码

- 1 使用在 Symantec Data Loss Prevention 安装过程中创建的帐户登录到 Enforce Server 计算机。

注意: 如果使用其他帐户（例如，根或管理员帐户）登录，请确保在后面的步骤中不会更改对任何 Symantec Data Loss Prevention 配置文件的权限或所有权。

- 2 将目录更改为 /opt/Vontu/Protect/bin (Linux) 或 c:\Vontu\Protect\bin (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。
- 3 使用以下语法执行 AdminPasswordReset 实用程序：

```
AdminPasswordReset -dbpass oracle_password -newpass new_administrator_password
```

将 *oracle_password* 替换为 Enforce Server 数据库的密码，将 *new_administrator_password* 替换为您想要设置的密码。

管理和添加角色

“系统” > “用户管理” > “角色” 屏幕会按字母顺序显示为您的组织定义的角色列表。

此屏幕上列出的角色显示以下信息：

- **名称** - 角色的名称
- **说明** - 角色的简要说明

假定您具有适当的权限，则可以按照以下方法查看、添加、修改或删除角色：

- 添加新角色或修改现有角色。
单击“添加角色”开始向系统添加新角色。
单击某行中的任意位置或“铅笔”图标（最右端）可修改该角色
请参见第 85 页的“[配置角色](#)”。
- 单击红色 X 图标（最右端）可删除角色，系统会显示一个对话框提示确认删除操作。

在编辑或删除角色之前，请注意以下准则：

- 如果您更改角色的权限，当前以该角色登录系统的用户不受影响。例如，如果您删除某个角色的编辑权限，当前登录的用户仍保留编辑该会话自定义属性的权限。然而，当用户下次登录时，对该角色所做的更改将会生效，这些用户将不能再编辑自定义属性。

- 如果您取消某个角色的事件查看权限，Enforce Server会自动删除所有依赖于该取消权限的已保存报告。例如，如果取消查看网络事件的权限，系统会删除与该新设定限制的角色相关的所有已保存网络事件报告。
- 在能够删除角色之前，您必须确保没有任何用户与该角色关联。
- 删除某个角色时，也会删除该角色的用户保存的所有共享的已保存报告。

请参见第 97 页的“[管理和添加用户](#)”。

管理和添加用户

“系统” > “用户管理” > “用户” 屏幕列出了系统中所有活动的用户帐户。

对于列出的每个用户帐户，会列出以下信息：

- **用户名** - 用户登录到 Enforce Server 时需要输入的名称
- **电子邮件** - 用户的电子邮件地址
- **访问** - 用户作为其中一成员的角色

如果您具有相应权限，则可以按照以下方法添加、编辑或删除用户帐户：

- 添加新的用户帐户，或修改现有的用户帐户。
单击“添加”开始向系统添加新用户。
单击某行的任意位置或单击“铅笔”图标（最右端）来查看和编辑用户帐户。
请参见第 91 页的“[配置用户帐户](#)”。
- 单击“红色X”图标（最右端）删除用户帐户，系统会显示一个对话框提示确认删除操作。

注意：安装时会创建管理员帐户，并且无法将其从系统中删除。

注意：删除某个用户帐户时，也会删除与该用户关联的所有私人保存的报告。

请参见第 96 页的“[管理和添加角色](#)”。

集成 Active Directory 以进行用户身份验证

可以配置 Enforce Server 以使用 Microsoft Active Directory 进行用户身份验证。

在切换至 Active Directory 身份验证后，仍需在 Enforce Server 管理控制台中定义用户。如果在管理控制台中输入的用户名与 Active Directory 用户匹配，系统会将任何新的用户帐户与 Active Directory 密码关联。在系统中创建了用户帐户后，可

以切换至 Active Directory 身份验证。在切换后，只有与 Active Directory 用户名匹配的现有用户名仍然有效。

用户登录时，必须使用自己的 Active Directory 密码。请注意，所有的 Symantec Data Loss Prevention 用户名仍要区分大小写，尽管 Active Directory 用户名不区分大小写。在 Symantec Data Loss Prevention 创建了用户名之后，可以切换至 Active Directory 身份验证。不过，用户在登录时，仍必须使用区分大小写的 Symantec Data Loss Prevention 用户名。

使用 Active Directory 身份验证

- 1 确认 Enforce Server 主机和 Active Directory 服务器的时间同步。

注意：确保 Active Directory 主机的时钟与 Enforce Server 主机的时钟同步在五分钟内。

- 2 (仅限 Linux) 请确保在 Enforce Server 主机上安装了以下 Red Hat RPM:

- krb5-workstation
- krb5-libs
- pam_krb5

- 3 创建 krb5.ini (对于 Linux，创建 krb5.conf) 配置文件，提供关于 Active Directory 域结构和 Active Directory 服务器地址的 Enforce Server 信息。

请参见第 98 页的“[创建 Active Directory 集成的配置文件](#)”。

- 4 确认 Enforce Server 可以与 Active Directory 服务器通信。

请参见第 100 页的“[验证 Active Directory 连接](#)”。

- 5 配置 Symantec Data Loss Prevention 以使用 Active Directory 身份验证。

请参见第 101 页的“[为 Active Directory 身份验证配置 Enforce Server](#)”。

创建 Active Directory 集成的配置文件

必须创建 krb5.ini (或者在 Linux 环境中为 krb5.conf) 配置文件，为 Symantec Data Loss Prevention 提供有关 Active Directory 域结构和服务器位置的信息。如果有多个 Active Directory 域，则此步骤是必需的。但是，即使 Active Directory 结构只包含一个域，仍建议创建该文件。kinit 实用程序使用该文件来确认 Symantec Data Loss Prevention 是否能够与 Active Directory 服务器进行通信。

注意：如果在 Linux 上运行 Symantec Data Loss Prevention，请使用 kinit 实用程序验证 Active Directory 连接。必须将 krb5.ini 文件重命名为 krb5.conf。在 Linux 上，kinit 实用程序要求将此文件命名为 krb5.conf。Symantec Data Loss Prevention 假设您使用 kinit 验证 Active Directory 连接，指导您将文件重命名为 krb5.conf。

Symantec Data Loss Prevention 提供了样例 krb5.ini 文件，您可以进行修改以便在自己的系统上使用。该样例文件存储在 *DLP_home\Protect\config*（例如，在 Windows 上为 \Vontu\Protect\config，在 Linux 上为 /opt/Vontu/Protect/config）中。如果在 Linux 运行 Symantec Data Loss Prevention，Symantec 建议将文件重命名为 krb5.conf。该样例文件分为两个部分，如下所示：

```
[libdefaults]
    default_realm = TEST.LAB
[realms]
    ENG.COMPANY.COM = {
        kdc = engAD.eng.company.com
    }
    MARK.COMPANY.COM = {
        kdc = markAD.eng.company.com
    }
    QA.COMPANY.COM = {
        kdc = qaAD.eng.company.com
    }
```

[libdefaults] 部分标识默认域。（请注意，Kerberos 区域与 Active Directory 域相对应。）[realms] 部分为每个域定义一个 Active Directory 服务器。在上例中，ENG.COMPANY.COM 的 Active Directory 服务器是 engAD.eng.company.com。

创建 krb5.ini 或 krb5.conf 文件

- 1 转至 *DLP_home\Protect\config*，并找到样例 krb5.ini 文件。例如，找到 \Vontu\Protect\config（Windows 上）或 /opt/Vontu/Protect/config（Linux 上）中的文件。
- 2 将样例 krb5.ini 文件复制到 c:\windows directory（Windows 上）或 /etc directory（Linux 上）。如果在 Linux 上运行 Symantec Data Loss Prevention，则计划使用 kinit 命令行工具验证 Active Directory 连接。将文件重命名为 krb5.conf。

请参见第 100 页的“[验证 Active Directory 连接](#)”。

- 3 使用文本编辑器打开 krb5.ini 或 krb5.conf 文件。

- 4 用默认域的完全限定域名替换样例 default_realm 值。（ default_realm 的值必须全部是大写字母。）例如，修改该值使其如下所示：

```
default_realm = MYDOMAIN.LAB
```

- 5 用实际域的域名替换其他样例域名。（域名必须全部是大写字母。）例如，用 ADOMAIN.COMPANY.COM 替换 ENG.COMPANY.COM。
- 6 用 Active Directory 服务器的主机名或 IP 地址替换样例 kdc 值。（请务必遵循指定格式，其中左括弧后面紧跟换行符。）例如，用 ADserver.eng.company.com 替换 engAD.eng.company.com，等等。
- 7 从配置文件中删除所有不使用的 kdc 条目。例如，如果除默认域外只有两个域，则请删除不使用的 kdc 条目。
- 8 保存文件。

验证 Active Directory 连接

kinit 是一个命令行工具，可以用来确认 Active Directory 服务器是否响应了请求。也可用于验证 Enforce Server 是否具有对 Active Directory 服务器的访问权限。对于 Microsoft Windows 安装，该实用程序由 Symantec Data Loss Prevention 安装程序安装在 *DLP_home\jre\bin* 目录中。对于 Linux 安装，该实用程序是 Red Hat Enterprise Linux 发行版的组成部分，并位于以下位置： /usr/kerberos/bin/kinit。您也可以下载 Java SE 6，并在 \java_home\jdk1.6.0\bin 中找到 kinit 工具。

如果在 Linux 上运行 Enforce Server，请使用 kinit 实用程序，从 Enforce Server 测试访问 Active Directory 服务器。将 krb5.ini 文件重命名为 krb5.conf。在 Linux 上，kinit 实用程序要求将此文件命名为 krb5.conf。

请参见第 101 页的“[为 Active Directory 身份验证配置 Enforce Server](#)”。

测试与 Active Directory 服务器的连接

- 1 在 Enforce Server 主机上，转至命令行并导航至 kinit 所在的目录。
- 2 请使用已知用户名和密码作为参数，输入 kinit 命令。（请注意，在命令行中键入密码时，会明文显示密码。）例如，输入以下命令：

```
kinit kchatterjee mypwd10#
```

第一次连接 Active Directory 时，您可能会收到错误，指出在预期位置找不到 krb5.ini 或 krb5.conf 文件。在 Windows 上，会出现类似以下的错误：

```
krb_error 0 Could not load configuration file c:\winnt\krb5.ini  
(The system cannot find the file specified) No error.
```

在这种情况下，请将 krb5.ini 或 krb5.conf 文件复制到预期的位置，然后重新运行上述 kinit 命令。

- 3 根据 Active Directory 服务器响应命令的方式，采取以下操作之一：
 - 如果 Active Directory 服务器指出其已成功创建 Kerberos 票证，请继续配置 Symantec Data Loss Prevention。
 - 如果收到错误消息，请咨询您的 Active Directory 管理员。

为 Active Directory 身份验证配置 Enforce Server

第一次设置 Active Directory 身份验证，或是想要修改现有 Active Directory 设置时，请执行本部分所述的过程。在启用 Active Directory 身份验证之前，请先确保已完成先决步骤。

请参见第 97 页的“[集成 Active Directory 以进行用户身份验证](#)”。

针对用户 Active Directory 配置 Enforce Server 以进行身份验证：

- 1 确保管理员以外的所有用户都已经注销系统。
- 2 在 Enforce Server 管理控制台中，转至“系统”>“设置”>“常规”，并单击“配置”（左上方）。
- 3 在显示的“编辑常规设置”屏幕上，找到靠近下方的“Active Directory 身份验证”部分，选择（选中）“执行 Active Directory 身份验证”。
然后，系统会显示多个要填写的字段。
- 4 在“默认 Active Directory 域”字段中，输入 Active Directory 系统默认域的名称。此为必填字段。所有的 Windows 域名称都必须使用大写（例如，TEST.LAB）。如果您的设置包括 krb5.ini 或 krb5.conf 文件，则默认 Active Directory 域会与 krb5.ini 或 krb5.conf 文件中的 default_realm 值相同。

- 5 在“默认 Active Directory KDC”字段中，键入 Active Directory 服务器的 IP 地址（或主机名）。KDC（密钥发布中心）是默认运行于端口 88 的 Active Directory 服务。如果 KDC 在其他端口上运行，请按以下格式指定端口：

`ipaddress_or_hostname:port_number`

例如，如果 AD 运行于主机 `Adserver.company.com`，并且 KDC 会在端口 53 上侦听时，请键入 `Adserver.company.com:53`。

- 6 如果您已创建 `krb5.ini` 或 `krb5.conf` 文件，请在“**krb5.ini** 文件路径”字段中输入文件的绝对路径。如果您的环境包括多个域，则需要此文件，即使只有一个域，也建议使用此文件。例如，键入 `C:\winnit\krb5.ini`（Windows 上）或 `/opt/Vontu/Protect/config/krb5.conf`（Linux 上）。

请参见第 98 页的“[创建 Active Directory 集成的配置文件](#)”。

- 7 如果您的环境有多个 Active Directory 域，请在“**Active Directory 域列表**”字段中输入各个域名称，以逗号分隔。系统会在用户登录页面的下拉列表中显示这些域。然后用户可在登录时选择适当的域。不必列出默认域，因为在默认情况下，默认域即会显示在下拉列表中。

- 8 单击“保存”。

- 9 转至操作系统服务工具，然后重新启动 Symantec Data Loss Prevention Manager 服务。

关于配置证书身份验证

通过证书身份验证，用户可以使用公钥基础架构 (PKI) 所生成的客户端证书自动登录到 Enforce Server 管理控制台。当用户访问 Enforce Server 管理控制台时，PKI 自动将用户的证书传递到托管该管理控制台的 Tomcat 容器。Tomcat 容器使用您在 Tomcat 信任存储区中配置的证书颁发机构验证客户端证书。

在客户端浏览器与 Enforce Server 执行 SSL 握手时，客户端证书会传递给 Enforce Server 计算机。例如，某些浏览器可能会配置为与智能卡读卡器配合使用以显示证书。或者，可以选择将 X.509 证书上传到浏览器并将浏览器配置为将证书发送到 Enforce Server。

如果证书有效，Enforce Server 管理控制台还可以确定证书是否已被取消。

请参见第 108 页的“[关于证书吊销检查](#)”。

如果证书有效且未被取消，则 Enforce Server 会使用该证书中的常见名称 (CN) 确定是否将该 CN 映射到具有 Enforce Server 配置中的角色的活动用户帐户。

注意：一些浏览器会缓存用户的客户端证书，并在用户选择注销后自动将用户登录到管理控制台。在这种情况下，用户必须关闭浏览器窗口才能完成注销过程。

下表介绍了在对 Symantec Data Loss Prevention 使用证书身份验证时所必需的步骤。

表 5-3 配置证书身份验证

阶段	操作	说明
阶段 1	在 Enforce Server 计算机上启用证书身份验证。	您可以在安装 Enforce Server 时启用证书身份验证，也可以通过重新配置现有 Enforce Server 来启用身份验证。 请参见第 104 页的“ 为 Enforce Server 管理控制台配置证书身份验证 ”。
阶段 2	添加证书颁发机构 (CA) 证书以建立信任链。	可在安装 Enforce Server 时将 CA 证书添加到 Tomcat 信任存储区。或者，可以使用 Java keytool 实用程序将证书手动添加到现有 Enforce Server。 请参见第 105 页的“ 将证书颁发机构(CA)证书添加到 Tomcat 信任存储区 ”。
阶段 3	(可选。) 更改 Tomcat 信任存储区密码。	Symantec Data Loss Prevention 安装程序将使用默认的 Tomcat 信任存储区密码配置每个新 Enforce Server 安装。 按照这些说明配置安全密码。 请参见第 106 页的“ 更改 Tomcat 信任存储区密码 ”。
阶段 4	将证书常见名称(CN)值映射到 Enforce Server 用户帐户。	请参见第 108 页的“ 将常见名称(CN)值映射到 Symantec Data Loss Prevention 用户帐户 ”。
阶段 5	配置 Enforce Server 以检查证书吊销。	请参见第 108 页的“ 关于证书吊销检查 ”。
阶段 6	验证使用基于证书的单一登录访问 Enforce Server。	请参见第 113 页的“ 排除证书身份验证故障 ”。
阶段 7	(可选。) 禁用基于表单的登录。	如果想要使用基于证书的单一登录来执行对 Enforce Server 的所有访问，请禁用基于表单的登录。 请参见第 114 页的“ 禁用密码身份验证和基于表单的登录 ”。

为 Enforce Server 管理控制台配置证书身份验证

如果在安装 Symantec Data Loss Prevention 时选择了证书身份验证作为单一登录选项，则 Enforce Server 管理控制台已配置为支持证书身份验证。

按照以下过程，在升级的 Symantec Data Loss Prevention 安装上手动启用证书身份验证，或者在 Enforce Server 上禁用或验证证书身份验证。或者，如果要为 Enforce Server 禁用密码身份验证（和基于表单的登录），请按照以下过程进行操作。

为 Enforce Server 管理控制台配置证书身份验证

- 1 使用在 Symantec Data Loss Prevention 安装过程中创建的帐户登录到 Enforce Server 计算机。

注意：如果使用其他帐户（例如，根或管理员帐户）登录，请确保在后面的步骤中不会更改对任何 Symantec Data Loss Prevention 配置文件的权限或所有权。

- 2 将目录更改为 /opt/Vontu/Protect/config (Linux) 或 c:\Vontu\Protect\config (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。
- 3 使用文本编辑器打开 Manager.properties 文件。
- 4 要启用或验证证书身份验证，请在该文件中添加或编辑以下行：

```
com.vontu.manager.certificate_authentication = true
```

要禁用证书身份验证，请将值更改为 false。但是，如果禁用证书身份验证，还应确保启用了密码身份验证，从而确保能够登录到 Enforce Server 管理控制台。要启用密码身份验证，请添加或编辑以下行：

```
com.vontu.manager.form_authentication = true
```

仅当需要为所有 Enforce Server 管理控制台帐户（包括管理员帐户）提供有效证书时，才将此选项设置为 false（禁用基于表单的登录）。确保已安装所有必需的证书并确定用户能够使用证书身份验证登录。

请参见第 105 页的“[将证书颁发机构 \(CA\) 证书添加到 Tomcat 信任存储区](#)”。

- 5 保存更改并退出文本编辑器。
- 6 将目录更改为 /opt/Vontu/Protect/tomcat/conf (Linux) 或 c:\Vontu\Protect\tomcat\conf (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。
- 7 使用文本编辑器打开 server.xml 文件。

- 8 要启用或验证证书身份验证，请添加或编辑 `clientAuth="want"` 选项，如该文件中的以下行所示：

```
<Connector URIEncoding="UTF-8" acceptCount="100" clientAuth="want"
debug="0" disableUploadTimeout="true" enableLookups="false"
keystoreFile="conf/.keystore" keystorePass="protect"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
port="443" scheme="https" secure="true" sslProtocol="TLS"
truststoreFile="conf/truststore.jks" truststorePass="protect"/>
```

- 9 保存更改并退出文本编辑器。
- 10 停止然后重新启动 Vontu Manager 服务以应用更改。
- 11 配置并启用证书吊销。

请参见第 108 页的“[关于证书吊销检查](#)”。

将证书颁发机构 (CA) 证书添加到 Tomcat 信任存储区

仅在 Symantec Data Loss Prevention 安装期间未导入 CA 证书，或升级早期 Symantec Data Loss Prevention 安装且要配置证书身份验证时，才需要执行此过程。在将 OCSP 响应器证书添加到一些 OCSP 配置的信任存储区时，也需要执行此过程。

要将证书身份验证用于 Symantec Data Loss Prevention，必须向 Tomcat 信任存储区添加验证系统中用户的身份所需的所有 CA 证书。每个 X.509 证书都必须以唯一编码规则(DER)格式在 .cer 文件中提供。如果需要使用多个 CA 来建立证书链，必须添加多个 .cer 文件。

将 CA 证书添加到 Tomcat 信任存储区

- 1 使用在 Symantec Data Loss Prevention 安装过程中创建的帐户登录到 Enforce Server 计算机。

注意：如果使用其他帐户（例如，根或管理员帐户）登录，请确保在后面的步骤中不会更改对任何 Tomcat 配置文件的权限或所有权。

- 2 将目录更改为 /opt/Vontu/Protect/tomcat/conf (Linux) 或 c:\Vontu\Protect\tomcat\conf (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。
- 3 复制要导入到 Enforce Server 计算机上 conf 目录的所有证书文件 (.cer 文件)。

- 4 使用随 Symantec Data Loss Prevention 一起安装的 keytool 实用程序将证书添加到 Tomcat 信任存储区。对于 Windows 系统，请输入：

```
c:\Vontu\jre\bin\keytool -import -trustcacerts -alias CA_CERT_1 -file certificate_1.cer  
-keystore .\truststore.jks
```

对于 Linux 系统，请输入：

```
/opt/Vontu/jre/bin/keytool -import -trustcacerts -alias CA_CERT_1 -file certificate_1.cer  
-keystore ./truststore.jks
```

在上述命令中，将 *CA_CERT_1* 替换为要导入的证书的唯一别名。将 *certificate_1.cer* 替换为复制到 Enforce Server 计算机的证书文件的名称。

- 5 当 keytool 实用程序提示您输入 keystore 密码时，请执行此操作。如果未更改默认的 keystore 密码，则密码为 protect。
- 6 要安装完成证书链所必需的所有证书文件，请重复执行这些步骤。
- 7 停止然后重新启动 Vontu Manager 服务以应用更改。
- 8 如果尚未更改默认的 Tomcat keystore 密码，请现在进行更改。

请参见第 106 页的“[更改 Tomcat 信任存储区密码](#)”。

更改 Tomcat 信任存储区密码

在安装 Symantec Data Loss Prevention 时，Tomcat 信任存储区使用默认密码 protect。在使用证书身份验证时，请按照以下过程为 Tomcat 信任存储区分配安全密码。

更改 Tomcat 信任存储区密码

- 1 使用在 Symantec Data Loss Prevention 安装过程中创建的帐户登录到 Enforce Server 计算机。

注意：如果使用其他帐户（例如，根或管理员帐户）登录，请确保在后面的步骤中不会更改对任何 Tomcat 配置文件的权限或所有权。

- 2 将目录更改为 /opt/Vontu/Protect/tomcat/conf (Linux) 或 c:\Vontu\Protect\tomcat\conf (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。

- 3 使用随 Symantec Data Loss Prevention 一起安装的 keytool 实用程序更改 Tomcat 信任存储区密码。对于 Windows 系统，请输入：

```
c:\Vontu\jre\bin\keytool -storepasswd -new new_password -keystore ./truststore.jks
```

对于 Linux 系统，请输入：

```
/opt/Vontu/jre/bin/keytool -storepasswd -new new_password -keystore ./truststore.jks
```

在上述命令中，将 *new_password* 替换为安全密码。

- 4 当 keytool 实用程序提示您输入 keystore 的当前密码时，请执行此操作。如果未更改默认的 keystore 密码，则密码为 protect。
5 将目录更改为 /opt/Vontu/Protect/tomcat/conf (Linux) 或 c:\Vontu\Protect\tomcat\conf (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。
6 使用文本编辑器打开 server.xml 文件。
7 在该文件的以下行中，编辑 truststorePass="protect" 条目以指定新密码：

```
<Connector URIEncoding="UTF-8" acceptCount="100" clientAuth="want"  
debug="0" disableUploadTimeout="true" enableLookups="false"  
keystoreFile="conf/.keystore" keystorePass="protect"  
maxSpareThreads="75" maxThreads="150" minSpareThreads="25"  
port="443" scheme="https" secure="true" sslProtocol="TLS"  
truststoreFile="conf/truststore.jks" truststorePass="protect"/>
```

将 *protect* 替换为您在 keytool 命令中定义的新密码。

- 8 保存更改并退出文本编辑器。
9 将目录更改为 /opt/Vontu/Protect/config (Linux) 或 c:\Vontu\Protect\config (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。
10 使用文本编辑器打开 Manager.properties 文件。
11 在该文件中添加以下行以指定新密码：

com.vontu.manager.tomcat.truststore.password = *password*
将 *password* 替换为新密码。请勿将密码放入引号中。
12 保存更改并退出文本编辑器。
13 停止然后重新启动 Vontu Manager 服务以应用更改。

将常见名称 (CN) 值映射到 Symantec Data Loss Prevention 用户帐户

对于要使用基于证书的单一登录访问 Enforce Server 管理控制台的每个用户，必须在 Enforce Server 配置中拥有一个活动用户帐户。该用户帐户会将用户客户端证书的常见名称 (CN) 值与 Enforce Server 管理控制台中的一个或多个角色关联。只能将一个 CN 值映射到一个 Enforce Server 用户帐户。

您创建的用户帐户不需要单独的 Enforce Server 管理控制台密码。但是，如果还希望允许用户从 Enforce Server 管理控制台登录页面登录，可以选择配置密码。如果启用了密码身份验证且用户在浏览器要求提供证书时未提供证书，则 Enforce Server 会显示登录页面。（如果禁用了密码身份验证且用户未提供证书，将显示登录失败。）

要使用户能够通过使用证书身份验证的单一登录方式进行登录，活动用户帐户必须识别用户的 CN 值，并在 Enforce Server 配置中为该用户帐户分配有效的角色。如果要在未取消用户客户端证书时防止用户访问 Enforce Server 管理控制台，请禁用或删除关联的 Enforce Server 用户帐户。

请参见第 91 页的“[配置用户帐户](#)”。

关于证书吊销检查

当管理公钥基础架构时，将需要使用 CA 定期取消客户端的证书。例如，如果员工离开公司或员工的凭据丢失或被盗，则应取消证书。在吊销证书时，CA 会使用一个或多个证书吊销列表 (CRL) 来公布那些不再有效的证书。Symantec Data Loss Prevention 还支持使用联机证书状态协议 (OCSP) 响应器，客户端可使用该响应器确定特定证书是否已被取消。OCSP 响应器可作为 CA 服务器上的一项服务来实现，也可以作为独立 OCSP 服务器实现。

OCSP 是 Symantec Data Loss Prevention 用来执行证书吊销检查的第一个机制。在 Tomcat 容器确定客户端证书有效后，Enforce Server 向指定的 OCSP 响应器发送 OCSP 请求以确定该证书是否已被取消。可用以下两种方法之一来提供用于联系 OCSP 响应器的信息：

- 客户端证书中的“颁发机构信息访问(AIA)”字段。客户端证书本身可在 AIA 字段中包含 OCSP 响应器的 URL。下面显示定义 OCSP 响应器的 AIA 字段示例：

```
[1]Authority Info Access Access Method=On-line
Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name: URL=http://my_ocsp_responder
```

在通过配置内部 CA 来提供 OCSP 响应器服务时，通常会使用此方法。如果可从 Enforce Server 计算机直接访问 AIA 字段中指定的 OCSP 响应器，则无需其他配置即可执行吊销检查。但是，如果仅能通过代理服务器访问 OCSP 响应器，则必须在 Symantec Data Loss Prevention 配置中配置代理服务器设置。

- OCSP 配置文件。您也可以使用 `manager-certauth.security` 配置文件手动配置 OCSP 响应器属性。如果选择使用此文件，则此文件中的配置会覆盖客户端证书的 AIA 字段中的所有信息。如果希望使用本地 OCSP 响应器而不是 AIA 字段中指定的响应器，或您的客户端证书不包含 AIA 字段，通常会使用此方法。
请参见第 112 页的“[手动配置 OCSP 响应器属性](#)”。

注意：如果此文件中配置的 OCSP 响应器未使用 CA 证书签署其响应，则必须将 OCSP 响应器的证书添加到 Tomcat 信任存储区。

请参见第 105 页的“[将证书颁发机构 \(CA\) 证书添加到 Tomcat 信任存储区](#)”。

如果使用 OCSP 无法确定证书的吊销状态，则 Symantec Data Loss Prevention 会从证书吊销列表分发点 (CRLDP) 检索吊销列表。要使用 CRLDP 检查吊销，客户端证书必须包含 CRL 分发点字段。下面显示 CRLDP 字段定义示例：

```
[1]CRL Distribution Point
  Distribution Point Name:
    Full Name: URL=http://my_crldp
```

注意：Symantec Data Loss Prevention 不支持使用 LDAP URL 指定 CRLDP。

如果每个证书中都定义了 CRL 分发点且 Enforce Server 可直接访问服务器，则无需其他配置即可执行吊销检查。但是，如果仅能通过代理服务器访问 CRL 分发点，则必须在 Symantec Data Loss Prevention 配置中配置代理服务器设置。

请参见第 111 页的“[使用代理访问 OCSP 响应器或 CRLDP](#)”。

无论您使用哪种吊销检查方法，都必须在 Enforce Server 计算机上启用证书吊销检查。如果在 Enforce Server 安装期间选择证书安装，则证书吊销检查在默认情况下处于启用状态。如果已升级现有 Symantec Data Loss Prevention 安装，则证书吊销在默认情况下未处于启用状态。

请参见第 110 页的“[配置证书吊销检查](#)”。

如果 Enforce Server 计算机必须使用代理访问 OCSP 响应器服务或 CRLDP，则必须在 Enforce Server 计算机上配置代理设置。

请参见第 111 页的“[使用代理访问 OCSP 响应器或 CRLDP](#)”。

如果将 OCSP 用于吊销检查但证书客户端证书 AIA 字段未指定有效的 OCSP 响应器，则必须在 `manager-certauth.security` 配置文件中手动配置 OCSP 响应器属性。

请参见第 112 页的“[手动配置 OCSP 响应器属性](#)”。

配置证书吊销检查

当您启用证书吊销检查时，Symantec Data Loss Prevention 会使用 OCSP 确定每个客户端证书是否已被证书颁发机构吊销。如果使用 OCSP 无法确定证书状态，Symantec Data Loss Prevention 将使用 CRLDP 确定吊销状态。

按照以下过程启用证书吊销检查。

配置证书吊销检查

- 1 确保在每个证书的 AIA 字段或 manager-certauth.security 文件中配置了 OCSP 响应器。

请参见第 108 页的“[关于证书吊销检查](#)”。

请参见第 112 页的“[手动配置 OCSP 响应器属性](#)”。
- 2 确保在每个客户端证书的 CRL 分发点字段中定义了 CRLDP。
- 3 使用在 Symantec Data Loss Prevention 安装过程中创建的帐户登录到 Enforce Server 计算机。

注意：如果使用其他帐户（例如，根或管理员帐户）登录，请确保在后面的步骤中不会更改对任何 Symantec Data Loss Prevention 配置文件的权限或所有权。

- 4 将目录更改为 /opt/Vontu/Protect/config (Linux) 或 c:\Vontu\Protect\config (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。
- 5 使用文本编辑器打开 VontuManager.conf 文件。
- 6 要启用证书吊销检查，请在该文件中添加或编辑以下行：

```
wrapper.java.additional.18=-Dcom.sun.net.ssl.checkRevocation=true
```

要禁用这些检查，请将值更改为 false。
- 7 如果要手动配置 OCSP 响应器服务器，请不要使用客户端证书中的 AIA 字段，而是在文件中编辑以下行：

```
wrapper.java.additional.19=-Djava.security.properties=../config/manager-certauth.security
```

此外，如果要禁用 OCSP 吊销检查，请在该文件启用此行。（然后可通过配置 manager-certauth.security 中的属性来禁用 OCSP 检查）。

确保配置参数指向所指示的 OCSP 配置文件。始终编辑现有 manager-certauth.security 文件，而不是创建新文件。

请参见第 112 页的“[手动配置 OCSP 响应器属性](#)”。

- 8 要使用 CRLDP 启用吊销检查，请在该文件中添加或取消注释以下行：

```
wrapper.java.additional.21=-Dcom.sun.security.enableCRLDP=true
```

对于新的 Symantec Data Loss Prevention 安装，此选项默认情况下处于启用状态。

- 9 如果使用 CRLDP 吊销检查，可以选择使用以下属性配置缓存寿命：

```
wrapper.java.additional.20=-Dsun.security.certpath.ldap.cache.lifetime=30
```

此参数指定缓存从 CRL 分发点获取的吊销列表的时间长度（以秒为单位）。达到此时间后，将执行查找，以在下次请求身份验证时刷新缓存。默认的缓存寿命为 30 秒。将此时间指定为 0 表示禁用缓存，指定为 -1 表示无限制地存储缓存结果。

- 10 停止然后重新启动 Vontu Manager 服务以应用更改。

使用代理访问 OCSP 响应器或 CRLDP

Symantec 建议允许从 Enforce Server 计算机直接访问执行证书吊销检查的所有 OCSP 响应器服务器和 CRLDP 服务器。但是，如果 OCSP 响应器或 CRLDP 服务器只能通过代理访问，则必须在 Enforce Server 计算机上配置代理设置。

配置代理时，Enforce Server 为所有 HTTP 连接（例如，连接到 Data Insight 服务器以获取证书时创建的连接）使用代理配置。请在配置这些代理设置之前与您的代理管理员协商，尽可能考虑允许对 OCSP 和 CRLDP 服务器的直接访问。

为 OCSP 响应器或 CRLDP 服务器配置代理设置

- 1 确保在每个证书的 AIA 字段配置了 OCSP 响应器。

请参见第 108 页的“[关于证书吊销检查](#)”。

- 2 确保在每个客户端证书的 CRL 分发点字段中定义了 CRLDP。

- 3 使用在 Symantec Data Loss Prevention 安装过程中创建的帐户登录到 Enforce Server 计算机。

注意：如果使用其他帐户（例如，根或管理员帐户）登录，请确保在后面的步骤中不会更改对任何 Symantec Data Loss Prevention 配置文件的权限或所有权。

- 4 将目录更改为 /opt/Vontu/Protect/config (Linux) 或 c:\Vontu\Protect\config (Windows) 目录。如果将 Symantec Data Loss Prevention 安装到了其他目录，请替换为正确的路径。
- 5 使用文本编辑器打开 VontuManager.conf 文件。

6 添加或编辑下列配置属性以确定代理:

```
wrapper.java.additional.22=-Dhttp.proxyHost=myproxy.mydomain.com
wrapper.java.additional.23=-Dhttp.proxyPort=8080
wrapper.java.additional.24=-Dhttp.nonProxyHosts=hosts
```

用代理服务器的主机名和端口替换 *myproxy.mydomain.com* 和 *8080*。用一个或多个代理不可用时可访问的 OCSP 响应器来替换 *hosts*。可以包括服务器主机名、完全限定域名或 IP 地址（以竖线字符分隔）。例如：

```
wrapper.java.additional.24=-Dhttp.nonProxyHosts=ocsp-server|
127.0.0.1|DataInsight_Server_Host
```

- 7 保存对配置文件所做的更改。
- 8 停止然后重新启动 Vontu Manager 服务以应用更改。

手动配置 OCSP 响应器属性

您可以选择编辑 *manager-certauth.security* 文件来为系统配置 OCSP 连接参数。默认情况下，此文件启用 OCSP 检查，但所有其他选项都被注释掉，处于非活动状态。如果取消注释该文件中的任何参数，这些参数将覆盖客户端证书的 AIA 字段中的 OCSP 配置。

请参见第 108 页的“[关于证书吊销检查](#)”。

注意：如果此文件中配置的 OCSP 响应器未使用 CA 证书签署其响应，则必须将 OCSP 响应器的证书添加到 Tomcat 信任存储区。

请参见第 105 页的“[将证书颁发机构 \(CA\) 证书添加到 Tomcat 信任存储区](#)”。

manager-certauth.security 位于 /opt/Vontu/Protect/config (Linux) 或 c:\Vontu\Protect\config (Windows) 目录。应始终编辑现有的 *manager-certauth.security* 文件，而不要创建新文件。您可能需要在进行更改之前备份文件，以保留原始内容。

该文件包含下列参数。

表 5-4 OCSP 配置参数

配置参数的示例	说明
ocsp.enable=true	如果 <i>VontuManager.properties</i> 文件中启用了证书吊销，则此参数将使 OCSP 进行吊销检查。默认情况下为所有 Symantec Data Loss Prevention 安装启用此参数。如果您希望仅使用 CRLDP 检查而不使用 OCSP，则禁用该属性。

配置参数的示例	说明
ocsp.responderURL=http://ocsp.example.net:80	定义 OCSP 响应器的 URL。如果不定义此参数，将从客户端证书中的 AIA 字段获取 URL（如果可用）。
ocsp.responderCertSubjectName=CN=OCSP Responder, O=XYZ Corp	定义与 OCSP 响应器相对应的证书的主题名称。默认情况下，Symantec Data Loss Prevention 假定客户端证书发行机构的证书与 OCSP 响应器的证书相对应。如果不使用此默认配置，必须使用其他方法来确定 OCSP 响应器的证书。还必须将 OCSP 响应器证书添加到 Tomcat 信任存储区。 请参见第 105 页的“ 将证书颁发机构(CA)证书添加到Tomcat信任存储区 ”。
ocsp.responderCertIssuerName=CN=Enterprise CA, O=XYZ Corp	如果仅使用主题名称无法明确确定 OCSP 响应器的证书，可同时使用 ocsp.responderCertIssuerName 和 ocsp.responderCertSerialNumber 参数，而不使用 ocsp.responderCertSubjectName。（如果定义 ocsp.responderCertSubjectName，则忽略此表中其余两个参数。） 组合使用此参数与 ocsp.responderCertSerialNumber 来确定 OCSP 响应器证书。此参数定义 OCSP 响应器的证书的证书发行机构。 如果使用此参数，不要同时使用 ocsp.responderCertSubjectName 参数。
ocsp.responderCertSerialNumber=2A:FF:00	组合使用此参数与 ocsp.responderCertIssuerName 来确定 OCSP 响应器证书。此参数定义 OCSP 响应器的证书的序列号。 如果使用此参数，不要同时使用 ocsp.responderCertSubjectName 参数。

manager-certauth.security 包含关于这些参数的其他信息。您也可以参阅 Java 文档，位置：

<http://download.oracle.com/javase/6/docs/technotes/guides/security/certpath/CertPathProgGuide.html#AppC>。但请注意，此 URL 处提供的某些示例在主题名定义部分包含引号，这不受支持。

排除证书身份验证故障

默认情况下，Symantec Data Loss Prevention 记录对 Enforce Server 管理控制台的每次成功登录请求。如果发出登录请求而未提供证书，或者有效证书中的 CN 未映射到 Enforce Server 配置中的有效用户帐户，则 Symantec Data Loss Prevention 还会记录错误消息。

注意：如果浏览器与 Enforce Server 管理控制台建立 HTTPS 连接时证书身份验证失败，Symantec Data Loss Prevention 不能记录错误消息。

您可以通过在 VontuManager.conf 文件中添加或取消注释下列系统属性来有选择地记录有关证书吊销检查的其他信息。

```
wrapper.java.additional.90=-Djava.security.debug=certpath
```

VontuManager.conf 位于 c:\Vontu\Protect\config (Windows) 或 /opt/Vontu/Protect/config (Linux) 目录。所有调试消息均记录于 c:\Vontu\Protect\logs\debug\VontuManager.log (Windows) 或 /var/log/Vontu/debug/VontuManager.log (Linux)。

禁用密码身份验证和基于表单的登录

当您配置和测试证书身份验证时，基于表单的登录和密码身份验证可用作备用访问机制。在配置证书身份验证后，可以选择禁用基于表单的登录和密码身份验证，以依靠公钥基础架构处理所有登录请求。要完全禁用基于表单的登录，请在 Manager.properties 配置文件中添加或编辑以下值。

```
com.vontu.manager.form_authentication = false
```

请参见第 104 页的“[为 Enforce Server 管理控制台配置证书身份验证](#)”。

必须停止然后重新启动 Vontu Manager 服务以应用更改。

注意：禁用基于表单的登录会对所有用户（包括拥有管理员权限的用户）禁用该功能。或者，可以通过配置单个用户的帐户对该用户禁用基于表单的登录或证书身份验证。

请参见第 91 页的“[配置用户帐户](#)”。

如果以后启用基于表单的登录但管理员用户帐户尚未配置密码，可以使用 AdminPasswordReset 实用程序重置管理员密码。

请参见第 95 页的“[重置管理员密码](#)”。

连接到组目录

本章节包括下列主题：

- [关于连接到目录组服务器](#)
- [配置目录服务器连接](#)
- [计划目录服务器索引编制](#)

关于连接到目录组服务器

Symantec Data Loss Prevention 支持与 LDAP 兼容目录服务器（例如 Microsoft Active Directory (AD)）的目录服务器连接。组目录连接指定 Enforce Server 或发现服务器如何连接至目录服务器。

在 Enforce Server 中创建任何用户组之前，必须建立与目录服务器的连接。Enforce Server 或发现服务器使用该连接来获取这些组的相关详细信息。如果不创建该连接，则无法定义任何组。该连接不是永久性的，但可配置为按指定的时间间隔同步。目录服务器包含创建用户组所需的所有信息。

如果使用包含自我签署的身份验证证书的目录服务器，则必须将该证书添加到 Enforce Server 或发现服务器。如果您的目录服务器使用预先授权的证书，系统会将其自动添加到 Enforce Server 或发现服务器。

请参见第 487 页的“[创建或修改用户组](#)”。

请参见第 485 页的“[关于实施同步的目录组匹配](#)”。

请参见第 190 页的“[将 SSL 证书导入到 Enforce Server 或发现服务器](#)”。

请参见第 314 页的“[关于用户组](#)”。

配置目录服务器连接

“系统” > “设置” > “组目录” > “配置目录连接” 是用于配置目录服务器连接的主页面。

请参见第 486 页的[“关于连接到目录组服务器”](#)。

建立目录连接

- 1 单击“创建新连接”。
- 2 输入目录服务器连接的“名称”。
- 3 指定目录服务器连接的“网络参数”。
- 4 指定连接至目录服务器所用的“身份验证”模式。

[表 6-1](#)

- 5 单击“测试连接”以验证连接情况。
如果连接出错，系统会显示一条错误消息来描述问题。
- 6 单击“保存”保存目录连接配置。
- 7 验证目录服务器是否已在“索引和复制状态”选项卡中编制索引。
在成功创建、测试并保存目录服务器连接后，系统将自动对目录服务器编制索引。验证“复制状态”是否显示“已完成 <日期> <时间>”。
- 8 视需要，从“索引设置”选项卡调整目录服务器编制索引日程表。
请参见第 118 页的[“计划目录服务器索引编制”](#)。

表 6-1 目录连接网络参数

网络参数	说明
主机名	您必须输入 LDAP 服务器的完全限定名称 (FQN)。请勿使用 IP 地址。 例如，LDAPserver1.hr.corp。
端口	LDAP 服务器端口。默认值为 389。例如，port = 389。

网络参数	说明
基本 DN	<p>LDAP 目录内开始搜索的起始深度。在定义此参数时，请记住，查询开始的位置离信息越近，响应就越快。例如，<code>basedn = DC=corp, DC=hr</code>。</p> <p>“基础 DN”是目录服务器的基础可分辨名称。通常，此名称是 AD 服务器的域名。一般情况下，使用代码来区分域名的每个部分。例如，代码 <code>DC=</code>。如果您希望连接到服务器 example.symantec.com，应使用以下术语来定义基本 DN：</p> <p><code>DC=example, DC=symantec, DC=com</code></p> <p>注意：如果您对判别名或 AD 服务器不太了解，请与您的 AD 服务器管理员联系以获取您的 AD 判别名。</p> <p>“组目录”屏幕中列出了当前组目录连接。</p> <p>可以按以下方式查看和排序现有连接：</p> <ul style="list-style-type: none"> ■ “连接名称”：用户定义的连接名称。 ■ “主机名”：安装目录服务器的计算机的主机名。 ■ “基础 DN”：目录服务器的基础可分辨名称。 ■ “端口”：启用目录服务器连接的端口。 ■ “加密方法”：无或安全。 <p>请参见第 190 页的“将 SSL 证书导入到 Enforce Server 或发现服务器”。</p>
加密方法	<p>如果想要使用 SSL 对 LDAP 服务器与 Enforce Server 之间的通信进行加密，请选择“安全的”选项。</p> <p>注意：如果您选择使用安全连接，可能需要将 LDAP 服务器安全证书导入 Enforce Server Keystore。请参见第 190 页的“将 SSL 证书导入到 Enforce Server 或发现服务器”。</p>

表 6-2 目录连接身份验证参数

身份验证	说明
匿名	<p>选择此身份验证模式会以匿名的形式连接到 LDAP 服务器。</p> <p>注意：大多数目录服务器不允许匿名连接。</p>
进行身份验证	默认值为 <code>simple</code> 。例如， <code>authtype = simple</code> 。如果无法建立连接，可能需要修改身份验证类型。

身份验证	说明
用户名	<p>有权访问 LDAP 服务器的帐户的用户名。例如，<code>username = symantec_dlp</code>。基于对 LDAP 服务器具有读取权限的帐户，该行的格式可能会有所变化。例如，Microsoft Active Directory 系统的用户名可能需要按以下格式来指定：域\用户名。而 Sun LDAP 服务器的用户名可能需要按以下格式来指定：<code>uid=用户名,ou=people,o=公司</code>。</p> <p>用于对 AD 连接进行身份验证的用户名。</p> <p>您可以在下列某项中输入用户名：</p> <ul style="list-style-type: none"> ■ Windows 登录 (Enterprise\firstname_lastname) ■ 用户名和域 (<code>username@domain.com</code>) <p>用户在AD服务器中的完整判别名 (<code>cn=用户名, cn=用户, dc=域, dc=com</code>)</p>
Password	<p>在上一个字段中指定的用户名的密码。例如，<code>password = Shazam!44</code>。</p> <p>注意：这些用户名和密码凭据以明文形式存储。如果这些凭据在 LDAP 服务器上发生了更改但未在此 properties 文件中更新，查找将失败。</p>

计划目录服务器索引编制

每个目录连接已设置为在创建初始连接的第二天上午 12:00，自动对已配置的 LDAP 服务器创建“一次”索引。您可以修改索引编制日程表以指定对索引进行同步的时间和频率。

将每个目录服务器连接设置为：在创建初始连接的第二天上午 12:00 自动对目录服务器中托管的已配置用户组编制索引“一次”。

在您创建、测试和保存目录服务器连接后，系统会自动为已建立连接的目录中托管的所有用户组编制索引。您可以修改此设置，可以每日、每周或每月计划索引编制。

计划组目录索引编制

1 从“系统”>“设置”>“组目录”屏幕中选择一个现有的组目录服务器连接。

您也可以创建一个新连接。

请参见第 116 页的[“配置目录服务器连接”](#)。

2 将“索引设置”调整为所需的计划。

请参见第 119 页的[表 6-3](#)。

表 6-3 计划组目录服务器索引编制并查看状态

索引设置	说明
编制目录服务器索引一次。	<p>默认情况下，选择“一次”设置并在您创建初始连接后的第二天 12:00 AM 自动对目录服务器编制索引。</p> <p>您可以通过指定期望重建索引的时间和频率来修改默认的“一次”索引编制计划。</p>
每日编制目录服务器索引一次。	<p>选择“每日”选项，以便每日都能对索引进行计划。</p> <p>对于此计划，可以将持续时间指定为“某一天的某个时间”或“直到”。</p>
每周编制目录服务器索引一次。	<p>选择“每周”选项，以便每周都能对索引编制计划一次。</p> <p>将编制索引的时间指定为“某一周的某一天”。</p> <p>指定要编制索引的“时间”。</p> <p>此外，对于此计划，也可以将持续时间指定为“直到”。</p>
每月编制目录服务器索引一次。	<p>指定在“某个月的某一天”的某个“时间”编制目录的索引。</p> <p>此外，对于此计划，也可以将持续时间指定为“直到”。</p>
查看索引编制和复制状态。	<p>选择“索引和复制状态”选项卡查看索引编制进程的状态。</p> <ul style="list-style-type: none">■ 索引状态 显示下次计划的索引、日期和时间。■ 检测服务器名称 显示部署了用户组配置文件的检测服务器。■ 复制状态 显示最近与目录组服务器同步的数据和时间。

管理存储的凭据

本章节包括下列主题：

- [关于凭据存储](#)
- [将新凭据添加到凭据存储中](#)
- [配置端点凭据](#)
- [管理凭据存储中的凭据](#)

关于凭据存储

身份验证凭据可以作为已命名凭据存储在中央凭据存储中。可以定义该凭据，然后由任意数量的发现目标引用。在存储密码之前，需对其进行加密。

凭据存储简化了用户名和密码更改的管理。

您可以添加、删除或编辑存储的凭据。

请参见第 121 页的“[将新凭据添加到凭据存储中](#)”。

请参见第 123 页的“[管理凭据存储中的凭据](#)”。

具有“凭据管理”权限的用户可以访问“凭据管理”屏幕。

当编辑或创建发现目标时，可以使用存储的凭据。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

将新凭据添加到凭据存储中

您可以将新凭据添加到凭据存储中。稍后可以通过凭据名称引用这些凭据。

添加存储的凭据

- 1 单击“系统”>“设置”>“凭据”，然后单击“添加凭据”。
- 2 输入下列信息：

凭据名称	输入该存储凭据的名称。 凭据名称在凭据存储内必须是唯一的。名称仅用于识别凭据。
访问用户名	输入用户名以进行身份验证。
访问密码	输入密码以进行身份验证。
重新输入访问密码	重新输入密码。

- 3 单击“保存”。
- 4 稍后您可以编辑或删除凭据存储中的凭据。
请参见第 123 页的[“管理凭据存储中的凭据”](#)。
请参见第 122 页的[“配置端点凭据”](#)。

配置端点凭据

必须先将凭据添加到凭据存储中，然后才可以访问 Endpoint FlexResponse 或 Endpoint Discover 隔离响应规则的凭据。这些凭据存储在连接到 Endpoint Server 的所有端点计算机上的加密文件夹中。由于所有端点计算机都存储凭据，因此必须注意存储的凭据的类型。使用无法访问系统其他区域的凭据。必须首先启用Enforce Server 识别端点凭据，然后才可以使用它们。

创建端点凭据

- 1 转至：“系统”>“设置”>“常规”。
- 2 单击“配置”。
- 3 在“凭据管理”部分下，确保选中“允许端点代理上的已保存凭据”复选框。
- 4 单击“保存”。
- 5 转至：“系统”>“设置”>“凭据”。
- 6 单击“添加凭据”。
- 7 在“常规”部分下，输入要添加的凭据的详细信息。

8 在“使用权限”下，选择“服务器和端点代理”。

9 单击“保存”。

请参见第 121 页的“[关于凭据存储](#)”。

请参见第 693 页的“[配置“Endpoint Discover: 隔离文件”操作](#)”。

管理凭据存储中的凭据

您可以删除或编辑存储的凭据。

删除存储的凭据

- 1 单击“系统”>“设置”>“凭据”。找出要删除的存储凭据的名称。
- 2 单击名称右侧的删除图标。只有发现目标或已编制索引的文档配置文件中当前均未引用此凭据，才可以将其删除。

编辑存储的凭据

- 1 单击“系统”>“设置”>“凭据”。找出要编辑的存储凭据的名称。
- 2 单击名称右侧的编辑图标（铅笔）。
- 3 更新用户名或密码。
- 4 单击“保存”。
- 5 如果您更改给定凭据的密码，则新密码可用于使用此凭据的所有后续发现扫描。

管理系统事件和消息

本章节包括下列主题：

- [关于系统事件](#)
- [系统事件报告](#)
- [使用保存的系统报告](#)
- [服务器事件详细信息](#)
- [配置触发事件的阈值](#)
- [关于系统事件响应](#)
- [启用 Syslog 服务器](#)
- [关于系统警报](#)
- [配置 Enforce Server 以发送电子邮件警报](#)
- [配置系统警报](#)
- [关于日志查看](#)
- [系统事件代码和消息](#)

关于系统事件

与 Symantec Data Loss Prevention 安装相关的系统事件会被监控、报告和记录。

可从 Enforce Server 管理控制台查看系统事件报告：

- 严重性为“警告”或“严重”的最近的五个系统事件会列在“服务器概述”屏幕（“系统”>“服务器”>“概述”）中。
请参见第 191 页的[“关于系统概述屏幕”](#)。

- 通过转至“系统”>“服务器”>“事件”来查看任何严重性的所有系统事件的报告。

请参见第 126 页的[“系统事件报告”](#)。

- 特定检测服务器的最近系统事件列在该服务器的“[服务器详细信息](#)”屏幕上。请参见第 194 页的[“服务器详细信息”屏幕](#)。

- 单击事件列表中的任何事件，转至该事件的“[事件详细信息](#)”屏幕。“[事件详细信息](#)”屏幕提供有关该事件的其他信息。

请参见第 129 页的[“服务器事件详细信息”](#)。

系统事件引起您注意的方式有三种：

- 显示在管理控制台上的系统事件报告

- 系统警报电子邮件

请参见第 135 页的[“关于系统警报”](#)。

- Syslog 功能

请参见第 134 页的[“启用 Syslog 服务器”](#)。

有些系统事件要求响应。

请参见第 132 页的[“关于系统事件响应”](#)。

要缩小系统事件管理的重点，您可以：

- 在多种系统事件通知方法中使用过滤器。

请参见第 126 页的[“系统事件报告”](#)。

- 为个别服务器配置系统事件阈值。

请参见第 130 页的[“配置触发事件的阈值”](#)。

系统事件报告

要查看所有系统事件，请转至系统事件报告屏幕（“系统”>“服务器”>“事件”）。此屏幕会列出事件（一行一个事件）。该列表包含那些与所选数据范围以及在“已应用过滤器”栏中列出的任何其他过滤器选项匹配的事件。对于每个事件，将显示下列信息：

表 8-1 系统事件列表

类型 事件的类型（严重性）。类型可能是表 8-2 中列出的任何一种。

时间 事件的日期和时间。

服务器 发生事件的服务器的名称。

主机 发生事件的服务器的 IP 地址或主机名。

代码 标识此类事件的编号。

请参见第 138 页的“[系统事件代码和消息](#)”。

摘要 事件的简要说明。单击摘要以获取有关事件的更多详细信息。

表 8-2 系统事件类型

 系统信息

 警告

 严重

可以从多个报告处理选项中进行选择。

请参见第 801 页的“[常见事件报告功能](#)”。

单击列表中的任何事件以转至该事件的“[事件详细信息](#)”屏幕。“[事件详细信息](#)”屏幕提供有关该事件的其他信息。

请参见第 129 页的“[服务器事件详细信息](#)”。

由于事件列表可能很长，所以系统提供了过滤器以帮助您仅选择感兴趣的事件。默认情况下，只启用了日期过滤器，并且其初始设置为“所有日期”。日期过滤器按事件发生的日期选择事件。

按发生的日期过滤系统事件列表

- 1 转至事件报告屏幕的“过滤”部分，并选择其中一个日期范围选项。
- 2 单击“应用”。
- 3 从日期列表中选择“自定义”以指定开始日期和结束日期。

除按日期范围过滤之外，您也可以应用高级过滤器。高级过滤器是与当前的日期过滤器累计的。这意味着当事件既与高级过滤器匹配又处于当前日期范围内时才会被列出。可应用多个高级过滤器。如果应用多个过滤器，则只列出与所有过滤器和日期范围相匹配的事件。

应用附加高级过滤器

- 1 单击“高级过滤器和摘要”。
- 2 单击“添加过滤器”。
- 3 从最左侧的下拉列表选择您想使用的过滤器。[表 8-3](#) 中列出了可用的过滤器。
- 4 从中间的下拉列表选择过滤运算符。
对于每个高级过滤器，您可以指定过滤运算符“为任一”或“都不是”。
- 5 在右侧的文本框中输入一个或多个过滤器值，或单击列表中的值进行选择。

- 要选择列表中的多个值，请按住 Ctrl 键并单击每个值。
 - 要选择列表中的一系列值，请单击第一个值，然后按住 Shift 键并单击您想选择的系列中的最后一个值。
- 6 (可选) 如果需要，请指定附加高级过滤器。
- 7 指定一个过滤器或一组过滤器后，请单击“应用”。
- 单击红色的 X 删除高级过滤器。

“已应用过滤器”栏列出了用于生成显示的事件列表的过滤器。请注意，多个过滤器是累积的。事件必须通过所有已应用的过滤器才能出现在列表中。

可以使用以下高级过滤器：

表 8-3 系统事件高级过滤器选项

事件代码	按识别此类事件的代码编号过滤事件。您可以按单一代码编号或多个由逗号分隔的代码编号（2121, 1202, 1204）进行过滤。不支持按代码编号范围、大于号或小于号操作符进行过滤。
事件类型	按事件严重性类型（信息、警告或严重）过滤事件。
服务器	按发生事件的服务器过滤事件。

注意：在触发系统事件的参数中，有少部分具有可配置的阈值。只能按照 Symantec 支持部门或专家服务的建议来调整这些参数。更改这些设置之前，应该彻底了解相关含义。默认值适用于大多数安装。

请参见第 130 页的“[配置触发事件的阈值](#)”。

请参见第 125 页的“[关于系统事件](#)”。

请参见第 129 页的“[服务器事件详细信息](#)”。

请参见第 128 页的“[使用保存的系统报告](#)”。

请参见第 130 页的“[配置触发事件的阈值](#)”。

请参见第 135 页的“[关于系统警报](#)”。

使用保存的系统报告

“系统报告”屏幕列出系统和先前保存的代理相关报告。要显示“系统报告”屏幕，请单击“系统”>“系统报告”。使用此屏幕来处理保存的系统报告。

创建保存的系统报告

1 转至下列屏幕之一：

- 系统事件（“系统” > “服务器” > “事件”）

- 代理概述（“系统” > “代理” > “概述”）

- 代理事件（“系统” > “代理” > “事件”）

请参见第 50 页的[“关于 Enforce Server 管理控制台”](#)。

- 2 选择自定义报告的过滤器和摘要。

请参见第 786 页的[“关于自定义报告和控制板”](#)。

- 3 选择“报告”>“另存为”。

- 4 输入已保存报告的信息。

请参见第 789 页的[“保存自定义事件报告”](#)。

- 5 单击“保存”。

“系统报告”屏幕分为两个部分：

- “系统事件” - “保存的报告”列出了保存的系统报告。

- “代理管理” - “保存的报告”列出保存的代理报告。

对于每个保存的报告，您可以执行以下操作：

- 共享报告。单击“共享”允许与您有相同角色的其他 Symantec Data Loss Prevention 用户共享此报告。共享报告不能撤消，报告一经共享，它就不再是专用的。共享报告后，共享该报告的所有用户都可查看、编辑或删除该报告。请参见第 789 页的[“保存自定义事件报告”](#)。

- 更改报告名称或说明。单击报告名称右侧的铅笔图标可对报告名称进行编辑。

- 更改报告日程表。单击报告名称右侧的日历图标可编辑报告的交付日程表和报告的接收者。

请参见第 789 页的[“保存自定义事件报告”](#)。

请参见第 791 页的[“事件和系统报告的交付日程表选项”](#)。

- 删除报告。单击报告名称右侧的红色 X 可以删除报告。

服务器事件详细信息

可通过“系统”>“服务器”>“事件”访问“服务器事件详细信息”屏幕，然后单击任一列出的事件。

请参见第 126 页的[“系统事件报告”](#)。

“服务器事件详细信息”屏幕显示了可用于所选事件的所有信息。此屏幕上的所有信息都是不可编辑的。

“服务器事件详细信息”屏幕分为两个部分 - “常规” 和 “消息”。

表 8-4 事件详细信息 - 常规

类型	事件属于以下类型之一：
	<ul style="list-style-type: none"> ■ 信息：有关系统的信息。 ■ 警告：没有严重到生成错误的问题。 ■ 严重：需要立即关注的错误。
时间	事件的日期和时间。
服务器	服务器的名称。
主机	服务器的主机名或 IP 地址。

表 8-5 事件详细信息 - 消息

代码	标识此类事件的编号。 请参见第 138 页的“ 系统事件代码和消息 ”。
摘要	事件的简要说明。
详细信息	有关事件的详细信息。 请参见第 125 页的“ 关于系统事件 ”。
	请参见第 129 页的“ 服务器事件详细信息 ”。
	请参见第 126 页的“ 系统事件报告 ”。
	请参见第 135 页的“ 关于系统警报 ”。

配置触发事件的阈值

在触发系统事件的参数中，有少部分具有可配置的阈值。这些参数针对每个检测服务器分别进行配置。只能按照 Symantec 支持部门或专家服务的建议来调整这些参数。更改这些设置之前，应该彻底了解相关含义。默认值适用于大多数安装。

请参见第 125 页的“[关于系统事件](#)”。

查看和更改可触发系统事件的可配置参数

- 1 转至“服务器概述”屏幕（“系统” > “服务器” > “概述”）。
- 2 单击检测服务器的名称，以显示该服务器的“[服务器详细信息](#)”屏幕。

3 单击“服务器设置”选项卡。

将显示该服务器的“高级服务器设置”屏幕。

4 根据需要更改可配置的参数。

表 8-6 会触发事件的可配置参数

参数	说明	事件
BoxMonitor.DiskUsageError	表示已占用的磁盘空间量（以百分比表示）达到多少时，会触发“严重”系统事件。例如，如果检测服务器安装在 C 驱动器上，且磁盘空间错误值为 90，则 C 驱动器使用率为 90% 或更高时，会发生“严重”事件，检测服务器会创建“严重”系统事件。默认值为 90。	磁盘空间不足
BoxMonitor.DiskUsageWarning	表示已占用的磁盘空间量（以百分比表示）达到多少时，会触发“警告”系统事件。例如，如果检测服务器安装在 C 驱动器上，且磁盘空间警告值为 80，则 C 驱动器使用率为 80% 或更高时，会发生“警告”事件，检测服务器会生成“警告”系统事件。默认值为 80。	磁盘空间不足
BoxMonitor.MaxRestartCount	表示一小时内的重新启动系统进程次数达到多少时，会生成“严重”系统事件。默认值为 3。	<i>process name</i> 重新启动次数过多
IncidentDetection.MessageWaitSevere	表示消息等待处理的时间达多少分钟时，会发送关于消息等待时间的“严重”系统事件。默认值为 240。	消息等待时间过长
IncidentDetection.MessageWaitWarning	表示消息等待处理的时间达多少分钟时，会发送关于消息等待时间的“警告”系统事件。默认值为 60。	消息等待时间过长
IncidentWriter.BacklogInfo	表示排入队列的事件数目到达多少时，会生成“信息”系统事件。此类型的积存通常表示由于系统变慢或停止而未处理或未正确处理事件。默认值为 1000。	队列中有 N 个事件
IncidentWriter.BacklogWarning	表示排入队列的事件数目到达多少时，会生成“警告”系统事件。此类型的积存通常表示由于系统变慢或停止而未处理或未正确处理事件。默认值为 3000。	队列中有 N 个事件

参数	说明	事件
IncidentWriter.BacklogSevere	表示排入队列的事件数目到达多少时，会生成“严重”系统事件。此类型的积存通常表示由于系统变慢或停止而未处理或未正确处理事件。默认值为 10000。	队列中有 N 个事件

关于系统事件响应

系统事件引起您注意的方式有三种：

- 显示在管理控制台上的系统事件报告
- 系统警报电子邮件
请参见第 135 页的“[关于系统警报](#)”。
- Syslog 功能
请参见第 134 页的“[启用 Syslog 服务器](#)”。

在大多数情况下，系统事件摘要和详细信息应提供足够的信息，以便采取调查与补救步骤。下表提供了一些响应系统事件的常规指导。

表 8-7 系统事件响应

系统事件或类别	相应的响应
磁盘空间不足	如果检测服务器上报告此事件，请在该检测服务器上重新开始 Symantec Data Loss Prevention 服务。检测服务器至 Enforce Server 的连接可能已中断，随后检测服务器会将其事件在本地排入队列，最终占满整个磁盘。 如果 Enforce Server 上报告此事件，请检查 Oracle 和 Vontu Incident Persister 服务的状态。如果事件未正确地从文件系统传输至数据库，则可能会造成磁盘空间不足。此事件也可能表示需要添加额外的磁盘空间。
表空间几乎已满	将其他数据文件添加至数据库。当硬盘容量已使用 80% 时，请不要再添加其他数据文件，而应改为获取更大容量的磁盘。 请参考《Symantec Data Loss Prevention 安装指南》。
授权许可和版本设置	联系 Symantec 支持部门。

系统事件或类别	相应的响应
监视器没有响应	<p>重新启动 Symantec Monitor 服务。如果事件仍存在，请检查网络连接。通过连接至托管检测服务器的计算机，以确保该计算机处于开启状态。您可以使用终端服务或其他远程桌面连接方法来连接。如果需要，请联系 Symantec 支持部门。</p> <p>请参见第 69 页的“关于 Enforce Server 服务”。</p>
警报或调度报告发送失败	转至“系统”>“设置”>“常规”，并确保已正确配置“报告和警报”和 SMTP 部分的设置。检查 Enforce Server 和 SMTP 服务器之间的网络连接。联系 Symantec 支持部门。
自动密钥启动失败	联系 Symantec 支持部门。
密码编译密钥不一致	联系 Symantec 支持部门。
消息等待时间过长	<p>通过添加更多 CPU 或将计算机替换为功能更强大的计算机，来增加检测服务器容量。</p> <p>减少检测服务器上的负载。您可以通过应用已配置为检测较少事件的通信过滤器，来减少负载。您也可以将部分通信重新路由至其他检测服务器。</p> <p>如果以下所有项目都属实，请增加阈值等待时间：</p> <ul style="list-style-type: none"> ■ 此消息在高峰时间段发出。 ■ 消息等待时间在下一个高峰之前降至零。 ■ 企业允许在消息处理时存在此类延迟。
process_name 重新启动次数过多	转至“系统”>“服务器”>“概述”检查此进程。要在此屏幕上查看各个进程，必须转至“系统”>“设置”>“常规”>“配置”启用“进程控制”。
队列中有 N 个事件	<p>调查事件占满队列的原因。</p> <p>最有可能的原因如下：</p> <ul style="list-style-type: none"> ■ 连接问题。响应：确保 Endpoint Server 与检测服务器之间的通信连接稳定。 ■ 相对于所生成事件的数目，连接带宽不足（通常为 WAN 连接）。响应：可以考虑（通过配置过滤器）更改策略，以减少其生成的事件。

启用 Syslog 服务器

Syslog 功能将“严重”系统事件发送到 Syslog 服务器。Syslog 服务器可让系统管理员使用更详细的级别来过滤并路由系统事件通知。定期使用 Syslog 监视其系统的系统管理员可能会选择使用 Syslog，而不使用警报。如果警报量过于庞大，不便以电子邮件发送时，选择 Syslog 更为可取。

Syslog 功能是一个开或关选项。如果打开 Syslog，会将所有“严重”事件发送到 Syslog 服务器。

启用 Syslog 功能

- 1 如果为 Windows，请转至 \SymantecDLP\Protect\config 目录；如果为 Linux，请转至 /opt/SymantecDLP/Protect/config 目录。
- 2 打开 Manager.properties 文件。
- 3 通过删除 #systemevent.syslog.host= 行首的 # 符号取消注释该行，然后输入 Syslog 服务器的主机名或 IP 地址。
- 4 通过删除 #systemevent.syslog.port= 行首的 # 符号取消注释该行。输入应接受 Enforce Server 服务器连接的端口号。默认值为 514。
- 5 通过删除 #systemevent.syslog.format= [{0}] {1} - {2} 行首的 # 符号取消注释该行。然后定义要发送至 syslog 服务器的系统事件消息格式：

如果取消注释该行且未做任何更改，将按以下格式发送通知消息：[服务器名称] 摘要 - 详细信息。格式变量为：

- {0} - 发生事件的服务器的名称
- {1} - 事件摘要
- {2} - 事件详细信息

例如，以下配置指定将“严重”系统事件通知发送到名为 server1 的 syslog 主机，该主机使用端口 600。

```
systemevent.syslog.host=server1
systemevent.syslog.port=600
systemevent.syslog.format= [{0}] {1} - {2}
```

在此示例中，来自名为 dlp-1 的主机上的 Enforce Server 的磁盘空间不足事件通知如下所示：

```
dlp-1 Low disk space - Hard disk space for
incident data storage server is low. Disk usage is over 82%.
```

注意：请确保取消注释 `#systemevent.syslog.format= [{0}] {1} - {2}` 行。请勿取消注释 `#systemevent.jmx.format= [{0}] {1} - {2}` 行。`jmx` 选项与 Syslog 服务器不兼容。

请参见第 125 页的“[关于系统事件](#)”。

关于系统警报

系统警报是发生特定的系统事件时发送到指定地址的电子邮件。您可以定义您希望用于安装的警报（如果有）。在“配置警报”屏幕上指定和编辑警报，可通过“系统”>“服务器”>“警报”>“添加警报”来访问该屏幕。

可以根据事件严重性、服务器名称、事件代码或这些因素的组合指定警报。可以发送任何系统事件的警报。

由警报生成的电子邮件的主题行以“Symantec Data Loss Prevention 系统警报”开头，后面跟着简短的事件摘要。电子邮件的正文包含的信息与“事件详细信息”屏幕显示的信息相同，以提供有关事件的完整信息。

请参见第 135 页的“[配置 Enforce Server 以发送电子邮件警报](#)”。

请参见第 136 页的“[配置系统警报](#)”。

请参见第 129 页的“[服务器事件详细信息](#)”。

配置 Enforce Server 以发送电子邮件警报

要发送有关指定系统事件的电子邮件警报，必须将 Enforce Server 配置为支持发送警报和报告。本部分介绍如何指定报告格式以及如何配置 Symantec Data Loss Prevention 来与 SMTP 服务器进行通信。

完成此处所述的配置之后，您便可以调度特定报告的发送，并创建特定系统警报。

配置 Symantec Data Loss Prevention 发送警报和报告

1 转至“系统”>“设置”>“常规”，然后单击“配置”。

将显示“编辑常规设置”屏幕。

2 在“报告和警报”部分中，选择下列分发方法之一：

- “将报告作为链接发送，需要登录才能查看”。Symantec Data Loss Prevention 发送带有指向报告的链接的电子邮件。您必须登录 Enforce Server 才能查看报告。

注意：如果设置了此选项，则不能分发带有事件数据的报告。

- “通过电子邮件发送报告数据”。Symantec Data Loss Prevention 发送电子邮件并附加报告数据。
- 3 在“完全限定的管理器名称”字段中输入 Enforce Server 域名或 IP 地址。
如果将报告作为链接发送，Symantec Data Loss Prevention 会在报告电子邮件中使用域名作为 URL 的基础。
请勿指定端口号，除非您已经将 Enforce Server 修改为在默认端口 443 以外的端口上运行。
- 4 如果希望警报收件人看到任何相关事件，请选中“启用关联”框。
启用关联后，用户可以在“事件快照”屏幕中看到它们。
- 5 在**SMTP**部分中，标识用于发送警报和报告的 SMTP 服务器。
在以下字段中输入相关信息：
- 服务器：Symantec Data Loss Prevention 用来传送系统事件和调度报告的 SMTP 服务器的完全限定主机名或 IP 地址。
 - 系统电子邮件：警报发件人的电子邮件地址。Symantec Data Loss Prevention 可将该电子邮件地址指定为所有传出电子邮件的发件人。您的 IT 部门可能要求系统电子邮件为 SMTP 服务器上的有效电子邮件地址。
 - 用户 ID：如果 SMTP 服务器要求用户 ID，请键入有效的用户名以访问该服务器。例如，输入 DOMAIN\bsmith。
 - 密码：如果 SMTP 服务器要求密码，请输入用户 ID 对应的密码。
- 6 单击“保存”。
- 请参见第 135 页的“[关于系统警报](#)”。
- 请参见第 136 页的“[配置系统警报](#)”。
- 请参见第 125 页的“[关于系统事件](#)”。

配置系统警报

您可以配置 Symantec Data Loss Prevention，使其在检测到指定的系统事件时发送电子邮件警报。可以根据事件严重性、服务器名称、事件代码或这些因素的组合指定警报。可以发送任何系统事件的警报。

请参见第 135 页的“[关于系统警报](#)”。

请注意，必须首先对 Enforce Server 进行配置，然后才能发送警报和报告。

请参见第 135 页的“[配置 Enforce Server 以发送电子邮件警报](#)”。

通过选择“系统”>“服务器”>“警报”，然后选择“添加警报”创建新警报，或者单击现有警报的名称对其进行修改，可以在“配置警报”屏幕上指定和编辑警报。

创建或修改警报

- 1 转至“警报”屏幕（“系统”>“服务器”>“警报”）。
- 2 单击“添加警报”选项卡创建新警报，或单击某个警报的名称对其进行修改。将显示“配置警报”屏幕。
- 3 填写（或修改）警报的名称。警报名称显示在警报电子邮件的主题行中。
- 4 填写（或修改）警报的说明。
- 5 单击“添加条件”指定触发警报的条件。

每次单击“添加条件”，您都能添加一个条件。如果您指定多个条件，则只有满足其中的每个条件才能触发警报。

单击条件旁边的红色 X 可将其从现有警报中删除。
- 6 输入将警报发送到的电子邮件地址。以逗号分隔多个地址。
- 7 在“每小时的最大数”框中输入一个数字，限制此警报在一小时内可以发送的最大次数。

如果没有在此框中输入数字，则此警报的发送次数没有限制。建议的做法是将警报次数限制为每小时一到两次，以后可根据需要替换成更大的数字。如果您指定的数字较大或者根本没有指定数字，则接受者的邮箱可能因持续收到警报而处于超负荷状态。
- 8 单击“保存”完成操作。

将显示警报列表。

您可以指定三种类型的条件来触发警报：

- 事件类型 - 事件的严重性。
- 服务器 - 与事件相关的服务器。
- 事件代码 - 标识某一特定种类的事件的代码编号。

对于每种条件，您都可以选择以下两个运算符之一：

- 为任一。
- 都不是。

对于每种条件，您都可以指定相应的参数：

- 事件类型。您可以选择“信息”、“警告”和“严重”中的一个或任意组合。单击事件类型即可指定。要指定多个类型，请在单击各个事件类型的同时按住 Ctrl 键。您可以指定一种、两种或全部三种类型。
- 服务器。您可以从可用服务器列表中选择一个或多个服务器。单击服务器的名称即可指定它。要指定多个服务器，请在单击各个服务器名称的同时按住 Ctrl 键。您可根据需要指定多个不同的服务器。
- 事件代码。输入代码编号。要输入多个代码编号，请使用逗号进行分隔或使用回车键在每个单独的行中输入一个代码。
[请参见第 138 页的“系统事件代码和消息”。](#)

通过组合多个条件，您可以定义涵盖各种系统条件的警报。

注意：如果您定义了多个条件，则将这些条件视为使用布尔运算符 AND 进行连接。这意味着只有在所有条件都满足的情况下 Enforce Server 才会发送警报。例如，如果您定义了一个事件类型条件和一个服务器条件，则只有在指定的服务器上发生指定的事件时 Enforce Server 才会发送警报。

[请参见第 135 页的“关于系统警报”。](#)

[请参见第 135 页的“配置 Enforce Server 以发送电子邮件警报”。](#)

[请参见第 126 页的“系统事件报告”。](#)

关于日志查看

Symantec Data Loss Prevention 的安装会包括多个日志文件。这些文件提供了有关服务器通信、Enforce Server 和检测服务器操作、事件检测等的信息。

默认情况下，Enforce Server 和检测服务器的日志会存储在以下目录中：

- Windows: \Protect\logs
- Linux: /var/log/Vontu

[请参见第 233 页的“关于日志文件”。](#)

另请参见《Symantec Data Loss Prevention 系统维护指南》以获取关于使用日志的其他信息。

系统事件代码和消息

Symantec Data Loss Prevention 系统事件会被监控、报告和记录。每个不同的事件均由下表列出的代码编号加以标识。

[请参见第 125 页的“关于系统事件”。](#)

可通过事件代码对系统事件列表和报告进行过滤。

请参见第 126 页的“[系统事件报告](#)”。

请注意，大括号括起的数字（例如 {0}）表示实际消息中插入的相应文本字符串。

代码	名称	说明
1000	已启动监视器	已启动所有监控进程。
1001	已启动本地监视器	已启动所有监控进程。
1002	已启动监视器	一些监控进程被禁用，尚未启动。
1003	已启动本地监视器	一些监控进程被禁用，尚未启动。
1004	已停止监视器	已停止所有监控进程。
1005	已停止本地监视器	已停止所有监控进程。
1006	{0} 未能启动	无法启动进程{0}。有关详细信息，请参见日志文件。
1007	{0} 重新启动次数过多	在最近的{2}分钟内，进程{0}已重新启动{1}次。
1008	{0} 已关闭	{0} 进程在完全启动之前关闭。
1010	已重新启动 {0}	由于{0}进程意外关闭，已将其重新启动。
1011	已重新启动 {0}	由于{0}没有响应，已将其重新启动。
1012	无法启动 {0}	无法绑定到关闭数据报套接字。将重试。
1013	{0} 已继续启动	已成功绑定到关闭套接字。
1014	磁盘空间不足	硬盘空间不足。Symantec Data Loss Prevention Server 磁盘使用率超过{0}%。
1100	已启动聚合器	
1101	聚合器未能启动	启动聚合器时出错。{0}不会检测到任何事件。
1200	已加载策略 “{0}”	已成功加载策略 “{0}” v{1} ({2})。
1201	已加载策略 {0}	

代码	名称	说明
1202	未加载策略	未找到任何相关策略。不会检测到任何事件。
1203	已卸载策略 “{0}”	已卸载策略 “{0}”。
1204	已更新策略 “{0}”	已成功更新策略 “{0}”。当前策略版本是 {1}。活动通道: {2}。
1205	已达到策略 “{0}” 的事件限制	策略 “{0}” 已在过去的 {2} 小时内在 {1} 封以上的邮件中找到事件。在更改策略之前，或达到 {2} 个小时的重置期之前，不会强制实施策略。
1206	消息等待时间过长	消息等待时间为 {0}:{1}:{2}:{3}。
1301	已启动文件读取器	
1302	文件读取器未能启动	启动文件读取器时出错。{0}不会检测到任何事件。
1303	无法删除文件夹	文件读取器无法删除文件系统中的文件夹 “{0}”。请进行调查，因为这将导致系统故障。
1304	已启用通道	已启用监控通道 “{0}”。
1305	已禁用通道	已禁用监控通道 “{0}”。
1306	已收到许可证。	{0}。
1400	已配置 ICAP 通道	此通道处于 {0} 模式。
1401	无效的许可证	ICAP通道未获得许可或许可证已过期。ICAP通道将不会检测到或阻止任何事件。
1402	内容删除不正确	第 {0} 行中的配置规则已过期或未以适当的语法格式编写。请将其从配置文件删除，或更新该规则。
1403	处理邮件时发生内存不足错误 (Web Prevent)	处理连接 ID={0} 上的请求时，发生内存不足错误。请调整流量负载设置。
1404	主机限制	任何主机 (ICAP 客户端) 都可以连接到 Web Prevent。

代码	名称	说明
1405	主机限制错误	无法获取主机 {0} 的 IP 地址
1406	主机限制错误	无法获取 Icap.AllowHosts 中任何主机的 IP 地址
1407	已启用协议跟踪	在 {0} 上跟踪可用 1408 无效的负载平衡系数 Icap.LoadBalanceFactor 已配置为 0。请将其视为 1。
1500	无效的许可证	SMTP Prevent 通道未获得许可或许可证已过期。SMTP Prevent 通道将不会检测到或阻止任何事件。
1501	绑定地址错误	无法绑定 {0}。有关详细信息，请检查配置的地址或查看 RequestProcessor 日志。
1502	MTA 限制错误	无法解析主机 {0}。
1503	已限制所有 MTA	客户端 MTA 受限制，但不会解析任何主机。请查看 RequestProcessor 日志获取详细信息并更正此 Prevent Server 的 RequestProcessor.AllowHosts 设置。
1600	无效的覆盖文件夹	监控通道 {0} 包含无效的源文件夹: {1}。使用文件夹: {2}。
1601	无效的源文件夹	监控通道 {0} 包含无效的源文件夹: {1}。已禁用此通道。
1700	扫描启动失败	不存在 ID 为 {0} 的发现目标。
1701	已经终止扫描 {0}	已经终止扫描 {0}
1702	已完成扫描	发现目标 “{0}” 成功完成扫描。
1703	扫描启动失败	{0}
1704	共享列表存在错误	{0}
1705	调度扫描失败	不能启动对发现目标 {0} 的调度扫描。{1}
1706	扫描挂起失败	{0}
1707	继续扫描失败	{0}

代码	名称	说明
1708	调度扫描挂起失败	扫描发现目标{0}时调度挂起失败。 {1}
1709	继续调度扫描失败	扫描发现目标{0}时调度挂起失败。 {1}
1800	Incident Persister 无法处理事件	Incident Persister 处理事件 {0} 时内存不足。
1801	Incident Persister 无法处理事件 {0}	
1802	接收到损坏的事件	接收到损坏的事件并将其重命名为{0}。
1803	策略配置错误	策略 “{0}” 没有关联的严重性。
1804	Incident Persister 无法启动	Incident Persister 无法启动，因为它不能访问事件文件夹{0}。请检查文件夹权限。
1805	Incident Persister 无法访问事件文件夹	Incident Persister 无法访问事件文件夹 {0}。请检查文件夹权限。
1806	响应规则处理无法启动	响应规则处理无法启动: {0}。
1807	响应规则处理执行失败	响应规则命令运行时执行失败，出现错误: {0}。
1808	无法写入事件	不能删除旧临时文件 {0}。
1809	无法写入事件	不能重命名临时事件文件 {0}。
1810	无法列出事件	不能列出文件夹{0}中的事件文件。请检查文件夹权限。
1811	发送事件时出错	发送事件时发生意外错误。{0}有关更多信息，请查看事件写入器日志。
1812	事件写入器已停止	发送事件文件{0}后不能将其删除。请手动删除此文件，更正问题并重新启动事件写入器。
1813	不能列出事件	不能列出文件夹{0}中的事件文件。请检查文件夹权限。
1814	事件队列已积存	此服务器的队列中包含{0}个事件。

代码	名称	说明
1815	事件服务器上的磁盘空间不足	事件数据存储服务器的硬盘空间不足。磁盘使用率超过 {0}%。
1900	不能加载更新软件包	加载软件更新软件包 {0} 时发生数据库连接错误。
1901	软件更新已失败	不能应用软件包 {0} 中的软件更新。请检查更新服务日志。
2000	密钥启动错误	不能使用新的启动密码启动密钥。将禁用确切数据配置文件。
2001	无法更新密钥启动密码。	密钥启动密码将不更新，因为加密密钥未启动。将禁用确切数据匹配。
2100	管理员已保存	管理员设置已成功保存。
2101	数据源已删除	ID 为 {0} 的数据源已由 {1} 删除。
2102	数据源已保存	{0} 数据源已由 {1} 保存。
2103	文档源已删除	ID 为 {0} 的文档源已由 {1} 删除。
2104	文档源已保存	{0} 文档源已由 {1} 保存。
2105	新协议已创建	新协议 {0} 已由 {1} 创建。
2106	协议顺序已更改	协议 {0} 已由 {2} 移动了 {1}。
2107	协议已删除	协议 {0} 已由 {1} 删除。
2108	协议已保存	协议 {0} 已由 {1} 编辑。
2109	用户已删除	ID 为 {0} 的用户已由 {1} 删除。
2110	用户已保存	用户 {0} 已由 {1} 保存。
2111	检测到失控查询	一个属性查找插件未正常完成并在系统中留下一个正在运行的线程。清理此线程可能需要重新启动管理器。
2112	已加载自定义属性查找插件	已加载以下自定义属性查找插件: {0}。
2113	未加载自定义属性查找插件	未找到自定义属性查找插件。
2114	自定义属性查找失败	查找插件 {0} 超时。已将其卸载。

代码	名称	说明
2115	自定义属性查找失败	不能实例化查找插件{0}。已将其卸载。错误消息: {1}
2116	策略已更改	{0} 策略已由 {1} 更改。
2117	策略已删除	{0} 策略已由 {1} 删除。
2118	警报或调度报告发送失败。{0}	由 {1} 配置的 {0} 包括以下不能接收邮件的电子邮件地址: {2}。不是地址错误，就是您的电子邮件服务器不允许传送到该地址。
2119	系统设置已更改	系统设置已由 {0} 更改。
2120	端点位置设置已更改	端点位置设置已由 {0} 更改。
2121	帐户 “{1}” 已锁定	帐户 “{1}” 的连续登录失败次数已超过允许的最大值{0}，因此该帐户已锁定。
2122	已加载 FlexResponse 操作	已加载以下 FlexResponse 操作: {0}。
2123	未加载 FlexResponse 操作。	未找到 FlexResponse 操作。
2124	检测到失控 FlexResponse 操作。	一个 FlexResponse 插件未正常完成并在系统中留下一个正在运行的线程。清理此线程可能需要重新启动管理器。
2200	已接受最终用户授权许可协议	Symantec Data Loss Prevention 最终用户授权许可协议已由 {0}、{1}、{2} 接受。
2201	许可证无效	
2202	许可证已过期	您的一个或多个产品许可证已过期。某些系统功能可能已禁用。请在“系统设置”页面上查看许可证状态。
2203	许可证即将到期	您的一个或多个产品许可证即将到期。请在“系统设置”页面上查看许可证状态。
2204	无许可证	许可证不存在、已过期或无效。不会检测到任何事件。

代码	名称	说明
2205	密钥已启动	已通过管理员登录启动了加密密钥。
2206	密钥启动失败	不能手动启动加密密钥。有关更多信息，请查看 Enforce Server 日志。将无法创建新的确切数据配置文件。
2207	自动密钥启动	加密密钥已自动启动。
2208	需要手动启动密钥	未配置自动启动加密密钥。需要管理员登录才可以启动加密密钥。管理员登录前，无法创建任何新的确切数据配置文件。
2300	磁盘空间不足	硬盘空间不足。Symantec Data Loss Prevention Enforce Server 磁盘使用率超过 {0}%。
2301	表空间几乎已满	Oracle 表空间 {0} 满载程度超过 {1}%。
2302	{0} 没有响应	检测服务器 {0} 至少有 20 分钟未更新其心跳。
2303	监视器配置已更改	{0} 监视器配置已由 {1} 更改。
2304	系统更新已上传	影响以下组件的系统更新已上传: {0}。
2305	无法访问 SMTP 服务器。	无法访问 SMTP 服务器。不能发送警报或调度报告。
2306	Enforce Server 已启动	Enforce Server 已启动。
2307	Enforce Server 已停止	Enforce Server 已停止。
2308	监视器状态更新程序异常	监视器状态更新程序发生一般性异常。有关更多信息，请查看 Enforce Server 日志。
2309	系统统计信息更新失败	无法更新 Enforce Server 磁盘使用率和数据库使用统计信息。有关更多信息，请查看 Enforce Server 日志。

代码	名称	说明
2310	统计信息聚合失败	统计信息汇总任务发生一般性异常。有关更多信息，请参阅 Enforce Server 日志。
2311	版本不匹配	Enforce 版本为 {0}，但此监视器的版本为 {1}。
2312	事件删除失败	事件删除失败。
2313	事件删除已完成	为 {0} 运行事件删除，并删除了 {1} 个事件。
2314	端点数据删除失败	端点数据删除失败。
2400	导出 Web 存档已完成	用户 {1} 的存档 “{0}” 已成功创建。
2401	导出 Web 存档已取消	用户 {1} 的存档 “{0}” 已取消。
2402	导出 Web 存档失败	不能为用户 {1} 创建存档 “{0}”。指定的报告包含的事件超过 {2} 个。
2403	导出 Web 存档失败	不能为用户 {1} 创建存档 “{0}”。在事件 {2} 处失败。
2404	无法运行调度报告	调度报告作业 {0} 无效并已删除。
2405	无法运行调度报告	{1} 拥有的调度报告 {0} 发生错误：{2}。
2406	报告调度已禁用	不能运行 {1} 拥有的调度报告 {0}，因为报告调度已禁用。
2407	报告调度已禁用	因为报告调度禁用，调度的报告不可能运行。
2408	无法运行调度报告	传递调度报告 {0}{1} 时无法连接到邮件服务器。
2409	无法运行调度报告	用户 {0} 不再属于调度报告 {2} 所属的角色 {1}。日程表已删除。
2410	无法运行调度报告	无法为用户 {1} 运行调度报告 {0}，因为该帐户当前已锁定。
2411	调度报告已发送	{1} 拥有的调度报告 {0} 已成功发送。

代码	名称	说明
2412		用户 [{0}] 导出 XML 报告时失败 用户 [{0}] 导出 XML 报告时失败
2420	无法运行调度数据所有者报告分发	无法按数据所有者分发报告 {0} (id={1})，因为已禁止发送报告数据
2421	按数据所有者的报告分发失败	按报告 {0} (id={1}) 的数据所有者进行报告分发失败
2422	按数据所有者的报告分发已完成	按报告 {0} (id={1}) 的数据所有者进行报告分发完成，产生针对 {3} 个数据所有者的 {2} 个事件。无法导出 {5} 个数据所有者的 {4} 个事件。
2423	给数据所有者的报告分发被截断	数据所有者 “{0}” 的报告分发 {1} (id={2}) 超过允许的大小上限。仅将前 {3} 个事件发送到 “{0}”。
2500	处理消息时发生意外错误	{0} 在处理消息时发生意外错误。有关详细信息，请参见日志文件。
2501	内存限制机制已禁用	内存限制需要使用 {0} x {1} 字节。仅有 {2} 字节可用。内存限制机制已禁用。
2600	通信错误	将 {1} 个更新发送到 {0} 时发生意外错误。{2} 有关更多信息，请查看监视控制器日志。
2700	监视控制器已启动	监视控制器服务已启动。
2701	监视控制器已停止	监视控制器服务已停止。
2702	更新已传输至 {0}	已成功将更新软件包 {1} 传输到检测服务器 {0}。
2703	更新传输完成	已成功将更新软件包 {0} 传输到所有检测服务器。
2704	更新 {0} 失败	不能将更新软件包传输到检测服务器 {0}。
2800	为数据包捕获配置的缓冲目录错误	数据包捕获已配置了缓冲目录:{0}。此目录不具有写入权限。请查看目录权限和监视器配置文件。然后重新启动监视器。
2801	不能发送 NIC 列表。 {0}	

代码	名称	说明
2900	EDM 配置文件搜索失败 {0}	
2901	密钥未启动	启动加密密钥前将禁用确切数据匹配。
2902	无法访问索引文件夹	不能列出索引文件夹 {0} 中的文件。请检查配置和文件夹权限。
2903	已创建索引文件夹	在配置中指定的本地索引文件夹 {0} 已不存在。它已创建。
2904	无效索引文件夹	在配置中指定的索引文件夹 {0} 不存在。
2905	{0} {1} 确切数据配置文件未创建。	
2906	已取消编制索引	数据库配置文件 {0} 的创建已取消。
2907	复制已取消	已取消将数据库配置文件 {0} 复制到服务器 {1}。
2908	复制失败	将数据库配置文件 {0} 复制到服务器 {1} 时，与数据库的连接断开。
2909	复制失败	将数据库配置文件 {0} 复制到服务器 {1} 时，发生数据库错误。
2910	不能删除索引文件	不能删除数据库配置文件 {0} 的索引文件 {1}。
2911	不能删除索引文件	不能删除数据库配置文件 {0} 的索引文件 {1}。
2912	不能删除孤立文件	不能删除孤立数据库配置文件索引文件 {0}。
2913	复制失败	将数据库配置文件 {0} 复制到服务器 {2} 时失败。{1} 有关更多详细信息，请查看监视控制器日志。
2914	复制已完成	已完成将数据库配置文件 {0} 复制到服务器 {2}。文件 {1} 传输成功。
2915	复制已完成	已完成将数据库配置文件 {0} 复制到服务器 {2}。文件 {1} 传输成功。 2916 数据库配置文件已删除 数据库配置文件 {0} 已删除。文件 {1} 删除成功。

代码	名称	说明
2917	数据库配置文件已删除	数据库配置文件 {0} 已删除。文件 {1} 删除成功。
2918	已加载数据库配置文件	已加载数据库配置文件 {0}(从 {1})。
2919	已卸载数据库配置文件	已卸载数据库配置文件 {0}。
2920	不能加载数据库配置文件 {1}	针对数据库配置文件 {0} 将不会检测到任何事件。
2921	不能卸载数据库配置文件 {1}	如果不重新启动监视器，将来可能无法重新加载数据库配置文件 {0}。
2922	找不到注册的内容	编制索引期间，在数据库中找不到 ID 为 {0} 的注册的内容。
2923	数据库错误	编制索引期间发生数据库错误。{0}
2924	在编制索引期间，进程关闭	在编制索引期间，进程已关闭。某些注册的内容可能未创建。
2925	策略不准确	策略 “{0}” 包含一个或多个对 {1} 的检测准确性不令人满意的规则。{2}
2926	已创建确切数据配置文件	已从文件 “{1}” 中创建了 {0}。处理的行数: {2} 无效行数: {3} 现在，确切数据配置文件将被复制到所有 Symantec Data Loss Prevention 服务器。
3000	{0} {1}	文档配置文件未创建。
3001	已取消编制索引	已取消创建文档配置文件 {0}。
3002	复制已取消	已取消将文档配置文件 {0} 复制到服务器 {1}。
3003	复制失败	将文档配置文件 {0} 复制到服务器 {1} 时，与数据库的连接断开。
3004	复制失败	将文档配置文件 {0} 复制到服务器 {1} 时，发生数据库错误。
3005	不能删除索引文件	不能删除文档配置文件 {0} 的索引文件 {1}。
3006	不能删除索引文件	不能删除文档配置文件 {0} 的索引文件 {1}。

代码	名称	说明
3007	不能删除孤立文件 {0}	
3008	复制失败	将文档配置文件 {0} 复制到服务器 {2} 时失败。{1} 有关更多详细信息，请查看监视控制器日志。
3009	复制已完成	已完成将文档配置文件 {0} 复制到服务器 {2}。文件 {1} 传输成功。
3010	复制已完成	

添加新的产品模块

本章节包括下列主题：

- [安装新的许可证文件](#)
- [关于系统升级](#)

安装新的许可证文件

首次购买 Symantec Data Loss Prevention 后，升级至更高版本或者购买附加产品模块时，必须安装一个或多个 Symantec Data Loss Prevention 许可证文件。许可证文件名称的格式为 *name.slf*。

您也可以先输入某个模块的许可证文件启动该产品，稍后再输入其他模块的许可证文件。

有关首次购买 Symantec Data Loss Prevention 后安装许可证文件的详细信息，请参见适用于您的操作系统的《Symantec Data Loss Prevention 安装指南》。

安装许可证：

1 下载新的许可证文件。

有关下载并解压缩许可证文件的信息，请参见 Symantec FileConnect 站点上提供的文档 *Acquiring Symantec Data Loss Prevention Software* (《获取 Symantec Data Loss Prevention 软件》)。

2 转至“系统”>“设置”>“常规”，然后单击“配置”。

3 在“编辑常规设置”屏幕上，向下滚至“许可证”部分。

- 4 在“安装许可证”字段中，浏览到您下载的新 Symantec Data Loss Prevention 许可证文件，然后单击“保存”，同意该软件的最终用户授权许可协议(EULA) 中的条款和条件，然后安装许可证。

注意：如果您不同意 EULA 中的条款和条件，则无法安装该软件。

- 5 要启用新产品许可证相关功能的全部功能，请重新启动 Vontu Manager 服务。

请参见第 69 页的“[关于 Enforce Server 服务](#)”。

“当前许可证”列表显示每个产品许可证的下列信息：

- 产品 - 单个 Symantec Data Loss Prevention 产品名称
- 数量 - 授权使用各产品的用户数量
- 状态 - 产品的当前状态
- 有效期限 - 产品的许可证过期日期

在许可证过期的前一个月，“系统”>“服务器”>“概述”屏幕上将会显示警告消息。当看到有关许可证过期的消息时，请在当前许可证过期之前与 Symantec 联系以购买新的许可证密钥。

关于系统升级

“系统概述”屏幕上的“升级”按钮可以启动将系统加载并升级到新版本的 Symantec Data Loss Prevention 的操作。

有关升级 Symantec Data Loss Prevention 软件的信息，请参见《Symantec Data Loss Prevention 升级指南》。

请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。

集成 Enforce 与 Symantec Protection Center (SPC)

本章节包括下列主题：

- [关于 Symantec Protection Center \(SPC\)](#)
- [关于 Enforce Server 与 SPC 集成](#)
- [Enforce Server 与 SPC 集成的注意事项和要求](#)
- [将 Enforce Server 与 SPC 集成](#)

关于 Symantec Protection Center (SPC)

Symantec Protection Center (SPC) 是一个公共用户界面，使您可以在一个 Web 控制台上集中 Symantec 和第三方安全产品的数据和管理。通过允许同时查看安全性的许多方面，此合并增加了企业系统安全状态的可见度。

使用 SPC，您可以：

- 查看报告。
- 查看通知。
- 执行补救任务。
- 配置 SPC 设置。
- 管理集成产品。

SPC 利用 Symantec Global Intelligence Network (GIN) 向客户提供企业系统安全方面的实时反馈，提供已检测的漏洞、客户网络内的已知威胁和客户网络的恶意流量流出的信息。SPC 还提供安全风险的智能优先排序，使客户可以区分风险解决方案（通过与修补系统和票证系统集成或更改安全产品中的配置设置）的优先次序。

请参见第 154 页的“[关于 Enforce Server 与 SPC 集成](#)”。

请参见第 154 页的“[Enforce Server 与 SPC 集成的注意事项和要求](#)”。

请参见第 155 页的“[将 Enforce Server 与 SPC 集成](#)”。

关于 Enforce Server 与 SPC 集成

通过将 Symantec Data Loss Prevention 与 Symantec Protection Center (SPC) 集成，可以从 SPC 界面内管理 Data Loss Prevention 服务器、管理策略以及补救事件。如果具有与 SPC 集成的其他 Symantec 产品，则该单一控制台特别有用。例如，如果您还使用 Symantec Messaging Gateway，则可以将它和 Data Loss Prevention 同时与 SPC 集成。这样，您可以一次登录两个产品（单一登录），并从同一 SPC 界面监视和管理两个产品配置。

此外，还可以将不属于 Symantec 的安全相关产品与 SPC 集成。有关此用途，请参考 SPC 文档。

注意：将 Enforce Server 与 SPC 集成不会影响 Symantec Data Loss Prevention 的操作。如果愿意，您仍可以从 Enforce Server 管理控制台的独立实例访问和使用 Data Loss Prevention。

请参见第 154 页的“[Enforce Server 与 SPC 集成的注意事项和要求](#)”。

请参见第 155 页的“[将 Enforce Server 与 SPC 集成](#)”。

Enforce Server 与 SPC 集成的注意事项和要求

在将 Enforce Server 与 SPC 集成之前，请谨记以下注意事项：

- Symantec Data Loss Prevention 11.1 版与 SPC 仅在界面层集成。不能通过 SPC 进行 Symantec Data Loss Prevention 的报告集成。
- Symantec Data Loss Prevention 与 SPC 集成不兼容其证书身份验证安装模式。如果已安装或启用证书身份验证模式的 Symantec Data Loss Prevention，并想要将 Enforce Server 与 SPC 集成，则：
 - 禁用 Enforce Server 的证书身份验证模式。
 - 将 Enforce Server 与 SPC 集成。
请参见第 155 页的“[将 Enforce Server 与 SPC 集成](#)”。
 - 续订 Enforce Server 的证书身份验证模式。
- 默认情况下，启用 Enforce Server 与 SPC 集成功能。
可以通过更改 `\Protect\configManager.properties` 文件中的 SPC 身份验证设置来禁用此功能。

在将 Enforce Server 与 SPC 集成之前，请遵循以下要求：

- 将 SPC 设备主机和所有要与 SPC 集成的 Enforce Server 主机的系统时钟同步到同一分钟内。
- 确保可以从安装 Enforce Server 的主机 ping 通 SPC 主机，反之亦然。
- 创建一个授予“Symantec Protection Center 注册”权限的专用 Data Loss Prevention 角色和用户。

此权限允许用户指示 Enforce Server 信任某个证书。这是一个重要权限，只有在 SPC 中注册和注销 Enforce Server 时才有必要使用。建议在 SPC 中注册完 Enforce Server 后取消此权限。至少，应限制添加到此专用角色和授予此权限的用户的数量。请注意，“Symantec Protection Center 注册”权限本身不会允许用户登录到 Enforce Server。
- 要授予 Data Loss Prevention 用户通过 SPC 访问 Enforce Server 的权限，必须将 Data Loss Prevention 用户映射到 SPC。

为简化用户访问，建议您在 SPC 中创建与 Enforce Server 中对应的用户帐户具有相同名称和密码的用户。

请参见第 155 页的“[将 Enforce Server 与 SPC 集成](#)”。

将 Enforce Server 与 SPC 集成

以下步骤假定已安装 Symantec Protection Center (SPC)。如果未安装 SPC 实例，请参考 *Symantec Protection Center Getting Started Guide*（《Symantec Protection Center 入门指南》），可在以下网站获取此书：

<http://www.symantec.com/business/protection-center> 获取并安装 SPC。

有两种方法可用于集成 Enforce Server 与 SPC：

- 通过将单个已知 Enforce Server 实例添加到 SPC。

请参见第 156 页的[表 10-1](#)。
- 通过发现一个或多个 Enforce Server 实例并将其注册到 SPC。

请参见第 159 页的[表 10-2](#)。

完成下列步骤可将单个已知 Enforce Server 实例与 SPC 集成。

表 10-1

将单个已知 Enforce Server 实例添加到 SPC

步骤	操作	说明
步骤 1	创建一个具有 SPC 权限的专用 Data Loss Prevention 角色和用户。	<p>要向 SPC 添加或注册 Enforce Server 管理控制台，必须首先将 SPC 注册权限授予 Data Loss Prevention 角色，再将用户分配给该角色。我们建议您创建一个专用角色和用户，专门用于集成 Enforce Server 和 SPC。</p> <p>创建一个专用角色用于集成 Enforce Server 和 SPC：</p> <ul style="list-style-type: none"> ■ 以具有“用户管理”权限的用户的身份登录到 Enforce Server 管理控制台。 ■ 创建一个新角色。 请参见第 85 页的“配置角色”。 ■ 为此角色授予“Symantec Protection Center 注册”权限。 无需为此角色授予其他任何权限。 ■ 创建一个新用户帐户。 请参见第 91 页的“配置用户帐户”。 ■ 将新用户添加到新创建的角色。 <p>注意：Symantec Protection Center 注册权限不允许用户登录到 Enforce Server。</p>

步骤	操作	说明
步骤 2	在 SPC 中添加并启用 Symantec Data Loss Prevention 产品。	<p>将 Data Loss Prevention 产品添加到 SPC:</p> <ul style="list-style-type: none">■ 以具有 SPC 管理员凭据的用户的身份登录到 SPC 设备。■ 选择“管理”选项卡。■ 单击“添加产品”。■ 在“添加并启用产品实例”屏幕中，输入以下信息：<ul style="list-style-type: none">■ 产品 从下拉菜单中，选择 Symantec Data Loss Prevention。■ 主机名或 IP 地址 输入装有 Enforce Server 管理控制台的系统的主机名或 IP 地址。■ 产品用户名 输入在步骤 1 中创建的且授予其 Symantec Protection Center 权限的用户的名称。■ 密码 输入此用户的密码。■ 单击“启用”。 系统会指示是否已成功启用。■ 单击“完成”。
步骤 3	验证 Symantec Data Loss Prevention 是否已添加到 SPC 并启用。	验证 Data Loss Prevention 是否已添加到 SPC: <ul style="list-style-type: none">■ 在 SPC 控制台中，导航至“管理”>“支持的产品”屏幕。■ 在“启用支持的产品”选项卡中，确认已列出 Symantec Data Loss Prevention 11.1.0.0 并显示已添加的 Enforce Server 主机的主机名或 IP 地址。

步骤	操作	说明
步骤 4	为 SPC 用户提供访问 Symantec Data Loss Prevention 的权限。	<p>Enforce Server 与 SPC 集成后，需要将每个 Data Loss Prevention 用户都映射到 SPC，以便每个用户都能通过 SPC 访问 Enforce Server 管理控制台。为 Data Loss Prevention 用户提供通过 SPC 访问 Enforce Server 的权限：</p> <ul style="list-style-type: none"> ■ 在 SPC 控制台中，选择“管理”>“用户管理”。 ■ 单击“新建”添加新用户。 ■ 选择“已经过本地身份验证的帐户”选项。 注意：有关利用 LDAP 同步功能创建多个用户帐户的详细信息，请参考 SPC 文档。 ■ 输入“用户名”和“密码”，可以是用户的实际名称和电子邮件地址。 ■ 单击“下一步”。 ■ 在“防护中心权限”屏幕中，单击“下一步”。这些权限是特定于 SPC 的。映射 Data Loss Prevention 用户后，无需再为这些用户授予 SPC 权限。 ■ 在“授予组织访问权限”屏幕中，单击“下一步”。 ■ 在“链接到集成的产品”屏幕中： <ul style="list-style-type: none"> ■ 集成的产品 选择已添加的 Enforce Server 实例。 ■ 链接的用户名 输入要授予其 SPC 访问权限的 Data Loss Prevention 用户的名称。 ■ 单击“添加”添加新用户并进行映射。 ■ 单击“保存”。 系统会确认授予的权限。 ■ 单击“完成”。 <p>注意：可以使用单个 Enforce 用户或 Enforce 角色\Enforce 用户组合映射 SPC 用户帐户。如果使用的是仅用户方法，当用户使用 SPC 登录到 Enforce 时，会使用默认角色。如果使用的是角色\用户方法，用户将以特定角色登录到 Enforce，但无法更改其角色。执行映射时，在输入 Enforce 用户名的同时可使用以下语法将该用户锁定到特定角色：<code><enforce role>\<enforce user></code>，例如：<code>remediator\bob</code>。</p>

步骤	操作	说明
步骤 5	验证 Enforce Server 是否已与 SPC 集成。	<p>验证是否已成功集成：</p> <ul style="list-style-type: none"> ■ 注销 SPC。 ■ 以在步骤 4 中创建的用户的身份重新登录到 SPC。 ■ 在 SPC “主页” 屏幕中，选择该界面左上方的目标图标。 ■ 选择 Symantec Data Loss Prevention 选项。 ■ 选择已添加的 Enforce Server 实例的主机名或 IP 地址。 <p>在您以已创建并映射的用户的身份登录后，应显示 Data Loss Prevention 系统。</p>
步骤 6	对所有连接问题进行故障排除。	请参考 表 10-2 中的步骤 7。
步骤 7	取消 SPC 注册权限。	<p>成功将 Enforce Server 实例与 SPC 集成后，建议禁用针对 SPC 集成分配给“Symantec Protection Center 注册”角色（步骤 1）的用户帐户。完成集成后，用户无需拥有此权限。如果需要从 SPC 重新集成或取消注册 Symantec Data Loss Prevention 产品，则可以重新启用分配给 SPC 角色的用户帐户。</p> <p>请参见第 161 页的表 10-3。</p>

完成以下步骤可以发现和注册一个或多个用于与 SPC 集成的 Enforce Server 实例，并对可能遇到的任何集成问题进行故障排除。

表 10-2 发现一个或多个 Enforce Server 实例并将其注册到 SPC 以及对任何连接问题进行故障排除

步骤	操作	说明
步骤 1	将 SPC 注册权限授予 Data Loss Prevention 角色和用户。	请参考 表 10-1 中的步骤 1。

步骤	操作	说明
步骤 2	发现一个或多个 Enforce Server 实例。	<p>发现 Enforce Server 实例：</p> <ul style="list-style-type: none"> ■ 使用管理员凭据登录到 SPC 设备。 ■ 从 SPC 控制台界面中，选择“管理”>“设置”>“产品发现”。 ■ 在“搜索IP选择”字段中，输入 Enforce Server 主机的 IP 地址。 <p>要将多个 Enforce Server 实例与 SPC 集成，请输入一个逗号分隔的 IP 地址列表。</p> <ul style="list-style-type: none"> ■ 选择（选中）Symantec DLP 11.1.0.0。 ■ 单击“搜索产品”。 <p>在“搜索产品”按钮下方会显示一则消息，用于指示是否已成功发现 Enforce Server 主机。</p>
步骤 3	将一个或多个 Enforce Server 实例注册到 SPC。	<p>注册已发现的 Enforce Server 实例：</p> <ul style="list-style-type: none"> ■ 在 SPC 控制台中，选择“管理”>“产品注册”。 ■ 选择“可用的支持产品”选项卡。 ■ 对于“主机名”，选择 Enforce Server 主机的 IP 地址。 ■ 输入已授予“Symantec Protection Center 注册”角色权限（在步骤 1 中）的 Data Loss Prevention 用户的“用户名”和“密码”。 ■ 单击“启用”。 <p>在控制台的右侧，应看到一则指示 Enforce Server 实例已成功注册的消息：“已成功启用支持的产品！”</p>
步骤 4	验证是否已将一个或多个 Enforce Server 实例注册到 SPC。	请参考表 10-1 中的步骤 3。
步骤 5	为用户提供从 SPC 访问 Symantec Data Loss Prevention 的权限。	请参考表 10-1 中的步骤 4。
步骤 6	验证 Symantec Data Loss Prevention 是否已与 SPC 集成。	请参考表 10-1 中的步骤 5。

步骤	操作	说明
步骤 7	对所有连接问题进行故障排除。	<p>调试连接问题：</p> <ul style="list-style-type: none"> ■ 如果您的浏览器无法从 SPC 连接到 Enforce Server，请确保已在浏览器中加载 Enforce Server 证书。可通过访问独立且位于 SPC 之外的 Enforce Server 管理控制台来执行此操作。 ■ 从 SPC 内部映射到的 Data Loss Prevention 用户必须具有相应权限才能访问 Enforce Server 资源、构建策略等。如果可从 SPC 登录到 Enforce Server，但无法在管理控制台内部执行任何操作，请更新 Data Loss Prevention 用户权限。 ■ 如果注册失败并收到错误“已检测到时间同步错误”，请确保 SPC 主机和 Enforce Server 主机上的系统时钟能够同步到分钟。 ■ 如果已集成多个 Enforce Server 实例，请在 SPC 中，单击 Symantec Data Loss Prevention 产品标题下方的箭头，然后选择要访问的 Enforce Server 实例。
步骤 8	取消 SPC 注册权限。	请参考表 10-1 中的步骤 7。

以下步骤介绍如何从 SPC 取消注册 Enforce Server 实例。

表 10-3 从 SPC 取消注册 Enforce Server

步骤	操作	说明
步骤 1	以管理员身份登录到 SPC。	以具有 SPC 管理员凭据的用户的身份登录到 SPC 设备。
步骤 2	从 SPC 取消注册 Enforce Server 实例。	<p>从 SPC 取消注册 Enforce Server 实例：</p> <ul style="list-style-type: none"> ■ 选择“管理”>“支持的产品”。 ■ 在“启用支持的产品”选项卡中，选择要取消注册的 Enforce Server 实例。 ■ 在该屏幕的左上方，选择“禁用产品”。此选项列在“支持的产品”标题下方。 ■ 输入已授予“Symantec Protection Center 注册”权限的 Data Loss Prevention 用户的用户名和密码。 ■ 单击“禁用”。 <p>系统将显示一则消息，指示取消注册是否已成功完成。</p>

将 Symantec Data Loss Prevention 服务器迁移到 64 位操作系统

本章节包括下列主题：

- 将 Symantec Data Loss Prevention 服务器从 32 位操作系统迁移到 64 位操作系统
- 将 Enforce Server 迁移到 64 位操作系统
- 将检测服务器迁移到 64 位操作系统

将 Symantec Data Loss Prevention 服务器从 32 位操作系统迁移到 64 位操作系统

Symantec Data Loss Prevention 支持在 64 位操作系统上运行 Enforce Server 和检测服务器。有关支持的64位操作系统和服务器硬件配置的信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。本节介绍将现有的 32 位 Symantec Data Loss Prevention 服务器迁移到单独的服务器计算机或虚拟机（如果服务器支持 VM 部署）上的受支持 64 位操作系统需要执行的步骤。

开始迁移过程之前，请考虑下面这些重要的限制和要求：

- 开始迁移过程之前，Symantec Data Loss Prevention 部署的所有组件（Enforce Server、Enforce Server 数据库和所有检测服务器）必须已完全升级到最新的 Symantec Data Loss Prevention 版本。迁移过程与 Symantec Data Loss Prevention 升级过程是分开进行的，您只能迁移已经使用了最新版本的服务器。不要尝试将 32 位的 10.x 版本组件迁移到 64 位。

- 将服务器迁移到 64 位操作系统不是自动化过程。必须在兼容的 64 位操作系统上安装新的 64 位 Symantec Data Loss Prevention 服务器软件，然后重新使用、重新创建或迁移 32 位 Symantec Data Loss Prevention 服务器中的支持文件。“原地”迁移服务器是不可能的。
- 不支持跨平台迁移。对于要迁移的每个 Symantec Data Loss Prevention 服务器，64 位目标操作系统的类型（Windows 或 Linux）必须与现有 32 位操作系统的类型相同。
- 部署到 64 位操作系统后，某些 Symantec Data Loss Prevention 产品在功能上可能有限制。例如，在 64 位平台上，Network Discover 不支持 Lotus Notes 本机扫描。另外，使用本机代码的任何 FlexResponse 插件只有在经过重新编译后才支持 64 位操作系统。请参阅《Symantec Data Loss Prevention 系统要求和兼容性指南》，以确保所有必需的 Symantec Data Loss Prevention 功能和第三方实用程序在 64 位目标平台上可用。
- 您可以迁移 Enforce Server 而不迁移存储 Enforce Server 数据库的 Oracle 数据库，反之亦然。如果要将 Oracle 数据库服务器迁移到 64 位，Symantec 建议您先迁移 Oracle，然后再迁移 Enforce Server。如果先迁移 Oracle，在迁移之后，就不必要重新配置 Enforce Server 以访问新的 Oracle 数据库。
- 您可以迁移检测服务器而不迁移 Enforce Server，反之亦然。
- 32 位 Enforce Server、Oracle 数据库服务器或检测服务器可与 64 位 Symantec Data Loss Prevention 服务器或 Oracle 数据库服务器一起运行。不必将 Symantec Data Loss Prevention 部署的所有组件都升级到 64 位。

在迁移过程中，会使用其他 Symantec Data Loss Prevention 文档中介绍的多个过程。例如，如果要将 Enforce Server 数据库迁移到 64 位平台，可参考《Symantec Data Loss Prevention Oracle 11g 安装和升级指南》将数据库软件升级到 Oracle 11g，然后将软件和数据库迁移到 64 位平台。迁移说明会在必要时将您引导至正确的指南和过程。

表 11-1 将 Symantec Data Loss Prevention 服务器从 32 位操作系统迁移到 64 位操作系统

阶段	操作	说明
阶段 1	将所有 Symantec Data Loss Prevention 服务器升级到最新版本。	开始迁移过程之前，现有的 Enforce Server 和所有检测服务器必须是最新版本。 请参见您平台的《Symantec Data Loss Prevention 升级指南》。
阶段 2	备份 Enforce Server 数据库。	请参见《Symantec Data Loss Prevention Oracle 11g 安装和升级指南》。

阶段	操作	说明
阶段 3	(可选) 将 Enforce Server 数据库迁移到 64 位操作系统。	要将现有的 Enforce Server 数据库迁移到 64 位，必须首先将数据库软件升级到 Oracle 11g。然后，便可以将 Enforce Server 数据库迁移到新的 64 位服务器计算机或虚拟机。 请参阅《Symantec Data Loss Prevention Oracle 11g 安装和升级指南》中的“从 Oracle 10g 32 位迁移到 Oracle 11g 64 位”一章。
阶段 4	在开始迁移 Enforce Server 或 Network Discover 检测服务器之前，停止所有 Network Discover 扫描。	请参见第 943 页的“ 管理 Network Discover 目标扫描 ”。 在完成服务器迁移之前，不要重新启动扫描。
阶段 5	(可选) 迁移 Enforce Server。	请参见第 165 页的“ 将 Enforce Server 迁移到 64 位操作系统 ”。
阶段 6	(可选) 在端点计算机上更新 Symantec DLP Agent 连接配置。	如果要将 Endpoint Prevent 检测服务器迁移到 64 位系统，请确保在迁移过程中，所有端点计算机上的 Symantec DLP Agent 已配置为使用可用的备份 Endpoint Prevent 检测服务器。 请参见第 1183 页的“ 关于 Endpoint Server 冗余 ”。 或者，更新端点计算机上的所有 Symantec DLP Agent，使其 Endpoint Prevent 服务器列表中包含 64 位新服务器的 IP 地址。现在进行此配置更改可确保端点计算机在新的 64 位 Endpoint Prevent 服务器可用时自动故障转移到该服务器。
阶段 7	(可选) 迁移检测服务器。	请参见第 168 页的“ 将检测服务器迁移到 64 位操作系统 ”。

将 Enforce Server 迁移到 64 位操作系统

将 Enforce Server 迁移到 64 位操作系统需要您安装新的 64 位 Enforce Server 并保留现有的 Enforce Server 数据库。使用以下过程以确保保留所有配置数据。

将 Enforce Server 迁移到 64 位操作系统

- 1 关闭 32 位 Enforce Server 并禁用服务。

请参见第 70 页的“[关于在 Windows 上启动和停止服务](#)”。

请参见第 73 页的“[在 Linux 上启动和停止服务](#)”。

- 2 验证服务已停止后，请将其禁用，以防重新启动服务器计算机时自动启动这些服务。

- 3 安装 64 位 Enforce Server，确保重新使用（不要初始化）现有的 Enforce Server 数据库：

- 在 **Oracle Database Server Information** 和 **Oracle Database User Configuration** 面板上，输入现有 Enforce Server 数据库的连接信息和凭据。
- 在 **Final Confirmation** 面板上，取消选中 **Initialize Enforce Data** 复选框。

警告：安装新的 64 位 Enforce Server 数据库时，请不要初始化 Enforce Server 数据库。必须保留现有数据库，以确保所有的配置、策略和事件数据转移到新系统中。

- 安装完成后，取消选中 **Start Services** 复选框。

请参见适用于所用平台的《Symantec Data Loss Prevention 安装指南》。

- 4 安装新的 64 位服务器后，手动将下列附加配置文件从 32 位服务器复制到 64 位计算机或虚拟机上的相同目录中：

目录

说明

DLP_home\Protect\plugins 或
/opt/DLP_home/Protect/plugins

如果使用了自定义插件，请复制 *plugins* 目录下的全部内容；否则如果使用 Network Discover 配置了本机扫描选项，则无需任何操作。

如果有任何插件需要 *plugins* 目录外部的资源，请同时复制这些资源。

注意：必须重新编译使用本机代码的任何插件，以便能够在 64 位 Enforce Server 计算机或虚拟机上使用。不要将 32 位本机插件复制到新服务器。

DLP_home\Protect\config 或
/opt/DLP_home/Protect/config

如果手动编辑了除 *jdbc.properties* 以外的其他 Symantec Data Loss Prevention 属性文件（扩展名为 *.properties*），请将该文件复制到 64 位 Enforce Server 计算机或虚拟机上的相同位置。

注意：不要将 *jdbc.properties* 文件复制到新的服务器计算机或虚拟机。不要将任何配置文件（扩展名为 *.conf*）复制到新计算机。

这些文件中的许多属性定义了目录和文件的位置。如果将某个属性文件复制到了 64 位计算机，还应在该文件的新位置对其进行编辑，以确保所有路径有效。例如，如果 32 位 Enforce Server 安装在 *c:* 驱动器上，而 64 位服务器位于 *d:* 驱动器上，那么，请编辑所有复制的属性文件，以便将 *d:* 指定为根驱动器。

DLP_home\Protect\scan\incremental_index 或
/var/Vontu/scan/incremental_index

如果配置了 Network Discover 增量扫描，请将整个 *incremental_index* 目录复制到 64 位 Enforce Server 安装，以保留索引数据。

注意：在 Linux 系统上，在系统之间复制文件时，请确保保留相同的文件权限和所有权属性。

- 5 重新安装您在 32 位 Enforce Server 上使用的所有语言包。

请参见第 61 页的“[关于 Symantec Data Loss Prevention 语言包](#)”。

将检测服务器迁移到 64 位操作系统

- 6 导入与安装的检测服务器、Active Directory 连接或 FlexResponse 插件进行通信所必需的所有自定义证书。

请参见适用于所用平台的《Symantec Data Loss Prevention 安装指南》中的“配置安全通信的证书”。

- 7 复制所有配置文件后，启动 64 位 Enforce Server。

请参见第 70 页的“[关于在 Windows 上启动和停止服务](#)”。

请参见第 73 页的“[在 Linux 上启动和停止服务](#)”。

将检测服务器迁移到 64 位操作系统

要迁移检测服务器，请按顺序执行以下步骤：

将检测服务器迁移到 64 位操作系统

- 1 确保 64 位检测服务器系统包含您要迁移的检测服务器的所有第三方软件。

例如，如果要迁移 32 位 Network Discover 检测服务器，则还可能需要在服务器计算机上安装 64 位版本的 Outlook 2010。

- 2 在指定的服务器计算机或虚拟机（如果检测服务器支持虚拟机部署）上安装 64 位检测服务器软件。

请参见适用于所用平台的《Symantec Data Loss Prevention 安装指南》。

- 3 安装新的 64 位服务器后，手动将下列附加配置文件从 32 位服务器复制到 64 位计算机或虚拟机上的相同目录中：

目录	说明
<i>DLP_home\Protect\plugins</i> 或 <i>/opt/DLP_home/Protect/plugins</i>	如果使用自定义插件，请复制 <i>plugins</i> 目录的整个内容。 如果有任何插件需要 <i>plugins</i> 目录外部的资源，请同时复制这些资源。
<i>DLP_home\Protect\config</i> 或 <i>/opt/DLP_home/Protect/config</i>	注意： 必须重新编译使用本机代码的任何插件，以便能够在 64 位检测服务器计算机或虚拟机上使用。不要将 32 位本机插件复制到新服务器。 如果手动编辑了除 <i>jdbc.properties</i> 以外的其他 Symantec Data Loss Prevention 属性文件（扩展名为 <i>.properties</i> ），请将该文件复制到 64 位 Enforce Server 计算机或虚拟机上的相同位置。
<i>DLP_home\Protect\scan\incremental_index</i> 或 <i>/var/Vontu/scan/incremental_index</i>	注意： 不要将 <i>jdbc.properties</i> 文件复制到新的服务器计算机或虚拟机。不要将任何配置文件（扩展名为 <i>.conf</i> ）复制到新计算机。 这些文件中的许多属性定义了目录和文件的位置。如果将某个属性文件复制到了 64 位计算机，还应在该文件的新位置对其进行编辑，以确保所有路径有效。例如，如果 32 位 Enforce Server 安装在 <i>c:\</i> 驱动器上，而 64 位服务器位于 <i>d:\</i> 驱动器上，那么，请编辑所有复制的属性文件，以便将 <i>d:\</i> 指定为根驱动器。
<i>DLP_home\Protect\lib\jdbc</i> 或 <i>/opt/DLP_home/Protect/lib/jdbc</i>	如果配置了 Network Discover 增量扫描，请将整个 <i>incremental_index</i> 目录复制到 64 位 Enforce Server 安装，以保留索引数据。
<i>DLP_home\Protect\lib\jdbc</i> 或 <i>/opt/DLP_home/Protect/lib/jdbc</i>	如果已将某个 JDBC 驱动程序添加到 32 位检测服务器，请将该驱动程序复制到 64 位检测服务器计算机，或者将该驱动程序的 64 位版本添加到 64 位服务器。

注意：在 Linux 系统上，在系统之间复制文件时，请确保保留相同的文件权限和所有权属性。

- 4 导入与 Enforce Server 和其他任何网络组件进行通信所必需的所有自定义证书。例如，可能需要在 Network Prevent for Email 服务器上重新导入 MTA 证书以支持 TLS 通信。

请参见适用于所用平台的《Symantec Data Loss Prevention 安装指南》中的“配置安全通信的证书”。

请参见《Symantec Data Loss Prevention MTA 集成指南（适用于 Network Prevent for Email）》中的“配置 TLS 的密钥和证书”。

- 5 如果 64 位检测服务器尚未运行，请将其启动。

请参见第 70 页的“[关于在 Windows 上启动和停止服务](#)”。

请参见第 73 页的“[在 Linux 上启动和停止服务](#)”。

- 6 登录到 Enforce Server 管理控制台进行部署。

- 7 选择“系统”>“服务器”>“概述”。

- 8 单击所迁移的 32 位检测服务器的名称。

- 9 单击“配置”。

- 10 编辑“主机”和“端口”字段，以指向新的 64 位服务器计算机或虚拟机。

- 11 单击“保存”。

- 12 单击“完成”。

- 13 关闭迁移的 32 位检测服务器。

请参见第 70 页的“[关于在 Windows 上启动和停止服务](#)”。

请参见第 73 页的“[在 Linux 上启动和停止服务](#)”。

3

部分

管理检测服务器

- 12. 安装和管理检测服务器
- 13. 管理日志文件
- 14. 使用 Symantec Data Loss Prevention 实用程序

安装和管理检测服务器

本章节包括下列主题：

- [关于管理 Symantec Data Loss Prevention 服务器](#)
- [启用高级进程控制](#)
- [服务器控件](#)
- [服务器配置 - 基本](#)
- [服务器配置 - 高级](#)
- [添加检测服务器](#)
- [删除服务器](#)
- [将 SSL 证书导入到 Enforce Server 或发现服务器](#)
- [关于系统概述屏幕](#)
- [服务器状态概述](#)
- [最近的错误和警告事件列表](#)
- [“服务器详细信息”屏幕](#)
- [高级服务器设置](#)
- [高级代理设置](#)

关于管理 Symantec Data Loss Prevention 服务器

可以从“系统”>“服务器”>“概述”屏幕管理 Symantec Data Loss Prevention 服务器。此屏幕提供系统概述，包括服务器状态和最近的系统事件。它会显示有关

所有 Symantec Data Loss Prevention 服务器的摘要信息，最近的错误和警告事件列表，以及有关许可证的信息。您可以从此屏幕添加或删除检测服务器。

- 单击服务器的名称，以显示“[服务器详细信息](#)”屏幕，通过该屏幕您能控制和配置此服务器。

请参见第 151 页的“[安装新的许可证文件](#)”。

请参见第 50 页的“[关于 Enforce Server 管理控制台](#)”。

请参见第 191 页的“[关于系统概述屏幕](#)”。

请参见第 194 页的“[“服务器详细信息”屏幕](#)”。

请参见第 187 页的“[添加检测服务器](#)”。

请参见第 189 页的“[删除服务器](#)”。

请参见第 175 页的“[服务器控件](#)”。

请参见第 176 页的“[服务器配置 - 基本](#)”。

启用高级进程控制

通过 Symantec Data Loss Prevention 高级进程控制，可以从 Enforce Server 管理控制台启动或停止单独的服务器进程。您不需要启动或停止整台服务器。此功能对调试很有帮助。高级进程控制处于关闭状态（默认）时，每个“[服务器详细信息](#)”屏幕只显示整台服务器的状态。打开高级进程控制后，“[服务器详细信息](#)”屏幕的“[常规](#)”部分显示各个进程。

请参见第 194 页的“[“服务器详细信息”屏幕](#)”。

个别进程和运行进程的服务器如下：

- 监视控制器 (Enforce Server) 控制检测服务器。
- 文件读取器（所有检测服务器）检测事件。
- 事件写入器（所有检测服务器，属于单层安装的除外）将事件上传到 Enforce Server。
- 数据包捕获 (Network Monitor) 捕获网络流。
- 请求处理器 (Network Prevent for Email) 处理 SMTP 请求。
- Endpoint Server (Endpoint Server) 与 Symantec DLP Agent 进行交互。

启用高级进程控制

1 转至“系统”>“设置”>“常规”，然后单击“配置”。

将显示“编辑系统设置”屏幕。

2 向下滚动至“进程控制”部分并选中“高级进程控制”框。

3 单击“保存”。

请参见第 176 页的[“服务器配置 - 基本”](#)。

有关使用系统设置的更多信息，请参考 Symantec Data Loss Prevention 联机帮助。

服务器控件

可从“[服务器详细信息](#)”屏幕中控制服务器及其进程。

■ 要访问特定服务器的“[服务器详细信息](#)”屏幕，请转至“概述”屏幕（“系统”>“服务器”>“概述”），然后单击列表中的服务器名称。

请参见第 194 页的[“服务器详细信息”屏幕](#)。

“[服务器详细信息](#)”屏幕的“常规”部分会显示服务器及其进程的状态。“启动”、“循环”和“停止”按钮可控制服务器和进程操作。

“[服务器详细信息](#)”屏幕的“常规”部分会显示服务器的当前状态。可能的值有：

表 12-1 服务器状态值

图标	状态
	正在启动 - 正在启动过程中。
	正在运行 - 正在运行并且没有错误。
	正在运行所选的 - 服务器上的某些进程已停止或有错误。要查看各进程的状态，您必须先启用“系统设置”屏幕上的“高级进程控制”。
	正在停止 - 正在停止过程中。
	已停止 - 已完全停止。
	未知 - 服务器遇到下列错误之一：

- 启动。要启动服务器或进程，请单击“启动”。
- 循环。要停止并重新启动服务器，请单击“循环”。
- 停止。要停止服务器或进程，请单击“停止”。
- 要在进程启动过程中终止进程，请单击“终止”。

注意：仅当为 Enforce Server 启用“高级进程控制”后，才会显示各个服务器进程的状态和控件。要启用“高级进程控制”，请转至“系统”>“设置”>“常规”>“配置”，选中“高级进程控制”框，并单击“保存”。

- 要更新状态，请根据需要单击屏幕右上角部分的刷新图标。

请参见第 49 页的[“关于 Symantec Data Loss Prevention 管理”](#)。

请参见第 191 页的[“关于系统概述屏幕”](#)。

请参见第 194 页的[“服务器详细信息”屏幕](#)。

请参见第 176 页的[“服务器配置 - 基本”](#)。

请参见第 126 页的[“系统事件报告”](#)。

请参见第 129 页的[“服务器事件详细信息”](#)。

服务器配置 - 基本

从“系统”>“设置”菜单中配置 Enforce Server。

从每个服务器各自的“配置服务器”屏幕中配置检测服务器。

配置服务器

- 1 转至“概述”屏幕（“系统”>“服务器”>“概述”）。
- 2 单击列表中服务器的名称。

此时将显示该服务器的“服务器详细信息”屏幕。“服务器详细信息”屏幕的左上部有下列按钮：

- 完成。单击“完成”可返回上一个屏幕。
- 配置。单击“配置”可指定该服务器的基本配置。
- 服务器设置。单击“服务器设置”可指定此服务器的高级配置参数。修改高级服务器设置时要十分小心。建议更改任何高级设置之前先向 Symantec 支持部门进行确认。
请参见第 187 页的[“服务器配置 - 高级”](#)。

有关高级服务器配置的信息，请参见 Symantec Data Loss Prevention 联机帮助。

- 3 单击“配置”或“服务器设置”，显示该类型服务器的配置屏幕。
- 4 根据需要，指定或更改屏幕上的设置，然后单击“保存”。
单击“取消”可返回到上一个屏幕，而不更改任何设置。

注意：必须重新启动服务器才能使新设置生效。

请参见第 175 页的“[服务器控件](#)”。

“配置服务器”屏幕包含一个适用于所有检测服务器的“常规”部分，该部分包含以下参数：

- **名称。**您为服务器选择的名称。此名称会显示在 Enforce Server 管理控制台中（“系统”>“服务器”>“概述”）。此名称不能超过 255 个字符。
- **主机。**托管服务器的系统的主机名或 IP 地址。必须完全限定主机名。如果主机具有多个 IP 地址，请指定检测服务器用于侦听与 Enforce Server 的连接所使用的地址。
- **端口。**检测服务器用来与 Enforce Server 通信的端口号。默认值为 8100。

对于单层安装，“与 Enforce 相同”选项可用。如果安装检测服务器的主机与 Enforce Server 所在的主机相同，请选择此选项以使用本地 IP 地址 (127.0.0.1) 自动填充“主机”字段。

“配置服务器”屏幕的其他部分随服务器类型的不同而不同。

请参见第 177 页的“[Network Monitor Server - 基本配置](#)”。

请参见第 184 页的“[Network Discover Server 和 Network Protect - 基本配置](#)”。

请参见第 179 页的“[Network Prevent for Email Server - 基本配置](#)”。

请参见第 182 页的“[Network Prevent for Web Server - 基本配置](#)”。

请参见第 185 页的“[Endpoint Server - 基本配置](#)”。

请参见第 194 页的““[服务器详细信息](#)”屏幕”。

请参见第 186 页的“[分类服务器 - 基本配置](#)”。

请参见第 194 页的““[服务器详细信息](#)”屏幕”。

Network Monitor Server - 基本配置

从每个服务器各自的“配置服务器”屏幕中配置检测服务器。要显示“配置服务器”屏幕，请转至“概述”屏幕（“系统”>“服务器”>“概述”），然后单击列

表中的服务器名称。此时将出现该服务器的“服务器详细信息”屏幕。单击“配置”可显示“配置服务器”屏幕。

Network Monitor Server 的“配置服务器”屏幕包括“常规”部分和两个选项卡：

- “常规”部分。使用此部分可以指定服务器的名称、主机和端口。
请参见第 176 页的“[服务器配置 - 基本](#)”。
- “数据包捕获”选项卡。使用此选项卡可以配置网络数据包捕获设置。
- “**SMTP 复制规则**”选项卡。使用此选项卡可以修改服务器用来检索 SMTP 邮件文件的源文件夹。

“数据包捕获”的顶端部分定义了常规的数据包捕获参数。它提供下列字段：

字段	说明
源文件夹覆盖	源文件夹是服务器在处理网络流之前用于缓冲网络流的目录。建议的设置是将“源文件夹覆盖”字段留空以接受默认值。要指定自定义缓冲目录，请键入该目录的完整路径。
存档文件夹	如果不想存档数据，请将“存档文件夹”字段留空。要存档数据，请输入用于该用途的目录的完整路径。
网络接口	选择用于监控的网络接口卡。请注意，要监控 NIC，必须在 Network Monitor Server 上安装 WinPcap 软件。 有关 NIC 的更多信息，请参见《Symantec Data Loss Prevention 安装指南》。

请参见第 881 页的“[实施 Network Monitor](#)”。

“数据包捕获”的“协议”部分用于指定要捕获的网络流量类型（按协议），还可指定要应用的任何自定义参数。此部分列出了已获得 Symantec 许可的标准协议，以及已添加的任何自定义 TCP 协议。

要监控某个特定协议，请选中相应的框。首次配置服务器时，每个选定协议的设置将继承系统范围的协议设置。可以转至“系统”>“设置”>“协议”来配置这些设置。系统范围的默认设置会列为“标准”。

有关使用系统范围的设置的信息，请参见 Symantec Data Loss Prevention 联机帮助。

要覆盖某个协议继承的过滤设置，请单击该协议的名称。可使用下列自定义设置（有些设置可能对于某些协议不可用）：

- IP 过滤器
- L7 发送者过滤器
- L7 接受者过滤器
- 内容过滤器
- 搜索深度 (数据包)
- 采样率
- 写入前的最长等待时间
- 丢弃前的最长等待时间
- 最大流数据包数
- 最小流大小
- 最大流大小
- 区段间隔
- 无流量通知超时（此设置的最大值为 360000 秒。）

使用“**SMTP 复制规则**”可修改此服务器用来检索 SMTP 邮件文件的源文件夹。可通过输入文件夹的完整路径来修改源文件夹。

请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。

请参见第 191 页的“[关于系统概述屏幕](#)”。

请参见第 194 页的“[“服务器详细信息”屏幕](#)”。

请参见第 176 页的“[“服务器配置 - 基本”](#)”。

请参见第 175 页的“[“服务器控件”](#)”。

除“**配置服务器**”屏幕中提供的设置外，还可为此服务器指定高级设置。要指定高级配置参数，请单击服务器的“**概述**”屏幕中的“**服务器设置**”。修改高级服务器设置时要十分小心。在更改任何高级设置之前，请联系 Symantec 支持部门。

请参见第 195 页的“[“高级服务器设置”](#)”。

有关高级服务器设置的信息，请参见 Symantec Data Loss Prevention 联机帮助。

Network Prevent for Email Server - 基本配置

从每个服务器各自的“**配置服务器**”屏幕中配置检测服务器。要显示“**配置服务器**”屏幕，请转至“**概述**”屏幕（“**系统**”>“**服务器**”>“**概述**”），然后单击列

表中的服务器名称。此时将出现该服务器的“服务器详细信息”屏幕。单击“配置”可显示“配置服务器”屏幕。

Network Prevent for Email Server 的“配置服务器”屏幕包括“常规”部分和“内联 SMTP”选项卡。“常规”部分用于指定服务器的名称、主机和端口。

请参见第 176 页的“[服务器配置 - 基本](#)”。

使用“内联SMTP”选项卡可配置不同的 Network Prevent for Email Server 功能：

字段	说明
试用模式	试用模式让您无需阻止请求即可测试阻止功能。选择试用模式后，服务器会检测事件并创建事件报告，但不会阻止任何消息。取消选择此选项将阻止违反 Symantec Data Loss Prevention 策略的消息。
Keystore 密码	如果在转发模式配置中使用 TLS 身份验证，请输入 Keystore 文件的正确密码。
确认 Keystore 密码	重新输入 Keystore 文件密码。
下一跳配置	选择“反射”以在反射模式下运行 Network Prevent for Email Server。选择“转发”以在转发模式下运行。 注意： 如果选择“转发”，则还必须选择“启用 MX 查找”或“禁用 MX 查找”，以配置用于确定下一跳 MTA 的方法。
启用 MX 查找	此选项仅适用于转发模式配置。 选择“启用 MX 查找”来根据域名执行 DNS 查询，以获取服务器的邮件交换 (MX) 记录。Network Prevent for Email Server 使用返回的 MX 记录来选择下一跳邮件服务器的地址。 如果选择“启用 MX 查找”，则同时在“输入域”文本框中添加一个或多个域名。例如： companyname.com Network Prevent for Email Server 会对您指定的域名执行 MX 记录查询。 注意： “输入域”文本框中必须至少包含一个有效条目，才可成功配置转发模式行为。

字段	说明
禁用 MX 查找	<p>此字段仅适用于转发模式配置。</p> <p>如果您要指定一个或多个下一跳 MTA 的确切主机名或 IP 地址，请选择“禁用 MX 查找”。Network Prevent for Email Server 将使用您指定的主机名或地址，且不会执行 MX 记录查找。</p> <p>如果选择“禁用 MX 查找”，请同时在“输入主机名”文本框中添加一个或多个下一跳 MTA 的主机名或 IP 地址。可以通过将每个条目放在单独的一行中来指定多个条目。例如：</p> <pre>smtp1.companyname.com smtp2.companyname.com smtp3.companyname.com</pre> <p>Network Prevent for Email Server 总是尝试使用您在列表中指定的第一个 MTA。如果该 MTA 不可用，Network Prevent for Email Server 会尝试代理到列表中下一个可用的条目。</p> <p>注意：“输入主机名”文本框中必须至少包含一个有效条目，才可成功配置转发模式行为。</p>

有关配置 Network Prevent for Email Server 选项的其他相关信息，请参见《Symantec Data Loss Prevention MTA 集成指南（适用于 Network Prevent for Email）》。

请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。

请参见第 191 页的“[关于系统概述屏幕](#)”。

请参见第 194 页的“[“服务器详细信息”屏幕](#)”。

请参见第 176 页的“[服务器配置 - 基本](#)”。

请参见第 175 页的“[服务器控件](#)”。

除“配置服务器”屏幕中提供的设置外，还可为此服务器指定高级设置。要指定高级配置参数，请单击服务器的“概述”屏幕中的“[服务器设置](#)”。修改高级服务器设置时要十分小心。在更改任何高级设置之前，请联系 Symantec 支持部门。

请参见第 195 页的“[高级服务器设置](#)”。

有关高级服务器设置的信息，请参见 Symantec Data Loss Prevention 联机帮助。

Network Prevent for Web Server - 基本配置

从每个服务器各自的“配置服务器”屏幕中配置检测服务器。要显示“配置服务器”屏幕，请转至“概述”屏幕（“系统”>“服务器”>“概述”），然后单击列表中的服务器名称。此时将出现该服务器的“服务器详细信息”屏幕。单击“配置”可显示“配置服务器”屏幕。

Network Prevent for Web Server 的“配置服务器”屏幕包括“常规”部分和一个选项卡：

- “常规”部分。此部分用于指定服务器的名称、主机和端口。
请参见第 176 页的[“服务器配置 - 基本”](#)。
- **ICAP** 选项卡。此选项卡用于配置 Internet 内容修改协议 (ICAP) 捕获。

使用 **ICAP** 选项卡可配置基于 Web 的网络流量。**ICAP** 选项卡分成四个部分：

- “试用模式”部分让您无需阻止流量即可测试阻止功能。选择试用模式后，服务器会检测事件并创建事件报告，但不会阻止任何流量。此选项让您无需阻止流量即可测试策略。要启用试用模式，请选中此框。
- “请求过滤”部分用于配置流量过滤条件：

字段	说明
忽略小于以下大小的请求	指定要在此服务器上检查的 HTTP 请求的最小正文大小。默认值为 4096 字节。系统不会检查正文小于此数值的 HTTP 请求。
忽略没有附件的请求	选中此框将仅检查包含附件的 HTTP 请求。
忽略主机或域的请求	输入请求应该过滤掉（忽略）的主机名或域。每行输入一个主机名或域名。
忽略来自用户代理的请求	输入请求应该过滤掉（忽略）的用户代理名称。每行输入一个代理。

- “响应过滤”部分用于配置过滤条件以管理 HTTP 响应：

字段	说明
忽略小于以下大小的响应	输入要在此服务器上检查的 HTTP 响应的最小正文大小。默认值为 4096 字节。系统不会检查正文小于此数值的 HTTP 响应。
检查内容类型	指定此服务器要监控的 MIME 内容类型。默认情况下，该字段包含标准 Microsoft Office、PDF 以及纯文本格式的内容类型值。您可以添加其他 MIME 内容类型值。每行输入一个单独的内容类型。例如，要检查 WordPerfect 5.1 文件，请输入 application/wordperfect5.1。
忽略来自主机或域的响应	输入响应将被忽略的主机名或域。每行输入一个主机名或域名。
忽略对用户代理的响应	输入响应将被忽略的用户代理名称。每行输入一个用户代理。

- “连接”部分用于配置 HTTP 代理服务器与 Network Prevent for Web Server 之间的 ICAP 连接设置：

字段	说明
TCP 端口	指定此服务器用于侦听 ICAP 请求的 TCP 端口号。必须在将 ICAP 请求发送给此服务器的 HTTP 代理上配置相同的端口号。建议值为 1344。
最大请求数	输入允许来自 HTTP 代理的最大并行 ICAP 连接数。默认值为 25。
最大响应数	输入允许来自 HTTP 代理的最大并行 ICAP 响应连接数。默认值为 25。

字段	说明
连接积压	输入允许的最大等待连接数。每个等待的连接表示一名用户在其浏览器中等待。最小值为 1。

请参见第 907 页的“[配置 Network Prevent for Web Server](#)”。

请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。

请参见第 191 页的“[关于系统概述屏幕](#)”。

请参见第 194 页的“[“服务器详细信息”屏幕](#)”。

请参见第 176 页的“[服务器配置 - 基本](#)”。

请参见第 175 页的“[服务器控件](#)”。

除“[配置服务器](#)”屏幕中提供的设置外，还可为此服务器指定高级设置。要指定高级配置参数，请单击服务器的“[概述](#)”屏幕中的“[服务器设置](#)”。修改高级服务器设置时要十分小心。在更改任何高级设置之前，请联系 Symantec 支持部门。

请参见第 195 页的“[高级服务器设置](#)”。

有关高级服务器设置的信息，请参见 Symantec Data Loss Prevention 联机帮助。

Network Discover Server 和 Network Protect - 基本配置

从每个服务器各自的“[配置服务器](#)”屏幕中配置检测服务器。要显示服务器的“[配置](#)”屏幕，请转至“[概述](#)”屏幕（“[系统](#)” > “[服务器](#)” > “[概述](#)”），然后单击列表中的服务器名称。此时将显示该服务器的“[服务器详细信息](#)”屏幕。单击“[配置](#)”。此时将显示服务器的“[配置服务器](#)”屏幕。

请参见第 924 页的“[修改 Network Discover Server 配置](#)”。

Network Discover Server 的“[配置服务器](#)”屏幕包括“[常规](#)”部分和一个选项卡：

- “[常规](#)”部分。此部分用于指定服务器的名称、主机和端口。

请参见第 176 页的“[服务器配置 - 基本](#)”。

- “[发现](#)”选项卡。此选项卡用于修改在此发现服务器上运行的并行扫描数。

可以随时增大最大计数。增大该值之后，可在 Network Discover Server 上运行的任何已排队扫描都会启动。只有在 Network Discover Server 没有运行中的扫描时，才能减小该计数。减小该计数之前，请暂停或停止该服务器上运行的所有扫描。

要查看 Network Discover Server 上运行的扫描，请转至“[管理](#)” > “[发现扫描](#)” > “[发现目标](#)”。

请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。

请参见第 194 页的“[“服务器详细信息”屏幕](#)”。

请参见第 176 页的“[服务器配置 - 基本](#)”。

请参见第 175 页的“[服务器控件](#)”。

除“配置服务器”屏幕中提供的设置外，还可为此服务器指定高级设置。要指定高级配置参数，请单击服务器的“服务器详细信息”屏幕中的“服务器设置”。修改高级服务器设置时要十分小心。建议更改任何高级设置之前先向 Symantec 支持部门进行确认。

请参见第 195 页的“[高级服务器设置](#)”。

Endpoint Server - 基本配置

从每个服务器各自的“配置服务器”屏幕中配置检测服务器。要显示服务器的“配置”屏幕，请转至“概述”屏幕（“系统”>“服务器”>“概述”），然后单击服务器的名称。此时显示该服务器的“服务器详细信息”屏幕。单击“配置”可显示该服务器的“配置服务器”屏幕。

请参见第 187 页的“[添加检测服务器](#)”。

Endpoint Server 的“配置服务器”屏幕包括“常规”部分和以下选项卡：

- “常规”。此部分用于指定服务器的名称、主机和端口。

请参见第 176 页的“[服务器配置 - 基本](#)”。

- “代理”。此部分用于将 Endpoint Server 配置为特定端点配置。

请参见第 1156 页的“[添加代理配置](#)”。

“代理侦听程序”。使用此部分可以配置 Endpoint Server 以侦听来自 Symantec DLP Agent 的连接：

字段	说明
绑定地址	输入 Endpoint Server 用于侦听来自 Symantec DLP Agent 的通信的 IP 地址。默认 IP 地址是 0.0.0.0，Endpoint Server 可通过此地址来侦听所有主机 IP 地址。
端口	输入 Endpoint Server 用于侦听来自 Symantec DLP Agent 的通信的端口。

“代理配置”。使用此部分可以指定您希望与新的 Endpoint Server 相关联的代理配置模块。

字段	说明
代理配置	在下拉菜单中选择所需的代理配置模块。如果仅定义了一个模块，Endpoint Server 会自动与该代理配置相关联。

请参见第 1155 页的“[关于代理配置](#)”。

分类服务器 - 基本配置

从每个服务器各自的“配置服务器”屏幕中配置检测服务器。要显示“配置服务器”屏幕，请转至“概述”屏幕（“系统”>“服务器”>“概述”），然后单击列表中的服务器名称。将显示针对该服务器的“服务器详细信息”屏幕。单击“配置”可显示“配置服务器”屏幕。

分类服务器的“配置服务器”屏幕分为两个部分：

- “常规”部分。此部分指定服务器名称、主机和用于与 Enforce Server 通信的端口。
请参见第 176 页的“[服务器配置 - 基本](#)”。
- “分类”部分。此部分指定供 Enterprise Vault 数据分类过滤器用来与分类服务器通信的连接属性。

使用“分类”部分中的字段可配置该服务器的连接属性：

最大会话数	输入分类服务器最多可以接受的来自 Enterprise Vault 数据分类过滤器的并发会话数。默认值是 12。分类服务器可以支持的最大会话数取决于该服务器中可用的 CPU 和内存。有关更多信息，请参见 <i>Symantec Enterprise Vault Data Classification Services Implementation Guide</i> （《Symantec Enterprise Vault 数据分类服务操作指南》）。
会话超时(毫秒)	输入在分类服务器终止会话之前，Enterprise Vault 数据分类过滤器可保持空闲的最大毫秒数。默认值为 30000 毫秒。
分类服务端口	指定分类服务器接受来自 Enterprise Vault 数据分类过滤器的连接的端口号。默认端口为 10080。

注意：分类服务器仅用于 Symantec Enterprise Vault 数据分类解决方案，该解决方案独立于 Symantec Data Loss Prevention 进行授权。您必须配置 Enterprise Vault 数据分类服务过滤器和分类服务器，使其相互通信。有关更多信息，请参见 *Symantec Enterprise Vault Data Classification Services Implementation Guide*（《Symantec Enterprise Vault 数据分类服务操作指南》）。

服务器配置 - 高级

Symantec Data Loss Prevention 为系统中的每个检测服务器提供高级服务器配置设置。

注意：在更改任何高级设置之前，请联系 Symantec 支持部门。如果在更改高级设置时出错，则可能会严重降低性能，甚至会禁用整台服务器。

更改检测服务器的高级配置设置

1 请转到“系统”>“服务器”>“概述”，并单击相应检测服务器的名称。

此时将出现该服务器的“服务器详细信息”屏幕。

2 单击“服务器设置”。

将显示“高级服务器设置”屏幕。

有关高级服务器配置的信息，请参见 Symantec Data Loss Prevention 联机帮助。

请参见第 195 页的“[高级服务器设置](#)”。

3 在 Symantec 支持部门的引导下，修改相应设置。

4 单击“保存”。

在此屏幕上所做的设置更改，通常会在重新启动服务器后才会生效。

请参见第 176 页的“[服务器配置 - 基本](#)”。

添加检测服务器

从“系统”>“服务器”>“概述”屏幕中将所需的检测服务器添加到 Symantec Data Loss Prevention 系统中。

您可以添加以下类型的服务器：

- Network Monitor Server，用于监视网络流量。

- Network Protect Server，用于检查存储数据是否存在策略违规 (Network Discover)。
- Network Prevent for Email Server，用于防止 SMTP 违规。
- Network Prevent for Web Server，用于防止 ICAP 代理服务器违规，例如 FTP、HTTP 和 HTTPS。
- Mobile Prevent for Web Server，用于监视和防止移动设备上的 HTTP、HTTPS 和 FTP 违规情况。

注意：如果您的 Symantec Data Loss Prevention 许可证既包括 Mobile Prevent for Web 又包括 Network Prevent (Web Server)，请添加一个名为 **Network and Mobile Prevent for Web Server** 的检测服务器。

- Endpoint Server，用于控制监视端点计算机的 Symantec DLP Agent。
- 分类服务器，用于分析 Symantec Enterprise Vault 过滤器发送的电子邮件，以及提供分类结果以供 Enterprise Vault 根据需要用于执行标记、归档和删除操作。

添加检测服务器

- 1 转至“系统概述”屏幕（“系统”>“服务器”>“概述”）。
请参见第 191 页的[“关于系统概述屏幕”](#)。
- 2 单击“添加服务器”。
将显示“添加服务器”屏幕。
- 3 选择要安装的服务器类型并单击“下一步”。
将显示针对该检测服务器的“配置服务器”屏幕。
- 4 要执行基本的服务器配置，请使用“配置服务器”屏幕，然后在完成配置时单击“保存”。
请参见第 177 页的[“Network Monitor Server - 基本配置”](#)。
请参见第 179 页的[“Network Prevent for Email Server - 基本配置”](#)。
请参见第 182 页的[“Network Prevent for Web Server - 基本配置”](#)。
请参见第 184 页的[“Network Discover Server 和 Network Protect - 基本配置”](#)。
请参见第 185 页的[“Endpoint Server - 基本配置”](#)。
请参见第 186 页的[“分类服务器 - 基本配置”](#)。

- 5 要返回到“系统概述”屏幕，请单击“完成”。
新服务器会出现在“服务器”列表中，状态为“未知”。
- 6 单击该服务器以显示其“服务器详细信息”屏幕。
请参见第 194 页的“[服务器详细信息屏幕](#)”。
- 7 单击“重新启动”重新启动服务器。
- 8 单击“完成”返回到“系统概述”屏幕。
服务器重新启动结束后，其状态显示“正在运行”。
- 9 如有必要，请单击“服务器详细信息”屏幕上的“服务器设置”以执行高级服务器配置。
请参见第 195 页的“[高级服务器设置](#)”。
有关高级服务器配置的信息，请参见 Symantec Data Loss Prevention 联机帮助。
请参见第 176 页的“[服务器配置 - 基本](#)”。

删除服务器

有关从服务器卸载 Symantec Data Loss Prevention 的信息，请参见相应的《Symantec Data Loss Prevention 安装指南》。

在“系统”>“概述”屏幕上，Enforce Server 管理控制台列出了向其注册的检测服务器。如果已将 Symantec Data Loss Prevention 从检测服务器中卸载，或者该服务器已停止或与网络断开连接，则其状态在控制台上显示为“未知”。

可以从 Enforce Server 管理控制台删除（取消注册）检测服务器。从 Enforce Server 删除检测服务器后，其 Symantec Data Loss Prevention 服务会继续运行。这意味着即使从 Enforce 取消注册检测服务器，除非采取行动来停止它，否则它仍可以继续运行。换句话说，即使从 Enforce Server 管理控制台中删除检测服务器，它仍可以继续运行。它检测到的事件存储在检测服务器上。如果重新注册 Enforce Server 检测服务器，则会将已检测到并存储的事件转发给 Enforce。

从 Enforce 删除（取消注册）检测服务器

1 转至“系统”>“概述”。

请参见第 191 页的[“关于系统概述屏幕”](#)。

2 在屏幕的“服务器”部分，单击服务器状态行上的红色 X 以将其从该 Enforce Server 管理控制台中删除。

请参见第 175 页的[“服务器控件”](#)。

3 单击“确定”进行确认。

将服务器的状态行从“系统概述”列表中删除。

将 SSL 证书导入到 Enforce Server 或发现服务器

可将 SSL 证书导入 Enforce Server 或发现服务器上 Java 信任的 Keystore。SSL 证书可以自我签署（服务器），或由知名的证书颁发机构 (CA) 颁发。

您可能需要导入 SSL 证书来与 Active Directory (AD) 之类的外部服务器建立安全的连接。如果公认的权威机构已经签署了外部服务器的证书，则该证书将会自动添加到 Enforce Server 中。如果服务器证书为自我签署证书，则必须手动将其导入到 Enforce Server 或发现服务器。

表 12-2 将 SSL 证书导入 Enforce Server 或发现服务器

步骤	说明
1	复制您要导入到 Enforce Server 或发现服务器计算机的证书文件。
2	转到 Enforce Server 或发现服务器计算机上的目录 c:\Vontu\jre\bin。
3	<p>执行带有 -importcert 选项的 Keytool 实用程序，以将公共密钥证书导入到 Enforce Server 或发现服务器 Keystore 中：</p> <pre>keytool -importcert -alias new_endpointgroup_alias -keystore ..\lib\security\cacerts -file my-domaincontroller.crt</pre> <p>在此示例命令中，<i>new_endpointgroup_alias</i> 是分配给导入证书的新别名，而 <i>my-domaincontroller.crt</i> 是指向您证书的路径。</p>
4	<p>当您收到提示时，请输入 Keystore 的密码。</p> <p>默认情况下，该密码是 changeit。如果需要，可在出现提示时更改此密码。</p> <p>要更改此密码，请使用：keytool -storepassword -alias <i>new_endpointgroup_alias</i> -keystore ..\lib\security\cacerts</p>
5	当询问您是否信任此证书时，请回答“是”。

步骤	说明
6	重新启动 Enforce Server 或发现服务器。

请参见第 116 页的“[配置目录服务器连接](#)”。

关于系统概述屏幕

可通过“系统”>“服务器”>“概述”访问“系统概述”屏幕。该屏幕提供系统状态的快照，其中列出了有关 Enforce Server 和每个注册的检测服务器的信息。

“系统概述”屏幕提供下列功能：

- “添加服务器”按钮用于注册检测服务器。安装后首次查看该屏幕时，仅列出 Enforce Server。您必须使用“添加服务器”按钮注册各种检测服务器。注册检测服务器后，它们会在屏幕的“服务器”部分列出。
请参见第 187 页的“[添加检测服务器](#)”。
 - “升级”按钮用于将 Symantec Data Loss Prevention 升级到更新的版本。
请参见第 152 页的“[关于系统升级](#)”。
另请参见相应的《Symantec Data Loss Prevention 升级指南》。
 - 该屏幕的“服务器”部分显示有关每台服务器状态的摘要信息。也可用于删除（取消注册）服务器。
请参见第 191 页的“[服务器状态概述](#)”。
 - “最近的错误和警告事件”部分针对“服务器”部分中列出的任何服务器，显示最近的五个严重程度为错误或警告的事件。
请参见第 193 页的“[最近的错误和警告事件列表](#)”。
 - 该屏幕的“许可证”部分列出授予您使用权限的各个 Symantec Data Loss Prevention 产品。
请参见第 176 页的“[服务器配置 - 基本](#)”。
- 请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。

服务器状态概述

可以通过“系统”>“服务器”>“概述”访问“系统概述”屏幕的“服务器”部分。屏幕的此部分提供系统状态的快速概述。

表 12-3 服务器状态

图标	状态	说明
	正在启动	服务器正在启动。
	正在运行	服务器正常运行并且没有错误。
	正在运行所选的	服务器上的某些 Symantec Data Loss Prevention 进程已停止或出现错误。要查看各进程的状态，您必须先启用“系统设置”屏幕上的“高级进程控制”。 请参见第 174 页的“ 启用高级进程控制 ”。
	正在停止	服务器正处于停止 Symantec Data Loss Prevention 服务的过程中。 请参见第 69 页的“ 关于 Enforce Server 服务 ”。
	已停止	所有 Symantec Data Loss Prevention 进程都已停止。
	未知	服务器发生下列错误之一： <ul style="list-style-type: none">■ 从服务器不能访问 Enforce Server。■ Symantec Data Loss Prevention 没有安装在服务器上。■ 没有为 Enforce Server 配置许可证密钥。■ Windows 中的 Symantec Data Loss Prevention 帐户权限存在问题。

对于每台服务器，将显示下列附加信息。您也可以单击任意服务器名称以显示该服务器的“服务器详细信息”屏幕。

表 12-4 服务器状态附加信息

列名	说明
消息（最近 10 秒）	最近 10 秒处理的消息数目。
消息（今天）	今天上午 12 点后处理的消息数目。
事件（今天）	今天上午 12 点后处理的事件数目。 对于 Endpoint Server，“消息”和“事件”并不一致。这是因为正在端点处理消息，而不是在 Endpoint Server 处理。不过，事件数仍在增长。

列名	说明
事件队列	对于 Enforce Server，这是数据库中尚未分配状态的事件数目。只要生成此屏幕，就会更新该数目。 对于其他类型的服务器，这是尚未写入 Enforce Server 的事件数目。大约每隔 30 秒会更新一次该数目。如果服务器已关闭，该数目将是服务器更新的最新数目。事件可能仍在事件文件夹中。
消息等待时间	消息进入系统后，处理消息所花费的时间。此数据适用于处理的上个消息。如果处理上个消息的服务器处于断开状态，则该数据是 N/A。

查看有关服务器的详细信息

- ◆ 单击任意服务器名称以查看有关此服务器的其他详细信息。

请参见第 194 页的“[“服务器详细信息”屏幕](#)”。

从 Enforce Server 删除服务器

- ◆ 单击该服务器的红色 X，然后确认您的决定。

注意：删除（取消注册）服务器仅会将其与此 Enforce Server 服务器断开，不会使检测服务器停止运行。

请参见第 189 页的[“删除服务器”](#)。

最近的错误和警告事件列表

可以通过“系统”>“服务器”>“概述”访问“系统概述”屏幕的“最近的错误和警告事件”部分。屏幕的这一部分针对“服务器”部分中列出的任何服务器，显示最近的五个严重程度为错误或警告的事件。

表 12-5 最近的错误和警告事件信息

列名	说明
类型	  <p>黄色三角表示警告，红色圆圈表示错误。</p>
时间	事件发生的日期与时间。
服务器	发生事件的服务器的名称。

列名	说明
主机	服务器所在的计算机的 IP 地址或名称。服务器名称和主机名称可能相同。
代码	系统事件代码。“消息”列提供代码文本。可以按代码编号对事件列表进行过滤。
消息	与该事件代码相关联的错误或警告消息摘要。

- 要显示所有错误和警告事件的列表，请单击“显示全部”。
- 要显示“事件详细信息”屏幕以了解有关某特定事件的更多信息，请单击该事件。

请参见第 191 页的[“关于系统概述屏幕”](#)。

请参见第 126 页的[“系统事件报告”](#)。

请参见第 129 页的[“服务器事件详细信息”](#)。

“服务器详细信息”屏幕

“服务器详细信息”屏幕提供关于单个所选服务器的详细信息。“服务器详细信息”屏幕还用于控制和配置服务器。

显示特定服务器的“服务器详细信息”屏幕

- 1 导航至“系统”>“服务器”>“概述”屏幕。
- 2 单击“服务器概述”列表中的检测服务器名称。

请参见第 191 页的[“关于系统概述屏幕”](#)。

“服务器详细信息”屏幕分为几个部分。所有服务器类型均会显示以下列出的部分。系统将根据检测服务器类型显示相应部分。

表 12-6 “服务器详细信息”屏幕中的显示信息

“服务器详细信息”中的显示部分	说明
常规	<p>“常规”部分可标识服务器、显示系统状态和统计信息，并能控制服务器及其进程的启动和停止。</p> <p>请参见第 175 页的“服务器控件”。</p>

“服务器详细信息”中的显示部分	说明
配置	“配置”部分显示检测服务器的“通道”、“策略组”、“代理配置”、“用户设备”和“配置状态”。
代理摘要	“代理摘要”部分显示分配给 Endpoint Server 的所有代理的摘要。 单击“所有代理”可转至“系统”>“代理”>“概述”屏幕，然后查看每个代理的详细信息。 注意： 系统仅对 Endpoint Server 才显示“代理摘要”部分。
最近的错误和警告事件	“最近的错误和警告事件”部分显示五个最近在此服务器上发生的警告或严重事件。 单击事件可显示事件详细信息。单击“显示全部”可显示所有错误和警告事件。 请参见第 125 页的 “关于系统事件” 。
所有最近事件	“所有最近事件”部分显示在过去 24 小时内在此服务器上发生的所有严重性级别的所有事件。 单击事件可显示事件详细信息。单击“显示全部”可显示所有的检测服务器事件。
已部署的数据配置文件	“已部署的数据配置文件”部分列出了所有已部署到检测服务器的“确切数据”或“文档配置文件”。系统会显示配置文件的索引版本。 请参见第 312 页的 “关于数据配置文件” 。

请参见第 191 页的[“关于系统概述屏幕”](#)。

请参见第 176 页的[“服务器配置 - 基本”](#)。

请参见第 175 页的[“服务器控件”](#)。

请参见第 126 页的[“系统事件报告”](#)。

请参见第 129 页的[“服务器事件详细信息”](#)。

高级服务器设置

使用检测服务器的“系统”>“服务器”>“概述”>“服务器详细信息”屏幕的“服务器设置”选项卡可以修改该服务器上的设置。

修改服务器上的这些设置时请谨慎行事。建议更改此屏幕上的任何设置之前先与 Symantec 支持部门确认。对这些设置所做的更改通常会在重新启动服务器之后才生效。

Enforce Server 上没有可以从其服务器详细信息屏幕修改的高级设置。

表 12-7 检测服务器高级设置

设置	默认值	说明
BoxMonitor.Channels	可变	<p>这些值区分大小写且以逗号分隔（如果有多个值）。</p> <p>虽然可以配置这些值的任意组合，但正式支持的配置如下所示：</p> <ul style="list-style-type: none"> ■ Network Monitor Server：“数据包捕获、复制规则” ■ Discover Server：发现 ■ Endpoint Server：端点 ■ Network Prevent for Email：内联 SMTP ■ Network Prevent for Web：ICAP ■ 分类服务器：分类
BoxMonitor.DiskUsageError	90	已占用的磁盘空间量（以百分比表示）达到多少时，会触发严重系统事件。例如，如果 Symantec Data Loss Prevention 安装在 C 驱动器上，并且此值是 90，则 C 驱动器使用率超过 90% 时，检测服务器会创建严重系统事件。
BoxMonitor.DiskUsageWarning	80	已占用的磁盘空间量（以百分比表示）达到多少时，会触发警告系统事件。例如，如果 Symantec Data Loss Prevention 安装在 C 驱动器上，并且此值是 80，则 C 驱动器使用率超过 80% 时，检测服务器会生成警告系统事件。
BoxMonitor.EndpointServer	on	启用 Endpoint Server。
BoxMonitor.EndpointServerMemory		可以使用 JVM 内存标志的任意组合。例如： -Xrs -Xms300M -Xmx1024M
BoxMonitor.FileReader	on	如果设为 off，则虽然仍可手动启动 FileReader，但 BoxMonitor 无法启动 FileReader。

设置	默认值	说明
BoxMonitor.FileReaderMemory		FileReader JVM 命令行参数。例如： -Xrs -Xms1200M -Xmx1200M
BoxMonitor.HeartbeatGapBeforeRestart	960000	BoxMonitor 等待监控进程（例如 FileReader 和 IncidentWriter）报告心跳的时间间隔（毫秒）。如果在此时间间隔内未接收到心跳，BoxMonitor 将重新启动进程。
BoxMonitor.IncidentWriter	on	如果设为 off，则虽然仍可手动启动 IncidentWriter，但 BoxMonitor 无法在双层模式中启动 IncidentWriter。此设置在单层模式中不起作用。
BoxMonitor.IncidentWriterMemory		IncidentWriter JVM 命令行参数。例如： -Xrs
BoxMonitor.InitialRestartWaitTime	5000	
BoxMonitor.MaxRestartCount	3	
BoxMonitor.MaxRestartCountDuringStartup	5	Monitor Server 将尝试独自重新启动的次数上限。
BoxMonitor.PacketCapture	on	如果设为 off，则虽然仍可手动启动 PacketCapture，但 BoxMonitor 无法启动 PacketCapture。必须启用 PacketCapture 通道，此设置才起作用。
BoxMonitor.PacketCaptureDirectives		PacketCapture 命令行参数（在 Java 中）。例如： -Xrs
BoxMonitor.ProcessLaunchTimeout	30000	监控进程（例如 FileReader）启动的时间间隔（毫秒）。
BoxMonitor.ProcessShutdownTimeout	45000	分配给每个监控进程用于正常关闭的时间间隔（毫秒）。如果此时间之后进程仍在运行，则 BoxMonitor 会尝试终止该进程。
BoxMonitor.RequestProcessor	on	如果设为 off，则虽然仍可手动启动 RequestProcessor，但 BoxMonitor 无法启动 RequestProcessor。必须启用内联 SMTP 通道，此设置才起作用。
BoxMonitor.RequestProcessorMemory		可以使用 JVM 内存标志的任意组合。 例如： -Xrs -Xms300M -Xmx1300M

设置	默认值	说明
BoxMonitor.RmiConnectionTimeout	15000	允许用于建立 RMI 对象连接的时间间隔（毫秒）。
BoxMonitor.RmiRegistryPort	37329	BoxMonitor 启动 RMI 注册表的 TCP 端口。
BoxMonitor.StatisticsUpdatePeriod	10000	经过此时间间隔（毫秒）后，将更新监控统计信息。
Classification.BindAddress	0.0.0.0	分类服务器在其上接受要进行检测的消息的 IP 地址。默认情况下，分类服务器在所有接口 (0.0.0.0) 上进行侦听。如果您拥有一台多址服务器计算机并希望将分类请求限制在特定网络接口，请在此字段中输入该接口的 IP 地址。
Classification.MaxMemory	120M	分类服务器分配的最大内存大小。达到此限制后，对 Exchange 邮件的所有其他分类请求都将缓冲到磁盘，直到释放内存为止。
Classification.SessionReapInterval	20000	分类服务器在其后清除过时会话的时间间隔（毫秒）。
Classification.WbserviceLogRetentionDays	7	保留分类服务器 Web 服务请求日志的天数。这些日志文件存储在 c:\Vontu\Protect\logs\jetty (Windows) 或 /var/log/Vontu/logs/jetty (Linux) 下。
ContentExtraction.EnableMetaData	off	允许检测文件元数据。如果此设置设为 on ，则您可以检测 Microsoft Office 和 PDF 文件的元数据。对于 Microsoft Office 文件，支持 OLE 元数据，这种元数据包括“标题”、“主题”、“作者”和“关键字”字段。对于 PDF 文件，仅支持文档信息字典元数据，这种元数据包括诸如“作者”、“标题”、“主题”、“创建日期”和“更新日期”等字段。不对可扩展元数据平台 (XMP) 内容进行检测。请注意，启用此元数据检测选项可能会导致误报。

设置	默认值	说明
ContentExtraction.LongContentSize	1M	如果邮件组件超出此大小（字节），则使用 ContentExtraction.LongTimeout，而不使用 ContentExtraction.ShortTimeout。
ContentExtraction.LongTimeout	可变	此设置的默认值因检测服务器类型而异（ 60,000 或 120,000 ）。指定给 ContentExtractor 用于处理大于 ContentExtraction.LongContentSize 的文档的时间间隔（毫秒）。如果在此指定时间内无法处理文档，则会将该文档报告为未处理。此值应大于 ContentExtraction.ShortTimeout，且小于 ContentExtraction.RunawayTimeout。
ContentExtraction.MarkupAsText	off	忽略确定为 XML 或 HTML 的文件的内容提取。此设置应该用于诸如标头块或脚本块中包含数据的 Web 2.0 页面的情况。默认值为 off。
ContentExtraction.MaxContentSize	30M	ContentExtractor 可以处理的文档的大小上限 (MB)。
ContentExtraction.RunawayTimeout	300,000	指定给 ContentExtractor 用于完成任何文档处理的时间间隔（毫秒）。如果 ContentExtractor 在此时间内未完成某些文档的处理，则会被视为不稳定，并将重新启动。此值应远大于 ContentExtraction.LongTimeout。
ContentExtraction.ShortTimeout	30,000	指定给 ContentExtractor 用于处理小于 ContentExtraction.LongContentSize 的文档的时间间隔（毫秒）。如果在此指定时间内无法处理文档，则会将该文档报告为未处理。此值应小于 ContentExtraction.LongTimeout。

设置	默认值	说明
ContentExtraction.TrackedChanges	off	<p>允许检测 Microsoft Office 文档中随时间变化的内容（“修订”内容）。</p> <p>注意：使用上述选项可能会降低 IDM 和数据标识符的准确率。默认值设为“关闭”（不允许）。</p> <p>如果要为随时间变化的内容编制索引，请在 \Protect\config\Indexer.properties 文件中设置 ContentExtraction.TrackedChanges=on。默认的和建议的设置是 ContentExtraction.TrackedChanges=off。</p>
DDM.MaxBinMatchSize	300,000,000	<p>用于为 IDM 中的确切二进制匹配生成 MD5 哈希的大小上限（字节）。不应更改此设置。必须符合下列条件，IDM 才能正确运作：</p> <ul style="list-style-type: none"> ■ 1 - 此设置必须与 Enforce Server 上 indexer.properties 文件中的 max_bin_match_size 设置完全相同。 ■ 2 - 此设置必须小于或等于 FileReader.FileMaxSize 值。 ■ 3 - 此设置必须小于或等于 Enforce Server 上 indexer.properties 文件中的 ContentExtraction.MaxContentSize 值。 <p>注意：如果更改 1) 和/或 3)，需要对所有 IDM 文件重新编制索引。</p>
DDM.UseJavaMD5	false	如果设为 true，则使用第三方的库生成 MD5 哈希。如果设为 false，则使用 Java 的默认 MD5 库。一般不应更改此设置。
Detection.EncodingGuessingDefaultEncoding	ISO-8859-1	指定字节流所采用的备份编码。
Detection.EncodingGuessingEnabled	on	指定是否应猜测未知字节流的编码。
Detection.EncodingGuessingMinimumConfidence	50	指定猜测未知字节流编码所需的可信度。

设置	默认值	说明
DI.MaxViolations	100	指定允许的数据标识符违规次数上限。
Discover.CountAllFilteredItems	false	通过对文件夹中由于过滤而忽略的项目进行计数，可提供更多的准确扫描统计信息。要对所有项目进行计数，请将此设置设为 true 。
Discover.Exchange.FollowRedirects	false	指定是否遵循重定向。
Discover.Exchange.ScanHiddenItems	false	如果设为 true ，则会扫描 Exchange 存储库中的隐藏项目。
Discover.Exchange.UseSecureHttpConnections	true	指定在使用 Exchange Web 服务爬网时，与 Exchange 存储库和 Active Directory 的连接是否安全。
Discover.FileSystem.OnlyAutoDiscoverAdministrativeShares	false	指定文件系统扫描是将发现指定服务器上所有打开共享，还是仅发现与逻辑驱动器对应的管理共享，例如 C\$、D\$ 等。
Discover.IgnorePstMessageClasses	IPM.Appointment,IPM.Contact,IPM.Task,REPORT,IPM.Note,DR,REPORT,IPM.Note,IPNRN	此设置指定以逗号分隔的 .pst 邮件类别列表。将忽略 .pst 文件中具有列表中邮件类别的所有项目（不会尝试提取 .pst 项目）。此设置区分大小写。
Discover.IncludePstMessageClasses	IPM.Note	此设置指定以逗号分隔的 .pst 邮件类别列表。将包括 .pst 文件中具有列表中邮件类别的所有项目。 如果包括设置和忽略设置均已定义，则 Discover.IncludePstMessageClasses 的优先级更高。
Discover.PollInterval	10000	指定在扫描时，Enforce 从发现监视器检索数据的时间间隔（毫秒）。
Discover.Sharepoint.FetchACL	true	关闭集成 SharePoint 扫描的 ACL 提取功能。默认值为 true （打开）。

设置	默认值	说明
Discover.ValidateSSLCertificates	false	<p>如果设为 true，可启用对 SharePoint 和 Exchange 目标之间 HTTPS 连接的 SSL 证书的验证。启用验证后，将无法使用自我签署或非信任证书扫描 SharePoint 或 Exchange 服务器。如果 SharePoint Web 应用程序或 Exchange 服务器已经过证书颁发机构(CA)颁发的证书签署，则服务器证书或服务器 CA 证书必须位于发现服务器所使用的 Java 信任 keystore 中。如果证书没有位于 keystore 中，则必须使用 keytool 实用程序手动将其导入。</p> <p>请参见第 190 页的“将 SSL 证书导入到 Enforce Server 或发现服务器”。</p>
EDM.MatchCountVariant	3	<p>指定如何对匹配项计数。</p> <ul style="list-style-type: none"> ■ 1 - 对匹配的数据行进行计数，无视多个匹配项使用相同令牌的情况 ■ 2 - 清除包括同组令牌的匹配项 ■ 3 - 清除由其他某些匹配项所用令牌子集组成的匹配项（默认） <p>请参见第 359 页的“配置确切数据匹配计数”。</p>
EDM.MaximumNumberOfMatchesToReturn	100	定义从每个 RAM 索引搜索返回匹配项的数量的最高限制。如果是多文件索引，则在组合搜索结果之前，会将此限制独立应用于每个子索引搜索。因此，对于多文件索引，实际匹配项的数量可能超出此限制。
EDM.RunProximityLogic	true	如果设为 true，则运行令牌邻近检查。自由形式（又称简单）文本邻近由 EDM.SimpleTextProximityRadius 设置定义。通过属于同一表格行来定义表格文本邻近。
EDM.SimpleTextProximityRadius	35	启用邻近检查时，到当前令牌的左侧及右侧的一起进行评估的令牌数。
EDM.VerifyJohnJohnCases	true	指定是否考虑多个数据库列具有相同值的匹配项。例如，名字和姓氏均为 John。此验证对性能有轻微的不利影响。

设置	默认值	说明
EndpointMessageStatistics.MaxFileDetectionCount	100	扫描有效文件的次数上限。文件不得导致事件。如果超过此数目，则会生成系统事件，建议滤除该文件。
EndpointMessageStatistics.MaxFolderDetectionCount	1800	扫描有效文件夹的次数上限。文件夹不得导致事件。如果超过此数目，则会生成系统事件，建议滤除该文件。
EndpointMessageStatistics.MaxMessageCount	2000	扫描有效邮件的次数上限。邮件不得导致事件。如果超过此数目，则会生成系统事件，建议滤除该文件。
EndpointMessageStatistics.MaxSetSize	3	所显示主机（有效文件、文件夹及邮件的来源）列表的数目上限。生成 EndpointMessageStatistics.MaxFileDetectionCount、EndpointMessageStatistics.MaxFolderDetectionCount 或 EndpointMessageStatistics.MaxMessageCount 的系统事件时，Symantec Data Loss Prevention 会列出生成这些系统事件的主机。此设置可限制列表中显示的主机数量。
EndpointServer.Discover.ScanStatusBatchInterval	10000	在将扫描状态成批发送给 MonitorController 之前，聚合器累积扫描状态的时间间隔（毫秒）。
EndpointServer.EndpointSystemEventQueueSize	20000	可以存储在端点代理的队列中以发送到 Endpoint Server 的最大系统事件数。如果数据库连接中断，或出现某些其他情况导致产生大量系统事件，则会丢弃在达到此数目后发生的所有其他系统事件。可以根据内存要求调整此值。
EndpointServer.MaxPercentageMemToStoreEndpointFiles	60	用于存储阴影高速缓存文件的内存数量上限（百分比）。
EndpointServer.MaxTimeToKeepEndpointFilesOpen	20000	端点文件保持打开状态或文件大小可以超出 EndpointServer.MaxEndpointFileSize 设置（两者中先发生的一项）的时间间隔（分钟）。
EndpointServer.MaxTimeToWaitForWriter	1000	代理等待连接到服务器的时间上限（毫秒）。
EndpointServer.NoOfRecievers	15	端点阴影高速缓存文件接受者的数量。

设置	默认值	说明
EndpointServer.NoOfWriters	10	端点阴影高速缓存文件写入者的数量。
FileReader.MaxValue	30M	要处理的消息的大小上限(MB)。会将更大的消息截短为此大小。
FileReader.MaxValueSystemCrawlerMemory	30M	为文件系统爬网程序分配的内存上限。如果此值小于.FileReader.MaxValue，则会分配两者中较大的值。
FileReader.MaxReadGap	15	子进程在停止发送心跳之前可以具有数据但不具有读取任何数据的时间。
FileReader.ScheduledInterval	1000	filereader 执行放置文件夹检查的时间间隔(毫秒)。此设置仅影响复制规则、数据包捕获和文件系统通道。
Icap.AllowHosts	any	默认值 any 允许所有系统在 ICAP 服务端口连接到 Network Prevent for Web Server。将 any 替换为一个或多个系统的 IP 地址或完全限定的域名(FQDN)会将 ICAP 链接仅限于这些指定的系统。要指定多个系统，请使用逗号分隔其 IP 地址或 FQDN。
Icap.AllowStreaming	false	如果设为 true，则 ICAP 输出将直接流入代理，而不会先缓冲 ICAP 请求。NetApp NetCache 6.0 不支持此类流动。
Icap.BindAddress	0.0.0.0	Network Prevent for Web Server 倾听绑定的 IP 地址。配置 BindAddress 时，服务器将只回答该 IP 地址的连接。默认值 0.0.0.0 是通配符，允许倾听所有可用地址(包括 127.0.0.1)。
Icap.BufferSize	3K	ICAP 请求流动和分块所使用的内存缓冲区的大小(千字节)。只有在请求大于.FileReader.MaxValue，且请求具有内容-长度标题时，才会发生流动。
Icap.DisableHealthCheck	false	如果设为 true，则会禁用 ICAP 定期自检。如果设为 false，则会启用 ICAP 定期自检。此设置对于进行调试，以便从日志删除自检请求产生的杂乱内容非常有用。

设置	默认值	说明
Icap.EnableIncidentSuppression	true	如果此参数设置为 true，则会对 Mobile Prevent for Web 上的 Gmail 通信启用事件禁止显示缓存。如果此参数设置为 false，则禁用禁止显示。
Icap.EnableTrace	false	如果设为 true，则在使用 Icap.TraceFolder 设置指定文件夹后，会启用协议调试跟踪。
Icap.ExchangeActiveSyncCommandsToInspect	SendMail	需通过 Symantec Data Loss Prevention 检测发送的 ActiveSync 命令的列表，各命令间用逗号分隔且命令区分大小写。如果此参数留空，则禁用 ActiveSync 支持。如果此参数设置为 any，则会检查所有 ActiveSync 命令。
Icap.LoadBalanceFactor	1	Network Prevent for Web Server 可进行通信的 Web 代理服务器的数量。例如，如果将服务器配置为与 3 个代理进行通信，请将 Icap.LoadBalanceFactor 值设为 3。
Icap.IncidentSuppressionCacheCleanupInterval	120000	运行事件禁止显示缓存清理线程的时间间隔（以毫秒为单位）。
Icap.IncidentSuppressionCacheTimeout	120000	以毫秒为单位表示的时间，经过此时间后事件禁止显示缓存条目就会变得无效。
Icap.SpoolFolder		ICAP 缓冲需要此值。从 Vontu DLP 5.0 U3 更新到 6.0 GA 时，必须将此设置设为正确的驱动器盘符，否则 FileReader 将不会启动。
Icap.TraceFolder		将 Icap.EnableTrace 设置设为 true 时，存储协议调试跟踪数据的文件夹或目录的完全限定名称。默认情况下，此设置的值留空。
IncidentDetection.IncidentLimitResetTime	86400000	指定 IncidentDetection.MaxIncidentsPerPolicy 设置所使用的时段（毫秒）。默认设置 86400000 等于一天。

设置	默认值	说明
IncidentDetection.MaxContentLength	2000000	仅适用于正则表达式规则。对于每个组件，只会扫描第一个 MaxContentLength 数量的字符是否违规。默认值 (2,000,000) 相当于超过 1000 页的典型文本。存在该限制以防止正则表达式规则耗时过长。
IncidentDetection.MaxIncidentsPerPolicy	10000	定义在 IncidentDetection.IncidentTimeLimitResetTime 中指定的时段内，特定策略于特定监控上检测到的事件数的上限。默认值为每个时间限制内每个策略 10,000 个事件。
IncidentDetection.MessageWaitSevere	240	发送有关消息等待时间的严重系统事件之前等待的分钟数。
IncidentDetection.MessageWaitWarning	60	发送有关消息等待时间的警告系统事件之前等待的分钟数。
IncidentDetection.MinNormalizedSize	30	此设置适用于 IDM 检测。它必须与 Enforce Server 上 Indexer.properties 文件中的对应设置（适用于编制索引）保持同步。派生的检测仅适用于规范化内容大于此设置时的消息。如果规范化内容的大小小于此设置，则 IDM 检测会执行标准二进制匹配。
IncidentDetection.patternConditionMaxViolations	100	检测突出显示的模式违规数目上限。在报告时，匹配项的确切数目可能仍是“正确”的，但仅对第一个 patternConditionMaxViolations 进行标记。如果增大此数目，则会增大事件的大小，并可能降低事件快照报告的速度。

设置	默认值	说明
IncidentDetection.StopCachingWhenMemoryLowerThan	400M	如果可用JVM内存降至此值之下（兆字节），则指示检测在执行规则的间歇停止缓存已标记化和加密的内容。如果将此属性设为0，则无论可用内存有多少，均可启用缓存，但不建议如此设置，因为可能会发生 OutOfMemoryErrors。 将此属性设为接近或大于 BoxMonitor.FileReaderMemory 中 -Xmx 选项的值可以有效禁用缓存。 请注意，将此值设置得太低可能会对性能产生严重影响。
IncidentDetection.TrialMode	false	通过设置阻止试用模式，可在未设置阻止的情况下生成阻止事件。 如果设为 true，则来自“复制规则”和“数据包捕获”通道的 SMTP 事件显示为似乎已遭到阻止，来自“数据包捕获”通道的 HTTP 事件显示为似乎已遭到阻止。
IncidentWriter.BacklogInfo	1000	生成关于消息数量的信息等级消息之前，日志中收集的事件数目。
IncidentWriter.BacklogSevere	10000	生成关于消息数量的严重等级消息之前，日志中收集的事件数目。
IncidentWriter.BacklogWarning	3000	生成关于消息数量的警告等级消息之前，日志中收集的事件数目。
IncidentWriter.ResolveIncidentDNSNames	false	如果设为 true，则只会从 IP 解析接受者主机名称。
IncidentWriter.ShouldEncryptContent	true	如果设为 true，则监控会在写入磁盘或发送到 Enforce 之前，先加密每封邮件、邮件组件以及已破解组件的正文。
L7.cleanHttpBody	true	如果设为 true，则会使用空格替换 HTML 实体引用。

设置	默认值	说明
L7.DefaultBATV	Standard	此设置可确定 Network Prevent for Email 用于解释邮件的“邮件发件人”标题中的“退回地址标记验证(BATV)”标记的标记方案。如果此设置为“标准”（默认值），Network Prevent 将使用 BATV 规范中所述的标记方案（请参见 http://tools.ietf.org/html/draft-levine-mass-batv-02 ）。如果将此设置更改为 Ironport，则可以与 IronPort 代理的 BATV 标记实施兼容。
L7.DefaultUrlEncodedCharset	UTF-8	定义在标头中缺失字符集信息时要在解码查询参数或 URL 编码的正文中使用的默认字符集。
L7.discardDuplicateMessages	true	如果设为 true，则监控会根据 messageID 忽略重复的消息。
L7.ExtractBATV	true	如果设为 true（默认值），Network Prevent for Email 将解释存在于邮件的“邮件发件人”标题中的“退回地址标记验证(BATV)”标记。这允许 Network Prevent 包括从具有 BATV 标记的邮件中生成的事件中某个有意义的发件人地址。如果此设置为 false，Network Prevent for Email 将不解释 BATV 标记，且包含 BATV 标记的邮件可能会生成具有无法读取的发件人地址的事件。 请参见 http://tools.ietf.org/html/draft-levine-mass-batv-02 以获取更多有关 BATV 的信息。
L7.httpClientIdHeader		发送者标识符标题名称。默认设置为 X-Forwarded-For 。
L7.MAX_NUM_HTTP_HEADERS	30	如果任何 HTTP 消息包含的标题行多于指定数量，则会丢弃该消息。
L7.maxWordLength	30	UTCP 字符串提取中允许的文字长度上限（字符）。

设置	默认值	说明
L7.messageIDCacheCleanupInterval	600000	缓存 messageID 的时间长度。如果 L7.discardDuplicateMessages 设置设为 true，则在此时间段内，系统不会缓存重复消息。
L7.minSizeOfGetUrl	100	要处理的 GET URL 大小的下限。如果 URL 的字节数小于此设置的值，则 Symantec Data Loss Prevention 不会检查 HTTP GET 操作是否违反策略。例如，如果使用默认值 100，则在浏览器显示 Symantec 网站（位于 http://www.symantec.com/index.jsp ）时，系统不会执行任何检测检查。原因在于该 URL 仅包含 33 个字符，小于下限 100。 注意： L7.minSizeofGetURL 不影响其他请求类型（例如 POST 或 PUT）。要让 Symantec Data Loss Prevention 检查所有 GET 操作，必须将 L7.processGets 设置设为 true。
L7.processGets	true	如果设为 true，则会处理 GET 请求。如果设为 false，则不会处理 GET 请求。请注意，此设置与 L7.minSizeofGetURL 设置相互作用。
Lexer.AllowCommasWithOtherSeparatorInTabular	true	
Lexer.IncludeLinesWithOnlyWordsInTabular	false	如果设为 true，则会将仅由单词构成的行识别为表格数据。
Lexer.IncludePostalCodeInMultiWord	true	如果设为 true，则会将邮政编码包括在表格文本的由多个单词构成的列中。
Lexer.IncludePunctuationInWords	true	如果设为 true，则会将标点符号视为单词的一部分。
Lexer.MaximumNumberOfTokens	30000	从每个邮件组件中提取的进行检测的令牌（包括分隔符）数目上限。适用于需要使用令牌化过程的所有检测技术（例如系统模式、EDM、DGM）。增大此值可能会造成检测耗尽内存并重新启动。默认值是 30,000。
Lexer.MultiWordRecognition	true	如果设为 true，则会识别表格数据中由多个单词组成的列。

设置	默认值	说明
Lexer.StopwordLanguages	en	可以清除指定语言的停用词。默认设置为“英语”。
Lexer.Validate	true	如果设为 true，则会执行系统模式特定验证。
MessageChain.ArchiveTimedOutStreams	false	指定是否应将消息存档到temp文件夹。
MessageChain.CacheSize	8	限制可以在消息链中排队的消息数量。
MessageChain.ContentDumpEnabled	false	
MessageChain.MaximumComponentTime	60,000	重新启动任何链组件之前允许的时间间隔（毫秒）。
MessageChain.MaximumFailureTime	360000	重新启动 filereader 前必须经历的毫秒数。此时间是在检测到邮件链错误但尚未对其进行恢复时跟踪的。
MessageChain.MaximumMessageTime	可变	此设置可以在 600,000 和 1,800,000 之间变化，具体取决于检测服务器类型。消息可以保留在消息链中的时间间隔上限（毫秒）。
MessageChain.MemoryThrottlerReservedBytes	200,000,000	在通过邮件链发送邮件之前需要使用的字节数。此设置可避免发生内存不足的问题。默认值为 200 MB。将此值设置为零可禁用此限制机制。
MessageChain.MinimumFailureTime	30000	在跟踪出现故障的邮件链之前必须经历的毫秒数。故障最终会导致重新启动邮件链或文件读取器。
MessageChain.NumChains	可变	此数字因检测服务器类型而异。它可以为 4 或 8 。 filereader 将并行处理的消息数量。建议不要将其设为大于 8 的数（和其他默认设置配合使用）。设置为更大的数不会大幅度地提升性能，反而会大幅提升耗尽内存的风险。将此值设为小于 8 的数（在某些情况下 1）对于处理大型文件的情况会很有帮助，但会使系统的速度锐减。

设置	默认值	说明
MessageChain.StopProcessingWhenMemoryLowerThan	200M	如果JVM可用内存降至此值之下，则指示检测停止进一步处理子文件。如果将此属性设为 0，则无论可用内存多小，都会强制进行子文件处理。将此属性设为接近或大于 BoxMonitor.FileReaderMemory 中 -Xmx 选项的值，将有效禁用子文件处理操作。
PacketCapture.DISCARD_HTTP_GET	true	如果设为 true，则会丢弃 HTTP GET 流。
PacketCapture.DOES_DISCARD_TRIGGER_STREAM_DUMP	false	如果设为 true，则在第一次接收丢弃消息时，会将 tcpstreams 列表转储到日志目录中的输出文件。
PacketCapture.ENDACE_BIN_PATH		要使用 Endace 卡启用数据包捕获，请输入 Endace/bin 目录的路径。请注意，环境变量（例如 %ENDACE_HOME%）无法用于此设置。例如：/usr/local/bin
PacketCapture.ENDACE_LIB_PATH		要使用 Endace 卡启用数据包捕获，请输入 Endace/lib 目录的路径。请注意，环境变量（例如 %ENDACE_HOME%）无法用于此设置。例如：/usr/local/lib
PacketCapture.ENDACE_XILINX_PATH		要使用 Endace 卡启用数据包捕获，请输入 Endace/xilinx 目录的路径。请注意，环境变量（例如 %ENDACE_HOME%）无法用于此设置。例如：/usr/local/dag/xilinx
PacketCapture.Filter		默认设置为 tcp ip proto 47 (vlan && (tcp ip proto 47)) 。 如果设为默认值，则会滤除所有非 TCP 数据包，不会将其发送到 Network Monitor。可以使用 tcpdump 程序中记录的 tcpdump 过滤器格式覆盖此默认值。此设置允许专家创建更加精确的过滤器（指定端口的源 IP 和目标 IP）。
PacketCapture.INPUT_SOURCE_FILE	/dummy.dmp	输入文件的完整路径和名称。

设置	默认值	说明
PacketCapture.IS_ARCHIVING_PACKETS	false	请勿使用此字段。诊断设置，可创建 packetcapture 中所捕获数据包的转储以供稍后重复使用。此功能不受支持，且不包括正常错误检查。可能会导致重复地重新启动 pcap。
PacketCapture.IS_ENDACE_ENABLED	false	要使用 Endace 卡启用数据包捕获，请将此值设为 true。
PacketCapture.IS_FTP_RETR_ENABLED	false	如果设为 true，则会处理 FTP GETS 和 FTP PUTS。如果设为 false，则仅会处理 FTP PUTS。
PacketCapture.IS_INPUT_SOURCE_FILE	false	如果设为 true，则会从 INPUT_SOURCE_FILE 所指示的 tcpdump 格式文件中持续读取数据包。安装 Endace 卡时，请设为 DAG。
PacketCapture.IS_NAPATECH_ENABLED	false	要使用 Napatech 卡启用数据包捕获，请将此值设置为 true。默认设置为 false。
PacketCapture.KERNEL_BUFFER_SIZE_I686	64M	对于 32 位 Linux 平台，此设置指定所分配的用于缓冲网络数据包的内存大小。指定以 K 表示 kilobytes (千字节)，以 M 表示 megabytes (兆字节)。请勿指定大于 128M 的值。
PacketCapture.KERNEL_BUFFER_SIZE_Win32	16M	对于 32 位 Windows 平台，此设置指定所分配的用于缓冲网络数据包的内存大小。指定以 K 表示 kilobytes (千字节)，以 M 表示 megabytes (兆字节)。
PacketCapture.KERNEL_BUFFER_SIZE_X64	64M	对于 64 位 Windows 平台，此设置指定所分配的用于缓冲网络数据包的内存大小。指定以 K 表示 kilobytes (千字节)，以 M 表示 megabytes (兆字节)。
PacketCapture.KERNEL_BUFFER_SIZE_X86_64	64M	对于 64 位 Linux 平台，此设置指定所分配的用于缓冲网络数据包的内存大小。指定以 K 表示 kilobytes (千字节)，以 M 表示 megabytes (兆字节)。请勿指定大于 64M 的值。

设置	默认值	说明
PacketCapture.MAX_FILES_PER_DIRECTORY	30000	处理指定数量的文件流后，创建新目录。
PacketCapture.MBYTES_LEFT_TO_DISABLE_CAPTURE	1000	如果 drop_pcap 驱动器上的剩余磁盘空间量 (MB) 低于此指定值，则会挂起数据包捕获。例如，如果此数是 100，则所安装驱动器上的剩余空间小于 100 MB 时，pcap 将停止写出 drop_pcap 文件。
PacketCapture.MBYTES_REQUIRED_TO_RESTART_CAPTURE	1500	表示由于缺乏空间而停止数据包捕获之后，drop_pcap 驱动器需要有多少磁盘空间 (MB)，捕获才会继续进行。例如，如果此值为 150 且数据包捕获已挂起，则在 drop_pcap 驱动器上的可用空间多于 150 MB 时，数据包捕获会继续进行。
PacketCapture.NAPATECH_TOOLS_PATH		此设置指定 Napatech 工具目录的位置。默认情况下，未设置此目录。如果对 Napatech 启用了数据包捕获，请输入 Napatech 工具安装目录的完全限定路径。
PacketCapture.NO_TRAFFIC_ALERT_PERIOD	86,400	两次无流量警报消息之间的刷新时间 (秒)。会根据此时间段为指定协议创建无流量系统事件。例如，如果将其设为 24*60*60 秒，则会每天发送一次表示无指定协议新流量的新消息。请勿将其与每协议流量超时混淆，后者表示最初多长时间无流量才会发送第一个警报。
PacketCapture.NUMBER_BUFFER_POOL_PACKETS	600000	将传入的流量置入缓冲区和进行排序时，所使用的具有标准大小且预先分配的数据包缓冲区的数量。
PacketCapture.NUMBER_JUMBO_POOL_PACKETS	1	将传入的流量置入缓冲区和进行排序时，所使用的大型且预先分配的数据包缓冲区的数量。
PacketCapture.NUMBER_SMALL_POOL_PACKETS	200000	将传入的流量置入缓冲区和进行排序时，所使用的小型且预先分配的数据包缓冲区的数量。

设置	默认值	说明
PacketCapture.RING_CAPTURE_LENGTH	1518	控制所捕获数据包数据的量。默认值 1518 足以用于捕获典型以太网网络和通过 802.1Q 所标记 VLAN 的以太网。
PacketCapture.RING_DEVICE_MEM	67108864	该设置已弃用。现在使用的是 PacketCapture.KERNEL_BUFFER_SIZE_I686 设置（对于 32 位 Linux 平台）或 PacketCapture.KERNEL_BUFFER_SIZE_X86_64 设置（对于 64 位 Linux 平台）。 指定根据设备要分配给缓冲区数据包的内存数量（字节）。（默认值 67108864 等同于 64MB。）
PacketCapture.SIZE_BUFFER_POOL_PACKETS	1540	标准大小缓冲池数据包的大小。
PacketCapture.SIZE_JUMBO_POOL_PACKETS	10000	大型缓冲池数据包的大小。
PacketCapture.SIZE_SMALL_POOL_PACKETS	150	小型缓冲池数据包的大小。
PacketCapture.SPOOL_DIRECTORY		对具有大量数据包的流进行缓冲的目录。此设置是用户定义的。
PacketCapture.STREAM_WRITE_TIMEOUT	5000	每次计数（StreamManager 的写入超时）之间的时间（毫秒）。
ProfileIndex.CheckAvailableRAM	true	指定载入 EDM 或 IDM 配置文件之前，是否应将可用 RAM 的数量与配置文件大小进行比较。如果是单层安装，请设为 false，否则无法编制 EDM 文件的索引。
ProfileIndex.MaximumInProcessIndexSize	100M	指定“进行中”索引最大大小的上限。超出此大小的配置文件由 RMI 在进程外载入。
ProfileIndex.MinimumMemoryReserve	200M	指定为执行进程外 EDM 和/或 IDM 算法而保留的内存大小。此设置用于按照 <code>index_size + MinimumMemoryReserve</code> 计算 JVM 堆大小。受 IDM（从 v7 开始）和 EDM（从 v8 开始）支持。
ProfileIndex.ProcessTimeout	10000	启动进程外编制索引的时间间隔（毫秒）。如果在此时间长度内未创建进程，则索引加载将失败。

设置	默认值	说明
RequestProcessor.AddDefaultHeader	true	如果设为 true，则会将默认标题添加到所处理的每封电子邮件（处于内联 SMTP 模式时）。默认标题是 RequestProcessor.DefaultHeader。会将此标题添加到通过系统的所有邮件，即如果将其重定向，如果添加其他标题，如果邮件没有违反策略，则会添加此标题。
RequestProcessor.AllowExtensions		默认设置为： 8BITMIME VRFY DSN HELP PIPELINING SIZE ENHANCEDSTATUSCODES STARTTLS 此设置列出了 Network Prevent for Email 与其他 MTA 进行通信时可以使用的 SMTP 协议扩展。
RequestProcessor.AllowHosts	any	默认值 any 允许所有系统在 SMTP 服务端口连接到 Network Prevent for Email Server。将 any 替换为一个或多个系统的 IP 地址或完全限定的域名 (FQDN) 会将 SMTP 链接仅限于这些指定的系统。要指定多个系统，请使用逗号分隔它们的地址。请仅使用逗号来分隔地址，不要在地址之间包含任何空格。
RequestProcessor.AllowUnauthenticatedConnections	false	此默认值可确保 MTA 必须通过 Network Prevent for Email 验证，以进行 TLS 通信。
RequestProcessor.Backlog	12	请求处理器为服务器套接字侦听程序指定的积压。
Requestprocessor.BindAddress	0.0.0.0	Network Prevent for Email Server 侦听绑定的 IP 地址。配置 BindAddress 时，服务器将只回答该 IP 地址的连接。默认值 0.0.0.0 是通配符，允许侦听所有可用地址（包括 127.0.0.1）。
Requestprocessor.DefaultCommandTimeout	300	指定关闭上游和下游 MTA 的连接之前，Network Prevent for Email Server 等待 SMTP 命令响应的秒数。默认值为 300 秒。此设置不适用于 . 命令 (DATA 命令的结尾)。如果没有先咨询 Symantec 支持部门，请勿修改默认值。

设置	默认值	说明
Requestprocessor.DefaultPassHeader		默认设置为： X-C Filter-Loop: Reflected 。 这是默认的标题，如果将 RequestProcessor.AddDefaultPassHeader 设为 true，将添加此标题（处于内联 SMTP 模式时）。标题格式必须有效，建议使用 X 标题。
Requestprocessor.DotCommandTimeout	600	指定关闭上游和下游 MTA 的连接之前，Network Prevent for Email Server 等待“.”命令（DATA 命令的结尾）响应的秒数。默认值为 600 秒。如果没有先咨询 Symantec 支持部门，请勿修改默认值。
RequestProcessor.ForwardConnectionTimeout	20000	转发到 MTA 时使用的超时值。
RequestProcessor.KeyManagementAlgorithm	SunX509	用于 TLS 通信的密钥管理算法。
RequestProcessor.MaxLineSize	1048576	外部 MTA 所预期的数据行大小上限（字节）。如果数据行大于此值，则会将其截短为此大小。
RequestProcessor.Mode	ESMTP	指定要使用的协议模式（SMTP 或 ESMTP）。
RequestProcessor.MTAResubmitPort	10026	这是 MTA 上的请求处理器重新发送 SMTP 邮件所使用的端口号。
RequestProcessor.NumberOfDNSAttempts	4	Network Prevent for Email 在尝试获取域的邮件交换（MX）记录时执行的最大 DNS 查询数。仅当启用 MX 记录查找后，Network Prevent for Email 才会使用此设置。
RequestProcessor.RPLTimeout	360000	允许 Prevent Server 进行电子邮件处理的时间上限（毫秒）。服务器会传递此时间间隔内未处理的所有电子邮件。
RequestProcessor.ServerSocketPort	10025	SMTP 监控侦听来自 MTA 的传入连接所使用的端口号。

设置	默认值	说明
RequestProcessor.TagHighestSeverity	false	设为 true 时，会在邮件中添加附加电子邮件标题，该标题可报告所有违反的策略的最高严重性。例如，如果电子邮件违反了严重性为“高”的策略和严重性为“低”的策略，则附加标题显示为：X-DLP-MAX-Severity:HIGH。
RequestProcessor.TagPolicyCount。	false	设为 true 时，会在邮件中添加附加电子邮件标题，该标题可报告邮件所违反策略的总数。例如，如果邮件违反 3 个策略，则添加的附加标题为：X-DLP-Policy-Count: 3。
RequestProcessor.TagScore	false	设为 true 时，会在邮件中添加附加电子邮件标题，该标题可报告邮件所违反所有策略的累计总分。使用以下公式计算分数：高=4，中=3，低=2，信息=1。例如，如果邮件违反了三项策略，其中一个的严重性为中，其他两个的严重性为低，则添加的附加标题为：X-DLP-Score: 7。
RequestProcessor.TrustManagementAlgorithm	PKIX	Network Prevent for Email 验证 TLS 通信的证书时所使用的信任管理算法。您可以选择指定内置的 Java 信任管理器算法（例如 SunX509 或 SunPKIX）或已开发的自定义算法。
RequestProcessorListener.ServerSocketPort	12355	FileReader 倾听来自 Network Prevent Server 上请求处理器的连接使用的本地 TCP 端口。
SocketCommunication.BufferSize	8K	Network Prevent for Web 用于处理 ICAP 请求的缓冲区的大小。仅在需要处理大于 8K 的 ICAP 请求时，才能增加默认值。某些功能（如 Active Directory 身份验证）可能要求增加缓冲区大小。
UnicodeNormalizer.AsiCharRanges	default	可用于覆盖检测引擎视为亚洲字符的字符的默认定义。必须为默认值或范围列表（以逗号分隔），例如：11A80-11F9,3200-321E
UnicodeNormalizer.Enabled	on	可用于禁用 Unicode 规范化。输入 off 可禁用此项。

设置	默认值	说明
UnicodeNormalizer.NewLineEliminationEnabled	on	可用于针对亚洲语言禁用换行符清除操作。 输入 off 可禁用此项。

请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。

请参见第 218 页的“[高级代理设置](#)”。

请参见第 191 页的“[关于系统概述屏幕](#)”。

请参见第 194 页的“[服务器详细信息”屏幕](#)”。

请参见第 176 页的“[服务器配置 - 基本](#)”。

请参见第 175 页的“[服务器控件](#)”。

高级代理设置

下列设置仅影响 Symantec DLP Agent。在没有 Symantec 支持部门帮助的情况下，不应修改这些设置。如果要对此服务器详细信息页面进行修改，请先联系 Symantec 支持部门，再做更改。

[表 12-8 提供了服务器设置列表及每个设置的默认值和说明。](#)

表 12-8 代理高级设置

设置名称	默认值	说明
AgentManagementDISABLE_ENABLE_TASK_TIMEOUT_SECONDS.int	300	在发送“需要重新启动代理”系统事件之前，“禁用”或“启用”代理故障排除任务所等待的时间（秒）。

设置名称	默认值	说明
AgentTamperProtection.ENABLE_AGENT_TAMPER_PROTECTION.int	7	<p>此设置将对 Symantec Data Loss Prevention 端点代理启用防篡改。</p> <p>设置为 0 时将禁用所有防篡改。</p> <p>设置为 1 时可阻止删除或修改代理和 Watchdog 文件。</p> <p>设置为 2 时可阻止停止代理和 Watchdog 服务。</p> <p>设置为 4 时可阻止从操作系统注册表中删除代理和 Watchdog 服务。</p> <p>设置为 7 时将启用文件、服务和注册表防护。</p>
AgentThreadPool.IDLE_TIME_IN_SECONDS.int	60	在从线程池删除某线程之前，该线程可以处于非活动状态的最长时间。线程也称为代理任务。
AgentThreadPool.MAX_CAPACITY.int	20	线程池中的最大线程数。线程可以处于活动或非活动状态。
AgentThreadPool.MIN_CAPACITY.int	2	线程池中所允许的最小线程数。线程池必须始终包含此数量的线程。线程可以处于活动或非活动状态。
ApplicationConnector.KEY_LENGTH.int	64	密钥的长度（字节），用于对代理与应用程序钩子之间的通信进行模糊处理。
ApplicationConnector.MAX_CONNECTIONS.int	255	可同时连接到代理的最大应用程序钩子数（按钩子类型）。
ApplicationConnector.TEMPORARY_DIRECTORY.str	%TMP%	应用程序钩子存储经过模糊处理的内容的临时位置。
ComponentLoaderSettings.MAX_COMPONENT_SHUTDOWN_TIME.int	60000	代理等待组件关闭的最长时间（毫秒）。
ComponentLoaderSettings.PROCESS_PRIORITY.str	NORMAL	优先级，即指明 Symantec DLP Agent 在端点计算机上运行的优先级。

设置名称	默认值	说明
CrashDump.ENABLE_CRASH_DUMP_COLLECTION.int	1	该设置允许系统在 Symantec DLP Agent 崩溃时创建转储文件。将此值设置为 1 将启用创建崩溃转储文件的功能。将此值设置为 0 将禁用该文件。
CrashDump.MAX_DAYS_TO_KEEP_DUMP.int	2	崩溃转储文件存储的最长时间（天）。
CrashDump.MAX_NUMBER_OF_FILES_IN_DUMP_FOLDER.int	1	在崩溃转储文件夹中保留的最大文件数。
Detection.CHUNK_OVERLAP.int	45	每个片段从上一个片段的结尾借用的字符数。
Detection.CHUNK_SIZE.int	65536	文本片段大小（字节）。
Detection.DAR_KVOOP_PRIORITY.str	BELOW_NORMAL	外部 kvoop 进程在其提取 Endpoint Discover 扫描的文本时的优先级。
Detection.DAR_THREAD_PRIORITY.str	BELOW_NORMAL	检测线程在其将策略应用于 Endpoint Discover 扫描的文本时的优先级。
Detection.ENABLE_METADATA.str	off	当用户尝试传输或打印文件时，允许在文件元数据中进行检测。如果此设置设为 on，则您可以检测 Microsoft Office 和 PDF 文件的元数据。对于 Microsoft Office 文件，支持 OLE 元数据，这种元数据包括“标题”、“主题”、“作者”和“关键字”字段。对于 PDF 文件，仅支持文档信息字典元数据，这种元数据包括诸如“作者”、“标题”、“主题”、“创建日期”和“更新日期”等字段。不对可扩展元数据平台 (XMP) 内容进行检测。启用此选项会导致误报。
Detection.FILTER_TIMEOUT.int	420000	过滤文本时的时间限制（毫秒）。

设置名称	默认值	说明
Detection.LOCAL_DRIVE_KVOOP_PRIORITY.str	BELOW_NORMAL	外部 kvoop 在其提取本地驱动器事件的文本时的优先级。
Detection.LOCAL_DRIVE_THREAD_PRIORITY.str	BELOW_NORMAL	检测线程在其将策略应用于本地驱动器事件的文本时的优先级。
Detection.MARKUP_AS_TEXT.str	off	停止对关联了 XML 或 HTML 标记的任何文本的检测。此设置应该用于诸如标头块或脚本块中包含数据的 Web 2.0 页面的情况。
Detection.MAX_DETECTION_TIME.int	900000	完成端点检测的最长时间（毫秒）。
Detection.MAX_FILTER_FILE_SIZE.int	31457280	文本过滤的最大文件大小（字节）。
Detection.MAX_NUM_MATCHES.int	300	给定匹配项的最大匹配数。
Detection.MAX_QUEUE_SIZE.int	10000	同时等待检测的最大项目数。
Detection.NEWLINE_ELIMINATION.str	on	设置是否在检测前清除换行符。
Detection.RULESRESULTSCACHE_ENABLED.str	on	规则结果缓存 (RRC) 是一种在不违反策略的 DLP Agent 上缓存内容结果的方法。 请参见第 283 页的“ 策略检测简介 ”。 默认情况下，RRC 设置为 On。如果您不想使用 RRC，可将此参数设置为 Off。
Detection.RULESRESULTSCACHE_FAST_CACHE_SIZE.int	1024	规则结果缓存首级数据库（级别 1 数据库）的大小。规则结果缓存将已记录的非违规文件的新条目发送到级别 1 数据库。级别 1 数据库已满后，会将条目清空到级别 2 数据库以维护级别 1 数据库的空间。
Detection.SHORT_DAR_DETECTION_TIME.int	2000	在文件被视为过大之前对其进行检测所用时间（毫秒）。

设置名称	默认值	说明
Detection.TRACKED.CHANGES.str	off	允许检测 Microsoft Office 文档中随时间变化的内容（“修订”内容）。使用此选项可能会降低 IDM 和数据标识符的准确率。
Detection.UNICODE_NORMALIZATION.str	on	在检测之前将特定字符转换为 UNICODE。在匹配包含多种亚洲语言的数据的策略时，需要进行此转换。
Discover.CRAWLER_THREAD_PRIORITY.str	BELOW_NORMAL	扫描驱动器时“发现”线程的优先级。
Discover.POST_SCAN_REPORT_INTERVAL.int	60000	两个 Endpoint Discover 状态报告之间的时间间隔（毫秒）。即代理到达扫描结尾后到整个扫描完成或中止前的时间。
Discover.SCAN_ONLY_WHEN_IDLE.int	2	<p>设置代理是否在端点用户空闲时执行 Endpoint Discover 扫描。</p> <p>如果设置为1，则代理仅在端点用户空闲时执行 Endpoint Discover 扫描。</p> <p>如果设置为2，则代理在端点计算机活动时仅扫描小文件，而在端点用户空闲时扫描较大的文件。如果扫描文件所用时间多于 <code>DetectionSHORT_DAR_DETECTION_TIME</code> 秒，则其被视为大文件。</p> <p>如果设置为0，则无论是什么用户活动，都会进行扫描。</p>
Discover.SECONDS_UNTIL_IDLE.int	120	如果代理在这段时间（秒）里没有检测到任何用户活动，则用户被视为空闲。如果时间非常短（少于60秒），可能无法做到精确吻合。

设置名称	默认值	说明
Discover.STANDARD_REPORT_INTERVAL.int	10000	进行扫描时两个 Endpoint Discover 状态报告之间的时间间隔（毫秒）。
FileService.MAX_CACHE_SIZE.int	250	记录的每台端点计算机进程中最近打开的最大文件路径数。
FileSystem.DRIVER_FILE_OPEN_REQUEST_TIMEOUT.int	10	允许您配置从驱动程序发送至代理的文件打开请求的超时值（秒）。此设置在文件系统连接器响应驱动程序的速度较慢的情况下非常有用。如果连接速度较慢，系统就不能正常运行。等待代理响应的驱动程序会推迟每个文件打开请求。此设置不能保留空白，值也不能为 0。
FileSystem.ENABLE_FILE_RESTORATION.int	1	此设置用于打开或关闭文件还原。文件还原是指在包含机密数据的较新文件重写了原始文件的情况下对原始文件进行还原。文件还原在默认情况下处于启用状态。
FileSystem.ENABLE_VEP_FILE_ELIMINATION.int	1	启用了该设置后，系统不会创建 VEP 文件。而是在需要时，对原始文件进行检测，并为 EDPA.exe 和 KVOOP.exe 解决所有共享违规。默认情况下，此设置是禁用的。要启用此设置，请将值设置为 1。 注意： 如果您的环境不包含以下任何一项，可启用此设置： <ul style="list-style-type: none">■ 数据保留策略■ 双层检测策略■ Endpoint Discover 或 Endpoint Prevent 加密软件
FileSystem.NUM_TIMES_TO_OVERWRITE_FILE.int	2	此设置指示在阻止期间删除某文件之前用安全模式对其进行重写的次数。值为 0 表示文件无法重写。

设置名称	默认值	说明
FileSystem.USE_CDDVD_DEFAULT_EXCLUDE_PATHS.int	1	<p>此设置允许用户从以下目录排除 CD/DVD 应用程序打开的任何文件：</p> <ul style="list-style-type: none"> ■ 应用程序的安装目录，例如，如果应用程序为 Roxio，则其安装目录为 c:\program files\roxio ■ 系统目录，例如，%windir%\system32 ■ Program Files\Common Files。 <p>默认情况下启用。</p>
FlexResponse.PLUGIN_HOST_LOG_MAXFILE_SIZE.long	5120000	插件日志文件的最大大小。默认数值以字节为单位。
FlexResponse.PLUGIN_HOST_LOG_MAX_NUMBER_OF_FILES.long	1	可以保留的最大插件日志文件数。
FlexResponse.PLUGIN_HOST_MESSAGE_TIMEOUT.long	180000	允许插件主机处理消息的时间。默认时间以毫秒为单位。
FlexResponse.PLUGIN_HOST_STARTUP_TIMEOUT.long	30000	允许插件主机启动的时间。默认时间以毫秒为单位。如果插件主机未在指定的时间内启动，它会向日志发送一个失败事件。
GroupResolution.DAYS_DATA_STALING.int	7	代理保留 Active Directory (AD) 用户组信息的时间（天）。如果信息的保留时间超过此限制，代理会联系 AD 服务器。
Hooking.APPLICATION_LOAD_TIMEOUT.int	300000	指定代理在应用程序加载时间过长时尝试钩入该应用程序的时间（毫秒）。
Hooking.EXPLORER_HOOKING.int	3	允许 Symantec DLP Agent 监控 Microsoft Windows Explorer 通信。

设置名称	默认值	说明
Hooking .USE_LOADLIBRARYW_FROM_IMAGE.int	0	查找 LoadLibraryW 函数地址的方法。可以将值指定为 0 或 1。 0 表示使用 GetProcAddress API 查找库。 1 表示读取 kernel32.dll 的导出表来查找库。
IE8_HTTPS.Monitor.int	1	设置 Symantec DLP Agent 9.x 版的 Internet Explorer 8 HTTPS 监视。Symantec DLP Agent 的 Internet Explorer 8 HTTPS 监视会自动执行。默认情况下，监视处于打开状态。若要关闭 Internet Explorer 8 监视，请将此设置更改为 0。
IncidentHandler.CACHE_SIZE_THRESHOLD.int	30	触发 Endpoint Discover 暂停的所用端点数据库缓存空间百分比。
IncidentHandler.MAX_BACKOFF.int	3600000	在首次尝试将事件发送至服务器失败后重试之前等待的最长时间（毫秒）。
IncidentHandler.MAX INCIDENT FILE SIZE	31457280	要从代理发送以进行双层检测的最大文件的大小（字节）。
IncidentHandler.MAX_TTD_FILE_SIZE	31457280	要从代理发送以进行双层检测的最大文件的大小（字节）。
IncidentHandler.MIN_BACKOFF.int	30000	在代理首次尝试将事件发送至 Endpoint Server 失败后重新发送之前等待的最短时间（毫秒）。
IncidentHandler.PERSISTENT_MAX_DAR_ENTRIES.int	5	队列中保存的最大持久 Endpoint Discover 事件数。
IncidentHandler.PERSISTENT_MAX_ENTRIES.int	25	代理启动逐出事件之前代理存储区中的最大事件限制。
IncidentHandler.SENDER_CHUNK_SIZE.int	65536	在发送文件时从数据库读取的片段的大小（字节）。

设置名称	默认值	说明
Logging.OperationLogFileSize.long	5120000	操作日志文件的大小。此设置指定每个操作日志的最大大小（字节）。不保留超过此设置的日志。
Logging.OperationLogMaxFiles.int	30	在任一时刻可保留的最大操作日志数（每一扫描）。如果超过此数量，将从文件夹中清除操作日志文件，直到达到限制为止。根据创建日期来清除日志文件。首先清除最早的日志文件。此设置不适用于整个目录。
Logging.OperationLogTTL.int	90	操作日志在目录中保留的天数。如果操作日志在指定天数内没有被访问或修改过，将删除该文件。
MonitorSystemUsers.CLIPBOARD.int	0	对剪贴板功能启用系统用户监控。默认情况下设置为非活动。设置为 1 即启用。
MonitorSystemUsers.LOCAL_DRIVE.int	0	对本地驱动器功能启用系统用户监控。默认情况下设置为非活动。设置为 1 即启用。
MonitorSystemUsers.NETWORK.int	0	对驱动程序中的网络协议（HTTP 和 FTP）启用系统用户监控。默认情况下设置为非活动。设置为 1 即启用。
MonitorSystemUsers.PRINT_FAX.int	0	对打印/传真功能启用系统用户监控。默认情况下，此功能设置为非活动。设置为 1 即启用。
NetworkMonitor.ENABLE_HTTP_GET_MONITORING.int	0	启用 HTTP/HTTPS GET 请求监控。默认情况下，此设置是禁用的。设置为 1 即启用。
NetworkMonitor.HTTP_DETECTION_TIMEOUT.int	120	代理在扫描 HTTP 和 HTTPS 数据期间等待的时间长度（秒）。

设置名称	默认值	说明
NetworkMonitor.IM_DETECTION_SESSION_TIMEOUT.int	120	所有即时消息传递客户端的检测会话窗口的持续时间（秒）。
PluginInstaller.TAMPERPROOFING_IGNORE_PROCESS_TIMEOUT.int	15000	允许您指定忽略不加载插件的任何短期进程的时间（毫秒）。如果进程在达到此时间限制之前结束，插件安装程序不会启动。
PostProcessor.ENABLE_FLEXRESPONSE.int	0	允许您启用或禁用 Endpoint FlexResponse 功能。默认情况下，Endpoint FlexResponse 处于关闭状态。将设置更改为 1 即可启用 Endpoint FlexResponse。
PostProcessor.FILE_SYSTEM_USER_RESPONSE_TIMEOUT.int	60	端点用户必须选择“用户取消”弹出通知的响应操作的时间（秒）。此设置仅适用于尝试传输违反策略文件时生成的事件。
PostProcessor.NETWORK_USER_RESPONSE_TIMEOUT.int	60	端点用户必须选择“用户取消”弹出通知的响应操作的时间（秒）。此设置仅适用于 HTTP、FTP 和 IM 事件。
PostProcessor.NOTIFY_ON_FIXED_DRIVE.int	0	对固定驱动器事件启用响应通知。默认设置为禁用通知。设置为 1 即启用。
PostProcessor.NOTIFY_WITH_CANCEL_DEFAULT_ACTION	1	如果端点用户未在指定时间内从“用户取消”弹出通知中选择操作，则执行默认操作。
PostProcessor.OTHER_USER_RESPONSE_TIMEOUT	60	端点用户必须选择“用户取消”弹出通知的响应操作的时间（秒）。此设置仅适用于剪贴板、打印、电子邮件和 HTTPS 事件。

设置名称	默认值	说明
Quarantine.MAX_QUEUE_SIZE.int	100	任一时刻队列中允许的最大隔离请求数。超过此数量的请求将被丢弃，不会对其进行隔离。
ResponseCache.CD_TIMEOUT.int	2000	CD/DVD 事件缓存的时间（毫秒）。在此时间段内不会生成重复事件，也不会导致出现“阻止”弹出式通知。
ResponseCache.FTP_TIMEOUT.int	10000	FTP 事件缓存的时间（毫秒）。在此时间段内不会生成重复事件，也不会导致出现“阻止”弹出式通知。
ResponseCache.HTTP_TIMEOUT.int	2000	HTTP/HTTPS 事件缓存的时间（毫秒）。在此时间段内不会生成重复事件，也不会导致出现“阻止”弹出式通知。
ResponseCache.MAX_SIZE.int	100	随时缓存的最大事件数。
SLEEP_TIME_IN_MS.ClipboardViewer.int	10	从剪贴板提取内容之前的睡眠时间或可配置的延迟（以毫秒为单位）。
SMP.AUTO_ENABLE.int	1	<p>自动向 Symantec Management Platform (SMP) 注册或取消注册 Symantec DLP Agent。如果不向 SMP 注册 Symantec DLP Agent，请更改此设置。</p> <p>设置为 0 时将禁用该功能。</p> <p>设置为 1 时将启用该功能并自动向 SMP 注册 Symantec DLP Agent。</p> <p>设置为 2 时将启用该功能并自动向 SMP 取消注册 Symantec DLP Agent。</p> <p>如果要由注册实用程序或 SMP 注册策略执行注册或取消注册操作，请确保将此参数设置为 0。否则，Symantec DLP Agent 将自动重置注册操作。</p>

设置名称	默认值	说明
ServerCommunication.CONNECTION_INTERVAL_SECONDS	86400	尝试成功连接的默认时间间隔（秒）。
ServerCommunication.CONNECTION_RETRY_ATTEMPTS.int	10	DLP Agent 尝试连接到 Endpoint Server 的最大次数。
ServerCommunication.CONNECTION_RETRY_INTERVAL_SECONDS.int	10	DLP Agent 在连接失败后尝试重新连接到 Endpoint Server 的时间间隔（秒）。
ServerCommunication.CONNECT_WHEN_IP_CHANGES.int	1	如果 Endpoint Server 的 IP 地址发生更改，DLP Agent 会尝试连接到服务器并重新获取策略信息。设置为 1 时，DLP Agent 会自动尝试重新连接到服务器。如果设置为 0，则 DLP Agent 不会尝试重新连接到服务器。
ServerRedundancy.FAILOVER_INTERVAL.long	3600	代理尝试故障转移至新的 Endpoint Server 之前尝试连接到 Endpoint Server 所用的时间间隔（秒）。
ServerRedundancy.MAX_TIME_BETWEEN_CONNECTION_ATTEMPTS.long	600	代理在两次尝试连接到同一 Endpoint Server 期间等待的最长时间（秒）。
UI.BUTTON_OK.str	确定	此设置控制“确定”按钮上的文本。如果使用不受支持的区域设置，请更改此设置。默认语言为“英语”。
UI.BUTTON_OKTOALL.str	全部确定	此设置控制“全部确定”按钮上的文本。如果使用不受支持的区域设置，请更改此设置。默认语言为“英语”。
UI.CONSECUTIVE_TRANSACTION_TIME.str	10	视为单个事务的两次文件操作之间的最长时间（秒）。
UI.MONITOR_MSG_TITLE.str		通知弹出式消息的消息标题。

设置名称	默认值	说明
UI.MONITOR_TITLEBAR.str	警告	此设置控制“端点通知”通知弹出式消息的标题栏中的静态标题消息。如果使用不受支持的区域设置，请更改此设置。默认设置为“警告”。
UI.NO_SCAN.int	0	如果值为非零的数字，则不会显示扫描对话框。
UI.NWC_EVENT_LIMIT_FS.int	5	在接受更多事件的默认操作之前可以进行排队的最大事件数。此设置仅适用于文件系统事件。
UI.NWC_EVENT_LIMIT_NW.int	2	在接受更多事件的默认操作之前可以进行排队的最大事件数。此设置仅适用于网络事件。
UI.pop-up_QUEUE_LIMIT.int	100	用户在单个会话中看到的弹出式通知的限制。这些弹出式通知要求用户输入验证的理由。如果超出限制，超过限制的任何弹出式通知自动包含“不适用(N/A)”理由。
UI.PREVENT_MSG_TITLE.str		阻止弹出式消息的消息标题。
UI.PREVENT_TIMEOUT.int	300	生成事件之前的超时值(秒)。如果超出此限制，不论用户从弹出窗口选择了哪种操作，都会生成此事件。
UI.PREVENT_TITLEBAR.str	已阻止	此设置控制“端点阻止”通知弹出式对话框的标题栏中的静态标题消息。如果使用不受支持的区域设置，请更改此设置。默认语言为“英语”。
UI.PREVENT_WINPOSITION.int	0	“阻止”对话框窗口的起始位置。
UI.QUARANTINE_PROMPT.str	文件的隔离位置为：	此设置控制指定隔离数据所在位置的文本。如果使用的区域设置不受支持，请更改此文本。默认设置采用英语。

设置名称	默认值	说明
UI.SCAN_BAR.str	(空白)	使用此设置，您可以更改扫描窗口正文部分的文本。此文本是静态的，无论端点计算机的区域设置为何，它都会显示。
UI.SCAN_DELAY.int	0	显示扫描对话框窗口之前过去的时间（秒）。
UI.SCAN_EMAIL.int	0	此设置可激活电子邮件扫描的切换。如果此设置设为0，用户无法选择电子邮件监控。
UI.SCAN_FTP.int	0	此设置可激活FTP扫描的切换。如果此设置设为0，用户无法选择FTP监控。
UI.SCAN_HTTP.int	0	此设置可激活HTTP监控的切换。如果此设置设为0，用户无法选择HTTP监控。
UI.SCAN_IM.int	0	此设置可激活即时消息(IM)扫描的切换。如果此设置设为0，用户无法选择IM监控。
UI.SCAN_PRINTFAX.int	0	此设置可激活打印/传真扫描的切换。如果此设置设为0，用户无法选择打印/传真监控。
UI.SCAN_REMOVABLEMEDIA.int	1	此设置可激活可移动介质扫描的切换。如果此设置设为0，用户不能选择可移动介质监控。
UI.SCAN_SHOWTIME.int	2	扫描对话框停留在屏幕上的最短时间（秒）。
UI.SCAN_TITLE.str	(空白)	此设置允许您输入向用户显示的扫描窗口的标题。此标题是静态消息，无论端点计算机的区域设置是什么，它都会显示。
UI.USERINPUT_PROMPT.str	其他：	此设置控制出现在用户输入字段的阻止弹出式消息与通知弹出式消息中的提示。如果使用不受支持的区域设置，请更改此提示。默认设置采用英语。

设置名称	默认值	说明
UninstallPassword.RETRY_LIMIT.int	3	此设置定义用户在不输入正确卸载密码的情况下可尝试卸载 Symantec Data Loss Prevention 代理的次数。

管理日志文件

本章节包括下列主题：

- [关于日志文件](#)
- [日志收集和配置屏幕](#)
- [配置服务器日志记录行为](#)
- [收集服务器日志和配置文件](#)
- [关于日志事件代码](#)

关于日志文件

Symantec Data Loss Prevention 提供了许多不同的记录软件行为信息的日志文件。日志文件分成以下类别：

- 操作日志文件记录有关软件执行的任务及在软件执行这些任务时发生的任何错误的详细信息。您可以使用操作日志文件的内容来验证软件是否按您预期的方式运行。您也可以使用这些文件来解答任何在该软件与其他系统组件集成时的疑难问题。
例如，您可以使用操作日志文件来验证 Network Prevent for Email Server 是否与网络上的特定 MTA 进行通信。
请参见第 234 页的“[操作日志文件](#)”。
- 调试日志文件记录有关构成 Symantec Data Loss Prevention 的单独进程或软件组件的细粒度技术详细信息。调试日志文件的内容不用于诊断系统配置错误或验证预期软件功能。您无需检查调试日志文件以管理或维护 Symantec Data Loss Prevention 安装。然而，Symantec 支持部门可能会在您报告问题时要求您提供调试日志文件以进行进一步的分析。默认情况下，不创建某些调试日志文件。
如有必要，Symantec 支持部门可以解释如何配置软件来创建文件。
请参见第 236 页的“[调试日志文件](#)”。

- 安装日志文件记录有关在特定计算机上执行的 Symantec Data Loss Prevention 安装任务的信息。您可以使用这些日志文件验证安装或排除安装错误。安装日志文件位于下列位置：
 - *installdir\SymantecDLP\.install4j\installation.log* 存储 Symantec Data Loss Prevention 的安装日志。
 - *installdir\oracle_home\admin\protect* 存储 Oracle 的安装日志。
有关更多信息，请参见《Symantec Data Loss Prevention 安装指南》。

操作日志文件

Enforce Server 和检测服务器将操作日志文件存储在 `\SymantecDLP\Protect\logs\` 目录中（Windows 安装）或 `/var/log/SymantecDLP/` 目录中（Linux 安装）。日志文件名末尾的数字表示计数（表 13-1 中显示为 0）。

[表 13-1](#) 列出并描述了 Symantec Data Loss Prevention 操作日志文件。

表 13-1 操作日志文件

日志文件名	说明	服务器
<code>agentmanagement_webservices_access_0.log</code>	记录访问代理管理 API Web 服务的成功与失败的尝试。	Enforce Server
<code>agentmanagement_webservices_soap_0.log</code>	记录对代理管理 API Web 服务的大多数请求的整个 SOAP 请求和响应。	Enforce Server
<code>boxmonitor_operational_0.log</code>	BoxMonitor 进程会监视属于该特定服务器类型的检测服务器进程。 例如，Network Monitor 上运行的进程是文件读取器和数据包捕获。 BoxMonitor 日志文件通常很小，显示的是应用程序进程的运行方式。	所有检测服务器
<code>Classification_Operational_0.log</code>	记录分类检测服务器、Web 容器和请求的状态。	分类检测服务器
<code>detection_operational_0.log</code>	检测操作日志文件提供有关检测服务器如何配置以及是否正常运行的详细信息。	所有检测服务器

日志文件名	说明	服务器
detection_operational_trace_0.log	<p>检测跟踪日志文件提供有关检测服务器处理的每封邮件的详细信息。日志文件包括如下的类似信息：</p> <ul style="list-style-type: none"> ■ 应用于邮件的策略 ■ 邮件中匹配的策略规则 ■ 邮件生成的事件数量。 	所有检测服务器
machinelearning_training_operational_0.log	本日志记录有关启动VML培训进程时调用的任务、日志和配置文件的信息。	Enforce Server
manager_operational_0.log.	有关 Symantec Data Loss Prevention 管理器进程（该进程实施 Enforce Server 管理控制台用户界面）的日志信息。	Enforce Server
monitorcontroller_operational_0.log	记录 Enforce Server 与所有检测服务器之间连接的详细日志。它提供关于这些服务器之间已交换信息的详细信息，包括策略是否已推送到检测服务器。	Enforce Server
SmtpPrevent0.log	此操作日志文件仅涉及 SMTP Prevent。它是用于跟踪 Network Prevent for Email 系统的运行状况和活动的主要日志。检查此文件以查找有关 MTA 与检测服务器之间通信的信息。	SMTP Prevent 检测服务器
spc_webservices_access_0.log	记录从 SPC 服务器进行的 Web 服务调用。	Enforce Server
spc_webservices_soap_0.log	记录在 Enforce Server 和 Symantec Protection Console 服务器之间交换的详细 Web 服务 SOAP 消息。	Enforce Server
WebPrevent_Access0.log	此访问日志文件包含 Network and Mobile Prevent for Web 检测服务器所处理请求的相关信息。它与代理服务器的 Web 访问日志类似。	<ul style="list-style-type: none"> ■ Network Prevent (Web) 检测服务器 ■ Mobile Prevent for Web 检测服务器

日志文件名	说明	服务器
WebPrevent_Operational0.log	此可操作的日志文件报告 Network and Mobile Prevent for Web 的运行状况，例如系统是启动还是关闭以及连接管理。	<ul style="list-style-type: none"> ■ Network Prevent (Web) 检测服务器 ■ Mobile Prevent for Web 检测服务器
webservices_access_0.log	此日志文件记录访问事件报告与更新 Web 服务的成功与失败的尝试。	Enforce Server
webservices_soap_0.log	对于“报告 API Web 服务”的大多数请求，包含整个 SOAP 请求和响应。此日志记录所有请求和响应（对事件二进制请求的响应除外）。默认情况下，不创建此日志文件。有关更多详细信息，请参见《Symantec Data Loss Prevention 事件报告和更新 API 开发指南》。	Enforce Server

请参见第 248 页的“[Network and Mobile Prevent for Web 操作日志文件和事件代码](#)”。

请参见第 250 页的“[Network and Mobile Prevent for Web 访问日志文件和字段](#)”。

请参见第 252 页的“[Network Prevent for Email 日志级别](#)”。

请参见第 253 页的“[Network Prevent for Email 操作日志代码](#)”。

请参见第 256 页的“[Network Prevent for Email 产生的响应和代码](#)”。

调试日志文件

Enforce Server 和检测服务器将调试日志文件存储在 \SymantecDLP\Protect\logs\ 目录中（Windows 安装）或 /var/log/SymantecDLP/ 目录中（Linux 安装）。日志文件名末尾的数字表示计数（调试日志文件中显示为 0）。

下表列出并描述了 Symantec Data Loss Prevention 调试日志文件。

表 13-2 调试日志文件

日志文件名	说明	服务器
Aggregator0.log	<p>此文件说明检测服务器与代理之间的通信。查看此日志可对下列问题进行故障排除：</p> <ul style="list-style-type: none"> ■ 连接到代理 ■ 找出应出现事件却不出现的原因 ■ 发生意外代理事件 	端点检测服务器
BoxMonitor0.log	<p>这个文件通常很小，显示的是应用程序进程的运行方式。BoxMonitor 进程会监视属于该特定服务器类型的检测服务器进程。</p> <p>例如，Network Monitor 上运行的进程是文件读取器和数据包捕获。</p>	所有检测服务器
ContentExtractionAPI_FileReader.log	记录将请求发送到插件主机的内容提取 API 文件读取器的行为。默认日志记录级别是“信息”，可使用 \Protect\config\log4cxx_config_filereader.xml 进行配置。	检测服务器
ContentExtractionAPI_Manager.log	记录将请求发送到插件主机的内容提取 API 管理器的行为。默认日志记录级别是“信息”，可使用 \Protect\config\log4cxx_config_manager.xml 进行配置。	Enforce Server
ContentExtractionHost_FileReader.log	记录内容提取文件读取器主机和插件的行为。默认日志记录级别是“信息”，可使用 \Protect\config\log4cxx_config_filereader.xml 进行配置。	检测服务器
ContentExtractionHost_Manager.log	记录内容提取管理器主机和插件的行为。默认日志记录级别是“信息”，可使用 \Protect\config\log4cxx_config_manager.xml 进行配置。	Enforce Server
DiscoverNative.log.0	包括 Network Discover 本机代码发出的日志语句。当前包括与 .pst 扫描相关的信息。此日志文件仅适用于 Windows 平台上运行的 Network Discover Server。	发现检测服务器
FileReader0.log	此日志文件涉及文件读取器进程，包括特定于应用程序的日志记录，这些记录有助于解决检测和创建事件中出现的问题。显示的一个症状就是内容提取程序超时。	所有检测服务器

日志文件名	说明	服务器
flash_client_0.log	记录来自 Adobe Flex 客户端的消息， Network Discover 可将这些消息用于文件夹风险报告。	Enforce Server
flash_server_remoting_0.log	包含来自 BlazeDS 的日志消息， BlazeDS 是一个开源组件，可响应 Adobe Flex 客户端的远程过程调用。该日志指示 Enforce Server 是否已收到来自 Flash 客户端的消息。在限制性弱的日志级别（ FINE 、 FINER 、 FINEST ）， BlazeDS 日志包含客户端对服务器的请求内容以及服务器对客户端的响应内容。	Enforce Server
IncidentPersister0.log	此日志文件涉及 Incident Persister 进程。此进程会读取 Enforce Server 上 incidents 文件夹中的事件，并将它们写入到数据库。如果 Enforce Server （管理器）上的事件队列增变得过长，请查看此日志。也可以通过检查 Enforce Server 上 incidents 文件夹中的事件是否已备份来观察这个情况。	Enforce Server
Indexer0.log	此日志文件包括编制 EDM 配置文件或 IDM 配置文件索引时的信息。还包括使用外部索引器时所收集的信息。如果编制索引失败，应参考此日志。	Enforce Server (或外部索引器运行所在的计算机)
jdbc.log	此日志文件是对 JDBC 调用数据库的跟踪。默认情况下，将关闭对此日志的写入。	Enforce Server
machinelearning_native_filereader.log	该日志文件记录了运行时类别分类（正面和负面）和关联可信度（针对 VML 配置文件检测的每个消息）。默认日志记录级别是“信息”，可使用 \\Protect\\config\\log4cxx_config_filereader.xml 进行配置。	检测服务器
machinelearning_training_0_0.log	该日志文件记录所有 VML 配置文件的 k-fold 评估的设计时基本准确率百分比。	Enforce Server
machinelearning_training_native_manager.log	该日志文件记录每个 VML 配置文件培训运行的设计时建模功能总数。默认日志记录级别是“信息”，可使用 \\Protect\\config\\log4cxx_config_manager.xml 进行配置。	Enforce Server
MonitorController0.log	此日志文件是 Enforce Server 与检测服务器之间连接的详细日志。它提供关于这些服务器之间已交换信息的详细信息，包括策略是否已推送到检测服务器。	Enforce Server

日志文件名	说明	服务器
PacketCapture.log	此日志文件涉及将数据包重组到邮件中并写入到 drop_pcap 目录的数据包捕获进程。如果已丢弃的数据包出现问题或流量低于预期, 请查看此日志。PacketCapture 不是 Java 进程, 因此不会遵循与其他 Symantec Data Loss Prevention 系统进程相同的日志记录规则。	Network Monitor
PacketCapture0.log	此日志文件说明 PacketCapture 通信的问题。	Network Monitor
RequestProcessor0.log	此日志文件仅涉及 SMTP Prevent。此日志文件主要用于 SmtpPrevent0.log 不能满足需要的情况。	SMTP Prevent 检测服务器
ScanDetail-target-0.log	其中 <i>target</i> 是扫描目标的名称。目标名称中的所有空格都会替换为连字符。此日志文件涉及发现服务器扫描。它会逐文件记录扫描中发生的事件。如果成功扫描文件, 它会显示成功, 接着是已扫描文件的路径、大小、时间、所有者和 ACL 信息。如果失败, 则会显示警告, 后跟文件名。	发现检测服务器
tomcat\localhost.date.log	这些 Tomcat 日志文件包含任何涉及用户界面的操作的信息。日志包括红色错误消息框中的用户界面错误、登录时密码无效, 以及 Oracle 错误 (ORA -#)。	Enforce Server
VontuIncidentPersister.log	此日志文件包括最少信息: 仅 stdout 和 stderr (致命事件)。	Enforce Server
VontuManager.log	此日志文件包括最少信息: 仅 stdout 和 stderr (致命事件)。	Enforce Server
VontuMonitor.log	此日志文件包括最少信息: 仅 stdout 和 stderr (致命事件)。	所有检测服务器
VontuMonitorController.log	此日志文件包括最少信息: 仅 stdout 和 stderr (致命事件)。	Enforce Server
VontuNotifier.log	此日志文件涉及 Notifier 服务及其与 Enforce Server 和 MonitorController 服务之间的通信。查看此文件以了解 MonitorController 服务是否记录了策略更改。	Enforce Server
VontuUpdate.log	更新 Symantec Data Loss Prevention 时会填充此日志文件。	Enforce Server

请参见第 252 页的“[Network and Mobile Prevent for Web 协议调试日志文件](#)”。

请参见第 252 页的“[Network Prevent for Email 日志级别](#)”。

日志收集和配置屏幕

使用“日志”屏幕（“系统”>“服务器”>“日志”），可以收集所有 Symantec Data Loss Prevention 服务器的日志文件或对其进行配置。“日志”屏幕包含两个提供下列功能的选项卡：

- **收集** - 使用此选项卡可收集一台或多台 Symantec Data Loss Prevention 服务器中的日志文件和配置文件。
请参见第 244 页的“[收集服务器日志和配置文件](#)”。
- **配置** - 使用此选项卡可配置 Symantec Data Loss Prevention 服务器的基本日志记录行为，或将自定义日志配置文件应用到服务器。
请参见第 240 页的“[配置服务器日志记录行为](#)”。

请参见第 233 页的“[关于日志文件](#)”。

配置服务器日志记录行为

使用“日志”屏幕（“系统”>“服务器”>“日志”）中的“配置”选项卡可更改 Symantec Data Loss Prevention 部署中任何服务器的日志记录配置参数。“选择诊断日志设置”菜单为 Enforce Server 以及检测服务器日志记录参数提供了预配置的设置。可以选择适用的预配置设置以定义常见日志级别或启用常见服务器功能的日志记录。“选择诊断日志设置”菜单还提供默认设置，可以将日志记录配置参数恢复为安装时使用的默认设置。

表 13-3 介绍了适用于 Enforce Server 的预配置日志设置。表 13-4 介绍了适用于检测服务器的预配置设置。

或者，您也可以上传使用文本编辑器创建或修改的自定义日志配置文件。（使用“**收集**”选项卡可下载要自定义的日志配置文件。）只能上传那些修改日志记录属性的配置文件（文件名以 Logging.properties 结尾）。将新日志配置文件上传到服务器后，服务器首先会备份相同名称的现有配置文件。随后将新文件复制到配置文件目录中，并立即应用其属性。

除非指示您重新启动服务器进程以使更改生效，否则不需要执行此操作。自当前软件版本起，仅对 PacketCaptureNativeLogging.properties 和 DiscoverNativeLogging.properties 文件进行更改后要求您重新启动服务器进程。

请参见第 175 页的“[服务器控件](#)”。

确保上传的配置文件包含适用于要配置的服务器类型的有效属性定义。如果上传日志配置文件时出错，请使用预配置的“还原默认值”设置将日志配置恢复为其原始安装状态。

Enforce Server 管理控制台仅对所上传的日志配置文件执行基本验证。这可确保：

- 配置文件名符合实际的日志记录配置文件名。
- 在配置文件中启用根级别日志记录。该配置可以确保某些基本日志记录功能始终可用于服务器。
- 定义日志记录级别的文件中的属性仅包含有效值（如 INFO、FINE 或 WARNING）。

如果服务器检测到这些项目中的任何一个有问题，它都将显示错误消息并将取消文件上传。

如果 Enforce Server 将日志配置文件更改成功上传到检测服务器，管理控制台将报告配置更改已提交。如果随后检测服务器在尝试应用配置更改时遇到任何问题，它将记录系统事件警告以指示该问题。

表 13-3 用于 Enforce Server 的预配置日志设置

“选择诊断日志设置”值	说明
还原默认值	将日志文件参数还原为其默认值。
报告 API SOAP 日志记录	对于报告 API Web 服务的大多数请求，会记录整个 SOAP 请求和响应消息。记录的消息存储在 webservices_soap.log 文件中，默认情况下该文件不随新安装一起创建。 创建报告 API Web 服务客户端时，可以使用 webservices_soap.log 的内容来诊断问题。有关更多信息，请参见《Symantec Data Loss Prevention 报告 API 开发人员指南》。
自定义属性查找日志记录	会在每次 Enforce Server 使用查找插件填充事件的自定义属性时记录诊断信息。查找插件会使用 LDAP、CSV 文件或其他数据存储库填充自定义属性数据。诊断信息记录在 Tomcat 日志文件 (c:\SymantecDLP\logs\tomcat\localhost.date.log 和 IncidentPersister_0.log 文件中)。 请参见第 833 页的“ 关于自定义属性 ”。 请参见第 834 页的“ 关于使用自定义属性 ”。

表 13-4 适用于检测服务器的预配置日志设置

“选择诊断日志设置”值	使用的检测服务器	说明
还原默认值	所有检测服务器	将日志文件参数还原为其默认值。
发现跟踪日志记录	Network Discover Server	启用 Network Discover 扫描的信息性日志记录。这些日志消息都存储在 FileReader0.log 中。
检测跟踪日志记录	所有检测服务器	<p>记录检测服务器处理的每封邮件的相关信息。包括如下信息：</p> <ul style="list-style-type: none"> ■ 应用于邮件的策略 ■ 邮件中匹配的策略规则 ■ 邮件生成的事件数量。 <p>启用“检测跟踪日志记录”后，生成的消息将存储在 detection_operational_trace_0.log 文件中。</p> <p>注意： 跟踪日志记录会产生大量数据，且数据以纯文本格式存储。请仅在需要调试特定问题时才使用跟踪日志记录。</p>
数据包捕获调试日志记录	Network Monitor 服务器	<p>为 Network Monitor 启用数据包捕获基本调试日志记录。此设置会将信息记录在 PacketCapture.log 文件中。</p> <p>尽管此类型的日志记录会产生大量数据，但是“数据包捕获调试日志记录”设置可以将日志文件大小限制为 50 MB，并将最大日志文件数限制为 10。</p> <p>如果将此日志配置设置应用到服务器，则必须重新启动服务器进程以启用更改。</p>

“选择诊断日志设置”值	使用的检测服务器	说明
电子邮件阻止日志记录	Network Prevent for Email 服务器	<p>为 Network Prevent for Email 服务器启用完整的邮件日志记录。此设置会记录完整的邮件内容，并包括执行和错误跟踪信息。记录的信息存储在 <code>SmtpPrevent0.log</code> 文件中。</p> <p>注意： 跟踪日志记录会产生大量数据，且数据以纯文本格式存储。请仅在需要调试特定问题时才使用跟踪日志记录。</p> <p>请参见第 253 页的“Network Prevent for Email 操作日志代码”。</p> <p>请参见第 256 页的“Network Prevent for Email 产生的响应和代码”。</p>
ICAP 阻止邮件处理日志记录	Network Prevent for Web 服务器	<p>为 Network Prevent for Web 启用操作和访问日志记录。此设置会将信息记录在 <code>FileReader0.log</code> 文件中。</p> <p>请参见第 248 页的“Network and Mobile Prevent for Web 操作日志文件和事件代码”。</p> <p>请参见第 250 页的“Network and Mobile Prevent for Web 访问日志文件和字段”。</p>

按照此过程更改 Symantec Data Loss Prevention 服务器的日志配置。

配置服务器的日志记录属性

- 1 请单击“配置”选项卡（如果尚未选中的话）。
- 2 如果要配置检测服务器的日志记录属性，请从“选择检测服务器”菜单中选择服务器名称。
- 3 如果要将预配置日志设置应用到服务器，请从要配置的服务器旁的“选择诊断配置”菜单中选择配置名称。

有关诊断配置的说明，请参见[表 13-3](#)和[表 13-4](#)。

- 4 如果改为想要使用自定义日志配置文件，请单击要配置的服务器旁的“浏览...”。然后从“文件上传”对话框中选择要使用的日志记录配置文件，并单击“打开”。只可上传日志记录配置文件，不可上传影响其他服务器功能的配置文件。

注意：如果“浏览”按钮由于先前的菜单选项而不可用，请单击“清除表单”。

- 5 单击“配置日志”以将预配置设置或自定义日志配置文件应用到选定服务器。
- 6 检查是否存在任何系统事件警告，指示在将配置更改应用到服务器时出现问题。

请参见第 240 页的[“日志收集和配置屏幕”](#)。

注意：以下调试日志文件是在可通过 Enforce Server 管理控制台访问的日志记录框架之外手动配置的：`ContentExtractionAPI_FileReader.log`、
`ContentExtractionAPI_Manager.log`、
`ContentExtractionHost_FileReader.log`、
`ContentExtractionHost_Manager.log`、
`machinelearning_native_filereader.log` 和
`machinelearning_training_native_manager.log`。有关配置详细信息，请参阅调试日志文件列表中针对每个上述日志文件的条目。请参见第 236 页的[“调试日志文件”](#)。

收集服务器日志和配置文件

使用“日志”屏幕的“收集”选项卡（“系统”>“服务器”>“日志”），从一个或多个 Symantec Data Loss Prevention 服务器上收集日志文件和配置文件。可从单个检测服务器或所有检测服务器，以及 Enforce Server 计算机上收集文件。您可以将所收集的文件限制为上次在指定的日期范围内更新的文件。

Enforce Server 管理控制台将收集的所有日志和配置文件存储在 Enforce Server 计算机上的单个 ZIP 文件中。如果从多个 Symantec Data Loss Prevention 服务器上检索文件，则每个服务器的文件存储在该 ZIP 文件的一个单独的子目录中。

“收集”选项卡上的复选框允许您从选定的服务器上收集不同类型的文件。[表 13-5](#)介绍了每个文件类型。

表 13-5 收集的文件类型

文件类型	说明
操作日志	<p>操作日志文件记录有关软件执行的任务及在软件执行这些任务时发生的任何错误的详细信息。您可以使用操作日志文件的内容来验证软件是否按您预期的方式运行。您也可以使用这些文件来解答任何在该软件与其他系统组件集成时的疑难问题。</p> <p>例如，您可以使用操作日志文件来验证 Network Prevent for Email Server 是否与网络上的特定 MTA 进行通信。</p>
调试和跟踪日志	<p>调试日志文件记录有关构成 Symantec Data Loss Prevention 的单独进程或软件组件的细粒度技术详细信息。调试日志文件的内容不用于诊断系统配置错误或验证预期软件功能。您无需检查调试日志文件以管理或维护 Symantec Data Loss Prevention 安装。然而，Symantec 支持部门可能会在您报告问题时要求您提供调试日志文件以进行进一步的分析。默认情况下，不创建某些调试日志文件。如有必要，Symantec 支持部门可以解释如何配置软件来创建文件。</p>

文件类型	说明
配置文件	<p>使用“配置文件”选项同时检索日志记录配置文件和服务器功能配置文件。</p> <p>日志记录配置文件定义了在服务器日志文件中记录的日志记录详细信息的整体级别。日志记录配置文件还确定了是否将特定的功能或子系统事件记录到日志文件中。</p> <p>例如，默认情况下 Enforce 控制台不记录从报告 API Web 服务客户端生成的 SOAP 消息。<code>ManagerLogging.properties</code> 文件包含一个可启用 SOAP 消息记录的属性。</p> <p>您可以通过使用“配置”选项卡上提供的预设置修改多个常规日志记录配置属性。</p> <p>如果要手动更新日志记录配置文件，请使用“配置文件”复选框为服务器下载配置文件。您可以通过使用文本编辑器修改单个日志记录属性，然后使用“配置”选项卡将修改的文件上传至服务器。</p> <p>请参见第 240 页的“配置服务器日志记录行为”。</p> <p>“配置文件”选项检索活动的日志记录配置文件以及使用“配置”选项卡时创建的任何备份日志配置文件。此选项还检索服务器功能配置文件。服务器功能配置文件影响服务器行为的许多方面，例如 Syslog 服务器的位置或服务器的通信设置。您可以收集这些配置文件以帮助诊断问题或验证服务器设置。但是，您不能使用“配置”选项卡更改服务器功能配置文件。您只能使用该选项卡更改日志记录配置文件。</p>
代理日志	<p>使用“代理日志”选项从 Endpoint Prevent 检测服务器收集 DLP 代理服务和操作日志文件。该选项仅适用于 Endpoint Prevent 服务器。要使用此选项收集代理日志，您必须已使用“提取日志”操作将日志文件从各自的代理中提取到 Endpoint Prevent 检测服务器。</p> <p>使用代理概述屏幕选择各自的代理，并将选定的日志文件提取到 Endpoint Prevent 检测服务器。然后请使用此页面上的“代理日志”选项来收集日志文件。</p> <p>从端点计算机提取日志时，日志以未加密的格式存储在 Endpoint Server 上。从 Endpoint Server 收集日志后，日志将从 Endpoint Server 中删除，且仅存储在 Enforce Server 上。您每次只能从一台端点计算机上收集日志。</p> <p>请参见第 1196 页的“代理概述操作”。</p> <p>请参见第 1193 页的“使用代理概述屏幕”。</p>

操作、调试和跟踪日志文件存储在 ZIP 文件的 *server_identifier/logs* 子目录中。*server_identifier* 标识生成日志文件的服务器，且对应于以下各值之一：

- 如果从 Enforce Server 收集日志文件，则 Symantec Data Loss Prevention 使用字符串 *Enforce* 替换 *server_identifier*。请注意，Symantec Data Loss Prevention 不使用 Enforce Server 的本地化名称。
- 如果检测服务器的名称只包含 ASCII 字符，则 Symantec Data Loss Prevention 使用检测服务器的名称作为 *server_identifier* 值。
- 如果检测服务器的名称包含非 ASCII 字符，则 Symantec Data Loss Prevention 使用字符串 *DetectionServer-ID-id_number* 作为 *server_identifier* 值。*id_number* 是检测服务器的唯一标识号码。

如果您从 Endpoint Prevent Server 收集代理服务日志文件或操作日志文件，则文件放置在 *server_identifier/agentlogs* 子目录中。每个代理日志文件使用各自的代理名称作为日志文件前缀。

请遵循此过程，从 Symantec Data Loss Prevention 服务器收集日志文件和日志配置文件。

从一个或多个服务器收集日志文件

- 1 单击“收集”选项卡（如果未选中）。
- 2 使用“日期范围”菜单选择想要收集的文件的日期范围。请注意，收集进程在任何情况下都不截断已下载的日志文件。日期范围将所收集的文件限制为上次在指定的范围内更新的文件。
- 3 要从 Enforce Server 收集日志文件，请选择 **Enforce Server** 条目旁的一个或多个复选框以指示想要收集的文件类型。
- 4 要从一个或所有检测服务器收集日志文件，请使用“选择检测服务器”菜单以选择检测服务器的名称或“从所有检测服务器收集日志”选项。然后选择该菜单旁的一个或多个复选框以指示想要收集的文件类型。
- 5 单击“收集日志”以开始日志收集进程。

管理控制台将日志收集进程的新条目添加到屏幕底部的“以前的日志收集”列表中。如果要检索多个日志文件，则需要定期刷新屏幕以确定日志收集进程何时完成。

注意：一次仅能运行一个日志收集进程。

- 6 要取消活动的日志收集进程，请单击日志收集条目旁的“取消”。如果一个或多个服务器处于脱机状态且收集进程无法完成，则您可能需要取消日志收集。当您取消日志收集时，ZIP 文件仅包含已成功收集的文件。

- 7 要将已收集的日志下载到本地计算机，请单击日志收集条目旁的“下载”。
- 8 要删除存储在 Enforce Server 上的 ZIP 文件，请单击日志收集条目旁的“删除”。

请参见第 240 页的[“日志收集和配置屏幕”](#)。

请参见第 233 页的[“关于日志文件”](#)。

关于日志事件代码

操作日志文件消息已格式化，以尽可能满足所涉及的各种协议的行业标准。这些日志消息包括描述特定任务（在记录消息时，软件试图执行）的事件代码。日志消息通常会格式化为：

Timestamp [Log Level] (Event Code) Event description [event parameters]

- 请参见第 248 页的[“Network and Mobile Prevent for Web 操作日志文件和事件代码”](#)。
- 请参见第 253 页的[“Network Prevent for Email 操作日志代码”](#)。
- 请参见第 256 页的[“Network Prevent for Email 产生的响应和代码”](#)。

Network and Mobile Prevent for Web 操作日志文件和事件代码

Network and Mobile Prevent for Web 日志文件名称的格式为 WebPrevent_OperationalX.log (其中 X 为数字)。可通过更改 FileReaderLogging.properties 文件中的值，来指定存储的文件数目及其大小。此文件位于 SymantecDLP\Protect\config 目录中。默认情况下，这些值为：

- com.vontu.icap.log.IcapOperationalLogHandler.limit = 5000000
- com.vontu.icap.log.IcapOperationalLogHandler.count = 5

表 13-6 按类别列出了定义的 Network and Mobile Prevent for Web 操作日志记录代码。文本的斜体部分包括事件参数。

表 13-6 Network and Mobile Prevent for Web 操作日志的状态代码

代码	文本和说明
操作事件	
1100	Starting Mobile Prevent for Web
1101	Shutting down Mobile Prevent for Web

代码	文本和说明
连接事件	
1200	<p>Listening for incoming connections at <i>icap_bind_address:icap_bind_port</i></p> <p>其中：</p> <ul style="list-style-type: none"> ■ <i>icap_bind_address</i> 是服务器侦听的 Network and Mobile Prevent for Web 绑定地址。此地址是使用“<i>Icap.BindAddress</i> 高级设置”指定的。 ■ <i>icap_bind_port</i> 是服务器侦听的端口。此端口是在“服务器”>“配置”页面中设置的。
1201	<p>Connection (<i>id=conn_id</i>) opened from host (<i>icap_client_ip:icap_client_port</i>)</p> <p>其中：</p> <ul style="list-style-type: none"> ■ <i>conn_id</i> 是分配给此连接的连接 ID。此 ID 有助于在多个日志间进行关联。 ■ <i>icap_client_ip</i> 和 <i>icap_client_port</i> 是用于执行到 Network and Mobile Prevent for Web 的连接操作的代理 IP 地址及端口。
1202	<p>Connection (<i>id=conn_id</i>) closed (<i>close_reason</i>)</p> <p>其中：</p> <ul style="list-style-type: none"> ■ <i>conn_id</i> 是分配给连接操作的连接 ID。 ■ <i>close_reason</i> 提供关闭连接的原因。
1203	<p>Connection states: REQMOD=N, RESPOND=N, OPTIONS=N, OTHERS=N</p> <p>其中，N 指出当记录此消息时处于各个状态下的连接的数目。</p> <p>此消息提供连接管理方面的系统状态。只要连接打开或关闭，都会被记录。</p>
连接错误	
5200	<p>Failed to create listener at <i>icap_bind_address:icap_bind_port</i></p> <p>其中：</p> <ul style="list-style-type: none"> ■ <i>icap_bind_address</i> 是服务器侦听的 Network and Mobile Prevent for Web 绑定地址。可使用“<i>Icap.BindAddress</i> 高级设置”指定此地址。 ■ <i>icap_bind_port</i> 是服务器侦听的端口。此端口是在“服务器”>“配置”页面上设置的。

代码	文本和说明
5201	Connection was rejected from unauthorized host (<i>host_ip:port</i>) 其中, <i>host_ip</i> 和 <i>port</i> 是用于尝试连接到 Network and Mobile Prevent for Web 的代理系统 IP 及端口地址。如果主机未列在“Icap.AllowHosts 高级”设置中，则不能形成连接。

请参见第 233 页的“[关于日志文件](#)”。

Network and Mobile Prevent for Web 访问日志文件和字段

Network and Mobile Prevent for Web 日志文件名称的格式为 `WebPrevent_AccessX.log` (其中 X 为数字)。可通过更改 `FileReaderLogging.properties` 文件中的值, 来指定存储的文件数目及其大小。默认情况下, 这些值为:

- `com.vontu.icap.log.IcapAccessLogHandler.limit = 5000000`
- `com.vontu.icap.log.IcapAccessLogHandler.count = 5`

Network and Mobile Prevent for Web 访问日志与代理服务器的 Web 访问日志类似。“启动”日志消息格式如下:

```
# Web Prevent starting: start_time
```

其中的 `start_time` 格式是 `date:time`, 例如: `13/Aug/2008:03:11:22:015-0700`。

说明消息格式如下:

```
# host_ip "auth_user" time_stamp "request_line" icap_status_code
request_size "referer" "user_agent" processing_time(ms) conn_id client_ip
client_port action_code icap_method_code traffic_source_code
```

表 13-7 列出了字段。此示例中包括在引号内的字段值, 在实际的消息中会括在引号内。如果不能判断字段值, 则消息会将 - 或 "" 显示为默认值。

表 13-7 Network and Mobile Prevent for Web 访问日志字段

字段	说明
<code>host_ip</code>	发出请求的主机 IP 地址。
<code>auth_user</code>	此请求的授权用户。
<code>time_stamp</code>	Network Prevent 和 Mobile Prevent 收到此请求的时间。
<code>request_line</code>	代表该请求的行。

字段	说明
icap_status_code	Network Prevent 和 Mobile Prevent 为此请求发送的 ICAP 响应码。
request_size	以字节为单位的请求大小。
referrer	请求的标头值，包括此请求的源 URI。
user_agent	与请求相关的用户代理。
processing_time (毫秒)	以微秒为单位的请求处理时间。这个值是接收时间、内容检测时间以及发送时间的总和。
conn_id	与请求相关的连接 ID。
client_ip	ICAP 客户端（代理）的 IP。
client_port	ICAP 客户端（代理）的端口。
action_code	表示 Network and Mobile Prevent for Web 所采取操作的整数。其中，操作码为下面的其中一个代码： <ul style="list-style-type: none">■ 0 = UNKNOWN■ 1 = ALLOW■ 2 = BLOCK■ 3 = REDACT■ 4 = ERROR■ 5 = ALLOW_WITHOUT_INSPECTION■ 6 = OPTIONS_RESPONSE■ 7 = REDIRECT
icap_method_code	代表与此请求相关的 ICAP 方法的整数。其中，ICAP 方法代码为下面的其中一个代码： <ul style="list-style-type: none">■ -1 = ILLEGAL■ 0 = OPTIONS■ 1 = REQMOD■ 2 = RESPMOD■ 3 = LOG
traffic_source_code	一个表示网络流量来源的整数。其中，通信来源代码为下面的其中一个代码： <ul style="list-style-type: none">■ 0 = MOBILE■ 1 = WEB■ 2 = UNKNOWN

请参见第 233 页的“[关于日志文件](#)”。

Network and Mobile Prevent for Web 协议调试日志文件

要启用 ICAP 跟踪记录，请将“`Icap.EnableTrace` 高级”设置设为 `true`，然后使用“`Icap.TraceFolder` 高级”设置，指定要接收跟踪的目录。必须重新启动 Symantec Data Loss Prevention 服务，此更改才会生效。

放置在指定目录中的跟踪文件的文件名采用以下格式：`时间戳-连接 ID`。跟踪文件的第一行提供有关连接的主机IP、端口以及时间戳的信息。从套接字中读取的数据以 `<<时间戳 读取的字节数` 格式显示。写入套接字的数据以 `>>时间戳 写入的字节数` 格式显示。最后一行将注明连接已关闭。

注意：跟踪记录会生成大量数据，因此需要大量的可用磁盘存储空间。跟踪记录应仅用于调试，因为数据会以纯文本写入文件。

请参见第 233 页的“[关于日志文件](#)”。

Network Prevent for Email 日志级别

Network Prevent for Email 日志文件名称的格式为 `EmailPrevent_OperationalX.log`（其中 `X` 为数字）。可通过更改 `FileReaderLogging.properties` 文件中的值，来指定存储的文件数目及其大小。默认情况下，这些值为：

- `com.vontu.mta.log.SmtpOperationalLogHandler.limit = 5000000`
- `com.vontu.mta.log.SmtpOperationalLogHandler.count = 5`

根据不同的日志级别，`com.vontu.mta.rp` 软件包中的组件会输出不同级别的详细信息。`com.vontu.mta.rp.level` 设置会在 `SymantecDLP\Protect\config` 目录下的 `RequestProcessorLogging.properties` 文件中指定日志级别。例如，`com.vontu.mta.rp.level = FINE` 会将详细信息级别指定为 `FINE`。

表 13-8 说明 Network Prevent for Email 日志级别。

表 13-8 Network Prevent for Email 日志级别

级别	准则
INFO	常规事件：连接与中断连接通知、有关每次连接时所处理的消息的信息。
FINE	其他一些执行跟踪信息。
FINER	信封命令流、消息标头、检测结果。
FINEST	完整的消息内容、最深入的执行跟踪和错误跟踪。

请参见第 233 页的“[关于日志文件](#)”。

Network Prevent for Email 操作日志代码

表 13-9 依类别列出了定义的 Network Prevent Email 操作日志代码。

表 13-9 Network Prevent for Email 操作日志的状态代码

代码	说明
核心事件	
1100	Starting Network Prevent for Email
1101	Shutting down Network Prevent for Email
1102	Reconnecting to FileReader (tid= <i>id</i>) 其中 <i>id</i> 为线程标识符。 RequestProcessor 会尝试重新创建与 FileReader 的连接，以进行检测。
1103	Reconnected to the FileReader successfully (tid= <i>id</i>) RequestProcessor 可重新创建至 FileReader 的连接。
核心错误	
5100	Could not connect to the FileReader (tid= <i>id</i> timeout=.3s) 尝试重新连接至 FileReader 的操作失败。
5101	FileReader connection lost (tid= <i>id</i>) RequestProcessor 至 FileReader 的连接已中断。
连接事件	
1200	Listening for incoming connections (local= <i>hostname</i>) <i>Hostnames</i> 是 IP 地址或完全限定域名。
1201	Connection accepted (tid= <i>id</i> cid=N local= <i>hostname:port</i> remote= <i>hostname:port</i>) 其中 N 为连接标识符。
1202	Peer disconnected (tid= <i>id</i> cid=N local= <i>hostname:port</i> remote= <i>hostname:port</i>)

代码	说明
1203	Forward connection established (tid=id cid=N local=hostname:port remote=hostname:port)
1204	Forward connection closed (tid=id cid=N local=hostname:port remote=hostname:port)
1205	Service connection closed (tid=id cid=N local=hostname:port remote=hostname:port messages=1 time=0.14s)
连接错误	
5200	Connection is rejected from the unauthorized host (tid=id local=hostname:port remote=hostname:port)
5201	Local connection error (tid=id cid=N local=hostname:port remote=hostname:port reason=Explanation)
5202	Sender connection error (tid=id cid=N local=hostname:port remote=hostname:port reason=Explanation)
5203	Forwarding connection error (tid=id cid=N local=hostname:port remote=hostname:port reason=Explanation)
5204	Peer disconnected unexpectedly (tid=id cid=N local=hostname:port remote=hostname:port reason=Explanation)
5205	Could not create listener (address=local=hostname:port reason=Explanation)
5206	Authorized MTAs contains invalid hosts: hostname, hostname, ...

代码	说明
5207	MTA restrictions are active, but no MTAs are authorized to communicate with this host
5208	TLS handshake failed (<i>reason=Explanation tid=id cid=N local=hostname remote=hostname</i>)
5209	TLS handshake completed (<i>tid=id cid=N local=hostname remote=hostname</i>)
5210	All forward hosts unavailable (<i>tid=id cid=N reason=Explanation</i>)
5211	DNS lookup failure (<i>tid=id cid=N NextHop=hostname reason=Explanation</i>)
5303	Failed to encrypt incoming message (<i>tid=id cid=N local=hostname remote=hostname</i>)
5304	Failed to decrypt outgoing message (<i>tid=id cid=N local=hostname remote=hostname</i>)
邮件事件	
1300	<p>Message complete (<i>cid=N message_id=3 dlp_id=message_identifier size=number sender=email_address recipient_count=N disposition=response estatus=statuscode rtime=N dtime=N mtime=N</i>)</p> <p>其中：</p> <ul style="list-style-type: none"> ■ Recipient_count 是“接受者”、“抄送”和“密件抄送”字段中地址的总数。 ■ Response 是 Network Prevent for Email 的响应，可以是下列其中之一： PASS、 BLOCK、 BLOCK_AND_REDIRECT、 REDIRECT、 MODIFY 或 ERROR。 ■ 此状态是增强状态代码。 <p>请参见第 256 页的“Network Prevent for Email 产生的响应和代码”。</p> <ul style="list-style-type: none"> ■ rtime 是 Network Prevent for Email 完全接收发送 MTA 所发送邮件的时间（以秒为单位）。 ■ dtime 是 Network Prevent for Email 对邮件执行检测的时间（以秒为单位）。 ■ mtime 是 Network Prevent for Email 处理“邮件错误”消息的时间总计（以秒为单位）。

代码	说明
邮件错误	
5300	Error while processing message (cid=N message_id=header_ID dlp_id=message_identifier size=0 sender=email_address recipient_count=N disposition=response estatus=statuscode rtime=N dtim=N mtime=N reason=Explanation 其中 header_ID 是“RFC 822 消息 ID”标头（如果存在）。
5301	Sender rejected during re-submit
5302	Recipient rejected during re-submit

请参见第 233 页的“[关于日志文件](#)”。

Network Prevent for Email 产生的响应和代码

Network Prevent for Email 生成下列响应。如果 Network Prevent for Email 将命令流响应从转发的 MTA 转发至发送的 MTA，则会产生其他协议响应。[表 13-10](#) 显示了在 Network Prevent 必须覆盖接收 MTA 时所生成的响应，还显示了 Network Prevent 对未自下游传送的事件生成特定响应的情况。

“增强状态”是与响应相关联的“RFC1893 增强状态代码”。

表 13-10 Network Prevent for Email 生成的响应

代码	增强状态	文本	说明
250	2.0.0	Ok: Carry on.	Network Prevent for Email 所使用的成功代码。
221	2.0.0	Service closing.	在没有处于活动状态的转发 MTA 连接的情况下收到 QUIT 请求时，Network Prevent for Email 所生成的正常连接终止代码。
451	4.3.0	Error: Processing error.	发生（潜在）可撤消错误时，会生成此“常规且暂时”的错误响应。如果无更具体的错误响应可用，则会使用此错误响应。转发连接有时会关闭，该连接的非预期终止有时会导致显示代码为 451、状态为 4.3.0 的响应。但是，除非发送 MTA 选择终止，否则在此情况下，发送连接应保持打开。

代码	增强状态	文本	说明
421	4.3.0	Fatal: Processing error. Closing connection.	发生严重且不可撤消的错误时，会生成此“常规且最终”的错误响应。此错误会导致发送者或接收人的所有连接立即终止。
421	4.4.1	Fatal: Forwarding agent unavailable.	尝试连接转发 MTA 被拒绝，或以其他方式不能正确创建连接。
421	4.4.2	Fatal: Connection lost to forwarding agent.	关闭连接。不能与发送 MTA 进一步对话时，中断转发 MTA 连接。此中断通常发生在对邮件标题或正文进行缓冲操作的过程中。会立即终止连接。
451	4.4.2	Error: Connection lost to forwarding agent.	转发 MTA 连接已中断，如果可以重新创建连接，则可恢复。除非发送 MTA 连接选择终止，否则将保留该连接。
421	4.4.7	Error: Request timeout exceeded.	发出的最后一个命令未在 RequestProcessor.DefaultCommandTimeout 定义的时间窗口（如果所发出的命令为“.”，则该时间窗口可能来自于 RequestProcessor.DotCommandTimeout）内接收到响应。会立即关闭连接。
421	4.4.7	Error: Connection timeout exceeded.	连接空闲（没有任何等候响应的活动命令）的时间超过 RequestProcessor.DefaultCommandTimeout 定义的时间段。
501	5.5.2	Fatal: Invalid transmission request.	发生了对 SMTP 协议（或其中的限制）的严重违规。此违规对重新发送邮件的尝试不会进行任何更改。仅在单个命令行或数据行超出 RequestProcessor.MaxLineLength 定义的边界时，才会发出此消息进行响应。

代码	增强状态	文本	说明
502	5.5.1	Error: Unrecognized command.	已定义但当前未使用。
550	5.7.1	User Supplied.	此代码与状态的组合表示已使用的“阻止”响应规则。 提供返回的文本，作为响应规则定义的一部分。

请注意，4xx 代码和 4.x.x 增强状态表示暂时错误。在此类情况下，MTA 可将邮件重新提交至 Network Prevent for Email Server。5xx 代码和 5.x.x 增强状态表示永久错误。在此类情况下，MTA 会将邮件视为不能传递。

请参见第 233 页的“[关于日志文件](#)”。

使用 Symantec Data Loss Prevention 实用程序

本章节包括下列主题：

- [关于 Symantec Data Loss Prevention 实用程序](#)
- [关于端点实用程序](#)
- [关于环境检查实用程序](#)
- [关于 DBPasswordChanger](#)
- [关于 sslkeytool 实用程序和服务器证书](#)
- [关于 SQL 预索引器](#)
- [关于远程 EDM 索引器](#)

关于 Symantec Data Loss Prevention 实用程序

Symantec 提供一套实用程序，可帮助用户完成不必经常执行的任务。实用程序通常会用于进行疑难解答和执行维护任务，也会用于准备数据和文件供 Symantec Data Loss Prevention 软件使用。

所提供的 Symantec Data Loss Prevention 实用程序适用于 Windows 和 Linux 操作系统。您可以在这两种操作系统上使用命令行运行实用程序。无论操作系统为何，实用程序都会以类似方式运行。

表 14-1 说明了如何以及何时使用每个实用程序。

表 14-1 Symantec Data Loss Prevention 实用程序

名称	说明
环境检查实用程序	审核 Symantec Data Loss Prevention 服务器系统的环境，并将信息收集到 ZIP 文件中。Symantec 支持部门可使用该 ZIP 文件来解答疑难问题。 请参见第 261 页的“ 关于环境检查实用程序 ”。
DBPasswordChanger	更改 Enforce Server 连接至 Oracle 数据库所用的加密密码。 请参见第 263 页的“ 关于 DBPasswordChanger ”。
sslkeytool	生成自定义身份验证密钥，以提高 Enforce Server 和检测服务器之间传输的数据的安全性。自定义身份验证密钥必须复制到每个 Symantec Data Loss Prevention 服务器。 请参见第 264 页的“ 关于 sslkeytool 实用程序和服务器证书 ”。
SQL 预索引器	创建 SQL 数据库的索引，或对数据库内的特定数据表运行 SQL 查询。此实用程序设计用于通过管道将输出直接传输到远程 EDM 索引器实用程序。 请参见第 269 页的“ 关于 SQL 预索引器 ”。
远程 EDM 索引器	将逗号分隔或 Tab 符分隔的数据文件转换成确切数据匹配索引。您可以在远程计算机上运行该实用程序，以提供 Enforce Server 本地可用的相同索引功能。 此实用程序通常会与 SQL 预索引器结合使用。SQL 预索引器可以运行 SQL 查询，并将生成的数据直接传递到远程 EDM 索引器以创建 EDM 索引。 请参见第 272 页的“ 关于远程 EDM 索引器 ”。

关于端点实用程序

表 14-2 介绍了适用于端点产品的实用程序。

请参见第 1127 页的“[关于 Endpoint Discover 和 Endpoint Prevent](#)”。

请参见第 1211 页的“[关于端点工具](#)”。

表 14-2 端点实用程序

名称	说明
endpointkeytool	endpointkeytool 实用程序会创建一个新的身份验证密钥，用来加密 Endpoint Server 和 Symantec DLP Agent 之间的通信。新的身份验证密钥会替换硬编码的 AES 密钥。请先使用 endpointkeytool 生成新的身份验证密钥，然后在端点计算机上安装 Symantec DLP Agent。
Service_Shutdown.exe	该实用程序可让管理员在端点计算机上同时关闭代理和看门狗服务。（为了防止篡改，用户不能停止代理或看门狗服务。）
vontu_sqlite3.exe	该实用程序提供了一个 SQL 接口，通过此接口，可以查看或修改 Symantec DLP Agent 所使用的加密数据库文件。要调查或更改 Symantec Data Loss Prevention 文件时，请使用此工具。
logdump.exe	通过该工具，可以查看 Symantec DLP Agent 所扩展的日志文件，这些文件因为安全原因而被隐藏。

关于环境检查实用程序

环境检查实用程序 (ECU) 可验证 Symantec Data Loss Prevention 服务器的运行环境。ECU 是随 Enforce Server 和检测服务器一起安装的故障排除工具。在大多情况下，信息从 Enforce Server 及其检测服务器处收集。仅当您在 Enforce Server 上运行该实用程序时才会执行一些检查。

有关在 Enforce Server 和检测服务器上执行的任务的说明，请参见 [表 14-3](#)。

表 14-3 环境检查实用程序任务

任务	服务器类型
<ul style="list-style-type: none"> ■ 检查并显示 Windows 或 Linux 操作系统版本。 ■ 验证必要的 Symantec Data Loss Prevention 服务是否已在运行中。 ■ 显示完整的 Symantec Data Loss Prevention 版本号码。 ■ 检查主机配置文件并将配置写入日志文件。 	Enforce Server 或检测服务器

任务	服务器类型
<ul style="list-style-type: none"> ■ 检查 Enforce Server 安装期间所创建的“系统帐户”用户是否存在。 ■ 检查每个已注册的检测服务器的已存储设置，并将信息写入 /Vontu/Protect/ECU/eculogs/monitorSettings 目录。 ■ 运行 Symantec Data Loss Prevention Notification and Lock Manager 服务来检查 Oracle 数据库。 ■ 检查从 Enforce Server 到每个已注册检测服务器之间的网络连接。 	Enforce Server

如果遇到安装问题，Symantec 支持部门可能会要求您运行此工具，来收集有关系统环境的信息。

在 Windows 上运行环境检查实用程序

如果使用默认安装目录，则环境检查实用程序位于 c:\Vontu\Protect\ECU 目录中。

在 Windows 上运行 ECU

- 1 从 Windows 的“开始”菜单，选择“运行”，然后在出现的“运行”对话框中，键入 cmd，以打开命令提示窗口。
- 2 转至 ECU 文件夹（如果安装在默认位置，则为 c:\Vontu\Protect\ECU）。
- 3 执行该实用程序：

EnvironmentCheckUtility.exe

请参见第 263 页的“[关于环境检查实用程序输出](#)”。

在 Linux 上运行环境检查实用程序

如果使用默认安装目录，则环境检查实用程序位于 /opt/Vontu/Protect/ECU 目录中。

在 Linux 上运行 ECU

1 键入以下命令，以 protect 用户身份登录：

```
su protect
```

2 转至 ECU 目录。如果在安装期间使用了默认值，请键入：

```
cd /opt/Vontu/Protect/ECU
```

3 执行该实用程序：

```
./EnvironmentCheckUtility
```

请参见第 263 页的“[关于环境检查实用程序输出](#)”。

关于环境检查实用程序输出

在运行环境检查实用程序时，它会在 ECU 子目录中生成一个 `eculogs.zip` 文件。该 ZIP 文件中包含数个具有系统信息的文件。如果该实用程序在 Enforce Server 计算机上运行，它还会生成名为 `eculogs\monitorSettings` 的子目录，该目录包含各个已注册检测服务器的相关信息。

存储在 `eculogs.zip` 中的输出文件如下：

- `ECUoutput.txt` 包含测试结果（通过或失败）以及测试失败的可能原因。
- `ecu_error_log.txt` 会记录该实用程序运行测试期间所发生的任何错误。
- `ecu_HostFileLog.txt` 包含主机文件内容的转储。
- `server_nameSettings.txt` 文件会记录已注册检测服务器的设置。只在 Enforce Server 计算机上会生成这些文件和 `eculogs/monitorSettings` 目录。

在创建 `eculogs.zip` 文件之后，请将它发送给 Symantec 支持部门以进一步进行分析。

请参见第 233 页的“[关于日志文件](#)”。

关于 DBPasswordChanger

Symantec Data Loss Prevention 会将 Oracle 数据库的加密密码存储在一个名为 `DatabasePassword.properties` 的文件中，该文件位于 `c:\Vontu\Protect\config (Windows)` 中或 `/opt/Vontu/Protect/config (Linux)` 中。由于文件的内容经过加密，因此您不能直接修改文件。DBPasswordChanger 实用程序可更改 Enforce Server 使用的已存储 Oracle 数据库密码。

必须先执行以下操作，才可以使用 DBPasswordChanger 更改 Oracle 数据库的密码：

- 关闭 Enforce Server。
- 使用 Oracle 实用程序更改 Oracle 数据库密码。

请参见第 264 页的“[使用 DBPasswordChanger 的示例](#)”。

DBPasswordChanger 语法

DBPasswordChanger 实用程序使用以下语法：

```
DBPasswordChanger password_file new_oracle_password
```

所有的命令行参数均为必需条目。下表说明每个命令行参数。

请参见第 264 页的“[使用 DBPasswordChanger 的示例](#)”。

表 14-4 DBPasswordChanger 命令行参数

参数	说明
<i>password_file</i>	指定包含加密密码的文件。默认情况下，此文件名为 ProtectPassword.properties，存储在 \Vontu\Protect\config (Windows) 或 /opt/Vontu/Protect/config (Linux) 中。
<i>new_oracle_password</i>	指定要加密和存储的新 Oracle 密码。

使用 DBPasswordChanger 的示例

如果 Symantec Data Loss Prevention 安装在默认位置，则 DBPasswordChanger 实用程序位于 c:\Vontu\Protect\bin (Windows) 或 /opt/Vontu/Protect/bin (Linux)。您必须是管理员（或根用户）才能运行 DBPasswordChanger。

例如，键入：

```
DBPasswordChanger \Vontu\Protect\bin\DatabasePassword.properties
protect_oracle
```

请参见第 264 页的“[DBPasswordChanger 语法](#)”。

关于 sslkeytool 实用程序和服务器证书

Symantec Data Loss Prevention 使用安全套接字层/传输层安全 (SSL/TLS) 来加密在服务器间传输的所有数据。Symantec Data Loss Prevention 还使用 SSL/TLS 协议在服务器间进行相互验证。服务器会通过强制使用客户端和服务器端证书来实现

身份验证。默认情况下，服务器之间的连接会使用单个自我签署的证书，该证书会安全地嵌入在 Symantec Data Loss Prevention 软件中。客户端所有 Symantec Data Loss Prevention 安装都使用该证书。

对于贵组织的安装，Symantec 建议您使用唯一的自我签署证书替换默认证书。请在 Enforce Server 上以及与其通信的每个检测服务器上各存储一份证书。这些证书是使用 sslkeytool 实用程序生成的。

注意：如果是在托管环境中安装 Network Prevent 检测服务器，则必须为 Symantec Data Loss Prevention 服务器生成唯一证书。不能使用内置的证书与托管的 Network Prevent 服务器进行通信。

注意：Symantec 建议您创建专用证书来与 Symantec Data Loss Prevention 服务器进行通信。若将 Enforce Server 配置为使用生成的证书，则安装中的所有检测服务器也必须使用生成的证书。不能对某些检测服务器使用内置的证书，也不能对其他服务器使用内置的证书。

请参见第 265 页的“[关于 sslkeytool 命令行选项](#)”。

请参见第 266 页的“[使用 sslkeytool 生成新的 Enforce Server 证书和检测服务器证书](#)”。

请参见第 268 页的“[使用 sslkeytool 添加新的检测服务器证书](#)”。

关于 sslkeytool 命令行选项

sslkeytool 是一个命令行应用程序，可用于生成唯一的一对 SSL 证书（keystore 文件）。sslkeytool 位于 \SymantecDLP\Protect\bin 目录 (Windows) 或 /opt/SymantecDLP/Protect/bin 目录 (Linux)。它必须以 Symantec Data Loss Prevention 操作系统用户帐户（默认为 protect）运行。此外，必须直接在 Enforce Server 计算机上运行 sslkeytool。

sslkeytool 可以使用下列命令格式和选项：

■ `-genkey [-dir=directory -alias=aliasFile]`

默认情况下，将生成两个唯一证书（keystore 文件）：一个用于 Enforce Server，另一个用于其他检测服务器。可选的 -dir 参数指定放置 keystore 文件的目录。可选的 -alias 参数可为 aliasFile 中指定的每个别名生成其他 keystore 文件。可以使用别名文件为系统中的每个检测服务器生成唯一证书（而不是在所有检测服务器上使用同一证书）。首次为 Symantec Data Loss Prevention 安装生成唯一证书时，请使用此命令格式。

■ `-list=file`

列出指定的 keystore 文件的内容。

■ `-alias=aliasFile -enforce=enforceKeystoreFile [-dir=directory]`

使用您在 *aliasFile* 中定义的别名为检测服务器生成多个证书文件。在生成新的检测服务器 keystore 文件时，必须指定要使用的现有 Enforce Server keystore 文件。可选的 *-dir* 参数指定放置 keystore 文件的目录。如果指定 *-dir* 参数，还必须将 Enforce Server keystore 文件放在指定目录中。使用此命令格式可将新的检测服务器证书添加到现有的 Symantec Data Loss Prevention 安装。

例如，命令 `sslkeytool -genkey` 会生成两个文件：

■ `enforce.timestamp.sslKeyStore`

■ `monitor.timestamp.sslKeyStore`

除非您使用 *-dir* 参数指定不同的目录，否则，这两个 keystore 文件会在 `sslkeytool` 应用程序所在的 `bin` 目录中创建。

请参见第 264 页的“[关于 sslkeytool 实用程序和服务器证书](#)”。

请参见第 266 页的“[使用 sslkeytool 生成新的 Enforce Server 证书和检测服务器证书](#)”。

请参见第 268 页的“[使用 sslkeytool 添加新的检测服务器证书](#)”。

使用 `sslkeytool` 生成新的 Enforce Server 证书和检测服务器证书

安装 Symantec Data Loss Prevention 后，请使用带有 `-genkey` 参数的 `sslkeytool`，为 Enforce Server 和检测服务器生成新的证书。Symantec 建议您使用唯一的自我签署证书替换用来保护服务器之间的通信的默认证书。`-genkey` 参数会自动生成两个证书文件。请将其中一个证书存储在 Enforce Server 上，并将第二个证书存储在每个检测服务器上。通过可选的 `-alias` 命令，可以为系统中的每个检测服务器生成唯一的证书文件。要使用 `-alias`，必须首先创建一个别名文件以列出要创建的每个别名名称。

生成 Symantec Data Loss Prevention 服务器的唯一证书

- 1 使用在 Symantec Data Loss Prevention 安装期间所创建的 `protect` 用户帐户登录到 Enforce Server 计算机。
- 2 从命令窗口，转至存储 `sslkeytool` 实用程序的 `c:\SymantecDLP\Protect\bin` 目录。

- 3 如果要为每个检测服务器创建专用证书文件，首先请创建一个文本文件以列出要创建的别名名称。将每个别名放在单独一行上。例如：

```
net_monitor01
protect01
endpoint01
smtp_prevent01
web_prevent01
classification01
```

注意：-genkey 参数会自动为 enforce 和 monitor 别名创建证书。不要将这些别名添加到您的自定义别名文件中。

- 4 运行带有 -genkey 参数和 -dir 可选参数的 sslkeytool 实用程序，以指定输出目录。如果创建了自定义别名文件，则还需要指定可选的 -alias 参数，如本示例中所示：

这会在指定的目录中生成新的证书（keystore 文件）。并且会使用 -genkey 参数自动生成两个文件：

- enforce.timestamp.sslKeyStore
- monitor.timestamp.sslKeyStore

sslkeytool 还会为别名文件中定义的所有别名生成单独的文件。例如：

- net_monitor01.timestamp.sslKeyStore
- protect01.timestamp.sslKeyStore
- endpoint01.timestamp.sslKeyStore
- smtp_prevent01.timestamp.sslKeyStore
- web_prevent01.timestamp.sslKeyStore
- classification01.timestamp.sslKeyStore

- 5 将名称以 enforce 开头的证书文件复制到 Enforce Server 上的 c:\SymantecDLP\Protect\keystore 目录。
- 6 如果您想要对所有检测服务器使用同一个证书文件，请将名称以 monitor 开头的证书文件复制到系统中每一个检测服务器上的 c:\SymantecDLP\Protect\keystore 目录。

如果为系统中每个检测服务器生成了唯一证书文件，请将相应的证书文件复制到每台检测服务器计算机上的 keystore 目录。

- 7 删除或保护证书文件的任何其他副本，防止对生成的密钥进行未授权的访问。
- 8 重新启动 Enforce Server 上的 Vontu Monitor Controller 服务和检测服务器上的 Vontu Monitor 服务。

在安装 Symantec Data Loss Prevention 服务器时，安装程序会在 `keystore` 目录中创建一个默认的 `keystore`。将生成的证书文件复制到此目录时，该生成的文件会覆盖默认证书。如果以后从 `keystore` 目录中删除该证书文件，Symantec Data Loss Prevention 会恢复为嵌入在应用程序中的默认 `keystore` 文件。此行为可确保数据通信始终受到保护。但是请注意，您不能对某些服务器使用内置的证书，也不能对其他服务器使用生成的证书。Symantec Data Loss Prevention 系统中的所有服务器必须使用内置的证书或自定义证书。

注意：如果 `keystore` 目录中有多个 `keystore` 文件，则不会启动服务器。

请参见第 268 页的“[使用 sslkeytool 添加新的检测服务器证书](#)”。

请参见第 265 页的“[关于 sslkeytool 命令行选项](#)”。

请参见第 264 页的“[关于 sslkeytool 实用程序和服务器证书](#)”。

使用 sslkeytool 添加新的检测服务器证书

使用带有 `-alias` 参数的 `sslkeytool` 为现有的 Symantec Data Loss Prevention 部署生成新证书文件。使用这种命令形式时，必须提供当前 Enforce Server Keystore 文件，以便 `sslkeytool` 可以在生成的新检测服务器证书文件中嵌入 Enforce Server 证书。

生成新的检测服务器证书

- 1 使用在 Symantec Data Loss Prevention 安装过程中创建的 `protect` 用户帐户登录 Enforce Server 计算机。
- 2 从命令窗口，转至存储 `sslkeytool` 实用程序的 `c:\SymantecDLP\Protect\bin` 目录。
- 3 创建将存储新的检测服务器证书文件的目录。例如：

```
mkdir new_certificates
```

- 4 将 Enforce Server 证书文件复制到新目录。例如：
- 5 创建列出要创建的新服务器别名的文本文件。将每个别名放在单独一行上。例如：

```
endpoint02
smtp_prevent02
```

- 6 运行带有 `-alias` 参数和 `-dir` 参数的 `sslkeytool` 实用程序以指定输出目录。此外，指定已复制到证书目录的 Enforce Server 证书文件的名称。例如：
这将为每个别名生成新的证书文件，并将新文件存储在指定目录中。每个证书文件还包括您指定的 Enforce Keystore 中的 Enforce Server 证书。
- 7 将每个新证书文件复制到相应检测服务器计算机上的 `c:\SymantecDLP\Protect\keystore` 目录中。
- 8 删除或保护证书文件的任何其他副本，防止对生成的密钥进行未授权的访问。
- 9 在每个检测服务器上重新启动 Vontu Monitor 服务以使用新证书文件。

验证服务器证书用法

Symantec Data Loss Prevention 使用系统事件来指示服务器是使用内置证书还是用户生成的证书来保护通信。如果服务器使用默认的内置证书，Symantec Data Loss Prevention 将生成警告事件。如果服务器使用生成的证书，Symantec Data Loss Prevention 将生成信息事件。

为提高安全性，Symantec 建议您使用生成的证书而不是内置证书。

如果将 Network Prevent 安装到托管环境中，则无法使用内置证书，必须为 Enforce Server 和检测服务器生成唯一证书并将其用于这些服务器。

确定 Symantec Data Loss Prevention 使用的证书类型

- 1 启动 Enforce Server 或重新启动 Enforce Server 计算机上的 Vontu Monitor Controller 服务。
- 2 启动每台检测服务器，或重新启动每台检测服务器计算机上的 Vontu Monitor 服务。
- 3 登录到 Enforce Server 管理控制台。
- 4 选择“系统”>“服务器”>“警报”。
- 5 检查警报列表，以确定 Symantec Data Loss Prevention 服务器使用的证书类型：
 - 如果服务器使用内置证书，Enforce Server 将显示代码为 2709 的警告事件：使用内置证书。
 - 如果服务器使用唯一生成的证书，Enforce Server 将显示代码为 2710 的信息事件：使用用户生成的证书。

关于 SQL 预索引器

本章说明如何使用 SQL 预索引器。SQL 预索引器实用程序通常会与远程 EDM 索引器实用程序结合使用。它会在安装远程 EDM 索引器期间，安装在

\Vontu\Protect\bin 目录中。SQL 预索引器实用程序会直接从 SQL 数据库生成索引。它会处理数据库查询，然后用管道将其传输到远程 EDM 索引器实用程序。

在运行 SQL 预索引器之前，请先阅读本指南中有关远程 EDM 索引器的章节。

请参见第 272 页的“[关于远程 EDM 索引器](#)”。

SQL 预索引器可从命令行运行。如果在 Linux 上运行，请将用户更改为 protect 用户，然后再运行 SQL 预索引器（安装程序会创建 protect 用户）。SQL 预索引器仅支持 Oracle 数据库。

以下是运行 SQL 预索引器的命令示例。SQL 预索引器会运行 SQL 查询，以便从 Oracle 数据库中的员工数据表捕获姓名和薪资数据。此示例显示如何将 SQL 查询的输出用管道传输到远程 EDM 索引器。远程 EDM 索引器会使用 ExportEDMProfile.edm 配置文件来创建结果的索引。生成的索引文件会存储在 EDMIndexDirectory 文件夹中。

```
SqlPreindexer -alias=@//myhost:1521/orcl -username=scott -password=tiger -query="SELECT name, salary FROM employee" | RemoteEDMIndexer -profile=C:\ExportEDMProfile.edm -result=C:\EDMIndexDirectory\
```

由于输出是从 SQL 预索引器用管道传输到远程 EDM 索引器，因此请查看有关远程 EDM 索引器命令功能和选项的章节。

请参见第 261 页的[表 14-2](#)。

SQL 预索引器命令功能和选项

SQL 预索引器需要 `-alias` 选项和 `-username` 选项。下表说明了 SQL 预索引器的所有命令选项。如果您忽略了 `-query` 选项，则该实用程序便会创建整个数据库的索引。

SQL 预索引器命令具有以下选项：

<code>-alias</code>	按以下格式指定用于连接数到数据库的数据库别名： @//localhost:port/sid 例如：@//myhost:1521/orcl 此选项为必需。
<code>-driver</code>	指定 JDBC 驱动程序类别（例如， <code>oracle.jdbc.driver.OracleDriver</code> ）。
<code>-encoding</code>	指定要创建索引的数据的字符编码。默认为 iso-8859-1，但是具有非英语字符的数据应该使用 UTF-8 或 UTF-16。
<code>-password</code>	指定数据库的密码。如果未指定此选项，便会从 <code>stdin</code> 读取密码。
<code>-query</code>	指定要运行的 SQL 查询。

-query_path	指定包含要运行的 SQL 查询的文件路径。当查询是长 SQL 语句时，可使用此选项来替代 -query。
-separator	指定输出列分隔符为逗号、竖线还是 Tab 符。默认分隔符为 Tab 符。若要指定逗号或竖线作为分隔符，请用引号将该字符括起来，如 "," 或 " "。
-subprotocol	指定 JDBC 连接字符串的子协议（例如，oracle:thin）。
-username	指定数据库用户的名称。此选项为必需。
-verbose	显示完成索引时创建索引操作的统计摘要。

请参见第 271 页的“[排除预索引错误](#)”。

排除预索引错误

在创建大量数据的索引时，可能会出现错误。通常，数据集会包含不完整、不一致或不准确的数据记录。数据行包括的列数若超出预期，或所含列数据类型不正确时，通常会无法正确创建索引，也无法识别。

SQL 预索引器可以配置为在完成索引时，提供创建索引操作的相关信息摘要。若要执行此操作，请在运行 SQL 预索引器时指定 verbose 选项。

若要查看远程 EDM 索引器并未创建索引的数据行，请使用以下过程调整 `Indexer.properties` 文件中的配置。

记录未创建索引的数据行

- 1 找出位于 `\Program Files\Vontu\Protect\config\Indexer.properties` (Windows) 或 `/opt/Vontu/Protect/confide/Indexer.properties` (Linux) 的 `Indexer.properties` 文件。
- 2 使用文本编辑器打开文件。
- 3 找出 `create_error_file` 属性，并将 `false` 设置更改为 `true`。
- 4 保存并关闭 `Indexer.properties` 文件。

远程 EDM 索引器会将错误记录在名称与正在创建索引的数据文件相同，且后缀为 `.err` 的文件中。

错误文件中所列出的数据行未经加密。请保护错误文件，防止数据暴露，以最大限度地降低任何安全风险。

请参见第 269 页的“[关于 SQL 预索引器](#)”。

关于远程 EDM 索引器

远程 EDM 索引器是一种实用程序，可将逗号分隔值或 Tab 符分隔的数据文件转换成确切数据匹配索引。该实用程序类似于 Enforce Server 所用的本地 EDM 索引器。不过，远程 EDM 索引器旨在用于不属于 Symantec Data Loss Prevention 服务器配置的计算机。

使用远程 EDM 索引器对远程计算机上的数据源编制索引比使用 Enforce Server 上的 EDM 索引器具有以下优势：

- 可让数据所有者（而非 Symantec Data Loss Prevention 管理员）创建数据的索引。
- 可将创建索引所需的系统负载转移到另一台计算机上。Enforce Server 上的 CPU 和 RAM 则留给其他任务使用。

SQL 预索引器通常会与远程 EDM 索引器结合使用。SQL 预索引器用于对 SQL 数据库运行 SQL 查询，并将生成的数据传递到远程 EDM 索引器。

请参见第 269 页的“[关于 SQL 预索引器](#)”。

请参见第 272 页的“[使用远程 EDM 索引器](#)”。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

远程 EDM 索引器的系统要求

远程 EDM 索引器可在 Symantec Data Loss Prevention 服务器所支持的 Windows 和 Linux 操作系统上运行。

有关操作系统要求的更多信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。

远程 EDM 紴引器的 RAM 要求视创建索引的数据文件的大小而异。可以从通用台式机为包含不到 100 万行记录的数据文件创建索引。而包含超过 100 万行记录的数据文件则应该在至少配备 4 GB 专用 RAM 的计算机上运行。创建数据文件索引所需的时间取决于行中的列数。列越多，创建索引所需的时间就越长。

使用远程 EDM 紴引器

本节简要的介绍在远程计算机上创建数据文件的索引，然后在 Symantec Data Loss Prevention 中使用该索引的步骤。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

表 14-5 使用远程 EDM 索引器的步骤

步骤	操作	说明
步骤 1	在不属于 Symantec Data Loss Prevention 系统的计算机上安装远程 EDM 索引器。	请参见第 273 页的“ 安装远程 EDM 索引器 ”。 请参见第 274 页的“ 从命令行进行安装（适用于 Linux） ”。
步骤 2	在 Enforce Server 上创建要与远程 EDM 索引器结合使用的确切数据配置文件。	请参见第 275 页的“ 创建 EDM 配置文件以便远程编制索引 ”。
步骤 3	将这个确切数据配置文件复制到远程 EDM 索引器所在的计算机上。	请参见第 275 页的“ 创建 EDM 配置文件以便远程编制索引 ”。
步骤 4	运行远程 EDM 紴引器并创建索引文件。	请参见第 277 页的“ 远程 EDM 索引器命令选项 ”。
步骤 5	将索引文件从远程计算机复制到 Enforce Server。	请参见第 278 页的“ 复制和使用生成的索引文件 ”。
步骤 6	将索引文件加载到 Enforce Server。	请参见第 278 页的“ 复制和使用生成的索引文件 ”。
步骤 7	对编制索引过程中发生的所有问题进行故障排除。	请参见第 278 页的“ 疑难解答索引作业 ”。

安装远程 EDM 索引器

与其他的 Symantec Data Loss Prevention 组件一样，远程 EDM 索引器也是使用相同的安装程序来进行安装。请将 ProtectInstaller_11.1.exe 文件复制到需创建索引的数据所在的远程计算机上。在 Linux 版的 Symantec Data Loss Prevention 可使用的安装程序中，有一个文本命令控制台选项。

请参见第 274 页的“[从命令行进行安装（适用于 Linux）](#)”。

注意：Symantec 建议您先禁用所有防病毒软件、弹出式阻止程序及注册表防护软件，然后再开始安装过程。

要导航整个安装过程：

- 单击“下一步”显示下一个安装屏幕。
- 单击“上一步”返回到上一个安装屏幕。
- 单击“取消”终止安装过程。

安装远程 EDM 索引器

- 1 转至已将 `ProtectInstaller_11.1.exe` (Windows) 或 `ProtectInstaller_11.1.sh` (Linux) 文件复制至其中的目录。
在某些情况下，您可能需要更改文件权限以便访问该文件。
 - 2 运行安装程序 (`ProtectInstaller_11.1.exe` 或 `ProtectInstaller_11.1.sh`)。
随即解压缩安装程序文件并显示 Welcome 屏幕。
 - 3 单击 **Next**，然后接受 Symantec 软件授权许可协议以继续。
 - 4 从出现的组件列表中选择 **Indexer**，然后单击 **Next**。
 - 5 在 **Select Destination Directory** 屏幕中，单击 **Next**，接受默认安装位置（建议）。或者，单击 **Browse** 导航至其他安装位置，然后单击 **Next**。
 - 6 若为 Windows，请选择“开始”菜单文件夹，然后单击 **Next**。
 - 7 随即出现安装屏幕，并显示安装进度栏。显示提示时，请单击 **Finish** 完成安装。
- 请参见第 279 页的“[在 Windows 平台上卸载远程索引器](#)”。

从命令行进行安装（适用于 Linux）

以下过程说明如何在 Linux 中从命令行进行安装。

安装远程 EDM 索引器

- 1 以根用户的身份登录，然后将 `ProtectInstaller_11.1.sh` 文件复制到计算机上的 `/tmp` 目录。
- 2 键入以下命令，将目录更改为 `/tmp`:
`cd /tmp`
- 3 您可能需要先更改文件的权限，然后才能运行文件。若是如此，请键入:
`chmod 775 ProtectInstaller_11.1.sh`
- 4 更改文件权限之后，您就可以键入以下命令来运行 `ProtectInstaller_11.1.sh` 文件:
`./ProtectInstaller_11.1.sh -i console`

控制台模式安装启动后，就会显示“简介”步骤。在大多数情况下，建议您在安装期间尽可能使用默认值。按 **Enter** 继续下一个步骤。

- 5 在“选择安装集”步骤中，请指定要安装的组件。要安装远程 EDM 索引器，请键入选项旁的数字，然后按**Enter**。
- 6 在“安装文件夹”步骤中，键入要安装文件的目录的绝对路径。您可以按**Enter** 选择默认位置。
- 7 在“安装前摘要”步骤中，查看您所选择的安装配置。如果您满意所选择的条目，请按**Enter** 开始安装。或者，键入**back** 并按**Enter**，直到出现您要更改的步骤。
- 8 安装完成后，请按**Enter** 关闭安装程序。

请参见第 279 页的[“在 Linux 平台上卸载远程索引器”](#)。

创建 EDM 配置文件以便远程编制索引

EDM 索引器会在运行时使用确切数据配置文件，以确保数据正确格式化。在使用远程 EDM 索引器之前，必须创建确切数据配置文件。此配置文件是一个模板，会说明组织数据所用的列，不需要包含任何数据。创建配置文件后，请将它复制到运行远程 EDM 索引器的计算机上。

请参见第 278 页的[“复制和使用生成的索引文件”](#)。

请参见第 356 页的[“关于实施确切数据匹配”](#)。

创建 EDM 配置文件以便远程创建索引

- 1 在 Enforce Server 管理控制台中，导航至“管理”>“数据配置文件”>“确切数据”屏幕。
- 2 单击“添加确切数据配置文件”。
- 3 在“名称”字段中，输入配置文件的名称。
- 4 在“数据源”字段中，选择“使用此文件名”，然后输入要创建的索引文件的名称。
- 5 在“列数”文本框中，指定数据源中要创建索引的列数。
- 6 如果数据源的第一行包含列名，请选择选项“将第一行读作列名”。
- 7 在“错误阈值”文本框中，输入可包含错误的行数的百分比上限。

如果在编制数据源索引期间，含错误的行数超出此处所指定的百分比，则编制索引操作会失败。
- 8 在“列分隔符”字段中，选择在数据源中分隔数据列所使用的字符类型。
- 9 在“文件编码”字段中，选择数据源中所用的字符编码。

如果使用的是拉丁字符，请选择 ISO-8859-1 选项。若为东亚语言，请使用 UTF-8 或 UTF-16 选项。

- 10 单击“下一步”，将列标题从数据源映射到配置文件。
- 11 在“字段映射”部分，通过从“系统字段”下拉列表中选择列名，将“数据源字段”映射到每个列的“系统字段”。

“数据源字段”会列出您在上一屏幕中指定的列数。“系统字段”包含标准列标题的列表。如果数据源中有任何列标题与“系统字段”列表中的可用选项匹配，请分别进行相应的映射。请确保使“系统字段”列中的选项与其在“数据源字段”中的相应编号列匹配。

例如，对于您在配置文件中已指定的具有三列的数据源，映射配置可能如下：

数据源字段	系统字段
第 1 列	名字
第 2 列	姓氏
第 3 列	社会安全号

- 12 如果“数据源字段”没有映射到“系统字段”列的可用选项中的标题值，请单击“高级视图”链接。

在“高级视图”中，系统会在“系统字段”列旁边显示一个“自定义名称”列。

在文本框中输入与数据源中相应列对应的正确列名称。

或者，可以通过从“类型”下拉列表中选择数据类型，指定所输入的“自定义名称”的数据类型。这些数据类型是系统定义的。单击“类型”名称旁边的“说明”链接，可查看有关系统定义的每个数据类型的详细信息。

- 13 如果您打算使用确切数据配置文件来实施包含一个或多个 EDM 规则的策略模板，则可以针对该模板验证您的配置文件映射。要执行此操作，请从“针对策略模板检查映射”下拉列表中选择模板，然后单击“立即检查”。系统会指出模板所需的所有未映射字段。

- 14 如果您打算远程编制索引，请不要选择此屏幕中提供的任何“编制索引”选项。

- 15 单击“完成”以完成配置文件创建过程。

- 16 完成确切数据配置文件的配置后，在“管理”>“数据配置文件”>“确切数据”屏幕上单击“下载配置文件”链接。

系统会提示您将 EDM 配置文件保存为文件。文件扩展名为*.edm。请将文件保存到您打算运行远程 EDM 索引器实用程序的远程计算机上。

远程 EDM 索引器命令选项

您可以从命令行运行索引器。如果在 Linux 上, 请将用户更改为 `protect` 用户, 然后再运行索引器。(安装程序会创建 `protect` 用户)。

使用远程 EDM 索引器时, 需要 `data`、`profile` 和 `result` 选项。但是, 如果未指定 `data` 选项, 则实用程序默认会读取 `stdin`。通常, 会从 SQL 预索引器实用程序管道传输数据。

[表 14-6](#) 描述了远程 EDM 索引器的命令选项。

表 14-6 远程 EDM 索引器选项

选项	说明
<code>-data</code>	指定包括要创建索引的数据的文件。如果未指定此选项, 则实用程序会从 <code>stdin</code> 读取数据。
<code>-encoding</code>	指定要创建索引的数据的字符编码。默认为 ISO-8859-1, 但是具有非英语字符的数据应该使用 UTF-8 或 UTF-16。此为可选项。
<code>-ignore_date</code>	如果配置文件已过期, 则会覆盖确切数据配置文件的过期日期。(默认情况下, 确切数据配置文件会在 30 天后到期。) 此为可选项。
<code>-profile</code>	指定要使用的确切数据配置文件。(此配置文件就是在 Enforce Server 管理控制台的“确切数据”屏幕上, 单击“下载链接”时所选择的配置文件。) 此为必需项。
<code>-result</code>	指定生成索引文件的目录。此为必需项。
<code>-verbose</code>	显示完成索引时创建索引操作的统计摘要。此为可选项。

例如, 若要指定名为 `ExportEDMProfile.edm` 的配置文件, 并将生成的索引置于 `EDMIndexDirectory` 目录中, 请键入:

```
RemoteEDMIndexer -profile=C:\ExportEDMProfile.edm
-result=C:\EDMIndexDirectory\
```

创建索引进程完成时, 远程 EDM 索引器会在指定的结果目录中生成数个文件。这些文件会以创建索引的数据文件来命名, 并且其中一个文件会使用 `.wdx` 扩展名, 还有一个文件会使用 `.rdx` 扩展名。请注意, 创建大型数据文件的索引可能会生成多个具有编号扩展名的 `.rdx` 文件。例如: `my_edm.rdx.1`、`my_edm.rdx.2` 等等。

复制和使用生成的索引文件

在远程计算机上创建索引文件后，必须将文件复制到 Enforce Server 并加载。

在 Enforce Server 上复制并加载文件

- 1 转至已生成索引文件的目录。（即使用 `result` 选项所指定的目录。）
- 2 将扩展名为 `.pdx` 和 `.rdx` 的所有索引文件复制到 Enforce Server 上的索引目录。此目录位于 `\Vontu\Protect\Index` (Windows) 或 `/var/Vontu/index` (Linux)。
- 3 在 Enforce Server 管理控制台中，导航至“管理”>“策略”>“确切数据”屏幕。此屏幕会列出系统中的所有确切数据配置文件。
- 4 单击要与远程 EDM 索引器结合使用的确切数据配置文件的名称。
- 5 若要加载新索引文件，请转至确切数据配置文件的“数据源”部分，然后选择“加载外部生成的索引”。
- 6 在“索引”部分中选择“保存时提交索引作业”。
- 7 单击“保存”。

请考虑在远程计算机上调度定期运行远程 EDM 索引器的作业。该作业也应将生成的文件复制到 Enforce Server 上的索引目录，然后，您可以选择“加载外部生成的索引”和“按日程表提交索引作业”，并配置索引编制日程表，以调度在 Enforce Server 上从配置文件加载更新的索引文件。

请参见第 275 页的[“创建 EDM 配置文件以便远程编制索引”](#)。

疑难解答索引作业

在创建大量数据的索引时，可能会出现错误。通常，数据集会含有不完整、不一致或格式不正确的数据记录。数据行包括的列数若超出预期，或所含数据类型不正确时，通常会无法在索引创建期间正确创建索引，也无法识别。在更正错误并重新运行远程 EDM 紴引器之前，将无法对含有错误的数据行创建索引。Symantec 提供了多种方式，允许您获取有关任何错误的信息，并使得最终可以成功创建索引。

远程 EDM 紴引器通常会显示一则消息，指出创建索引操作是否成功完成。结果视您在配置文件中所指定的错误阈值而定。只要任何错误百分比低于该阈值，操作就会成功完成。若要获取有关创建索引操作的更多详细信息，可使用 `verbose` 选项。

在运行远程 EDM 紹引器时指定 `verbose` 选项，可提供有关完成创建索引操作后的信息统计摘要。此信息包括错误数和出现错误的位置。

请参见第 277 页的[“远程 EDM 紹引器命令选项”](#)。

若要查看远程 EDM 紹引器无法创建索引的实际数据行，请修改 `Indexer.properties` 文件。

修改 Indexer.properties 文件

- 1 找出位于 \Program Files\Vontu\Protect\config\Indexer.properties (Windows) 或 /opt/Vontu/Protect/config/Indexer.properties (Linux) 的 Indexer.properties 文件。
- 2 若要编辑文件, 请在文本编辑器中打开它。
- 3 找出 create_error_file 属性参数, 并将 false 值更改为 true。
- 4 保存并关闭 Indexer.properties 文件。

远程 EDM 索引器会将错误记录在名称与已创建索引的数据文件相同, 且扩展名为 .err 的文件中。该错误文件在日志目录中创建。

错误文件中所列出的数据行未经加密。请对错误文件加密, 防止数据暴露, 以最大限度地降低任何安全风险。

在 Windows 平台上卸载远程索引器

卸载远程 EDM 索引器所需的文件位于 Symantec Data Loss Prevention 安装目录的根文件夹中。请遵循此过程, 卸载 Windows 上的实用程序。

从 Windows 系统卸载远程 EDM 紴引器

- 1 在安装了索引器的计算机上, 找出并运行 (双击) \Vontu\uninstall.exe 程序。

卸载程序便会启动, 并显示“卸载”屏幕。

- 2 单击 **Next**。当卸载进程完成时, 将显示“卸载完成”屏幕。
- 3 单击 **Finish** 关闭程序。

请参见第 272 页的“[关于远程 EDM 紴引器](#)”。

在 Linux 平台上卸载远程索引器

卸载远程 EDM 索引器所需的文件位于 Symantec Data Loss Prevention 安装目录的根文件夹中。请遵循此过程, 卸载 Linux 上的实用程序。

从命令行删除远程 EDM 索引器

- 1 以根用户身份登录，并键入以下命令来更改至 Uninstall 目录：

```
cd /opt/Vontu/Uninstall
```

- 2 键入以下命令来运行卸载程序：

```
./Uninstall -i console
```

- 3 按屏幕上的说明进行操作。

请参见第 272 页的“[关于远程 EDM 索引器](#)”。

4

部分

实施策略检测

- 15. 检测数据丢失
- 16. 策略创建
- 17. 基于模板创建策略
- 18. 配置策略
- 19. 管理策略
- 20. 使用确切数据匹配来检测内容
- 21. 使用索引文档匹配来检测内容
- 22. 使用向量机学习来检测内容
- 23. 使用数据标识符检测内容
- 24. 使用关键字匹配检测内容
- 25. 使用正则表达式检测内容
- 26. 检测文件属性
- 27. 检测网络事件
- 28. 检测移动事件
- 29. 检测端点事件

- 30. 检测所述身份
- 31. 检测已同步的身份
- 32. 检测已配置的身份
- 33. 检测国际内容
- 34. 文件格式
- 35. 数据标识符
- 36. 策略模板

检测数据丢失

本章节包括下列主题：

- [策略检测简介](#)
- [可用检测技术](#)
- [检测规则简介](#)
- [实施策略检测](#)

策略检测简介

Symantec Data Loss Prevention 可检测几乎任何类型的邮件或文件、任何用户、发送者或接受者的内容（只要您的数据或端点存在）。您可以检测企业内数据的内容和上下文。可从基于 Web 的集中式 Enforce Server 管理控制台定义和管理策略。

请参见第 283 页的“[关于可检测的内容](#)”。

请参见第 284 页的“[关于可检测的文件属性](#)”。

请参见第 284 页的“[关于可监控的协议](#)”。

请参见第 284 页的“[关于可检测的端点事件](#)”。

请参见第 285 页的“[关于可检测的身份](#)”。

请参见第 285 页的“[关于可检测的语言](#)”。

关于可检测的内容

Symantec Data Loss Prevention 检测数据和文档内容，包括文本、标记、演示文稿、电子表格、存档文件及其内容、电子邮件、数据库文件、设计和图表、多媒体文件等。

例如，检测引擎可打开压缩文件，在压缩文件中的 Microsoft Word 文档中扫描关键字 confidential。如果匹配关键字，则检测引擎将邮件标记为事件。

请参见第 290 页的“[内容匹配条件](#)”。

内容检测基于实际内容，而非文件本身。检测服务器可检测受保护或所描述内容的压缩内容或衍生内容。此内容可能包括复制并粘贴到其他文档或电子邮件的部分文档。检测服务器还可识别除源文件以外的其他文件格式的敏感数据。例如，如果机密 Word 文件进行了指纹加密，则检测引擎可匹配以 PDF 附件形式通过电子邮件发送的内容。

关于可检测的文件属性

Symantec Data Loss Prevention 识别很多不同类型的文件和附件：文字处理格式、多媒体文件、电子表格、演示文稿、图片、封装格式，加密格式等。

检测引擎无需依赖文件扩展名来识别文件类型。例如，即使用户将 Microsoft Word 文件的扩展名更改为 .txt，检测引擎也可识别该文件。检测服务器检查文件的二进制签名来匹配其类型。

除了文件类型，Symantec Data Loss Prevention 还可根据名称和大小识别文件。

请参见第 291 页的“[文件属性匹配条件](#)”。

关于可监控的协议

Symantec Data Loss Prevention 通过识别以下协议签名检测网络上的消息：电子邮件 (SMTP)、Web (HTTP)、文件传输 (FTP)、新闻组 (NNTP)、TCP、Telnet 和 SSL。

您可以配置检测服务器，以侦听非默认端口的数据丢失违规情况。例如，如果您的网络在端口 81 而非端口 80 上传输 Web 流量，则系统仍然将传输的内容识别为 HTTP。

请参见第 292 页的“[网络协议匹配](#)”。

关于可检测的端点事件

Symantec Data Loss Prevention 允许您检测多个端点目标的数据丢失违规。这些目标包括本地驱动器、CD/DVD 驱动器、可移动存储设备、网络文件共享、Windows 剪贴板、打印机和传真以及应用程序文件。也可以针对电子邮件 (SMTP)、Web (HTTP) 和文件传输 (FTP) 流量检测端点的协议事件。

例如，DLP Agent（安装在每台端点计算机上）可以检测机密文件到 USB 设备的复制操作。或者，该代理可以允许将文件仅复制到满足公司加密要求的特定类别的 USB 设备。

请参见第 293 页的“[端点匹配条件](#)”。

关于可检测的身份

Symantec Data Loss Prevention 允许您使用各种方法检测数据用户、邮件发送者和邮件接受者的身份。这些方法包括指定内容匹配、确切数据匹配和同步目录服务器匹配。

例如，可以检测特定用户发送的电子邮件，或允许从特定用户组发送电子邮件。

请参见第 293 页的“[组（身份）匹配条件](#)”。

关于可检测的语言

Symantec Data Loss Prevention 提供了多种语言版本的国际支持，以检测数据丢失。支持的语言包括大多数西欧和中欧语言、希伯来语、阿拉伯语、中文（简体和繁体）、日语、韩语等。

请参见第 58 页的“[支持的检测语言](#)”。

检测引擎在内部使用 Unicode。您可以在任何支持的语言中，使用任何检测技术构建本地化的策略规则和例外。

请参见第 495 页的“[关于实施非英语语言检测](#)”。

可用检测技术

Symantec Data Loss Prevention 提供几种类型的检测技术，以检测数据是否丢失。每种类型的检测技术都会提供独特的功能。通常，您可以策略中结合使用多种技术来取得精确的检测结果。

表 15-1 可用检测技术

技术	说明
确切数据匹配 (EDM)	确切匹配结构化或非结构化数据。 请参见第 286 页的“ 关于确切数据匹配 ”。
索引文档匹配 (IDM)	确切匹配非结构化数据。 请参见第 287 页的“ 关于索引文档匹配 ”。
向量机学习 (VML)	类似匹配非结构化数据。 请参见第 287 页的“ 关于向量机学习 ”。
指定内容匹配 (DCM)	匹配描述的内容（如模式）和邮件上下文（如协议和目标）。 请参见第 288 页的“ 关于指定内容匹配 ”。

技术	说明
目录组匹配 (DGM)	匹配来自目录服务器或数据库的确切身份。 请参见第 288 页的“ 关于目录组匹配 ”。
自定义检测方法	通过扩展检测功能匹配唯一数据。 请参见第 289 页的“ 关于自定义检测 ”。

请参见第 305 页的“[关于策略](#)”。

关于确切数据匹配

确切数据匹配(EDM)用于检测以结构化或表格格式存储的要保护的内容。例如，可以使用 EDM 来检测数据库中的机密客户信息。或者，也可以使用 EDM 来检测电子表格中的敏感财务信息。

要实施 EDM，请确定要保护的结构化数据。然后使用 Enforce Server 管理控制台对数据源编制索引。在编制索引过程中，系统会对数据进行指纹加密，具体做法是：访问、提取并规范化基于文本的内容，然后使用不可逆哈希为其提供保护。为了进行精确的连续检测，可以安排定期的索引编制过程，使数据始终保持最新。通过配置“内容匹配确切数据源”策略检测规则，可匹配已配置数据的各个片段。为提高准确性，可以配置该规则来匹配特定记录中的数据字段组合。对数据源进行编制索引并部署策略后，检测引擎即可检测结构化或非结构化格式的数据。

请注意以下示例。

贵公司维护的员工数据库包含以下五列：

- 名字
- 姓氏
- SSN
- 入职日期
- 薪资

在数据库中，每一行包括一名员工的相关信息。您要将这些记录导出到数据源文件。每条记录位于单独一行上。每个数据项以逗号、制表符或竖线字符进行分隔。例如，数据源文件中的某一行包含 Bob,Smith,123-45-6789,05/26/99,\$42500。您需要对该数据源文件编制索引并创建确切数据配置文件。在配置该配置文件时，请映射您要保护的数据元素（列）。然后配置 EDM 策略规则来引用该确切数据配置文件。在本例中，若一条消息同时包含名字、姓氏和 SSN，即表示匹配该规则。在运行时，如果检测引擎在任意入站消息中检测到 Bob,Smith,123-45-6789，它便会报告一个事件。但是包含 Betty,Smith,123-45-6789 的消息不匹配，因为配置文件中没有该记录。包含 Bob,Smith,415-789-0000 的消息也不匹配，因为此编号不是社会安全号。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

关于索引文档匹配

索引文档匹配 (IDM) 匹配来自敏感专有文档的非结构化数据。支持的文档类型示例包括 Microsoft Word、PowerPoint、PDF、设计规划、源代码、CAD/CAM 图像、财务报告、机密并购文档等。

IDM 可注册所提取数据的不同部分并进行指纹加密。它通过删除标点和格式来规范化文本。规范化过程可确保内容的呈现方式不会影响或中断检测。

IDM 使用统计采样方法来存储经指纹加密的文档的哈希部分。并不是所有文本都存储在文档配置文件中。通过此方法，IDM 可拥有很高的准确率，同时，您还可以通过添加检测服务器来轻松调整您的策略。还可以将内容列入白名单并从匹配中排除它。

配置 IDM 策略时，请建立必须匹配文档配置文件才能触发事件的内容百分比。如果在指纹中检测到所有哈希段，则可以使用 IDM 检测文本文档的确切内容匹配。这样就可以检测衍生文档，如修订版和版本。还可以使用 IDM 匹配部分文档内容和文本段，例如复制到其他文档或邮件中的内容片段。

除全部和部分文档匹配之外，您还可以使用 IDM 检测二进制内容。除了为部分文档匹配创建的哈希，还需要创建二进制内容的 MD5 哈希才能实现此检测。可以使用这种形式的 IDM 检测系统无法破解和提取文本内容的文件类型，如媒体文件或专有文件格式。

请参见第 377 页的“[关于实施索引文档匹配](#)”。

关于向量机学习

向量机学习 (VML) 通过执行统计分析确定内容是否与您培训的示例内容相似来保护非结构化数据。

不同于其他检测技术，使用 VML 时无需找到要保护的所有数据并对这些数据进行指纹加密，也无需对其进行描述，且没有发生潜在不准确的风险。使用 VML，可根据您提供的示例文档培训系统，以使其了解您要保护的内容类型。

VML 检测基于 VML 配置文件。通过从特定数据类别上传具有代表性的内容来创建 VML 配置文件。系统会扫描内容、提取特征并根据示例文档中关键字的频率来创建统计模型。在运行时，系统应用模型来分析和检测其特征在统计学上与配置文件相似的内容。

VML 简化了基于文本的非结构化内容的检测，同时可能提供很高的准确性。实施 VML 的关键是用来自培训系统的示例内容。您必须仔细选择文档，这些文档必须很好地代表您要保护的内容类型。并且，您必须选择要忽略的内容的代表性示例，这些示例必须与要保护的内容密切相关。

请参见第 396 页的“[实施向量机学习 \(VML\)](#)”。

关于指定内容匹配

Symantec Data Loss Prevention 提供许多检测方法，统称为指定内容匹配(DCM)。这种样式的检测会匹配具有常见特性（例如关键字、数据类型、文件元数据、协议签名、端点目标和身份模式）的数据。

可以使用 DCM 检测您可以描述的任何数据，结构化和非结构化数据均可。DCM 的准确度很高，且易于实施，因为无需配置数据源。当不可能收集要保护的所有数据但可以描述这些数据时，DCM 最为有用。通常可以将 DCM 和其他检测方法结合使用，从而获得准确结果。

表 15-2 可用的 DCM 检测方法

方法	说明
数据标识符	使用精确模式和数据验证器来匹配内容。 请参见第 414 页的“ 关于数据标识符 ”。
关键字	使用关键字、关键短语和关键字字典来匹配内容。 请参见第 445 页的“ 关于实施关键字匹配 ”。
正则表达式	使用正则表达式来匹配字符、模式和字符串。 请参见第 453 页的“ 关于正则表达式匹配 ”。
文件属性	匹配文件类型、名称和大小。 请参见第 457 页的“ 关于实施文件属性匹配 ”。
用户、发送者、接受者	根据模式来匹配身份。 请参见第 479 页的“ 关于指定身份匹配 ”。
网络协议	根据协议签名来匹配网络和移动通信。 请参见第 465 页的“ 关于对网络进行的协议监控 ”。
端点事件	匹配端点目标、设备和协议。 请参见第 469 页的“ 关于进行端点事件检测 ”。

关于目录组匹配

目录组匹配(DGM) 检测数据用户、邮件发送者和接受者的确切身份。

Symantec Data Loss Prevention 提供了两种目录组匹配类型：同步和配置。同步的 DGM 使用与目录服务器实例 (Microsoft Active Directory) 的连接来匹配身份。配置的 DGM 使用目录服务器或数据库的静态确切数据配置文件来匹配身份。

要实施同步的 DGM，需要在 Enforce Server 管理控制台中定义一个或多个用户组并将这些组与目录服务器同步。然后，将这些用户组与相应的发送者/用户和接受者检测规则相关联。将某个用户组与其中任一规则关联后，该规则将仅适用于该组用户。例如，您可以使用目录服务器匹配来检测特定用户组（例如 Engineering）发送的所有电子邮件。

请参见第 485 页的“[关于实施同步的目录组匹配](#)”。

要实施配置的 DGM，需要从目录服务器或数据库导出身份记录，对这些数据编制索引，并创建确切数据配置文件。然后，在相应的发送者/用户和接受者检测规则中引用此配置文件。配置的 DGM 利用确切数据匹配 (EDM) 技术精识别和检测身份。例如，您可以使用静态 DGM 配置文件来识别网络用户活动或将用户相关内容包括在分析范围内。或者，将某些电子邮件地址排除在分析范围外。或是想要防止某些人通过电子邮件发送机密信息。

请参见第 491 页的“[关于实施配置的目录组匹配](#)”。

关于自定义检测

Symantec Data Loss Prevention 为您提供了多种方式，以便扩展检测范围和匹配所需的任何类型的数据、内容或文件。

您可以编写脚本、表达式和插件来自定义检测引擎的功能。

表 15-3 可用的检测自定义方法

方法	说明
自定义数据标识符	实现您自己的数据标识符模式和系统定义的验证器。 请参见第 414 页的“ 关于数据标识符 ”。
数据标识符的自定义脚本验证器	使用 Symantec Data Loss Prevention 脚本语言验证自定义数据类型。 请参见第 439 页的“ 实施自定义数据标识符 ”。
自定义文件类型识别	使用 Symantec Data Loss Prevention 脚本语言检测自定义文件类型。 请参见第 458 页的“ 关于自定义文件类型识别 ”。
自定义端点设备检测	使用正则表达式检测或允许任何端点设备。 请参见第 470 页的“ 关于端点设备检测 ”。
自定义网络协议检测	定义 TAP 的自定义 TCP 端口。 请参见第 465 页的“ 关于对网络进行的协议监控 ”。

方法	说明
自定义内容提取	<p>编写插件以识别自定义文件格式并提取内容供检测引擎进行分析。</p> <p>请参考 <i>Symantec Data Loss Prevention Content Extraction Plugin Developers Guide</i>《Symantec Data Loss Prevention 内容提取插件开发人员指南》，可从 DLP 知识库 获得此指南。</p>

检测规则简介

Symantec Data Loss Prevention 提供了多种类型的检测规则，每类规则都有独特的功能。

您可以在策略中实施检测规则。规则声明了一个或多个条件以匹配数据。您也可以为规则创建例外条件。

请参见第 296 页的“[关于规则例外](#)”。

表 15-4 检测规则和例外类型

规则类型	说明
内容	请参见第 290 页的“ 内容匹配条件 ”。
文件属性	请参见第 291 页的“ 文件属性匹配条件 ”。
网络	请参见第 292 页的“ 网络协议匹配 ”。
端点	请参见第 293 页的“ 端点匹配条件 ”。
组（身份）	请参见第 293 页的“ 组（身份）匹配条件 ”。

内容匹配条件

Symantec Data Loss Prevention 提供了几条用于检测邮件内容的规则。

对于内容检测，您可以匹配各个邮件组件：标头、主题、正文和附件。

请参见第 294 页的“[关于可以匹配的邮件组件](#)”。

表 15-5 可用的内容匹配条件

内容规则类型	说明
内容匹配正则表达式	使用正则表达式匹配所述内容。 请参见第 453 页的“ 关于正则表达式匹配 ”。 请参见第 453 页的“ 配置“内容匹配正则表达式”条件 ”。 注意： 此检测规则不可用作例外。
内容匹配来自确切数据配置文件的确切数据	匹配来自数据库或 CSV 文件这样的结构化数据源的确切数据。 请参见第 356 页的“ 关于实施确切数据匹配 ”。 请参见第 372 页的“ 配置“内容匹配确切数据”条件 ”。
内容匹配关键字	使用关键字、关键短语和数据字典匹配所述内容。 请参见第 445 页的“ 关于实施关键字匹配 ”。 请参见第 448 页的“ 配置“内容匹配关键字”条件 ”。
内容匹配来自索引文档配置文件的文档签名	使用指纹加密精确匹配非结构化文档内容。 请参见第 377 页的“ 关于实施索引文档匹配 ”。 请参见第 380 页的“ 配置“内容匹配文档签名”条件 ”。
内容匹配数据标识符	使用数据标识符模式和验证器匹配所述内容。 请参见第 414 页的“ 关于数据标识符 ”。 请参见第 428 页的“ 配置“内容匹配数据标识符”条件 ”。
使用向量机学习配置文件检测	匹配与已提供的示例内容功能相似的非结构化文档内容。 请参见第 408 页的“ 配置 VML 策略规则 ”。 请参见第 410 页的“ 配置 VML 策略例外 ”。

文件属性匹配条件

Symantec Data Loss Prevention 提供了几种检测包括文件类型、文件大小和文件名在内的文件属性的方法。

请参见第 457 页的“[关于实施文件属性匹配](#)”。

表 15-6 可用的文件属性检测规则

检测规则类型	说明
邮件附件类型或文件类型匹配	检测特定的文件格式和附件。 请参见第 458 页的“ 关于文件类型检测 ”。 请参见第 460 页的“ 配置“邮件附件类型或文件类型匹配”条件 ”。
邮件附件大小或文件大小匹配	检测文件或附件是大于还是小于指定大小。 请参见第 459 页的“ 关于文件大小检测 ”。 请参见第 461 页的“ 配置“邮件附件大小或文件大小匹配”条件 ”。
邮件附件名或文件名匹配	检测具有特定名称或匹配通配符的文件或附件。 请参见第 459 页的“ 关于文件名检测 ”。 请参见第 462 页的“ 配置“邮件附件名或文件名匹配”条件 ”。
邮件/电子邮件属性和特性	根据特定的电子邮件属性（MAPI 属性）对 Microsoft Exchange 电子邮件分类。 注意： 此检测规则仅适用于 Enterprise Vault 产品的数据分类。 有关更多信息，请参见 <i>Enterprise Vault Data Classification Services Implementation Guide</i> （《Enterprise Vault 数据分类服务操作指南》）。
自定义文件类型签名	根据使用脚本的二进制签名检测自定义文件类型。 请参见第 458 页的“ 关于自定义文件类型识别 ”。 请参见第 463 页的“ 启用自定义文件类型检测 ”。

网络协议匹配

Symantec Data Loss Prevention 提供了“协议监控”条件来检测网络流量。

请参见第 465 页的“[关于对网络进行的协议监控](#)”。

表 15-7 网络检测的协议监控

检测规则	说明
协议监控	检测网络中使用指定协议（包括 SMTP、FTP、HTTP/S、IM 和 NNTP）传输的事件。 请参见第 284 页的“ 关于可监控的协议 ”。 请参见第 466 页的“ 配置用于网络检测的“协议监控”条件 ”。

端点匹配条件

Symantec Data Loss Prevention 提供了几种检测端点事件的方法。

请参见第 284 页的“[关于可检测的端点事件](#)”。

表 15-8 端点检测规则

检测规则	说明
协议或端点监控	<p>使用指定的传输协议匹配传输的端点邮件。</p> <p>当数据被移动或复制到一个特定目标时匹配端点事件。</p> <p>请参见第 469 页的“关于进行端点事件检测”。</p> <p>请参见第 471 页的“配置端点监控条件参数”。</p>
端点设备类或 ID	<p>匹配在指定的硬件设备上发生的端点事件。</p> <p>请参见第 469 页的“关于进行端点事件检测”。</p> <p>请参见第 476 页的“配置“端点设备类或 ID”条件”。</p>
端点位置	<p>根据端点代理在企业网络内还是在企业网络外检测端点事件。</p> <p>请参见第 469 页的“关于进行端点事件检测”。</p> <p>请参见第 476 页的“配置“端点位置”条件”。</p>

组（身份）匹配条件

Symantec Data Loss Prevention 提供了几个用于检测用户和组以及邮件发送者和接受者的身份的规则。

请参见第 285 页的“[关于可检测的身份](#)”。

表 15-9 可用于进行身份匹配的组规则

组规则	说明
发送者/用户匹配模式	<p>根据电子邮件地址、用户 ID、IM 昵称和 IP 地址匹配邮件发送者和用户。</p> <p>请参见第 479 页的“关于指定身份匹配”。</p> <p>请参见第 480 页的“配置“发送者/用户匹配模式”条件”。</p>
接受者匹配模式	<p>根据电子邮件、IP 地址或 Web 域匹配邮件接受者。</p> <p>请参见第 479 页的“关于指定身份匹配”。</p> <p>请参见第 482 页的“配置“接受者匹配模式”条件”。</p>

组规则	说明
发送者/用户基于目录服务器匹配用户组	<p>匹配来自同步的目录服务器的邮件发送者和用户。</p> <p>请参见第 485 页的“关于实施同步的目录组匹配”。</p> <p>请参见第 488 页的“配置“发送者/用户基于目录服务器匹配用户组”条件”。</p>
发送者/用户根据来自确切数据配置文件的本地目录匹配用户组	<p>匹配来自配置的目录服务器的邮件发送者和用户。</p> <p>请参见第 491 页的“关于实施配置的目录组匹配”。</p> <p>请参见第 489 页的“配置“接受者基于目录服务器匹配用户组”条件”。</p>
接受者基于目录服务器匹配用户组	<p>匹配来自同步的目录服务器的邮件接受者。</p> <p>请参见第 485 页的“关于实施同步的目录组匹配”。</p> <p>请参见第 493 页的“配置“发送者/用户匹配来自确切数据配置文件的目录”条件”。</p>
接受者根据来自确切数据配置文件的本地目录匹配用户组	<p>匹配来自配置的目录服务器的邮件接受者。</p> <p>请参见第 491 页的“关于实施配置的目录组匹配”。</p> <p>请参见第 493 页的“配置“接受者匹配来自确切数据配置文件的目录”条件”。</p>

关于可以匹配的邮件组件

系统以邮件的形式接收数据以进行分析。系统决定邮件类型；例如，电子邮件或 Word 文档。根据邮件类型的不同，系统或者将邮件内容解析为一个或多个组件（标题、主题、正文、附件），或者保持邮件完整。系统将评估邮件或邮件组件，看是否有任何条件适用。如果某条件适用并支持组件匹配，系统将针对每个选定的邮件组件来评估内容。如果条件不支持组件匹配，系统将评估整个邮件。

可以将所述内容条件配置为在所有邮件组件中进行匹配。EDM 支持信封组件、正文组件和附件组件。文档内容和文件大小条件会对邮件正文和附件进行匹配。文件类型和文件名条件仅对邮件附件进行匹配。协议、端点和身份条件会对整个邮件进行匹配。由 DLP Agent 评估的任何条件都会对整个邮件进行匹配，而与单独选定的邮件组件无关。主题组件只适用于 SMTP 电子邮件或 NNTP 邮件；对于其他邮件，主题组件即使选择了也会被忽略。

注意：主题组件会对从分类服务器传递过来的 Exchange 邮件进行匹配。信封组件不适用于从分类服务器传递过来的 Exchange 电子邮件。有关更多信息，请参见 *Enterprise Vault Data Classification Services Implementation Guide* (《Enterprise Vault 数据分类服务操作指南》)。

请参见第 339 页的“[选择匹配的组件](#)”。

表 15-10 用于匹配的邮件组件

条件类型	信封	主题	正文	附件
描述内容 (DCM) (关键字、数据标识符、正则表达式)	匹配	匹配	匹配	匹配
确切数据 (EDM)	匹配		匹配	匹配
已编制索引的文档内容 (IDM)			匹配	匹配
相似的文档内容 (VML)			匹配	匹配
文件大小 (DCM)			匹配	匹配
文件类型和文件名 (DCM)				匹配
协议 (DCM)		匹配 (整个邮件)		
端点 (DCM)		匹配 (整个邮件)		
身份 (DCM 和 DGM)		匹配 (整个邮件)		
DLP Agent 评估的任何内容		匹配 (整个邮件)		

关于规则严重性

设置检测规则严重性以标记与特定严重性等级匹配的条件。然后可使用响应规则根据严重性等级采取操作。例如，可以将响应规则配置为在出现指定次数的“高”严重性违规后采取操作。

请参见第 661 页的“[关于响应规则条件](#)”。

配置检测规则时，选择默认的严重性等级。除非更改，否则默认的严重性等级设置为“高”。默认的严重性等级适用于检测规则匹配的任何条件。例如，如果默认的严重性等级设置为“高”，则每个检测规则违规都将标记为此严重性等级。

请参见第 337 页的“[定义规则严重性](#)”。

如果不使用特定严重性标记每个违规，可以定义确定严重性等级的条件。在这种情况下，将覆盖默认行为。例如，可将“高”严重性等级定义为仅在发生指定次数的条件匹配项后应用。

此外，可以定义多个严重性等级以将严重性报告分层。例如，可在超过 100 个匹配项之后设置“高”严重性等级，在超过 50 个匹配项之后应用“中”严重性等级。

表 15-11 规则严重性等级

规则严重性等级	说明
高	如果出现条件匹配，将标记“高”严重性。
中	如果出现条件匹配，将标记“中”严重性。
低	如果出现条件匹配，将标记“低”严重性。
信息	如果出现条件匹配，将标记“信息”严重性。

关于规则例外

Symantec Data Loss Prevention 提供了检测例外和组例外，可用于从检测中排除邮件、邮件组件或身份。检测例外不是必需的，但经常用于优化检测规则和组规则的范围。

系统首先根据策略例外评估入站邮件或邮件组件，然后再根据策略规则进行评估。如果例外支持跨组件匹配（基于内容的例外），则例外会对各个邮件组件进行匹配。否则，例外会与整个邮件匹配。如果符合例外条件，系统将拒绝包含触发过例外的内容的整个邮件或邮件组件。根据策略规则进行评估时，将不再提供被拒绝的邮件或邮件组件。系统不仅将放弃匹配的内容或数据项，还将放弃包含排除项的整个邮件或邮件组件。

注意：Symantec Data Loss Prevention 不支持匹配级别例外，仅支持组件或邮件级别例外。

例如，试考虑这样一个策略，该策略既声明了带有单项条件的检测规则，又声明了带有单项条件的检测例外。该规则与包含 Word 附件的所有邮件匹配并为每个匹配项生成一个事件。该例外排除来自 `ceo@company.com` 的任何邮件，即使在与此例外匹配的情况下也不生成事件。在这种情况下，包含 Word 附件的来自 `ceo@company.com` 的电子邮件将不会进行匹配，也不会触发事件。排除所有 `ceo@company.com` 邮件的例外优先于该检测规则。

请参见第 297 页的“[关于检测服务器策略执行](#)”。

您可以实施所有可作为例外使用的检测规则条件和组规则条件，实施 EDM 的条件除外。您可以将 IDM 作为例外实施，但例外将从检测中排除特定文档类型而非文档中的特定内容。要排除文档中的内容，需将其列入“白名单”。

对于连续不断的误报，如果该内容属于同一类别，则可将 VML 用作检测例外。

请参见第 340 页的“[向策略中添加例外](#)”。

请参见第 589 页的“[CAN-SPAM 法案策略模板](#)”。

请参见第 383 页的“[将内容排除（加入白名单）在检测范围之外](#)”。

关于复合匹配条件

有效的策略必须至少声明一个规则，其中至少定义了一个匹配条件。该条件匹配输入数据，以检测数据丢失。或者，您可以在单个检测规则或组规则中声明多个条件。

具有单个条件的规则是简单规则。具有多个条件的规则是复合规则。对于复合规则，只有每个条件都匹配才能触发事件。因此，对于单个策略，如果声明了一个具有两个条件的规则，其中一个条件匹配，而另一个不匹配，则检测引擎不会将其报告为匹配。如果两个条件都匹配，则检测引擎会将其报告为匹配，并假设该规则已设置为对所有匹配进行计数。

请参见第 297 页的“[关于检测服务器策略执行](#)”。

与规则一样，您可以在单个例外中声明多个条件。在这种情况下，例外的所有条件都必须匹配才能应用该例外。

请参见第 296 页的“[关于规则例外](#)”。

关于检测服务器策略执行

您可以在一个策略中包含任何检测和组规则以及例外的组合。每个规则或例外可包含一个或多个条件。

请参见第 296 页的“[关于规则例外](#)”。

系统首先评估例外。如果符合任何例外，将弹出与该例外匹配的整个邮件或邮件组件，并且不再适用于检测。不报告任何事件。

如果不符不符合任何例外或策略中不存在例外，则引擎将基于各个规则评估检测和组规则。如果策略中包含同一类型的多个规则，如果符合任何规则，系统将报告事件。如果存在不同类型的规则，必须匹配各个规则才会报告事件。

在编程术语中，当您有单个策略定义时，同一规则或例外中各条件之间的关系为 AND。同一类型的两个或更多个规则之间的关系为 OR（例如 2 个检测规则）。不过，如果在单个策略中结合使用不同类型的规则（例如使用 1 个检测规则和 1 个组规则），则这些规则之间的关系为 AND。在这种配置中，这两个规则必须匹配才会触发事件。不过请注意，跨“检测”和“组”选项卡创建的例外条件之间为隐式 OR 关系。

表 15-12 检测服务器的策略执行逻辑

逻辑	方法	类型	基数	条件	匹配
----	----	----	----	----	----

逻辑	方法	类型	基数	条件	匹配
IF	排除 1	检测或组	简单	条件	匹配项
OR					
	排除 N	检测或组	复合	条件 1	匹配项
AND					
				条件 N	匹配项
THEN	不报告任何事件。				
ELSE	规则 1	检测	简单	条件	匹配项
OR					
	规则 N	检测	复合	条件 1	匹配项
AND					
				条件 N	匹配项
THEN	报告事件。				
ELSE	规则 1	组	简单	条件	匹配项
OR					
	规则 N	组	复合	条件 1	匹配项
AND					
				条件 N	匹配项
THEN	报告事件。				
ELSE	规则 N	组	简单或复合	条件 N	匹配项
AND					
	规则 N	检测	简单或复合	条件 N	匹配项
THEN	报告事件。				

实施策略检测

实施能够达到数据丢失防护目标的检测过程需要考虑业务和技术。有关该过程的概述，请参阅下表。

操作	说明
制订数据丢失防护策略。	评估您的业务要求并制订数据丢失防护策略。 请参见第 299 页的“ 关于制定数据泄露防护策略 ”。
实施几项关键策略。	准备好实施此技术后，首先从细节抓起。您可以使用一些简单规则处理特定目标，然后继续进行。 请参见第 300 页的“ 关于策略检测的制定 ”。
适当地使用检测技术和方法。	不必从头开始创建策略和检测规则。许多策略模板和系统定义的数据标识符经过少许修改或不用任何修改就可以处理您的目标。使用适当的技术和方法获得准确的检测结果。 请参见第 302 页的“ 关于使用适当的检测方法 ”。 请参见第 303 页的“ 关于使用例外缩小检测范围 ”。 请参见第 303 页的“ 关于使用复合规则进行精确检测 ”。
测试和优化策略检测。	在生成和检查事件时调整检测方法。 请参见第 301 页的“ 关于要避免的常见检测问题 ”。 请参见第 300 页的“ 关于获得精确检测结果 ”。
实施响应规则并部署策略。	优化策略检测后，您可以实施响应规则以在发生策略违规时采取操作。 请参见第 653 页的“ 关于响应规则 ”。

关于制定数据泄露防护策略

数据泄露防护从检测开始。要防止数据泄露，必须能够在数据面临泄露危险时检测到这种危险。只有这样才能保护数据。

要利用 Symantec Data Loss Prevention 的检测技术和功能，请对您要保护的数据类型、您检测数据丢失事件的方式以及防止数据丢失的方式进行分析。实质上，需要将企业数据安全目标转换为有效的数据泄露防护策略，这些策略包括检测敏感数据的检测规则和条件，允许合理地使用数据，并可在检测到违规行为时采取适当的应对措施来保护数据。

制定数据泄露防护策略的常用方法有两种：

- 基于信息 - 确定敏感数据并创建策略来防止数据泄露。
- 基于法规 - 审查政府和行业法规并创建策略来遵守这些法规。

对于基于信息的方法，从确定要保护的特定数据项及数据组合开始。此类数据的示例包括数据库中配置的字段、一系列关键字、一组用户，或这些元素的组合。然后，将类似的数据项组合到一起，并创建策略以便识别并保护它们。当对数据的访问具有限制或不是特别关注特定法规时，该方法最合适。

对于基于法规的方法，从基于必须遵守的法规的策略模板开始。此类模板的示例包括 HIPAA 或 FACTA。同时，要从规模较大的一组数据（如客户或员工数据）开始。使用法规规定的高级别要求作为此种方法的基础。然后，确定企业中的哪些敏感数据项和文档符合这些要求。这些数据项将成为策略中检测规则和例外的条件。确定最适合您的检测方法，然后根据测试结果视需要修改这些方法。最后，在定义数据泄露防护策略时，要考虑组织中已计划的报告和补救结构。确定组织的结构是围绕敏感数据的特定主体，还是围绕任何特定的法规集。然后相应地实施策略。

请参见第 82 页的“[关于建议的组织角色](#)”。

请参见第 301 页的“[关于要避免的常见检测问题](#)”。

请参见第 300 页的“[关于策略检测的制定](#)”。

关于策略检测的制定

您不必创建复杂的检测规则便可以快速对检测功能入门。您可以添加一个检测服务器并部署一个或多个基本策略，对机密数据进行监视但不采取阻止或隔离操作。

请参见第 187 页的“[添加检测服务器](#)”。

例如，您可以创建一个策略，定义“关键字匹配”检测规则，用以检测“机密”这个词。或者，也可以使用预先建立的 65 个策略检测模板。例如，您可以使用 HIPAA 策略检测模板，该模板使用关键字匹配功能来检测医疗敏感信息。

请参见第 329 页的“[添加新的策略或策略模板](#)”。

查看策略检测到的事件。在实施较为复杂的检测方法和规则前，可以优化检测规则，以最大程度地减少误报。例如，您可以添加其他基于数据配置文件的规则来检测社会安全号，或添加基于用户组的策略，将策略检测限定到特定个人。

请参见第 300 页的“[关于获得精确检测结果](#)”。

关于获得精确检测结果

要防止数据丢失，必须准确检测所有类型的机密数据，不论这些数据是在何处进行存储、复制或传输都应如此。没有准确的检测，数据安全系统可能生成大量误报和漏报。

误报是将没有违规的邮件或文件检测为策略违规。漏报是没有将违规的文件或邮件检测为策略违规。误报会使调查和解决貌似有问题的事件所花费的时间和资源成本增高。漏报会隐藏安全漏洞，造成数据丢失、可能的财务损失、法律风险以及对组织声誉的损坏。

配置检测规则时，请尽量将策略配置为可捕获尽可能多的真正事件而不生成大量误报。如果策略的检测规则过于宽松，便可能会生成许多误报。另一方面，如果策略的检测规则过于具体，系统可能无法检测出所有敏感数据。

获取精确检测结果的最佳方法是添加包含一个或两个检测条件的策略，查看策略生成的事件数（数量）和类型（质量），然后根据需要调整检测规则。如果策略生成的误报数超出预期，则应通过调整现有条件、添加其他条件以及添加例外，使检测条件更加具体。如果策略不能检测到某些事件，应使检测条件更加模糊。

请参见第 301 页的“[关于要避免的常见检测问题](#)”。

关于要避免的常见检测问题

Symantec Data Loss Prevention 提供强大的检测技术。通过仔细考虑和分析自己对数据泄露防护的要求，您可以实施高效的检测规则。您必须确保检测规则和例外都是有用的，并且不会降低系统性能。一般来说，一项匹配大量邮件的检测策略可能会生成过多的误报。

因此在创建检测策略时，需要避免以下两个常见的问题：

■ 策略过于宽松。

如果您添加的策略非常概括，则它会在没有发生真正匹配时生成事件（误报）。例如，一个策略使用模式规则查找字母 e，而几乎网络上的每封邮件都会与此匹配。

■ 策略过于严格。

如果您的策略使用严格的规则，对其检测的数据规定过于具体，则可能会漏掉许多您想捕获的匹配。例如，一个策略同时包含针对 Word 文档的例外条件和匹配条件。

目标是通过认真考虑后制定的适当规则，采用正确的条件类型和组合，并在必要时设置例外，最终得到精确的结果。

例如，您想要保护客户的名称。您创建一个为包含姓氏和名字的任何内容生成事件的策略。但是大部分邮件都包含名称 - 多数情况既包含姓氏又包含名字。此策略过于宽松。尽管您的策略可能会捕获所有从外部网络发送的客户名称，但此策略可能返回许多误报。例如，此策略也许检测到不会泄露受保护信息的电子邮件。因为几乎没有组织有能力处理许多误报，所以确保您的策略报告真正事件很重要。

此问题的解决方案是创建寻找特定数据的策略。达到此目标的一个方法是使用数据库条件，而非基于模式的条件。例如，社会安全号 (SSN) 由九个数字组成。这表示有 10 亿个可能的 SSN 号，其中大约有 8 亿个有效。如果您基于任何九位数的 SSN 模式创建规则，则策略可能会为 8 亿 SSN 号中任何出现在邮件中的 SSN 号创建事件。但是，它还为其他类型的九位数创建事件，如欧洲电话号码或各种类型的帐号。您可能对保护全部 8 亿 SSN 和所有其他九位数不感兴趣。在这种情况下，您需要找到一个只保护员工和客户数据库中的 SSN 的方法。完成该目标的最佳方法是使用数据库条件而非模式条件添加规则。此方法能提供最准确的结果。

请参见第 302 页的“[关于使用适当的检测方法](#)”。

关于使用适当的检测方法

为了最大程度地减少误报，需要使用适当的检测技术和方法来检测要保护的数据。

例如，如果想要检测所有社会安全号 (SSN)，您需要使用 SSN 数据标识符，而不是正则表达式。数据标识符具有许多数据模式和验证器，比正则表达式更准确，且性能更好。对于检测复杂的数据模式，数据标识符比正则表达式更为高效，且运行时的执行速度更快。数据标识符中包含不同数据类型的有效号码范围的情报。通过这额外的一层情报，可以筛选出测试数据和其他误报事件触发器。还可以识别特定于广泛的行业、国家/地区和区域的数据类型。

如果您只想检测员工的社会安全号，可以使用确切数据配置文件，该配置文件中包含员工数据库中的特定 SSN。EDM 配置文件要比 SSN 数据标识符更为精确。减少误报的另一个方法是搜索数据组合。如果 EDM 配置文件包含名字、姓氏和社会安全号的字段，您可以配置一项策略，查找同时包含社会安全号及相关名字与姓氏的内容。根据您的要求，相较于仅检测 SSN 的策略，此类策略可能更能检测出明显的数据丢失。

另一个示例是“内容匹配确切数据”规则，它允许您指定匹配所需的列的精确组合。使用数据标识符或正则表达式规则，您只能查找社会安全号模式。使用 EDM，您不仅可以检测特定社会安全号，还可以检测拥有该社会安全号的人所对应的姓氏。

假设您的数据库中有下列字段：

- 名字
- 姓氏
- SSN

仅保护“名字”和“姓氏”字段的策略会生成大量误报。同样，如果数据库中有其他类型的九位数，仅保护 SSN 字段的策略也可能生成误报。您需要添加一个将特定的 SSN 与特定的姓氏和名字联系起来的策略。保护每条记录上的姓氏、名字和 SSN 的策略所捕获的事件要少于上述的其他策略。但是，此策略仍然生成由员工发送姓氏、名字和 SSN 引起的事件。

要避免此问题，请配置条件以要求姓氏、名字和 SSN 的两个或多个实例。使用此方法，您可以降低误报，但是仍会错过某些真正事件。例如，如果 Bob 发送 Alice 的姓氏、名字和 SSN，该信息将不能被检测到。

目录组匹配 (DGM) 检测员工和基于组的用户属性，您会通过公司 LDAP (Active Directory) 或人力资源数据库对这些属性编制索引。静态 DGM 利用与 EDM 相同的指纹加密技术根据用户活动保护数据。静态 DGM 使用确切数据索引检测策略违规，而不会直接访问目录。要使用静态 DGM，您需要创建带有特定数据字段的确切数据配置文件，以识别各个用户。

请参见第 303 页的“[关于使用例外缩小检测范围](#)”。

请参见第 303 页的“[关于使用复合规则进行精确检测](#)”。

关于使用例外缩小检测范围

在检测时，可以加入检测例外来排除通用或非机密的数据。实施检测例外有助于优化检测范围。

假设您的数据库中有下列字段：

- 名字
- 姓氏
- SSN
- 电话号码
- 帐号

最初，您可能想要添加一个指定包含这些字段中任意两个字段的任何电子邮件为事件的策略。但是，您可能发现报告的大部分事件包含姓氏和名字。在这种情况下，您的规则需要更加具体。要获得最佳结果，您可以为名字和姓氏组合添加一项例外。

请参见第 296 页的“[关于规则例外](#)”。

请参见第 297 页的“[关于检测服务器策略执行](#)”。

关于使用复合规则进行精确检测

假设您担心源自网络的 Microsoft Word 文档。最初，您添加一项策略，该策略使用附件类型条件捕获所有 Word 文件。您很快发现许多包含 Word 文件附件的邮件并不泄露受保护的信息。

当您更仔细地检查事件时，您意识到您更担心的是包含词“机密”的 Word 文件。在这种情况下，您可以为词“机密”添加一个模式规则，将附件类型条件转化为复合规则。这种配置将获得更加精确的检测结果。

此外，要解决策略生成过多事件的问题，您可以设置事件最大值。要执行此操作，您可以将每个检测服务器配置为在给定的时间段内报告指定数量的事件。默认值是每台服务器在 24 小时内报告 10,000 个事件。

请参见第 297 页的“[关于复合匹配条件](#)”。

策略创建

本章节包括下列主题：

- [关于策略](#)
- [关于策略组件](#)
- [关于系统定义的策略模板](#)
- [关于解决方案软件包](#)
- [关于策略组](#)
- [关于策略部署](#)
- [关于策略创建权限](#)
- [关于策略模板导入和导出](#)
- [关于数据配置文件](#)
- [关于用户组](#)
- [实施策略](#)
- [策略最佳做法](#)

关于策略

通过实施策略可以检测和防止数据丢失。策略组合了检测规则和响应操作。如果违反了策略规则，系统将生成可报告和采取操作的事件。您实施的策略规则基于信息安全目标。为响应策略违规而执行的操作基于遵从性要求。

Enforce Server 管理控制台为创建策略提供了基于 Web 的集中式界面。

请参见第 306 页的“[关于策略组件](#)”。

表 16-1 策略创建功能

功能	说明
构建直观策略	策略生成器界面支持检测配置的布尔逻辑。 可以在单个策略中组合不同的检测方法和技术。 请参见第 297 页的“ 关于检测服务器策略执行 ”。
分离的响应规则	系统将响应规则和策略存储为单独的实体。 您可以管理和更新响应规则而不必更改策略；您可以在策略之间重复使用响应规则。 请参见第 653 页的“ 关于响应规则 ”。
细粒度的策略报告	系统提供了策略违规的严重性级别。 您可以按照最高严重性报告策略违规的整体严重性。 请参见第 295 页的“ 关于规则严重性 ”。
数据和组的集中式配置	系统将数据和组的配置文件与策略分开存储。 这样，无需更改策略即可管理和更新配置文件。 请参见第 312 页的“ 关于数据配置文件 ”。
基于模板的策略创建	系统提供了预先构建的 65 个策略模板。 您可以使用这些模板快速配置和部署策略。 请参见第 308 页的“ 关于系统定义的策略模板 ”。
策略共享	系统支持策略模板的导入和导出。 您可以在环境和系统中共享策略模板。 请参见第 311 页的“ 关于策略模板导入和导出 ”。
基于角色的访问控制	系统为各种用户功能和管理功能提供了基于角色的访问控制。 可以创建用于策略创建、策略管理和响应规则创建的角色。 请参见第 310 页的“ 关于策略创建权限 ”。

请参见第 314 页的“[实施策略](#)”。

请参见第 283 页的“[策略检测简介](#)”。

关于策略组件

一项有效的策略必须至少声明一个检测规则或组规则，检测规则或组规则至少包含一个匹配条件。响应规则是可选策略组件。

请参见第 305 页的“[关于策略](#)”。

表 16-2 策略组件

组件	使用	说明
策略组	必需	必须将策略分配给单个策略组。 请参见第 309 页的“ 关于策略组 ”。
策略名称	必需	策略名称在策略组内必须是唯一的。 请参见第 347 页的“ 管理和添加策略 ”。
策略规则	必需	一项有效的策略必须至少包含一个规则，该规则至少声明一个匹配条件。 请参见第 290 页的“ 检测规则简介 ”。
数据配置文件	可能需要	如果策略中的检测方法需要数据配置文件，该策略将需要数据配置文件。 请参见第 312 页的“ 关于数据配置文件 ”。
用户组	可能需要	仅当某个策略中的组方法需要用户组时，该策略才需要用户组。 同步的 DGM 规则和例外需要用户组。 请参见第 314 页的“ 关于用户组 ”。
策略说明	可选	策略说明帮助用户识别策略的用途。 请参见第 330 页的“ 配置策略 ”。
响应规则	可选	策略可以实施一个或多个响应规则以报告和补救事件。 请参见第 653 页的“ 关于响应规则 ”。
策略例外	可选	策略可包含一个或多个例外以从匹配项中排除数据。 请参见第 296 页的“ 关于规则例外 ”。
复合匹配条件	可选	策略规则或例外可以实施多个匹配条件。 请参见第 297 页的“ 关于复合匹配条件 ”。

请参见第 311 页的“[关于策略模板导入和导出](#)”。

关于系统定义的策略模板

Symantec Data Loss Prevention 提供了策略模板来帮助您在企业中快速部署数据丢失策略。通过将策略规则和例外作为模板导入和导出，可以在系统和环境之间共享策略。

使用策略模板可节省时间，并且有助于避免策略中出现错误和信息漏洞，因为已经预定义了检测方法。您可以编辑模板以创建能够精确满足您需求的策略。

请参见第 317 页的“[从模板创建策略](#)”。

某些策略模板基于众所周知的法律法规，例如“支付卡行业数据安全标准”、“金融服务现代化法案”、“美国加州参议院 1386 号法案”以及 HIPAA。其他策略模板更为常规，例如“客户数据保护”、“员工数据保护”以及“加密的数据”。虽然基于法规的模板有助于解决相关法规的要求，但还是要咨询法律顾问来验证是否符合法规。

请参见第 311 页的“[关于策略模板导入和导出](#)”。

表 16-3 可用策略模板

策略模板类型	说明
美国监管执法	请参见第 319 页的“ “美国监管执法”策略模板 ”。
英国与国际监管执法	请参见第 321 页的“ “英国与国际监管执法”策略模板 ”。
客户和员工数据保护	请参见第 322 页的“ “客户和员工数据保护”策略模板 ”。
机密的或分类的数据保护	请参见第 323 页的“ “机密的或分类的数据保护”策略模板 ”。
网络安全执法	请参见第 324 页的“ “网络安全执法”策略模板 ”。
可接受使用执法	请参见第 325 页的“ “可接受使用执法”策略模板 ”。
导入的模板	请参见第 311 页的“ 关于策略模板导入和导出 ”。
Enterprise Vault 的分类	请参见 <i>Enterprise Vault Data Classification Services Implementation Guide</i> (《Enterprise Vault 数据分类服务操作指南》)。

关于解决方案软件包

Symantec Data Loss Prevention 针对多个垂直行业提供了解决方案软件包。解决方案软件包包含支持特定行业或组织的已配置策略、响应规则、用户角色、报告、协议以及事件状态。有关可用解决方案软件包的列表及说明，请参考《Symantec Data Loss Prevention 安装指南》中的第 4 章“[导入解决方案软件包](#)”。您可将一个解决方案软件包导入到 Enforce Server。

导入解决方案软件包后，请通过查看策略来启动。默认情况下，解决方案软件包激活提供的策略。

请参见第 347 页的“[管理和添加策略](#)”。

关于策略组

可使用策略组将策略部署到检测服务器。策略组可限制特定用户可以访问的策略、事件和检测机制。

每项策略属于一个策略组。配置策略时，必须将它分配给策略组。您可以更改策略组分配，但不能将一个策略分配给多个策略组。可将策略组部署到一个或多个检测服务器。

为 Enforce Server 配置了一个名为“默认策略组”的策略组。系统会将默认策略组部署到所有检测服务器。如果您定义一个新策略，系统会将其分配到默认策略组，除非您创建并指定其他策略组。您可以更改默认策略组的名称。解决方案软件包会创建多个策略组，并为这些策略组分配策略。

创建策略组之后，您可以将策略、发现目标和角色链接到该策略组。创建发现目标时，您必须将其与单个策略组相关联。将角色与特定策略组关联时，可以限制使用该角色的用户。该策略组中的策略会检测事件并将其报告给具有分配给该策略组的角色的用户。

策略组和检测服务器之间的关系取决于服务器类型。您可以将一个策略组部署到一个或多个 Network Monitor、Network Prevent、Mobile Prevent 或 Endpoint Server。部署到 Endpoint Server 的策略组适用于在该服务器上注册的所有 DLP Agent。Enforce Server 会自动将所有策略组与所有 Network Discover Server 相关联。

对于 Network Monitor 和 Network Prevent，将每个策略组分配给一个或多个 Network Monitor Server、Email Prevent Server 或 Network Prevent (Web) Server。对于 Mobile Prevent，每个策略组都可指派给一个或多个 Mobile Prevent for Web Server。对于 Network Discover，将策略组分配给单个发现目标。一个检测服务器可处理尽可能多的策略组以扫描其目标。对于 Endpoint Monitor，将策略组分配给 Endpoint Server，这些策略组会应用于已注册的所有 DLP Agent。

请参见第 308 页的“[关于解决方案软件包](#)”。

请参见第 308 页的“[关于解决方案软件包](#)”。

请参见第 350 页的“[管理和添加策略组](#)”。

请参见第 349 页的“[创建和修改策略组](#)”。

关于策略部署

您可以使用策略组以各种方式组织和部署策略。例如，考虑一下在跨多个国家/地区的系统上设置检测服务器的情形。您可以使用策略组来确保检测服务器只运行对特定位置有效的策略。

您可以使用一些检测服务器专门监视内部网络流量，使用其他检测服务器专门监视网络退出点。您可以使用策略组将具有较少限制的策略部署到监视内部流量的服务器。同时，您可以将具有较严格限制的策略部署到监视离开您网络的流量的服务器。

请参见第 309 页的“[关于策略组](#)”。

您可以使用策略组按业务单位、部门、地理位置或其他任何组织单位组织策略和事件。例如，特定部门的策略组可能适合安全责任已分散到各组的那种情形。在这种情况下，策略组适用于查看和编辑事件时需实施的基于角色的访问控制。您根据组织中所需的访问权限划分来部署策略组（例如，按业务单位）。

请参见第 77 页的“[关于基于角色的访问控制](#)”。

您可以将策略组用于检测服务器分配，这在安全部门比较集中的情形中更常见。在这些情况下，您应仔细为每个角色选择检测服务器分配并在策略组名称中反映服务器名称。例如，您可能将组命名为“入站”和“出站”，“美国”和“国际”，或“测试”和“生产”。

在更加复杂的环境中，您可以在部署策略时考虑下列策略组的某些组合：

- 销售和营销 - 美国
- 销售和营销 - 欧洲
- 销售和营销 - 亚洲
- 销售和营销 - 澳大利亚、新西兰
- 人力资源 - 美国
- 人力资源 - 国际
- 研究与开发
- 客户服务

最后，您可以使用策略组测试策略后再在生产环境中部署策略，还可以使用策略组管理旧策略以及导入和导出策略模板。

关于策略创建权限

策略作者配置并管理策略及其规则和例外。要创建策略，必须为用户分配可授予策略创建权限的角色。可以扩展此角色以包括策略组的管理、扫描目标和凭据。

请参见第 77 页的“[关于基于角色的访问控制](#)”。

响应规则创建权限是一种与策略创建和管理权限不同的凭据。策略作者是否具有响应规则创建权限取决于企业需要。

请参见第 664 页的“[关于响应规则创建权限](#)”。

表 16-4 策略创建权限

角色权限	说明
创建策略	<ul style="list-style-type: none">■ 添加、配置和管理策略。■ 添加、配置和管理策略规则和例外。■ 导入和导出策略模板。■ 修改系统定义的数据标识符并创建自定义数据标识符。■ 添加、配置和管理用户组。■ 向策略添加响应规则（但不创建响应规则）。
Enforce Server 管理	<ul style="list-style-type: none">■ 添加、配置和管理策略组。
创建响应规则	<ul style="list-style-type: none">■ 添加、配置和管理响应规则（但不将其添加到策略）。

关于策略模板导入和导出

您可以从 Enforce Server 导出策略模板以及向其导入策略模板。此功能允许您跨环境共享策略、对现有策略进行版本控制和存档旧版策略。

请参见第 351 页的“[导入策略模板](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

请设想这样一种情形，在测试系统上创建并优化策略，然后将策略作为模板导出。然后将该策略导入到生产系统以部署到一个或多个检测服务器。或者，如果您要废弃某个策略，可以将它作为模板导出以进行存档，然后将其从系统中删除。

策略模板为 XML 文件。该模板包含策略元数据以及检测和组规则及例外。如果策略模板包含需要数据配置文件的多个条件，则系统仅导入这些条件中的某一个。策略模板不包含策略响应规则，或者修改的或自定义数据标识符。

请参见第 352 页的“[将 10 版数据标识符或关键字策略导入 11 版系统](#)”。

表 16-5 策略模板中包含的组件

策略组件	包含在模板中
策略元数据（名称、说明）。	是
模板的名称必须少于 60 个字符，否则不会显示在“导入的模板”列表中。	
指定内容匹配 (DCM) 规则和例外。 注意： 无法将带有数据标识符或关键字匹配规则或例外的版本 10 策略模板导入到版本 11 系统。请参见第 352 页的“ 将 10 版数据标识符或关键字策略导入 11 版系统 ”。	是
单个 EDM 检测规则，或单个 IDM 检测规则或例外。 如果模板包含多种 EDM 或 IDM 方法，则仅导出其中之一。 如果模板包含一种 EDM 和一种 IDM 方法，则系统会放弃 IDM。	是
用户组方法。 仅当用户组在导入前存在于目标上时，导入时才能保留用户组方法。	否
不导出策略组。 导入时您可以选择本地策略组，否则系统会将策略分配到默认策略组。	否
不导出响应规则。 您必须在本地 Enforce Server 实例上定义响应规则，并将其添加到策略。	否
不导出数据配置文件。 导入时您必须引用本地定义的数据配置文件，否则系统将放弃需要数据配置文件的任何方法。	否
不导出修改的和自定义数据标识符。	否
不导出自定义协议。	否
不导出策略状态（活动/已挂起）。	否

关于数据配置文件

Symantec Data Loss Prevention 允许创建不同类型的数据配置文件，用于敏感数据和内容的确切、精确或相似检测。

表 16-6 数据配置文件的类型

数据配置文件类型	说明
EDM 策略的确切数据配置文件	<p>确切数据配置文件包含已从结构化数据源（例如数据库、目录服务器或 CSV 文件）编制索引的确切数据。</p> <p>例如，员工数据库可能包含“名字”、“姓氏”、SSN、“入职日期”和“薪水”列。该数据库中的每一行条目都将在每列包含一个值。要创建确切数据配置文件，请将数据库导出到文件，然后系统对其进行索引。每行均显示为一个独立的行，并且使用分隔符（逗号、制表符或竖线字符）分隔一行中的每个数据项。例如，某一行可能显示以下内容：Bob,Smith,000-00-000,05/26/99,\$42500。在创建确切数据配置文件时，将保护数据库中每个单元格的数据。例如，假设策略指定，如果同时找到名字、姓氏和 SSN，则生成一个事件。如果邮件包含 Joe,Smith,000-00-0000，则它不是匹配项，因为名字不匹配。但是，如果邮件包含 Bob,Smith,000-00-0000，则它是一个匹配项并生成一个事件。</p> <p>确切数据配置文件在检测服务器上运行。如果将 EDM 策略部署到某个端点，DLP Agent 会将邮件发送给检测服务器进行评估（双层检测）。</p> <p>请参见第 356 页的“关于实施确切数据匹配”。</p> <p>请参见第 356 页的“实施确切数据匹配”。</p>
IDM 策略的索引文档配置文件	<p>索引文档配置文件包含已从一组机密文档编制索引的确切数据。</p> <p>例如，您可以创建 IDM 索引，用于设置指纹并保护存储在财务文档、新闻稿草稿或源代码中的内容。您可以在网络文件共享中编制文档索引，也可以将这些文档上传到 Enforce Server。您可以将索引文档配置文件部署到策略中，并在找到索引文档的确切版本或经指纹加密的文档的段落或章节被暴露时进行检测。</p> <p>索引文档配置文件在检测服务器上运行。如果将 IDM 策略部署到某个端点，DLP Agent 会将邮件发送给检测服务器进行评估（双层检测）。</p> <p>请参见第 377 页的“关于实施索引文档匹配”。</p> <p>请参见第 382 页的“实施索引文档匹配”。</p>

数据配置文件类型	说明
VML 策略的向量机学习配置文件	<p>向量机学习配置文件包含从要保护的内容中提取的特征（关键字）的统计模型。</p> <p>例如，您可以创建 VML 配置文件来保护源代码。在这种情况下，可使用正面示例文档（要保护的专有代码）和负面示例文档（不必保护的开放源代码）对系统进行培训。VML 策略引用 VML 配置文件来分析消息数据并识别与正面特征相似的内容。可对 VML 配置文件进行调整，并且可通过在培训集中添加或删除文档轻松地更新此配置文件。</p> <p>检测服务器和 DLP Agent 将 VML 配置文件加载到内存中。VML 不需要双层检测。</p> <p>请参见第 396 页的“实施向量机学习 (VML)”。</p> <p>请参见第 396 页的“实施向量机学习 (VML)”。</p>

关于用户组

您可以在 Enforce Server 上定义用户组。用户组包含您通过将 Enforce Server 与组目录服务器 (Microsoft Active Directory) 同步来填充的用户身份信息。

要定义用户组，您必须至少具有策略创建权限或服务器管理员权限。必须在同步用户之前定义用户组。

定义用户组后，使用目录服务器中的用户、组和业务单位填充该用户组。填充用户组后，将该组与“用户/发送者和接受者”检测规则或例外关联。该策略仅适用于该用户组中的成员。

请参见第 288 页的“[关于目录组匹配](#)”。

请参见第 485 页的“[关于实施同步的目录组匹配](#)”。

请参见第 116 页的“[配置目录服务器连接](#)”。

请参见第 487 页的“[创建或修改用户组](#)”。

实施策略

策略用于定义您要检测的内容、事件上下文和身份。策略还可以定义违反策略后的响应操作。

请参见第 305 页的“[关于策略](#)”。

成功的策略创建是一个需要认真分析并正确配置以获取最优结果的过程。

表 16-7 策略实施过程

操作	说明
自行熟悉 Symantec Data Loss Prevention 所提供的不同类型的检测技术和方法。	请参见第 285 页的“ 可用检测技术 ”。 请参见第 290 页的“ 检测规则简介 ”。 请参见第 310 页的“ 关于策略创建权限 ”。
创建策略检测战略以定义要防止发生数据丢失的数据类型。	
查看 Symantec Data Loss Prevention 附带的策略模板和您手动导入或解决方案软件包导入的任何模板。	请参见第 308 页的“ 关于系统定义的策略模板 ”。 请参见第 308 页的“ 关于解决方案软件包 ”。
创建策略组以控制访问、编辑和部署策略的方式。	请参见第 309 页的“ 关于策略组 ”。 请参见第 310 页的“ 关于策略部署 ”。
要检测确切数据、内容或类似非结构化数据，请创建一个或多个数据配置文件。	请参见第 312 页的“ 关于数据配置文件 ”。
要从同步的目录服务器(Active Directory)中检测确切身份，请配置一个或多个用户组。	请参见第 314 页的“ 关于用户组 ”。
配置检测条件并将规则和例外分组。	请参见第 317 页的“ 从模板创建策略 ”。
测试和优化策略。	
向策略中添加响应规则，用于在违反策略时执行相应操作。	请参见第 653 页的“ 关于响应规则 ”。
管理企业中的策略。	请参见第 347 页的“ 管理和添加策略 ”。

策略最佳做法

实施策略时，请注意下列事项：

- 使用系统提供的策略模板作为实施策略的起点。
请参见第 317 页的“[从模板创建策略](#)”。
- 精心创建的策略会准确检测受保护数据和内容，同时将误报减到最少。从细节开始检测。启用一个或两个策略模板或几个条件，例如关键字匹配。查看策略检测到的事件。在实施响应规则以采取操作前，请调整结果。

请参见第 299 页的“[实施策略检测](#)”。

- 请注意实施策略所需的角色。策略创建权限会授予对策略配置的访问权限，包括规则和例外。Enforce Server 管理员权限会授予对数据配置文件定义和管理的访问权限。响应规则创建权限是一种与策略创建不同的权限。

请参见第 82 页的“[关于建议的组织角色](#)”。

- 在实际运行中使用策略之前，使用策略组对其进行测试。创建一个只有您具有访问权限的测试策略组。然后，创建策略并将其添加到该测试策略组。查看测试策略捕获的事件。优化策略并确认其捕获所需事件后，重命名该策略组并授予其相应的角色访问权限。

请参见第 309 页的“[关于策略组](#)”。

- 使用策略组管理旧策略以及要导入或计划导出的策略。

请参见第 353 页的“[关于删除策略和策略组](#)”。

基于模板创建策略

本章节包括下列主题：

- [从模板创建策略](#)
- [“美国监管执法”策略模板](#)
- [“英国与国际监管执法”策略模板](#)
- [“客户和员工数据保护”策略模板](#)
- [“机密的或分类的数据保护”策略模板](#)
- [“网络安全执法”策略模板](#)
- [“可接受使用执法”策略模板](#)
- [选择确切数据配置文件](#)
- [选择索引文档配置文件](#)

从模板创建策略

您可以从系统提供的模板或从导入到 Enforce Server 中的模板创建策略。

请参见第 308 页的[“关于系统定义的策略模板”](#)。

请参见第 311 页的[“关于策略模板导入和导出”](#)。

表 17-1 从模板创建策略

操作	说明
从模板添加策略。	请参见第 329 页的 “添加新的策略或策略模板” 。

操作	说明
<p>选择要使用的模板。</p>	<p>在“管理”>“策略”>“策略列表”>“添加策略 - 模板列表”屏幕中，系统会列出所有策略模板。</p> <p>系统提供的模板类别：</p> <ul style="list-style-type: none"> ■ 请参见第 319 页的“美国监管执法”策略模板”。 ■ 请参见第 321 页的“英国与国际监管执法”策略模板”。 ■ 请参见第 322 页的“客户和员工数据保护”策略模板”。 ■ 请参见第 323 页的“机密的或分类的数据保护”策略模板”。 ■ 请参见第 324 页的“网络安全执法”策略模板”。 ■ 请参见第 325 页的“可接受使用执法”策略模板”。 <p>“导入的模板”在导入后会单独显示：</p> <ul style="list-style-type: none"> ■ 请参见第 351 页的“导入策略模板”。 <p>注意：有关分类策略模板的信息，请参见 <i>Enterprise Vault Data Classification Services Implementation Guide</i> (《Enterprise Vault 数据分类服务操作指南》)。</p>
<p>单击“下一步”配置策略。</p>	<p>例如，选择 Webmail 策略模板，然后单击“下一步”。</p> <p>请参见第 330 页的“配置策略”。</p>
<p>选择“数据配置文件”(如有提示)。</p>	<p>如果该模板依赖于一个或多个数据配置文件，系统会提示您选择下列各项：</p> <ul style="list-style-type: none"> ■ 确切数据配置文件 请参见第 326 页的“选择确切数据配置文件”。 ■ 已编制索引的文档配置文件 请参见第 327 页的“选择索引文档配置文件”。 <p>如果没有“数据配置文件”，则可以执行下列操作之一：</p> <ul style="list-style-type: none"> ■ 取消策略定义过程，定义配置文件，然后继续从模板创建策略。 ■ 单击“下一步”配置策略。 <p>创建策略时，系统会关闭依赖于数据配置文件的所有规则或例外。</p> <p>注意：如果模板要求使用配置文件，则应使用该配置文件。</p>

操作	说明
编辑策略名称或说明（可选）。	<p>如果打算修改系统定义的模板，可能需要更改名称，以便可以与原来的模板区分开。</p> <p>请参见第 330 页的“配置策略”。</p> <p>注意：如果要将策略导出为模板，策略名称必须少于 60 个字符。如果多于 60 个字符，模板将不会显示在“模板列表”屏幕的“导入的模板”部分中。</p>
选择策略组（如有必要）。	<p>如果已定义了策略组，则从“策略组”列表中选择它。</p> <p>请参见第 349 页的“创建和修改策略组”。</p> <p>如果尚未定义策略组，则系统会将策略部署到“默认策略组”。</p>
编辑策略规则或例外（如有必要）。	<p>“配置策略”屏幕将显示策略提供的规则和例外（如果有）。您可以修改、添加和删除满足要求的策略规则和例外。</p> <p>请参见第 334 页的“配置策略规则”。</p> <p>请参见第 342 页的“配置策略例外”。</p>
保存策略并将其导出（可选）。	<p>单击“保存”保存该策略。</p> <p>您可以将策略检测导出为模板以进行共享或存档。</p> <p>请参见第 351 页的“将策略检测导出为模板”。</p> <p>例如，如果已更改系统定义的策略模板的配置，则可能希望将其导出以在整个环境中共享。</p>
测试和调整策略（建议）。	<p>使用策略应检测到或不应检测到的数据测试和调整策略。</p> <p>查看策略生成的事件。根据需要优化策略规则和例外，以减少误报和漏报。</p>
添加响应规则（可选）。	<p>将响应规则添加到策略以报告违规并对其进行补救。</p> <p>请参见第 664 页的“实施响应规则”。</p> <p>注意：响应规则未包含在策略模板中。</p>

“美国监管执法”策略模板

Symantec Data Loss Prevention 提供了几个支持美国监管执法准则的策略模板。请参见第 317 页的“[从模板创建策略](#)”。

表 17-2 “美国监管执法”策略模板

策略模板	说明
CAN-SPAM 法案	确立发送商业电子邮件的要求。 请参见第 589 页的“ CAN-SPAM 法案策略模板 ”。
国防信息系统 (DMS) 的常规服务分类	检测分类为机密的信息。 请参见第 597 页的“ 国防信息系统 (DMS) 的常规服务分类策略模板 ”。
出口管理条例 (EAR)	强制实施美国商务部出口管理条例 (EAR)。 请参见第 600 页的“ 出口管理条例 (EAR) 策略模板 ”。
FACTA 2003 (红色标记规则)	强制实施公平准确信用交易法案 (FACTA) 2003 的第 114 和 315 (或红色标记规则) 部分。 请参见第 602 页的“ FACTA 2003 (红色标记规则) 策略模板 ”。
金融服务法案	此策略会限制金融机构对客户信息进行共享。 请参见第 606 页的“ 金融服务法案”策略模板 ”。
HIPAA 和 HITECH (包括 PHI)	此策略会强制实施美国医疗保险流通与责任法案 (HIPAA)。 请参见第 608 页的“ HIPAA 和 HITECH (包括 PHI) 策略模板 ”。
国际武器贸易条例 (ITAR)	此策略会强制实施美国国务院 ITAR 条款。 请参见第 613 页的“ 国际武器贸易条例 (ITAR) 策略模板 ”。
NASD 规则 2711 以及 NYSE 规则 351 和 472	此策略会保护参与即将进行的股票发行的任何公司的名称。 请参见第 616 页的“ NASD 规则 2711 以及 NYSE 规则 351 和 472 策略模板 ”。
NASD 规则 3010 和 NYSE 规则 342	此策略会监视券商的通信情况。 请参见第 618 页的“ NASD 规则 3010 和 NYSE 规则 342 策略模板 ”。
NERC 电气设备安全指导	此策略会为电力行业检测北美电力可靠性委员会 (NERC) 安全指导中所列出的信息。 请参见第 619 页的“ NERC 电气设备安全指导策略模板 ”。

策略模板	说明
外国资产管制办公室 (OFAC)	此模板会检测涉及目标 OFAC 组的通信情况。 请参见第 622 页的“ 外国资产管制办公室 (OFAC) 策略模板 ”。
OMB 备忘录 06-16 和 FIPS 199 条例	此模板会检测分类为机密的信息。 请参见第 623 页的“ OMB 备忘录 06-16 和 FIPS 199 条例策略模板 ”。
支付卡行业数据安全标准	此模板会检测 Visa 和 MasterCard 信用卡号数据。 请参见第 625 页的“ 支付卡行业 (PCI) 数据安全标准策略模板 ”。
萨班斯-奥克斯利法案 (Sarbanes-Oxley)	此模板会检测敏感的财务数据。 请参见第 632 页的“ 萨班斯-奥克斯利法案策略模板 ”。
SEC 公平披露规则	此模板会检测披露重要财务信息的数据。 请参见第 634 页的“ SEC 公平披露规则策略模板 ”。
州数据隐私	此模板会检测违反州/省规定的机密性的行为。 请参见第 637 页的“ 州数据隐私策略模板 ”。
美国情报控制标记 (CAPCO) 和 DCID 1/7	此模板会检测已认可词汇，以便识别美国联邦情报机构的分类信息。 请参见第 644 页的“ 美国情报控制标记 (CAPCO) 和 DCID 1/7 策略模板 ”。

“英国与国际监管执法”策略模板

Symantec Data Loss Prevention 为 “英国与国际监管执法” 提供了几个策略模板。
请参见第 317 页的“[从模板创建策略](#)”。

表 17-3 “英国与国际监管执法” 策略模板

策略模板	说明
Caldicott 报告	此策略会保护英国患者的信息。 请参见第 587 页的“ Caldicott 报告策略模板 ”。

策略模板	说明
1998 年英国数据保护法案	此策略会保护个人身份信息。 请参见第 594 页的 “1998 年数据保护法案（英国）策略模板” 。
欧盟数据保护规定	此策略会检测特定于欧盟指令的个人数据。 请参见第 596 页的 “数据保护规定（欧盟）策略模板” 。
1998 年人权法	此策略会强制实施英国公民法案第 8 条。 请参见第 612 页的 “1998 年人权法策略模板” 。
PIPEDA	此策略会检测加拿大公民客户数据。 请参见第 626 页的 “PIPEDA 策略模板” 。

“客户和员工数据保护”策略模板

Symantec Data Loss Prevention 为“客户和员工数据保护”提供了几个策略模板。

请参见第 317 页的[“从模板创建策略”](#)。

表 17-4 “客户和员工数据保护”策略模板

策略模板	说明
加拿大社会保险号	此策略会检测指示加拿大社会保险号 (SIN) 的模式。 请参见第 589 页的 “加拿大社会保险号策略模板” 。
信用卡号	此策略会检测指示信用卡号的模式。 请参见第 592 页的 “信用卡号策略模板” 。
客户数据保护	此策略会检测客户数据。 请参见第 593 页的 “客户数据保护策略模板” 。
员工数据保护	此策略会检测员工数据。 请参见第 599 页的 “员工数据保护策略模板” 。
个人纳税识别号 (ITIN)	此策略会检测由 IRS 颁发的税务处理号。 请参见第 613 页的 “个人纳税识别号 (ITIN) 策略模板” 。
SWIFT 代码	此策略会检测银行用于跨国界转账的代码。 请参见第 641 页的 “SWIFT 代码策略模板” 。

策略模板	说明
英国驾照号	此策略会检测英国驾照号。 请参见第 642 页的 “英国驾照号策略模板” 。
英国选民登记号	此策略会检测英国选民登记号。 请参见第 642 页的 “英国选民登记号策略模板” 。
英国国家保险号码	此策略会检测英国国家保险号码。 请参见第 643 页的 “英国国家保险号码策略模板” 。
英国国民保健服务号	此策略会检测 NHS 颁发的个人标识号码。 请参见第 642 页的 “英国国民保健服务 (NHS) 号策略模板” 。
英国护照号	此策略会检测有效的英国护照。 请参见第 643 页的 “英国护照号策略模板” 。
英国税号	此策略会检测英国税号。 请参见第 644 页的 “英国税号策略模板” 。
美国社会安全号	此策略会检测指示社会安全号的模式。 请参见第 645 页的 “美国社会安全号策略模板” 。

“机密的或分类的数据保护”策略模板

Symantec Data Loss Prevention 为“机密的或分类的数据保护”提供了几个策略模板。

请参见第 317 页的[“从模板创建策略”](#)。

表 17-5 “机密的或分类的数据保护”策略模板

策略模板	说明
机密文档	此策略会检测公司机密文档。 请参见第 591 页的 “机密文档策略模板” 。
设计文档	此策略会检测各种类型的设计文档。 请参见第 598 页的 “设计文档策略模板” 。
加密的数据	此策略会通过多种方法来检测是否使用了加密。 请参见第 600 页的 “加密数据策略模板” 。

策略模板	说明
金融信息	此策略会检测财务数据和信息。 请参见第 605 页的“ 金融信息策略模板 ”。
并购协议	此策略会检测有关即将进行的并购活动的信息和通信内容。 请参见第 615 页的“ 并购协议策略模板 ”。
价格信息	此策略会检测特定的 SKU 或价格信息。 请参见第 628 页的“ 价格信息策略模板 ”。
项目数据	此策略会检测对敏感项目的讨论。 请参见第 629 页的“ 项目数据策略模板 ”。
专有媒体文件	此策略会检测各种类型的视频和音频文件。 请参见第 629 页的“ 专有媒体文件策略模板 ”。
出版文档	此策略会检测各种出版文档。 请参见第 630 页的“ 出版文档策略模板 ”。
简历	此策略会检测活动的职位搜索。 请参见第 631 页的“ 简历策略模板 ”。
源代码	此策略会检测各种源代码。 请参见第 637 页的“ 源代码策略模板 ”。
Symantec DLP 感知与避免	此策略会检测引用 Symantec DLP 或其他数据丢失防护系统的任何通信和可能的检测避免行为。 请参见第 641 页的“ Symantec DLP 感知与避免策略模板 ”。

“网络安全执法”策略模板

Symantec Data Loss Prevention 为“网络安全执法”提供了几个策略模板。

请参见第 317 页的“[从模板创建策略](#)”。

表 17-6 “网络安全执法”策略模板

策略模板	说明
常见间谍软件上传站点	此策略会检测对常见间谍软件上传网站的访问。 请参见第 591 页的“ 常见间谍软件上传站点策略模板 ”。

策略模板	说明
网络图	此策略会检测计算机网络图。 请参见第 620 页的“ 网络图策略模板 ”。
网络安全	此策略会检测是否存在黑客工具和攻击计划。 请参见第 621 页的“ 网络安全策略模板 ”。
密码文件	此策略会检测密码文件格式。 请参见第 625 页的“ 密码文件策略模板 ”。

“可接受使用执法”策略模板

Symantec Data Loss Prevention 为下列允许的信息用途提供了几个策略模板。
请参见第 317 页的“[从模板创建策略](#)”。

表 17-7 “可接受使用执法”策略模板

策略模板	说明
竞争对手通信	此策略会检测与竞争对手之间的禁止的通信。 请参见第 591 页的“ 竞争对手通信策略模板 ”。
禁止访问的网站	此策略会检测对指定网站的访问。 请参见第 605 页的“ 禁止访问的网站策略模板 ”。
赌博	此策略会检测对赌博的任何引用。 请参见第 606 页的“ 赌博策略模板 ”。
非法药品	此策略会检测有关非法药品和管制物的对话。 请参见第 612 页的“ 非法药品策略模板 ”。
媒体文件	此策略会检测各种类型的视频和音频文件。 请参见第 614 页的“ 媒体文件策略模板 ”。
攻击性语言	此策略会检测攻击性语言的使用。 请参见第 621 页的“ 攻击性语言策略模板 ”。
种族歧视语言	此策略会检测种族歧视语言的使用。 请参见第 630 页的“ 种族歧视语言策略模板 ”。

策略模板	说明
受限文件	此策略会检测通常不适合发送到公司之外的各种文件类型。 请参见第 631 页的“ 受限文件策略模板 ”。
受限接受者	此策略会检测与指定接受者之间的通信。 请参见第 631 页的“ 受限接受者策略模板 ”。
下流语言	此策略会检测下流内容。 请参见第 636 页的“ 下流语言策略模板 ”。
暴力与武器	此策略会检测暴力语言和有关武器的讨论。 请参见第 646 页的“ 暴力与武器策略模板 ”。
Webmail	此策略会检测各种 Webmail 服务的使用情况。 请参见第 646 页的“ Webmail 策略模板 ”。
Yahoo 留言板活动	此策略会检测 Yahoo 留言板活动。 请参见第 647 页的“ Yahoo 留言板活动策略模板 ”。
端口 80 上的 Yahoo 和 MSN Messenger	此策略会检测 Yahoo IM 和 MSN Messenger 活动。 请参见第 648 页的“ 端口 80 上的 Yahoo 和 MSN Messenger 策略模板 ”。

选择确切数据配置文件

如果选择的策略模板实施确切数据匹配 (EDM)，系统会提示您选择“确切数据配置文件”。

请参见第 286 页的“[关于确切数据匹配](#)”。

使用确切数据配置文件

1 从可用配置文件的列表中选择“[确切数据配置文件](#)”。

2 单击“[下一步](#)”继续从模板创建策略。

单击“[上一步](#)”返回到策略模板的列表。

请参见第 317 页的“[从模板创建策略](#)”。

如果没有“[确切数据配置文件](#)”，则可以取消策略创建操作并定义配置文件。或者，可以选择不使用“[确切数据配置文件](#)”。在这种情况下，系统会禁用策略模板中关联的 EDM 检测规则。您可以使用策略模板提供的所有 DCM 规则或例外。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

注意：当系统提示您选择“确切数据配置文件”时，显示屏会列出该配置文件中要包含的数据列，以提供最高水平的准确性。如果在所选策略模板中未显示确切数据配置文件中的数据字段，系统会在您定义检测规则时为内容匹配显示这些字段。

表 17-8 实施确切数据匹配 (EDM) 的策略模板

策略模板	说明
Caldicott 报告	请参见第 587 页的“ Caldicott 报告策略模板 ”。
客户数据保护	请参见第 593 页的“ 客户数据保护策略模板 ”。
1988 年数据保护法案	请参见第 594 页的“ 1998 年数据保护法案（英国）策略模板 ”。
员工数据保护	请参见第 599 页的“ 员工数据保护策略模板 ”。
欧盟数据保护规定	请参见第 596 页的“ 数据保护规定（欧盟）策略模板 ”。
出口管理条例 (EAR)	请参见第 600 页的“ 出口管理条例 (EAR) 策略模板 ”。
FACTA 2003 (红色标记规则)	请参见第 602 页的“ FACTA 2003 (红色标记规则) 策略模板 ”。
金融服务法案	请参见第 606 页的“ 金融服务法案”策略模板 ”。
HIPAA 和 HITECH (包括 PHI)	请参见第 608 页的“ HIPAA 和 HITECH (包括 PHI) 策略模板 ”。
1998 年人权法	请参见第 612 页的“ 1998 年人权法策略模板 ”。
国际武器贸易条例 (ITAR)	请参见第 613 页的“ 国际武器贸易条例(ITAR)策略模板 ”。
支付卡行业数据安全标准	请参见第 625 页的“ 支付卡行业(PCI)数据安全标准策略模板 ”。
PIPEDA	请参见第 626 页的“ PIPEDA 策略模板 ”。
价格信息	请参见第 628 页的“ 价格信息策略模板 ”。
简历	请参见第 631 页的“ 简历策略模板 ”。
州数据隐私	请参见第 634 页的“ SEC 公平披露规则策略模板 ”。

选择索引文档配置文件

如果选择的策略模板使用索引文档匹配 (IDM) 检测，系统会提示您选择“文档配置文件”。

请参见第 287 页的“[关于索引文档匹配](#)”。

使用文档配置文件

- 1 从可用配置文件的列表中选择“文档配置文件”。
- 2 单击“下一步”从模板创建策略。

请参见第 317 页的“[从模板创建策略](#)”。

如果没有“文档配置文件”，则可以取消策略创建操作并定义“文档配置文件”。或者，可以选择不使用“文档配置文件”。在这种情况下，系统会禁用策略实例的所有 IDM 规则或例外。如果策略模板包含 DCM 规则或例外，则可以使用它们。

请参见第 377 页的“[关于实施索引文档匹配](#)”。

表 17-9 实施索引文档匹配 (IDM) 的策略模板

策略模板	说明
CAN-SPAM 法案 (IDM 例外)	请参见第 589 页的“ CAN-SPAM 法案策略模板 ”。
NASD 规则 2711 以及 NYSE 规则 351 和 472	请参见第 616 页的“ NASD 规则 2711 以及 NYSE 规则 351 和 472 策略模板 ”。
NERC 电气设备安全指导	请参见第 619 页的“ NERC 电气设备安全指导策略模板 ”。
萨班斯-奥克斯利法案 (Sarbanes-Oxley)	请参见第 632 页的“ 萨班斯-奥克斯利法案策略模板 ”。
SEC 公平披露规则	请参见第 634 页的“ SEC 公平披露规则策略模板 ”。
机密文档	请参见第 591 页的“ 机密文档策略模板 ”。
设计文档	请参见第 598 页的“ 设计文档策略模板 ”。
金融信息	请参见第 605 页的“ 金融信息策略模板 ”。
项目数据	请参见第 629 页的“ 项目数据策略模板 ”。
专有媒体文件	请参见第 629 页的“ 专有媒体文件策略模板 ”。
出版文档	请参见第 630 页的“ 出版文档策略模板 ”。
源代码	请参见第 637 页的“ 源代码策略模板 ”。
网络图	请参见第 620 页的“ 网络图策略模板 ”。

配置策略

本章节包括下列主题：

- [添加新的策略或策略模板](#)
- [配置策略](#)
- [将规则添加至策略中](#)
- [配置策略规则](#)
- [定义规则严重性](#)
- [配置匹配计数](#)
- [选择匹配的组件](#)
- [向策略中添加例外](#)
- [配置策略例外](#)
- [配置复合匹配条件](#)

添加新的策略或策略模板

作为策略作者，您可以从头开始或从模板定义新策略。

请参见第 314 页的“[实施策略](#)”。

添加新的策略或策略模板

1 单击“管理”>“策略”>“策略列表”屏幕中的“添加策略”。

请参见第 347 页的[“管理和添加策略”](#)。

2 在“新建策略”屏幕中选择要添加的策略的类型。

选择“添加空白策略”添加新的空策略。

请参见第 306 页的[“关于策略组件”](#)。

选择“从模板添加策略”从模板添加策略。

请参见第 308 页的[“关于系统定义的策略模板”](#)。

3 单击“下一步”配置策略或策略模板。

请参见第 330 页的[“配置策略”](#)。

请参见第 317 页的[“从模板创建策略”](#)。

单击“取消”将不添加策略并返回到“策略列表”屏幕。

配置策略

“管理”>“策略”>“策略列表”>“配置策略”屏幕是用于配置策略的主页。

表 18-1 配置策略

操作	说明
定义新的策略或编辑现有策略。	添加新的空白策略。 请参见第 329 页的 “添加新的策略或策略模板” 。 从模板创建策略。 请参见第 317 页的 “从模板创建策略” 。 在“管理”>“策略”>“策略列表”屏幕上选择现有策略，以对其进行编辑。 请参见第 347 页的 “管理和添加策略” 。
输入策略“名称”和“说明”。	策略名称在您将策略部署到的策略组中必须是唯一的。 要导入策略作为模板，策略名称必须少于 60 个字符，否则策略名称不会出现在“导入的模板”列表中。

操作	说明
从要部署策略的列表中选择“策略组”。	<p>如果没有已配置的策略组，则会选择“默认策略组”。</p> <p>请参见第 349 页的“创建和修改策略组”。</p>
设置策略的“状态”。	<p>可以启用（默认设置）或禁用策略。禁用的策略已部署但不会检测事件。</p> <p>请参见第 347 页的“管理和添加策略”。</p>
向策略添加规则或编辑现有规则。	<p>单击“添加规则”以添加规则。</p> <p>请参见第 332 页的“将规则添加至策略中”。</p> <p>选择现有规则进行编辑。</p>
使用一个或多个条件配置规则。	<p>对于有效策略，必须至少配置一个规则，而一个规则至少声明一个条件。复合条件和例外是可选的。</p> <p>请参见第 334 页的“配置策略规则”。</p>
或者，添加一个或多个策略例外或编辑现有例外。	<p>单击“添加例外”以添加例外。</p> <p>请参见第 340 页的“向策略中添加例外”。</p> <p>选择现有的例外进行编辑。</p>
配置所有例外。	请参见第 342 页的 “配置策略例外” 。
保存策略配置。	<p>单击“保存”，将策略配置保存到Enforce Server 数据库。</p> <p>请参见第 306 页的“关于策略组件”。</p>
将策略导出为模板。	<p>或者，可以将策略规则和例外导出为模板。</p> <p>请参见第 351 页的“将策略检测导出为模板”。</p>
向策略添加一个或多个响应规则。	<p>配置独立于策略的响应规则。</p> <p>请参见第 669 页的“配置响应规则”。</p> <p>请参见第 352 页的“向策略添加自动响应规则”。</p>

注意：“策略操作”设置仅适用于分类策略。有关更多信息，请参见 *Enterprise Vault Data Classification Services Implementation Guide*（《Enterprise Vault 数据分类服务操作指南》）。

将规则添加至策略中

在“管理”>“策略”>“策略列表”>“配置策略 - 添加规则”屏幕中，可以向策略中添加一个或多个规则。

您可以向策略中添加两种类型的规则：检测和组。如果某策略中的两个或多个规则属于同一类型，系统会使用 OR 将其连接起来。如果同一策略中的两个或多个规则属于不同类型，系统会使用 AND 将其连接起来。

请参见第 297 页的[“关于检测服务器策略执行”](#)。

表 18-2 添加策略规则

规则	先决条件	说明
内容		
内容匹配正则表达式		请参见第 453 页的 “关于正则表达式匹配” 。
内容匹配确切数据	确切数据配置文件	请参见第 356 页的 “关于实施确切数据匹配” 。 请参见第 326 页的 “选择确切数据配置文件” 。
内容匹配关键字		请参见第 445 页的 “关于实施关键字匹配” 。
内容匹配文档签名	已编制索引的文档配置文件	请参见第 377 页的 “关于实施索引文档匹配” 。 请参见第 327 页的 “选择索引文档配置文件” 。
内容匹配数据标识符	数据标识符	请参见第 414 页的 “关于数据标识符” 。 请参见第 430 页的 “选择系统数据标识符宽度” 。
文件属性		
邮件附件类型或文件类型匹配		请参见第 458 页的 “关于文件类型检测” 。
邮件附件大小或文件大小匹配		请参见第 459 页的 “关于文件大小检测” 。
邮件附件名或文件名匹配		请参见第 459 页的 “关于文件名检测” 。

规则	先决条件	说明
邮件/电子邮件属性和特性	Enterprise Vault 集成	有关更多信息, 请参见 <i>Enterprise Vault Data Classification Services Implementation Guide</i> (《Enterprise Vault 数据分类服务操作指南》)。
自定义文件类型签名	已启用规则 自定义脚本	请参见第 458 页的“ 关于自定义文件类型识别 ”。
“协议” 和端点		
协议监控	自定义协议 (如果有)	请参见第 465 页的“ 关于对网络进行的协议监控 ”。 请参见第 467 页的“ 关于移动的协议监控 ”。
端点监控		请参见第 470 页的“ 关于端点协议、目标和应用程序检测 ”。
端点设备类或 ID	自定义设备	请参见第 470 页的“ 关于端点设备检测 ”。
端点位置		请参见第 471 页的“ 关于端点位置检测 ”。
组 (身份)		
发送者/用户匹配模式 接受者匹配模式		请参见第 479 页的“ 关于指定身份匹配 ”。
发送者/用户基于目录服务器组匹配用户组 接受者基于目录服务器组匹配用户组	用户组	请参见第 485 页的“ 关于实施同步的目录组匹配 ”。 请参见第 487 页的“ 创建或修改用户组 ”。
基于本地目录的发送者/用户匹配用户组 基于本地目录的接收者匹配用户组	确切数据配置文件	请参见第 491 页的“ 关于实施配置的目录组匹配 ”。 请参见第 326 页的“ 选择确切数据配置文件 ”。

将一个或多个规则添加至策略中

1 选择要添加到策略的规则的类型（检测或组）。

要添加检测规则，请选择“检测”选项卡，然后单击“添加规则”。

要添加组（身份）规则，请选择“组”选项卡，然后单击“添加规则”。

请参见第 290 页的[“检测规则简介”](#)。

2 从规则列表中选择要实施的检测或组规则。

请参见第 332 页的[表 18-2](#)。

3 如果需要，请选择先决条件组件。

如果策略规则需要“数据配置文件”、“数据标识符”或“用户组”，请从列表中选择它。

4 单击“下一步”配置策略规则。

请参见第 334 页的[“配置策略规则”](#)。

注意：选择“例外”选项卡添加策略例外。请参见第 340 页的[“向策略中添加例外”](#)。

配置策略规则

在“管理”>“策略”>“策略列表”>“配置策略 - 编辑规则”屏幕上，使用一个或多个匹配条件配置策略规则。每个规则条件的配置取决于其类型。

请参见第 334 页的[表 18-3](#)。

表 18-3 配置策略规则条件

规则	说明
内容	
内容匹配正则表达式	请参见第 453 页的 “配置‘内容匹配正则表达式”条件” 。
内容匹配确切数据	请参见第 372 页的 “配置‘内容匹配确切数据”条件” 。
内容匹配关键字	请参见第 448 页的 “配置‘内容匹配关键字”条件” 。
内容匹配文档签名	请参见第 380 页的 “配置‘内容匹配文档签名”条件” 。
内容匹配数据标识符	请参见第 428 页的 “配置‘内容匹配数据标识符”条件” 。
文件属性	

规则	说明
邮件附件类型或文件类型匹配	请参见第 460 页的“ 配置“邮件附件类型或文件类型匹配”条件 ”。
邮件附件大小或文件大小匹配	请参见第 461 页的“ 配置“邮件附件大小或文件大小匹配”条件 ”。
邮件附件名或文件名匹配	请参见第 462 页的“ 配置“邮件附件名或文件名匹配”条件 ”。
电子邮件/MAPI 属性	有关更多信息，请参见 <i>Enterprise Vault Data Classification Services Implementation Guide</i> (《Enterprise Vault 数据分类服务操作指南》)。
自定义文件类型签名	请参见第 463 页的“ 配置自定义文件类型签名条件 ”。
协议和端点	
网络或移动监控	请参见第 466 页的“ 配置用于网络检测的“协议监控”条件 ”。
端点监控	请参见第 471 页的“ 配置端点监控条件参数 ”。
端点设备类或 ID	请参见第 476 页的“ 配置“端点设备类或 ID”条件 ”。
端点位置	请参见第 476 页的“ 配置“端点位置”条件 ”。
组(身份)	
发送者/用户匹配模式	请参见第 480 页的“ 配置“发送者/用户匹配模式”条件 ”。
接受者匹配模式	请参见第 482 页的“ 配置“接受者匹配模式”条件 ”。
发送者/用户基于目录服务器匹配用户组	请参见第 488 页的“ 配置“发送者/用户基于目录服务器匹配用户组”条件 ”。
接受者基于确切数据配置文件匹配用户组	请参见第 489 页的“ 配置“接受者基于目录服务器匹配用户组”条件 ”。
发送者/用户基于目录服务器匹配用户组	请参见第 493 页的“ 配置“发送者/用户匹配来自确切数据配置文件的目录”条件 ”。
接受者基于确切数据配置文件匹配用户组	请参见第 493 页的“ 配置“接受者匹配来自确切数据配置文件的目录”条件 ”。

表 18-4 配置策略规则

步骤	操作	说明
步骤 1	向策略添加规则或修改规则。	<p>请参见第 332 页的“将规则添加至策略中”。</p> <p>要修改现有规则，请在“配置策略 - 编辑规则”屏幕上的策略生成器界面中选择相应规则。</p>
步骤 2	命名规则或修改名称。	在规则“常规”部分的“规则名称”字段中输入名称，或者修改现有规则的名称。
步骤 3	设置规则严重性。	<p>在规则的“严重性”部分中，选择或修改“默认”严重性级别。</p> <p>除默认的严重性之外，还可以将多个严重性级别添加到规则。</p> <p>请参见第 337 页的“定义规则严重性”。</p>
步骤 4	配置匹配条件。	<p>在规则的“条件”部分中，为规则配置一个或多个匹配条件。条件的配置取决于其类型。</p> <p>请参见第 334 页的表 18-3。</p>
步骤 5	配置匹配计数（如果需要）。	<p>如果规则调用匹配计数，请配置您希望计算匹配数的方式。</p> <p>请参见第 337 页的“配置匹配计数”。</p>
步骤 6	选择组件以进行匹配（如果可用）。	<p>如果规则是基于内容的，请选择一个或多个可用内容规则进行匹配。</p> <p>请参见第 339 页的“选择匹配的组件”。</p>
步骤 7	添加并配置一个或多个其他匹配条件（可选）。	<p>要定义复合规则，请从“同时匹配”列表中“添加”其他匹配条件。</p> <p>根据条件类型（步骤 3）配置其他条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p> <p>注意：只有单个规则中的所有条件都匹配时才能触发事件。</p> <p>请参见第 297 页的“关于检测服务器策略执行”。</p>
步骤 8	保存策略配置。	<p>完成规则的配置后，单击“确定”。</p> <p>通过此操作可返回到“保存”策略的“配置策略”屏幕。</p> <p>请参见第 347 页的“管理和添加策略”。</p>

定义规则严重性

系统为策略规则违规分配严重性级别。默认设置为“高”。您可以配置默认设置，并添加一个或更多其他严重性级别。

请参见第 295 页的“[关于规则严重性](#)”。

策略规则严重性与“严重性”响应规则条件一起使用。如果将默认策略规则严重性级别设置为“高”并定义其他严重性级别，系统不会根据匹配数将其他严重性分配给该事件。结果就是，如果某响应规则的匹配数严重性等级设置为低于默认的“高”严重性，则不会执行该响应规则。

请参见第 681 页的“[配置“严重性”响应条件](#)”。

定义策略规则严重性

- 1 配置策略规则。

请参见第 334 页的“[配置策略规则](#)”。

- 2 从“严重性”列表中选择“默认”级别。

默认的严重性级别是系统报告的基线级别。除非其他严重性级别覆盖了默认设置，否则系统将对任何规则匹配应用默认的严重性级别。

- 3 单击“添加严重性”为规则定义其他严重性级别。

如果添加严重性级别，它将基于匹配数。

- 4 选择所需的严重性级别，选择匹配数范围并输入匹配数。

例如，您可以将 X 范围内的“中”严重性设置为在匹配数达到 100 后匹配。

- 5 如果添加其他严重性级别，您可以选择它作为默认的严重性。

- 6 要删除定义的严重性级别，请单击严重性定义旁边的 X 图标。

配置匹配计数

某些条件允许您指定希望计算匹配项的方式。计算所有匹配项是默认行为。您可以配置导致事件所需的最小匹配项数。或者，您可以将所有匹配项算作一个事件。如果条件支持匹配计数，则可以为策略规则和策略例外配置此设置。

请参见第 338 页的[表 18-6](#)。

表 18-5 配置匹配计数

参数	条件类型	事件说明
检查是否存在	简单	如果存在一个或多个匹配项，此配置会将匹配数报告为 1；它不计算多个匹配项。例如，10 个匹配项算作一个事件。
	复合	如果存在一个或多个匹配项，且规则或例外的所有条件都设置为“检查是否存在”，此配置会将匹配数报告为 1。
计算所有匹配项	简单	此配置报告的匹配数是由该条件检测的匹配项的确切数目。例如，10 个匹配项算作 10 个事件。
	复合	此配置报告的匹配数是规则或例外中的所有条件匹配项的总和。默认为每个条件匹配项作为一个事件，并且如果规则或例外的所有条件都设置为“计算所有匹配项”，则应用该默认设置。 例如，如果规则具有两个条件，一个条件设置为“计算所有匹配项”并检测到 4 个匹配项，另一个条件设置为“检查是否存在”并检测到 6 个匹配项，则报告的匹配数为 10。如果该规则的第三个条件检测到 1 个匹配项，则匹配数为 11。
仅报告至少具有 _ 个匹配项的事件		<p>您可以通过指定报告事件所需的最小匹配项数来更改默认的每个匹配项算作一个事件。</p> <p>例如，在具有两个条件的规则中，如果将一个条件配置为计算所有匹配项并为每个条件指定 5 作为最小匹配项数，如果两个条件生成两个事件，则报告 10 个匹配项的总和。必须保持一致并为规则或例外中的每个条件选择此选项，才能实现此行为。</p> <p>注意：“计算所有匹配项”设置适用于您匹配的每个邮件组件。例如，请考虑一个策略，其中指定匹配数为 3 并配置关键字规则与所有 4 个邮件组件匹配（此条件的默认设置）。如果收到的邮件在正文中有一个关键字实例且在信封中有一个关键字实例，则系统不会将此报告为匹配项。然而，如果三个关键字实例出现在附件中（或任何其他的单个邮件组件），则系统会将它报告为匹配项。</p>
对所有唯一匹配项进行计数	对唯一匹配项进行计数	<p>对唯一匹配项计数是 Symantec Data Loss Prevention 11.6 版的新功能，仅适用于数据标识符。</p> <p>请参见第 426 页的“关于数据标识符的唯一匹配项计数”。</p>

表 18-6 支持匹配计数的条件

条件	说明
内容匹配正则表达式	<p>请参见第 453 页的“关于正则表达式匹配”。</p> <p>请参见第 453 页的“配置“内容匹配正则表达式”条件”。</p>

条件	说明
内容匹配关键字	请参见第 445 页的“ 关于实施关键字匹配 ”。 请参见第 448 页的“ 配置“内容匹配关键字”条件 ”。
内容匹配文档签名 (IDM)	请参见第 377 页的“ 关于实施索引文档匹配 ”。 请参见第 380 页的“ 配置“内容匹配文档签名”条件 ”。
内容匹配数据标识符	请参见第 414 页的“ 关于数据标识符 ”。 请参见第 428 页的“ 配置“内容匹配数据标识符”条件 ”。 请参见第 436 页的“ 对数据标识符进行唯一匹配项计数 ”。
接受者匹配模式	请参见第 479 页的“ 关于指定身份匹配 ”。 请参见第 482 页的“ 配置“接受者匹配模式”条件 ”。

注意：确切数据匹配支持匹配计数，但它在“高级服务器设置”屏幕上进行配置。
请参见第 359 页的“[配置确切数据匹配计数](#)”。

选择匹配的组件

匹配的一个或多个邮件组件的可用性取决于您实施的规则或例外条件的类型。

请参见第 294 页的“[关于可以匹配的邮件组件](#)”。

表 18-7 匹配组件

组件	说明
信封	如果条件支持与“信封”组件匹配，则选择该条件以与邮件元数据匹配。如果邮件是 SMTP 电子邮件，则信封包含标题、传输信息和主题。 如果条件不支持与“信封”组件匹配，则此选项显示为灰色。 如果条件与整个邮件匹配，则选择“信封”且无法对其取消选择，并且无法选择其他组件。

组件	说明
主题	<p>某些检测条件与某些类型的邮件的“主题”组件匹配。</p> <p>请参见第 294 页的“关于可以匹配的邮件组件”。</p> <p>对于支持主题组件匹配的检测条件，您可以与下列类型的邮件的“主题”匹配：</p> <ul style="list-style-type: none"> ■ 来自 Network Monitor 或 Network Prevent for Email 的 SMTP（电子邮件）邮件。 ■ 来自 Network Monitor 的 NNTP 邮件。 ■ 由分类服务器传递的 Exchange 电子邮件。 <p>有关更多信息，请参见 <i>Enterprise Vault Data Classification Services Implementation Guide</i>（《Enterprise Vault 数据分类服务操作指南》）。</p> <p>要与“主题”组件匹配，您必须针对策略规则选择（选中）“主题”组件并取消选中（取消选择）“信封”组件。如果选择这两个组件，系统将与主题进行两次匹配，因为邮件主题作为标题的一部分包含在信封中。</p>
正文	如果条件与“正文”邮件组件匹配，则选择该条件以与邮件的文本或内容匹配。
附件	如果条件与“附件”邮件组件匹配，则选择该条件以检测通过邮件发送、下载或附加到邮件中的文件的内容。

向策略中添加例外

在“管理”>“策略”>“策略列表”>“配置策略 - 添加例外”屏幕中，可以向策略中添加一个或多个例外。如果策略与例外匹配，则检测引擎不会触发事件。

请参见第 296 页的[“关于规则例外”](#)。

可以向策略中添加一个或多个检测或组例外。策略例外在策略规则之前执行。

请参见第 297 页的[“关于检测服务器策略执行”](#)。

注意：可以为所有策略规则创建例外，但那些实施确切数据匹配的策略规则除外。

表 18-8 选择策略例外

例外	先决条件	说明
内容		
内容匹配正则表达式		请参见第 453 页的 “关于正则表达式匹配” 。
内容匹配关键字		请参见第 445 页的 “关于实施关键字匹配” 。

例外	先决条件	说明
内容匹配文档签名	已编制索引的文档配置文件	<p>请参见第 377 页的“关于实施索引文档匹配”。</p> <p>请参见第 327 页的“选择索引文档配置文件”。</p>
内容匹配数据标识符	数据标识符	<p>请参见第 414 页的“关于数据标识符”。</p> <p>请参见第 430 页的“选择系统数据标识符宽度”。</p>
文件属性		
邮件附件类型或文件类型匹配		请参见第 458 页的“ 关于文件类型检测 ”。
邮件附件大小或文件大小匹配		请参见第 459 页的“ 关于文件大小检测 ”。
邮件附件名或文件名匹配		请参见第 459 页的“ 关于文件名检测 ”。
邮件/电子邮件属性和特性	Enterprise Vault 集成	有关更多信息，请参见 <i>Enterprise Vault Data Classification Services Implementation Guide</i> (《Enterprise Vault 数据分类服务操作指南》)。
自定义文件类型签名	已启用例外 自定义脚本	请参见第 458 页的“ 关于自定义文件类型识别 ”。
协议和端点		
网络或移动协议		<p>请参见第 465 页的“关于对网络进行的协议监控”。</p> <p>请参见第 467 页的“关于移动的协议监控”。</p>
端点协议、目标、应用程序		请参见第 470 页的“ 关于端点协议、目标和应用程序检测 ”。
端点设备类或 ID		请参见第 470 页的“ 关于端点设备检测 ”。
端点位置		请参见第 471 页的“ 关于端点位置检测 ”。
组(身份)		
发送者/用户匹配模式 接受者匹配模式		请参见第 479 页的“ 关于指定身份匹配 ”。
发送者/用户基于目录服务器匹配 用户组 接受者基于目录服务器匹配用户组	用户组	<p>请参见第 485 页的“关于实施同步的目录组匹配”。</p> <p>请参见第 487 页的“创建或修改用户组”。</p>

向策略中添加例外

1 向策略中添加例外。

要添加检测规则例外，请选择“检测”选项卡，然后单击“添加例外”。

要添加组规则例外，请选择“组”选项卡，然后单击“添加例外”。

2 选择要实施的策略例外。

“添加检测例外”屏幕会列出可添加至策略的所有可用检测例外。

“添加组例外”屏幕会列出可添加至策略的所有可用组例外。

请参见第 340 页的[表 18-8](#)。

3 如果需要，请选择配置文件、数据标识符或用户组。

4 单击“下一步”配置例外。

请参见第 342 页的[“配置策略例外”](#)。

配置策略例外

在“管理”>“策略”>“策略列表”>“配置策略 - 编辑例外”屏幕中，可以为策略例外配置一个或多个条件。

请参见第 342 页的[表 18-9](#)。

如果与某个例外条件匹配，系统将丢弃系统中匹配的组件。此组件对于评估将不再可用。

请参见第 296 页的[“关于规则例外”](#)。

表 18-9 配置策略例外条件

例外	说明
内容	
内容匹配正则表达式	请参见第 453 页的 “配置“内容匹配正则表达式”条件” 。
内容匹配关键字	请参见第 448 页的 “配置“内容匹配关键字”条件” 。
内容匹配文档签名	请参见第 380 页的 “配置“内容匹配文档签名”条件” 。
内容匹配数据标识符	请参见第 428 页的 “配置“内容匹配数据标识符”条件” 。
文件属性	
邮件附件类型或文件类型匹配	请参见第 460 页的 “配置“邮件附件类型或文件类型匹配”条件” 。

例外	说明
邮件附件大小或文件大小匹配	请参见第 461 页的“配置“邮件附件大小或文件大小匹配”条件”。
邮件附件名或文件名匹配	请参见第 462 页的“配置“邮件附件名或文件名匹配”条件”。
电子邮件/MAPI 属性	有关更多信息，请参见 <i>Enterprise Vault Data Classification Services Implementation Guide</i> （《Enterprise Vault 数据分类服务操作指南》）。
自定义文件类型签名	请参见第 463 页的“配置自定义文件类型签名条件”。
协议和端点	
网络或移动协议	请参见第 466 页的“配置用于网络检测的“协议监控”条件”。
端点协议或目标	请参见第 471 页的“配置端点监控条件参数”。
端点设备类或 ID	请参见第 476 页的“配置“端点设备类或 ID”条件”。
端点位置	请参见第 476 页的“配置“端点位置”条件”。
组(身份)	
发送者/用户匹配模式	请参见第 480 页的“配置“发送者/用户匹配模式”条件”。
接受者匹配模式	请参见第 482 页的“配置“接受者匹配模式”条件”。
基于目录服务器的发送者/用户匹配用户组	请参见第 488 页的“配置“发送者/用户基于目录服务器匹配用户组”条件”。
基于目录服务器的接受者匹配用户组	请参见第 493 页的“配置“发送者/用户匹配来自确切数据配置文件的目录”条件”。

表 18-10 配置策略例外

步骤	操作	说明
步骤 1	添加新的策略例外或编辑现有例外。	请参见第 340 页的“向策略中添加例外”。 选择要修改的现有策略例外。
步骤 2	对该例外进行命名或编辑现有名称或说明。	在“常规”部分中，输入例外的唯一名称或修改现有例外的名称。 注意： 此例外名称不能超过 60 个字符。

步骤	操作	说明
步骤 3	选择要应用例外的组件（如果可用）。	<p>如果例外基于内容，则可以与整个邮件或各个邮件组件匹配。</p> <p>请参见第 294 页的“关于可以匹配的邮件组件”。</p> <p>选择其中一个“将例外应用于”选项：</p> <ul style="list-style-type: none"> ■ 整个消息 此选项可将例外应用于整个邮件。 ■ 仅限匹配的部分 此选项可将例外应用于从例外的“条件”部分的“匹配位置”选项中选择的每个邮件组件。
步骤 4	配置例外条件。	<p>在“配置策略 - 编辑例外”屏幕的“条件”部分中，定义策略例外的条件。条件的配置取决于例外类型。</p> <p>请参见第 342 页的表 18-9。</p>
步骤 5	将一个或多个附加条件添加到例外（可选）。	<p>您可以添加条件，直至根据要求完成例外的构建。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p> <p>要将其他条件添加到例外，请从“同时匹配”列表中选择条件。</p> <p>单击“添加”并配置条件。</p>
步骤 6	保存并管理策略。	<p>单击“确定”完成例外的定义过程。</p> <p>单击“保存”保存该策略。</p> <p>请参见第 347 页的“管理和添加策略”。</p>

配置复合匹配条件

您可以为策略规则和例外创建复合匹配条件。

请参见第 344 页的“[配置复合匹配条件](#)”。

检测引擎使用 AND 连接复合条件。只有符合规则或例外中的所有条件才会触发或排除事件。

请参见第 297 页的“[关于检测服务器策略执行](#)”。

规则或例外中可以包括的匹配条件的数量没有限制。然而，在一个规则或例外中声明的多个条件在逻辑上应该是关联的。不要将复合规则或例外与一个策略中的多个规则或例外混淆。

表 18-11 配置复合策略规则或例外

步骤	操作	说明
步骤 1	修改或配置现有策略规则或例外。	<p>您可以在“配置策略-编辑规则”屏幕上将一个或多个其他匹配条件添加到某个策略规则中。</p> <p>您可以在“配置策略-编辑规则”或“配置策略-编辑例外”屏幕上将一个或多个其他匹配条件添加到某个规则或例外中。</p>
步骤 2	选择一个其他匹配条件。	<p>从“同时匹配”列表中选择其他匹配条件。</p> <p>此列表显示在现有规则或例外的“条件”部分底部。</p>
步骤 3	查看可用条件。	<p>系统列出了所有您可以添加到策略规则或例外中的其他可用条件。</p> <p>请参见第 332 页的“将规则添加至策略中”。</p> <p>请参见第 340 页的“向策略中添加例外”。</p>
步骤 4	添加其他条件。	<p>单击“添加”可将其他匹配条件添加到策略规则或例外中。</p> <p>添加后，您可以折叠和展开规则或例外中的每个条件。</p>
步骤 5	配置其他条件。	<p>请参见第 334 页的“配置策略规则”。</p> <p>请参见第 342 页的“配置策略例外”。</p>
步骤 6	选择要进行匹配的同一组件或任何组件。	<p>如果条件支持组件匹配，请指定必须匹配数据的组件，以生成或排除事件。</p> <p>“同一组件” - 匹配的数据必须与同样支持组件匹配的其他条件位于同一组件中才能触发匹配。</p> <p>“任何组件” - 匹配的数据可以位于您选择的任何组件中。</p> <p>请参见第 419 页的“关于数据标识符的跨组件匹配”。</p>
步骤 6	对规则或例外中的其他匹配条件重复此过程。	<p>您可以根据需要向规则或例外中添加任意数量的条件。</p> <p>必须符合一个规则或例外中的所有条件才能触发事件或触发例外。</p>
步骤 7	保存策略。	<p>单击“确定”以关闭规则或例外配置屏幕。</p> <p>单击“保存”以保存策略配置。</p>

管理策略

本章节包括下列主题：

- 管理和添加策略
- 创建和修改策略组
- 管理和添加策略组
- 导入策略模板
- 将策略检测导出为模板
- 将 10 版数据标识符或关键字策略导入 11 版系统
- 向策略添加自动响应规则
- 关于删除策略和策略组

管理和添加策略

通过实施策略可以检测和报告数据丢失。“管理”>“策略”>“策略列表”屏幕是添加和管理策略的主页。

请参见第 314 页的“[实施策略](#)”。

表 19-1 “策略列表” 屏幕中可执行的操作

操作	说明
添加策略	单击“添加策略”创建新的策略。 请参见第 329 页的“ 添加新的策略或策略模板 ”。
修改策略	单击策略对应行的任意位置可修改现有策略。 请参见第 330 页的“ 配置策略 ”。

操作	说明
激活策略	单击策略名称旁边的红色圆圈图标可激活该策略。
挂起策略	单击策略名称旁边的绿色圆圈图标。 注意： 默认情况下，安装解决方案包时所有解决方案包策略均已激活。
对策略排序	单击任意“列标题”对策略列表进行排序。
删除策略	单击位于策略对应行的末尾处的红色X图标。经过确认后，系统会删除该策略。 注意： 无法删除具有活动事件的策略。 请参见第 353 页的 “关于删除策略和策略组” 。
导出和导入策略模板	请参见第 351 页的 “导入策略模板” 。 请参见第 351 页的 “将策略检测导出为模板” 。

表 19-2 “策略列表” 屏幕中显示的字段

列	说明
名称	按策略的名称进行查看和排序。 请参见第 305 页的 “关于策略” 。
说明	查看策略的说明。 请参见第 308 页的 “关于系统定义的策略模板” 。
策略组	按策略部署到的策略组进行查看和排序。 请参见第 309 页的 “关于策略组” 。
上次修改时间	按上次更新策略的日期进行查看和排序。 请参见第 310 页的 “关于策略创建权限” 。
配置错误的策略	策略图标为黄色警告符号。 请参见第 306 页的 “关于策略组件” 。
活动策略	策略图标为绿色。活动策略可以检测事件。
挂起策略	策略图标为红色。可以部署挂起策略，但不能用于检测事件。

创建和修改策略组

在“系统”>“服务器”>“策略组”屏幕上，可以配置新的策略组或修改现有策略组。

请参见第 309 页的[“关于策略组”](#)。

配置策略组

- 1 添加新的策略组或修改现有策略组。

请参见第 350 页的[“管理和添加策略组”](#)。

- 2 输入策略组的“名称”或者修改现有名称。

使用一个信息比较丰富的名称。策略作者和 Enforce Server 管理员在将策略组与策略、角色和目标关联时会依赖于策略组名称。

该名称的值不能超过 256 个字符。

- 3 输入策略组的“说明”，或修改现有策略组的现有说明。

- 4 选择一个或多个要将策略组分配到的“服务器”。

系统会为当前使用 Enforce Server 配置和注册的每个检测服务器显示一个复选框。

■ 选择（选中）“所有服务器”选项，将策略组分配到系统中的所有检测服务器。如果不选中此复选框，可将策略组分配到各个服务器。

“所有发现服务器”条目是不可配置的，因为系统会自动将所有策略组分配到所有 Network Discover Server。该功能可让您将策略组分配给各发现目标。

请参见第 930 页的[“为 Network Discover 目标配置必填字段”](#)。

■ 取消选择（取消选中）“所有服务器”选项，将策略组分配到各个检测服务器。

系统会为当前使用 Enforce Server 配置和注册的每个服务器显示一个复选框。

选择各个检测服务器以分配策略组。

- 5 单击“保存”保存策略组配置。

注意：“策略组”屏幕的“此组中的策略”部分列出了策略组中的所有策略。您无法编辑这些条目。当创建新策略组时，此部分为空白。在您将一个或多个策略部署到策略组（策略配置期间）后，“此组中的策略”部分会显示策略组中的每个策略。

请参见第 330 页的[“配置策略”](#)。

请参见第 310 页的“[关于策略部署](#)”。

管理和添加策略组

“系统” > “服务器” > “策略组” 屏幕会列出系统中已配置的策略组。

在 “策略组” 屏幕中，可以管理现有策略组以及添加新的策略组。

表 19-3 “策略组” 屏幕中的操作

操作	说明
添加策略组	单击 “添加策略组” 以定义新的策略组。 请参见第 309 页的“ 关于策略组 ”。
修改策略组	要修改现有策略组，请单击该组的名称，或者单击对应行最右端的铅笔图标。 请参见第 349 页的“ 创建和修改策略组 ”。
删除策略组	单击对应行最右端的红色 X 图标，以从系统中删除该策略组。完成确认删除的对话框。 注意： 如果删除某个策略组，则会删除为该组分配的所有策略。 请参见第 353 页的“ 关于删除策略和策略组 ”。
查看组中的策略	要查看部署到现有策略组中的策略，请导航至 “系统” > “服务器” > “策略组” > “配置策略组” 屏幕。 请参见第 349 页的“ 创建和修改策略组 ”。

表 19-4 “策略组” 屏幕中的显示字段

列	说明
名称	策略组的名称。
说明	策略组的说明。
可用服务器	部署策略组的检测服务器。 请参见第 310 页的“ 关于策略部署 ”。
上次修改时间	策略组的上次修改时间。

导入策略模板

可将一个或多个策略模板导入到 Enforce Server。您必须具有策略系统权限才能导入策略模板。

请参见第 311 页的“[关于策略模板导入和导出](#)”。

将一个或多个策略模板导入到 Enforce Server

- 1 将一个或多个策略模板 XML 文件放置到 Enforce Server 主机的 \\Vontu\\Protect\\config\\templates 目录中。

可通过将多个策略放置在模板目录中来导入这些策略。
- 2 确保 protect 系统用户可读取目录和文件。
- 3 使用策略创建权限登录到 Enforce Server 管理控制台。
- 4 导航至“管理”>“策略”>“策略列表”，然后单击“添加策略”。
- 5 选择选项“从模板添加策略”，然后单击“下一步”。
- 6 在“导入的模板”部分中，向下滚动至模板列表的底部。

可看到您在模板目录中放置的每个 XML 文件的条目。
- 7 选择导入的策略模板，然后单击“下一步”对其进行配置。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

请参见第 352 页的“[将 10 版数据标识符或关键字策略导入 11 版系统](#)”。

将策略检测导出为模板

可以将策略检测规则和例外导出到某个模板（XML文件）。但无法导出策略响应规则。一次只能导出一个策略模板。

请参见第 311 页的“[关于策略模板导入和导出](#)”。

将策略导出为模板

- 1 使用管理员权限登录到 Enforce Server 管理控制台。
- 2 导航到“管理”>“策略”>“策略列表”>“配置策略”屏幕以查找要导出的策略。
- 3 在“配置策略”屏幕的底部，单击“将此策略导出为模板”链接。
- 4 将策略保存到所选的本地或网络目标中。

例如，系统将名为 **Webmail** 的策略保存到策略模板文件 **Webmail.xml**，您可以将该文件保存到本地驱动器。

请参见第 351 页的“[导入策略模板](#)”。

请参见第 352 页的“[将 10 版数据标识符或关键字策略导入 11 版系统](#)”。

将 10 版数据标识符或关键字策略导入 11 版系统

Symantec Data Loss Prevention 11 版实施了针对数据标识符和关键字匹配检测规则的关键增强功能。这些更改不向前兼容。因此，您不能从 10 版系统导出关键字或数据标识符策略并将其导入 11 版系统，并假设策略会按预期运作。

如果您具有的 10 版策略仅包含关键字或数据标识符规则，则必须在 11 版系统上重建整个策略。如果您具有的 10 版策略包含关键字或数据标识符规则以及其他类型的规则，则可以使用以下解决方法。

注意：此情形不适用于系统升级。升级到 11 版的 10 版系统上的所有策略将自动升级，无需手动重建。请参阅《Symantec Data Loss Prevention 升级指南》，了解关于升级版本的详细信息。

将 10 版数据标识符或关键字策略模板导入 11 版系统

1 在 v10 系统上，按原样导出策略。

为其提供恰当的命名，如 **Original**。

请参见第 311 页的“[关于策略模板导入和导出](#)”。

2 使用 10 版策略生成器界面从策略中删除任何关键字和数据标识符条件。

将策略重名为 **Modified**。

3 通过 10 版系统将 **Modified** 策略导出为模板。

请参见第 351 页的“[将策略检测导出为模板](#)”。

4 将 **Modified** 策略模板导入 11 版 Enforce Server。

请参见第 351 页的“[导入策略模板](#)”。

5 重建已从策略中删除的关键字或数据标识符条件。

请参见第 330 页的“[配置策略](#)”。

向策略添加自动响应规则

可以向策略添加一个或多个自动响应规则，以便在违反策略时执行操作。

请参见第 653 页的“[关于响应规则](#)”。

注意：智能响应规则手动执行且未部署到策略之中。

向策略添加自动响应规则

- 1 使用策略创建权限登录到 Enforce Server 管理控制台。
请参见第 310 页的“[关于策略创建权限](#)”。
- 2 导航到“管理”>“策略”>“策略列表”>“配置策略”屏幕以查找要向其添加响应规则的策略。
- 3 从下拉菜单中可用的响应规则中选择要添加的响应规则。
策略和响应规则是分别配置的。要向策略添加响应规则，必须首先定义并单独保存响应规则。
请参见第 664 页的“[实施响应规则](#)”。
- 4 单击“添加响应规则”向策略添加响应规则。
- 5 重复该过程，向策略添加其他响应规则。
- 6 在添加完响应规则后，“保存”策略。
- 7 向策略添加响应规则后，验证策略状态是否为绿色。
请参见第 347 页的“[管理和添加策略](#)”。

注意：如果策略状态为黄色警告符号，则表明未正确配置策略。系统不支持某些响应规则操作 - 策略检测规则或例外对。请参见第 1137 页的[表 74-2](#)。

关于删除策略和策略组

在从 Enforce Server 中删除策略或策略组之前，请考虑以下准则。

表 19-5 **删除策略和策略组的准则**

操作	说明	准则
删除策略	如果尝试删除具有关联事件的策略，系统将不允许删除该策略。	如果要删除某个策略，必须首先从 Enforce Server 中删除所有与该策略关联的事件。 请参见第 347 页的“ 管理和添加策略 ”。 一种替代方法是创建一个未部署的策略组（即未分配给任何检测服务器的策略组）。在维护旧版策略和事件时，此方法会非常有用，可以不必在已部署的策略组中保持这些策略即可进行查看。 请参见第 311 页的“ 关于策略模板导入和导出 ”。

操作	说明	准则
删除策略组	如果尝试删除包含一个或多个策略的策略组，系统将显示错误消息。并且，无法删除该策略组。	<p>在删除策略组之前，可通过删除该组中的所有策略或将策略分配到其他策略组来删除该策略组中的所有策略。</p> <p>请参见第 350 页的“管理和添加策略组”。</p> <p>如果要删除策略组，请先创建维护策略组，然后将要删除的策略移动到该维护组。</p> <p>请参见第 349 页的“创建和修改策略组”。</p>

请参见第 305 页的“[关于策略](#)”。

请参见第 309 页的“[关于策略组](#)”。

使用确切数据匹配来检测内容

本章节包括下列主题：

- [关于实施确切数据匹配](#)
- [实施确切数据匹配](#)
- [关于数据所有者例外](#)
- [关于字段映射](#)
- [关于索引调度](#)
- [配置确切数据匹配计数](#)
- [管理并添加确切数据配置文件](#)
- [创建确切数据源文件](#)
- [迁移旧有数据所有者例外配置](#)
- [为编制索引准备确切数据源文件](#)
- [将确切数据源文件上传到 Enforce Server](#)
- [创建和修改确切数据配置文件](#)
- [映射确切数据配置文件字段](#)
- [调度确切数据配置文件索引编制](#)
- [配置“内容匹配确切数据”条件](#)
- [EDM 最佳做法](#)

关于实施确切数据匹配

要准确的检测数据，Symantec Data Loss Prevention 需要一个特殊的索引版本数据。索引是一个安全的文件（或一组文件）。它包括了数据源中每个字段的确切数据值的哈希，以及这些数据值的相关信息。索引不包括数据值本身，因此是安全的。

请参见第 286 页的“[关于确切数据匹配](#)”。

索引由一个或多个安全的二进制.rdx 文件组成，每个文件的大小都可容纳于检测服务器上的随机存取内存 (RAM)。对于大型数据源文件，Symantec Data Loss Prevention 可能会将数据分成多个.rdx 文件。在实际运行时，系统会使用应用于索引的相同算法，将输入内容转换成哈希数据值。然后对来自输入内容的数据值和适当.rdx 文件中的数据值进行比较，以识别匹配项。

默认情况下，在 Enforce Server 和所有检测服务器上，Symantec Data Loss Prevention 会在 C:\Vontu\Protect\index (Windows 上) 或 /var/Vontu/index (Linux 上) 中存储索引文件。当策略处于活动状态时，Symantec Data Loss Prevention 会将索引部署到检测服务器，而检测服务器会将索引加载到 RAM。

请参见第 356 页的“[实施确切数据匹配](#)”。

实施确切数据匹配

要实施EDM，请创建确切数据配置文件，编制数据源索引，并定义一个或多个EDM 检测规则以完全匹配已配置的数据。

表 20-1 实施确切数据匹配

步骤	操作	说明
1	创建数据源文件。	将源数据从数据库（或其他数据存储库）导出到表式文本文件。 请参见第 357 页的“ 关于数据所有者例外 ”。 如果要从匹配中排除数据所有者，则需要在数据源文件中包括特定的数据项。 请参见第 491 页的“ 关于实施配置的目录组匹配 ”。 如果要匹配已配置的目录组匹配(DGM)的标识，则需要在数据源文件中包括特定的数据项。
2	准备好要编制索引的数据源文件。	从数据源文件中删除不规则情况。 请参见第 363 页的“ 为编制索引准备确切数据源文件 ”。

步骤	操作	说明
3	将数据源文件上传到 Enforce Server。	可以将数据源文件复制或上传到 Enforce Server，或者对其进行远程访问。 请参见第 364 页的“ 将确切数据源文件上传到 Enforce Server ”。
4	创建确切数据配置文件。	“确切数据配置文件”指定数据源、索引编制参数及索引编制日程表。 请参见第 365 页的“ 创建和修改确切数据配置文件 ”。
5	映射数据字段。	将源数据字段映射到系统数据类型或系统验证的自定义数据类型。例如，社会安全号数据字段要有九个数字。 请参见第 358 页的“ 关于字段映射 ”。 请参见第 369 页的“ 映射确切数据配置文件字段 ”。
6	编制数据源索引，或调度索引编制。	请参见第 358 页的“ 关于索引调度 ”。 请参见第 371 页的“ 调度确切数据配置文件索引编制 ”。
7	配置并调整一个或多个 EDM 检测条件。	请参见第 372 页的“ 配置“内容匹配确切数据”条件 ”。 请参见第 359 页的“ 配置确切数据匹配计数 ”。

关于数据所有者例外

使用数据所有者例外 (DOE) 功能，数据所有者可以发送或接收其自己的、原本会被系统阻止传递或接收的数据。

要实现数据所有者例外功能，您必须在数据源文件中包含以下两个字段或其中之一：

- 电子邮件地址
- 域地址

注意：要实施 DOE 并将数据所有者排除在检测之外，必须在数据配置文件中显示加入每个用户的电子邮件地址或域地址。必须将每个预期域（例如，**symantec.com**）显示添加到数据配置文件。系统不会自动匹配子域（例如，**fileconnect.symantec.com**）。必须将每个子域显示添加到数据配置文件。

配置包括这些数据元素之一的确切数据配置文件后，您可以将任一字段标记为数据所有者。在运行时，如果数据的发送者或接受者为所有者，该状况不会触发匹配。其结果是数据将被传递或接收。

请参见第 372 页的“[配置“内容匹配确切数据”条件](#)”。

如果您以前使用配置文件手动实现了 DOE，则必须重新配置这些例外，以使其在最新的 Enforce Server 上运行。

请参见第 362 页的“[迁移旧有数据所有者例外配置](#)”。

关于字段映射

数据源中的列标题对于视觉参考很有帮助。但是，它们不会告知 Symantec Data Loss Prevention 列中包含哪种数据。使用“添加确切数据配置文件”屏幕的“字段映射”部分可以指定数据源中字段之间的映射。也可以使用此屏幕指定 Symantec Data Loss Prevention 在其策略模板中识别的字段。“字段映射”部分还提供了用于指定自定义字段的高级选项。

以下是一个字段映射的使用示例。公司想要保护包括员工社会安全号在内的员工数据。您可以基于“员工数据保护”模板创建一项策略。该策略需要带有社会安全号和其他员工数据字段的确切数据索引。准备数据源，然后创建确切数据配置文件。指定数据源中的社会安全号字段映射到策略模板的“社会安全号”系统字段。

请参见第 369 页的“[映射确切数据配置文件字段](#)”。

关于索引调度

配置确切数据配置文件时，可以设置对数据源编制索引的日程表。

设置日程表之前，请注意下列事项：

- 如果只是偶尔更新数据源（如频率低于每月一次），则不需要创建日程表。可在每次更新数据源时编制数据索引。
- 将编制索引时间调度到系统使用率最低的时段。编制索引会影响整个 Symantec Data Loss Prevention 系统的性能，并且大型数据源的索引编制可能会花费较长时间。
- 添加或修改确切数据配置文件后立即对相应的数据源编制索引，无论何时更新数据源都重新编制数据源索引。例如，考虑在每个星期三的凌晨 2:00 更新数据源的情景。在这种情况下，您应调度在每个星期三的凌晨 3:00 编制索引。不要每天都对数据源编制索引，这会降低性能。
- 监视结果并相应修改索引编制日程表。例如，如果性能良好，而您希望更新更加及时，可以调度更频繁的数据更新和索引编制活动。

请参见第 356 页的“[实施确切数据匹配](#)”。

配置确切数据匹配计数

通过调整检测服务器的 EDM.MatchCountVariant 设置，您可以配置如何对 EDM 匹配项计数。

请参见第 195 页的“[高级服务器设置](#)”。

以具有下列三条记录的数据库配置文件为例：

- Kathy, Stevens, 123-45-6789, 1111-1111-1111-1111
- Kathy, Stevens, 123-45-6789, 2222-2222-2222-2222
- Kathy, Stevens, 123-45-6789, 3333-3333-3333-3333

如果将策略规则设为匹配 4 个中的任意 3 个，并且某人发送具有以下一行内容的邮件：

- Kathy, Stevens, 123-45-6789

按以下方式对匹配项进行计数：

- EDM.MatchCountVariant=1: 3 (数据库配置文件记录匹配项的数量)
- EDM.MatchCountVariant=2: 1 (唯一令牌组匹配项的数量)
- EDM.MatchCountVariant=3: 1 (包括令牌组匹配项的数量)

如果某人发送具有以下 2 行内容的邮件：

- Kathy, Stevens, 123-45-6789, 1111-1111-1111-1111
- Kathy, Stevens, 123-45-6789

则按以下方式对匹配项进行计数：

- EDM.MatchCountVariant=1: 3 (数据库配置文件记录匹配项的数量)
- EDM.MatchCountVariant=2: 2 (唯一令牌组匹配项的数量)
- EDM.MatchCountVariant=3: 1 (包括令牌组匹配项的数量，第一个令牌组包括第二个令牌组)。

请参见第 356 页的“[实施确切数据匹配](#)”。

管理并添加确切数据配置文件

“管理” > “数据配置文件” > “确切数据” 屏幕列出了系统中配置的所有确切数据配置文件。实施确切数据匹配 (EDM) 策略要求有确切数据配置文件。

请参见第 312 页的“[关于数据配置文件](#)”。

可以从“确切数据”屏幕管理现有配置文件并添加新的配置文件。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

表 20-2 确切数据屏幕操作

操作	说明
添加 EDM 配置文件	单击“添加确切数据配置文件”可以定义新的确切数据配置文件。 请参见第 356 页的“ 实施确切数据匹配 ”。
编辑 EDM 配置文件	要修改现有“确切数据配置文件”，可单击该配置文件的名称，或者单击配置文件行最右端的铅笔图标。 请参见第 365 页的“ 创建和修改确切数据配置文件 ”。
删除 EDM 配置文件	单击配置文件行最右端的红色 X 图标，以从系统中删除确切数据配置文件。完成确认删除的对话框。 注意： 以下情况下无法编辑或删除配置文件：当前其他用户正修改该配置文件，或存在依赖于该配置文件的策略。
下载 EDM 配置文件	单击“下载配置文件”链接以下载并保存确切数据配置文件。 这对于在多个环境中存档和共享配置文件很有用。文件采用二进制 *.edm 格式。
刷新 EDM 配置文件状态	单击“确切数据”屏幕右上方的刷新箭头图标，以获取索引编制进程的最新状态。 如果您正在编制索引，则系统会显示消息“正在启动编制索引...”。系统不会在编制索引过程完成时自动刷新屏幕。

表 20-3 确切数据屏幕详细信息

列	说明
确切数据配置文件	确切数据配置文件的名称。
上一个活动版本	确切数据配置文件的版本和运行该配置文件的检测服务器的名称。

列	说明
状态	<p>确切数据配置文件的当前状态，可以是以下任何状态：</p> <ul style="list-style-type: none">■ 下次调度索引编制（如果当前未编制索引）■ 正在将索引发送给检测服务器■ 正在编制索引■ 正在部署到服务器
	<p>此外，还包括每个检测服务器的索引编制过程的当前状态，可以是以下任何状态：</p> <ul style="list-style-type: none">■ 已完成，包括完成日期■ 挂起的索引完成（正在等待 Enforce Server 完成对确切数据源文件编制索引）■ 正在复制索引编制■ 正在创建索引（内部）■ 正在构建缓存
错误消息	<p>“确切数据”屏幕以红色显示所有错误消息。</p> <p>例如，如果确切数据配置文件已损坏或不存在，系统将显示错误消息。</p>

请参见第 372 页的[“配置“内容匹配确切数据”条件”](#)。

创建确切数据源文件

EDM 索引编制过程的第一步是创建数据源。数据源是一个包含标准分隔格式的数据的平面文件。

如果您计划使用策略模板，请在创建数据源文件之前检查该模板，以了解策略将使用哪些数据字段。对于相对较小的数据源，请在数据源中包括尽可能多的建议字段。但要注意，包括的字段越多，生成的索引所占的内存越大。如果有大型数据源，务必要考虑到此问题。创建数据配置文件时，您可以确认数据源中的字段与模板的建议字段之间的匹配程度。

表 20-4 创建确切数据源文件

步骤	说明
1	<p>将希望保护的数据从数据库或其他表式数据格式（如 Excel 电子表格）导出到文件中。所创建的数据源文件必须是表式文本文件，并且包含来自原始源的数据行。来自原始源的每一行都会作为数据源文件中的一行。可使用 Tab、逗号或竖线分隔多个列。</p> <p>必须将从源数据库表或类似于表的格式中导出的所有结构化数据保留在一个数据源文件中。您不能将数据源拆分为多个文件。</p> <p>数据源文件不得超过 21 亿个单元格。除此之外，数据源的大小仅受 Enforce Server 主机上可用磁盘空间大小的限制。如果您计划将数据源上传到 Enforce Server，则浏览器容量会将数据源大小限制为 2GB。对于超过此大小的文件，可以使用 FTP/S 将文件复制到 Enforce Server。</p>
2	<p>包括特定 EDM 实现的必需数据字段：</p> <ul style="list-style-type: none"> ■ 数据所有者例外 请参见第 357 页的“关于数据所有者例外”。 ■ 目录组匹配 请参见第 492 页的“为 DGM 创建确切数据配置文件”。 ■ 关键字字典
3	<p>准备好要编制索引的数据源文件。</p> <p>请参见第 363 页的“为编制索引准备确切数据源文件”。</p>

迁移旧有数据所有者例外配置

在 Symantec Data Loss Prevention 的早期版本中，数据所有者例外功能是使用配置文件实现的。如果您之前使用配置文件实现数据所有者例外，则需要将这些例外迁移到当前的 Enforce Server 版本中。另外，您必须删除系统中的所有早期数据所有者例外配置文件。

请参见第 357 页的“[关于数据所有者例外](#)”。

迁移旧有数据所有者例外配置

- 1 删除或注释掉以下配置文件中所有的旧有数据所有者例外条目：

`\Vontu\protect\config\ownerexception.properties`

- 2 创建确切数据配置文件时，使用 Enforce Server 管理控制台映射数据所有者例外字段。

请参见第 365 页的“[创建和修改确切数据配置文件](#)”。

- 3 在一个或多个策略中手动配置旧有数据所有者例外。

请参见第 372 页的“[配置“内容匹配确切数据”条件](#)”。

为编制索引准备确切数据源文件

创建了确切数据源文件后，您必须对其进行准备以便可以有效地对要保护的数据编制索引。

对确切数据配置文件编制索引时，Enforce Server 会记录视为错误的空单元格和所有放置错误的数据。例如，可能的错误包括名称显示在电话号码列中。错误可在配置文件的数据中占一定的百分比（默认情况下为百分之五）。如果满足此默认错误阈值，则 Symantec Data Loss Prevention 会停止编制索引。然后，显示一条错误消息，警告数据可能已混乱或损坏。仅当数据源至少包含一千行时，Symantec Data Loss Prevention 才会检查错误。

为有效进行 EDM 索引编制准备确切数据源

- 1 确保数据源文件按如下所示格式化：

- 如果数据源超过 200,000 行，请验证它至少包含两列数据。其中一列应包含相当明确的值。例如，信用卡号、驾驶执照号码或帐号（而不是相对较普遍的姓名）。
- 验证已使用逗号、制表符或竖线 (|) 分隔数据源。如果数据源使用逗号作为分隔符，则删除不是用作分隔符的所有逗号。例如，如果地址列中的一个值为 346 Guerrero St., Apt.2，则删除 Guerrero St. 之后的逗号。

注意：井号 (#)、等号 (=)、加号 (+)、分号 (;) 和冒号 (:) 字符也会被视为分隔符。

- 验证数据值没用引在引号中。
- 从数据源中删除单个字符和简写的数据值。（例如，删除可能值为 Y 和 N 的列的列名及所有值。）还可以选择删除包含少于五位数字值的所有列，因为这些列会在实际运行时导致误报。

- 验证号码（如信用卡号或社会安全号）内部由短横线或空格分开，或者不使用任何分隔符。确保不要在此类号码中使用数据字段分隔符（如逗号）作为内部分隔符；例如：123-45-6789、123 45 6789 或 123456789，但不能是 123,45,6789。
- 去除重复记录，重复记录会在实际运行时产生重复匹配项。
- 通过将数据分隔至两个或多个字段，消除数据中的空格。例如，姓名 Joe Brown，在输入内容中显示时可能含有中间名或首大写字母；例如：Joe R Brown、Joe R. Brown 或 Joe Robert Brown。如果值 Joe Brown 出现于数据源的单个字段中，Symantec Data Loss Prevention 仅检测字面上的文本字符串 Joe Brown。不会检测姓名的其他变体。要确保系统对姓名的不同形式进行检测，应将姓名分为两个字段：一个“名”字段，一个“姓”字段。此外，您可能还需要删除由空格分隔的所有相对不太重要的文本。例如，对于数据值 Mary Jo，您可能想要整个删除 Jo。此外，某些数据值（如 San Francisco 和 New York）包含固有间距，可能并非匹配条件的关键要素，因此可以保持不变。
- 去除重复记录，重复记录会导致实际运行时的重复事件。
- 不要对常见值编制索引。EDM 最好与唯一值搭配使用。您需要考虑要编制索引的数据（从而进行保护）。此数据是否真正有价值？如果这个值是常见的值，则将其作为 EDM 值没有意义。例如，假设您要查找“州”。由于只有 50 个州，因此如果您的确切数据配置文件包含 300,000 行，则结果中会包含许多重复的常见值。无论数据是否用于策略，Symantec Data Loss Prevention 都会对确切数据配置文件中的所有值编制索引。使用不太常见的值，最好是唯一的值，是一种很好的做法，这样可以利用 EDM 获得最佳结果。

2 准备好确切数据源文件之后，继续执行 EDM 过程的下一步：将确切数据源文件加载到 Enforce Server 以配置要保护的数据。

请参见第 364 页的“[将确切数据源文件上传到 Enforce Server](#)”。

将确切数据源文件上传到 Enforce Server

为编制索引准备好数据源文件后，将其加载到 Enforce Server 以便可以对数据源编制索引。

此处所列出的三个选项可使 Enforce Server 可以使用数据源文件。请咨询数据库管理员确定可以满足您需要的最佳方法。

使 Enforce Server 可以使用数据源

1 如果数据源文件较大（超过 50 MB），请将其复制到安装 Enforce 的主机上的 datafiles 目录。

- 在 Windows 上，此目录位于 *DLP_home\Protect\datafiles*（例如，*C:\Vontu\Protect\datafiles*）中。

- 在 Linux 上，此目录位于 */var/Vontu/datafiles*。

此选项十分便捷，因为在配置“确切数据配置文件”过程中，使用该选项可通过下拉列表引用数据文件。如果文件较大，请使用第三方解决方案（如 Secure FTP）将数据源文件传输到 Enforce Server。

注意：确保 Enforce 用户（通常称为 protect）对 datafiles 目录中的所有文件具有“修改”权限（Windows 上）或“读写”权限（Linux 上）。

- 2 如果数据源文件较小（小于 50 MB），则使用 Enforce Server 管理控制台（Web 接口）将数据源文件上传到 Enforce Server。创建“确切数据配置文件”时，您可以指定文件路径或浏览至相应的目录并上传数据源文件。

注意：由于浏览器容量的限制，可以上传的最大文件大小为 2 GB。不过，建议不要上传任何超过 50 MB 的文件，因为上传超过此大小的文件需要较长的时间。如果您的数据源文件超过 50 MB，请考虑使用第一个选项，将数据源文件复制到 datafiles 目录。

- 3 在某些环境中，将数据源文件复制或上传到 Enforce Server 可能并不安全或不可行。在这种情况下，您可以使用“远程 EDM 索引器实用程序”远程对数据源编制索引。

请参见第 272 页的“[关于远程 EDM 索引器](#)”。

此实用程序允许您在 Enforce Server 主机以外的计算机上对确切数据源编制索引。如果您不希望将数据源文件复制到与 Enforce Server 相同的计算机时，此功能非常有用。例如，考虑一下发送数据的部门希望避免将数据复制到部门外主机的安全风险的情形。在这种情况下，您可以使用远程 EDM 索引器。

请参见第 272 页的“[使用远程 EDM 索引器](#)”。

- 4 继续执行 EDM 过程的下一步：配置确切数据配置文件和对数据源编制索引。

请参见第 365 页的“[创建和修改确切数据配置文件](#)”。

创建和修改确切数据配置文件

“管理”>“数据配置文件”>“确切数据”>“添加确切数据配置文件”屏幕是管理和添加确切数据配置文件的主页。需要有确切数据配置文件，才能实施“内容匹配确切数据”检测规则的实例。

请参见第 356 页的“[实施确切数据匹配](#)”。

确切数据配置文件指定数据源、索引编制参数及索引编制日程表。创建了 EDM 配置文件后，您可以对数据源编制索引并配置一个或多个检测规则，以便使用配置文件并检测确切内容匹配。

创建或修改确切数据配置文件

1 确保您已创建数据源文件。

请参见第 361 页的“[创建确切数据源文件](#)”。

2 确保您已准备好数据源以编制索引。

请参见第 363 页的“[为编制索引准备确切数据源文件](#)”。

3 在 Enforce Server 管理控制台中，导航至“管理”>“数据配置文件”>“确切数据”。

4 单击“添加确切数据配置文件”。

5 输入配置文件唯一的说明性名称（不超过 256 个字符）。

为便于引用，请选择描述数据内容和索引类型的名称（例如，Employee Data EDM）。

如果您修改现有确切数据配置文件，则可以更改配置文件名称。

6 选择以下“数据源”选项之一，使数据源文件可用于 Enforce Server：

■ 立即将数据源上传至服务器

如果您要创建新的配置文件，请单击“浏览”并选择数据源文件，或者输入数据源文件的完整路径。

如果您要修改现有的配置文件，请选择“立即上传”。

请参见第 364 页的“[将确切数据源文件上传到 Enforce Server](#)”。

■ 参考管理器主机上的数据源

如果您将数据源文件复制到 Enforce Server 上的 datafiles 目录，它会显示在下拉列表中以供选择。

请参见第 364 页的“[将确切数据源文件上传到 Enforce Server](#)”。

■ 使用此文件名

如果您尚未创建数据源文件，但要使用占位符数据源配置 EDM 规则，请选择此选项。输入您计划创建的数据源的文件名，包括要创建的列数。当您确实创建了数据源后，必须将其复制到 datafiles 目录。

注意：请谨慎使用该选项。切记创建数据源文件并将其复制到 datafiles 目录。数据源文件名称与此处输入的名称完全相同并且要包含此处指定的正确列数。

■ 加载外部生成的索引

如果您已使用远程 EDM 索引器在远程计算机上创建了索引，请选择此选项。此选项仅在定义并保存配置文件后才可用。

请参见第 364 页的“[将确切数据源文件上传到 Enforce Server](#)”。

- 7 如果数据源的第一行包含“列名”，请选中“将第一行读作列名”复选框。
- 8 指定“错误阈值”，即编制索引停止前包含错误的行的最大百分比。

数据源错误是指单元格为空、单元格中包含错误的数据类型或数据源中包含额外的单元格。例如，名称出现在电话号码列中即为一个错误。如果错误超过整体数据源的一定百分比（默认情况下为 5%），则系统会退出索引编制过程，并显示编制索引错误消息。如果指定 100% 作为错误阈值，则 Symantec Data Loss Prevention 会直接对数据源编制索引，不检查错误。

注意：有时，允许数据集中一定百分比的行包含错误。不过，超过特定的百分比可能表明数据源文件已损坏、格式不正确或者无法读取。您可以指定，如果特定百分比的行中包含错误，则停止编制索引。默认设置为 5%。

请参见第 363 页的“[为编制索引准备确切数据源文件](#)”。

- 9 选择您用来分隔数据源文件中的值的列分隔符（分隔符）。您可以使用的分隔符包括制表符、逗号或竖线。
- 10 为要分析的内容选择以下其中一个编码值，该编码值必须与数据源的编码匹配：
 - ISO-8859-1 (Latin-1) (默认值)**
使用拉丁字母表的西欧语言的标准 8 位编码。
 - UTF-8**
对所有使用 Unicode 4.0 标准（所有单字节和双字节字符）的语言使用此编码，包括那些东亚语言。
 - UTF-16**
对所有使用 Unicode 4.0 标准（所有单字节和双字节字符）的语言使用此编码，包括那些东亚语言。

注意：请确保您选择了正确的编码。系统不会阻止您使用错误编码创建 EDM 配置文件。当 EDM 策略尝试匹配入站数据时，系统在运行时仅报告一个错误。要确保您选择了正确的编码，请在单击“下一步”后，验证列名是否正确显示。如果列名称不能正确显示，说明您选择了错误的编码。

- 11 单击“下一步”转至第二个“[添加确切数据配置文件](#)”屏幕。

12 “字段映射”部分显示数据源中的列和“确切数据配置文件”中每列所映射的字段。现有“确切数据配置文件”中的字段映射是固定的，因此不可编辑。

请参见第 369 页的[“映射确切数据配置文件字段”](#)。

确认数据源中的列名准确地显示在“数据源字段”列。如果选择了“列名”选项，则“数据源字段”列会列出数据源第一行中的名称。如果没有选择“列名称”选项，则列会列出 Col 1、Col 2 等等。

13 在“系统字段”列中，从每个数据源字段的下拉列表中选择一个字段。（如果您使用策略模板或要检查数据源中的错误，则此步骤是必需的。）

例如，对于称为 SOCIAL_SECURITY_NUMBER 的数据源字段，请从相应下拉列表中选择“社会安全号”。“系统字段”下拉列表中的值包括所有策略模板的所有建议字段。

14 或者，指定和命名任何自定义字段（即“系统字段”下拉列表中未预先填入的字段）。要执行此操作，请按以下顺序执行这些步骤：

- 单击“字段映射”标题右侧的“高级视图”。此屏幕会显示两个额外的列（“自定义名称”和“类型”）。
- 要添加自定义系统字段名称，请转至适当的“系统字段”下拉列表。选择“自定义”，在相应的“自定义名称”文本字段键入名称。
- 要指定模式类型（为进行错误检查），请转至适当的“类型”下拉列表，并选择想要的模式。（要了解所有可用模式类型的说明，请单击列顶部的“说明”。）

15 针对计划使用的策略模板的建议字段检查字段映射。为此，请转至“针对策略模板检查映射”下拉列表，选择一个模板，并单击右侧的“立即检查”。

系统会显示已经映射的所有模板字段的列表。您可以返回并立即映射这些字段。或者，您可能想要扩展数据源以包括尽可能多的预期字段，然后重新创建确切数据配置文件。Symantec 建议您包括尽可能多的预期数据字段。

16 在屏幕的“编制索引”部分，选择下列选项之一：

■ **保存时提交索引作业**

当您保存确切数据配置文件时，选择此选项开始对数据源编制索引。

■ **按日程表提交索引作业**

选择此选项根据特定的日程表对数据源编制索引。从“日程表”下拉列表中进行选择，并根据需要指定星期、日期和时间。

请参见第 371 页的“[调度确切数据配置文件索引编制](#)”。

17 单击“完成”。

Symantec Data Loss Prevention 完成索引编制后，会从 Enforce Server 中删除原始数据源。对数据源编制索引后，将无法更改其架构。如果在对数据源编制索引后更改其列映射，则必须创建新的确切数据配置文件。

编制索引过程完成后，您可以为引用已创建的“确切数据配置文件”的策略创建新的 EDM 规则。

请参见第 357 页的“[关于数据所有者例外](#)”。

请参见第 358 页的“[关于字段映射](#)”。

请参见第 358 页的“[关于索引调度](#)”。

请参见第 57 页的“[关于字符集、语言和区域设置支持](#)”。

请参见第 372 页的“[配置“内容匹配确切数据”条件](#)”。

请参见第 275 页的“[创建 EDM 配置文件以便远程编制索引](#)”。

映射确切数据配置文件字段

在添加和配置了数据源文件和设置之后，通过“管理”>“数据配置文件”>“确切数据”>“添加确切数据配置文件”屏幕，您可以将字段从数据源文件映射到正在配置的确切数据配置文件。

要对数据源中的字段启用错误检查或将索引用于使用系统字段的策略模板，您必须将数据源中的字段映射到该系统字段。通过“字段映射”部分，可以将原始数据源中的列映射到确切数据配置文件中的系统字段。

表 20-5 字段映射选项

字段	说明
数据源字段	<p>如果在“添加确切数据配置文件”屏幕上选择了“列名”选项，此列将列出从数据源第一行中找到的值。如果您未选择此选项，则此列将按常规名称（如 Col 1、Col 2 等）列出各列。</p> <p>注意：如果要实施数据所有者例外，必须映射电子邮件和域字段之一或同时映射两者。</p> <p>请参见第 372 页的“配置“内容匹配确切数据”条件”。</p>

字段	说明
系统字段	<p>选择每列的系统字段。</p> <p>一个系统字段值（“未选择任何内容”除外）不能映射到多个列。</p> <p>有些系统字段具有与其相关的系统模式（如社会安全号），有些则没有（如姓氏）。</p> <p>注意：系统不能将模式 XXX-XXX-XXXX 识别为有效的电话号码格式，因为此格式频繁用于其他形式的识别。如果数据源包含此种格式的电话号码列，则选择“未选择任何内容”以避免电话号码和其他数据之间的混淆。</p>
针对策略模板检查映射	<p>从下拉列表中选择要针对其比较字段映射的策略模板，然后单击“立即检查”。</p> <p>实施 EDM 的所有策略模板都会显示在下拉菜单中（包括所有已导入的模板）。</p> <p>请参见第 326 页的“选择确切数据配置文件”。</p> <p>如果您计划使用多个策略模板，选择一个并对其进行检查，然后选择另一个并进行检查，依此类推。</p> <p>对于策略模板中的任何字段，如果数据源中没有对应的数据，则会显示一条消息，列出缺失的字段。但是，您仍然可以保存配置文件，或使用其他确切数据配置文件。</p>
高级视图	<p>如果您要自定义确切数据配置文件的架构，请单击“高级视图”显示高级字段映射选项。</p> <p>表 20-6列出并说明了可在“高级视图”屏幕中指定的其他列。</p>
正在编制索引	<p>选择其中一个编制索引选项。</p> <p>请参见第 371 页的“调度确切数据配置文件索引编制”。</p>
完成	当配置完确切数据配置文件时，请单击“完成”。

从“高级视图”中，可以将系统和数据源字段映射到系统模式。系统模式将指定的结构映射到确切数据配置文件中的数据，并对索引器启用有效错误检查和提示。

表 20-6 “高级视图”选项

字段	说明
自定义名称	如果对“系统字段”选择“自定义名称”，请输入它的唯一名称，然后选择“类型”值。此名称不能超过 60 个字符。

字段	说明
类型	如果对“系统字段”选择“自定义”以外的值，则某些数据类型会自动选择“类型”值。例如，如果对“系统字段”选择“出生日期”，则自动选择“日期”作为“类型”。您可以接受此选择，也可以对其进行更改。 某些数据类型不会自动选择“类型”值。例如，如果对“系统字段”选择“帐号”，则“类型”会保持未选择状态。您可以指定特定帐号的数据类型。
说明	单击“类型”列标题旁边的“(说明)”链接，以显示包含可用系统数据类型的弹出窗口。
简单视图	单击“简单视图”将返回到简单视图（“自定义名称”和“类型”列将隐藏）。

请参见第 365 页的[“创建和修改确切数据配置文件”](#)。

调度确切数据配置文件索引编制

配置确切数据配置文件时，可以设置对数据源编制索引的日程表（“按日程表提交索引作业”）。

请参见第 358 页的[“关于索引调度”](#)。

设置日程表之前，请注意以下建议事项：

- 如果只是偶尔更新数据源（如频率低于每月一次），则不需要创建日程表。可在每次更新数据源时编制数据索引。
- 将编制索引时间调度到系统使用率最低的时段。编制索引会影响整个 Symantec Data Loss Prevention 系统的性能，并且大型数据源的索引编制可能会花费较长时间。
- 添加或修改确切数据配置文件后立即对相应的数据源编制索引，无论何时更新数据源都重新编制数据源索引。例如，考虑在每个星期三的凌晨 2:00 更新数据源的情景。在这种情况下，您应调度在每个星期三的凌晨 3:00 编制索引。不要每天都对数据源编制索引，这会降低性能。
- 监视结果并相应修改索引编制日程表。例如，如果性能良好，而您希望更新更加及时，可以调度更频繁的数据更新和索引编制活动。

“编制索引”部分允许您在保存“确切数据配置文件”之后立即对其编制索引（推荐）或根据定期日程表编制索引，如下所示：

表 20-7 调度确切数据配置文件的索引编制

参数	说明
保存时提交索引作业	选择此选项可在单击“保存”时对“确切数据配置文件”编制索引。
按日程表提交索引作业	选择此选项可调度索引作业。默认选项为“无定期日程表”。如果要根据日程表编制索引，请按照如下所述选择所需的日程表期限。
编制索引一次	<p>日期 - 输入格式为 MM/DD/YY 的文档配置文件的编制索引日期。您也可以单击日期工具并选择日期。</p> <p>时间 - 选择开始编制索引的时间。</p>
每天编制索引一次	<p>时间 - 选择开始编制索引的时间。</p> <p>直到 - 选中此复选框以 MM/DD/YY 格式指定编制索引应停止的日期。您也可以单击日期工具并选择日期。</p>
每周编制索引一次	<p>每周的日期 - 选择在星期几对文档配置文件编制索引。</p> <p>时间 - 选择开始编制索引的时间。</p> <p>直到 - 选中此复选框以 MM/DD/YY 格式指定编制索引应停止的日期。您也可以单击日期工具并选择日期。</p>
每月编制索引一次	<p>每月的日期 - 输入希望每月发生编制索引的日期。日期必须是 1 到 28 之间的数字。</p> <p>时间 - 选择开始编制索引的时间。</p> <p>直到 - 选中此复选框以 MM/DD/YY 格式指定编制索引应停止的日期。您也可以单击日期工具并选择日期。</p>

请参见第 369 页的“[映射确切数据配置文件字段](#)”。

请参见第 365 页的“[创建和修改确切数据配置文件](#)”。

配置“内容匹配确切数据”条件

定义了确切数据配置文件和编制数据源索引之后，您可以在策略检测规则中配置一个或多个“内容匹配确切数据”条件。EDM 条件对策略例外不可用。

请参见第 330 页的“[配置策略](#)”。

表 20-8 配置“内容匹配确切数据”条件

操作	说明
配置 EDM 策略检测规则。	在策略中创建新的 EDM 检测规则，或者修改现有的 EDM 规则。 请参见第 334 页的 “配置策略规则” 。
当所有这些数据都匹配时匹配数据行	
选择要匹配的字段。	<p>“检查”要让条件匹配的每个数据字段。</p> <p>选择为匹配此规则而必须在邮件中检测到的数据字段数。</p> <p>您必须至少选择与检查的数据字段数相同的字段进行匹配。</p> <p>例如，如果从下拉菜单中选择“其中 2 个选定字段”，您必须至少检查 2 个检测字段。您可以检查超过 2 个字段。</p> <p>您可以一次“全选”或“取消全选”所有字段。</p>
选择 Where 子句可输入要匹配的特定字段值（可选）。	Where 选项匹配指定的字段值。通过从下拉菜单中选择确切数据字段来指定值。在相邻的文本框中输入该字段的值。如果要输入多个值，请用逗号分隔各个值。
当所有这些数据都匹配时忽略数据行	
忽略数据所有者。	<p>如果正在实施数据所有者例外，请选择以下选项之一：</p> <ul style="list-style-type: none"> ■ 发送者匹配 - 选择此选项可从检测中排除数据发送者。 ■ 任意或所有接受者匹配 - 选择这些选项之一可从检测中排除任何或所有数据接受者。 <p>要从检测中排除数据所有者，您的确切数据配置文件必须包含电子邮件地址字段或域地址字段（例如，symantec.com）。启用后，如果机密信息的发送者或接受者是数据所有者（通过电子邮件地址或域），则检测引擎允许在不生成事件的情况下发送或接收数据。</p> <p>请参见第 357 页的“关于数据所有者例外”。</p>

操作	说明
排除数据字段组合。	<p>已排除的组合只可用于匹配 2 个或 3 个字段。</p> <p>要启用此选项，您必须从条件配置顶部的“其中_个选定字段”下拉菜单中选择 2 个或 3 个要匹配的字段。</p> <p>您可以使用排除数据字段组合来指定从检测中排除的数据值组合。如果数据出现在排除的对或组中，则其不会成为匹配项。</p> <p>从显示的每个“字段 N”列中选择一个选项。然后单击向右箭头图标将字段组合添加到“已排除的组合”列表。要从列表中删除字段，请选择该字段并单击左箭头图标。</p> <p>注意：按住 Ctrl 键可在最右边的列中选择多个字段。</p>
附加匹配条件参数	
选择事件所需的最小数。	<p>输入或修改条件报告事件所需的最小匹配项数。</p> <p>例如，考虑这样一种情况，为社会安全号字段指定“其中1个选定字段”并指定事件所需的最少数为5。在这种情况下，引擎必须在单个邮件中至少检测到 5 个匹配的社会安全号才能触发事件。</p> <p>请参见第 359 页的“配置确切数据匹配计数”。</p>
选择要匹配的组件。	<p>选择要匹配的一个或多个邮件组件：</p> <ul style="list-style-type: none"> ■ 信封 - 邮件标头。 ■ 主题 - (对 EDM 不可用。) ■ 正文 - 邮件的内容。 ■ 附件 - 附加至邮件或通过邮件传输的所有文件的内容。 <p>请参见第 339 页的“选择匹配的组件”。</p>
选择还要匹配的一个或多个条件。	<p>选择此选项可创建复合条件。必须匹配所有条件，规则才能触发事件。</p> <p>您可以从列表中“添加”任何可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

EDM 最佳做法

确切数据匹配 (EDM) 是最强大的检测类型之一。您可以使用 EDM 来完全匹配数据库、电子表格或关键字列表中的数据。此类数据的示例可能包括社会安全号、姓氏、帐号等。这些数据配置文件可能包含数百万行的信息。

虽然对您在 EDM 索引中可以编制的列数没有限制，但我们建议您编制 2-3 列包含要匹配的关键标识符的索引。例如，通常不会将名字列包含在索引中，因为记录中可能有太多重复。正确创建的索引标识符可提供高度准确性。

EDM 规则对邮件执行全文搜索，针对每一个字词（已经排除的字词除外）检查潜在的匹配项。匹配算法是将邮件中的每一个字词与数据配置文件中每个单元格的内容进行比较。如果数据配置文件中的某个单元格包含多个字词，则该单元格绝对不可能匹配邮件中的字词。这是因为匹配算法不能将单个字词与一组字词进行匹配。

也存在例外，那就是某些类型的文本会触发表格搜索。例如，解压缩邮件时，它可能包含以逗号或竖线分隔的特定数据或者 Excel 文件附件。在这种情况下，即使单元格包含多个字词，也会针对数据配置文件对每个单元格（或数据片段）单独进行测试。例如，地址可以匹配。

“最小匹配数”字段对于调整 EDM 规则的敏感度很有帮助。例如，传出电子邮件中，一名员工的名字和姓氏是可接受的。但是，出现 100 名员工的名字和姓氏是严重违规的。另一个示例可能是姓氏和社会安全号策略。该策略可能会允许员工向医生发送信息，但发送两个姓氏和社会安全号是十分可疑的。

考虑通过选择生成的列组合。例如，两个或更多社会安全号、名字、电话号码或姓氏包含大量潜在的没有意义的组合（这可能包括名字 + 电话号码、电话号码 + 姓氏以及名字 + 姓氏）。要确保生成有用的事件，请通过要求更多列（即，要求存在三个或更多项目）来调整策略。或者，也可以使用例外排除无关紧要的组合。

仅当选择两个、三个或更多列时，列例外才可用。列名反映了在添加确切数据配置文件时创建的列映射。如果存在未映射的列，则其称为 Col X，其中 X 是原始数据配置文件中的列编号（从 1 开始）。

匹配项总是来自同一行。例如，如果规则指定两个或更多姓氏和社会安全号，则引擎只会检测那些与姓氏对应的社会安全号。

通常，数据库会组织成行列形式的表。每个列包含一种特定的数据类型。每行代表一条记录，包含每列数据类型的相关值。有些数据列可能包含多个单词。例如，“城市”列可能包含词语“旧金山”。目前，系统只能检测以表格格式数据显示的多字数据，例如 Excel 文件中的数据。此限制仅适用于数据库规则，而不适用于模式规则。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

使用索引文档匹配来检测内容

本章节包括下列主题：

- [关于实施索引文档匹配](#)
- [管理并添加已编制索引的文档配置文件](#)
- [配置“内容匹配文档签名”条件](#)
- [实施索引文档匹配](#)
- [准备文档源以便编制索引](#)
- [将内容排除（加入白名单）在检测范围之外](#)
- [创建和修改索引文档配置文件](#)
- [使用 WebDAV 创建远程 SharePoint 文件的索引](#)
- [IDM 最佳做法](#)

关于实施索引文档匹配

要实施索引文档匹配，首先要识别含有您想要保护的特定内容的文档。然后使用 Enforce Server 管理控制台对这些文档编制索引。在编制索引过程中会提取相关内容，并对其进行规范化和指纹加密操作。然后配置“内容匹配文档签名源”检测规则，用于检测来自原始受保护文档、草稿或不同版本的受保护文档内容的提取部分。通过索引文档匹配可排除（加入白名单）内容（如标准样板文件文本），从而调整检测结果并减少误报。

请参见第 382 页的“[实施索引文档匹配](#)”。

使用索引文档匹配 (IDM) 可对敏感文档中的特定数据进行指纹加密和检测。例如，您可以使用 IDM 保护包含专有软件编码、研究规范或并购文档的文档。您可以创建策略以检测邮件包含整个文档或部分文档时的匹配项。要使用 IDM，请创建包含来自源的哈希数据的安全文档索引。然后，会在一个或多个策略的检测规则中引用此索引。这样，您的策略在实际运行时就可以使用该索引。

请参见第 378 页的“[管理并添加已编制索引的文档配置文件](#)”。

要检测特定文档，Symantec Data Loss Prevention 需要一个特殊的索引版本文档。索引文档配置文件是一个安全的文件（或一组文件），包括来自一个或多个源文档的文本段的哈希。概括来说，单个文档的哈希称为文档指纹。索引不包含实际文档内容，因此是安全的。Symantec Data Loss Prevention 将索引与网络上的文档进行比较。检测引擎可以检测完全匹配或部分匹配。完全匹配适用于二进制文件，如 .gif、.mpg 和 .avi。

索引由一个或多个安全的二进制.rdx 文件组成，每个文件的大小都可容纳于检测服务器的随机存取内存 (RAM)。对于大型文档，Symantec Data Loss Prevention 可能会将数据分成多个.rdx 文件。在实际运行时，Symantec Data Loss Prevention 会使用应用于索引的算法，来将输入内容转换成哈希文本段。然后对来自输入内容的文本段和适当.rdx 文件中的文本段进行比较，以识别匹配项。部分匹配表示 Symantec Data Loss Prevention 会检测输入文档中索引文本的一部分。Symantec Data Loss Prevention 可以仅针对文本文档（例如，相对于音频文件或视频文件）执行部分匹配。

Symantec Data Loss Prevention 在 Enforce Server 的 C:\Vontu\Protect\index（Windows 上）或 /var/Vontu/index（Linux 上）中存储文档索引。它会在所有检测服务器上存储索引。只有在您将索引包括在策略中，然后在检测服务器上启用该策略时，Symantec Data Loss Prevention 才会部署索引。当策略处于活动状态时，检测服务器会将索引加载到 RAM。

创建文档配置文件后，可以立即在策略中对其进行引用。不过必须先编制文档索引，Symantec Data Loss Prevention 才能在实际运行时检测文档。

管理并添加已编制索引的文档配置文件

“管理” > “数据配置文件” > “已编制索引的文档” 屏幕列出了系统中所有配置好的已编制索引的文档配置文件。您可以在此屏幕中管理现有配置文件并添加新的配置文件。

请参见第 377 页的“[关于实施索引文档匹配](#)”。

表 21-1 已编制索引的文档的屏幕操作

列	说明
添加 IDM 配置文件	单击“添加文档配置文件”以新建已编制索引的文档配置文件。 请参见第 382 页的 “实施索引文档匹配” 。
编辑 IDM 配置文件	单击文档配置文件的名称或单击配置文件最右边的铅笔图标，以修改现有的文档配置文件。 请参见第 384 页的 “创建和修改索引文档配置文件” 。
删除 IDM 配置文件	单击文档配置文件行最右端的红色 X 图标，以从系统中删除该配置文件。 注意： 以下情况下无法编辑或删除配置文件：当前其他用户正修改该配置文件，或存在依赖于该配置文件的策略。
刷新 IDM 配置文件状态	单击“已编制索引的文档”屏幕右上方的刷新箭头图标，以获取索引编制进程的最新状态。如果您正在编制索引，则系统会显示消息“正在启动编制索引...”。系统不会在编制索引过程完成时自动更新屏幕。

表 21-2 已编制索引的文档的屏幕详细信息

列	说明
文档配置文件	文档数据配置文件的名称。
检测服务器	为文档配置文件和文档配置文件版本编制索引的检测服务器的名称。 单击文档配置文件名称旁边的“三角图标”以显示此信息。此信息显示在文档配置文件名称的下面。
位置	Enforce Server 上系统已配置且编制索引的文件的位置。
文档	系统为文档配置文件索引的文档数。

列	说明
状态	<p>文档索引编制过程的当前状态，可以是以下任何状态：</p> <ul style="list-style-type: none"> ■ 下次调度索引编制（如果当前未编制索引） ■ 正在将索引发送给检测服务器 ■ 正在编制索引 ■ 正在部署到检测服务器 <p>此外，在索引编制过程的状态下，系统会显示每个检测服务器的状态，可以是以下任何状态：</p> <ul style="list-style-type: none"> ■ 已完成，包括完成日期 ■ 挂起的索引完成（即，正在等待 Enforce Server 完成对文件编制索引） ■ 正在复制索引编制 ■ 正在创建索引（内部） ■ 正在构建缓存
错误消息	“已编制索引的文档”屏幕还会以红色显示所有的错误消息（例如，文档配置文件已损坏或不存在）。

请参见第 312 页的“[关于数据配置文件](#)”。

请参见第 388 页的“[计划文档配置文件的索引编制](#)”。

请参见第 380 页的“[配置“内容匹配文档签名”条件](#)”。

配置“内容匹配文档签名”条件

“内容匹配文档签名”基于指定文档源（称为文档配置文件）对非结构化文档内容进行匹配。

请参见第 377 页的“[关于实施索引文档匹配](#)”。

“内容匹配文档签名”可用于检测规则和例外。

请参见第 330 页的“[配置策略](#)”。

配置“内容匹配文档签名”条件

1 向策略规则或例外添加 IDM 条件，或者修改现有的条件。

请参见第 334 页的“[配置策略规则](#)”。

请参见第 342 页的“[配置策略例外](#)”。

2 配置 IDM 条件参数。

请参见第 381 页的[表 21-3](#)。

3 保存策略配置。

表 21-3 “内容匹配文档签名”条件的参数

操作	说明
设置最小文档外泄风险。	从下拉列表中选择一个选项。 您选择的数字表示匹配的百分比。如果您选择“确切”，则仅将内容与源文档内容完全匹配的文档视为匹配。
配置“匹配计数”。	选择希望计算匹配项的方式： <ul style="list-style-type: none">■ 检查是否存在 如果存在一个或多个条件匹配项，则将匹配数报告为 1。■ 计算所有匹配项 报告精确匹配项数目。 <p>请参见第 337 页的“配置匹配计数”。</p>
为“匹配位置”选择组件。	选择可用邮件组件之一进行匹配： <ul style="list-style-type: none">■ 正文 - 邮件的内容。■ 附件 - 附加至邮件或通过邮件传输的所有文件。 <p>请参见第 339 页的“选择匹配的组件”。</p>
配置“同时匹配”的其他条件。	选择此选项可创建复合条件。必须符合所有条件才能触发或排除匹配项。 您可以从下拉菜单中“添加”任何可用的条件。

实施索引文档匹配

实施 IDM

- 1 准备好要编制索引的文档。

请参见第 382 页的“[准备文档源以便编制索引](#)”。

- 2 也可以配置 Symantec Data Loss Prevention，在编制索引和检测期间将指定的文本列入白名单。

请参见第 383 页的“[将内容排除（加入白名单）在检测范围之外](#)”。

- 3 创建指定文档源的文档配置文件（在 Enforce Server Admin Console 中）。

请参见第 384 页的“[创建和修改索引文档配置文件](#)”。

- 4 配置所有文档源过滤器。

请参见第 386 页的“[根据文件名和大小过滤文档](#)”。

- 5 根据需要调度索引编制。

请参见第 388 页的“[计划文档配置文件的索引编制](#)”。

- 6 配置 IDM 规则和策略。

请参见第 380 页的“[配置“内容匹配文档签名”条件](#)”。

准备文档源以便编制索引

文档源是包含要编制索引的文档的 ZIP 存档文件，也可以是本地或远程计算机上文件共享中的文件。文档源存档文件可以包含任何文件类型和任何文件组合。如果您的文件共享中已经包含要保护的文档，则可以在文档配置文件中引用该共享。您还可以在文档配置文件中指定文件名和文件大小过滤器。编制索引过程中，这些过滤器会告知系统要包括哪些文件、忽略哪些文件。

准备文档源以便编制索引

- 1 创建包含您希望保护的文档的文档源存档文件。不要在文档源存档文件中包含任何内部存档文件。任何内部存档文件都未打开和编制索引。

- 2 要保护大的文档集合，请在共享目录或文件存档中分隔这些文档。然后为每个目录或存档创建单独的文档配置文件。

在编制索引的过程中，大的文档源会影响性能。要减轻编制索引时的负载，Symantec Data Loss Prevention 会将每个文档源的大小限制到大约 300,000 或 400,000 个文档。Symantec Data Loss Prevention 允许的具体文档数取决于平均提取的文本大小（每个文档源）。

- 3 要让文档源出现在“添加文档配置文件”屏幕上的便捷下拉列表中，请将其复制到下列目录之一：

- 在 Windows 上，将其复制到 *DLP_home\Protect\documentprofiles*（例如，*c:\Vontu\Protect\documentprofiles*）。
 - 在 Linux 上，将其复制到 */var/Vontu/documentprofiles*。
- 4 继续执行此过程的下一步骤：配置文档配置文件。或者，如果您要将特定文档内容排除在检测范围之外，请将其加入白名单。
请参见第 384 页的“[创建和修改索引文档配置文件](#)”。
请参见第 383 页的“[将内容排除（加入白名单）在检测范围之外](#)”。

将内容排除（加入白名单）在检测范围之外

通常情况下，敏感文档包含不要求保护的标准样板文件文本。在这种情况下，您可将系统配置为排除此文本（加入白名单）。Enforce Server 不为加入白名单的文本编制索引，因此可将其排除在检测范围之外。如果要将特定文档源中的文本排除在检测范围之外，必须在编制索引前执行本部分中的步骤。

要将文档内容排除在检测范围之外，请为您要编制索引的每个文档配置文件创建 *Whitelisted.txt* 文件。当您对文档源编制索引时，Enforce Server 会查找 *Whitelisted.txt* 文件。如果该文件存在，Enforce Server 会将其复制到 *Whitelisted.x.txt*，其中 x 是唯一的文档配置文件标识号。将来对同一配置文件编制索引时，使用配置文件特定的白名单文件，而不是普通文件。

将文档内容加入白名单

- 1 将要加入白名单的所有内容复制到一个文本文件中，并将该文件保存为 *Whitelisted.txt*。
- 2 将该文件保存到适当的目录：
 - 在 Windows 上，将其保存到 *DLP_home\Protect\documentprofiles\whitelisted* 中。*DLP_home* 是 Symantec Data Loss Prevention 安装目录。例如，将该文件保存到 *c:\Vontu\Protect\documentprofiles\whitelisted*。
 - 在 Linux 上，将文件保存到 */var/Vontu/documentprofiles/whitelisted*。

默认情况下，您编制索引的文件必须至少包含 130 个字符。该默认设置也适用于 *Whitelisted.txt* 文件。对于加入白名单的文本，您可以更改此默认设置。

注意：如果减小默认最小值，Enforce Server 会利用其编制索引的更小的文档部分创建哈希。默认最小值越小，Enforce Server 需要用于文档的哈希数就越多。检测过程中，更多数量的哈希会增加索引大小以及计算负载。

更改加入白名单的文本的默认最小值

- 1 在 Symantec Data Loss Prevention 主机上，导航至 `DLP_home\Protect\config`。例如，在 Windows 上，请转至 `c:\Vontu\Protect\config`。或者，在 Linux 上，请转至 `/opt/Vontu/Protect/config`。
- 2 使用文本编辑器打开 `Indexer.properties` 文件，然后查找以下文本：

```
# Guarantee threshold t  
com.vontu.profiles.documents.t=130
```

- 3 更改 `Guarantee threshold t` 值的数值部分，以反映 `Whitelisted.txt` 中所允许的最小所需字符数。例如，要将最小值更改为 80 个字符，修改该值使其如下所示：

```
# Guarantee threshold t  
com.vontu.profiles.documents.t=80
```

- 4 保存文件。

请参见第 384 页的“[创建和修改索引文档配置文件](#)”。

创建和修改索引文档配置文件

在“管理”>“数据配置文件”>“已编制索引的文档”>“配置文档配置文件”屏幕上定义和配置文档配置文件。

文档配置文件可指定源文档、索引编制参数及索引编制日程表。必须定义适当的文档配置文件，才能实施“内容匹配文档签名”检测。

配置文档配置文件

- 1 使用策略创建权限登录到 Enforce Server 管理控制台。
- 2 导航到“管理”>“数据配置文件”>“已编制索引的文档”屏幕。
- 3 在“已编制索引的文档”屏幕上，单击“添加文档配置文件”。
或者，单击现有的文档配置文件对其进行编辑。
请参见第 378 页的“[管理并添加已编制索引的文档配置文件](#)”。
- 4 为文档配置文件输入名称。为便于引用，请选择描述数据内容及索引类型的名称（如 Research Docs IDM）。文档配置文件的名称限于 256 个字符。
- 5 每个文档配置文件都是一组您希望保护的文件。必须先将文档配置文件的文件复制到 Enforce 并添加引用它的文档配置文件，然后才能在策略中使用该文档配置文件。

通过选择以下选项之一指定数据源：

■ 立即将文档存档上传至服务器

键入文档存档 (.zip 文件) 的完整路径和文件名，或单击“浏览”进行选择。例如，输入 c:\Documents\Research.zip。如果要编辑文档配置文件并更改数据源文件，会显示“立即上传”选项。指定新的文件位置之后，请单击“立即上传”。

注意：如果此存档中的文件是另一个存档文件 (*.zip)，Symantec Data Loss Prevention 不会对其解压缩和编制索引。只有在处理完全匹配时才会考虑这种嵌入式存档，与图像文件和其他不受支持的文件格式类似。

注意：存档文件的最大大小仅受分配给 Enforce Server 的磁盘空间的限制。最大上传大小是 2 GB，但不建议上传 50 MB 以上的文件。上传大文件可能需要很长时间。如果存档文件超过 50 MB，请使用第三方解决方案（例如安全 FTP）将其复制到 Enforce Server，然后您可以从“**使用管理器上的本地路径**”下拉菜单中选择此文件。

■ 引用 Enforce Server 上的存档

如果已将文档源复制到 Symantec Data Loss Prevention 文档文件目录，则可以从下拉列表中选择文档源。下拉列表中不会显示任何当前由其他文档配置文件引用的文档源。

请参见第 382 页的“[准备文档源以便编制索引](#)”。

■ 使用 Enforce Server 上的本地路径

键入要编制索引的文档所在目录的路径。例如，键入 c:\Documents。您必须指定确切的路径，而不是相对路径。不要在路径中包括实际文件名。请注意，不能使用本方法对包含于 .zip 文件中的文档编制索引。

■ 使用远程 SMB 共享

输入要编制索引的文档所在的服务器消息块 (SMB) 共享的通用命名约定 (UNC) 路径。（UNC 路径包括服务器名称、共享名称和可选的文件路径。例如，\\server\share\file_path。）为共享输入有效的用户名和密码，然后再次输入密码。

注意：指定的用户必须具有共享驱动器的常规访问权限以及其中文件的读取权限。

或者，您可以使用保存的凭据（前提是下拉菜单中提供了这些凭据）。

请参见第 121 页的“[关于凭据存储](#)”。

- 6 在“文件名包括过滤器”和“文件名排除过滤器”文本框中，输入要使用的所有过滤器。例如，在“文件名包括过滤器”文本框中输入*.doc，可使Symantec Data Loss Prevention 仅对文档源中的*.doc 文件编制索引。

请参见第 386 页的[“根据文件名和大小过滤文档”](#)。

- 7 在“大小过滤器”字段中，指定对 Symantec Data Loss Prevention 应编制索引的文件大小的任何限制。例如，要避免对超过 2 MB 的文件编制索引，请在“忽略大于以下大小的文件”字段中输入 2 并从相应的下拉列表中选择 MB。例如，要避免 Symantec Data Loss Prevention 对超过 1 KB 的文件编制索引，请在“忽略小于以下大小的文件”字段中输入 1 并从相应的下拉列表中选择 KB。

- 8 在“编制索引”部分，选择以下选项之一：

■ 保存时提交索引作业

可使 Symantec Data Loss Prevention 在保存文档配置文件时对文档编制索引。

■ 按日程表提交索引作业

可使 Symantec Data Loss Prevention 显示日程表选项。从“日程表”下拉列表中进行选择，并根据需要指定星期、日期和时间。

请参见第 388 页的[“计划文档配置文件的索引编制”](#)。

- 9 单击“完成”。

Symantec Data Loss Prevention 完成索引编制后，会从 Enforce Server 中删除文档源。例如，Symantec Data Loss Prevention 从

c:\Vontu\Protect\documentprofiles (在 Windows 上) 或

/var/Vontu/documentprofiles (在 Linux 上) 删除文档源存档文件。

注意：如果选择了“使用远程 SMB 共享”，Symantec Data Loss Prevention 不会删除文档。

根据文件名和大小过滤文档

过滤器可让您指定在编制索引时要包括或排除的文档。过滤器的类型包括文件名包括过滤器、文件名排除过滤器和大小过滤器。

文件名过滤器：

- 如果“文件名包括过滤器”字段为空，会对指定文档配置文件中的所有文档进行匹配。如果您在该字段中输入任何内容，则会被视为包括过滤器。在这种情况下，只有文档与您指定的过滤器相匹配时，才会对文档编制索引。

- 检测服务器会忽略您在“文件名排除过滤器”字段指定的所有文本。
- 使用文件名过滤器时，Symantec 建议选择排除过滤器或包括过滤器，而不要二者同时选择。

表 21-4 介绍了“文件名过滤器”功能所接受的语法。

表 21-4 文件名过滤语法

运算符	说明
星号 (*)	代表任意数目的字符。
问号 (?)	代表单个字符。
逗号 (,) 和换行符	代表逻辑运算符 OR。

对于“文件名过滤器”，Symantec Data Loss Prevention 将正斜杠 (/) 和反斜杠 (\) 同等对待。它忽略模式开头和末端的空白字符。文件名过滤不支持转义字符，因此无法匹配文本问号、逗号或星号。

以下列表包括一些过滤器示例，以及如果在“文件名包括过滤器”字段中键入这些过滤器的行为描述：

表 21-5 文件名过滤器示例

过滤器	说明
.txt、.doc	系统只对.zip 文件或文件共享中的.txt 和.doc 文件编制索引，忽略所有其他文件。
?????.doc	系统只对扩展名为.doc 的文件和名称为五个字符的文件编制索引，例如 hello.doc 和 stats.doc（而不是 good.doc 或 foobar.doc）。
/documentation/、*/specs/*	系统只对根目录下名为 documentation 和 specs 的两个子目录中的文件编制索引。

使用大小过滤器根据文件大小从匹配进程中排除文件。与大小过滤器相匹配的所有文件将会被忽略。

表 21-6 介绍了文件大小过滤器选项。

表 21-6 文件大小过滤器配置选项

过滤器	说明
忽略小于以下大小的文件	要排除小于特定大小的文件，请在此字段中输入一个数字。然后从旁边的下拉列表中选择适合的文件大小单位：字节、KB（千字节）或 MB（兆字节）。
忽略大于以下大小的文件	要排除大于特定大小的文件，请在此字段中输入一个数字。然后从旁边的下拉列表中选择适合的文件大小单位：字节、KB 或 MB。

计划文档配置文件的索引编制

在创建文档配置文件的过程中，可以设置对文档源编制索引的日程表。

配置文档配置文件时，请选择“保存时提交索引作业”，以便于保存文档配置文件后，可立即对其编制索引（建议）。或者，可以设置对文档源编制索引的日程表。

设置索引编制日程表之前，请注意以下建议事项：

- 如果您只是偶尔更新文档源（比如少于每月一次），就没有创建日程表的必要。您可以在每次更新文档时编制文档索引。
- 将编制索引时间调度到系统使用率最低的时段。编制索引会影响整个 Symantec Data Loss Prevention 系统的性能，编制大型文档的索引可能要花费较长时间。
- 请在添加或修改相应的文档配置文件后立即编制索引，并在每次更新文档时重新编制索引。例如，考虑在每星期三凌晨 2:00 更新文档。在这种情况下，将索引进程调度在每个星期三凌晨 3:00 运行是最佳的。建议不要每天编制文档索引，因为这样会过于频繁并且还会降低服务器性能。
- 监视结果并相应修改索引编制日程表。如果性能良好，且您想要更新更加及时，则可以调度更频繁的文档更新和索引编制活动。
- Symantec Data Loss Prevention 执行增量索引。在对先前已编制索引的共享或目录再次编制索引时，仅对已更改或已添加的文件编制索引。在此编制索引期间，将删除不再位于存档中的任何文件。所以，重新编制索引操作的运行速度明显快于初始编制索引操作的速度。

注意：Enforce Server 一次只能对一个文档配置文件编制索引。如果在运行某个索引进程的同时调度启动另一个索引进程，则在第一个进程完成之后才会开始新进程。

要计划文档的索引编制，请选择“按日程表提交索引作业”，然后从下拉列表中选择一个日程表，如表 21-7 中所述。

表 21-7 用于计划文档配置文件索引编制的选项

参数	说明
编制索引一次	日期 - 输入格式为 MM/DD/YY 的文档配置文件的编制索引日期。您也可以单击日期工具并选择日期。 时间 - 选择开始编制索引的时间。
每天编制索引一次	时间 - 选择开始编制索引的时间。 直到 - 选中此复选框以 MM/DD/YY 格式指定编制索引应停止的日期。您也可以单击日期工具并选择日期。
每周编制索引一次	每周的日期 - 选择在星期几对文档编制索引。 时间 - 选择开始编制索引的时间。 直到 - 选中此复选框以 MM/DD/YY 格式指定编制索引应停止的日期。您也可以单击日期工具并选择日期。
每月编制索引一次	每月的日期 - 输入希望每月发生编制索引的日期。日期必须是 1 到 28 之间的数字。 时间 - 选择开始编制索引的时间。 直到 - 选中此复选框以 MM/DD/YY 格式指定编制索引应停止的日期。您也可以单击日期工具并选择日期。

使用 WebDAV 创建远程 SharePoint 文件的索引

请完成下列任务来实施使用 WebDAV 创建 SharePoint 文件的远程索引。

表 21-8 使用 WebDAV 在 SharePoint 上创建远程文件的索引

步骤	任务	说明
1	针对 SharePoint 启用 WebDAV。	请参见第 392 页的“ 针对 IIS 启用 WebDAV ”。
2	启动 WebClient 服务。	从安装 Enforce Server 的计算机上，使用“服务”控制台启动 WebClient 服务。如果该服务为“已禁用”，请在服务上右键单击，然后选择“属性”。启用服务、将它设置为“手动”，然后启动它。 注意： 您必须具有管理权限才能启用此服务。

步骤	任务	说明
3	访问 SharePoint 实例。	从安装 Enforce Server 的计算机上，使用浏览器和下列地址格式访问 SharePoint： <code>http://<server_name>:port</code> 。例如， <code>http://protect-x64:80</code> 。
4	以授权用户的身份登入 SharePoint。	您不需要拥有 SharePoint 管理权限。
5	找到要扫描的文档。	在 SharePoint 中，导航到您要扫描的文档。通常，SharePoint 文档会保存在“主页” > “共享文档”屏幕上。您的文档可能存储在不同的位置。
6	查找文档的 UNC 路径。	在 SharePoint 中，针对您要扫描的文件，选择“库” > “使用资源管理器打开”选项。Windows 资源管理器应该会打开一个窗口并显示文档。在“地址”字段中查找文档的路径。该地址为远程扫描文档所需的 UNC 路径。例如： <code>\protect-x64\Shared Documents</code> 。将该路径复制到剪贴板或文本文件。
7	创建 IDM 索引。	<p>配置远程索引源：</p> <ul style="list-style-type: none"> ■ 对于“文档来源”字段，选择“使用远程 SMB 共享”选项。 ■ 对于“UNC 路径”，粘贴（或输入）上一步复制的地址。例如：<code>\protect-x64\Shared Documents</code>。 ■ 对于“用户凭据”，输入 SharePoint 用户名和密码，或从“已保存的凭据”下拉列表中选择用户名和密码。 ■ 选择“保存时提交索引”选项，然后单击“保存”。 <p>注意：若要创建 IDM 索引，请参阅联机帮助主题，或《Symantec Data Loss Prevention 管理指南》中的《创建和修改已编制索引的文档配置文件》标题。</p>
8	验证是否成功。	<p>在“管理” > “数据配置文件” > “已编制索引的文档”屏幕上，应该会看到索引已成功创建。检查“状态”和已编制索引的文档数。如果已成功创建索引，现在您就可以使用它来创建 IDM 策略。</p> <p>请参见第 393 页的“故障排除”。</p>

关于使用 WebDAV 对 SharePoint 文档远程 IDM 编制索引

您可以借助 Symantec Data Loss Prevention 11.1 版，使用 WebDAV 对存储在远程 SharePoint 服务器上的文档编制索引。

WebDAV（基于 Web 的步进式创建及版本）是一种标准，用于提供扩展名给 HTTP 1.1 协议，以允许用户相互协作编辑和管理远程 Web 服务器上的文件。可以启用托管 SharePoint 实例的 Microsoft IIS 部署，以接受来自 Web 客户端的 WebDAV 连接。

一旦您为 SharePoint 启用了 WebDAV，就可以使用 IDM 索引配置期间可用的“远程 SMB 共享”选项，对远程文档的编制索引。Symantec Data Loss Prevention 支持使用 WebDAV 对 SharePoint 2007 和 SharePoint 2010 实例进行远程 IDM 编制索引。

使用 WebDAV 创建远程 SharePoint 文件的索引

请完成下列任务来实施使用 WebDAV 创建 SharePoint 文件的远程索引。

表 21-9 使用 WebDAV 在 SharePoint 上创建远程文件的索引

步骤	任务	说明
1	针对 SharePoint 启用 WebDAV。	请参见第 392 页的“ 针对 IIS 启用 WebDAV ”。
2	启动 WebClient 服务。	从安装 Enforce Server 的计算机上，使用“服务”控制台启动 WebClient 服务。如果该服务为“已禁用”，请在服务上右键单击，然后选择“属性”。启用服务、将它设置为“手动”，然后启动它。 注意： 您必须具有管理权限才能启用此服务。
3	访问 SharePoint 实例。	从安装 Enforce Server 的计算机上，使用浏览器和下列地址格式访问 SharePoint： <code>http://<server_name>:port</code> 。例如， <code>http://protect-x64:80</code> 。
4	以授权用户的身份登入 SharePoint。	您不需要拥有 SharePoint 管理权限。
5	找到要扫描的文档。	在 SharePoint 中，导航到您要扫描的文档。通常，SharePoint 文档会保存在“主页”>“共享文档”屏幕上。您的文档可能存储在不同的位置。

步骤	任务	说明
6	查找文档的 UNC 路径。	在 SharePoint 中，针对您要扫描的文件，选择“库”>“使用资源管理器打开”选项。Windows 资源管理器应该会打开一个窗口并显示文档。在“地址”字段中查找文档的路径。该地址为远程扫描文档所需的 UNC 路径。例如：\\protect-x64\Shared Documents。将该路径复制到剪贴板或文本文件。
7	创建 IDM 索引。	<p>配置远程索引源：</p> <ul style="list-style-type: none"> ■ 对于“文档来源”字段，选择“使用远程 SMB 共享”选项。 ■ 对于“UNC 路径”，粘贴（或输入）上一步复制的地址。例如：\\protect-x64\Shared Documents。 ■ 对于“用户凭据”，输入 SharePoint 用户名和密码，或从“已保存的凭据”下拉列表中选择用户名和密码。 ■ 选择“保存时提交索引”选项，然后单击“保存”。 <p>注意：若要创建 IDM 索引，请参阅联机帮助主题，或《Symantec Data Loss Prevention 管理指南》中的《创建和修改已编制索引的文档配置文件》标题。</p>
8	验证是否成功。	<p>在“管理”>“数据配置文件”>“已编制索引的文档”屏幕上，应该会看到索引已成功创建。检查“状态”和已编制索引的文档数。如果已成功创建索引，现在您可以使用它来创建 IDM 策略。</p> <p>请参见第 393 页的“故障排除”。</p>

针对 IIS 启用 WebDAV

有多种方法可以启用 WebDAV。下列步骤提供的方法以 Windows Server 2008 为案例。此方法仅作为示例提供。您的方法和环境可能有所不同。

针对 SharePoint 启用 WebDAV

- 1 登录您要启用 WebDAV 的 SharePoint 系统。
- 2 打开 Internet Information Services (IIS) 管理员控制台。
- 3 在 IIS 树状结构中选择服务器名称。
- 4 展开这个树状结构，单击“网站”文件夹并展开它。

- 5 从列表中选择 SharePoint 实例。
- 6 右键单击 SharePoint 实例，并选择“新建”>“虚拟目录”。
- 7 虚拟目录创建向导随即显示。单击“下一步”。
- 8 在“别名”字段输入名称（例如 WebDAV），然后单击“下一步”。
- 9 在“网站内容目录”字段输入目录路径。这可以是任何存在的目录路径。单击“下一步”。
- 10 选择“读取权限”，然后单击“下一步”。
- 11 单击“完成”。
- 12 右键单击所创建的虚拟目录，然后选择“属性”。
- 13 在“虚拟目录”选项卡，选择“重定向到 URL”选项，然后单击“创建”。别名会填入“应用程序名称”字段中。
- 14 在“重定向到”字段输入 SharePoint 网站 URL，然后单击“确定”。此时就会启用 WebDAV 以用于 SharePoint 实例。

请参见第 391 页的[“使用 WebDAV 创建远程 SharePoint 文件的索引”](#)。

故障排除

如果在启用 WebDAV 后无法将 Enforce Server 计算机连接到 SharePoint Server 计算机，请确保您已在 Enforce Server 计算机上启动 WebClient 服务。在您配置 IDM 编制索引前，必须先启动此服务并测试 WebDAV 连接。

如果您计划在 SharePoint 文档更新时，定期对这些文档重新编制索引，或许将远程网络资源映射到安装 Enforce Server 的本地计算机会有帮助。您可以使用“net use”MS-DOS 命令，来映射使用 UNC 路径的 SharePoint。例如：

- `net use`
这个命令未加上参数时，会检索和显示网络连接列表。
- `net use s: \\sharepoint_server\Shared Documents`
此命令会将 SharePoint Server 分配（映射）至本地“S”驱动器。
- `net use * \\sharepoint_server\Shared Documents`
该命令会将 SharePoint Server 分配（映射）至下一台可用的盘符驱动器。
- `net use s: /delete`
该命令会删除指定驱动器的网络映射。

文档上次更新日期：2011 年 7 月 15 日。

IDM 最佳做法

如果 Symantec Data Loss Prevention 无法为文档（例如图像文件）的内容编制索引，检测会执行完全匹配。即使选择了最低的文档外泄风险百分比（小于完全匹配），也会发生这种情况。另外，检测引擎会针对非常小的文件使用完全匹配，即使这些文件是文本文件也是如此。（确切的长度随文件的内容变化而变化。通常，该长度约为 300 个字符或更少。）

例如，考虑包含五个 Microsoft Word 文档、一个 Microsoft Excel 文档和三个图像文件的文档源。选择 50% 作为最小文档相似度。Symantec Data Loss Prevention 为 Word 和 Excel 文档编制索引并针对这些文档查找 50% 匹配。与此相反，它会针对三个图像文件查找确切数据匹配。对于 50% 的暴露度，如果文档包含了大约 50% 的所选文档配置文件中的内容，则被视为匹配。

文档可能包含更多的内容，但是系统仅保护已编制索引的内容（作为文档配置文件的一部分）。例如，请考虑这种情况：为一页的文档编制索引，该一页的文档是 100 页的文档的一部分。该 100 页的文档被视为 100% 匹配，因为其内容与一页的文档完全匹配。

注意：匹配的文档的文件类型或格式不必与已编制索引的文档相同。例如，如果您将 Word 文档作为文档配置文件的一部分编制索引，用户将其内容粘贴到电子邮件的正文或者从该 Word 文档创建 PDF，则引擎会将其视为匹配。

请参见第 377 页的“[关于实施索引文档匹配](#)”。

使用向量机学习来检测内 容

本章节包括下列主题：

- 实施向量机学习 (VML)
- 关于培训的内容
- 创建新的 VML 配置文件
- 结合使用“当前配置文件”选项卡与“临时工作区”选项卡
- 上传培训的示例文档
- 培训 VML 配置文件
- 调整内存分配
- 关于培训的基本准确百分比率
- 管理培训集文档
- 管理 VML 配置文件
- 更改 VML 配置文件的名称和说明
- 配置 VML 策略规则
- 关于在策略中使用被拒绝的 VML 配置文件
- 配置 VML 策略例外
- 关于相似度阈值和相似度评分
- 调整相似度阈值

实施向量机学习 (VML)

向量机学习 (VML) 通过执行统计分析确定内容是否与您培训的文档示例集相似来保护非结构化数据。

请参见第 287 页的“[关于向量机学习](#)”。

下表介绍了实施 VML 的过程。

表 22-1 实施 VML

步骤	操作	说明
步骤 1	收集用于培训系统的示例文档。	收集代表性数量的示例文档，其中包含要保护的正面内容和要忽略的负面内容。 请参见第 397 页的“ 关于培训的内容 ”。
步骤 2	创建一个新 VML 配置文件。	根据用于派生正面和负面培训集的特定业务类别的数据，定义一个新 VML 配置文件。 请参见第 398 页的“ 创建新的 VML 配置文件 ”。
步骤 3	上传示例文档。	分别将示例正面培训集和示例负面培训集上传到 Enforce Server。 请参见第 399 页的“ 上传培训的示例文档 ”。
步骤 4	培训 VML 配置文件。	对系统进行培训以了解要保护的内容类型并生成 VML 配置文件。 请参见第 401 页的“ 培训 VML 配置文件 ”。
步骤 5	接受或拒绝已培训配置文件。	接受已培训配置文件来对其进行部署。或者，拒绝配置文件，更新培训集之一或两者（通过添加或删除示例文档），以及重新启动培训进程。 请参见第 404 页的“ 关于培训的基本准确百分比率 ”。 请参见第 406 页的“ 管理 VML 配置文件 ”。
步骤 6	创建一个 VML 策略和测试检测。	创建一个引用 VML 配置文件的 VML 策略。 请参见第 408 页的“ 配置 VML 策略规则 ”。 根据“相似度评分”测试并查看事件。 请参见第 411 页的“ 关于相似度阈值和相似度评分 ”。

步骤	操作	说明
步骤 7	调整 VML 配置文件。	<p>根据需要调整“相似度阈值”设置以优化检测结果。请参见第 412 页的“调整相似度阈值”。</p> <p>注意：有关其他信息，请参考 <i>Symantec Data Loss Prevention Vector Machine Learning Best Practices Guide</i>（《Symantec Data Loss Prevention 向量机学习最佳做法指南》），该文档可在 DLP 知识库中获取 (https://kb-vontu.altiris.com)，文章编号 54340。</p>

关于培训的内容

收集用于培训的文档是向量机学习过程中最重要的步骤。向量机学习仅与您用于培训的示例内容一样准确。

请参见第 396 页的“[实施向量机学习 \(VML\)](#)”。

VML 配置文件基于代表特定企业用例的内容类别。内容类别包括两个培训集：正面和负面。

正面培训集是您要保护的内容。内容的类别越具体，准确性就越高。例如，“客户购买订单”比“财务文档”更好，因为它更具体。

负面培训集是您要忽略的内容，与正面培训集相关。例如，如果正面培训集是“每周销售报告”，则负面培训集可能包含“销售新闻稿”。

您收集的正面和负面内容（主要基于文本）应在数量上相等。不必收集所有想要保护的内容，但需要使培训集足够大以生成可靠的统计信息。

建议每个培训集收集 250 个文档。每个培训集包含的最小文档数是 50。

下表概述了为 VML 配置文件培训收集的内容的基线要求。

表 22-2 VML 培训集要求

内容类别	数据类型	培训集	数量	内容	大小
一个特定企业用例	基于文本（主要）	正面	建议的数量：250 个文档 最小数量：50 个文档	要保护的内容。	每次上传 30 MB
		负面	与正面类别的数量近似相等。	不想要保护但在主题方面与正面类别相关的内容。	每个类别没有大小限制。

创建新的 VML 配置文件

VML 配置文件包含根据培训集内容生成的模型。定义 VML 配置文件之后，可使用它来创建一个或多个 VML 策略。

请参见第 396 页的“[实施向量机学习 \(VML\)](#)”。

注意：必须有 Enforce Server 管理员权限才能创建 VML 配置文件。

创建新的 VML 配置文件

- 在“管理”>“数据配置文件”>“向量机学习”屏幕中，单击“新建配置文件”（如果您尚未执行该操作）。
- 在“创建新的配置文件”对话中输入 VML 配置文件的“名称”。

使用与要保护的数据类别相对应的 VML 配置文件的逻辑名称。

请参见第 397 页的“[关于培训的内容](#)”。

- (可选) 输入 VML 配置文件的“说明”。
您可能需要提供确定 VML 配置文件的用途的说明。
- 单击“创建”创建新的 VML 配置文件。
或者，单击“取消”取消该操作。
- 单击“管理配置文件”上传示例文档。
请参见第 399 页的“[上传培训的示例文档](#)”。

结合使用“当前配置文件”选项卡与“临时工作区”选项卡

对于任意单个 VML 配置文件，都有两个可能的版本：当前版本和临时版本。当前配置文件是运行时版本；临时配置文件是设计时版本。通常，在开发 VML 配置文件时，会同时存在已经培训、接受且可能部署到一个或多个策略的当前配置文件和当前正在编辑和调整的临时配置文件。

Enforce Server 管理控制台会在单独的选项卡中显示 VML 配置文件的每个版本：

■ 当前配置文件

此版本是 VML 配置文件的活动实例。此版本已经成功培训和接受，可以部署到一个或多个策略。

■ 临时工作区

此版本是 VML 配置文件的可编辑版本。此版本没有培训或接受，或者既没有培训也没有接受，不能部署到策略。

最初创建新 VML 配置文件时，系统仅显示一个“当前配置文件”选项卡，其中包含一个空的培训集。首次培训并接受 VML 配置文件后，“当前配置文件”选项卡中的“培训集”表将填充有培训集的相关详细信息。此表和选项卡中显示的信息是只读的。

编辑 VML 配置文件

- ◆ 单击“当前配置文件”选项卡最右侧的“管理配置文件”。

系统会在“临时工作区”选项卡中显示配置文件的可编辑版本。现在，您可以继续培训和管理配置文件。

请参见第 401 页的[“培训 VML 配置文件”](#)。

在培训并接受新的 VML 配置文件版本之前，“临时工作区”选项卡会一直显示在用户界面中。换言之，如果不培训和接受配置文件（即使未对配置文件进行任何更改），将无法关闭“临时工作区”选项卡。

接受新的 VML 配置文件版本后，系统将使用新接受的版本覆盖以前的“当前配置文件”。无法恢复到以前接受的“当前配置文件”。但是，可以将“临时配置文件”的培训集恢复到以前的版本。

请参见第 405 页的[“管理培训集文档”](#)。

上传培训的示例文档

培训集包括您要针对其对系统进行培训的正面示例和负面示例文档。您可以分别上传正面文档和负面文档。

注意：虽然您可以上传单个文档，但是建议您上传包含推荐数量（250）或最低数量（50）示例文档的文档存档（例如 ZIP、RAR 或 TAR）。最大上传大小是 30 MB。如果您要上传的数据超过 30 MB，则可以对存档中的文档进行分割。请参见第 397 页的“[关于培训的内容](#)”。

上传培训集

- 1 单击“当前配置文件”选项卡中的“管理配置文件”（如果尚未执行此操作）。
此操作允许在“临时工作区”选项卡中对 VML 配置文件进行编辑。
请参见第 399 页的“[结合使用“当前配置文件”选项卡与“临时工作区”选项卡](#)”。
- 2 单击“上传内容”（如果尚未执行此操作）。
此操作将打开“上传内容”对话框。
- 3 选择要上传的内容类别：
 - 选择“正例：匹配与这些相似的内容”上传正面文档存档。
 - 选择“负例：忽略与这些相似的内容”上传负面文档存档。
- 4 单击“浏览”选择要上传的文档存档。
- 5 在文件系统中导航到存储示例文档的位置。
- 6 选择要上传的文件并单击“打开”。
- 7 验证选择的上传内容类别是否正确：“正面”或“负面”。
如果与上传的内容不匹配（选择“负面”，但上传“正面”文档存档），则生成的配置文件不准确。
- 8 单击“提交”将文档存档上传到 Enforce Server。
系统将显示一条消息，指示文件是否成功上传。如果上传成功，文档存档将出现在“新文档”表中。此表将显示文档类型、名称、大小、上传日期和上传用户。如果上传失败，请检查错误消息并重试上传。单击“删除”列中的 X 图标将已上传的文档或文档存档从培训集中删除。
- 9 单击“上传内容”对其他培训集重复此过程。
只有上传了最低数量的正面示例文档和负面示例文档，配置文件才算完整，才能进行培训。
请参见第 398 页的[表 22-2](#)。
- 10 成功上传了正面培训集和负面培训集这两个培训集后，就可以准备培训 VML 配置文件了。
请参见第 401 页的“[培训 VML 配置文件](#)”。

培训 VML 配置文件

在配置文件培训过程中，系统会扫描培训内容、提取主要特征并生成统计模型。成功完成培训过程后，系统将提示您接受或拒绝培训配置文件。如果您接受培训结果，该版本的 VML 配置文件将变为“当前配置文件”，表示该配置文件处于活动状态并可用于一个或多个策略。

请参见第 396 页的“[实施向量机学习 \(VML\)](#)”。

表 22-3 培训 VML 配置文件

步骤	操作	说明
步骤 1	启用培训模式。	<p>从“管理”>“数据配置文件”>“向量学习”屏幕选择要培训的 VML 配置文件。或者，创建新的 VML 配置文件。 请参见第 398 页的“创建新的 VML 配置文件”。</p> <p>单击“当前配置文件”选项卡最右侧的“管理配置文件”。 系统会在“临时工作区”选项卡中显示要培训的配置文件。 请参见第 399 页的“结合使用“当前配置文件”选项卡与“临时工作区”选项卡”。</p>
步骤 2	上传培训内容。	<p>自行熟悉培训集要求和建议。 请参见第 397 页的“关于培训的内容”。</p> <p>将正面和负面培训集用单独的文档存档上传到 Enforce Server。 请参见第 399 页的“上传培训的示例文档”。</p>
步骤 3	调整内存分配（仅在必要时）。	<p>默认值为“高”，该值通常会产生最佳培训集准确率。通常，不需要更改该设置。对于某些情况，可能需要选择“中”或“低”内存设置（例如，将配置文件部署到端点）。</p> <p>请参见第 403 页的“调整内存分配”。</p> <p>注意：如果要更改内存设置，必须在培训配置文件之前执行该操作，以确保产生准确的培训结果。如果您已经培训了配置文件，则必须在调整内存分配之后重新培训。</p>

步骤	操作	说明
步骤 4	开始培训进程。	<p>单击“开始培训”开始配置文件培训过程。</p> <p>在培训进程中，系统进行以下操作：</p> <ul style="list-style-type: none">■ 从内容中提取主要特征；■ 创建模型；■ 根据整个培训集的平均误报和漏报率计算预计的准确性；■ 生成 VML 配置文件。
步骤 5	检验培训完成。	<p>培训进程完成时，系统指示是否已经成功创建培训配置文件。</p> <p>如果培训进程失败，系统会显示错误。检查调试日志文件并重新启动培训进程。</p> <p>请参见第 236 页的“调试日志文件”。</p> <p>成功完成培训进程后，系统将显示“新建配置文件”的以下信息：</p> <ul style="list-style-type: none">■ 培训的示例文档 系统培训和配置的每个培训集中的示例文档数。■ 培训的准确率 培训集的质量，表示为基本误报和基本漏报百分率。 请参见第 404 页的“关于培训的基本准确百分比率”。■ 内存■ 在运行时加载配置文件以进行检测所需的最小内存数量。 <p>注意：如果先前接受了配置文件，系统还会显示“当前配置文件”统计信息用于并排比较。</p>

步骤	操作	说明
步骤 6	接受或拒绝培训配置文件。	<p>如果培训进程成功，系统将提示您接受或拒绝培训配置文件。您的决定取决于“培训的准确率”百分比。</p> <p>请参见第 404 页的“关于培训的基本准确百分比率”。</p> <p>接受或拒绝培训配置文件：</p> <ul style="list-style-type: none">■ 单击“接受”，将培训结果保存为活动的当前配置文件。 接受培训配置文件之后，它将显示在“当前配置文件”选项卡中，并且将删除“临时工作区”选项卡。■ 单击“拒绝”放弃培训结果。 配置文件将保留在“临时工作区”选项卡中，以待编辑。可通过添加或删除文档调整其中一个或所有两个培训集，然后重新培训配置文件。 请参见第 405 页的“管理培训集文档”。 <p>注意：除非您接受培训的 VML 配置文件，否则该配置文件处于非活动状态。虽然系统允许您根据尚未培训或接受的 VML 配置文件创建策略，但是只有接受配置文件才能将 VML 配置文件部署到该策略。请参见第 410 页的“关于在策略中使用被拒绝的 VML 配置文件”。</p>
步骤 7	测试并调整配置文件。	<p>成功培训并接受 VML 配置文件后，即可使用它来定义策略规则并可调整 VML 配置文件。</p> <p>请参见第 408 页的“配置 VML 策略规则”。</p> <p>请参见第 411 页的“关于相似度阈值和相似度评分”。</p> <p>注意：有关更多信息，请参考 <i>Symantec Data Loss Prevention Vector Machine Learning Best Practices Guide</i>（《Symantec Data Loss Prevention 向量机学习最佳做法指南》），可从 DLP 知识库获取（网址为 https://kb-vontu.altiris.com/），文章编号 54340。</p>

调整内存分配

“内存分配”设置确定在策略检测运行时加载 VML 配置文件所需的内存量。培训较大的 VML 配置文件需要分配更多的内存，因为需要建模更多的功能。默认情况下，该值设置为“高”。一般不应该调整此值。但是，如果打算将 VML 配置文件部署到端点，该端点上资源可能有限，则可能需要使用较低内存设置来减少配置文件的大小。

调整内存分配

- 1 单击“内存分配”设置旁边的“调整”。

此设置在“临时工作区”选项卡中可用。如果不可用，请单击“当前配置文件”选项卡中的“管理配置文件”。

请参见第 399 页的“[结合使用“当前配置文件”选项卡与“临时工作区”选项卡](#)”。

- 2 选择所需的内存分配级别。

提供以下选项：

■ 高

要求较高的运行时内存量；一般可提供较高的检测准确性（默认设置）。

■ 中

■ 低

要求较低的运行时内存；可能导致较低的检测准确性。

- 3 单击“保存”保存该设置。

“内存设置”显示应该反映您所做的调整。

- 4 单击“开始培训”启动培训过程。

在培训 VML 配置文件之前，您必须调整内存分配。如果已经对配置文件进行了培训，则在调整此设置之后重新培训。

请参见第 401 页的“[培训 VML 配置文件](#)”。

- 5 验证运行 VML 配置文件所需的内存量。

培训 VML 配置文件之后，系统将显示“所需内存 (KB)”值，表示在运行时加载配置文件所需的最低内存量。

请参见第 406 页的“[管理 VML 配置文件](#)”。

关于培训的基本准确百分比率

在 VML 配置文件培训进程期间，系统将提取示例文档内容并将其转换成原始文本。系统使用专有算法选择功能（或关键字）并生成 VML 配置文件。在培训进程中，系统将计算并报告误报和漏报的基本准确率。培训的基本准确百分比率表示正面培训集和负面培训集的质量。

如果目标是达到 100% 准确（基本错误率为 0%），则两个培训集均达到此质量级别通常是不可能的。一般来说，如果基本误报率或基本漏报率超过 5%，应拒绝培训配置文件。相对高的基本错误百分比率表示培训集的分类不是很精确。在这种情况下，您需要将文档添加到未被充分代表的培训集和/或从代表性过度的培训集中删除文档。

请参见第 405 页的“[管理培训集文档](#)”。

下表介绍了对于给定的 VML 配置文件的正面和负面培训集，培训的基本准确百分比率的含义。

表 22-4 培训的基本准确率

准确率	说明
基本误报率 (%)	从统计学上说，负面培训集中的内容所占的百分比与正面内容相似。
基本漏报率 (%)	从统计学上说，正面培训集中的内容所占的百分比与负面内容相似。

管理培训集文档

在培训和调整 VML 配置文件时，可能需要调整其中一个或两个培训集。例如，如果拒绝了培训配置文件，则需要通过添加或删除示例文档来提高培训准确率。

请参见第 404 页的“[关于培训的基本准确百分比率](#)”。

将文档添加到培训集

1 针对要编辑的配置文件，单击“管理配置文件”。

可编辑的配置文件出现在“临时工作区”选项卡中。

2 单击“上传内容”。

请参见第 399 页的“[上传培训的示例文档](#)”。

从培训集删除文档

1 针对要编辑的配置文件，单击“管理配置文件”。

可编辑的配置文件出现在“临时工作区”选项卡中。

2 针对要删除的培训文件，单击“标记为已删除”列中的红色 X。

删除的文档将出现在“已删除文档”表中。根据需要重复此过程以从培训集中删除所有不需要的文档。

3 单击“开始训练”以重新培训配置文件。

必须重新培训并接受更新的配置文件才能完成文档删除过程。如果未接受新配置文件，则尝试删除的文档仍是配置文件的一部分。

请参见第 401 页的“[培训 VML 配置文件](#)”。

恢复删除的文档

- 1 针对已删除的文档，单击“恢复”列中的恢复图标。
文档将重新添加到培训集中。
- 2 单击“开始训练”以重新培训配置文件。
即使将配置文件恢复到了原始配置，也必须重新培训并重新接受配置文件。

管理 VML 配置文件

“管理”>“数据配置文件”>“向量机学习”屏幕是管理现有 VML 配置文件的主页以及创建新的 VML 配置文件的起点。

请参见第 396 页的[“实施向量机学习 \(VML\)”](#)。

注意：必须有 Enforce Server 管理员权限才能管理和创建 VML 配置文件。

表 22-5 创建和管理 VML 配置文件

操作	说明
创建新的配置文件。	单击“新建配置文件”可以创建新的 VML 配置文件。 请参见第 398 页的 “创建新的 VML 配置文件” 。
查看配置文件并对配置文件进行排序。	系统在“向量机学习”屏幕上列出所有现有 VML 配置文件及其状态。 单击列标题，可按名称或状态对 VML 配置文件进行排序。
管理和培训配置文件。	从列表中选择一个 VML 配置文件，以显示和管理该配置文件。 “当前配置文件”选项卡显示活动的配置文件。 请参见第 399 页的 “结合使用“当前配置文件”选项卡与“临时工作区”选项卡” 。 单击“管理配置文件”以编辑配置文件。 可编辑的配置文件出现在“临时工作区”选项卡中。通过该选项卡，您可以执行以下操作： <ul style="list-style-type: none">■ 上传培训集文档。 请参见第 399 页的“上传培训的示例文档”。■ 培训配置文件。 请参见第 401 页的“培训 VML 配置文件”。■ 从培训集添加和删除文档。 请参见第 405 页的“管理培训集文档”。

操作	说明
监控配置文件。	<p>系统会列出并描述所有 VML 配置文件的状态。</p> <ul style="list-style-type: none"> ■ 所需内存 (KB) 在内存中加载配置文件以进行检测所需的最小内存数量。 请参见第 403 页的“调整内存分配”。 ■ 状态 配置文件的目前状态。 请参见第 407 页的表 22-6。 ■ 部署状态 配置文件的历史状态。 请参见第 408 页的表 22-7。
删除配置文件。	<p>单击最右侧的 X 图标以删除现有配置文件。</p> <p>如果您删除现有配置文件，系统会从 Enforce Server 中删除配置文件元数据和培训集。</p>

“状态” 字段显示每个 VML 配置文件的当前状态。

表 22-6 VML 配置文件的状态值

状态值	说明
接受<日期>	接受培训配置文件的日期。
管理	启用当前配置文件以进行编辑。
空	创建了配置文件，但没有上传内容。
等待接受	配置文件已可以接受。
取消培训	系统正在取消培训。
已取消培训	已取消培训进程。
已失败	培训进程失败。
培训<时间>	培训正在进行中（对于指定的时间）。

“部署状态” 字段指示是否接受过 VML 配置文件。

表 22-7

VML 配置文件的部署状态值

状态值	说明
从未接受	从未接受 VML 配置文件。 请参见第 410 页的“ 关于在策略中使用被拒绝的 VML 配置文件 ”。
接受<日期>	已在指定的日期接受 VML 配置文件。

更改 VML 配置文件的名称和说明

如果必要，您可以更改 VML 配置文件的名称或编辑其说明。例如，当您准备将 VML 配置文件部署到一项或多项策略时，您可能需要为配置文件提供一个较为自述性的名称，以方便策略创建者可以轻松识别。

注意：如果更改配置文件名称或说明，则不需要对其重新培训。

更改 VML 配置文件的名称或说明

- 1 从“管理”>“数据配置文件”>“向量机学习”屏幕上选择 VML 配置文件。
请参见第 406 页的“[管理 VML 配置文件](#)”。
- 2 单击该 VML 配置文件名称旁边的“编辑”链接。
- 3 在出现的“更改名称和说明”对话框中，编辑配置文件的名称和说明。
- 4 单击“确定”保存对该 VML 配置文件名称或说明的更改。
- 5 验证 VML 配置文件在主屏幕上的更改。

配置 VML 策略规则

培训并接受 VML 配置文件后，可使用“[使用向量机学习配置文件检测](#)”条件配置 VML 策略。此条件引用 VML 配置文件来检测与已培训的示例内容相似的内容。

请参见第 396 页的“[实施向量机学习 \(VML\)](#)”。

表 22-8 配置 VML 策略规则

步骤	操作	说明
步骤 1	创建并培训 VML 配置文件。	<p>请参见第 398 页的“创建新的 VML 配置文件”。</p> <p>请参见第 401 页的“培训 VML 配置文件”。</p> <p>请参见第 410 页的“关于在策略中使用被拒绝的 VML 配置文件”。</p>
步骤 2	配置新的或现有的策略。	请参见第 330 页的“ 配置策略 ”。
步骤 3	向策略添加 VML 规则。	<p>从“配置策略”屏幕中：</p> <ul style="list-style-type: none"> ■ 选择“添加规则”。 ■ 从内容规则列表中选择“使用向量机学习配置文件检测”规则。 ■ 从下拉菜单中选择要使用的 VML 配置文件。 ■ 单击Next。
步骤 4	配置 VML 检测规则。	<p>命名规则并配置规则严重性。</p> <p>请参见第 334 页的“配置策略规则”。</p>
步骤 5	选择要匹配的组件。	<p>为“匹配位置”选择一个或两个邮件组件：</p> <ul style="list-style-type: none"> ■ 正文 - 邮件的内容 ■ 附件 - 通过邮件传输的任何文件 <p>注意：在端点上，Symantec DLP Agent 匹配整个邮件，而不是单个邮件组件。</p> <p>请参见第 339 页的“选择匹配的组件”。</p>
步骤 6	配置其他条件（可选）。	<p>或者，您可以通过向规则添加更多条件来创建复合检测规则。</p> <p>要添加其他条件，请从下拉菜单中选择所需的条件并单击“添加”。</p> <p>注意：必须匹配所有条件，规则才能触发事件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>
步骤 7	保存策略配置。	单击“ 确定 ”，然后单击“ 保存 ”以保存策略。

关于在策略中使用被拒绝的 VML 配置文件

系统允许您创建基于从未被接受的 VML 配置文件的策略。但是，只有初次接受配置文件后，VML 配置文件才会处于活动状态并部署到引用的策略。

请参见第 401 页的“[培训 VML 配置文件](#)”。

如果您的 VML 策略引用了从未被接受的 VML 配置文件，则此配置的结果取决于检测服务器的类型。下表描述了这一行为：

检测服务器	说明
发现服务器	直到载入所有策略依赖关系后，发现扫描才会启动。同样，直到引用的 VML 配置文件被接受后，基于发现扫描的 VML 策略才会启动。在这种情况下，系统会在发现扫描界面中显示一条消息，表示扫描正在等待依赖关系载入。
网络和 Endpoint Server	<p>对于简单规则或条件为“逻辑与”关系的复合规则，整个规则将失败，因为 VML 条件无法匹配。如果这是策略中唯一的一个规则，则该策略将不会运行。</p> <p>对于具有多个规则（“逻辑或”关系）的策略，则只有 VML 规则失败；将评估策略中的其他规则。</p> <p>请参见第 297 页的“关于检测服务器策略执行”。</p>

配置 VML 策略例外

在某些情况下，您可能要实施 VML 策略例外以忽略某些内容。

请参见第 396 页的“[实施向量机学习 \(VML\)](#)”。

表 22-9 配置 VML 策略例外

步骤	操作	说明
步骤 1	创建并培训 VML 配置文件。	<p>请参见第 398 页的“创建新的 VML 配置文件”。</p> <p>请参见第 401 页的“培训 VML 配置文件”。</p>
步骤 2	配置新的或现有的策略。	请参见第 330 页的“ 配置策略 ”。

步骤	操作	说明
步骤 3	向策略添加 VML 例外。	从“ 配置策略 ”屏幕中： <ul style="list-style-type: none"> ■ 选择“添加例外”。 ■ 从内容例外列表中选择“使用向量机学习配置文件检测”例外。 ■ 从下拉菜单中选择要使用的 VML 配置文件。 ■ 单击“下一步”。
步骤 4	配置策略例外。	对例外进行命名。 选择要应用例外的组件： <ul style="list-style-type: none"> ■ 整个消息 选择此选项可将例外与整个邮件进行比较。如果例外在邮件中随处可见，则触发例外且不发生任何匹配。 ■ 仅限匹配的部分 选择此选项，可针对与规则相同的组件匹配例外。例如，如果规则与“正文”匹配且附件中出现例外，则不触发例外。
步骤 5	配置条件。	通常，您可以接受策略例外的默认条件设置。 请参见第 342 页的“ 配置策略例外 ”。
步骤 6	保存策略配置。	单击“确定”，然后单击“保存”以保存策略。

关于相似度阈值和相似度评分

各个VML配置文件都包含一个称为“相似度阈值”的设置，其设置范围为0到10。此设置可用于调整培训集中的不完整信息来达到可能的最佳准确性。在检测期间，只有消息的“相似度评分”高于“相似度阈值”，才能生成事件。“相似度阈值”是在配置文件级别（而不是在策略规则中）设置，因为理想的“相似度阈值”设置对培训集是唯一的，并可以达到最佳准确率（无论是误报还是漏报）。

当 VML 策略检测到事件时，系统将在 Enforce Server 管理控制台的“事件快照”的匹配突出显示部分中显示“相似度评分”。“相似度评分”表示检测的内容与 VML 配置文件的相似程度。从统计学上说，评分越高，消息表示的与 VML 配置文件中的正面示例文档的相似度越高。

例如，“相似度阈值”设置为4，且检测到“相似度评分”为5的消息。在这种情况下，系统会在突出显示匹配时将匹配报告为事件并显示“相似度评分”。但是，如果检测到“相似度评分”为3的消息，系统将不会报告匹配（并且没有事件），因为“相似度评分”低于“相似度阈值”。

下表介绍了“相似度阈值”和“相似度评分”数。

表 22-10 相似度阈值和相似度评分详细信息

相似度	说明
相似度阈值	<p>“相似度阈值”是一个介于 0 和 10 之间的可配置参数，并且对各个 VML 配置文件都是唯一的。默认设置是 10，要求 VML 配置文件功能和检测的消息内容之间的匹配最为相似。同样，此设置可能生成较少的事件。设置为 0 会生成大量的匹配项，其中的许多匹配可能是误报。</p> <p>请参见第 412 页的“调整相似度阈值”。</p>
相似度评分	<p>“相似度评分”是一个介于 0 和 10 之间的只读运行时统计值，该值是系统根据 VML 策略的检测结果所报告的。要报告事件，“相似度评分”必须高于“相似度阈值”，否则 VML 策略不会报告匹配。</p>

调整相似度阈值

调整“相似度阈值”设置以调整 VML 配置文件。“相似度阈值”确定检测的内容与 VML 配置文件相似程度必须达到多少时才会生成事件。

请参见第 411 页的“[关于相似度阈值和相似度评分](#)”。

注意：在调整“相似度阈值”之后不必重新培训 VML 配置文件，除非根据测试结果修改培训集。

调整相似度阈值的当前值

1 单击要调整的 VML 配置文件的“相似度阈值”标签旁边的“编辑”。

此操作将打开“相似度阈值”对话框。

2 将计量器拖至所需的“当前值”设置。

可以将“相似度阈值”设置为 0 到 10 范围内的十进制值。默认值是 10，可生成较少的事件；设置为 0，可生成较多的事件。

3 单击“保存”保存该“相似度阈值”设置。

4 使用 VML 策略测试 VML 配置文件。

比较匹配项之间的“相似度评分”。检测的消息的“相似度评分”必须高于“相似度阈值”，才会生成事件。根据需要进一步调整“相似度阈值”设置以优化和调整 VML 配置文件。

请参见第 408 页的“[配置 VML 策略规则](#)”。

使用数据标识符检测内容

本章节包括下列主题：

- 关于数据标识符
- 可用的系统数据标识符
- 关于数据标识符宽度
- 关于可选验证器
- 关于数据标识符的跨组件匹配
- 关于修改数据标识符
- 关于数据标识符模式
- 关于数据标识符的模式语言限制
- 关于验证器
- 关于自定义数据标识符
- 关于数据规范化程序
- 关于数据标识符配置
- 关于数据标识符的唯一匹配项计数
- 关于更改随机化美国 SSN
- 管理和添加数据标识符
- 配置“内容匹配数据标识符”条件
- 修改和创建数据标识符
- 数据标识符最佳做法

关于数据标识符

Symantec Data Loss Prevention 提供了数据标识符来检测所描述内容的特定实例。使用数据标识符，您只需以最小的努力即可快速实现精确、简短格式的数据匹配。

数据标识符是将模式匹配与数据验证器相结合来进行内容检测的算法。模式类似于正则表达式，但更加有效，因为它们已经过优化，可精确匹配数据。验证器用于进行准确性检查，这种检查着重于检测范围并确保遵从性。

例如，“信用卡号”系统数据标识符用于检测与特定模式匹配的号码。匹配的模式会经过“Luhn 检查”（是一种算法）进行验证。在这种情况下，将验证号码前 15 位数字算出的值是否等于第 16 位数字。

Symantec Data Loss Prevention 提供了预配置的数据标识符，用于检测常用的敏感数据（例如，信用卡号、社会安全号和驾驶执照号码）。数据标识符具有三种宽度（大、中、小），因此您可以调整检测结果。数据标识符为检测国际内容提供广泛支持。

请参见第 430 页的“[选择系统数据标识符宽度](#)”。

如果系统定义的数据标识符不满足您的要求，可以对其进行修改。还可以定义自定义的数据标识符来检测可以描述的任何内容。

表 23-1 数据标识符类别

类别	说明
个人身份	检测北美、欧洲和亚太地区的各种标识号码。 请参见第 415 页的 表 23-2 。 请参见第 416 页的 表 23-6 。 请参见第 417 页的 表 23-7 。
财务	检测财务标识号码，例如信用卡号或 ABA 汇款路径号码。 请参见第 415 页的 表 23-3 。
医疗	检测美国和国际药品代码。 请参见第 416 页的 表 23-4 。
信息技术	检测 IP 地址。 请参见第 416 页的 表 23-5 。
国际关键字	使用关键字检测并验证常见国际内容。 请参见第 497 页的“ 使用国际系统数据标识符的查找关键字 ”。
已修改	您修改的由系统定义的数据标识符。 请参见第 419 页的“ 关于修改数据标识符 ”。

类别	说明
自定义	用户定义的数据标识符。 请参见第 439 页的“ 实施自定义数据标识符 ”。

可用的系统数据标识符

Symantec Data Loss Prevention 提供了 36 种系统定义的数据标识符，以帮助您准确检测和验证基于模式的敏感数据。

表 23-2 北美个人身份

数据标识符	说明
美国社会安全号 (SSN)	请参见第 577 页的“ 美国社会安全号 (SSN) 数据标识符 ”。
加拿大社会保险号	请参见第 526 页的“ 加拿大社会保险号码数据标识符 ”。
美国个人纳税识别号 (ITIN)	请参见第 573 页的“ 英国税号数据标识符 ”。
驾驶执照号码 - 加利福尼亚州	请参见第 540 页的“ 驾驶执照号码 - 加利福尼亚州数据标识符 ”。
驾驶执照号码 - 伊利诺斯州	请参见第 543 页的“ 驾驶执照号码 - 伊利诺斯州数据标识符 ”。
驾驶执照号码 - 新泽西州	请参见第 544 页的“ 驾驶执照号码 - 新泽西州数据标识符 ”。
驾驶执照号码 - 纽约州	请参见第 545 页的“ 驾驶执照号码 - 纽约州数据标识符 ”。
驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州	请参见第 541 页的“ 驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州数据标识符 ”。

表 23-3 财务

数据标识符	说明
信用卡号	请参见第 532 页的“ 信用卡号数据标识符 ”。
ABA 汇款路径号码	请参见第 522 页的“ ABA 汇款路径号码数据标识符 ”。
CUSIP 号	请参见第 538 页的“ CUSIP 号码数据标识符 ”。

数据标识符	说明
SWIFT 代码	请参见第 561 页的“ SWIFT 代码数据标识符 ”。
信用卡磁条数据	请参见第 529 页的“ 信用卡磁条数据数据标识符 ”。
IBAN 西部	请参见第 552 页的“ IBAN 西部数据标识符 ”。
IBAN 中部	请参见第 548 页的“ IBAN 中部数据标识符 ”。
IBAN 东部	请参见第 549 页的“ IBAN 东部数据标识符 ”。

表 23-4 医疗

数据标识符	说明
国家药品代码	请参见第 556 页的“ 国家药品代码 (NDC) 数据标识符 ”。
澳大利亚医疗号码	请参见第 525 页的“ 澳大利亚医疗号码数据标识符 ”。

表 23-5 信息技术

数据标识符	说明
IP 地址	请参见第 554 页的“ IP 地址数据标识符 ”。

表 23-6 欧洲个人身份

数据标识符	说明
税号	请参见第 529 页的“ 意大利税号数据标识符 ”。
西班牙 DNI ID	请参见第 561 页的“ 西班牙 DNI ID 数据标识符 ”。
荷兰税号	请参见第 526 页的“ 荷兰税号数据标识符 ”。
英国驾照号	请参见第 564 页的“ 英国驾照号数据标识符 ”。
英国税号	请参见第 573 页的“ 英国税号数据标识符 ”。
英国护照号	请参见第 571 页的“ 英国护照号数据标识符 ”。
英国国家保险号码	请参见第 569 页的“ 英国国家保险号码数据标识符 ”。

数据标识符	说明
英国国民保健服务 (NHS) 号	请参见第 567 页的“ 英国国民保健服务 (NHS) 号数据标识符 ”。
英国选民登记号	请参见第 566 页的“ 英国选民登记号数据标识符 ”。
法国国家统计局代码	请参见第 546 页的“ 法国国家统计局代码数据标识符 ”。
瑞士 AHV 号码	请参见第 563 页的“ 瑞士 AHV 号码数据标识符 ”。

表 23-7 亚太区个人身份

数据标识符	说明
澳大利亚税务号码	请参见第 525 页的“ 澳大利亚税务号码数据标识符 ”。
中华人民共和国 ID	请参见第 558 页的“ 中华人民共和国 ID 数据标识符 ”。
香港特别行政区 ID	请参见第 547 页的“ 香港特别行政区 ID 数据标识符 ”。
新加坡 NRIC	请参见第 559 页的“ 新加坡 NRIC 数据标识符 ”。
韩国居民登记号码	请参见第 559 页的“ 韩国居民登记号码数据标识符 ”。
中国台湾 ID	请参见第 563 页的“ 中国台湾 ID 数据标识符 ”。

关于数据标识符宽度

系统数据标识符是按宽度实施的。宽度定义了该数据标识符的检测范围。每个数据标识符至少实施一种检测宽度。可用于数据标识符的最大宽度选项可能产生最多的误报匹配项；而最小宽度选项则产生最少的误报匹配项。通常，验证器和模式随宽度的不同而不同。

请参见第 418 页的[表 23-8](#)。

例如，“美国社会安全号(SSN)”数据标识符提供三种检测宽度：大、中和小。“驾驶执照号码 - 加利福尼亚州”系统数据标识符提供大宽度和中宽度。在这两种情况下，最小宽度都实施关键字验证器。

注意：并非所有的系统数据标识符都提供每种检测宽度。请参考数据标识符和宽度的完整列表来确定哪种可用。

请参见第 430 页的“[选择系统数据标识符宽度](#)”。

表 23-8 系统数据标识符的可用规则宽度

宽度	说明
大	大宽度定义了一个或多个用于创建最大数量匹配的模式。通常，此宽度产生比中宽度和小宽度更高的误报率。
中	中宽度可以优化检测模式和/或添加一个或多个数据验证器来限制匹配项的数量。
小	小宽度提供最严密的模式和最严格的验证，以提供最准确可靠的匹配项。通常，此选项要求存在关键字或其他验证限制才能触发匹配。

关于可选验证器

可选验证器有助于缩小数据标识符的检测范围。当配置数据标识符实例时，您可以从五个可选验证器中进行选择。

请参见第 418 页的[表 23-9](#)。

每个可选验证器所接受的字符类型取决于数据标识符。

请参见第 434 页的“[可选验证器的可接受字符](#)”。

注意：可选验证器仅适用于您正在配置的策略实例；它们不适用于整个系统。

表 23-9 可用于策略实例的可选验证器

可选验证器	说明
需要开始字符	对匹配数据项的开始（前导）字符进行匹配。 例如，对于加利福尼亚驾驶执照数据标识符，可能要求开始字符为字母 C。在此示例中，引擎匹配执照号码 C6457291。 请参见第 434 页的“ 可选验证器的可接受字符 ”。
需要结束字符	对匹配数据项的结束（尾随）字符进行匹配。 请参见第 434 页的“ 可选验证器的可接受字符 ”。
排除开始字符	从匹配中排除匹配数据的开始（前导）字符。 请参见第 434 页的“ 可选验证器的可接受字符 ”。

可选验证器	说明
排除结束字符	从匹配中排除匹配数据项的结束（尾随）字符。 请参见第 434 页的“ 可选验证器的可接受字符 ”。
查找关键字	匹配除了匹配数据项之外的一个或多个关键字或关键短语。 必须在与数据标识符内容所在的同一邮件组件中检测到关键字，才能报告匹配。 请参见第 419 页的“ 关于数据标识符的跨组件匹配 ”。 此可选验证器接受任何字符（数字、字母和其他字符）。 请参见第 434 页的“ 可选验证器的可接受字符 ”。

关于数据标识符的跨组件匹配

数据标识符支持组件匹配。这意味着您可以配置数据标识符来对一个或多个邮件组件进行匹配。然而，如果数据标识符实施验证器（可选或必需），例如查找关键字，验证的数据和匹配的数据必须存在于同一组件才能触发或排除事件。

请参见第 294 页的“[关于可以匹配的邮件组件](#)”。

例如，考虑实施小宽度版本的美国社会安全号数据标识符 (SSN) 的情景。此数据标识符可以对各种 9 数字模式进行检测，并使用关键字验证器缩小检测范围。（列表中的关键字和短语为“社会安全号、ssn、ss#”）。如果检测引擎收到的邮件的号码模式为 123-45-6789、关键字为“社会安全号”且这两个数据项均包含在邮件附件组件中，则检测引擎将会报告匹配项。然而，如果附件包含号码，但正文包含关键字验证器，则检测引擎不会将其视为匹配项。

请参见第 428 页的“[配置“内容匹配数据标识符”条件](#)”。

关于修改数据标识符

可以修改数据标识符以符合您的要求。可以修改系统定义的数据标识符，以及所创建的任何自定义数据标识符。您对数据标识符所做的任何修改会在系统范围内生效。这意味着修改将应用于声明修改的数据标识符的任何策略。

请参见第 437 页的“[修改和创建数据标识符](#)”。

修改系统定义的数据标识符最常见的用例是编辑接受数据输入的验证器的数据输入。例如，如果数据标识符实现“查找关键字”验证器，您可能要从关键字列表中添加或删除值。

请参见第 438 页的“[编辑所需的验证器输入](#)”。

另一个用例可能涉及将验证器添加到数据标识符或从数据标识符中删除验证器，或更改一个或多个由数据标识符定义的模式。

数据标识符一经修改，便无法自动恢复到其原始配置。在修改系统数据标识符前，应考虑对其进行手动克隆。

请参见第 438 页的“[在修改系统数据标识符之前手动克隆它](#)”。

系统不会将已修改的数据标识符包含在作为模板导出的策略中。修改系统数据标识符前，请导出对其进行声明的任何策略。

关于数据标识符模式

数据标识符实施模式以匹配数据。数据标识符模式语法与正则表达式语言类似，但具有更多限制。例如，数据标识符模式语法不支持某些正则表达式功能，包括分组、前瞻和回望表达式以及许多特殊字符（特别是点“.”字符）。此外，系统只允许在数据标识符模式中使用 ASCII 字符。

请参见第 420 页的“[关于数据标识符的模式语言限制](#)”。

编辑系统数据标识符时，系统将显示模式以供查看和编辑。已为精确内容匹配调整并优化了系统定义的数据标识符模式。

请参见第 430 页的“[选择系统数据标识符宽度](#)”。

此外，您可以创建自定义数据标识符，在这种情况下必须实施至少一种模式。了解如何编写模式的最佳方法是检查系统定义的数据标识符模式。

请参见第 440 页的“[实施模式以匹配数据](#)”。

关于数据标识符的模式语言限制

数据标识符模式语言是正则表达式词典的一个有限子集。数据标识符模式语言并非支持所有的正则表达式字符和构造。转换成数据标识符模式的正则表达式模式将需要进行一些语法上的修改。

下表列出了正则表达式与数据标识符模式语言之间的已知差异。

表 23-10 数据标识符模式语言限制

字符	说明
*	不支持将星号 (*)、竖线 () 和句点 (.) 字符用于数据标识符模式。
.	
\w	\w 构造不能用于匹配下划线字符 (_)。

字符	说明
\s	\s 构造不能用于匹配空格字符；应改用实际空格。
\d	对于数字，请使用 \d 构造。
分组	分组仅在模式开头起作用，例如： \d{4} - 2049 不起作用；应改用 2049 - \d{4} \d{2} /19 \d{2} 不起作用；应改用 \d{2} /[1][9] \d{2} 允许在模式开头进行分组，例如在信用卡数据标识符中。

关于验证器

验证器是应用于与数据标识符模式进行匹配的数据的验证检查。验证器有助于缩小检测范围和减少误报。许多验证器允许数据输入。例如，关键字验证器允许您输入关键字的列表。

请参见第 421 页的 [表 23-11](#)。

修改数据标识符时，可以编辑接受数据的任何验证器的输入值。下表中名称旁边带有星号 (*) 标记的验证器需要数据输入。

请参见第 438 页的“[编辑所需的验证器输入](#)”。

修改数据标识符时，可以添加和删除数据验证器。创建自定义数据标识符时，可以配置一个或多个验证器。系统还允许您创建自定义脚本验证器以定义自己的验证检查。

请参见第 441 页的“[选择所需的数据验证器](#)”。

表 23-11 可用于系统数据标识符和自定义数据标识符的验证器

验证器	说明
ABA 校验和	每个 ABA 汇款路径号码必须以下列两个数字开头：00-15、21-32、61-72、80，并通过 ABA 特定的位置权重校验和。
高级 KRRN 验证	验证第 3 个数字和第 4 个数字是否为有效月份，第 5 个数字和第 6 个数字是否为有效日，以及校验和是否匹配校验数位。
高级 SSN	验证器将在所有组中检查 SSN 是否包含零，地区号码（第一组）是否小于 773 且不为 666，组之间的分隔符是否相同，号码不是由全部相同的数字组成，且该号码未保留供通知使用（123-45-6789, 987-65-432x）。
澳大利亚税务验证检查	计算校验和并根据校验和对模式进行验证
基本 SSN	执行最小 SSN 验证。

验证器	说明
荷兰税号检查	执行荷兰税号检查。
中国 ID 校验和验证器	计算校验和并根据校验和对模式进行验证
意大利税号控制键检查	计算该控制键并检查其是否有效。
Cusip 验证	验证器将检查无效的 CUSIP 范围并计算 CUSIP 校验和（Modulus 10 Double Add Double 算法）。
自定义脚本*	输入自定义脚本，对此数据标识符宽度的模式匹配进行验证。 请参见第 442 页的“ 实施自定义脚本验证器 ”。
DNI 控制键检查	计算该控制键并检查其是否有效。
重复数字	保证数字字符串不全相同。
确切匹配*	输入一个逗号分隔值列表。如果这些值是数字，则不要输入任何短横线或其他分隔符。每个值可以具有任意长度。
排除开始字符*	输入一个逗号分隔值列表。如果这些值是数字，则不要输入任何短横线或其他分隔符。每个值可以具有任意长度。
排除开始字符*	输入一个逗号分隔值列表。如果这些值是数字，则不要输入任何短横线或其他分隔符。每个值可以具有任意长度。
排除确切匹配*	输入一个逗号分隔值列表。每个值可以具有任意长度。
排除前缀*	输入一个逗号分隔值列表。每个值可以具有任意长度。
排除后缀*	输入一个逗号分隔值列表。每个值可以具有任意长度。
查找关键字*	输入一个逗号分隔值列表。每个值可以具有任意长度。
香港特别行政区 ID	计算校验和并根据校验和对模式进行验证
INSEE 控制键	验证器将计算 INSEE 控制键，并将其与模式的最后两个数字进行比较。
IP 基本检查	每个 IP 地址必须符合格式 x.x.x.x，且每个号码必须小于 256。
IP 八位字节检查	每个 IP 地址必须符合格式 x.x.x.x，每个号码必须小于 256，且任何 IP 地址都不能仅包含单个数字的号码 (1.1.1.2)。
IP 保留范围检查	检查 IP 地址是否属于任何 Bogons 范围。若是如此，则匹配项无效。
Luhn 检查	验证器将计算 Luhn 校验和，每个加拿大保险号都必须通过该验证。

验证器	说明
Mod 97 验证器	计算完全匹配项的 ISO 7064 Mod 97-10 校验和。
无验证	不执行验证。
数字分隔符	通过检查周围的字符验证匹配。
需要开始字符*	输入一个逗号分隔值列表。如果这些值是数字，则不要输入任何短横线或其他分隔符。每个值可以具有任意长度。
需要结束字符*	输入一个逗号分隔值列表。如果这些值是数字，则不要输入任何短横线或其他分隔符。每个值可以具有任意长度。
新加坡 NRIC	计算新加坡 NRIC 的校验和，并根据该校验和对模式进行验证。
SSN 地区组号码	对于给定的地区号码（第一组），并非所有的组号码（第二组）都可由 SSA 分配。验证器将排除包含无效组号码的 SSN。
瑞士 AHV	瑞士 AHV Modulus 11 校验和。
中国台湾 ID	中国台湾 ID 校验和。
英国驾照	每个英国驾照必须包括 16 个字符，第 8 和第 9 位置的数字必须大于 00 且小于 32。
英国 NHS	英国 NHS 校验和。

关于自定义数据标识符

您可以定义自己的数据标识符。要创建自定义数据标识符，请实施一个或多个检测模式，选择一个或多个数据验证器（可选），提供数据输入（如果验证器需要）并选择一个数据规范化程序。

配置完成后，策略作者可以在一个或多个策略中使用自定义数据标识符。

请参见第 439 页的“[实施自定义数据标识符](#)”。

表 23-12 自定义数据标识符的组件

组件	说明
模式	定义一个或多个正则表达式模式，各模式之间以换行符分隔。
验证器	添加或删除验证器以对由模式检测到的数据执行验证检查。
数据条目	为需要数据输入的任何验证器提供逗号分隔的数据值。
规范化程序	选择一个规范化程序，在对数据进行匹配之前将其标准化。

关于数据规范化程序

创建自定义数据标识符时，您必须选择一个规范化程序以使模式检测到的数据符合验证器所需的格式。[表 23-13](#) 列出并说明了您可以为自定义数据标识符实施的规范化程序。

注意：不能修改系统定义的数据标识符的规范化程序。

表 23-13 可用的数据规范化程序

规范化程序	说明
数字	仅允许数字字符。
数字和字母	允许字母数字字符。
小写	仅允许字母，需规范化为小写形式。
SWIFT 代码	代码必须符合 SWIFT 要求。
不执行任何操作	在用户输入数据时，不对数据进行规范化和评估。

关于数据标识符配置

可以配置下列三种类型的数据标识符：

- 实例 - 在策略级别定义
- 已修改 - 在系统级别配置
- 自定义 - 在系统级别创建

您实施的数据标识符的类型取决于您的业务要求。对于大多数用例，使用未修改的、系统定义的数据标识符配置策略实例足以用来准确检测数据丢失。如果需要，可以通过修改系统定义的数据标识符来扩展它，或者可以实施一个或多个自定义数据标识符来检测唯一数据。

注意：系统会导出策略模板中已修改的和自定义的数据标识符。系统还导出对系统数据标识符的引用。导入策略模板的目标系统提供实际的数据标识符。

在策略实例级别完成的数据标识符配置特定于该策略。

请参见第 428 页的“[配置“内容匹配数据标识符”条件](#)”。

表 23-14 策略实例配置选项

在策略级别可选	不可配置
<ul style="list-style-type: none"> ■ 宽度 可以在实例级别实施数据标识符支持的任何宽度。 ■ 可选验证器 可以在实例级别选择一个或多个可选验证器。 	<ul style="list-style-type: none"> ■ 模式 不能在实例级别修改匹配模式。 ■ 活动验证器 不能在实例级别修改、添加或删除所需的验证器。

系统允许您修改系统定义的数据标识符，但您不能删除它们。您对系统定义的数据标识符的配置所做的任何修改都将在系统范围内生效。这意味着这些修改会应用到当前正在声明数据标识符或随后声明数据标识符的任何策略。

请参见第 437 页的“[修改和创建数据标识符](#)”。

表 23-15 系统数据标识符修改选项

在系统级别可修改	不可配置
<ul style="list-style-type: none"> ■ 模式 可以在系统级别编辑一个或多个数据标识符模式。 ■ 活动验证器 可以在系统级别添加或删除所需的验证器。 ■ 数据条目 可以为系统数据标识符编辑活动验证器的输入。 	<ul style="list-style-type: none"> ■ “名称”、“说明”和“类别” 不能修改系统数据标识符的名称、说明或类别。 ■ 宽度 不能为系统数据标识符定义新检测宽度，只能修改现有宽度。 ■ 可选验证器 不能在系统级别定义可选验证器。只能在策略级别配置可选验证器。 ■ 数据规范化程序 不能修改由系统数据标识符实施的数据规范化程序的类型。 ■ 删除 不能删除系统数据标识符。

可以创建和删除一个或多个自定义数据标识符。自定义数据标识符可以跨策略使用。在系统级别对自定义数据标识符所做的更改会影响当前正在声明自定义数据标识符或随后声明自定义数据标识符的任何策略。

请参见第 439 页的“[实施自定义数据标识符](#)”。

表 23-16 自定义数据标识符实施选项

在自定义级别可配置	不可配置
<ul style="list-style-type: none"> ■ “名称”和“说明” <p>必须为自定义数据标识符提供唯一名称。</p> <p>最好为自定义数据标识符提供说明。可以在修改自定义数据标识符时更改它的名称或说明。</p> ■ 模式 <p>必须至少定义一种模式，自定义数据标识符才能有效。</p> ■ 活动验证器 <p>可以向自定义数据标识符添加一个或多个所需的验证器。</p> ■ 数据条目 <p>可以编辑接受数据输入的活动验证器的输入。</p> ■ 数据规范化程序 <p>在定义自定义数据标识符时，必须选择数据规范化程序。</p> 	<ul style="list-style-type: none"> ■ 类别 <p>系统将自定义数据标识符分配到“自定义”类别。不能更改此设置。</p> ■ 宽度 <p>系统将自定义数据标识符分配到“宽”规则宽度。不能更改此设置。</p> ■ 可选验证器 <p>自定义数据标识符支持所有可选验证器，但可选验证器是在策略实例级别配置的。</p>

关于数据标识符的唯一匹配项计数

使用 Symantec Data Loss Prevention 11.6 版或更高版本时，如果您定义一条新的数据标识符规则，“对所有唯一匹配项进行计数”是对匹配项进行计数的默认方法。如名称所示，此选项只会对唯一的模式匹配项进行计数。

如果您只想检测唯一模式的存在情况，而不想检测每一个匹配的模式，则唯一匹配项计数功能很有用。例如，您可以使用唯一匹配项计数功能在文档中包含 10 个或更多个唯一社会安全号时触发事件。在这种情况下，如果文档包含同一个社会安全号的 10 个实例，这项策略不会触发事件。

下表介绍了唯一匹配项计数功能的特征。

表 23-17 唯一匹配项计数功能的特征

唯一匹配项计数功能的特征	说明
第一个匹配项是唯一的	<p>唯一匹配项是指在邮件组件中找到的第一个匹配项。</p> <p>请参见第 294 页的“关于可以匹配的邮件组件”。</p>
针对每个唯一匹配项更新匹配项计数	每有一个唯一模式匹配项，匹配项计数就会增加 1。

唯一匹配项计数功能的特征	说明
仅突出显示唯一匹配项	不会对重复的匹配项进行计数，也不会将它们突出显示在“事件快照”屏幕上。请参见第 715 页的“ 补救事件 ”。
唯一性指的是邮件组件范围内的唯一性	例如，如果同一个 SSN 既出现在邮件正文中又出现在附件中，则会生成二个唯一匹配项，而不是一个。这是因为在单独的邮件组件中检测到的每个实例。
包含数据标识符和关键字邻近条件的复合规则	在一条既包含数据标识符条件又包含指定了关键字邻近逻辑的关键字条件的复合规则中，报告的匹配项不是第一个找到的匹配项，而是在关键字邻近范围实例内的第一个匹配项。
不具有向后兼容性	唯一匹配项计数功能仅适用于使用 11.6 版或更高版本 Enforce Server 配置的策略。另外，只有 11.6 版或更高版本的 Detection Server 和 DLP Agent 才可以运行包含唯一匹配项计数功能的策略。 请参见第 436 页的“ 对数据标识符进行唯一匹配项计数 ”。

请参见第 428 页的“[配置“内容匹配数据标识符”条件](#)”。

关于更改随机化美国 SSN

在 2009 年，卡内基美隆大学 (Carnegie Mellon University) 的研究员发表了一篇研究论文，帮助他们能够根据出生地和出生日期，准确合理地猜出某人的社会安全号码 (SSN)。为了响应该情况以及大众对身份盗用日益增加的关切，美国政府社会安全管理局 (SSA) 开始开发新的方案来核发 SSN。

从 2011 年 6 月 25 日开始，SSA 会利用这个新的方案开始核发“随机化 SSN”。高组号码 (SSN 的第二部分) 不再对应于地区号码 (SSN 的第一部分)。此外，地区号码的范围现在将提升为 899 (而非 773)。

所有存储、处理或传输 SSN 的组织都会受到 SSN 随机化更改的影响。可能会在近期受影响的行业包括金融服务、保险、医疗保健、教育和政府。这包括在美国使用 SSN 数据标识符监视 SSN 的大多数 Symantec Data Loss Prevention 客户。

新的随机化方法适用于 2011 年 6 月 25 日当日及以后取得核发 SSN 的个人，这在 Symantec Data Loss Prevention 中将需要一个新的数据标识符 (DI)。这不影响、也不适用于现有的 SSN。短期漏报风险为低到中，因为随机化主要适用至新生儿、归化入籍公民和临时办公人员、学生与观光客。

若要应对随机化的更改，现有 Symantec Data Loss Prevention 客户应实施新的自定义 DI，用于检测根据 SSA 的新“随机化”结构所核发的 SSN。

请参见第 580 页的“[美国 SSN - 随机化自定义数据标识符 \(DI\)](#)”。

请参见第 582 页的“[使用美国 SSN - 随机化自定义 DI 的建议](#)”。

请参见第 580 页的“[美国 SSN - 随机化自定义数据标识符 \(DI\)](#)”。

管理和添加数据标识符

“管理” > “策略” > “数据标识符” 屏幕列出了所有数据标识符，包括系统定义的和自定义的数据标识符。可以在此屏幕上管理和修改现有数据标识符以及添加新的数据标识符。

请参见第 414 页的[“关于数据标识符”](#)。

表 23-18 管理数据标识符

操作	说明
编辑数据标识符。	从列表中选择数据标识符以修改它。 请参见第 430 页的 “选择系统数据标识符宽度” 。 请参见第 419 页的 “关于修改数据标识符” 。 请参见第 437 页的 “修改和创建数据标识符” 。
定义自定义数据标识符。	单击“添加数据标识符”以创建自定义数据标识符。 请参见第 423 页的 “关于自定义数据标识符” 。 请参见第 439 页的 “实施自定义数据标识符” 。
排序并查看数据标识符。	列表按“名称”的字母顺序排序。 您还可以按“类别”排序。 左侧的铅笔图标表示数据标识符是从其原始状态修改的或者数据标识符是自定义的。
删除数据标识符。	单击右侧的 X 图标以删除数据标识符。 系统不允许您删除系统数据标识符。您只能删除自定义数据标识符。

配置“内容匹配数据标识符”条件

您可以在策略检测规则和例外中配置“内容匹配数据标识符”条件。

请参见第 414 页的[“关于数据标识符”](#)。

表 23-19 配置“内容匹配数据标识符”条件

步骤	操作	说明
步骤 1	向策略添加数据标识符规则或例外，或者配置现有的规则或例外。	<p>在“添加检测规则”或“添加例外”屏幕上选择“内容匹配数据标识符”条件。</p> <p>请参见第 332 页的“将规则添加至策略中”。</p> <p>请参见第 340 页的“向策略中添加例外”。</p>
步骤 2	选择数据标识符。	<p>从列表中选择数据标识符并单击“下一步”。</p> <p>请参见第 415 页的“可用的系统数据标识符”。</p>
步骤 3	选择检测的“宽度”。	<p>使用宽度选项可缩小检测范围。</p> <p>请参见第 417 页的“关于数据标识符宽度”。</p> <p>“宽”为默认设置，用于检测最宽泛的一组匹配项。中宽度和小宽度（如果可用）用于检查其他条件并检测较少的匹配项。</p> <p>请参见第 430 页的“选择系统数据标识符宽度”。</p>
步骤 4	选择并配置一个或多个“可选验证器”。	<p>可选验证器可限制匹配条件和减少误报。</p> <p>请参见第 418 页的“关于可选验证器”。</p>
步骤 5	配置“匹配计数”。	<p>选择希望计算匹配项的方式：</p> <ul style="list-style-type: none"> ■ 检查是否存在 不计算多个匹配项；对于一个或多个匹配项，将匹配数报告为 1。 ■ 计算所有匹配项 计算每个匹配项；指定报告事件所需的最小匹配项数。 请参见第 337 页的“配置匹配计数”。 ■ 对所有唯一匹配项进行计数 这是 11.6 版和更新版本的默认设置。 请参见第 426 页的“关于数据标识符的唯一匹配项计数”。 请参见第 436 页的“对数据标识符进行唯一匹配项计数”。
步骤 6	为“匹配位置”配置邮件组件。	<p>选择要匹配的一个或多个邮件组件。</p> <p>在端点上，检测引擎匹配整个邮件，而不是单个组件。</p> <p>请参见第 339 页的“选择匹配的组件”。</p> <p>如果数据标识符使用可选或必需的关键字验证器，则匹配的数据标识符内容所在的组件中必须存在该关键字。</p> <p>请参见第 419 页的“关于数据标识符的跨组件匹配”。</p>

步骤	操作	说明
步骤 7	配置“同时匹配”的其他条件。	<p>或者，您可以在“同时匹配”条件列表中“添加”一个或多个可用的其他条件。</p> <p>必须匹配复合规则或例外中的所有条件才能触发或排除事件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

选择系统数据标识符宽度

每个系统数据标识符都提供一个或多个检测宽度。当配置系统数据标识符实例时，或当修改系统数据标识符时，您可以选择要实施的宽度。并非所有的宽度选项对每个数据标识符均可用。

请参见第 417 页的[“关于数据标识符宽度”](#)。

注意：您无法更改系统数据标识符实施的规范化程序。当实施一个或多个可选验证器时，了解此信息是有帮助的。请参见第 434 页的[“可选验证器的可接受字符”](#)。

表 23-20 系统数据标识符宽度和规范化程序

数据标识符	宽度	规范化程序
ABA 汇款路径号码 请参见第 522 页的 “ABA 汇款路径号码数据标识符” 。	大 中 小	仅数字
澳大利亚医疗号码 请参见第 525 页的 “澳大利亚医疗号码数据标识符” 。	大	仅数字
澳大利亚税务号码 请参见第 525 页的 “澳大利亚税务号码数据标识符” 。	大	仅数字
荷兰税号 请参见第 526 页的 “荷兰税号数据标识符” 。	大	仅数字
加拿大社会保险号 请参见第 526 页的 “加拿大社会保险号码数据标识符” 。	大 中 小	仅数字

数据标识符	宽度	规范化程序
税号 请参见第 529 页的“ 意大利税号数据标识符 ”。	大	仅数字字母
信用卡磁条数据 请参见第 529 页的“ 信用卡磁条数据数据标识符 ”。	中	仅数字
信用卡号 请参见第 532 页的“ 信用卡号数据标识符 ”。	大 中 小	仅数字
CUSIP 号 请参见第 538 页的“ CUSIP 号码数据标识符 ”。	大 中 小	小写
驾驶执照号码 - 加利福尼亚州 请参见第 540 页的“ 驾驶执照号码 - 加利福尼亚州数据标识符 ”。	大 中	小写
驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州 请参见第 541 页的“ 驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州数据标识符 ”。	大 中	小写
驾驶执照号码 - 伊利诺斯州 请参见第 543 页的“ 驾驶执照号码 - 伊利诺斯州数据标识符 ”。	大 中	小写
驾驶执照号码 - 新泽西州 请参见第 544 页的“ 驾驶执照号码 - 新泽西州数据标识符 ”。	大 中	小写
驾驶执照号码 - 纽约州 请参见第 545 页的“ 驾驶执照号码 - 纽约州数据标识符 ”。	大 中	小写
法国国家统计局代码 请参见第 546 页的“ 法国国家统计局代码数据标识符 ”。	大	仅数字

数据标识符	宽度	规范化程序
香港特别行政区 ID 请参见第 547 页的“ 香港特别行政区 ID 数据标识符 ”。	大	小写
IBAN 中部 请参见第 548 页的“ IBAN 中部数据标识符 ”。	大	无
IBAN 东部 请参见第 549 页的“ IBAN 东部数据标识符 ”。	大	无
IBAN 西部 请参见第 552 页的“ IBAN 西部数据标识符 ”。	大	无
IP 地址 请参见第 554 页的“ IP 地址数据标识符 ”。	大 中 小	无
国家药品代码 请参见第 556 页的“ 国家药品代码 (NDC) 数据标识符 ”。	大 中 小	无
中华人民共和国 ID 请参见第 558 页的“ 中华人民共和国 ID 数据标识符 ”。	大	小写
新加坡 NRIC 请参见第 559 页的“ 新加坡 NRIC 数据标识符 ”。	大	小写
韩国居民登记号码 请参见第 559 页的“ 韩国居民登记号码数据标识符 ”。	大 中	仅数字
西班牙 DNI ID 请参见第 561 页的“ 西班牙DNIID 数据标识符 ”。	大	小写
SWIFT 代码 请参见第 561 页的“ SWIFT 代码数据标识符 ”。	大 小	SWIFT
瑞士 AHV 号码 请参见第 563 页的“ 瑞士 AHV 号码数据标识符 ”。	大	仅数字

数据标识符	宽度	规范化程序
中国台湾 ID 请参见第 563 页的“ 中国台湾 ID 数据标识符 ”。	大	无
英国驾照号 请参见第 564 页的“ 英国驾照号数据标识符 ”。	大 中	小写
英国选民登记号 请参见第 566 页的“ 英国选民登记号数据标识符 ”。	大	小写
英国国民保健服务 (NHS) 号 请参见第 567 页的“ 英国国民保健服务 (NHS) 号数据标识符 ”。	中 小	仅数字
英国国家保险号码 请参见第 569 页的“ 英国国家保险号码数据标识符 ”。	大 中 小	小写
英国护照号 请参见第 571 页的“ 英国护照号数据标识符 ”。	大 中 小	无
英国税号 请参见第 573 页的“ 英国税号数据标识符 ”。	大 中 小	无
美国个人纳税识别号 (ITIN) 请参见第 574 页的“ 美国个人纳税识别号 (ITIN) 数据标识符 ”。	大 中 小	仅数字
美国社会安全号 (SSN) 请参见第 577 页的“ 美国社会安全号 (SSN) 数据标识符 ”。	大 中 小	仅数字

配置可选验证器

实施可选验证器可缩小在策略实例中定义的数据标识符的范围。系统数据标识符和自定义数据标识符都支持可选验证器的配置。

请参见第 418 页的“[关于可选验证器](#)”。

可选验证器允许的输入类型（数字、字母、字符）取决于数据标识符。如果您输入不可接受的输入字符并尝试保存配置，则系统将报告错误。

例如，美国社会安全号(SSN)数据标识符仅接受数字。如果您配置“需要结束字符”可选验证器并提供字母输入，则将在尝试保存配置时收到以下错误：“对‘需要结束字符’验证器的输入不正确：列表包含非数字字符”。

请参见第 434 页的[表 23-21](#)。

配置可选验证器

1 针对您正在配置的数据标识符实例单击“可选验证器”标签旁边的加号。

请参见第 428 页的[“配置‘内容匹配数据标识符’条件”](#)。

2 选择一个或多个可选验证器。

请参见第 418 页的[“关于可选验证器”](#)。

3 为您选择的各个可选验证器提供所需输入。

每个值可以具有任意长度。使用逗号分隔多个值。

4 单击“保存”保存配置。

如果系统显示错误消息，请确保您已输入类型正确的所需字符输入。

请参见第 434 页的[表 23-21](#)。

可选验证器的可接受字符

每个可选验证器都要求您输入一些数据值。您必须输入适当类型的数据。

请参见第 418 页的[“关于可选验证器”](#)。

可选验证器所需的数据类型取决于数据标识符。大多数数据标识符/可选验证器对仅接受数字；还有一部分接受字母数字值，另有很少一部分接受任何字符。如果您输入不可接受的输入并尝试保存策略，则系统将报告错误。

请参见第 433 页的[“配置可选验证器”](#)。

注意：“查找关键字”可选验证器接受任何字符作为所有数据标识符的值。

表 23-21 可选验证器的可接受字符

数据标识符	需要结束字符	排除结束字符	需要开始字符	排除开始字符
美国社会安全号 (SSN)			仅数字	
加拿大社会保险号			仅数字	

数据标识符	需要结束字符	排除结束字符	需要开始字符	排除开始字符		
美国个人纳税识别号 (ITIN)	仅数字					
驾驶执照号码 - 加利福尼亚州	仅数字		任何字符 (规范化为小写形式)			
驾驶执照号码 - 伊利诺斯州	仅数字		任何字符 (规范化为小写形式)			
驾驶执照号码 - 新泽西州	仅数字		任何字符 (规范化为小写形式)			
驾驶执照号码 - 纽约州	仅数字					
驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州	仅数字		任何字符 (规范化为小写形式)			
信用卡号	仅数字					
ABA 汇款路径号码	仅数字					
CUSIP 号	仅数字					
SWIFT 代码	字母数字 (数字或字母)					
信用卡磁条数据	仅数字					
IBAN 西部	字母数字 (数字或字母)					
IBAN 中部	字母数字 (数字或字母)					
IBAN 东部	字母数字 (数字或字母)					
国家药品代码	仅数字					
澳大利亚医疗号码	仅数字					
IP 地址	任何字符					
税号	仅数字					
西班牙 DNI ID	仅数字					
荷兰税号	仅数字					
英国驾照号	字母数字 (规范化为小写形式)					
英国税号	仅数字					
英国护照号	仅数字					
英国国家保险号码	字母数字 (规范化为小写形式)					

数据标识符	需要结束字符	排除结束字符	需要开始字符	排除开始字符		
英国国民保健服务 (NHS) 号	仅数字					
英国选民登记号	仅数字		任何字符（规范化为小写形式）			
法国国家统计局代码	仅数字					
瑞士 AHV 号码	仅数字					
澳大利亚税务号码	仅数字					
中华人民共和国 ID	仅数字					
香港特别行政区 ID	仅数字					
新加坡 NRIC	仅数字					
韩国居民登记号码	仅数字					
中国台湾 ID	仅数字					

对数据标识符进行唯一匹配项计数

“对所有唯一匹配项进行计数”是使用 Symantec Data Loss Prevention 11.6 或更高版本创建的新数据标识符的默认选择项。

对于升级到 11.6 版或更高版本的系统，以及对于导入到 11.6 版系统的 11.6 版之前的数据标识符，会保留针对这项策略所配置的现有匹配项计数方法。若要利用唯一匹配项计数功能，您必须手动将现有数据标识符规则配置为使用唯一匹配项计数功能。如果将一项包含唯一匹配项数据标识符规则的策略部署至不是 11.6 版或更高版本的 DLP Agent，则 DLP Agent 不会加载这项策略。有关更多详细信息，请参阅《Symantec Data Loss Prevention 升级指南》。

配置唯一匹配项计数

- 在“管理”>“策略”>“策略列表”屏幕上，选择包含您要更新的数据标识符规则的策略。
- 在“配置策略”屏幕上，选择该数据标识符规则。
- 选择匹配项计数选项“对所有唯一匹配项进行计数”。
- 单击“确定”应用唯一匹配项计数配置更改。

5 单击“保存”保存策略更改。

6 测试唯一匹配项计数。

创建一个包含某个数据标识符模式的多个实例的事件，例如，在同一个邮件组件（如，在电子邮件附件）中同一社会安全号的多个实例。

在“事件快照”中，验证是否仅突出显示了唯一匹配项以及是否仅对其进行计数。

请参见第 426 页的[“关于数据标识符的唯一匹配项计数”](#)。

修改和创建数据标识符

您可以修改和创建数据标识符，包括模式、验证器和验证器输入。修改将传播到任何声明数据标识符的策略。不能重命名系统数据标识符。在修改系统数据标识符之前，请考虑手动创建克隆的副本。

请参见第 419 页的[“关于修改数据标识符”](#)。

表 23-22 修改和创建系统数据标识符

步骤	操作	说明
步骤 1	创建一个自定义数据标识符，或修改一个现有的数据标识符。	请参见第 439 页的 “实施自定义数据标识符” 。 如果您修改系统数据标识符，请单击加号以显示宽度并编辑该数据标识符。 请参见第 430 页的 “选择系统数据标识符宽度” 。
步骤 2	提供或编辑一种或多种“模式”。	您可以修改数据标识符提供的任何模式。 请参见第 440 页的 “实施模式以匹配数据” 。
步骤 3	编辑接受输入的任何验证器的数据输入。	请参见第 438 页的 “编辑所需的验证器输入” 。
步骤 4	根据需要添加或删除“验证器”。	请参见第 441 页的 “选择所需的数据验证器” 。
步骤 5	保存数据标识符。	单击“保存”保存修改。 保存数据标识符后，“数据标识符”屏幕上的图标指示标识符是从其原始状态修改的或者它是自定义的。 请参见第 428 页的 “管理和添加数据标识符” 。 注意： 单击“取消”不保存数据标识符。

步骤	操作	说明
步骤 6	在策略规则或例外中实施数据标识符。	请参见第 428 页的“ 配置“内容匹配数据标识符”条件 ”。

在修改系统数据标识符之前手动克隆它

Enforce Server 不提供克隆系统数据标识符的自动机制。

请参见第 419 页的“[关于修改数据标识符](#)”。

在您修改系统数据标识符之前，请考虑手动克隆它以便在需要时可以恢复为原始配置。至少，您应首先将策略导出为模板，然后再修改由该策略声明的任何系统数据标识符。

手动克隆系统数据标识符

- 1 查看要修改的数据标识符的原始配置。
- 2 创建自定义数据标识符。
请参见第 439 页的“[实施自定义数据标识符](#)”。
- 3 将原始数据标识符的配置复制到自定义数据标识符。
添加模式、验证器、任何数据输入以及规范化程序。
请参见第 430 页的“[选择系统数据标识符宽度](#)”。
- 4 保存自定义数据标识符。
- 5 修改自定义数据标识符以使其满足您的需要。

编辑所需的验证器输入

您可以在系统级别编辑所需的验证器接受的数据输入。并不是所有验证器都接受数据输入。

请参见第 421 页的“[关于验证器](#)”。

编辑所需的验证器输入

- 1 通过从“管理”>“策略”>“数据标识符”屏幕选择数据标识符来对它进行编辑。
- 2 选择要修改的“规则宽度”。
通常，中宽度和小宽度选项包括接受数据输入的验证器。
- 3 从“活动验证器”列表选择要编辑其输入的验证器。
例如，选择“[查找关键字](#)”。

- 4 在“说明和数据项”字段中编辑验证器的输入。
- 5 单击“更新验证器”保存您对验证器输入所做的更改。
单击“放弃更改”不保存更改。
- 6 单击“保存”保存数据标识符。

实施自定义数据标识符

您可以实施自定义数据标识符来检测唯一内容。要实施自定义数据标识符，您必须至少定义一个模式并选择数据规范化程序。验证器是可选的。

请参见第 423 页的[“关于自定义数据标识符”](#)。

当定义自定义数据标识符时，系统会默认将其指定为“大”宽度。然而，这不是限制，因为实际检测范围取决于您定义的模式和验证器。

表 23-23 实施自定义数据标识符

步骤	操作	说明
步骤 1	选择“管理>策略>数据标识符”。	“数据标识符”屏幕列出了系统中可用的所有数据标识符。
步骤 2	选择“添加数据标识符”。 为自定义数据标识符输入“名称”。 该名称必须是唯一的。 为自定义数据标识符输入“说明”。 默认情况下，将自定义数据标识符指定为“自定义”类别，并且无法更改。	
步骤 3	输入要匹配数据的一个或多个“模式”。 必须至少输入一个模式，自定义数据标识符才能有效。 通过换行符分隔多个模式。 请参见第 440 页的 “实施模式以匹配数据” 。	
步骤 4	选择“数据规范化程序”。 您必须选择数据规范化程序。 提供了以下规范化程序： <ul style="list-style-type: none">■ 数字■ 数字和字母■ 小写■ SWIFT 代码■ 不执行任何操作 如果您不希望规范化数据，请选择此选项。 请参见第 424 页的 “关于数据规范化程序” 。	

步骤	操作	说明
步骤 5	选择零个或多个“验证器”。	包括用于检查和验证模式匹配的验证器是可选的。 请参见第 441 页的 “选择所需的数据验证器” 。
步骤 6	“保存”自定义数据标识符。	单击屏幕左上方的“保存”。 定义并保存自定义数据标识符后，该标识符将按字母顺序显示在“数据标识符”屏幕上的数据标识符列表中。 要编辑自定义数据标识符，请从列表中选择该标识符。 请参见第 437 页的 “修改和创建数据标识符” 。 注意： 单击“取消”不保存自定义数据标识符。
步骤 7	在一个或多个策略中实施自定义数据标识符。	系统列出所有的自定义数据标识符，并显示在“内容匹配数据标识符”条件（位于“配置策略 - 添加规则”和“配置策略 - 添加例外”屏幕上）的“自定义”类别下。 请参见第 428 页的 “配置‘内容匹配数据标识符’条件” 。 您可以在策略实例级别为自定义数据标识符配置可选验证器。 请参见第 433 页的 “配置可选验证器” 。

实施模式以匹配数据

如果修改现有的数据标识符，您可以编辑其模式。如果创建自定义数据标识符，则必须实施至少一种模式。数据标识符模式是使用与正则表达式语言类似的语法实施的，不过有一些限制。此外，系统只允许在数据标识符模式中使用 ASCII 字符。

请参见第 420 页的[“关于数据标识符模式”](#)。

编辑或实施模式

- 1 查看要修改的数据标识符的模式。
请参见第 430 页的[“选择系统数据标识符宽度”](#)。
- 2 如果您要修改系统数据标识符，可以考虑克隆该数据标识符。
请参见第 438 页的[“在修改系统数据标识符之前手动克隆它”](#)。
- 3 在 Enforce Server 管理控制台上选择“管理”>“策略”>“数据标识符”。
- 4 选择要修改的数据标识符。
- 5 选择要修改的数据标识符的宽度。
通常情况下，不同的检测宽度对应的模式不同。

- 6 在“模式”字段，修改现有模式，或输入一个或多个新模式，以换行符分隔。实施数据标识符模式如同实施正则表达式一样。但是，很多正则表达式语法是不受支持的。
请参见第 420 页的[“关于数据标识符的模式语言限制”](#)。
- 7 单击“保存”保存数据标识符。

选择所需的数据验证器

Symantec Data Loss Prevention 提供一组完整的验证器来实现模式匹配的准确性。
请参见第 421 页的[“关于验证器”](#)。

修改数据标识符时，系统将向您显示数据标识符使用过的活动验证器。修改或创建数据标识符时，系统将向您显示系统定义的所有数据验证器以供选择。

注意：活动验证器允许并定义输入，而“可选验证器”是为特定数据标识符的任何运行时实例配置的验证器，二者不能混淆。可选验证器始终在实例级别可配置。而活动验证器只在系统级别可配置。

从左侧的“验证检查”列表中选择验证器，然后单击右侧的“添加验证器”。如果验证器需要输入，请使用以逗号分隔的列表提供所需数据，然后单击“添加验证器”。

请参见第 441 页的[“选择所需的数据验证器”](#)。

选择模式验证器

- 1 创建自定义数据标识符。
请参见第 439 页的[“实施自定义数据标识符”](#)。
- 2 在“验证器”部分，选择所需的验证器。
请参见第 421 页的[“关于验证器”](#)。
- 3 如果验证器不需要数据输入，请单击“添加验证器”。
验证器将添加到“活动验证器”列表。
- 4 如果验证器需要数据输入，请在“说明和数据项”字段输入数据值。
输入完值以后，单击“添加验证器”。
验证器将添加到“活动验证器”列表。

- 5 要删除验证器，请在“活动验证器”列表中选择该验证器，然后单击红色的 X 图标。
- 6 单击“保存”以保存数据标识符的配置。

实施自定义脚本验证器

通过自定义脚本验证检查，可以输入自定义脚本以验证模式匹配。要实施自定义验证器，请使用 Symantec Data Loss Prevention 脚本语言。

可以在您修改的系统数据标识符中或自定义数据标识符中实施自定义脚本验证器。

注意：有关使用 Symantec Data Loss Prevention 脚本语言的详细信息，请参考《Symantec Data Loss Prevention 检测自定义指南》。

实施自定义脚本验证器

- 1 修改现有的数据标识符或创建自定义数据标识符。
请参见第 439 页的[“实施自定义数据标识符”](#)。
- 2 从“验证检查”列表中选择“自定义脚本”验证器。
- 3 在“说明和数据项”字段中输入自定义脚本。
- 4 单击“添加验证器”将自定义验证器添加到“活动验证器”列表。
- 5 单击“保存”以保存数据标识符的配置。

数据标识符最佳做法

当调整配置以便使误报和漏报保持最少时，针对内容匹配数据标识符通常要求进行微调。当检测规则检测出非违规内容时，发生误报。当检测规则未检测出违规内容时，发生漏报。要正确配置数据标识符以匹配内容，需要正确处理漏报和误报之间的平衡关系。

配置“内容匹配数据标识符”条件的实例后，需要了解匹配项并调整配置以确保最佳数据匹配成功。

有时，要减少误报，不匹配“信封”邮件组件可能有用。包含在 HTTP 传输的邮件标头中的信息包含可触发错误数据标识符匹配的会话 ID。例如，某些社交媒体站点（例如 Facebook 和 LinkedIn）包含可以时常完全匹配 CCN/SSN 的会话 ID。

请参见第 300 页的[“关于获得精确检测结果”](#)。

在修改系统数据标识符或创建自定义标识符之前，请考虑以下最佳做法：

- 如果要修改系统数据标识符，请将其作为自定义数据标识符进行克隆，然后修改克隆的副本。

- 数据标识符不会作为策略模板的一部分导出。

导出的模板包含对在该策略中实施的每个数据标识符的引用。导入到目标系统时，模板会使用标识符引用来选择本地数据标识符。如果修改了系统数据标识符，导入时目标系统将无法识别该标识符。也可以将数据标识符添加到策略，然后在修改数据标识符之前将策略作为模板导出。最佳做法是引用系统数据标识符的文档，再手动将其克隆为自定义数据标识符，然后修改克隆的版本。以这种方式即可保留原始系统数据标识符的状态。

使用关键字匹配检测内容

本章节包括下列主题：

- [关于实施关键字匹配](#)
- [关于关键字邻近匹配](#)
- [关键字匹配示例](#)
- [关键字语法要求](#)
- [配置“内容匹配关键字”条件](#)
- [关键字匹配最佳做法](#)

关于实施关键字匹配

Symantec Data Loss Prevention 提供关键字匹配检测。关键字匹配使用由一个或多个关键字或短语构成的列表来检测数据丢失。检测引擎会针对列表中的每个关键字来检查邮件组件的匹配情况。

表 24-1 实施关键字匹配

关键字匹配功能	说明
全字或部分关键字和关键短语匹配。	以换行形式或逗号分隔每个关键字或短语。 请参见第 446 页的“ 关键字匹配示例 ”。
通配符星号 (*) 字符匹配。	匹配关键字末尾的通配符（仅限于全字模式）。 请参见第 446 页的“ 关键字匹配示例 ”。
关键字邻近匹配。	跨一系列关键字匹配。 请参见第 446 页的“ 关于关键字邻近匹配 ”。

关键字匹配功能	说明
查找关键字。	实施数据标识符中的一个或多个关键字以优化检测范围。 请参见第 414 页的“ 关于数据标识符 ”。
策略规则和例外。	您可以在策略规则和例外中实施关键字匹配。 请参见第 448 页的“ 配置“内容匹配关键字”条件 ”。
跨组件匹配。	关键字匹配检测一个或多个邮件组件。 请参见第 294 页的“ 关于可以匹配的邮件组件 ”。
关键字字典。	如果关键字字典较大，可以创建确切数据配置文件并对关键字列表编制索引。

关于关键字邻近匹配

使用关键字邻近方法，策略创建者可以定义一对关键字，并指定这对关键字之间的字范围。如果出现位于该范围内的字，便会触发匹配。例如，“内容匹配关键字”规则的实例可能会要求，任何时候，只要 confidential 与 information 出现在相距 10 个字的范围内，便触发匹配。

或者，您可以将“内容匹配关键字”规则用作检测例外，使用关键字邻近来排除指定距离内的匹配字。这种情况下，任何出现在相距 10 个字的距离内的 confidential 和 information 都会从匹配中排除。

注意：字间距（邻近值）不包括检测到的关键字。因此，如果字间距为 10，则允许邻近窗口有 12 个字。

请参见第 446 页的“[关键字匹配示例](#)”。

请参见第 448 页的“[配置“内容匹配关键字”条件](#)”。

关键字匹配示例

要实施关键字匹配，您可以输入一个或多个关键字或短语，中间用逗号或换行符隔开。您可以全字匹配或部分匹配，还可以指定区分大小写。星号(*)通配符可用于检测关键字后缀（仅在全字模式下）。

表 24-2 关键字匹配示例

关键字类型	关键字		匹配项	不匹配
关键字	confidential		confidential -confidential; ®"confidential" ®Confidential ®CONFIDENTIAL	confidentially (仅在全字模式下不匹配, 否则会匹配)
关键短语	internal use only		internal use only internal use ONLY (如果选中了不区分大小写)	internal use
关键字列表	由换行符分隔:	由逗号分隔:	hacks	hackers
	hack	hack, hacker,	hack	shack
	hacker	hacks	hacker	
带通配符的关键字	priv*		private privilege privy privity privs priv	prize prevent
关键字字典	account number, account ps, american express, americanexpress, amex, bank card, bankcard, card num, card number, cc #, cc#, ccn, check card, checkcard, credit card, credit card #, credit card number, credit card#, debit card, debitcard, diners club, dinersclub, discover, enroute, japanese card bureau, jcb, mastercard, mc, visa (等等...)		如果出现任何关键字或关键短语, 则会匹配数据: amex credit card mastercard	amx creditcard master card car

请参见第 448 页的“关键字语法要求”。

关键字语法要求

当您定义关键字规则时，系统会对照每个邮件组件评估条件列表中的每个关键字。调整关键字列表时，请考虑下面的一般性建议。

表 24-3 有关关键字列表的一般注意事项

行为	说明
引号	输入关键字或短语时请勿使用引号，因为会按字面解释引号，并且在匹配时会用到引号。
空格	系统会剔除关键字或关键短语前面及后面的空格。
是否区分大小写	您选择的区分大小写选项适用于列表中该条件的所有关键字。
复数和动词变形	所有复数和动词变形都必须专门列出。如果不胜枚举，请使用通配符（星号 [*]）检测关键字后缀（仅限于全字模式）。
关键字短语	您可以输入关键字短语，例如 socialsecurity number （不加引号）。系统会查找整个短语，而不会返回单个字词（例如， social 或 security ）的匹配条目。
关键字变体	系统只检测确切的关键字，不检测变体。例如，如果您指定 socialsecurity number 这一关键短语，则检测引擎不会匹配在字之间包含两个空格的短语。
匹配多个关键字	系统在关键字之间隐含了 OR。即，如果内容包含任意关键字（不必包含所有关键字），则该内容匹配。要执行 ALL（或者 AND）匹配，请在复合规则或例外中合并多个关键字条件。

配置“内容匹配关键字”条件

“内容匹配关键字”检测规则使您可以使用关键字和关键短语来匹配内容。

请参见第 445 页的“[关于实施关键字匹配](#)”。

您可以在策略规则和例外中实施关键字匹配条件。

请参见第 330 页的“[配置策略](#)”。

配置“内容匹配关键字”条件

1 向策略规则或例外添加新的关键字条件，或者修改现有的关键字条件。

请参见第 334 页的“[配置策略规则](#)”。

请参见第 342 页的“[配置策略例外](#)”。

2 配置关键字匹配参数。

请参见第 449 页的[表 24-4](#)。

3 保存策略。

表 24-4 配置“内容匹配关键字”条件

操作	说明
输入匹配类型。	选择希望关键字匹配： “区分大小写”还是“不区分大小写” 默认为不区分大小写。
选择关键字分隔符。	选择用于分隔多个关键字的关键字分隔符： “换行符”或“逗号”。 默认为换行符。
匹配任意关键字。	输入要匹配的关键字或关键短语。使用已选的分隔符（换行符或逗号）分隔多个关键字或关键短语条目。 您可以在任何关键字的结尾使用星号 (*) 通配符匹配该关键字中的一个或多个后缀字符。如果使用星号通配符，必须仅进行全字匹配。例如， confid* 关键字条目将匹配 confidential 和 confide ，但不匹配 confine 。只要关键字前缀匹配，检测引擎就使用通配符匹配其余字符。 请参见第 446 页的“ 关键字匹配示例 ”。

操作	说明
配置关键字邻近匹配（可选）。	<p>关键字邻近匹配允许您指定关键字对之间的检测范围。请参见第 446 页的“关于关键字邻近匹配”。</p> <p>实施关键字邻近匹配：</p> <ul style="list-style-type: none">■ 在规则生成器界面的“条件”部分中选择（选中）“关键字邻近匹配”选项。■ 单击“添加关键字对”。■ 输入关键字对。■ 指定“字间距”。 关键字之间的最大间距为 999，因为这受到“字间距”字段的长度（为 3 位数）的限制。字间距是检测到的关键字所独有的。例如，字间距 10 允许 12 个字的范围，包括构成关键字对的 2 个字。■ 重复该过程来添加其他关键字对。 系统连接多个关键字对条目（使用布尔运算符 OR），意味着检测引擎独立地评估每个关键字对。
匹配整个或部分关键字。	<p>选择“仅限全字”选项可仅匹配整个关键字。请参见第 446 页的“关键字匹配示例”。</p> <p>注意：如果您在列表中输入任何带有星号 (*) 通配符的关键字，则必须仅进行全字匹配。</p>
配置匹配条件。	<p>关键字匹配允许您指定希望计算条件匹配项的方式。</p> <p>选择以下选项之一：</p> <ul style="list-style-type: none">■ 检查是否存在 系统将所有匹配项报告为一个事件。■ 计算所有匹配项 系统将每个匹配项报告为一个事件（默认设置）。■ 仅报告至少具有_个匹配项的事件 系统将报告每个满足指定匹配阈值的匹配项。 <p>请参见第 337 页的“配置匹配计数”。</p>

操作	说明
选择要匹配的组件。	<p>关键字匹配检测支持邮件组件间的匹配。请参见第 339 页的“选择匹配的组件”。</p> <p>选择要匹配的一个或多个邮件组件：</p> <ul style="list-style-type: none"> ■ 信封 - 用于传输邮件的标头元数据 ■ 主题 - 邮件的电子邮件主题（仅适用于 SMTP） ■ 正文 - 邮件的内容 ■ 附件 - 附加至邮件或通过邮件传输的所有文件 <p>注意：在端点上，DLP Agent 匹配整个邮件，而不是单个组件。请参见第 294 页的“关于可以匹配的邮件组件”。</p>
还匹配一个或多个其他条件。	<p>选择此选项可创建复合条件。必须符合所有条件才能报告匹配项。您可以从列表中“添加”任何可用的条件。请参见第 344 页的“配置复合匹配条件”。</p>

请参见第 448 页的“[关键字语法要求](#)”。

关键字匹配最佳做法

进行关键字匹配检测时，请注意以下内容：

- 系统会检查输入内容是否包括了条件中的每一个关键字。
- 输入关键短语时，不要使用引号。因为检测规则会对引号逐字解释。（即，也要求对其进行匹配。）
- 关键字或关键短语前后的空白会被删除。
- 您选择的区分大小写选项适用于列表中该条件的所有关键字。
- 如果启用了仅全字匹配（默认选项），则仅在单词边界处匹配关键字（熟悉正则表达式的用户可使用 \W）。除 A-Z、a-z 和 0-9 之外的所有字符都被解释为单词边界。
- 如果启用了仅全字匹配（默认选项），则关键字必须至少包含一个字母数字字符（字母或数字）。忽略仅包含空白（如 ..）的关键字。
- 必须枚举复数和动词屈折变化。如果枚举的数量繁多，请考虑使用正则表达式规则。
- 您可以输入关键短语，例如“身份证号”（不包括引号）。系统会查找整个短语，不会返回个别字组（例如，身份或证）的匹配条目。

- 系统只检测确切的关键字，不检测变体。例如，如果您指定关键短语“社会安全号”，则检测引擎不会匹配在字之间包含两个空格的短语。
- 系统在关键字之间隐含了OR。即，如果内容包含任意关键字（不必包含所有关键字），则该内容匹配。要执行 ALL（或者 AND）匹配，请在复合规则或例外中合并多个关键字条件。
- 要匹配全部大量的关键字（关键字字典），请使用确切数据配置文件。

有时，您可能要保护一个较长的列表或关键字字典。例如项目代码名称的列表。在这种情况下，可以创建一个包含所有要保护的关键字的文件，其中每个关键字位于单独的一行（如同一个包含一列的表）。然后根据关键字数据源文件创建确切数据配置文件。定义策略时，可以选择配置文件，以便保护与定义的关键字匹配的数据。当您基于关键字字典添加 EDM 规则时，检测引擎会在各种语言中都排除许多常见字词。如果您使用关键字列表并且想要检测常见字词，请从 *DLP_home\Protect\config\stopwords* 目录中的对应文件中删除相应的字词。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

使用正则表达式检测内容

本章节包括下列主题：

- [关于正则表达式匹配](#)
- [配置“内容匹配正则表达式”条件](#)
- [关于编写正则表达式](#)
- [正则表达式检测最佳做法](#)

关于正则表达式匹配

正则表达式提供了一种用于识别文本字符串（如特定字符、单词或字符模式）的机制。

“内容匹配正则表达式”检测方法有助于匹配和排除没有系统提供的数据标识符的唯一数据类型。示例可能包括内部帐号和长度变化极大的数据类型，如电子邮件地址。

请参见第 453 页的[“配置“内容匹配正则表达式”条件”](#)。

配置“内容匹配正则表达式”条件

“内容匹配正则表达式”检测条件使您可以使用正则表达式检测和排除邮件内容。

请参见第 453 页的[“关于正则表达式匹配”](#)。

您可以在策略规则和例外中实施此条件。

请参见第 330 页的[“配置策略”](#)。

配置“内容匹配正则表达式”条件

1 向策略中添加“内容匹配正则表达式”条件，或者编辑现有的条件。

请参见第 334 页的[“配置策略规则”](#)。

请参见第 342 页的[“配置策略例外”](#)。

2 配置“内容匹配正则表达式”条件的参数。

请参见第 454 页的[表 25-1](#)。

3 保存策略配置。

表 25-1 “内容匹配正则表达式”的参数

操作	说明
匹配正则表达式。	<p>指定要匹配的正则表达式。</p> <p>请参见第 454 页的“关于编写正则表达式”。</p>
配置“匹配计数”。	<p>配置希望计算匹配项的方式。</p> <p>请参见第 337 页的“配置匹配计数”。</p> <p>如果存在一个或多个匹配项，“检查是否存在”将匹配数报告为 1。对于复合规则或例外，必须通过此方式配置所有条件。</p> <p>“计算所有匹配项”报告所有匹配项的总和；如果所有条件均使用此参数，则将应用此方式。</p>
匹配一个或多个邮件组件。	<p>通过选择要匹配的一个或多个邮件组件配置跨组件匹配。</p> <ul style="list-style-type: none"> ■ 信封 - 邮件标头、传输元数据。 ■ 主题 - 电子邮件主题（只适用于电子邮件）。 ■ 正文 - 邮件的内容。 ■ 附件 - 附加至邮件或通过邮件传输的所有文件的内容。 <p>请参见第 339 页的“选择匹配的组件”。</p> <p>注意：在端点上，无论任何单独选定的组件为何，DLP Agent 都会匹配整个邮件。请参见第 294 页的“关于可以匹配的邮件组件”。</p>
还匹配一个或多个其他条件。	<p>选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。</p> <p>您可以从列表中“添加”任何可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

关于编写正则表达式

尽管不能代替好的正则表达式教程，但以下提供了一些字符匹配的参考构造。

注意：数据标识符模式匹配基于正则表达式语法。但是，数据标识符模式并不支持下表中列出的所有正则表达式构造。请参见第 420 页的“[关于数据标识符模式](#)”。

表 25-2 正则表达式构造

正则表达式构造	说明
.	任意单个字符（换行符除外） 注意： 数据标识符模式不支持点(.)字符的使用。
\d	任意数字(0-9)
\s	任意空白字符
\w	任意字的字符(a-z、A-Z、0-9、_) 注意： 在数据标识符模式中实施时，\w 构造方法与下划线(_)字符不匹配。
\D	除数字外的任意字符
\S	除空白字符外的任意字符
[]	方括号内的元素为字符类（例如，[abc] 匹配 1 个字符：a、b 或 c）。
^	位于字符类的开头，表示否定（例如，[^abc] 匹配除了 a、b 或 c 以外的任意字符）。
+	位于正则表达式的后面，表示 1 个或多个（例如，\d+ 表示 1 个或多个数字）。
?	位于正则表达式的后面，表示 0 个或 1 个（例如，\d? 表示 1 个或没有数字）。
*	位于正则表达式的后面，表示任意数量（例如，\d* 表示 0 个、1 个或更多个数字）。
(?i)	位于正则表达式的开头，使其不区分大小写（默认情况下，正则表达式区分大小写）。
(?:)	将正则表达式组合在一起（?: 可以使性能略有提高）。
(?u)	使句点(.)甚至匹配换行符
	表示 OR（例如，A B 表示正则表达式 A 或正则表达式 B）。

请参见第 453 页的“[关于正则表达式匹配](#)”。

正则表达式检测最佳做法

请考虑在实施正则表达式检测前使用数据标识符。由于为提高准确性对数据标识符的模式进行了精确调整，因此数据标识符更有效。例如，如果要搜索社会安全号，请使用美国社会安全号 (SSN) 数据标识符，而不是正则表达式。

正则表达式对计算性能有较高的要求。如果添加正则表达式条件，请对系统进行一小时的观察。确保系统速度不会降低，且不存在误报。

请参见第 453 页的“[关于正则表达式匹配](#)”。

系统实施了重要的增强功能，可提高正则表达式的性能。要实现性能提高，前瞻和回望部分必须与一个支持的标准部分完全匹配。下表列出了此性能提高支持的标准前瞻和回望部分。如果任何一部分稍有不同，则该部分会作为正则表达式的一部分执行，性能没有任何提高。

表 25-3 前瞻和回望标准部分

操作	构建
前瞻	(?=(:[^-\w]) \$)
回望	(?<=(^ (?:[^)+\d][^-\w+])) 以及 (?<=(^ (?:[^)+\d][^-\w+]) \t))

请参见第 454 页的“[关于编写正则表达式](#)”。

检测文件属性

本章节包括下列主题：

- 关于实施文件属性匹配
- 关于文件类型检测
- 关于自定义文件类型识别
- 关于文件大小检测
- 关于文件名检测
- 使用表达式模式来匹配文件名
- 配置“邮件附件类型或文件类型匹配”条件
- 配置“邮件附件大小或文件大小匹配”条件
- 配置“邮件附件名或文件名匹配”条件
- 启用自定义文件类型检测
- 配置自定义文件类型签名条件
- 文件属性检测最佳做法

关于实施文件属性匹配

Symantec Data Loss Prevention 提供了检测邮件、文件和附件上下文的各种方法。您可以检测文件和附件的类型、大小和名称。您也可以使用这些方法基于文件和附件上下文从检测中排除这些文件和附件。

表 26-1 文件属性检测条件

检测条件	说明
邮件附件类型或文件类型匹配	按照类型检测或排除特定文件和附件。 请参见第 458 页的“ 关于文件类型检测 ”。 请参见第 460 页的“ 配置“邮件附件类型或文件类型匹配”条件 ”。
邮件附件大小或文件大小匹配	按照大小检测或排除特定文件和附件。 请参见第 459 页的“ 关于文件大小检测 ”。 请参见第 461 页的“ 配置“邮件附件大小或文件大小匹配”条件 ”。
邮件附件名或文件名匹配	按照名称检测或排除特定文件和附件。 请参见第 459 页的“ 关于文件名检测 ”。 请参见第 462 页的“ 配置“邮件附件名或文件名匹配”条件 ”。
自定义文件类型签名	检测或排除自定义文件类型。

关于文件类型检测

Symantec Data Loss Prevention 能标识 100 多种文件格式。

检测引擎不依靠文件扩展名进行匹配。例如，用户将.mp3文件扩展名更改为.doc，并通过电子邮件发送该文件。检测引擎会查看该文件的二进制签名，以确定它是 MP3 文件，而不考虑文件扩展名。

邮件附件类型和文件类型匹配的使用示例如下所示：

- 某类型的文档永远不会离开组织（例如 PGP 文档或 EXE 文件）。
- 某类型的匹配可能只在某类型的文档（例如 Word 文档）中发生。

有关配置的详细信息，请参考相关主题。

请参见第 460 页的“[配置“邮件附件类型或文件类型匹配”条件](#)”。

关于自定义文件类型识别

如果要检测的文件类型不是受支持的系统默认文件类型，通过 Symantec Data Loss Prevention 可以使用脚本检测自定义文件类型。

要检测自定义文件类型，请使用 Symantec Data Loss Prevention 脚本语言编写自定义脚本，该脚本检测您要保护的文件格式的二进制签名。默认情况下自定义文件类型检测处于禁用状态。要实施该检测方法，您需要在 Enforce Server 中启用它。

请参见第 463 页的“[配置自定义文件类型签名条件](#)”。

有关编写自定义文件类型脚本的详细信息，请参见《Symantec Data Loss Prevention 检测自定义指南》。

关于文件大小检测

Symantec Data Loss Prevention 提供邮件附件和文件大小匹配。检测基于正文和/或附件邮件组件，而非整个邮件。

例如，请考虑指定附件大小大于 50k 发生匹配的条件。具有 5k 的标题、10k 的正文和 55k 的附件的邮件是匹配的，因为检测的邮件组件为附件，在这种情况下，其大小已超过了 50k 阈值。而具有 5k 的标题、10k 的正文和 45k 的附件的邮件就不匹配，即使整个邮件大于 50K。

请参见第 461 页的“[配置“邮件附件大小或文件大小匹配”条件](#)”。

关于文件名检测

Symantec Data Loss Prevention 提供了邮件附件名和文件名匹配。此检测方法用于检测文件和附件的名称。

该检测引擎支持 DOS 模式匹配语法，可用来检测文件名，包括通配符。

表 26-2 用于文件名检测的 DOS 运算符

运算符	说明
.	使用点来分隔文件名和扩展名。
*	使用星号作为通配符来匹配任意数量的字符（包括一个也没有）。
?	使用问号来匹配单个字符。

请参见第 460 页的[表 26-3](#)。

请参见第 462 页的“[配置“邮件附件名或文件名匹配”条件](#)”。

使用表达式模式来匹配文件名

以下 DOS 模式匹配表达式作为配置“邮件附件”或“文件名”条件的示例提供。

表 26-3 文件名检测示例

示例

您输入的所有字符（DOS 运算符除外）完全匹配。

例如，要匹配以 ENG- 开头，其后为任意八个字符的 Word 文件名，可输入：ENG-?????????.doc

如果不确定该文件是否为 Word 文档，可输入：ENG-?????????.*

如果不确定 ENG- 后面有多少个字符，可输入：ENG-*.*

要匹配以 ENG- 开头的所有文件名和以 ITA- 开头的所有文件名，请输入：ENG-*.*,ITA-*（逗号分隔），或者可以用行距分隔文件名。

配置“邮件附件类型或文件类型匹配”条件

“邮件附件类型或文件类型匹配”检测条件对附件邮件组件的文件类型进行匹配或排除。

请参见第 458 页的[“关于文件类型检测”](#)。

您可以在策略规则和例外中配置此条件的实例。

请参见第 330 页的[“配置策略”](#)。

配置“邮件附件类型或文件类型匹配”条件

1 向策略规则或例外添加“邮件附件类型或文件类型匹配”条件，或编辑现有的条件。

请参见第 334 页的[“配置策略规则”](#)。

请参见第 342 页的[“配置策略例外”](#)。

2 配置“邮件附件类型或文件类型匹配”条件的参数。

请参见第 461 页的[表 26-4](#)。

3 单击“保存”保存该策略。

表 26-4 “邮件附件类型或文件类型匹配” 检测规则

操作	说明
选择文件类型。	<p>选择要匹配的所有格式。</p> <p>单击“全选”或“取消全选”来选择或取消选择所有格式。</p> <p>要选择特定类别中的所有格式（例如，所有文字处理格式），请单击小节标题。</p> <p>系统在您选择的所有文件类型中隐含了 OR 运算符。例如，如果选择 Microsoft Word 和 Microsoft Excel 文件类型附件，系统将检测附加了 Word 或 Excel 文档的所有文件，而不是检测同时具有两种附件类型的邮件。</p>
仅附件匹配。	<p>此条件仅匹配“邮件附件”组件。</p> <p>请参见第 294 页的“关于可以匹配的邮件组件”。</p>
还匹配一个或多个其他条件。	<p>选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。</p> <p>您可以从列表中“添加”所有可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

配置“邮件附件大小或文件大小匹配”条件

“邮件附件大小或文件大小匹配”条件对指定大小的匹配文件进行匹配或排除。

请参见第 459 页的[“关于文件大小检测”](#)。

您可以在策略规则和例外中配置此条件的实例。

请参见第 330 页的[“配置策略”](#)。

配置“邮件附件大小或文件大小匹配”条件

1 向策略添加“邮件附件大小或文件大小匹配”条件，或编辑现有的条件。

请参见第 334 页的[“配置策略规则”](#)。

请参见第 342 页的[“配置策略例外”](#)。

2 配置“邮件附件类型或文件类型匹配”条件的参数。

请参见第 462 页的[表 26-5](#)。

3 单击“保存”保存该策略。

表 26-5 “邮件附件大小或文件大小匹配”的参数

操作	说明
输入大小。	<p>要指定要匹配的附件的最小大小，请选择“超过”。</p> <p>要指定要匹配的附件的最大大小，请选择“少于”。</p> <p>输入一个数字，并选择度量单位：字节、千字节 (KB)、兆字节 (MB) 或千兆字节 (GB)。</p>
匹配正文或附件。	<p>选择作为匹配基础的下一个或两个邮件组件：</p> <ul style="list-style-type: none"> ■ 正文 - 邮件的内容。 ■ 附件 - 附加至邮件或通过邮件传输的所有文件。 <p>请参见第 339 页的“选择匹配的组件”。</p>
还匹配一个或多个其他条件。	<p>选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。</p> <p>您可以从列表中“添加”所有可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

配置“邮件附件名或文件名匹配”条件

“邮件附件名或文件名匹配”检测条件基于附加至邮件的文件名对邮件进行检测或排除。

请参见第 459 页的“[关于文件名检测](#)”。

您可以在策略规则和例外中配置此条件的实例。

请参见第 330 页的“[配置策略](#)”。

配置“邮件附件名或文件名匹配”条件

1 向策略添加“邮件附件名或文件名匹配”条件，或编辑现有的条件。

请参见第 334 页的“[配置策略规则](#)”。

请参见第 342 页的“[配置策略例外](#)”。

2 配置“邮件附件类型或文件类型匹配”条件的参数。

请参见第 463 页的[表 26-6](#)。

3 单击“保存”保存该策略。

表 26-6 “邮件附件名或文件名匹配”的参数

操作	说明
指定文件名。	<p>指定要匹配的文件名，使用 DOS 模式匹配语言表示文件名中的模式。</p> <p>使用逗号分隔多个匹配模式，或将其分别放在单独的行上。</p> <p>请参见第 459 页的“使用表达式模式来匹配文件名”。</p> <p>请参见第 334 页的“配置策略规则”。</p>
匹配附件。	<p>此条件仅匹配“邮件附件”组件。</p> <p>请参见第 294 页的“关于可以匹配的邮件组件”。</p>
还匹配一个或多个其他条件。	<p>选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。</p> <p>您可以从列表中“添加”所有可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

启用自定义文件类型检测

默认情况下，不启用自定义文件类型策略规则。要实施“自定义文件类型签名”条件，您必须首先启用它。

请参见第 458 页的“[关于自定义文件类型识别](#)”。

启用“自定义文件类型签名”规则

- 1 使用文本编辑器打开文件 C:\Vontu\Protect\config\Manager.properties
- 2 将以下选项设置为 true:
`com.vontu.manager.policy.showcustomscriptrule=true`
- 3 停止并重新启动 Vontu Manager 服务。
- 4 重新登录到 Enforce Server 管理控制台并添加一个新的空白策略。
- 5 添加一个新的检测规则或例外，在文件属性标题下面，会显示“自定义文件类型签名”条件。
- 6 使用自定义脚本配置条件。

请参见第 463 页的“[配置自定义文件类型签名条件](#)”。

配置自定义文件类型签名条件

自定义文件类型签名条件与您编写了脚本的自定义文件类型匹配。

请参见第 458 页的“[关于自定义文件类型识别](#)”。

您可以在策略规则和例外中实施自定义文件类型签名条件。

请参见第 330 页的“[配置策略](#)”。

配置自定义文件类型签名条件

- 1 将自定义文件类型签名条件添加到策略规则或例外，或编辑现有的条件。

请参见第 334 页的“[配置策略规则](#)”。

请参见第 342 页的“[配置策略例外](#)”。

- 2 配置自定义文件类型签名条件参数。

请参见第 464 页的[表 26-7](#)。

- 3 单击“保存”保存该策略。

表 26-7 自定义文件类型签名参数

操作	说明
输入脚本名称。	指定脚本的名称。此名称在策略中必须是唯一的。
输入脚本文件类型。	输入文件类型匹配签名脚本以检测自定义文件类型的二进制签名。 有关编写自定义脚本的详细信息，请参考《Symantec Data Loss Prevention 检测自定义指南》。
仅匹配附件。	此条件仅匹配“邮件附件”组件。 请参见第 294 页的“ 关于可以匹配的邮件组件 ”。
还匹配一个或多个其他条件。	选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。 您可以从列表中“添加”所有可用的条件。 请参见第 344 页的“ 配置复合匹配条件 ”。

文件属性检测最佳做法

实施文件属性检测时，请谨记下列注意事项：

- 文件类型识别不会破解文件和检测内容；只根据文件的二进制签名检测文件类型。要检测内容，请使用内容检测规则。
- 文件大小方法将同时计算正文和具有指定文件大小的任何附件。

检测网络事件

本章节包括下列主题：

- [关于对网络进行的协议监控](#)
- [配置用于网络检测的“协议监控”条件](#)

关于对网络进行的协议监控

Symantec Data Loss Prevention 提供了允许您根据通信传输方法检测网络邮件的协议检测方法。

Symantec Data Loss Prevention 支持根据主要 Internet 协议来检测事件，其中包括以下协议：

- 电子邮件/SMTP
- HTTP
- HTTP/SSL
- IM:MSN
- IM:AIM
- IM:Yahoo
- FTP
- NNTP

此外，您也可以添加自定义协议（如特定端口上的 TCP TAP）来检测网络事件。

请参见第 466 页的[“配置用于网络检测的“协议监控”条件”](#)。

请参见第 467 页的[“关于移动的协议监控”](#)。

配置用于网络检测的“协议监控”条件

“协议监控”条件提供用于匹配网络和移动事件协议的参数。

您可以在一个或多个策略检测规则和例外中实施“协议监控”条件的实例。

请参见第 330 页的[“配置策略”](#)。

表 27-1 配置“协议监控”条件的参数

操作	说明
添加或修改“协议或端点监控”条件。	<p>向策略规则或例外添加新的“协议或端点监控”条件，或者修改现有的规则或例外条件。</p> <p>请参见第 334 页的“配置策略规则”。</p> <p>请参见第 342 页的“配置策略例外”。</p>
选择一个或多个要匹配的协议。	<p>要检测网络或移动事件，请选择一个或多个“协议”。</p> <ul style="list-style-type: none"> ■ 电子邮件/SMTP - 简单邮件传输协议，一种在服务器之间发送电子邮件的协议。 ■ HTTP - 超文本传输协议，是支持万维网的基础协议。HTTP 定义了如何对邮件进行格式化和传输以及 Web 服务器和浏览器在响应各种命令时应采取什么操作。 ■ HTTPS/SSL - 安全套接字层上的超文本传输协议，是用于在客户端与服务器之间安全地发送数据的协议。 ■ IM:MSN - MSN 即时消息传送是一种通信服务，允许您创建可与别人聊天的私人聊天室。 ■ IM:AIM - AIM 即时消息传送。（仅限网络） ■ IM:Yahoo - Yahoo! 即时消息传送。（仅限网络） ■ FTP - 文件传输协议，是在 Internet 上使用的协议，用于在计算机之间传输文件。 ■ NNTP - 网络新闻传输协议，用于发送、分发和检索 Usenet 邮件。 ■ TCP:custom_protocol - 传输控制协议，用户定义的 TCP 流量。
配置端点监控。	请参见第 471 页的 “配置端点监控条件参数” 。
匹配整个邮件。	<p>“协议监控”条件匹配整个邮件，而不是单个邮件组件。</p> <p>默认情况下选择“信封”选项。您无法选择单个邮件组件。</p> <p>请参见第 294 页的“关于可以匹配的邮件组件”。</p>
还匹配一个或多个其他条件。	<p>选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。</p> <p>您可以从列表中“添加”所有可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

检测移动事件

本章节包括下列主题：

- [关于移动的协议监控](#)
- [配置移动监测的协议监控条件](#)

关于移动的协议监控

Symantec Data Loss Prevention 提供了“协议监控”检测方法，可以使用这种方法检测某些协议的基于移动的流量。

Symantec Data Loss Prevention 支持使用以下协议进行基于移动的检测：

- HTTP
- HTTP/SSL
- FTP

请参见第 466 页的[“配置用于网络检测的“协议监控”条件”](#)。

配置移动监测的协议监控条件

“协议监控”条件提供用于匹配网络和移动事件协议的参数。

您可以在一个或多个策略检测规则和例外中实施“协议监控”条件的实例。

请参见第 330 页的[“配置策略”](#)。

表 28-1 配置“协议监控”条件的参数

操作	说明
添加或修改“协议或端点监控”条件。	向策略规则或例外添加新的“协议或端点监控”条件，或者修改现有的规则或例外条件。 请参见第 334 页的 “配置策略规则” 。 请参见第 342 页的 “配置策略例外” 。
选择一个或多个要匹配的协议。	若要检测移动事件，请选择一个或多个“ 协议 ”。 <ul style="list-style-type: none">■ HTTP - 超文本传输协议，是支持万维网的基础协议。HTTP 定义了如何对邮件进行格式化和传输以及 Web 服务器和浏览器在响应各种命令时应采取什么操作。■ HTTPS/SSL - 安全套接字层上的超文本传输协议，是用于在客户端与服务器之间安全地发送数据的协议。■ FTP - 文件传输协议，是在 Internet 上使用的协议，用于在计算机之间传输文件。
配置端点监控。	请参见第 471 页的 “配置端点监控条件参数” 。
匹配整个邮件。	“协议监控”条件匹配整个邮件，而不是单个邮件组件。 默认情况下选择“ 信封 ”选项。您无法选择单个邮件组件。 请参见第 294 页的 “关于可以匹配的邮件组件” 。
还匹配一个或多个其他条件。	选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。 您可以从列表中“ 添加 ”所有可用的条件。 请参见第 344 页的 “配置复合匹配条件” 。

检测端点事件

本章节包括下列主题：

- [关于进行端点事件检测](#)
- [关于端点协议、目标和应用程序检测](#)
- [关于端点设备检测](#)
- [关于端点位置检测](#)
- [配置端点监控条件参数](#)
- [收集端点设备 ID](#)
- [管理及添加端点设备](#)
- [创建及修改端点设备配置](#)
- [配置“端点设备类或 ID”条件](#)
- [配置“端点位置”条件](#)
- [端点检测最佳做法](#)

关于进行端点事件检测

端点检测与安装了 Symantec DLP Agent 的端点计算机上的事件匹配。

请参见第 1130 页的[“关于 Endpoint Prevent 监视”](#)。

Symantec Data Loss Prevention 提供了多种方法来检测和排除端点事件，并提供了一系列响应规则对其进行响应。

请参见第 656 页的[“端点检测的响应规则”](#)。

表 29-1 检测端点事件

端点匹配条件	详细信息
端点监控	根据协议、目标或应用程序检测端点数据。 请参见第 470 页的“ 关于端点协议、目标和应用程序检测 ”。 请参见第 471 页的“ 配置端点监控条件参数 ”。
端点设备或类 ID	检测何时用户将端点数据移动到特定设备。 请参见第 470 页的“ 关于端点设备检测 ”。 请参见第 476 页的“ 配置“端点设备类或 ID”条件 ”。
端点位置	检测端点何时在企业网络内或企业网络外。 请参见第 471 页的“ 关于端点位置检测 ”。 请参见第 476 页的“ 配置“端点位置”条件 ”。

关于端点协议、目标和应用程序检测

在端点上，您可以根据传输协议（例如电子邮件(SMTP)、Web(HTTP)和文件传输(FTP)）检测数据丢失。

您还可以检测发生数据复制或移动的目标（例如CD/DVD驱动器、USB设备或剪贴板）上的端点数据丢失。

您可以为允许的使用情况创建例外。

请参见第 471 页的“[配置端点监控条件参数](#)”。

关于端点设备检测

Symantec Data Loss Prevention 允许您基于描述的设备元数据来检测或排除特定的端点设备。可以配置一个条件以允许端点用户将文件复制到特定的设备类，如来自单个制造商的 USB 驱动器。

请参见第 474 页的“[管理及添加端点设备](#)”。

例如，策略作者具有一组 USB 闪存驱动器，其序列号范围为 001 到 010。应该只允许这些闪存驱动器访问公司的端点计算机。策略管理员将序列号元数据添加到策略的例外中，以便策略适用于除序列号在 001-010 元数据内的驱动器之外的所有 USB 闪存驱动器。这样，设备元数据就可以只允许“可信设备”含有公司数据。

请参见第 474 页的“[创建及修改端点设备配置](#)”。

“端点设备类或 ID” 条件基于其定义检测特定的可移动存储设备。“端点监控” 条件中的“端点目标” 参数检测端点上的任何可移动存储设备。

请参见第 476 页的“[配置“端点设备类或 ID”条件](#)”。

关于端点位置检测

您可以根据端点的位置检测或排除事件。

使用“端点位置”检测方法，您可以选择仅当端点位于网络内还是位于网络外时检测事件。

例如，您可以将此条件配置为仅当用户位于公司网络外时匹配，因为您已有其他规则可用于检测网络事件。在这种情况下，实施“端点位置”检测方法将取得此结果。

请参见第 476 页的“[配置“端点位置”条件](#)”。

配置端点监控条件参数

端点监控条件匹配端点邮件协议、目标和应用程序。

您可以在一个或多个策略检测规则和例外中实施端点监控条件的实例。

请参见第 330 页的“[配置策略](#)”。

表 29-2 配置端点监控条件

操作	说明
添加或修改端点监控条件。	向策略规则或例外添加新的“协议或端点监控”条件，或者修改现有的规则或例外条件。 请参见第 334 页的“配置策略规则” 。 请参见第 342 页的“配置策略例外” 。

操作	说明
选择一个或多个要匹配的端点协议。	<p>要检测端点事件, 请选择一个或多个“端点协议”:</p> <ul style="list-style-type: none"> ■ 电子邮件/SMTP - 简单邮件传输协议, 一种在服务器之间发送电子邮件的协议。 ■ HTTP - 超文本传输协议, 是支持万维网的基础协议。HTTP 定义了如何对邮件进行格式化和传输以及 Web 服务器和浏览器在响应各种命令时应采取什么操作。 ■ HTTPS/SSL - 安全套接字层上的超文本传输协议, 是用于在客户端与服务器之间安全地发送数据的协议。 ■ IM:MSN - MSN 即时消息传递是一种通信服务, 允许您创建可与别人聊天的私人聊天室。 ■ IM:AIM - AOL 即时消息传递。 ■ IM:Yahoo - Yahoo! 即时消息传递。 ■ FTP - 文件传输协议是 Internet 上广泛使用的协议, 用于在计算机之间传输文件。
选择一个或多个网络协议。	<p>要检测网络事件, 请选择一个或多个“网络协议”。</p> <p>请参见第 466 页的“配置用于网络检测的“协议监控”条件”。</p>
选择一个或多个端点目标。	<p>要在用户在端点上移动数据时检测, 请选择一个或多个“端点目标”:</p> <ul style="list-style-type: none"> ■ 本地驱动器 - 检测本地磁盘上的事件。 ■ CD/DVD - 端点计算机上的 CD/DVD 刻录机。该目标可以是任意一种第三方 CD/DVD 刻录软件。 ■ 可移动存储设备 - 检测传输到任何通过 eSATA、FireWire 或 USB 连接的存储设备的数据。 ■ 复制到网络共享 - 检测传输到任何网络共享或远程文件访问的数据。 ■ 打印机/传真机 - 检测传输到与端点计算机连接的打印机或传真机的数据。该目标还可以是 print-to-file 文档。 ■ 剪贴板 - Windows 剪贴板, 用于在 Windows 应用程序之间复制和粘贴数据。
监控端点应用程序。	<p>要在端点应用程序访问文件时检测, 请选择“应用程序文件访问”选项。</p> <p>DLP Agent 会在应用程序访问敏感文件时监视应用程序。</p> <p>请参见第 1207 页的“关于应用程序监控”。</p> <p>DLP Agent 监控在“系统”>“代理”>“应用程序监控”屏幕上添加和配置的任何第三方应用程序。</p> <p>请参见第 1208 页的“添加应用程序”。</p>

操作	说明
匹配整个邮件。	DLP Agent 评估整个邮件，而不是单个邮件组件。 默认情况下选择“信封”选项。您不能选择其他邮件组件。 请参见第 294 页的 “关于可以匹配的邮件组件” 。
还匹配一个或多个其他条件。	选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。 您可以从列表中“添加”所有可用的条件。 请参见第 344 页的 “配置复合匹配条件” 。

请参见第 470 页的[“关于端点协议、目标和应用程序检测”](#)。

收集端点设备 ID

将设备元数据信息添加到 Enforce Server，并创建一个或多个策略检测方法用于检测或排除特定设备实例或设备类。系统支持使用正则表达式语法定义元数据。系统在补救期间将设备元数据显示在“事件快照”屏幕上。

请参见第 474 页的[“创建及修改端点设备配置”](#)。

系统定义设备实例或设备类所需的元数据是“设备实例 ID”。在 Windows 上，您可以从设备管理器获取“设备实例 ID”。

此外，Symantec Data Loss Prevention 还提供 DeviceID.exe 实用程序。可以使用此实用程序提取设备实例 ID 字符串。此实用程序还报告系统可以识别哪些设备用于检测。此实用程序适用于 Enforce Server 安装文件。

请参见第 1216 页的[“关于设备 ID 实用程序”](#)。

注意：Symantec Endpoint Protection (SEP) 也使用设备实例 ID。

获取设备实例 ID (在 Windows 上)

- 1 右键单击“我的电脑”。
- 2 选择“管理”。
- 3 选择“设备管理器”。
- 4 单击任何设备旁边的加号展开其设备实例的列表。
- 5 双击设备实例。或者，右键单击设备实例并选择“属性”。

6 在“**详细信息**”选项卡中查找“**设备实例 ID**”。

7 使用该 ID 创建设备元数据表达式。

请参见第 474 页的“[创建及修改端点设备配置](#)”。

请参见第 470 页的“[关于端点设备检测](#)”。

请参见第 474 页的“[管理及添加端点设备](#)”。

管理及添加端点设备

您可从“系统”>“代理”>“端点设备”屏幕管理现有的端点设备以及添加新的端点设备。

请参见第 470 页的“[关于端点设备检测](#)”。

表 29-3 管理端点设备

操作	说明
添加端点设备。	单击“添加设备”来定义新的端点设备。定义后，设备将添加到列表中。 请参见第 473 页的“ 收集端点设备 ID ”。
修改现有的端点设备配置。	要编辑设备定义，请选择设备行中的任何位置，或单击铅笔图标。 请参见第 474 页的“ 创建及修改端点设备配置 ”。
查看已配置的端点设备。	“端点设备”屏幕列出所有已配置的端点设备。 各列显示以下信息： <ul style="list-style-type: none"> ■ 设备名称 ■ 设备说明 ■ 设备定义 (Regex)
对端点设备进行排序。	可按名称、说明或定义对端点设备列表进行排序。

创建及修改端点设备配置

您可为特定端点检测配置一个或多个设备。配置设备表达式后，可在[一个或多个策略规则或例外](#)中实施端点设备类或 ID 条件来拒绝或允许对特定设备的使用。

请参见第 473 页的“[收集端点设备 ID](#)”。

创建及修改端点设备 ID 表达式

1 单击“添加设备”。

从“系统”>“代理”>“端点设备”屏幕执行此操作。

2 输入“设备名称”。

3 输入“设备说明”。

4 输入“设备定义”表达式。

设备定义必须符合正则表达式语法。

请参见第 475 页的[表 29-4](#)。

请参见第 454 页的[“关于编写正则表达式”](#)。

5 单击“保存”保存设备配置。

6 在检测规则或例外中实施“端点设备类或 ID”条件。

请参见第 476 页的[“配置“端点设备类或 ID”条件”](#)。

表 29-4 端点设备表达式示例

设备类和表达式示例

通用 USB 设备

USBSTOR\\DISK&VEN_SANDISK&PROD_ULTRA_BACKUP&REV_8\\.32\\3485731392112B52

iPod 常规

USBSTOR\\DISK&VEN_APPLE&PROD_IPOD&.*

Lexar 常规

USBSTOR\\DISK&VEN_LEXAR.*

光盘驱动器

IDE\\DISKST9160412ASG_____0002SDM1\\4&F4ACADA&0&0\\.0\\.0

硬盘驱动器

USBSTOR\\DISK&VEN_MAXTOR&PROD_ONETOUCH_II&REV_023D\\B60899082H___&0

Blackberry 常规

USBSTOR\\DISK&VEN_RIM&PROD_BLACKBERRY...&REV.*

移动电话

USBSTOR\\DISK&VEN_PALM&PROD_PRE&REV_000\\FBB4B8FF4CAEFEC1124DED689&0

请参见第 470 页的“[关于端点设备检测](#)”。

请参见第 474 页的“[管理及添加端点设备](#)”。

配置“端点设备类或 ID”条件

“端点设备类或 ID”条件允许您检测用户将端点数据移动到特定设备的时间。

您可以在一个或多个策略检测规则或例外中实施“端点设备类或 ID”条件。

请参见第 330 页的“[配置策略](#)”。

表 29-5 配置“端点设备类或 ID”条件

操作	说明
添加或修改“端点设备”条件。	<p>向策略规则或例外添加新的“端点设备类或 ID”条件，或修改现有的条件。</p> <p>请参见第 334 页的“配置策略规则”。</p> <p>请参见第 342 页的“配置策略例外”。</p>
选择一个或多个设备。	<p>当用户将数据从端点计算机移动到选定设备时，会匹配该条件。</p> <p>单击“创建端点设备”来定义一个或多个设备。</p> <p>请参见第 474 页的“创建及修改端点设备配置”。</p>
匹配整个邮件。	<p>DLP Agent 匹配整个邮件，而不是单个邮件组件。</p> <p>默认情况下选择“信封”选项。您无法选择其他组件。</p> <p>请参见第 294 页的“关于可以匹配的邮件组件”。</p>
还匹配一个或多个其他条件。	<p>选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。</p> <p>您可以从下拉菜单中“添加”任何可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

请参见第 470 页的“[关于端点设备检测](#)”。

请参见第 474 页的“[管理及添加端点设备](#)”。

配置“端点位置”条件

“端点位置”条件基于安装了 DLP Agent 的端点计算机的位置对端点事件进行匹配。

您可以在一个或多个策略检测规则和例外中实施“端点位置”条件的实例。

请参见第 330 页的“[配置策略](#)”。

表 29-6 配置“端点位置”检测条件

操作	说明
添加或修改“端点位置”条件。	向策略规则或例外添加新的“端点位置”检测条件，或者修改现有的策略规则或例外。 请参见第 334 页的“ 配置策略规则 ”。 请参见第 342 页的“ 配置策略例外 ”。
选择要监控的位置。	选择要监控的以下端点位置之一： <ul style="list-style-type: none">■ 在企业网络外 当端点计算机在企业网络外时，可选择此选项以检测或排除事件。■ 在企业网络内 当端点计算机在企业网络内时，可选择此选项以检测或排除事件。 此选项为默认选择。 请参见第 471 页的“ 关于端点位置检测 ”。
匹配整个邮件。	DLP Agent 评估整个邮件，而不是单个邮件组件。 默认情况下选择“信封”选项。无法选择其他邮件组件。 请参见第 294 页的“ 关于可以匹配的邮件组件 ”。
还匹配一个或多个其他条件。	选择此选项可创建复合条件。必须匹配所有条件才能触发或排除事件。 您可以从列表中“添加”所有可用的条件。 请参见第 344 页的“ 配置复合匹配条件 ”。

请参见第 471 页的“[关于端点位置检测](#)”。

端点检测最佳做法

实施端点检测时，请注意下列事项：

- 在端点上执行的任何检测方法与整个邮件匹配，而不是与单个邮件组件匹配。
- 不要将“Endpoint Prevent:通知”或“Endpoint Prevent:阻止”响应规则与双层检测方法组合使用，包括确切数据匹配、索引文档匹配或配置的（静态的）目录组匹配。如果这样做，系统将对策略检测和响应规则显示警告。

- 您可能经常将端点上的组和检测方法组合使用。请谨记，策略语言与检测和组方法之间是逻辑“与”关系，而类型相同的方法（例如两个规则）之间是逻辑“或”关系。

请参见第 297 页的“[关于检测服务器策略执行](#)”。

检测所述身份

本章节包括下列主题：

- [关于指定身份匹配](#)
- [配置“发送者/用户匹配模式”条件](#)
- [配置“接受者匹配模式”条件](#)
- [指定身份匹配最佳做法](#)

关于指定身份匹配

指定身份检测匹配来自电子邮件发送者和接受者、Windows 用户、IM 用户、URL 域和 IP 地址的邮件中的模式。

表 30-1 模式身份匹配示例

示例模式	匹配项	不匹配
fr、cu	发往 .fr (法国) 或 .cu (古巴) 地址的所有 SMTP 电子邮件。	发往扩展域名为 .com 而非 .fr 的法国公司的所有电子邮件。 通过基于 Web 的邮件应用程序（例如 Yahoo 邮件）发往 .fr 地址的所有 HTTP 发布内容。
company.com	发往特定域 URL (例如 symantec.com) 的所有 SMTP 电子邮件。	不是发往特定域 URL 的任何 SMTP 电子邮件。
3rdlevel.company.com	发往特定的第 3 级域 (例如 dlp.symantec.com) 的所有 SMTP 电子邮件。	不是发往特定的第 3 级域的任何 SMTP 电子邮件。

示例模式	匹配项	不匹配
bob@company.com	发往 bob@company.com 的所有 SMTP 电子邮件。 发往 BOB@COMPANY.COM (格式不区分大小写) 的所有 SMTP 电子邮件。	不是专门发往如下所示的 bob@company.com 的任何电子邮件: ■ sally@company.com ■ robert.bob@company.com ■ bob@3rdlevel.company.com
192.168.0.*	专门发往 192.168.0.[0-255] 的所有电子邮件、Web 或 URL 流量。 此结果假设 IP 地址映射到所需的域，例如 web.company.com。	注意: 如果 IP 地址不匹配，则改用一个或多个域 URL。

请参见第 480 页的“[配置“发送者/用户匹配模式”条件](#)”。

请参见第 482 页的“[配置“接受者匹配模式”条件](#)”。

配置“发送者/用户匹配模式”条件

“发送者/用户匹配模式”检测条件对所描述的用户和邮件发送者身份进行匹配。

您可以在策略检测规则或例外中使用此条件。

请参见第 479 页的“[关于指定身份匹配](#)”。

表 30-2 配置“发送者/用户匹配模式”条件

操作	说明
输入一个或多个发送者模式以匹配一个或多个邮件发送者。	<p>电子邮件地址模式:</p> <ul style="list-style-type: none"> ■ 要匹配特定电子邮件地址，请输入完整电子邮件地址: <code>sales@symantec.com</code> ■ 要匹配多个确切的电子邮件地址，请输入以逗号分隔的列表: <code>john.smith@company.com, johnsmith@company.com, jsmith@company.com</code> ■ 要匹配部分电子邮件地址，请输入一个或多个域模式: <ul style="list-style-type: none"> ■ 输入一个或多个顶级域扩展名，例如: <code>.fr、.cu、.in、.jp</code> ■ 输入一个或多个域名，例如: <code>company.com、symantec.com</code> ■ 输入一个或多个三级（或更低级）域名: <code>web.company.com、mail.yahoo.com、smtp.gmail.com、dlp.security.symantec.com</code>
	<p>Windows 用户名</p> <p>输入一个或多个 Windows 用户，例如: <code>john.smith、jsmith</code></p>
	<p>IM 屏幕名称</p> <p>输入在即时消息传递系统中使用的一个或多个 IM 屏幕名称，例如: <code>john_smith、jsmith</code></p>
	<p>IP 地址</p> <p>输入将映射到您要匹配的域的一个或多个 IP 地址，例如:</p> <ul style="list-style-type: none"> ■ 确切 IP 地址匹配，例如: <code>192.168.1.1</code> ■ 通配符匹配 - 星号 (*) 字符可以代替一个或多个字段，例如: <code>192.168.1.* 或 192.*.168.*</code>
匹配整个邮件。	<p>此条件匹配整个邮件。默认情况下选择“信封”选项。您无法选择任何其他邮件组件。</p> <p>请参见第 294 页的“关于可以匹配的邮件组件”。</p>
还匹配其他条件。	<p>选择此选项可创建复合条件。必须同时匹配所有条件才能触发事件。</p> <p>您可以从列表中“添加”任何可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

请参见第 482 页的“[配置“接受者匹配模式”条件](#)”。

配置“接受者匹配模式”条件

“接受者匹配模式”条件对所描述的邮件接受者身份进行匹配。

您可以在策略检测规则或例外中使用此条件。

请参见第 479 页的“[关于指定身份匹配](#)”。

表 30-3 “接受者匹配模式”条件的参数

操作	说明
输入一个或多个接受者模式以匹配一个或多个邮件接受者。请使用以逗号分隔的多个项。	电子邮件地址/新闻组模式 输入一个或多个电子邮件或新闻组地址以匹配所需的接受者。 要匹配特定电子邮件地址，请输入完整地址，例如 sales@symantec.com。要匹配特定域内的电子邮件地址，请仅输入域名，例如 symantec.com。
	IP 地址 输入一个或多个 IP 地址模式，这些模式将解析为您要匹配的域。可以使用星号 (*) 通配符代替一个或多个字段。
	URL 域 输入一个或多个 URL 域匹配基于 Web 的流量，包括基于 Web 的电子邮件和网站发布内容。例如，如果您想要禁止接收通过 Hotmail 发送的特定类型的数据，请输入 hotmail.com。
配置“匹配计数”。	选择下列选项之一以指定必须匹配的电子邮件接受者的数量： <ul style="list-style-type: none">■ 所有接受者必须匹配(仅限电子邮件)，如果选择此选项，除非所有电子邮件接受者都匹配指定的模式，否则不能算作匹配。■ 至少_个接受者必须匹配(仅限电子邮件)，通过此选项可以指定必须匹配的电子邮件接受者的最少计数数量。 选择下列选项之一以指定计算匹配项数目的方式： <ul style="list-style-type: none">■ 检查是否存在 如果存在一个或多个匹配项，则将匹配数报告为 1。■ 计算所有匹配项 报告所有匹配项的总和。 请参见第 337 页的“ 配置匹配计数 ”。

操作	说明
匹配整个邮件。	此条件匹配整个邮件。默认情况下选择“信封”选项。您无法选择任何其他邮件组件。 请参见第 294 页的 “关于可以匹配的邮件组件” 。
还匹配其他条件。	选择此选项可创建复合条件。必须匹配规则或例外中的所有条件才能触发事件。 您可以从列表中“添加”任何可用的条件。 请参见第 344 页的 “配置复合匹配条件” 。

请参见第 480 页的[“配置“发送者/用户匹配模式”条件”](#)。

指定身份匹配最佳做法

当您在策略检测规则或例外中实施“发送者/用户匹配模式”或“接受者匹配模式”条件时，请谨记以下注意事项：

- 发送者/用户和接受者条件均匹配整个邮件，而不是单个邮件组成部分。如果将任一条件用作例外，则匹配将排除整个邮件，而不仅是标头。
请参见第 297 页的[“关于检测服务器策略执行”](#)。
- 系统在所有逗号分隔列表项之间和所有字段之间隐式应用OR运算符。例如，如果电子邮件地址列表中的任何一个电子邮件地址匹配，条件将会报告（或排除）事件。或者，如果电子邮件地址、域名或IP地址匹配，条件将会报告（或排除）事件。
请参见第 479 页的[“关于指定身份匹配”](#)。
- 电子邮件地址必须完全匹配。例如，`bob@company.com` 不匹配 `bob@something.company.com`。但是，域名模式，如 `company.com` 或 `something.company.com` 匹配 `bob@something.company.com`。
- 电子邮件地址字段与 Web 发布内容的发送者或接受者不匹配。例如，如果 Bob 使用 Web 浏览器发送或接收电子邮件，则与电子邮件地址 `bob@yahoo.com` 不匹配。在这种情况下，必须使用域模式 `mail.yahoo.com` 匹配 `bob@yahoo.com`。
- URL 域模式可匹配到特定 URL 域的 HTTP 流量。不要输入整个 URL。例如，输入 `mail.yahoo.com` 而不是 `http://www.mail.yahoo.com`。
- 系统不能将 URL 域解析为 IP 地址。例如，对于某个特定域，可以指定 IP 地址 `192.168.1.1`。如果用户使用 Web 浏览器访问域 URL，则系统不能匹配通过 IP 地址传输的电子邮件。在这种情况下，请使用域模式而不是 IP 地址，例如 `internalmemos.com`。

- 您可以基于一个或多个 IP 地址检测发送者/用户和接受者。然而，要执行该操作，您必须慎重考虑检测服务器在网络中的位置。如果将检测服务器安装在 Web 代理和 Internet 之间，则来自组织内的人员的所有 Web 流量的 IP 地址看上去来自 Web 代理。如果将检测服务器安装在 Web 代理和公司内部网络之间，则来自组织外的所有 Web 流量的 IP 地址看上去流向 Web 代理。最佳做法是匹配域名而不是 IP 地址。

请参见第 480 页的“配置“发送者/用户匹配模式”条件”。

请参见第 482 页的“配置“接受者匹配模式”条件”。

检测已同步的身份

本章节包括下列主题：

- [关于实施同步的目录组匹配](#)
- [关于连接到目录组服务器](#)
- [创建或修改用户组](#)
- [配置“发送者/用户基于目录服务器匹配用户组”条件](#)
- [配置“接受者基于目录服务器匹配用户组”条件](#)
- [同步的 DGM 最佳做法](#)

关于实施同步的目录组匹配

Symantec Data Loss Prevention 提供目录组匹配 (DGM)，以检测用户、发送者和接受者的确切身份。

请参见第 288 页的“[关于目录组匹配](#)”。

可以将 Enforce Server 或发现服务器连接至组目录服务器，以根据组从属关系检测用户。例如，您希望将策略应用到公司工程部门的员工，而不是人力资源部门的员工。

您可从公司的目录服务器内定义的用户、组和业务单元中选择该组。构建用户组之后，可将其与用户/发送者和接受者条件相关联，或与发现目标相关联。将策略或目标应用到组后，此策略或目标仅适用于该组中的用户。如果所检测到的身份是用户，则该用户必须主动登录到启用代理的系统。再举一个例子，您想要创建一个应用到除 CEO 之外的整个公司的策略。您可以创建只有 CEO 一个成员的用户组，并将该组用作策略的例外。您可以根据所需的任何要求创建任意数目的组。

到您要使用的每个目录服务器组的连接称为组目录。组目录连接可指定您要用作定义确切身份用户组的源信息的目录服务器。身份组编辑页面是您使用源信息创建身份组的位置。

表 31-1 检测来自同步目录组服务器的身份

步骤	任务	说明
1	创建与目录服务器的连接。	建立从 Enforce Server 或发现服务器到配置了用户和组的目录服务器的连接。 请参见第 116 页的“ 配置目录服务器连接 ”。
2	创建用户组。	在 Enforce Server 上创建一个或多个用户组，并使用来自 Microsoft Active Directory 的身份进行填充。 请参见第 487 页的“ 创建或修改用户组 ”。
3	创建策略。	配置新策略或编辑现有策略。 请参见第 314 页的“ 关于用户组 ”。 请参见第 330 页的“ 配置策略 ”。
4	配置一个或多个用户组规则或例外。	将用户组规则或例外添加到策略。 链接策略和组之后，策略将仅适用于该组。 请参见第 488 页的“ 配置“发送者/用户基于目录服务器匹配用户组”条件 ”。 请参见第 489 页的“ 配置“接受者基于目录服务器匹配用户组”条件 ”。

关于连接到目录组服务器

Symantec Data Loss Prevention 支持与 LDAP 兼容目录服务器（例如 Microsoft Active Directory (AD)）的目录服务器连接。组目录连接指定 Enforce Server 或发现服务器如何连接至目录服务器。

在 Enforce Server 中创建任何用户组之前，必须建立与目录服务器的连接。Enforce Server 或发现服务器使用该连接来获取这些组的相关详细信息。如果不创建该连接，则无法定义任何组。该连接不是永久性的，但可配置为按指定的时间间隔同步。目录服务器包含创建用户组所需的所有信息。

如果使用包含自我签署的身份验证证书的目录服务器，则必须将该证书添加到 Enforce Server 或发现服务器。如果您的目录服务器使用预先授权的证书，系统会将其自动添加到 Enforce Server 或发现服务器。

请参见第 487 页的“[创建或修改用户组](#)”。

请参见第 485 页的“[关于实施同步的目录组匹配](#)”。

请参见第 190 页的“[将 SSL 证书导入到 Enforce Server 或发现服务器](#)”。

请参见第 314 页的“[关于用户组](#)”。

创建或修改用户组

“管理” > “策略” > “用户组” 屏幕显示已配置的用户组，该屏幕是创建新用户组的起点。

请参见第 314 页的[“关于用户组”](#)。

创建或修改用户组

- 建立到您想要同步的 Active Directory 服务器的连接。

请参见第 116 页的[“配置目录服务器连接”](#)。

- 在 “管理” > “策略” > “用户组” 屏幕上，单击 “创建新组”。

或者，要编辑现有用户组，请在 “用户组” 屏幕中选择该组。

- 根据需要配置用户组参数。

请参见第 487 页的[表 31-2](#)。

注意：如果这是您首次配置用户组，您必须选择 “保存时刷新组目录索引” 选项来填充用户组。

- 找到所需的用户之后，使用 “添加” 和 “删除” 选项在用户组中包括或排除这些用户。

- 单击 “保存”。

请参见第 485 页的[“关于实施同步的目录组匹配”](#)。

表 31-2 配置用户组

操作	说明
输入组名。	“组名” 是您用于识别该组的名称。 使用一个便于以后识别该组的说明性名称。
输入组说明	输入对组的简短 “说明”。
查看使用该组的策略。	最初，创建新用户组时，“已在策略中使用” 字段会显示 “无”。 如果用户组已经存在并且您对其进行修改，系统将显示实施用户组的策略列表（假设已为该用户组创建了一个或多个基于组的策略）。

操作	说明
刷新组目录索引。	如果这是您首次配置用户组，您必须选择“保存时刷新组目录索引”选项以便用最新的索引复制结果填充用户组配置文件。当“保存”配置文件时，系统会将配置文件与最新索引同步。 请参见第 118 页的 “计划目录服务器索引编制” 。
选择目录服务器。	从“目录服务器”列表中选择要使用的目录服务器。 在创建用户组配置文件之前，必须建立与目录服务器的连接。 请参见第 116 页的 “配置目录服务器连接” 。
浏览用户组的目录。	您可以浏览组和用户的目录树，方法是单击并展开各个节点，直到您看到所需的组或节点。 浏览结果中会显示每个节点的名称。这些名称会授予您特定的用户身份。 默认情况下，搜索结果的上限为 20 个条目。单击“查看更多”可查看高达 1000 条结果。
向配置文件添加用户组。	要将组或用户添加到用户组配置文件中，请从树中将其选中，然后单击“添加”。 选择节点并将其添加到“添加的组”列之后，系统会显示通用名称(CN)和可分辨名称(DN)。
搜索特定用户的目录。	通过“搜索目录”字段，可搜索特定用户的目录。 您可以使用以下搜索条件“ 搜索 ”目录： <ul style="list-style-type: none">■ 单个节点的名称■ 电子邮件地址 搜索结果将显示包含用户的目录服务器的通用名称(CN)和可分辨名称(DN)。这些名称会授予您特定的用户身份。结果上限为 1000 个条目。 “清除”选项会将您返回至“浏览目录”功能。在“搜索”字段中输入一个新搜索字符串可激活“搜索目录”功能。
保存用户组。	单击“保存”保存您已配置的用户组配置文件。

配置“发送者/用户基于目录服务器匹配用户组”条件

“发送者/用户基于目录服务器匹配用户组”条件基于从目录组服务器同步的邮件发送者和端点计算机用户对策略违规进行匹配。

您可以在策略组（身份）规则或例外中实施此条件。

请参见第 330 页的“[配置策略](#)”。

表 31-3 “发送者/用户匹配用户组”条件的参数

参数	说明
选择要包括在此策略中的用户组	选择要让此策略检测的一个或多个用户组。 如果未创建用户组，请单击“ 创建新的用户组 ”。 请参见第 487 页的“ 创建或修改用户组 ”。
匹配位置	此条件匹配整个邮件。默认情况下选择“ 信封 ”选项。您无法选择任何其他邮件组件。 请参见第 294 页的“ 关于可以匹配的邮件组件 ”。
同时匹配	选择此选项可创建复合条件。必须匹配规则或例外中的所有条件才能触发事件。 您可以从列表中“ 添加 ”任何可用的条件。 请参见第 344 页的“ 配置复合匹配条件 ”。

请参见第 485 页的“[关于实施同步的目录组匹配](#)”。

请参见第 288 页的“[关于目录组匹配](#)”。

配置“接受者基于目录服务器匹配用户组”条件

“接受者基于目录服务器组匹配用户组”条件基于从目录组服务器同步的特定邮件接受者对策略违规进行匹配。

您可以在策略组（身份）规则或例外中实施此条件。

请参见第 330 页的“[配置策略](#)”。

表 31-4 “接受者基于目录服务器组匹配用户组”条件

参数	说明
选择要包括在此策略中的用户组	选择要让此策略匹配的用户组。 如果未创建用户组，请单击“ 创建新的端点用户组 ”选项。 请参见第 487 页的“ 创建或修改用户组 ”。
匹配位置	此规则检测整个邮件，而不是各个组件。默认情况下选择“ 信封 ”选项。您无法选择任何其他邮件组件。 请参见第 294 页的“ 关于可以匹配的邮件组件 ”。

参数	说明
同时匹配	<p>选择此选项可创建复合条件。必须匹配规则或例外中的所有条件才能触发事件。</p> <p>您可以从列表中“添加”任何可用的条件。</p> <p>请参见第 344 页的“配置复合匹配条件”。</p>

请参见第 485 页的[“关于实施同步的目录组匹配”](#)。

请参见第 288 页的[“关于目录组匹配”](#)。

同步的 DGM 最佳做法

实施用户组目录服务器策略时，请注意以下事项：

- 如果将用户组条件和检测条件组合到一个策略中，可使用 AND 表达式来组合这些规则。结果是两个条件都必须匹配策略才能触发事件。
请参见第 294 页的[“关于可以匹配的邮件组件”](#)。
- 如果您将发送者/用户或接受者条件应用到非端点检测服务器，则不会忽略条件。而是，基于组的条件将失败并会导致该策略忽略可能的违规，因为所有条件均未满足。如果要将策略应用于非端点检测邮件，请勿在该策略中包含基于组的条件。
- 涉及用户的基于身份的检测适用于基于 DLP 代理的端点计算机配置组中的用户。使用端点用户组，许多不同的用户可登录到同一台计算机，具体取决于商业惯例。每个用户在端点计算机上所看到的响应会有所不同，具体取决于用户是如何分组的。请将这种样式的端点检测与端点目标或位置方法（特定于端点计算机而不是基于用户）进行对比。
请参见第 485 页的[“关于实施同步的目录组匹配”](#)。

检测已配置的身份

本章节包括下列主题：

- [关于实施配置的目录组匹配](#)
- [为 DGM 创建确切数据配置文件](#)
- [配置“发送者/用户匹配来自确切数据配置文件的目录”条件](#)
- [配置“接受者匹配来自确切数据配置文件的目录”条件](#)
- [配置的 DGM 的最佳做法](#)

关于实施配置的目录组匹配

使用 Symantec Data Loss Prevention 可以基于配置的目录服务器或数据库检测数据用户、邮件发送者以及接受者的确切身份。

Symantec Data Loss Prevention 提供两种静态目录组匹配方法。两种方法都要求使用带有特定数据字段的确切数据配置文件。

表 32-1 配置的目录组匹配检测规则

组规则	说明
来自确切数据配置文件的发送者/用户匹配目录	与组相关的属性可能包含 IP 地址、电子邮件、Windows 用户名、业务单元、部门、管理员、职务、就业状况。其他属性可能包括员工是否同意对其进行监控，或者员工是否可以访问敏感信息。
来自确切数据配置文件的接受者匹配目录	您可以对接受者电子邮件地址列表编制索引并基于该索引数据创建策略。例如，可以编写一个检测规则，要求邮件发送者来自于客户服务部门时违反该策略。或者，可以编写电子邮件接受者位于批准的列表时不违反该策略的检测例外。

请参见第 288 页的“[关于目录组匹配](#)”。

为 DGM 创建确切数据配置文件

配置的 DGM 要求使用带有特定数据字段的确切数据源。

为 DGM 创建确切数据源文件

- 1 为要配置的目录服务器或数据库创建一个数据源文件。

请参见第 361 页的“[创建确切数据源文件](#)”。

- 2 要实施配置的 DGM，系统需要一个或多个特定数据元素类型来检测邮件用户、发送者或接受者。

确切数据源文件必须包含下列一个或多个字段：

- 电子邮件地址
- IP 地址
- Windows 用户名
- AOL IM 名称
- Yahoo! IM 名称
- MSN IM 名称

注意：如果要实施数据所有者例外 (DOE)，可以使用电子邮件地址、域地址或此二者。请参见第 357 页的“[关于数据所有者例外](#)”。

- 3 准备用于编制索引的数据源文件，并将可用的数据源文件上传到 Enforce Server。

请参见第 363 页的“[为编制索引准备确切数据源文件](#)”。

请参见第 364 页的“[将确切数据源文件上传到 Enforce Server](#)”。

- 4 创建确切数据配置文件，映射数据字段，然后对数据源编制索引。

请参见第 365 页的“[创建和修改确切数据配置文件](#)”。

请参见第 369 页的“[映射确切数据配置文件字段](#)”。

请参见第 371 页的“[调度确切数据配置文件索引编制](#)”。

配置“发送者/用户匹配来自确切数据配置文件的目录”条件

“发送者/用户匹配目录源”检测规则使您可以根据发送者身份或（对于端点事件）用户身份创建检测规则。

“发送者/用户匹配目录源”检测规则依赖于 EDM 检测技术，需要确切数据配置文件。

请参见第 356 页的[“关于实施确切数据匹配”](#)。

选择数据配置文件后，当您配置此规则时，所选的目录和发送者标识符显示在页面顶部。

表 32-2 配置“发送者/用户匹配来自确切数据配置文件的目录”条件

参数	说明
其中	选择此选项可使 Symantec Data Loss Prevention 针对指定的字段值进行匹配。通过从下拉列表中选择一个字段并在相邻的文本框中键入此字段的值来指定值。（如果要输入多个值，请用逗号分隔各个值。）例如，对于包含“部门”字段的“员工”目录组配置文件，请选择“其中”，再在下拉列表中选择“部门”，然后在文本框中键入 Marketing,Sales 。对于检测规则，仅当发送者或用户在“营销”或“销售”部门工作时，此示例才会导致 Symantec Data Loss Prevention 捕获事件（只要输入内容满足其他全部检测条件）。而对于例外，当发送者或用户在“营销”或“销售”部门工作时，此示例会阻止 Symantec Data Loss Prevention 捕获事件。
为任一	输入或修改要匹配的信息。例如，如果您想要匹配“销售”部门中的任何发送者，请从下拉列表中选择“部门”，然后在此字段输入“销售”（假设您的数据包含“部门”列）。如果要指定多个值，请使用逗号分隔列表。

配置“接受者匹配来自确切数据配置文件的目录”条件

使用“接受者匹配目录源”检测规则，您可以根据接受者的身份创建检测方法。此方法需要确切数据配置文件。

请参见第 356 页的[“关于实施确切数据匹配”](#)。

选择数据配置文件后，当您配置此规则时，所选的目录和接受者标识符显示在页面顶部。

表 32-3 配置“接受者匹配来自确切数据配置文件的目录”条件

参数	说明
其中	选择此选项可使 Symantec Data Loss Prevention 针对指定的字段值进行匹配。通过从下拉列表中选择一个字段并在在相邻的文本框中键入此字段的值来指定值。（如果要输入多个值，请用逗号分隔各个值。）例如，对于包含“部门”字段的“员工”目录组配置文件，请选择“其中”，再在下拉列表中选择“部门”，然后在文本框中输入 Marketing, Sales 。对于检测规则，仅当至少有一名接受者在“营销”或“销售”部门工作时，此示例才会导致 Symantec Data Loss Prevention 捕获一个事件（只要输入内容满足其他全部检测条件）。对于例外，当至少有一名接受者在“营销”或“销售”部门工作时，此示例会阻止 Symantec Data Loss Prevention 捕获事件。
为任一	输入或修改要匹配的信息。例如，如果要匹配“销售”部门中的任何接受者，请从下拉列表中选择“部门”，然后在此字段中输入“销售”（假设您的数据包括一个“部门”列）。如果要指定多个值，请使用逗号分隔列表。

配置的 DGM 的最佳做法

实施配置的目录组匹配时，请记住以下注意事项：

- 必须在“确切数据配置文件”中加入正确的字段才能实施配置的 DGM。
请参见第 492 页的[“为 DGM 创建确切数据配置文件”](#)。
- 在策略例外中无法使用“发送者/用户匹配目录”或“接受者匹配目录”条件。要将邮件用户、发送者和接受者排除在检测之外，请使用身份模式匹配条件。
请参见第 479 页的[“关于指定身份匹配”](#)。
- 要将数据所有者排除在检测之外，必须在数据配置文件中加入这些用户的电子邮件地址或电子邮件域。
请参见第 357 页的[“关于数据所有者例外”](#)。
- 不能在一个策略中结合使用“发送者/用户匹配目录源”组规则与“Endpoint：阻止”或“Endpoint：通知”响应规则。如果结合使用，系统会报告该策略配置错误。
- 不能在一个策略中结合使用“接受者匹配目录源”组规则与“Endpoint：阻止”或“Endpoint：通知”响应规则。如果结合使用，系统会报告该策略配置错误。

检测国际内容

本章节包括下列主题：

- [关于实施非英语语言检测](#)
- [国际策略模板](#)
- [使用国际系统数据标识符的查找关键字](#)

关于实施非英语语言检测

Symantec Data Loss Prevention 的检测功能支持 Microsoft Windows 操作系统的许多本地化版本。要使用国际字符集，用于查看 Enforce Server 管理控制台的 Windows 系统必须具有相应的功能。

请参见第 57 页的“[关于字符集、语言和区域设置支持](#)”。

请参见第 60 页的“[使用国际字符](#)”。

您可以使用任意受支持的语言创建策略和检测违规。您可以使用本地化的关键字、正则表达式和数据配置文件来检测数据丢失。另外，Symantec Data Loss Prevention 提供了多个国际数据标识符和策略模板来保护机密数据。

请参见第 58 页的“[支持的检测语言](#)”。

请参见第 495 页的“[国际策略模板](#)”。

请参见第 497 页的“[使用国际系统数据标识符的查找关键字](#)”。

国际策略模板

Symantec Data Loss Prevention 提供多个可在企业中快速部署的国际策略模板。

请参见第 317 页的“[从模板创建策略](#)”。

表 33-1 国际策略模板

策略模板	说明
加拿大社会保险号	此策略会检测指示加拿大社会保险号 (SIN) 的模式。 请参见第 589 页的“ 加拿大社会保险号策略模板 ”。
Caldicott 报告	此策略会保护英国患者的信息。 请参见第 587 页的“ Caldicott 报告策略模板 ”。
1998 年英国数据保护法案	此策略会保护个人身份信息。 请参见第 594 页的“ 1998 年数据保护法案（英国）策略模板 ”。
欧盟数据保护规定	此策略会检测特定于欧盟指令的个人数据。 请参见第 596 页的“ 数据保护规定（欧盟）策略模板 ”。
1998 年英国人权法案	此策略会强制实施英国公民法案第 8 条。 请参见第 612 页的“ 1998 年人权法策略模板 ”。
PIPEDA（加拿大）	此策略会检测加拿大公民客户数据。 请参见第 626 页的“ PIPEDA 策略模板 ”。
SWIFT 代码（国际银行业务）	此策略检测银行用于跨国界转账的代码。 请参见第 641 页的“ SWIFT 代码策略模板 ”。
英国驾照号	此策略会检测英国驾照号。 请参见第 642 页的“ 英国驾照号策略模板 ”。
英国选民登记号	此策略会检测英国选民登记号。 请参见第 642 页的“ 英国选民登记号策略模板 ”。
英国国家保险号码	此策略会检测英国国家保险号码。 请参见第 643 页的“ 英国国家保险号码策略模板 ”。
英国国民保健服务号	此策略会检测 NHS 颁发的个人标识号码。 请参见第 642 页的“ 英国国民保健服务(NHS)号策略模板 ”。
英国护照号	此策略会检测有效的英国护照。 请参见第 643 页的“ 英国护照号策略模板 ”。
英国税号	此策略会检测英国税号。 请参见第 644 页的“ 英国税号策略模板 ”。

使用国际系统数据标识符的查找关键字

数据标识符为检测国际内容提供广泛支持。

请参见第 414 页的“[关于数据标识符](#)”。

一些国际数据标识符仅提供检测的大宽度。在这种情况下，您可以利用“查找关键字”可选验证器来缩小检测的范围。利用该可选验证器可帮助您清除策略匹配的所有误报。

请参见第 430 页的“[选择系统数据标识符宽度](#)”。

下表提供了多个国际数据标识符的关键字。

使用国际数据标识符的关键字

1 使用该表中列出的系统提供的国际数据标识符之一来创建策略。

请参见第 497 页的[表 33-2](#)。

2 选择“查找关键字”可选验证器。

请参见第 428 页的“[配置“内容匹配数据标识符”条件](#)”。

3 从列表中复制相应的以逗号分隔的关键字，并将其粘贴到“查找关键字”可选验证器字段。

请参见第 433 页的“[配置可选验证器](#)”。

表 33-2 国际数据标识符和关键字列表

数据标识符	语言	关键字	简体中文翻译
Burgerservicenummer (BSN)	荷兰语	Personnummer, sofinummer, sociaal-fiscaal nummer, persoonsgebonden	社会安全号, 税号(简称), 税号, 个人相关号码
税号	意大利语	codice fiscal, dati anagrafici, partita I.V.A., p. iva	免税代码, 个人数据, 增值 税号, 增值税号
法国国家统计局代 码	法语	INSEE, numéro de sécu, code sécu	INSEE, 社会安全号, 社会 安全代码
香港特别行政区 ID	繁体中文	身份证, 三颗星	身份证, 香港特别行政区永 久居民身份证
国际银行账号 (IBAN) (中部)	法语	Code IBAN, numéro IBAN	IBAN 代码, IBAN 号码

数据标识符	语言	关键字	简体中文翻译
国际银行账号 (IBAN) (东部)	法语	Code IBAN, numéro IBAN	IBAN 代码, IBAN 号码
国际银行账号 (IBAN) (西部)	法语	Code IBAN, numéro IBAN	IBAN 代码, IBAN 号码
中华人民共和国 ID	简体中文	身份证, 居民信息, 居民身份信息	身份证, 居民信息, 居民身份信息
韩国居民登记号码	韩语	주민등록번호, 주민번호	居民登记号码, 登记号码
西班牙 DNI ID	西班牙语	DNI	DNI
瑞士 AHV 号码	法语	Numéro AVS, numéro d'assuré, identifiant national, numéro d'assurance vieillesse, numéro de sécurité sociale, Numéro AVH	AVS 号码, 保险号, 国民标识符, 国家保险号码, 社会安全号, AVH 号码
	德语	AHV-Nummer, Matrikelnummer, Personenidentifikationsnummer	AHV 号码, 瑞士登记号码, PIN
	意大利语	AVS, AVH	AVS, AVH
中国台湾 ID	繁体中文	中国台湾身份证	中国台湾身份证

文件格式

本章节包括下列主题：

- [可提取其内容的文件格式](#)
- [可识别的文件类型](#)

可提取其内容的文件格式

Symantec Data Loss Prevention 可识别 100 多种文件格式。对于其中许多格式，您都可以使用基于内容的检测规则来破解文件并提取其内容，包括文本、元数据和子文件。对于非默认的文件格式，Symantec Data Loss Prevention 允许开发人员扩大文件类型识别范围和自定义内容提取。

下表列出了 Symantec Data Loss Prevention 可提取其内容的各种文件格式类别。请参阅相关链接，以了解相应类别支持的各个文件格式。

表 34-1 可破解的文件格式类别

文件格式类别	默认支持列表
文字处理文件格式	请参见第 500 页的“可提取其内容的文字处理文件格式”。
演示文稿文件格式	请参见第 501 页的“可提取其内容的演示文稿文件格式”。
电子表格文件格式	请参见第 502 页的“可提取其内容的电子表格文件格式”。
封装文件格式	请参见第 503 页的“可提取其内容的封装文件格式”。
文本和标记文件格式	请参见第 504 页的“可提取其内容的文本和标记文件格式”。
电子邮件文件格式	请参见第 505 页的“可提取其内容的电子邮件文件格式”。
CAD 文件格式	请参见第 505 页的“可提取其内容的计算机辅助设计文件格式”。
图形文件格式	请参见第 505 页的“可提取其内容的图形文件格式”。

文件格式类别	默认支持列表
数据库文件格式	请参见第 506 页的“ 可提取其内容的数据库文件格式 ”。
其他文件格式	请参见第 506 页的“ 可提取其内容的其他文件格式 ”。

可提取其内容的文字处理文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的文字处理文件格式。

表 34-2 可破解的文字处理文件格式

格式名称	格式扩展名
Adobe FrameMaker Interchange Format	MIF
Apple iWork Pages	PAGES
ApplixWords	AW
Corel WordPerfect Linux	WPS
Corel WordPerfect Macintosh	WPS
Corel WordPerfect Windows	WO
Corel WordPerfect Windows	WPD
DisplayWrite	IP
Folio Flat File	FFF
Fujitsu Oasys	OA2
Haansoft Hangul	HWP
IBM DCA/RFT (可修订的表单文本)	DC
JustSystems Ichitaro	JTD
Lotus AMI Pro	SAM
Lotus AMI ProfessionalWrite Plus	AMI
LotusWord Pro	LWP
Lotus SmartMaster	MWP
Microsoft Word PC	DOC

格式名称	格式扩展名
Microsoft Word Windows	DOC
Microsoft Word Windows XML	DOCX
Microsoft Word Windows Template XML	DOTX
Microsoft Word Windows Macro-Enabled Template XML	DOTM
Microsoft Word Macintosh	DOC
Microsoft Works	WPS
Microsoft Windows Write	WRI
OpenOfficeWriter	SXW
OpenOfficeWriter	ODT
StarOfficeWriter	SXW
StarOfficeWriter	ODT
WordPad	RTF
XML Paper Specification	XPS
XyWrite	XY4

可提取其内容的演示文稿文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的演示文稿文件格式。

表 34-3 可破解的演示文稿文件格式

格式名称	格式扩展名
Apple iWork Keynote	KEYNOTE
Applix Presents	AG
Corel Presentations	SHW
Lotus Freelance Graphics	PRZ
Lotus Freelance Graphics 2	PRE
Macromedia Flash	SWF

格式名称	格式扩展名
Microsoft PowerPoint Windows	PPT
Microsoft PowerPoint PC	PPT
Microsoft PowerPoint Windows XML	PPTX
Microsoft PowerPoint Windows Macro-Enabled XML	PPTM
Microsoft PowerPoint Windows XML Template	POTX
Microsoft PowerPoint Windows Macro-Enabled XML Template	POTM
Microsoft PowerPoint Windows XML Show	PPSX
Microsoft PowerPoint Windows Macro-Enabled Show	PPSM
Microsoft PowerPoint Macintosh	PPT
OpenOffice Impress	SXI
OpenOffice Impress	SXP
OpenOffice Impress	ODP
StarOffice Impress	SXI
StarOffice Impress	SXP
StarOffice Impress	ODP

可提取其内容的电子表格文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的电子表格文件格式。

表 34-4 可破解的电子表格文件格式

格式名称	格式扩展名
Apple iWork Numbers	NUMBERS
Applix Spreadsheets	AS
逗号分隔值	CSV
Corel Quattro Pro	WB2
Corel Quattro Pro	WB3

格式名称	格式扩展名
数据交换格式	DIF
Lotus 1-2-3	123
Lotus 1-2-3	WK4
Lotus 1-2-3 图表	123
Microsoft Excel Windows	XLS
Microsoft Excel Windows XML	XLSX
Microsoft Excel 图表	XLS
Microsoft Excel 2007 Binary	XLSB
Microsoft Excel Macintosh	XLS
Microsoft Works 电子表格	S30
Microsoft Works 电子表格	S40
OpenOffice Calc	SXC
OpenOffice Calc	ODS
StarOffice Calc	SXC
StarOffice Calc	ODS

可提取其内容的封装文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的封装文件格式。请注意，封装文件的内容是子文件。

表 34-5 可破解的封装文件格式

格式名称	格式扩展名
BinHex	HQX
GZIP	GZ
Java 存档	JAR
Microsoft Cabinet	CAB
Microsoft 压缩文件夹	LZH

格式名称	格式扩展名
Microsoft 压缩文件夹	LHA
PKZIP	ZIP
WinZip	ZIP
RAR 存档	RAR
磁带存档	TAR
UNIX 压缩	Z
UUEncoding	UUE

可提取其内容的文本和标记文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的文本和标记文件格式。

表 34-6 可破解的文本和标记文件格式

格式名称	格式扩展名
ANSI	TXT
ASCII	TXT
HTML	HTM
Microsoft Excel Windows XML	XML
Microsoft Word Windows XML	XML
Microsoft Visio XML	VDX
Oasis 开放文档格式	ODT
Oasis 开放文档格式	ODS
Oasis 开放文档格式	ODP
富文本格式	RTF
Unicode 文本	TXT
XHTML	HTM
XML（常规）	XML

可提取其内容的电子邮件文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的电子邮件文件格式。

表 34-7 可破解的电子邮件文件格式

格式名称	格式扩展名
Domino XML 语言	DXL
EMC EmailXtender 本机邮件	ONM
Microsoft Outlook	MSG
Microsoft Outlook Express	EML
文本邮件 (MIME)	各种
传输中性封装格式	各种

可提取其内容的计算机辅助设计文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的计算机辅助设计 (CAD) 文件格式。

表 34-8 可破解的 CAD 文件格式

格式名称	格式扩展名
AutoCAD 绘图	DWG
AutoCAD 绘图交换	DFX
Microsoft Visio	VSD
Microstation	DGN

可提取其内容的图形文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的图形文件格式。

表 34-9 可破解的图形文件格式

格式名称	格式扩展名
增强型元文件	EMF

格式名称	格式扩展名
Lotus Pic	PIC
标签图像文件（仅元数据）	TIFF
Windows 图元文件	WMF

可提取其内容的数据库文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的数据
库文件格式。

表 34-10 可破解的数据库文件格式

格式名称	格式扩展名
Microsoft Access	MDB
Microsoft Project（仅元数据）	MPP

可提取其内容的其他文件格式

下表列出了 Symantec Data Loss Prevention 可提取其内容以进行策略评估的其他
文件格式。

表 34-11 其他可破解的文件格式

格式名称	格式扩展名
Adobe PDF	PDF
MPEG-1 Audio layer 3（仅元数据）	MP3
Microsoft Windows 备份实用程序文件	BKF

可识别的文件类型

下表列出了 Symantec Data Loss Prevention 可以识别的文件类型。

注意：不扫描这些文件的内容，仅识别文件类型。请参见第 499 页的“[可提取其内容的文件格式](#)”。

表 34-12 可识别的文件类型

可识别的文件类型
7-Zip 压缩文件 (7Z)
Ability Office (SS)
Ability Office (DB)
Ability Office (GR)
Ability Office (WP)
Ability Office (COM)
ACT
Adobe FrameMaker
Adobe FrameMaker Interchange Format
Adobe FrameMaker 标记语言
Adobe PDF
AES Multiplus Comm
Aldus Freehand (Macintosh)
Aldus PageMaker (DOS)
Aldus PageMaker (Macintosh)
Amiga IFF-8SVX 声音
Amiga MOD 声音
ANSI
Apple Double
Apple Single
Applix Alis
Applix Asterix
Applix Graphics
Applix Presents
Applix Spreadsheets

可识别的文件类型

Applix Words

ARC/PAK 存档

ASCII

ASCII-armored PGP encoded

ASCII-armored PGP Public Keyring

ASCII-armored PGP signed

音频交换文件格式

AutoCAD 绘图

AutoCAD 绘图交换

AutoDesk Animator FLIC Animation

AutoDesk Animator Pro FLIC Animation

AutoDesk WHIP

AutoShade Rendering

BinHex

CADAM 绘图 (CDD)

CADAM Drawing Overlay

CATIA 绘图 (CAT)

CCITT Group 3 1-Dimensional (G31D)

COMET TOP Word

逗号分隔值

Compactor/Compact Pro 存档

计算机图元文件

Convergent Tech DEF Comm.

Corel Draw CMX

Corel Presentations

Corel Quattro Pro (WB2)

可识别的文件类型

Corel Quattro Pro (WB3)

Corel WordPerfect Linux

Corel WordPerfect Macintosh

Corel WordPerfect Windows (WO)

Corel WordPerfect Windows (WPD)

CorelDRAW

cpio 存档 (UNIX)

cpio 存档 (VAX)

cpio 存档 (SUN)

CPT 通信

Creative Voice (VOC) 声音

Curses 屏幕图像 (UNIX)

Curses 屏幕图像 (VAX)

Curses 屏幕图像 (SUN)

数据交换格式

Data Point VISTAWORD

dBase 数据库

DCX 传真

DCX 传真系统

DEC WPS PLUS

DECdx

桌面分色 (DCS)

设备无关文件 (DVI)

DG CEOwrite

DG 公用数据流 (CDS)

DIF 电子表格

可识别的文件类型

数字文件交换格式 (DDIF)

磁盘加倍器压缩

DisplayWrite

Domino XML 语言

EBCDIC 文本

EMC EmailXtender 容器文件 (EMX)

ENABLE

ENABLE 电子表格 (SSF)

Encapsulated PostScript (光栅)

增强型元文件

Envoy (EVY)

可执行文件 - 其他

可执行文件 - UNIX

可执行文件 - VAX

可执行文件 - SUN

FileMaker (Macintosh)

Folio Flat File

Framework

Framework II

FTP 会话数据

Fujitsu Oasys

GEM 位图像

GIF

图形环境管理器 (GEM VDI)

GZIP

Haansoft Hangul

可识别的文件类型

Harvard Graphics

Hewlett-Packard

Honey Bull DSA101

HP 图形语言 (HPG)

HP 打印机控制语言 (PCL)

HTML

IBM 1403 行式打印机

IBM DCA/RFT (可修订的表单文本)

IBM DCA-FFT

IBM DCF 脚本

Informix SmartWare II

Informix SmartWare II 通信文件

Informix SmartWare II 数据库

Informix SmartWare 电子表格

Interleaf

Java 存档

JPEG

JPEG 文件交换格式 (JFIF)

JustSystems Ichitaro

KW ODA G31D (G31)

KW ODA G4 (G4)

KW ODA 内部 G32D (G32)

KW ODA 内部原始位图 (RBM)

Lasergraphics 语言

Legato Extender

链接库 - 其他

可识别的文件类型

链接库 - UNIX

链接库 - VAX

链接库 - SUN

Lotus 1-2-3 (123)

Lotus 1-2-3 (WK4)

Lotus 1-2-3 图表

Lotus AMI Pro

Lotus AMI Professional Write Plus

Lotus AMIDraw Graphics

Lotus Freelance Graphics

Lotus Freelance Graphics 2

Lotus Notes 位图

Lotus Notes CDF

Lotus Notes 数据库

Lotus Pic

Lotus Screen Cam

Lotus SmartMaster

Lotus Word Pro

Lyrix MacBinary

MacBinary

Macintosh Raster

MacPaint

Macromedia Director

Macromedia Flash

MacWrite

MacWrite II

可识别的文件类型

MASS-11

Micrografx Designer

Microsoft Access

Microsoft 高级系统格式 (ASF)

Microsoft 压缩文件夹 (LZH)

Microsoft 压缩文件夹 (LHA)

Microsoft 设备无关位图

Microsoft Excel 图表

Microsoft Excel Macintosh

Microsoft Excel Windows

Microsoft Excel Windows XML

Microsoft Office Access (ACCDB)

Microsoft Office 绘图

Microsoft Outlook 个人文件夹

Microsoft Outlook

Microsoft Outlook Express

Microsoft PowerPoint Macintosh

Microsoft PowerPoint PC

Microsoft PowerPoint Windows

Microsoft PowerPoint Windows XML

Microsoft PowerPoint Windows Macro-Enabled XML

Microsoft PowerPoint Windows XML Template

Microsoft PowerPoint Windows Macro-Enabled XML Template

Microsoft PowerPoint Windows XML Show

Microsoft PowerPoint Windows Macro-Enabled Show

Microsoft Project

可识别的文件类型

Microsoft Publisher

Microsoft Visio

Microsoft Visio XML

Microsoft Wave Sound

Microsoft Windows Cursor (CUR) 图形

Microsoft Windows 组文件

Microsoft Windows 帮助文件

Microsoft Windows 图标 (ICO)

Microsoft Windows OLE 2 封装

Microsoft Windows Write

Microsoft Word (UNIX)

Microsoft Word Macintosh

Microsoft Word PC

Microsoft Word Windows

Microsoft Word Windows XML

Microsoft Word Windows Template XML

Microsoft Word Windows Macro-Enabled Template XML

Microsoft Works (Macintosh)

Microsoft Works

Microsoft Works 通信 (Macintosh)

Microsoft Works 通信 (Windows)

Microsoft Works 数据库 (Macintosh)

Microsoft Works 数据库 (PC)

Microsoft Works 数据库 (Windows)

Microsoft Works 电子表格 (S30)

Microsoft Works 电子表格 (S40)

可识别的文件类型

Microsoft Works 电子表格 (Macintosh)

Microstation

MIDI

MORE Database Outliner (Macintosh)

MPEG-1 Audio layer 3

MPEG-1 视频

MPEG-2 音频

MS DOS 批处理文件格式

MS DOS 设备驱动程序

MultiMate 4.0

Multiplan 电子表格

Navy DIF

NBI Async 存档格式

NBI Net 存档格式

Netscape 书签文件

NeWS 字体文件 (SUN)

NeXT/Sun 音频

NIOS TOP

Nota Bene

Nurestor 绘图 (NUR)

Oasis 开放文档格式 (ODT)

Oasis 开放文档格式 (ODS)

Oasis 开放文档格式 (ODP)

对象模块 - UNIX

对象模块 - VAX

对象模块 - SUN

可识别的文件类型

ODA/ODIF

ODA/ODIF (FOD 26)

Office Writer

OLE DIB 对象

OLIDIF

OmniOutliner (OO3)

OpenOffice Calc (SXC)

OpenOffice Calc (ODS)

OpenOffice Impress (SXI)

OpenOffice Impress (SXP)

OpenOffice Impress (ODP)

OpenOffice Writer (SXW)

OpenOffice Writer (ODT)

Open PGP

OS/2 PM 图元文件图形

Paradox (PC) 数据库

PC COM 可执行文件

PC 库模块

PC 对象模块

PC 画笔

PC TrueType 字体

PCD 图像

PeachCalc 电子表格

Persuasion 演示文稿

PEX 二进制存档 (SUN)

PGP 压缩数据

可识别的文件类型

PGP 加密数据

PGP 公钥环

PGP 密钥环

PGP 签名证书

PGP 签名和加密的数据

PGP 签名数据

Philips 脚本

PKZIP

Plan Perfect

Portable Bitmap Utilities (PBM)

Portable Greymap Utilities (PGM)

可移植网络图形

Portable Pixmap Utilities (PPM)

PostScript 文件

PRIMEWORD

程序信息文件

Q & A for DOS

Q & A for Windows

Quadratron Q-One (V1.93J)

Quadratron Q-One (V2.0)

Quark Express (Macintosh)

QuickDraw 3D 元文件 (3DMF)

QuickTime 影片

RAR 存档

Real 音频

Reflex 数据库

可识别的文件类型

富文本格式

RIFF 设备无关位图

RIFF MIDI

RIFF 多媒体影片

SAMNA Word IV

序列化对象格式 (SOF) 封装

SGI RGB 图像

SGML

简单矢量格式 (SVF)

SMTP 文档

SolidWorks 绘图

StarOffice Calc (SXC)

StarOffice Calc (ODS)

StarOffice Impress (SXI)

StarOffice Impress (SXP)

StarOffice Impress (ODP)

StarOffice Writer (SXW)

StarOffice Writer (ODT)

Stuff It 存档 (Macintosh)

Sun 光栅图像

SUN vfont 定义

Supercalc 电子表格

SYLK 电子表格

Symphony 电子表格

标签图像文件

磁带存档

可识别的文件类型

Targon Word (V 2.0)

文本邮件 (MIME)

传输中性封装格式

Truevision Targa

Ultracalc 电子表格

Unicode 文本

Uniplex (V6.01)

Uniplex Ucalc 电子表格

UNIX 压缩

UNIX SHAR 封装

Usenet 格式

UUEncoding

Volkswriter

VRML

Wang Office GDL 标头封装

WANG PC

Wang WITA

WANG WPS Comm.

Windows 动画光标

Windows 位图

Windows C++ 对象存储

Windows 图标光标

Windows 图元文件

Windows Micrografx Draw (DRW)

Windows 调色板

Windows Media 视频 (WMV)

可识别的文件类型

Windows Media 音频 (WMA)

Windows 视频 (AVI)

WinZip (解压缩读取器)

WinZip

Word Connection

WordERA (V 1.0)

WordMARC 文字处理器

WordPad

WordPerfect 常规文件

WordPerfect Graphics 1

WordPerfect Graphics 2

WordStar

WordStar 2000

WordStar 6.0

WriteNow

Writing Assistant 文字处理器

X Bitmap (XBM)

X 图像

X Pixmap (XPM)

Xerox 860 Comm.

Xerox Writer 文字处理器

XHTML

XML (常规)

XML Paper Specification

XyWrite

数据标识符

本章节包括下列主题：

- ABA 汇款路径号码数据标识符
- 澳大利亚医疗号码数据标识符
- 澳大利亚税务号码数据标识符
- 荷兰税号数据标识符
- 加拿大社会保险号码数据标识符
- 意大利税号数据标识符
- 信用卡磁条数据数据标识符
- 信用卡号数据标识符
- CUSIP 号码数据标识符
- 驾驶执照号码 - 加利福尼亚州数据标识符
- 驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州数据标识符
- 驾驶执照号码 - 伊利诺斯州数据标识符
- 驾驶执照号码 - 新泽西州数据标识符
- 驾驶执照号码 - 纽约州数据标识符
- 法国国家统计局代码数据标识符
- 香港特别行政区 ID 数据标识符
- IBAN 中部数据标识符
- IBAN 东部数据标识符

- [IBAN 西部数据标识符](#)
- [IP 地址数据标识符](#)
- [国家药品代码 \(NDC\) 数据标识符](#)
- [中华人民共和国 ID 数据标识符](#)
- [新加坡 NRIC 数据标识符](#)
- [韩国居民登记号码数据标识符](#)
- [西班牙 DNI ID 数据标识符](#)
- [SWIFT 代码数据标识符](#)
- [瑞士 AHV 号码数据标识符](#)
- [中国台湾 ID 数据标识符](#)
- [英国驾照号数据标识符](#)
- [英国选民登记号数据标识符](#)
- [英国国民保健服务 \(NHS\) 号数据标识符](#)
- [英国国家保险号码数据标识符](#)
- [英国护照号数据标识符](#)
- [英国税号数据标识符](#)
- [美国个人纳税识别号 \(ITIN\) 数据标识符](#)
- [美国社会安全号 \(SSN\) 数据标识符](#)
- [美国 SSN - 随机化自定义数据标识符 \(DI\)](#)

ABA 汇款路径号码数据标识符

美国银联 (ABA) 汇款路径号码也称为银行转帐号码 (RTN)，用于标识金融机构和处理交易。

ABA 汇款路径号码数据标识符可检测 9 位数字号码，并提供三种检测宽度：

- 大宽度版本使用最后检查数字验证检测到的号码。
请参见第 523 页的“[ABA 汇款路径号码大宽度](#)”。
- 中宽度版使用最后检查数字验证检测到的号码，并排除常见测试号码。
请参见第 523 页的“[ABA 汇款路径号码中宽度](#)”。

- 小宽度版本使用最后检查数字验证检测到的号码，排除常见测试号码，并要求存在与 ABA 相关的关键字。
请参见第 524 页的“[ABA 汇款路径号码小宽度](#)”。

ABA 汇款路径号码大宽度

大宽度版本的 ABA 汇款路径号码数据标识符检测 9 位数的号码。它使用最终检查数字验证号码。

表 35-1 ABA 汇款路径号码大宽度模式

模式
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

表 35-2 ABA 汇款路径号码大宽度验证器

必选验证器	说明
ABA 校验和	每个 ABA 汇款路径号码必须以下列两个数字开头：00-15、21-32、61-72、80，并通过 ABA 特定的位置权重校验和。

ABA 汇款路径号码中宽度

中宽度版本的 ABA 汇款路径号码 DI 检测 9 位数的号码。它使用最终检查数字验证号码。

它排除常见测试号码（例如 123456789）、保留供将来使用的范围，以及数字全部相同的号码。

表 35-3 ABA 汇款路径号码中宽度模式

模式
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

表 35-4

ABA 汇款路径号码中宽度验证器

必选验证器	说明
ABA 校验和	每个 ABA 汇款路径号码必须以下列两个数字开头：00-15、21-32、61-72、80，并通过 ABA 特定的位置权重校验和。
排除开始字符	选中此选项时，将不会匹配开头为以下列表中任意值的数据。 输入：123456789
重复数字	保证数字字符串不全相同。
数字分隔符	通过检查周围的数字验证匹配。

ABA 汇款路径号码小宽度

小宽度版本的 ABA 汇款路径号码数据标识符检测 9 位数的号码，并使用最终检查数字验证号码。它排除常见测试号码（例如 123456789）、保留供将来使用的范围，以及数字全部相同的号码。它还要求存在与 ABA 相关的关键字。

表 35-5

ABA 汇款路径号码小宽度模式

模式
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

表 35-6

ABA 汇款路径号码小宽度验证器

必选验证器	说明
ABA 校验和	每个 ABA 汇款路径号码必须以下列两个数字开头：00-15、21-32、61-72、80，并通过 ABA 特定的位置权重校验和。
排除开始字符	选中此选项时，将不会匹配开头为以下列表中任意值的数据。 输入：123456789
重复数字	保证数字字符串不全相同。

必选验证器	说明
查找关键字	选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。输入： aba、aba #、aba routing #、aba routing number、aba#、abarouting#、abaroutingnumber、american bank association routing #、american bank association routing number、americanbankassociationrouting#、americanbankassociationroutingnumber、bank routing #、bank routing number、bankrouting#、bankroutingnumber
数字分隔符	通过检查周围的数字验证匹配。

澳大利亚医疗号码数据标识符

澳大利亚医疗号码是由澳大利亚健康保险委员会依据医疗机制为符合条件的人员分配的个人标识符。该标识符位于澳大利亚医疗卡上。

澳大利亚医疗号码数据标识符可检测 8 或 9 位数字的号码，该号码匹配澳大利亚医疗号码的格式。此数据标识符不实施任何验证器。

表 35-7 澳大利亚医疗号码大宽度模式

模式
\d{4} \d{5} \d \d
\d{4}-\d{5}-\d-\d

澳大利亚税务号码数据标识符

澳大利亚税务号码 (TFN) 是 8 或 9 位数字的号码，由澳大利亚税务局 (ATO) 颁发给纳税人（个人、公司、养老保险基金、股东或信托），用于标识其澳大利亚纳税情况。

澳大利亚税务号码数据标识符可检测 8 或 9 位数字的号码，并确保检测到的号码可通过校验和验证。

表 35-8 澳大利亚税务号码大宽度模式

模式
\d{8}
\d{9}

表 35-9 澳大利亚税务号码大宽度验证器

必选验证器	说明
澳大利亚税务验证检查	计算校验和并根据校验和对模式进行验证

荷兰税号数据标识符

在荷兰，税号用于唯一地标识公民，并且打印在驾照、护照和国际 ID 卡上的“个人号码”标题下。

荷兰税号数据标识符可检测通过校验和验证的 8 或 9 位数字的号码。

表 35-10 荷兰税号大宽度模式

模式
\d{9}

表 35-11 荷兰税号大宽度验证器

必选验证器	说明
荷兰税号检查	荷兰税号检查。

加拿大社会保险号码数据标识符

加拿大社会保险号 (SIN) 是由加拿大人力资源和技能发展部颁发的个人识别号，主要用于管理国家退休和就业计划。

加拿大社会保险号数据标识符可提供三种检测宽度：

- 大
请参见第 527 页的“[加拿大社会保险号大宽度](#)”。
- 中
请参见第 527 页的“[加拿大社会保险号中宽度](#)”。
- 小

请参见第 528 页的“[加拿大社会保险号小宽度](#)”。

加拿大社会保险号大宽度

大宽度版本的加拿大社会保险号数据标识符可检测 9 位数字的号码，号码格式为 DDD-DDD-DDD，以短横线、空格、句点、斜杠分隔或不使用分隔符分隔。该模式会执行 Luhn 检查验证。

表 35-12 加拿大社会保险号大宽度模式

模式
\d{3} \d{3} \d{3}
\d{9}
\d{3}/\d{3}/\d{3}
\d{3}. \d{3}. \d{3}
\d{3}-\d{3}-\d{3}

表 35-13 加拿大社会保险号大宽度验证器

必选验证器	说明
Luhn 检查	验证器将计算 Luhn 校验和，每个加拿大保险号都必须通过该验证。

加拿大社会保险号中宽度

中宽度版本的加拿大社会保险号数据标识符可检测 9 位数字的号码，号码的格式为 DDD-DDD-DDD，以短横线、空格或句点分隔。它会执行 Luhn 检查验证并排除未指定的号码和常见测试号码。

表 35-14 加拿大社会保险号中宽度模式

模式
\d{3} \d{3} \d{3}
\d{3}. \d{3}. \d{3}
\d{3}-\d{3}-\d{3}

表 35-15 加拿大社会保险号中宽度验证器

必选验证器	说明
Luhn 检查	验证器将计算 Luhn 校验和，每个加拿大保险号都必须通过该验证。
数字分隔符	通过检查周围的数字验证匹配。
排除开始字符	选中此选项时，将不会匹配开头为以下列表中任意值的数据。 输入： 8, 123456789

加拿大社会保险号小宽度

小宽度版本的加拿大社会保险号数据标识符可检测 9 位数字的号码，号码的格式为 DDD-DDD-DDD，以短横线或空格分隔。该模式会执行 Luhn 检查验证。排除未指定的号码、假设指定的号码和常见测试号码。要求存在与社会保险号相关的关键字。

表 35-16 加拿大社会保险号小宽度模式

模式
\d{3} \d{3} \d{3}
\d{3}-\d{3}-\d{3}

表 35-17 加拿大社会保险号小宽度验证器

必选验证器	说明
Luhn 检查	验证器将计算 Luhn 校验和，每个加拿大保险号都必须通过该验证。
数字分隔符	通过检查周围的数字验证匹配。
排除开始字符	选中此选项时，将不会匹配开头为以下列表中任意值的数据。 输入： 0, 8, 123456789

必选验证器	说明
查找关键字	<p>选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。</p> <p>输入：</p> <p>pension、pensions、soc ins、ins #、social ins、CSIN、SSN、social security、social insurance、Canada、Canadian</p>

意大利税号数据标识符

在意大利，每个意大利人在出生时都会获得一个意大利税号。意大利税号唯一标识意大利公民或永久外国居民，该代码由财政部统一颁发。

意大利税号数据标识符可检测 16 个字符的标识符。最后的字符必须匹配校验和算法。

表 35-18 意大利税号大宽度模式

模式
[A-Z]{6}[0-9LMNPQRSTUVA-Z]{2}[ABCDEFHLMRST][0-9LMNPQRSTUVA-Z]{2}[A-Z] [0-9LMNPQRSTUVA-Z]{3}[A-Z]
[A-Z]{3} [A-Z]{3} [0-9LMNPQRSTUVA-Z]{2}[ABCDEFHLMRST][0-9LMNPQRSTUVA-Z]{2} [A-Z][0-9LMNPQRSTUVA-Z]{3}[A-Z]

表 35-19 意大利税号大宽度验证器

必选验证器	说明
意大利税号控制键检查	计算该控制键并检查其是否有效。

信用卡磁条数据数据标识符

信用卡的磁条包含关于该卡的信息。存储这些数据的完整版本是一种违反支付卡行业 (PCI) 数据安全标准的做法。

信用卡磁条数据数据标识符可检测从信用卡磁条获取的以下原始数据：

- 磁道 1 中格式 B 的数据，这些数据通常包含帐号、姓名、过期日期，并且可能包含卡验证值或卡验证代码 1 (CVV1/CVC1)。
- 磁道 2 中的数据，这些数据通常包含帐号，并且可能包含过期日期、服务代码以及卡验证值或卡验证代码 1 (CVV1/CVC1)。

信用卡磁条数据数据标识符可检测磁道 2 数据所特有的数据模式，包含起始标记、格式代码、主帐号、姓名、过期日期、服务代码、任意数据和结束标记。它还包括标准字段分隔符。该标识符使用 **Luhn** 检查验证器验证数据。

表 35-20 信用卡磁条数据中宽度模式

模式	模式(续)
;1800\d{11}=	%B3[068]\d{12}^*[A-Z]{1}
;6011-\d{4}-\d{4}-\d{4}=	%B3[068]\d{2}\d{6}\d{4}^*[A-Z]{1}
;6011 \d{4} \d{4} \d{4}=	%B3[068]\d{2}-\d{6}-\d{4}^*[A-Z]{1}
;6011\d{12}=	%B4\d{12}^*[A-Z]{1}
;3[068]\d{12}=	%B3[47]\d{2}-\d{6}-\d{5}^*[A-Z]{1}
;3[068]\d{2}\d{6}\d{4}=	%B4\d{3}\d{4}\d{4}\d{4}^*[A-Z]{1}
;3[068]\d{2}-\d{6}-\d{4}=	%B3[47]\d{2}\d{6}\d{5}^*[A-Z]{1}
;4\d{12}=	%B4\d{15}^*[A-Z]{1}
;3[47]\d{2}-\d{6}-\d{5}=	%B3[47]\d{13}^*[A-Z]{1}
;4\d{3}\d{4}\d{4}\d{4}=	%B5[1-5]\d{2}-\d{4}-\d{4}-\d{4}^*[A-Z]{1}
;3[47]\d{2}\d{6}\d{5}=	%B4\d{3}-\d{4}-\d{4}-\d{4}^*[A-Z]{1}
;4\d{15}=;3[47]\d{13}=	%B5[1-5]\d{2}\d{4}\d{4}\d{4}^*[A-Z]{1}
;5[1-5]\d{2}-\d{4}-\d{4}-\d{4}=	%B5[1-5]\d{14}^*[A-Z]{1}
;4\d{3}-\d{4}-\d{4}-\d{4}=	%B2131\d{11}^*[A-Z]{1}
;5[1-5]\d{2}\d{4}\d{4}\d{4}=	%B3\d{3}-\d{4}-\d{4}-\d{4}^*[A-Z]{1}
;5[1-5]\d{14}=;2131\d{11}=	%B3\d{3}\d{4}\d{4}\d{4}^*[A-Z]{1}
;3\d{3}-\d{4}-\d{4}-\d{4}=	%B3\d{15}^*[A-Z]{1}
;3\d{3}\d{4}\d{4}\d{4}=	%B2149\d{11}^*[A-Z]{1}
;3\d{15}=	%B2149\d{6}\d{5}^*[A-Z]{1}
;2149\d{11}=	%B2149-\d{6}-\d{5}^*[A-Z]{1}
;2149 \d{6} \d{5}=	%B2014\d{11}^*[A-Z]{1}
;2149-\d{6}-\d{5}=	%B2014 \d{6}\d{5}^*[A-Z]{1}
;2014\d{11}=	%B2014-\d{6}-\d{5}^*[A-Z]{1}
;2014 \d{6} \d{5}=	
;2014-\d{6}-\d{5}=	
%B1800\d{11}^*[A-Z]{1}	
%B6011-\d{4}-\d{4}-\d{4}^*[A-Z]{1}	
%B6011 \d{4} \d{4}	
\d{4}^*[A-Z]{1}	
%B6011\d{12}^*[A-Z]{1}	

表 35-21 信用卡磁条数据中宽度验证器

验证器	说明
Luhn 检查	计算每个实例必须通过的 Luhn 校验和。

信用卡号数据标识符

处理信用卡交易需要的帐号。通常缩写为 CCN。也称为主帐号 (PAN)。

信用卡号数据标识符可提供三种检测宽度：

- 大宽度
请参见第 532 页的“[信用卡号大宽度](#)”。
- 中宽度
请参见第 533 页的“[信用卡号中宽度](#)”。
- 小宽度
请参见第 535 页的“[信用卡号小宽度](#)”。

信用卡号大宽度

大宽度信用卡号数据标识符会检测以空格、短横线、句点分隔或不带分隔符的有效信用卡号。

此验证器包括 American Express、Diner's Club、Discover、Japan Credit Bureau (JCB)、MasterCard 和 Visa 格式。

此验证器会执行 Luhn 检查验证。

表 35-22 信用卡号大宽度模式

模式	模式(续)
\d{16}	2149-\d{6}-\d{5}
\d{4}.\d{4}.\d{4}.\d{4}	3[068]\d{12}
\d{4} \d{4} \d{4} \d{4}	3[068]\d{2}.\d{6}.\d{4}
\d{4}-\d{4}-\d{4}-\d{4}	3[068]\d{2}\d{6}\d{4}
1800\d{11} 2014.\d{6}.\d{5}	3[068]\d{2}-\d{6}-\d{4}
2014\d{11} 2014 \d{6} \d{5}	3[47]\d{13}
2014-\d{6}-\d{5}	3[47]\d{2}.\d{6}.\d{5}
2131\d{11}	3[47]\d{2}\d{6}\d{5}
2149.\d{6}.\d{5}	3[47]\d{2}-\d{6}-\d{5}
2149\d{11}	4\d{12}
2149 \d{6} \d{5}	

表 35-23 加拿大社会保险号大宽度验证器

必选验证器	说明
Luhn 检查	计算每个信用卡号必须通过的 Luhn 校验和。

信用卡号中宽度

中宽度信用卡号数据标识符会检测以空格、短横线、句点分隔或不带分隔符的有效信用卡号。此验证器会执行 Luhn 检查验证。此验证器包括 American Express、Diner's Club、Discover、Japan Credit Bureau (JCB)、MasterCard 和 Visa 格式。该验证器会排除常见测试号码，包括保留供信用卡发行机构用于测试的号码。

表 35-24 信用卡号中宽度模式

模式	模式 (续)
1800\d{11}	3\d{3}.\d{4}.\d{4}.\d{4}
2014.\d{6}.\d{5}	3\d{3} \d{4} \d{4} \d{4}
2014\d{11}	3\d{3}-\d{4}-\d{4}-\d{4}
2014 \d{6} \d{5}	4\d{12} 4\d{15}
2014-\d{6}-\d{5}	4\d{3}.\d{4}.\d{4}.\d{4}
2131\d{11}	4\d{3} \d{4} \d{4} \d{4}
2149.\d{6}.\d{5} 2149\d{11}	4\d{3}-\d{4}-\d{4}-\d{4}
2149 \d{6} \d{5}	5[1-5]\d{14}
2149-\d{6}-\d{5}	5[1-5]\d{2}.\d{4}.\d{4}.\d{4}
3[068]\d{12}	5[1-5]\d{2} \d{4} \d{4} \d{4}
3[068]\d{2}.\d{6}.\d{4}	5[1-5]\d{2}-\d{4}-\d{4}-\d{4}
3[068]\d{2} \d{6} \d{4}	6011.\d{4}.\d{4}.\d{4}
3[068]\d{2}-\d{6}-\d{4}	6011\d{12}
3[47]\d{13}	6011 \d{4} \d{4} \d{4}
3[47]\d{2}.\d{6}.\d{5}	6011-\d{4}-\d{4}-\d{4}
3[47]\d{2} \d{6} \d{5}	
3[47]\d{2}-\d{6}-\d{5}	
3\d{15}	

表 35-25 信用卡号中宽度验证器

必选验证器	说明
Luhn 检查	验证器计算每个信用卡号必须通过的 Luhn 校验和。
排除数据匹配	排除与指定文本匹配的任意内容。

必选验证器	说明
排除数据匹配输入	0111111111111111, 1234567812345670, 180025848680889, 180026939516875, 20140000000009, 201411032364438, 201431736711288, 21000295634412, 214906110040367, 30000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 3088000000000000, 3088000000000009, 3088272824427380, 3096666928988980, 3158060990195830, 340000000000009, 341019464477148, 341111111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 370000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 4007000000027, 401288888881880, 4024007116284, 411111111111110, 411111111111111, 4222222222222, 4242424242424242, 4485249610564758, 4539399050593, 4539475158333170, 4539603277651940, 4539687075612974, 4539890911376230, 4556657397647250, 4716733846619930, 4716976758661, 4916437046413, 4916451936094420, 4916491104658550, 4916603544909870, 4916759155933, 5105105105100, 5119301340696760, 5263386793750340, 5268196752489640, 5283145597742620, 5424000000000015, 5429800397359070, 543111111111111, 5455780586062610, 5472715456453270, 5500000000000004, 5539878514522540, 5547392938355060, 555555555554440, 555555555554444, 5556722757422205, 6011000000000000, 601100000000004, 60110000000012, 6011000990139420, 60111111111110, 60111111111117, 6011312054074430, 6011354276117410, 6011601160116611, 6011905056260500, 869908581608894, 869933317208876, 869989278167071
数字分隔符	通过检查周围号码来验证匹配项。

信用卡号小宽度

小宽度版本的信用卡号数据标识符会检测以空格、短横线、句点分隔或不带分隔符的有效信用卡号。它执行 Luhn 检查验证。包括 American Express、Diner's Club、Discover、Japan Credit Bureau (JCB)、MasterCard 和 Visa 格式。排除常见测试号码，包括保留供信用卡发行机构用于测试的号码。并且要求存在与信用卡相关的关键字。

表 35-26 信用卡号小宽度模式

模式	模式(续)
2149 \d{6} \d{5}	5[1-5]\d{2}-\d{4}-\d{4}-\d{4}
2149-\d{6}-\d{5}	5[1-5]\d{2} \d{4} \d{4} \d{4}
2014\d{11}	5[1-5]\d{14}
2014 \d{6} \d{5}	5[1-5]\d{2}.\d{4}.\d{4}.\d{4}
2014-\d{6}-\d{5}	2131\d{11}
6011-\d{4}-\d{4}-\d{4}	3\d{3}-\d{4}-\d{4}-\d{4}
6011 \d{4} \d{4} \d{4}	3\d{3} \d{4} \d{4} \d{4}
6011\d{12}	3\d{15}
3[068]\d{12}	2149\d{11}
3[068]\d{2} \d{6} \d{4}	
3[068]\d{2}-\d{6}-\d{4}	
3[47]\d{2}-\d{6}-\d{5}	
3[47]\d{2} \d{6} \d{5}	
3[47]\d{13}	
4\d{3}-\d{4}-\d{4}-\d{4}	
3\d{3}.\d{4}.\d{4}.\d{4}	
2149.\d{6}.\d{5}	
2014.\d{6}.\d{5}	
6011.\d{4}.\d{4}.\d{4}	
3[068]\d{2}.\d{6}.\d{4}	
3[47]\d{2}.\d{6}.\d{5}	
4\d{3}.\d{4}.\d{4}.\d{4}	
1800\d{11}	
4\d{12}	
4\d{3} \d{4} \d{4} \d{4}	
4\d{15}	

表 35-27 信用卡号小宽度验证器

必选验证器	说明
Luhn 检查	验证器计算每个信用卡号必须通过的 Luhn 校验和。

必选验证器	说明
排除数据匹配	排除与指定文本匹配的任意内容。
排除数据匹配输入	011111111111111, 1234567812345670, 180025848680889, 180026939516875, 20140000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 3000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 3088000000000000, 3088000000000009, 3088272824427380, 309666928988980, 3158060990195830, 3400000000000009, 341019464477148, 341111111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 370000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 4007000000027, 401288888881880, 4024007116284, 411111111111110, 411111111111111, 422222222222, 4242424242424242, 4485249610564758, 4539399050593, 4539475158333170, 4539603277651940, 4539687075612974, 4539890911376230, 4556657397647250, 4716733846619930, 4716976758661, 4916437046413, 4916451936094420, 4916491104658550, 4916603544909870, 4916759155933, 5105105105100, 5119301340696760, 5263386793750340, 5268196752489640, 5283145597742620, 5424000000000015, 5429800397359070, 543111111111111, 5455780586062610, 5472715456453270, 550000000000004, 5539878514522540, 5547392938355060, 555555555554440, 555555555554444, 5556722757422205, 6011000000000000, 6011000000000004, 6011000000000012, 6011000990139420, 601111111111110, 6011111111111117, 6011312054074430, 6011354276117410, 6011601160116611, 6011905056260500, 869908581608894, 869933317208876, 869989278167071
数字分隔符	通过检查周围号码来验证匹配项。
查找关键字	选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。
查找关键字输入	account number、account ps、american express、americanexpress、amex、bank card、bankcard、card num、card number、cc#、cc#、ccn、check card、checkcard、credit card、credit card #、credit card number、credit card#、debit card、debitcard、diners club、dinersclub、discover、enroute、japanese card bureau、jcb、mastercard、mc、visa

CUSIP 号码数据标识符

CUSIP 号码是指定给北美股票交易所或其他证券交易所的唯一标识符。此号码由统一证券识别程序委员会 (CUSIP) 颁发，用于帮助完成交易。

CUSIP 号码数据标识符检测 9 个字符的字符串。

此数据标识符提供三个检测宽度：

- 大版本验证最终检查数字。
请参见第 538 页的“[CUSIP 号码大宽度](#)”。
- 中版本验证最终检查数字，且要求存在关键字。
请参见第 538 页的“[CUSIP 号码中宽度](#)”。
- 小版本验证最终检查数字，且要求存在关键字。
请参见第 539 页的“[CUSIP 号码小宽度](#)”。

CUSIP 号码大宽度

大宽度版本的 CUSIP 号码数据标识符检测 9 个字符的字符串。第 5、6、7 和 8 个字符可以是字母或数字，所有其他字符都是数字。验证最终检查数字。

表 35-28 CUSIP 号码大宽度模式

模式
\d{4}\w{4}\d

表 35-29 CUSIP 号码大宽度验证器

必选验证器	说明
Cusip 验证	验证器将检查无效的 CUSIP 范围并计算 CUSIP 校验和 (Modulus 10 Double Add Double 算法)。

CUSIP 号码中宽度

大宽度版本的 CUSIP 号码数据标识符检测 9 个字符的字符串。第 5、6、7 和 8 个字符可以是字母或数字，所有其他字符都是数字。

此版本的验证器验证最终检查数字，而且要求存在与 CUSIP 相关的关键字。

表 35-30 CUSIP 号码中宽度模式

模式
\d{4}\w{4}\d

表 35-31 CUSIP 号码中宽度验证器

必选验证器	说明
Cusip 验证	验证器将检查无效的 CUSIP 范围并计算 CUSIP 校验和（Modulus 10 Double Add Double 算法）。
查找关键字	选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。
查找关键字输入	cusip、c.u.s.i.p.、Committee on Uniform Security Identification Procedures、American Bankers Association、Standard & Poor's、S&P、National Numbering Association、NNA、National Securities Identification Number

CUSIP 号码小宽度

大宽度版本的 CUSIP 号码数据标识符检测 9 个字符的字符串。第 5、6、7 和 8 个字符可以是字母或数字，所有其他字符都是数字。

此版本的验证器验证最终检查数字，而且要求存在与 CUSIP 相关的关键字。

因为该版本的数据标识符未将 NNA 缩写包含为关键字，所以它比中宽度窄。

表 35-32 CUSIP 号码小宽度模式

模式
\d{4}\w{4}\d

表 35-33 CUSIP 号码小宽度验证器

必选验证器	说明
Cusip 验证	验证器将检查无效的 CUSIP 范围并计算 CUSIP 校验和（Modulus 10 Double Add Double 算法）。
查找关键字	选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。
查找关键字输入	cusip、c.u.s.i.p.、Committee on Uniform Security Identification Procedures、American Bankers Association、Standard & Poor's、S&P、National Numbering Association、NNA、National Securities Identification Number

驾驶执照号码 - 加利福尼亚州数据标识符

此号码是由美国加利福尼亚州颁发的个人驾照的标识号码。

驾驶执照号码 - 加利福尼亚州数据标识符可检测是否存在 7 个数字的号码。

此数据标识符提供两个验证宽度：

- 大宽度版本可检测任意 7 个数字的号码。
请参见第 540 页的“[驾驶执照号码 - 加利福尼亚州大宽度](#)”。
- 中宽度版本针对关键字验证已检测的数字。
请参见第 540 页的“[驾驶执照号码 - 加利福尼亚州中宽度](#)”。

驾驶执照号码 - 加利福尼亚州大宽度

大宽度版本的加利福尼亚驾驶执照号码数据标识符检测 8 个字符的字符串，该字符串以一个字母开头，后跟 7 个数字。

注意：此宽度选项不包括任何验证器。

表 35-34 驾驶执照号码大宽度模式

模式
\l\d{7}

驾驶执照号码 - 加利福尼亚州中宽度

中宽度版本的数据标识符检测 8 个字符的字符串，该字符串以一个字母开头，后跟 7 个数字。

它通过要求存在驾照关键字和与加利福尼亚相关的关键字来验证已检测的数字。

表 35-35 驾驶执照号码 - 加利福尼亚州中宽度模式

模式
\l\d{7}

表 35-36 驾驶执照号码 - 加利福尼亚州中宽度验证器

必选验证器	说明
查找关键字	选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。

必选验证器	说明
查找关键字输入	driver license、drivers license、driver's license、driver licenses、drivers licenses、driver's licenses、dl#、dls#、lic#、lics#
查找关键字	选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。
查找关键字输入	ca、calif、california

驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州数据标识符

这些号码是由以下其中一个美国州颁发的个人驾照的标识号码：佛罗里达州、密歇根州或明尼苏达州。将这些州分组在一起是因为这些州的驾照具有相同的模式。

此数据标识符检测 13 个字符的字符串，该字符串以一个字母开头，后跟 12 个数字。

此数据标识符提供两个验证宽度：

- 大宽度版本检测任意 13 个字符的字符串，即一个字母后跟 12 个数字。
请参见第 541 页的“[驾驶执照号码-佛罗里达州、密歇根州和明尼苏达州大宽度](#)”。
- 中宽度通过要求存在关键字来缩小范围。
请参见第 542 页的“[驾驶执照号码-佛罗里达州、密歇根州和明尼苏达州中宽度](#)”。

驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州大宽度

大宽度版本的该数据标识符检测任意 13 个字符的字符串，即一个字母后跟 12 个数字。

对于密歇根州执照号码，符合以下格式：L-DDD-DDD-DDD-DDD。

注意：此宽度选项不包括任何验证器。

表 35-37 驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州大宽度模式

模式
\l \d{3} \d{3} \d{3} \d{3}
\d{12}
\d{3}-\d{3}-\d{2}-\d{3}-\d
\-\d{3}-\d{3}-\d{3}-\d{3}

驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州中宽度

中宽版本的该数据标识符实施模式来检测任意 13 个字符的字符串，即一个字母后跟 12 个数字。对于密歇根州执照号码，符合以下格式：L-DDD-DDD-DDD-DDD。

该数据标识符通过要求存在驾照关键字以及与州相关的关键字来验证数字。

表 35-38 驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州中宽度模式

模式
\l \d{3} \d{3} \d{3} \d{3}
\d{12}
\d{3}-\d{3}-\d{2}-\d{3}-\d{3}-\d
\-\d{3}-\d{3}-\d{3}-\d{3}

表 35-39

必选验证器	说明
查找关键字	要求至少存在一个输入关键字或关键短语，以便匹配数据。
查找关键字输入	driver license、drivers license、driver's license、driver licenses、drivers licenses、driver's licenses、dl#、dls#、lic#、lics#
查找关键字	要求至少存在一个输入关键字或关键短语，以便匹配数据。
查找关键字输入	fla、fl、florida、michigan、mi、minnesota、mn

驾驶执照号码 - 伊利诺斯州数据标识符

此号码是由美国伊利诺斯州颁发的个人驾照的标识号码。

驾驶执照号码 - 伊利诺斯州数据标识符检测是否存在伊利诺斯驾驶执照号码。

此数据标识符提供两个验证宽度：

- 大宽度版本检测是否存在 12 个字符的字符串。
请参见第 543 页的“[驾驶执照号码 - 伊利诺斯州大宽度](#)”。
- 中宽度通过要求存在关键字来缩小范围。
请参见第 543 页的“[驾驶执照号码 - 伊利诺斯州中宽度](#)”。

驾驶执照号码 - 伊利诺斯州大宽度

大宽度版本的驾驶执照号码 - 伊利诺斯州数据标识符检测 12 个字符的字符串，该字符串以一个字母（个人姓氏的第一个字母）开头，后跟 11 个数字。

注意：此宽度选项不包括任何验证器。

表 35-40 驾驶执照号码 - 伊利诺斯州大宽度模式

模式
\\\d{3}-\\d{4}-\\d{4}
\\d{11}

驾驶执照号码 - 伊利诺斯州中宽度

中宽度版本的驾驶执照号码 - 伊利诺斯州系统数据标识符检测 12 个字符的字符串，该字符串以一个字母（个人姓氏的第一个字母）开头，后跟 11 个数字。

该宽度还要求同时存在驾照关键字和与伊利诺斯相关的关键字。

表 35-41 驾驶执照号码 - 伊利诺斯州中宽度模式

模式
\\\\d{3}-\\d{4}-\\d{4}
\\d{11}

表 35-42 驾驶执照号码 - 伊利诺斯州中宽度验证器

必选验证器	说明
查找关键字	要求至少存在一个输入关键字或关键短语，以便匹配数据。
查找关键字输入	driver license、drivers license、driver's license、driver licenses、drivers licenses、driver's licenses、dl#、dls#、lic#、lics#
查找关键字	要求至少存在一个输入关键字或关键短语，以便匹配数据。
查找关键字输入	il、illinois

驾驶执照号码 - 新泽西州数据标识符

此号码是由美国新泽西州颁发的个人驾照的标识号码。

驾驶执照号码 - 新泽西州数据标识符检测是否存在新泽西州驾驶执照号码。

此数据标识符提供两个验证宽度：

- 大宽度版本检测是否存在 15 个字符的字符串。
请参见第 544 页的“[驾驶执照号码 - 新泽西州大宽度](#)”。
- 中宽度通过要求存在关键字来缩小范围。
请参见第 545 页的“[驾驶执照号码 - 新泽西州中宽度](#)”。

驾驶执照号码 - 新泽西州大宽度

大宽度版本的驾驶执照号码-新泽西州数据标识符检测 15 个字符的字符串，该字符串以一个字母（个人姓氏的第一个字母）开头，后跟 14 个数字。

注意：大宽度选项不包括任何验证器。

表 35-43 驾驶执照号码 - 新泽西州大宽度模式

模式
\l\l\d{4} \d{5} \d{5}
\l\d{14}

驾驶执照号码 - 新泽西州中宽度

中宽度版本的驾驶执照号码 - 新泽西州数据标识符检测 15 个字符的字符串，该字符串以一个字母（个人姓氏的第一个字母）开头，后跟 11 个数字。

该宽度还要求同时存在驾照关键字和与新泽西相关的关键字。

表 35-44 驾驶执照号码 - 新泽西州中宽度模式

模式
\\\d{3}-\\d{4}-\\d{4}
\\d{11}

表 35-45 驾驶执照号码 - 新泽西州中宽度验证器

验证器	说明
查找关键字	要求至少存在一个输入关键字或关键短语，以便匹配数据。
查找关键字输入	driver license、drivers license、driver's license、driver licenses、drivers licenses、driver's licenses、dl#、dls#、lic#、lics#
查找关键字	要求至少存在一个输入关键字或关键短语，以便匹配数据。
查找关键字输入	nj、new jersey、newjersey

驾驶执照号码 - 纽约州数据标识符

此号码是美国纽约州颁发的个人驾照的标识号码。

驾驶执照号码 - 纽约州数据标识符检测是否存在纽约州驾驶执照号码。

此数据标识符提供两个验证宽度：

- 大宽度版本检测 9 个数位的字符串。
请参见第 544 页的“[驾驶执照号码 - 新泽西州大宽度](#)”。
- 中宽度通过要求存在关键字来缩小范围。
请参见第 545 页的“[驾驶执照号码 - 新泽西州中宽度](#)”。

驾驶执照号码 - 纽约州大宽度

大宽度版本的驾驶执照号码 - 纽约州数据标识符检测 9 位数的字符串。

注意：大宽度选项不包括任何验证器。

表 35-46 驾驶执照号码 - 纽约州大宽度模式

模式
\d{3} \d{3} \d{3}
\d{9}

驾驶执照号码 - 纽约州中宽度

中宽度版本的驾驶执照号码 - 纽约州数据标识符检测 9 个数位的字符串。

该宽度还要求同时存在驾照关键字和与纽约相关的关键字。

表 35-47 驾驶执照号码 - 纽约州大宽度模式

模式
\I\d{3}-\d{4}-\d{4}
\d{11}

表 35-48

必选验证器	说明
查找关键字	要求至少存在一个输入关键字或关键短语，以便匹配数据。
查找关键字输入	driver license、drivers license、driver's license、driver licenses、drivers licenses、driver's licenses、dl#、dls#、lic#、lics#
查找关键字	要求至少存在一个输入关键字或关键短语，以便匹配数据。
查找关键字输入	new york、ny、newyork

法国国家统计局代码数据标识符

法国国家统计局代码用作社会保险号码、国家标识号码，并且还用于纳税和就业目的。

法国国家统计局代码数据标识符检测国家统计局号码是否存在。

大宽度版本的法国国家统计局代码数据标识符检测 15 个数字的号码，它是对出生日期、源部门、源社区和订单号的编码。前 13 个数字后的空格分隔符是可选的。国家统计局代码的最后两个数字是对用于验证校验和的控制键的编码。

表 35-49 法国国家统计局代码大宽度模式

模式
\d{13} \d{2}
d{15}

表 35-50 法国国家统计局代码大宽度验证器

必选验证器	说明
INSEE 控制键	该验证器将计算 INSEE 控制键，并将其与模式的最后两个数字进行比较。

香港特别行政区 ID 数据标识符

香港特别行政区 ID 是所有香港特别行政区居民的唯一标识符，显示在香港特别行政区身份证上。

香港特别行政区 ID 数据标识符检测香港特别行政区 ID 是否存在。

大宽度版本的香港特别行政区 ID 数据标识符检测格式为 LDDDDDDD(D) 或 LDDDDDDD(A) 的 8 个字符。已检测的字符串中的最后一个字符用于验证校验和。

表 35-51 香港特别行政区 ID 大宽度模式

模式
\w\d{6}(\d)
\w\d{6}(A)
U\w\d{6}(\d)
U\w\d{6}(A)

表 35-52 香港特别行政区 ID 大宽度验证器

必选验证器	说明
香港特别行政区 ID	计算校验和并根据校验和对模式进行验证

IBAN 中部数据标识符

国际银行账号 (IBAN) 是用于识别跨国界的银行账户的国际标准。

IBAN 中部数据标识符检测安道尔、奥地利、比利时、德国、意大利、列支敦士登、卢森堡、马耳他、摩纳哥、圣马力诺和瑞士的 IBAN 号码。

大宽度版本的 IBAN 中部数据标识符检测通过校验和的国家/地区特定的 IBAN 号码。IBAN 号码可以包括空格分隔符、短横线分隔符或不包括任何分隔符。

表 35-53 IBAN 中部大宽度模式

模式	说明
AD\{2}\d{4}\d{4}\w{4}\w{4}\w{4}	安道尔模式
AD\{2} \d{4} \d{4} \w{4} \w{4} \w{4}	
AD\{2}-\d{4}-\d{4}-\w{4}-\w{4}-\w{4}	
AT\{2}\d{4}\d{4}\d{4}\d{4}	奥地利模式
AT\{2} \d{4} \d{4} \d{4} \d{4}	
AT\{2}-\d{4}-\d{4}-\d{4}-\d{4}	
BE\d{2}\d{4}\d{4}\d{4}	比利时模式
BE\d{2} \d{4} \d{4} \d{4}	
BE\{2}-\d{4}-\d{4}-\d{4}	
CH\d{2}\d{4}\d{w{3}}\w{4}\w{4}\w	瑞士模式
CH\{2} \d{4} \d{w{3}} \w{4} \w{4} \w	
CH\{2}-\d{4}-\d{w{3}}-\w{4}-\w{4}-\w	
DE\{2}\d{4}\d{4}\d{4}\d{2}	德国模式
DE\{2} \d{4} \d{4} \d{4} \d{2}	
DE\{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	
IT\{2}[A-Z]\d{3}\d{4}\d{3}\w{4}\w{4}\w{3}	意大利模式
IT\{2} [A-Z]\d{3} \d{4} \d{3} \w{4} \w{4} \w{3}	
IT\{2}-[A-Z]-\d{3}-\d{4}-\d{3}-\w{4}-\w{4}-\w{3}	
LI\d{2}\d{4}\d\w{3}\w{4}\w{4}\w	列支敦士登模式
LI\{2} \d{4} \d \w{3} \w{4} \w{4} \w	
LI\{2}-\d{4}-\d\w{3}-\w{4}-\w{4}-\w{4}	

模式	说明
LU\{2}\{3}\w\{4}\w\{4}\w\{4}	卢森堡模式
LU\{2}\{3}\w\{4}\w\{4}\w\{4}	
LU\{2}-\{3}\w-\w\{4}-\w\{4}-\w\{4}	
MC\{2}\{4}\{4}\{2}\w\{2}\w\{4}\w\{4}\w\{2}	摩纳哥模式
MC\{2}\{4}\{4}\{2}\w\{2}\w\{4}\w\{4}\w\{2}	
MC\{2}-\{4}-\{4}-\{2}\w\{2}-\w\{4}-\w\{4}-\w\{2}	
MT\{2}[A-Z]\{4}\{4}\{2}\w\{3}\w\{4}\w\{4}\w\{3}	马耳他模式
MT\{2}[A-Z]\{4}\{4}\{2}\w\{3}\w\{4}\w\{4}\w\{4}\w\{3}	
MT\{2}[A-Z]\{4}-\{4}-\{2}\w\{3}-\w\{4}-\w\{4}-\w\{4}-\w\{3}	
SM\{2}[A-Z]\{3}\{4}\{3}\w\{4}\w\{4}\w\{3}	圣马力诺模式
SM\{2}[A-Z]\{3}\{4}\{3}\w\{4}\w\{3}\w\{4}\w\{4}\w\{3}	
SM\{2}[A-Z]\{3}-\{4}-\{3}\w-\w\{4}-\w\{4}-\w\{3}	

表 35-54 IBAN 中部大宽度验证器

验证器	说明
Mod 97 验证器	计算完全匹配项的 ISO 7064 Mod 97-10 校验和。

IBAN 东部数据标识符

国际银行账号 (IBAN) 是用于识别跨国界的银行账户的国际标准。

IBAN 东部数据标识符检测波斯尼亚、保加利亚、克罗地亚、塞浦路斯、捷克共和国、爱沙尼亚、希腊、匈牙利、以色列、拉脱维亚、立陶宛、马其顿、黑山、波兰、罗马尼亚、塞尔维亚、斯洛伐克、斯洛文尼亚、土耳其和突尼斯的 IBAN 号码。

大宽度 IBAN 东部数据标识符检测通过校验和的国家/地区特定的 IBAN 号码。IBAN 号码可以包括空格分隔符、短横线分隔符或不包括任何分隔符。

表 35-55 IBAN 东部大宽度模式

模式	说明
BA\d{2}\d{4}\d{4}\d{4}\d{4}	波斯尼亚模式
BA\d{2}\d{4}\d{4}\d{4}\d{4}	
BA\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	
BG\d{2}[A-Z]\d{4}\d{4}\d{2}\w{2}\w{4}\w{2}	保加利亚模式
BG\d{2}[A-Z]\d{4}\d{4}\d{2}\w{2}\w{4}\w{2}	
BG\d{2}-[A-Z]\d{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{2}	
CY\d{2}\d{4}\d{4}\w{4}\w{4}\w{4}\w{4}	塞浦路斯模式
CY\d{2}\d{4}\d{4}\w{4}\w{4}\w{4}\w{4}	
CY\d{2}-\d{4}-\d{4}-\w{4}-\w{4}-\w{4}-\w{4}	
CZ\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	捷克共和国模式
CZ\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	
CZ\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
EE\d{2}\d{4}\d{4}\d{4}\d{4}	爱沙尼亚模式
EE\d{2}\d{4}\d{4}\d{4}\d{4}	
EE\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	
GR\d{2}\d{4}\d{3}\w{\w{4}}\w{4}\w{3}	希腊模式
GR\d{2}\d{4}\d{3}\w{\w{4}}\w{4}\w{4}\w{3}	
GR\d{2}-\d{4}-\d{3}\w{\w{4}}-\w{4}-\w{4}-\w{3}	
HR\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	克罗地亚模式
HR\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	
HR\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
HU\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4}	匈牙利模式
HU\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4}	
HU\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
IL\d{2}\d{4}\d{4}\d{4}\d{4}\d{3}	以色列模式
IL\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{3}	
IL\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{3}	

模式	说明
LT\d{2}\d{4}\d{4}\d{4}\d{4}	立陶宛模式
LT\d{2}\d{4}\d{4}\d{4}\d{4}	
LT\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	
LV\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w	拉脱维亚模式
LV\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w	
LV\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{4}-\w	
ME\d{2}\d{4}\d{4}\d{4}\d{4}\d{2}	黑山模式
ME\d{2}\d{4}\d{4}\d{4}\d{4}\d{2}	
ME\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	
MK\d{2}\d{3}\w{4}\w{4}\w{4}\w\d{2}	马其顿模式
MK\d{2}\d{3}\w{4}\w{4}\w{4}\w\d{2}	
MK\d{2}-\d{3}-\w{4}-\w{4}-\w{4}-\w\d{2}	
PL\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	波兰模式
PL\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	
PL\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
RO\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w{4}\w{4}	罗马尼亚模式
RO\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w{4}\w{4}	
RO\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{4}-\w{4}	
RS\d{2}\d{4}\d{4}\d{4}\d{4}\d{2}	塞尔维亚模式
RS\d{2}\d{4}\d{4}\d{4}\d{4}\d{2}	
RS\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	
SI\d{2}\d{4}\d{4}\d{4}\d{4}\d{3}	斯洛文尼亚模式
SI\d{2}\d{4}\d{4}\d{4}\d{4}\d{3}	
SI\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{3}	
SK\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	斯洛伐克共和国模式
SK\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	
SK\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	

模式	说明
TN59\d{4}\d{4}\d{4}\d{4}\d{4}	突尼斯模式
TN59 \d{4} \d{4} \d{4} \d{4} \d{4}	
TN59-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
TR\d{2}\d{4}\d\w{3}\w{4}\w{4}\w{4}\w{2}	土耳其模式
TR\d{2}\d{4}\d\w{3}\w{4}\w{4}\w{4}\w{2}	
TR\d{2}-\d{4}-\d\w{3}-\w{4}-\w{4}-\w{4}-\w{2}	

表 35-56 IBAN 东部大宽度验证器

验证器	说明
Mod 97 验证器	计算完全匹配项的 ISO 7064 Mod 97-10 校验和。

IBAN 西部数据标识符

国际银行账号 (IBAN) 是用于识别跨国界的银行账户的国际标准。

IBAN 西部数据标识符检测丹麦、法罗群岛、芬兰、法国、直布罗陀、格陵兰、冰岛、爱尔兰、荷兰、挪威、葡萄牙、西班牙、瑞典和英国的 IBAN 号码。

大宽度 IBAN 西部数据标识符检测通过校验和的国家/地区特定的 IBAN 号码。IBAN 号码可以包括空格分隔符、短横线分隔符或不包括任何分隔符。

表 35-57 IBAN 西部大宽度模式

模式	说明
DK\d{2}\d{4}\d{4}\d{4}\d{2}	丹麦模式
DK\d{2} \d{4} \d{4} \d{4} \d{2}	
DK\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	
ES\d{2}\d{4}\d{4}\d{4}\d{4}	西班牙模式
ES\d{2} \d{4} \d{4} \d{4} \d{4}	
ES\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	
FI\d{2}\d{4}\d{4}\d{4}\d{2}	芬兰模式
FI\d{2} \d{4} \d{4} \d{4} \d{2}	
FI\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	

模式	说明
FO\d{2}\d{4}\d{4}\d{4}\d{2}	法罗群岛模式
FO\d{2} \d{4} \d{4} \d{4} \d{2}	
FO\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	
FR\d{2}\d{4}\d{4}\d{2}\w{2}\w{4}\w{4}\w{2}	法国模式
FR\d{2} \d{4} \d{4} \d{2} \w{2} \w{4} \w{4}	
FR\d{2}-\d{4}-\d{4}-\d{2}\w{2}\w{4}-\w{4}-\w{2}	
GB\d{2}[A-Z]\d{4}\d{4}\d{4}\d{4}\d{2}	英国模式
GB\d{2} [A-Z]\d{4} \d{4} \d{4} \d{4} \d{2}	
GB\d{2}-[A-Z]\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	
GI\d{2}[A-Z]\d{4}\w{4}\w{4}\w{4}\w{3}	直布罗陀模式
GI\d{2} [A-Z]\d{4} \w{4} \w{4} \w{4} \w{3}	
GI\d{2}-[A-Z]\d{4}-\w{4}-\w{4}-\w{4}-\w{3}	
GL\d{2}\d{4}\d{4}\d{4}\d{4}\d{2}	格陵兰模式
GL\d{2} \d{4} \d{4} \d{4} \d{4} \d{2}	
GL\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	
IE\d{2}[A-Z]\d{4}\d{4}\d{4}\d{4}\d{2}	爱尔兰模式
IE\d{2} [A-Z]\d{4} \d{4} \d{4} \d{4} \d{2}	
IE\d{2}-[A-Z]\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	
IS\d{2}\d{4}\d{4}\d{4}\d{4}\d{2}	冰岛模式
IS\d{2} \d{4} \d{4} \d{4} \d{4} \d{2}	
IS\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	
NL\d{2}[A-Z]\d{4}\d{4}\d{4}\d{2}	荷兰模式
NL\d{2} [A-Z]\d{4} \d{4} \d{4} \d{2}	
NL\d{2}-[A-Z]\d{4}-\d{4}-\d{4}-\d{2}	
NO\d{2}\d{4}\d{4}\d{3}	黑山模式
NO\d{2} \d{4} \d{4} \d{3}	
NO\d{2}-\d{4}-\d{4}-\d{3}	

模式	说明
PT\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4}	葡萄牙模式
PT\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{4}	
PT\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
SE\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	瑞典模式
SE\d{2} \d{4} \d{4} \d{4} \d{4} \d{4}	
SE\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	

表 35-58 IBAN 西部大宽度模式

验证器	说明
Mod 97 验证器	计算完全匹配项的 ISO 7064 Mod 97-10 校验和。

IP 地址数据标识符

IP 地址是用于标识设备和方便通信的计算机网络代码。

IP 地址数据标识符可检测 IP 地址。

此数据标识符提供三种检测宽度：

- 大
请参见第 554 页的“[IP 地址大宽度](#)”。
- 中
请参见第 555 页的“[IP 地址中宽度](#)”。
- 小
请参见第 555 页的“[IP 地址小宽度](#)”。

IP 地址大宽度

大宽度版本的 IP 地址数据标识符检测 DDD.DDD.DDD.DDD 格式（具有可选 /DD）的号码。每三个数字组必须介于 0 和 255 之间（包括 0 和 255），/DD 必须介于 0 和 32 之间。此外，不允许使用 0.0.0.0。

表 35-59 IP 地址大宽度模式

模式
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}

模式

\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[0-9]

\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[1-2][0-9]?

\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?

表 35-60 IP 地址大宽度验证器

验证器	说明
IP 基本检查	每个 IP 地址必须符合格式 x.x.x.x，且每个号码必须小于 256。

IP 地址中宽度

中宽度版本的 IP 地址数据标识符检测 DDD.DDD.DDD.DDD 格式（具有可选 /DD）的号码。每三个数字组必须介于 0 和 255 之间（包括 0 和 255），/DD 必须介于 0 和 32 之间。此外，不允许使用 0.0.0.0。而且，排除常见虚构地址，例如全部为 1 位数匹配组（例如 1.1.1.2）。

表 35-61 IP 地址中宽度模式

模式

\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}

\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[0-9]

\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[1-2][0-9]?

\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?

表 35-62 IP 地址中宽度验证器

必选验证器	说明
IP 八位字节检查	每个 IP 地址必须符合格式 x.x.x.x，每个号码必须小于 256，且任何 IP 地址都不能仅包含单个数字的号码 (1.1.1.2)。

IP 地址小宽度

小宽度版本的 IP 地址数据标识符检测 DDD.DDD.DDD.DDD 格式（具有可选 /DD）的号码。每三个数字组必须介于 0 和 255 之间（包括 0 和 255），/DD 必须介于 0

和 32 之间。此外，不允许使用 0.0.0.0。而且，排除常见虚构地址，例如全部为 1 位数匹配组（例如 1.1.1.2）。并排除未指定的 IP 地址 (Bogon)。

表 35-63 IP 地址中宽度模式

模式
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[0-9]
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[1-2][0-9]?
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?

表 35-64 IP 地址大宽度验证器

必选验证器	说明
IP 八位字节检查	每个 IP 地址必须符合格式 x.x.x.x，每个号码必须小于 256，且任何 IP 地址都不能仅包含单个数字的号码 (1.1.1.2)。
IP 八位字节检查	检查 IP 地址是否属于任何 Bogons 范围。若是如此，则匹配项无效。

国家药品代码 (NDC) 数据标识符

国家药品代码 (NDC) 是由美国食品药品管理局 (FDA) 为单种药品颁发的标识符。HIPAA 条例定义了一种替代格式。

国家药品代码数据标识符检测是否存在 NDC 以及 HIPAA 版本。

此数据标识符提供三个检测宽度：

- 大宽度检查是否存在 NDC 号码或其 HIPAA 版本。
请参见第 541 页的“驾驶执照号码-佛罗里达州、密歇根州和明尼苏达州大宽度”。
- 中宽度限制检测号码的模式。
请参见第 542 页的“驾驶执照号码-佛罗里达州、密歇根州和明尼苏达州中宽度”。
- 小宽度要求具有关键词匹配项。
请参见第 542 页的“驾驶执照号码-佛罗里达州、密歇根州和明尼苏达州中宽度”。

国家药品代码 (NDC) 大宽度

大宽度版本的国家药品代码 (NDC) 数据标识符检测标准 FDA 格式，它是 10 个数字的号码，格式为 4-4-2、5-4-1 或 5-3-2，该号码以短横线或空格分隔。

此外，该数据标识符还检测 HIPAA 格式，它是 11 个数字的号码，格式为 5-4-2。HIPAA 格式可以包括代表缺失数字的单个星号。

表 35-65 国家药品代码 (NDC) 大宽度模式

模式
*?\d{4} \d{4} \d{2}
*?\d{4}-\d{4}-\d{2}
\d{5} *?\d{3} \d{2}
\d{5}-*?\d{3}-\d{2}
\d{5} \d{4} *?\d
\d{5}-\d{4}-*?\d
\d{5} \d{4} \d{2}
\d{5}-\d{4}-\d{2}

国家药品代码 (NDC) 中宽度

中宽度版本的国家药品代码 (NDC) 数据标识符检测标准 FDA 格式，它是 10 个数字的号码，格式为 4-4-2、5-4-1 或 5-3-2，该号码以短横线分隔。

此外，该数据标识符还检测 HIPAA 格式，它是 11 个数字的号码，格式为 5-4-2。HIPAA 格式可以包括代表缺失数字的单个星号。

注意：中宽度版本的该数据标识符不包括任何验证器。

注意：大宽度版本的该数据标识符允许以空格分隔 NDC 号码，而中宽度版本不允许。这就是该数据标识符的大宽度版本和中宽度版本之间的差异。

表 35-66 国家药品代码 (NDC) 中宽度模式

模式
*?\d{4}-\d{4}-\d{2}
\d{5}-*?\d{3}-\d{2}
\d{5}-\d{4}-*?\d
\d{5}-\d{4}-\d{2}

国家药品代码 (NDC) 小宽度

小宽度版本的国家药品代码 (NDC) 数据标识符检测标准 FDA 格式，它是 10 个数字的号码，格式为 4-4-2、5-4-1 或 5-3-2，该号码以短横线分隔。

此外，该数据标识符还检测 HIPAA 格式，它是 11 个数字的号码，格式为 5-4-2。HIPAA 格式可以包括代表缺失数字的单个星号。此数据标识符还要求存在与 NDC 相关的关键字。

表 35-67 国家药品代码 (NDC) 小宽度模式

模式
*?\d{4}-\d{4}-\d{2}
\d{5}-*\?\d{3}-\d{2}
\d{5}-\d{4}-*\?\d
\d{5}-\d{4}-\d{2}

表 35-68 国家药品代码 (NDC) 小宽度验证器

必选验证器	说明
查找关键字	选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。
查找关键字输入	ndc、国家药品代码

中华人民共和国 ID 数据标识符

中华人民共和国 ID 用于居住登记、征兵登记、结婚/离婚登记、出国旅行、参加各种国家考试以及参与国内其他社会或民间事务。

中华人民共和国 ID 数据标识符可检测此 18 位数字号码的存在。

大宽度版本的中华人民共和国 ID 数据标识符检测 18 位数字的号码，最后一位数用于验证校验和。

表 35-69 中华人民共和国 ID 大宽度模式

模式
\d{17}[Xx]
\d{18}

表 35-70 中华人民共和国 ID 大宽度验证器

必选验证器	说明
中国 ID 校验和验证器	计算校验和并根据校验和对模式进行验证

新加坡 NRIC 数据标识符

新加坡 NRIC（国民登记身份证）是新加坡使用的身份证明文件。对于某些政府程序、商业事务（例如开设银行帐户或通过交付或者换取出入证来进入建筑物），NRIC 是一个必需的文件。

大宽度版本的新加坡 NRIC 数据标识符可检测符合 LDDDDDDDDL 模式的 9 个字符。最后一个字符用于验证校验和。

表 35-71 新加坡 NRIC 大宽度模式

模式
[SFTGsftg]\d{7}\w

表 35-72 新加坡 NRIC 大宽度验证器

必选验证器	说明
新加坡 NRIC	计算新加坡 NRIC 的校验和，并根据该校验和对模式进行验证。

韩国居民登记号码数据标识符

韩国居民登记号码是一个颁发给所有韩国居民的 13 位号码。与其他国家/地区的国家身份证号码类似，它用于在各种私人事务（例如银行业务和就业）中标识人的身份。此外，该号码还广泛用于在线标识用途。

韩国居民登记号码数据标识符可检测此 13 位数字号码的存在。

此数据标识符提供两个验证宽度：

- 大宽度版本匹配使用短横线分隔符或不使用分隔符的号码。
请参见第 560 页的“[韩国居民登记号码大宽度](#)”。
- 中宽度版本仅匹配使用短横线分隔的号码。
请参见第 560 页的“[韩国居民登记号码中宽度](#)”。

此数据标识符不提供小宽度选项。

韩国居民登记号码大宽度

大宽度版本的韩国居民登记号码数据标识符检测包含已编码的出生日期、性别和籍贯的13位数字字符。该版本可匹配带短横线或无分隔符的模式，并使用校验和验证该模式。

表 35-73 韩国居民登记号码大宽度模式

模式
\d{2}[01]\d[0123]\d{8}
\d{2}[01]\d[0123]\d-\d{7}

表 35-74 韩国居民登记号码大宽度验证器

必选验证器	说明
数字分隔符	通过检查周围的数字验证匹配。
高级 KRRN 验证	验证第3个数字和第4个数字是否为有效月份，第5个数字和第6个数字是否为有效日，以及校验和是否匹配检查数字。

韩国居民登记号码中宽度

中宽度版本的韩国居民登记号码数据标识符检测包含已编码的出生日期、性别和籍贯的13位数字字符，并且也会使用校验和验证模式。此模式要求有短横线分隔符。

表 35-75 韩国居民登记号码中宽度模式

模式
\d\d[01]\d[0123]\d-\d{7}

表 35-76 韩国居民登记号码中宽度验证器

验证器	说明
数字分隔符	通过检查周围的数字验证匹配。
高级 KRRN 验证	验证第3个数字和第4个数字是否为有效月份，第5个数字和第6个数字是否为有效日，以及校验和是否匹配检查数字。

西班牙 DNI ID 数据标识符

西班牙 DNI ID 号码显示在身份证件 (DNI) 上，由 Hacienda Publica 颁发给每位西班牙公民。它是在西班牙使用的最重要的唯一标识符，开户、签署合同、纳税以及选举都要使用该号码。

大宽度版本的西班牙 DNIID 数据标识符可检测后跟连字符与字母的 8 位数字号码。对于外国国民，字母 X 和连字符可能显示在开头。最后一个字母必须匹配校验和算法。

表 35-77 西班牙 DNI ID 大宽度模式

模式
\d{8}-\w
X-\d{8}-\w

表 35-78 西班牙 DNI ID 大宽度验证器

必选验证器	说明
DNI 控制键检查	计算该控制键并检查其是否有效。

SWIFT 代码数据标识符

SWIFT 代码是银行的唯一标识符。由环球同业银行金融电讯协会 (SWIFT) 管理。金融机构之间转账时需要 SWIFT 代码。该代码也称为银行标识码 (BIC)。

SWIFT 代码数据标识符可检测 SWIFT 代码的存在。

此数据标识符提供两个验证宽度：

- 大宽度
请参见第 561 页的“[SWIFT 代码大宽度](#)”。
- 小宽度
请参见第 562 页的“[SWIFT 代码小宽度](#)”。

SWIFT 代码大宽度

大宽度版本的 SWIFT 代码数据标识符检测 8 个或 11 个字符的字符串。第 5 和第 6 个字符是国家/地区代码。此宽度模式还要求存在与 SWIFT 相关的关键字。

表 35-79 SWIFT 代码大宽度模式

模式
[A-Z]{6}\w{2}
[A-Z]{6}\w{5}

表 35-80 SWIFT 代码大宽度验证器

必选验证器	说明
需要开始字符	选中此选项时，匹配数据的开头需要以下列表中的任意值。
查找关键字	选中此选项时，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。
查找关键字输入	bic、bic#、international organization for standardization 9362、iso 9362、iso9362、swift、swift#、swiftcode、swiftnumber、swiftroutingnumber。

SWIFT 代码小宽度

小宽度版本的 SWIFT 代码数据标识符可检测 8 个或 11 个字符的字符串。第 5 和第 6 个字符是指代国家/地区代码的字母。此宽度还要求存在具体的与 SWIFT 相关的关键字。

表 35-81 SWIFT 代码小宽度模式

模式
[A-Z]{6}\w{2}
[A-Z]{6}\w{5}

表 35-82 SWIFT 代码小宽度验证器

验证器	说明
需要开始字符	选中此选项时，匹配数据的开头需要以下列表中的任意值。
查找关键字	选中此选项，对于要匹配的数据，必须至少存在以下关键字或关键短语之一。

验证器	说明
查找关键字输入	bic#、international organization for standardization 9362、iso 9362、iso9362、swift#、swiftcode、swiftnumber、swiftroutingnumber、swift code、swift number、swift routing number、bic number、bic code、bic #

瑞士 AHV 号码数据标识符

在瑞士，老年和遗属保险基金号码（Alters- und Hinterlassenensversicherungsnummer - AHV 号码）是最重要的公共 ID 号码。

瑞士 AHV 号码数据标识符可检测带有或不带标准句点分隔符的 11 位数字的标识符 (DDD.DD.DDD.DDD)，并会对照校验和算法进行验证。

表 35-83 瑞士 AHV 号码大宽度模式

模式
\d{8}\w
X-\d{8}\w

表 35-84 瑞士 AHV 号码大宽度验证器

验证器	说明
瑞士 AHV	瑞士 AHV Modulus 11 校验和。
数字分隔符	通过检查周围的数字验证匹配。

中国台湾 ID 数据标识符

在中国台湾，所有年龄超过 14 周岁的公民都必须使用身份证。该身份证自 1965 年以来统一编号。

中国台湾 ID 数据标识符检测存在的中国台湾标识号码，该标识号码基于两种类型的公用 ID 模式。最后一个匹配的字符用于验证校验和。

表 35-85 中国台湾 ID 大宽度模式

模式
[A-Z][12][0-3]\d{7}

模式

[A-Z][ABCD]\d{8}

表 35-86

中国台湾 ID 大宽度验证器

验证器**说明**

中国台湾 ID	中国台湾 ID 校验和。
---------	--------------

英国驾照号数据标识符

英国驾照号是由英国驾驶员与车辆管理所颁发的个人驾照的标识号码。

英国驾照号数据标识符检测英国驾照号是否存在。

此数据标识符提供三种验证宽度：

- 大

请参见第 564 页的“[英国驾照号大宽度](#)”。

- 中

请参见第 564 页的“[英国驾照号中宽度](#)”。

- 小

请参见第 565 页的“[英国驾照号小宽度](#)”。

英国驾照号大宽度

大宽度版本的英国驾照号数据标识符可检测以下格式的 16 个字符的字符串：

AAAAAAD[0,1,5,6]DDDDAAALL，其中 A 是字母数字字符，D 是数字，L 是字母。

注意：此宽度选项不包括任何验证器。

表 35-87

英国驾照号大宽度模式

模式

\w{5}\d{0156}\d{4}\w{3}\l{2}

\w{5} \d{0156}\d{4} \w{3}\l{2}

英国驾照号中宽度

中宽度版本的英国驾照号数据标识符可检测以下格式的 16 个字符的字符串：

AAAAAAD[0,1,5,6]DDDDAAALL，其中 A 是字母数字字符，D 是数字，L 是字母。

数字部分中的第一个数字限制为 0、1、5 或 6。此外，数字部分中的第 4 和 5 个数字必须介于 01 和 31 之间（包括 01 和 31）。

表 35-88 英国驾照号中宽度模式

模式
\w{5}\d[0156]\d{4}\w{3}\l{2}
\w{5} \d[0156]\d{4} \w{3}\l{2}

表 35-89 英国驾照号中宽度验证器

必选验证器	说明
英国驾照	每个英国驾照必须包括 16 个字符，第 8 和第 9 位置的数字必须大于 00 且小于 32。

英国驾照号小宽度

小宽度版本的英国驾照号数据标识符可检测以下格式的 16 个字符的字符串：
AAAAAD[0,1,5,6]DDDDAAALL，其中 A 是字母数字字符，D 是数字，L 是字母。
数字部分的第一个数字限制为 0、1、5 或 6。此外，数字部分的第 4 和 5 个数字必须介于 01 和 31 之间（包括 01 和 31）。

此外，小宽度版本还要求同时存在与驾照相关的关键字和与英国相关的关键字。

表 35-90 英国驾照号小宽度模式

模式
\w{5}\d[0156]\d{4}\w{3}\l{2}
\w{5} \d[0156]\d{4} \w{3}\l{2}

表 35-91 英国驾照号小宽度验证器

必选验证器	说明
英国驾照	每个英国驾照必须包括 16 个字符，第 8 和第 9 位置的数字必须大于 00 且小于 32。
查找关键字：与驾照相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： british、the united kingdom、uk、united kingdom、unitedkingdom

必选验证器	说明
查找关键字：与英国相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： british、the united kingdom、uk、united kingdom、unitedkingdom

英国选民登记号数据标识符

选民登记号是颁发给个人以进行英国选举登记的标识号码。该号码的格式按英国内阁办公厅的英国政府标准指定。

英国选民登记号数据标识符可检测英国选民登记号的存在。该标识符实施了一个模式，用于检测包含 2 到 3 个字母并且后跟 1 到 4 个数字的字符串。

表 35-92 英国选民登记号大宽度模式

模式
\{2,3\}\d{1,4}

大宽度版本的选民登记号数据标识符实施了两个验证器，要求存在与选民号码相关的关键字和与英国相关的关键字。

表 35-93 英国选民登记号大宽度验证器

验证器	说明
查找关键字：与选民号码相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： electoral #、electoral number、electoral roll #、electoral roll no.、electoral roll number、electoral roll#、electoral#、electoralnumber、electoralroll#、electoralrollno
查找关键字：与英国相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： british、the united kingdom、uk、united kingdom、unitedkingdom

英国国民保健服务 (NHS) 号数据标识符

英国国民保健服务 (NHS) 是由英国国家卫生署 (NHS) 颁发的个人标识号码，用于进行医疗管理。

英国国民保健服务 (NHS) 号数据标识符可检测英国国民保健服务 (NHS) 号的存在。

此数据标识符提供两个验证宽度：

■ 中

请参见第 567 页的“[英国国民保健服务 \(NHS\) 号中宽度](#)”。

■ 小

请参见第 568 页的“[英国国民保健服务 \(NHS\) 号小宽度](#)”。

注意：此数据标识符不提供大宽度选项。

英国国民保健服务 (NHS) 号中宽度

英国国民保健服务 (NHS) 号数据标识符的中宽度版实施用于检测当前定义的、包含各种分隔符的 NHS 格式 DDD-DDD-DDDD（其中 D 是一个数字）的编号的模式。

表 35-94 英国国民保健服务 (NHS) 号中宽度模式

模式	说明
\d{3}.\d{3}.\d{4}	该模式用于检测以句点分隔的 DDD-DDD-DDDD 格式。
\d{3} \d{3} \d{4}	该模式用于检测以空格分隔的 DDD-DDD-DDDD 格式。
\d{3}-\d{3}-\d{4}	该模式用于检测以短横线分隔的 DDD-DDD-DDDD 格式。

英国国民保健服务 (NHS) 号数据标识符的中宽度版实施三个验证器：一个用于验证 NHS 校验和，另一个使用最后数字执行数值验证，第三个用于检查是否存在与 NHS 相关的关键字。

表 35-95 英国国民保健服务 (NHS) 号中宽度验证器

验证器	说明
英国 NHS	英国 NHS 校验和。
数字分隔符	通过检查周围的数字验证匹配。

验证器	说明
查找关键字：与 NHS 相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： national health service、NHS

英国国民保健服务 (NHS) 号小宽度

小宽度版本的英国国民保健服务 (NHS) 号数据标识符实施多种模式来检测当前定义格式的号码：DDD-DDD-DDDD（其中 D 是数字），由短横线、空格或句点分隔。

表 35-96 英国国民保健服务 (NHS) 号小宽度模式

模式	说明
\d{3}.\d{3}.\d{4}	该模式用于检测以句点分隔的 DDD-DDD-DDDD 格式。
\d{3} \d{3} \d{4}	该模式用于检测以空格分隔的 DDD-DDD-DDDD 格式。
\d{3}-\d{3}-\d{4}	该模式用于检测以短横线分隔的 DDD-DDD-DDDD 格式。

小宽度版本的英国国民保健服务 (NHS) 号数据标识符实施了四个验证器：一个验证 NHS 校验和，另一个使用最后数字执行数字验证，第三个要求存在与 NHS 相关的关键字，第四个要求存在与英国相关的关键字。

表 35-97 英国国民保健服务 (NHS) 号小宽度验证器

必选验证器	说明
英国 NHS	英国 NHS 校验和。
数字分隔符	通过检查周围的数字验证匹配。
查找关键字：与 NHS 相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： national health service、NHS
查找关键字：与英国相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： uk、united kingdom、britain、england、gb

英国国家保险号码数据标识符

英国国家保险号码是由英国就业及退休金部(DWP)颁发的，用于标识国家保险计划中的个人。也称为 NI 号码、NINO 或 NINo。

英国国家保险号码数据标识符可检测英国国家保险号码的存在。

此数据标识符提供三种验证宽度：

- 大
请参见第 569 页的“[英国国家保险号码大宽度](#)”。
- 中
请参见第 569 页的“[英国国家保险号码中宽度](#)”。
- 小
请参见第 570 页的“[英国国家保险号码小宽度](#)”。

英国国家保险号码大宽度

大宽度版本的英国国家保险号码数据标识符实施多种模式来检测 9 位数的号码，号码的格式为 LL DD DD DD L（其中 L 是字母，D 是数字），由空格、句点、短横线分隔或全部处于一个字符串中。

第一和第二个字母不能是 D、F、I、Q、U 和 V。此外，第二个字母还不能是 O。

表 35-98 英国国家保险号码大宽度模式

模式	说明
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z].\d{2}.\d{2}.\d{2}-[ABCD]	由句点分隔。
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]\d{2}\d{2}\d{2}[ABCD]	未分隔。
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	由空格分隔。
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]-\d{2}-\d{2}-\d{2}-[ABCD]	由短横线分隔。
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	多个号码位组成一个字符串。

英国国家保险号码中宽度

中宽度版本的英国国家保险号码数据标识符实施多种模式来检测 9 位数的号码，号码的格式为 LL DD DD DD L（其中 L 是字母，D 是数字），由空格分隔或全部处于一个字符串中。

第一和第二个字母不能是 D、F、I、Q、U 和 V。此外，第二个字母还不能是 O。

表 35-99 英国国家保险号码中宽度模式

模式	说明
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	未分隔。
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	由空格分隔。
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	多个字符组成一个字符串。

英国国家保险号码小宽度

小宽度版本的英国国家保险号码数据标识符实施多种模式来检测 9 位数的号码，号码的格式为 LL DD DD DD L（其中 L 是字母，D 是数字），由空格分隔或全部处于一个字符串中。

第一和第二个字母不能是 D、F、I、Q、U 和 V。此外，第二个字母还不能是 O。

表 35-100 英国国家保险号码小宽度模式

模式	说明
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	未分隔。
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	由空格分隔。
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	多个字符组成一个字符串。

小宽度版本的英国国家保险号码数据标识符实施了一个验证器，要求存在与国家保险相关的关键字。

表 35-101 英国国家保险号码小宽度验证器

必选验证器	说明
查找关键字：与保险相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： insurance no.、insurance number、insurance#、insurancenumber、national insurance number、nationalinsurance#、nationalinsurancenumber、nin、nino

英国护照号数据标识符

英国护照号使用英国内阁办公厅的英国政府标准的当前官方规范来标识英国护照。

英国护照号数据标识符可检测英国护照号的存在。

此数据标识符提供三种验证宽度：

■ 大

请参见第 571 页的“[英国护照号大宽度](#)”。

■ 中

请参见第 571 页的“[英国护照号中宽度](#)”。

■ 小

请参见第 572 页的“[英国护照号小宽度](#)”。

英国护照号大宽度

大宽度版本的英国护照号数据标识符实施一个模式来检测 9 位数的号码。

注意：大宽度版本的英国护照号数据标识符不包含任何验证器。

表 35-102 英国护照号大宽度模式

模式	说明
\d{9}	该模式用于检测 9 位数的号码。

英国护照号中宽度

中宽度版本的英国护照号数据标识符实施一个模式来检测 9 位数的号码。

表 35-103 英国护照号中宽度模式

模式	说明
\d{9}	该模式用于检测 9 位数的号码。

中宽度版本的英国护照号数据标识符实施了三个验证器：一个用于排除常见测试号码，例如123456789；另一个用于排除数字全部相同的号码；第三个则要求存在与护照相关的关键字。

表 35-104 英国护照号中宽度验证器

必选验证器	说明
排除开始字符	将不会匹配开头为以下列表中任意值的数据： 123456789
重复数字	保证数字字符串不全相同。
查找关键字：与护照相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： passport、passport#、passportID、passportno、passportnumber

英国护照号小宽度

小宽度版本的英国护照号数据标识符实施一个模式来检测 9 位数的号码。

表 35-105 英国护照号小宽度模式

模式	说明
\d{9}	该模式用于检测 9 位数的号码。

小宽度版本的英国护照号数据标识符实施了四个验证器：一个用于排除常见测试号码，例如123456789；另一个用于排除数字全部相同的号码；第三个要求存在与护照相关的关键字；第四个要求存在与英国相关的关键字。

表 35-106 英国护照号小宽度验证器

必选验证器	说明
排除开始字符	将不会匹配开头为以下列表中任意值的数据： 123456789
重复数字	保证数字字符串不全相同。
查找关键字：与护照相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： passport、passport#、passportID、passportno、passportnumber
查找关键字：与英国相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： uk、united kingdom、britain、england、gb

英国税号数据标识符

英国税号是按英国内阁办公厅的英国政府标准提供的个人标识号码。

英国税号数据标识符可检测英国税号的存在。

此数据标识符提供三种验证宽度：

■ 大

请参见第 573 页的“[英国税号大宽度](#)”。

■ 中

请参见第 573 页的“[英国税号中宽度](#)”。

■ 小

请参见第 574 页的“[英国税号小宽度](#)”。

英国税号大宽度

大宽度版本的英国税号数据标识符实施一个单个模式来检测 10 个数字的号码。

注意：大宽度版本的英国税号数据标识符不包含任何验证器。

表 35-107 英国护照号大宽度模式

模式	说明
\d{10}	该模式用于检测 10 位数的号码。

英国税号中宽度

中宽度版本的英国税号数据标识符实施一个单个模式来检测 10 个数字的号码。

表 35-108 英国税号中宽度模式

模式	说明
\d{10}	该模式用于检测 10 位数的号码。

中宽度版本的英国税号数据标识符实施了两个验证器：一个用于排除常见测试号码，例如 1234567890，另一个用于排除数字全部相同的号码。

表 35-109 英国税号中宽度验证器

必选验证器	说明
重复数字	保证数字字符串不全相同。

必选验证器	说明
排除开始字符	将不会匹配开头为以下列表中任意值的数据: 0123456789, 1234567890, 9876543210, 0987654321

英国税号小宽度

小宽度版本的英国税号数据标识符实施一个单个模式来检测 10 个数字的号码。

表 35-110 英国税号小宽度模式

模式	说明
\d{10}	该模式用于检测 10 位数的号码。

小宽度版本的英国税号数据标识符实施了三个验证器：一个用于排除常见测试号码，例如 1234567890；另一个用于排除数字全部相同的号码；第三个则要求存在与税务 ID 相关的关键字。

表 35-111 英国税号小宽度验证器

必选验证器	说明
重复数字	保证数字字符串不全相同。
排除开始字符	将不会匹配开头为以下列表中任意值的数据： 0123456789, 1234567890, 9876543210, 0987654321
查找关键字：与税务 ID 相关	对于要匹配的数据，必须至少存在以下关键字或关键短语之一： tax id、tax id no.、tax id number、tax identification、tax identification#、tax no.、tax#、taxid#

美国个人纳税识别号 (ITIN) 数据标识符

美国个人纳税识别号 (ITIN) 是由美国国税局 (IRS) 颁发的用于税务处理的号码。IRS 颁发 ITIN 以便跟踪无资格获取社会安全号 (SSN) 的个人。

美国个人纳税识别号 (ITIN) 数据标识符可检测美国 ITIN 号码的存在。

此数据标识符提供三种验证宽度：

- 大

请参见第 575 页的“[美国个人纳税识别号 \(ITIN\) 大宽度](#)”。

■ 中

请参见第 575 页的“[美国个人纳税识别号 \(ITIN\) 中宽度](#)”。

■ 小

请参见第 576 页的“[美国个人纳税识别号 \(ITIN\) 小宽度](#)”。

美国个人纳税识别号 (ITIN) 大宽度

大宽度版本的美国个人纳税识别号 (ITIN) 数据标识符实施了多种模式来检测 9 个数位的号码，号码模式为 DDD-DD-DDDD，以短横线、空格、句点、斜杠分隔或不使用分隔符分隔。

该号码必须以 9 开头，第 4 个数字为 7 或 8。

注意：大宽度版本的美国个人纳税识别号 (ITIN) 数据标识符不包含任何验证器。

表 35-112 美国个人纳税识别号 (ITIN) 大宽度模式

模式	说明
9\ d{2}[78]\ d\ d{4}	该模式用于检测不使用分隔符的 ITIN 格式。
9\ d{2}\ \ 78]\ d\ \ \ d{4}	该模式用于检测不使用分隔符的 ITIN 格式。
9\d{2}/[78]\d/\d{4}	该模式用于检测以斜杠分隔的 ITIN 格式。
9\d{2}.[78]\d.\d{4}	该模式用于检测以句点分隔的 ITIN 格式。
9\d{2} [78]\d \d{4}	该模式用于检测以空格分隔的 ITIN 格式。
9\d{2}-[78]\d-\d{4}	该模式用于检测以短横线分隔的 ITIN 格式。

美国个人纳税识别号 (ITIN) 中宽度

中宽度版本的美国个人纳税识别号 (ITIN) 数据标识符实施多种模式来检测 9 位数的号码，号码模式为 DDD-DD-DDDD，以短横线、空格或句点分隔。

该号码必须以 9 开头，第 4 个数字为 7 或 8。

表 35-113 美国个人纳税识别号 (ITIN) 中宽度模式

模式	说明
9\d{2}.[78]\d.\d{4}	该模式用于检测以句点分隔的 ITIN 格式。
9\d{2} [78]\d \d{4}	该模式用于检测以空格分隔的 ITIN 格式。

模式	说明
9\d{2}-[78]\d-\d{4}	该模式用于检测以短横线分隔的 ITIN 格式。

中宽度版本的美国个人纳税识别号 (ITIN) 数据标识符实施了一个单个验证器来检查周围的字符。

表 35-114 美国个人纳税识别号 (ITIN) 中宽度验证器

必选验证器	说明
数字分隔符	通过检查周围的字符来验证匹配项。

美国个人纳税识别号 (ITIN) 小宽度

小宽度版本的美国个人纳税识别号 (ITIN) 数据标识符采用检测 9 位数字号码的模式，这种号码的模式为 DDD-DD-DDDD，以短横线或空格分隔。

该号码必须以 9 开头，第 4 个数字为 7 或 8。

表 35-115 美国个人纳税识别号 (ITIN) 小宽度模式

模式	说明
9\d{2} [78]\d \d{4}	该模式用于检测以空格分隔的 ITIN 格式。
9\d{2}-[78]\d-\d{4}	该模式用于检测以短横线分隔的 ITIN 格式。

小宽度版本的美国个人纳税识别号 (ITIN) 数据标识符采用三个验证器：一个用于检查周围的字符，另一个用于确保 ITIN 字符串中的数字不完全相同，第三个验证器要求存在与 ITIN 相关的关键字。

表 35-116 美国个人纳税识别号 (ITIN) 小宽度验证器

必选验证器	说明
数字分隔符	通过检查周围的字符来验证匹配项。
重复数字	保证数字字符串不全相同。
查找关键字：ITIN 相关	对于要匹配的数据，必须存在至少一个下列关键字或关键短语。 个人纳税识别号、itin、it.i.n.

美国社会安全号 (SSN) 数据标识符

美国个人纳税识别号 (ITIN) 是由美国政府的社会保障局颁发的个人标识号码。尽管主要用于管理社会保障计划，但也广泛用作各种目的下的个人标识号码。

美国社会安全号 (SSN) 数据标识符用于检测是否存在美国社会安全号。

此数据标识符提供三种验证宽度：

- 大
请参见第 577 页的“[美国社会安全号 \(SSN\) 大宽度](#)”。
- 中
请参见第 578 页的“[美国社会安全号 \(SSN\) 中宽度](#)”。
- 小
请参见第 579 页的“[美国社会安全号 \(SSN\) 小宽度](#)”。

美国社会安全号 (SSN) 大宽度

大宽度版本的美国社会安全号 (SSN) 数据标识符采用检测 9 位数字号码的模式，这种号码的模式为 DDD-DD-DDDD，以短横线、空格、句点、斜杠分隔或不使用分隔符。

该号码必须以 9 开头，第 4 个数字为 7 或 8。

表 35-117 社会安全号 (SSN) 大宽度模式

模式	说明
\d{3}-\d{2}-\d{4}	匹配标准 SSN 格式，即任何三位数后跟连字符、两位数、连字符和任何四位数。
\d{3}.\d{2}.\d{4}	匹配由句点分隔的 SSN 格式。
\d{3} \d{2} \d{4}	匹配由空格分隔的 SSN 格式。
\d{3}\\\d{2}\\\d{4}	匹配由反斜杠分隔的 SSN 格式。
\d{3}/\d{2}/\d{4}	匹配由正斜杠分隔的 SSN 格式。
\d{9}	匹配未进行分隔的任何 9 位数字号码。

大宽度版本的美国社会安全号 (SSN) 数据标识符采用三个验证器，以确保检测的 SSN 处于指定的有效号码范围内、排除常见测试号码（例如 123456789）并且排除数字全部相同的号码。

表 35-118 社会安全号 (SSN) 大宽度验证器

验证器	说明
数字分隔符	通过检查周围的字符来验证匹配项。
高级 SSN	检查 SSN 的任何组中是否包含零，地区号码（第一组）是否小于 773 且不为 666，组之间的分隔符是否相同，号码不是由全部相同的数字组成，且该号码未保留作为广告用途（123-45-6789、987-65-432x）。
SSN 地区组号码	对于给定的地区号码（第一组），并非所有的组号码（第二组）都可由 SSA 分配。验证器将排除包含无效组号码的 SSN。

美国社会安全号 (SSN) 中宽度

中宽度版本的美国社会安全号 (SSN) 数据标识符采用检测 9 位数号码的模式，这种号码的模式为 DDD-DD-DDDD，以短横线、空格或句点分隔。

表 35-119 社会安全号 (SSN) 中宽度模式

模式	说明
\d{3}-\d{2}-\d{4}	匹配标准 SSN 格式，即任何三位数后跟连字符、两位数、连字符和任何四位数。
\d{3}.\d{2}.\d{4}	匹配由句点分隔的 SSN 格式。
\d{3} \d{2} \d{4}	匹配由空格分隔的 SSN 格式。

中宽度版本的美国社会安全号 (SSN) 数据标识符采用三个验证器，以确保检测的 SSN 处于指定的有效号码范围内、不是常见的测试号码（例如 123456789）并且不是所有数字都相同的号码。

表 35-120 社会安全号 (SSN) 中宽度验证器

验证器	说明
数字分隔符	通过检查周围的字符来验证匹配项。
高级 SSN	检查 SSN 的任何组中是否包含零，地区号码（第一组）是否小于 773 且不为 666，组之间的分隔符是否相同，号码不是由全部相同的数字组成，且该号码未保留作为广告用途（123-45-6789、987-65-432x）。

验证器	说明
SSN 地区组号码	对于给定的地区号码（第一组），并非所有的组号码（第二组）都可由 SSA 分配。验证器将排除包含无效组号码的 SSN。

美国社会安全号 (SSN) 小宽度

小宽度版本的美国社会安全号 (SSN) 数据标识符采用检测 9 位数字号码的模式，这种号码的模式为 DDD-DD-DDDD，以短横线、空格分隔或不使用分隔符。

表 35-121 美国社会安全号 (SSN) 小宽度模式

模式	说明
\d{3}-\d{2}-\d{4}	匹配标准 SSN 格式，即任何三位数后跟连字符、两位数、连字符和任何四位数。
\d{3} \d{2} \d{4}	匹配由空格分隔的 SSN 格式。
\d{9}	匹配未进行分隔的任何 9 位数字号码。

小宽度版本的美国社会安全号 (SSN) 数据标识符采用四个验证器，以确保检测的 SSN 处于指定的有效号码范围内、不是常见的测试号码（例如 123456789）、不是所有数字都相同的号码，并且含 SSN 的消息包含某个关键字。

表 35-122 社会安全号 (SSN) 小宽度验证器

必选验证器	说明
数字分隔符	通过检查周围的字符来验证匹配项。
高级 SSN	检查 SSN 的任何组中是否包含零，地区号码（第一组）是否小于 773 且不为 666，组之间的分隔符是否相同，号码不是由全部相同的数字组成，且该号码未保留作为广告用途（123-45-6789、987-65-432x）。
SSN 地区组号码	对于给定的地区号码（第一组），并非所有的组号码（第二组）都可由 SSA 分配。验证器将排除包含无效组号码的 SSN。
查找关键字：社会安全相关	对于要匹配的数据，必须存在至少一个下列关键字或关键短语： 社会安全号、ssn、ss#

美国 SSN - 随机化自定义数据标识符 (DI)

下表提供用于创建美国 SSN - 随机化自定义 DI 的模式和验证器。如果您熟悉如何创建自定义 DI，您可以使用该表格中提供的信息来创建自定义 DI。如果您不熟悉如何创建自定义 DI，请参阅以下主题来获取指导：[创建“美国 SSN - 随机化”自定义 DI](#)。请确保按照建议使用此自定义 DI。

表 35-123 美国 SSN - 随机化自定义 DI

DI 组件	值
名称	US SSN - Randomized
模式	<p>[0-8]\d{2}\\\d{1}[1-9]\\\d{4}</p> <p>[0-8]\d{2}.\d{1}[1-9].\d{4}</p> <p>[0-8]\d{2} \d{1}[1-9] \d{4}</p> <p>[0-8]\d{3}[1-9]\d{4}</p> <p>[0-8]\d{2}/\d{1}[1-9]/\d{4}</p> <p>[0-8]\d{2}[1-9]\d{5}</p> <p>[0-8]\d{2}-\d{1}[1-9]-\d{4}</p> <p>[0-8]\d{2}\\\d{1}[1-9]\d{4}</p> <p>[0-8]\d{2}[1-9]\d{1}\d{4}</p> <p>[0-8]\d{2}/[1-9]\d{1}/\d{4}</p> <p>[0-8]\d{2}.[1-9]\d{1}.\d{4}</p> <p>[0-8]\d{2}-[1-9]\d{1}-\d{4}</p>
数据规范化程序	数字
活动验证器和输入（如果有）	<p>数字分隔符</p> <p>排除开始字符： 666,000,123456789,11111111,22222222,33333333, 44444444,55555555,66666666,77777777,88888888</p> <p>排除结束字符： 0000</p> <p>查找关键字： 社会安全号、ssn、ss#</p>

创建“美国 SSN - 随机化”自定义 DI

下表提供定义“美国 SSN - 随机化”自定义 DI 的说明。

表 35-124 创建“美国 SSN - 随机化”自定义 DI

步骤	操作	说明
步骤 1	登录到 Enforce Server。	若要创建自定义 DI，您必须以具有创建策略权限的用户身分登录。
步骤 2	导航到数据标识符列表。	选择“管理”>“策略”>“数据标识符”。
步骤 3	添加一个新的数据标识符。	选择“添加数据标识符”。 此操作会创建您从头配置的新自定义 DI。
步骤 4	输入“名称”和“说明”。	名称：美国 SSN - 随机化 说明：用于检测在 2011 年 6 月 25 或之后发布的随机 SSN 的自定义 DI。
步骤 5	输入“模式”。	将上一主题所提供的所有模式复制/粘贴“模式”输入字段。以新行分隔每个模式。确保您添加与所提供的完全相同的所有 12 个模式。 请参见第 580 页的 表 35-123 。 这些模式会共同检测开头为所有可能数字的 9 位数字，包括 773 至 899 的新随机化范围，同时排除开头为 9xx 的数字，即使对随机化进行更改之后，这类数字仍无效。
步骤 6	选择“数据规范化程序”。	从下拉菜单中，选择“数字”。

步骤	操作	说明
步骤 7	添加验证检查和数据输入。	<p>若要添加“数字分隔符”验证器，请从“验证检查”列表中选择，然后单击“添加验证器”。一旦添加，验证检查便会显示在“活动验证器”列表中。由于此验证器不接受输入，因此不需要进行任何操作来实施。</p> <hr/> <p>添加“排除开始字符”验证检查。该验证器需要输入。添加输入：</p> <ul style="list-style-type: none"> ■ 在显示器屏幕右侧的“说明和数据项”字段，输入下列要排除匹配的数字： 666,000,123456789,111111111,222222222,333333333, 44444444,555555555,666666666,77777777,888888888 <hr/> <p>■ 单击“活动验证器”将自定义验证器添加到“活动验证器”列表。</p> <hr/> <p>对“排除结束字符”验证检查重复此过程。输入0000作为排除的数字。</p> <hr/> <p>最后，添加“查找关键字”验证器，并输入以下内容： social security number,ssn,ss#。</p>
步骤 8	保存自定义 DI。	单击“保存”。返回到“管理”>“策略”>“数据标识符”屏幕，“美国SSN-随机化”会显示在列表中。
步骤 9	测试自定义 DI。	创建一项测试策略，并定义声明“美国SSN-随机化”自定义DI的规则作为规则中的唯一条件。将这项策略部署至策略组，然后根据开头为 773-899 范围内数字的SSN示例，测试自定义DI。确保这项策略会检测随机化的SSN。
步骤 10	将自定义DI添加到现有的SSN策略。	<p>创建自定义DI的单独规则，使规则以隐式OR与系统定义的DI规则连接。通过这个配置，如果任一条件满足，就会违反这项策略。</p> <p>请参见第582页的“使用美国SSN-随机化自定义DI的建议”。</p>

Copyright © 2011 Symantec Corporation. © 2011 年 Symantec Corporation 版权所有。All rights reserved. 保留所有权利。

使用美国 SSN - 随机化自定义 DI 的建议

若要更新SSN随机化的策略，请勿修改系统定义的美国SSN数据标识符。对于2011年6月25日前发布的SSN，此DI仍有效。一旦您创建并测试美国SSN - 随

机化的自定义 DI 后，建议您同时部署自定义 DI 与系统定义的 DI 作为相同策略的一部分。

因此，对于会实施系统定义 SSN 的每项既有策略，只要将其他检测规则添加到声明美国 SSN - 随机化自定义 DI 的策略作为其单一条件即可。请将自定义 DI 规则的严重性设为低于系统定义 DI 规则的严重性。

确保将自定义 DI 添加到单机规则，并且不作为现有系统定义 DI 规则的条件。作为相同策略中的单独规则，条件会使用隐式 OR 进行连接，因此，如果任一条件匹配时，就会是事件（假设您对所有匹配项进行计数）。如果不想将条件包含在同一规则中，因为这将会需要两个条件都满足，才会触发事件。

策略模板

本章节包括下列主题：

- [Caldicott 报告策略模板](#)
- [加拿大社会保险号策略模板](#)
- [CAN-SPAM 法案策略模板](#)
- [常见间谍软件上传站点策略模板](#)
- [竞争对手通信策略模板](#)
- [机密文档策略模板](#)
- [信用卡号策略模板](#)
- [客户数据保护策略模板](#)
- [1998 年数据保护法案（英国）策略模板](#)
- [数据保护规定（欧盟）策略模板](#)
- [国防信息系统 \(DMS\) 的常规服务分类策略模板](#)
- [设计文档策略模板](#)
- [员工数据保护策略模板](#)
- [加密数据策略模板](#)
- [出口管理条例 \(EAR\) 策略模板](#)
- [FACTA 2003（红色标记规则）策略模板](#)
- [金融信息策略模板](#)
- [禁止访问的网站策略模板](#)

- 赌博策略模板
- “金融服务法案”策略模板
- HIPAA 和 HITECH（包括 PHI）策略模板
- 1998 年人权法策略模板
- 非法药品策略模板
- 个人纳税识别号 (ITIN) 策略模板
- 国际武器贸易条例 (ITAR) 策略模板
- 媒体文件策略模板
- 并购协议策略模板
- NASD 规则 2711 以及 NYSE 规则 351 和 472 策略模板
- NASD 规则 3010 和 NYSE 规则 342 策略模板
- NERC 电气设备安全指导策略模板
- 网络图策略模板
- 网络安全策略模板
- 攻击性语言策略模板
- 外国资产管制办公室 (OFAC) 策略模板
- OMB 备忘录 06-16 和 FIPS 199 条例策略模板
- 密码文件策略模板
- 支付卡行业 (PCI) 数据安全标准策略模板
- PIPEDA 策略模板
- 价格信息策略模板
- 项目数据策略模板
- 专有媒体文件策略模板
- 出版文档策略模板
- 种族歧视语言策略模板
- 受限文件策略模板
- 受限接受者策略模板

- 简历策略模板
- 萨班斯-奥克斯利法案策略模板
- SEC 公平披露规则策略模板
- 下流语言策略模板
- 源代码策略模板
- 州数据隐私策略模板
- SWIFT 代码策略模板
- Symantec DLP 感知与避免策略模板
- 英国驾照号策略模板
- 英国选民登记号策略模板
- 英国国民保健服务 (NHS) 号策略模板
- 英国国家保险号码策略模板
- 英国护照号策略模板
- 英国税号策略模板
- 美国情报控制标记 (CAPCO) 和 DCID 1/7 策略模板
- 美国社会安全号策略模板
- 暴力与武器策略模板
- Webmail 策略模板
- Yahoo 留言板活动策略模板
- 端口 80 上的 Yahoo 和 MSN Messenger 策略模板

Caldicott 报告策略模板

英国首席医疗官委托发行了 Caldicott 报告（1997 年 12 月），以便改进国民医疗服务处理并保护患者信息的方式。Caldicott 委员会审核整个 NHS 中数据的机密性，而不是直接管理或进行医学研究，也不是有关的信息法律要求这么做。这些建议现在正通过 NHS 和医疗保护代理应用于实践中。

EDM 规则

患者数据和药品关键字

此复合规则会结合“处方药品名称”字典中的关键字查找以下数据的任何匹配项。必须同时满足这两个条件，规则才能触发事件。

- 英国 NIN (国家保险号码)
- 帐号
- 姓氏
- 身份证号
- 电子邮件
- 电话
- 英国 NHS (国民保健服务) 号

EDM 规则

患者数据和疾病关键字

此复合规则会结合“疾病名称”字典中的关键字查找以下数据的任何匹配项。必须同时满足这两个条件，规则才能触发事件。

- 英国 NIN (国家保险号码)
- 帐号
- 姓氏
- 身份证号
- 电子邮件
- 电话
- 英国 NHS (国民保健服务) 号

EDM 规则

患者数据和治疗关键字

此复合规则会结合“药物治疗关键字”字典中的关键字查找以下数据的任何匹配项。必须同时满足这两个条件，规则才能触发事件：

- 英国 NIN (国家保险号码)
- 帐号
- 姓氏
- 身份证号
- 电子邮件
- 电话
- 英国 NHS (国民保健服务) 号

DCM 规则

英国 NHS 号和药品关键字

此规则结合与英国 NIN 数据标识符匹配的模式和“处方药品名称”字典中的关键字，查找“英国 NIN 关键字”字典中的关键字。

DCM 规则

英国 NHS 号和疾病关键字

此规则结合与英国 NIN 数据标识符匹配的模式和“疾病名称”字典中的关键字，查找“英国 NIN 关键字”字典中的关键字。

DCM 规则

英国 NHS 号和治疗关键字

此规则结合与英国 NIN 数据标识符匹配的模式和“药物治疗关键字”字典中的关键字，查找“英国 NIN 关键字”字典中的关键字。

请参见第 326 页的[“选择确切数据配置文件”](#)。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

加拿大社会保险号策略模板

此策略会检测指示有泄露风险的加拿大社会保险号 (SIN) 的模式。

DCM 规则

加拿大社会保险号

此规则会查找与“加拿大社会保险号”数据标识符和“加拿大社会保险号字词”字典中的关键字匹配的项。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

CAN-SPAM 法案策略模板

控制不请自来的色情和营销行为攻击的法案(CAN-SPAM)建立了发送商业电子邮件的要求。

CAN-SPAM法案模板会检测组织的批量邮件发送者的活动，帮助确保遵守CAN-SPAM法案要求。

检测例外“**排除包含强制关键字的电子邮件**”允许包含“CAN-SPAM例外关键字”字典（用户定义的）中的一个或多个关键字的邮件通过。

表 36-1

检测例外：排除包含强制关键字的电子邮件

方法	条件	配置
简单例外	内容匹配关键字 (DCM)	<p>排除包含强制关键字的电子邮件（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 匹配 [physical postal address] 或 advertisement 中的关键字。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。 <p>注意：定义关键字后，可以选择计算所有匹配项并要求匹配列表中的两个关键字。</p>

“符合 CAN-SPAM 法案的电子邮件” 检测例外将选定 IDM 索引中至少 100% 匹配的项排除在文档内容检测范围之外。

表 36-2

检测例外：符合 CAN-SPAM 法案的电子邮件

方法	条件	配置
简单例外	内容匹配文档配置文件 (IDM)	<p>符合 CAN-SPAM 法案的电子邮件例外 (IDM)：</p> <ul style="list-style-type: none"> ■ 确切内容匹配 (100%) ■ 查找邮件正文和附件。 ■ 检查是否存在。 <p>请参见第 327 页的“选择索引文档配置文件”。</p>

如果不符合例外，检测规则“监控来自批量邮件发送者的电子邮件”将查找与“批量邮件发送者电子邮件地址”列表（用户定义）中的条目匹配的发送者的电子邮件地址。

表 36-3

检测规则：监控来自批量邮件发送者的电子邮件

方法	条件	配置
简单规则	发送者/用户匹配模式 (DCM)	<p>监控来自批量邮件发送者的电子邮件（发送者）：</p> <ul style="list-style-type: none"> ■ 匹配发送者模式：[bulk-mailer@company.com]（用户定义） ■ 严重性：高度。

请参见第 317 页的“[从模板创建策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

常见间谍软件上传站点策略模板

“常见间谍软件上传站点”策略检测对常见间谍软件上传网站的访问。

DCM 规则	禁止访问的网站 1
这是一种复合规则，用于查找“禁止访问的网站 1”字典中的指定 IP 地址或 URL。	

DCM 规则	禁止访问的网站 2
此规则会查找与“禁止访问的网站 2”字典中指定的 URL 匹配的项。	

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

竞争对手通信策略模板

“竞争对手通信”策略会检测与竞争对手之间禁止的通信。

DCM 规则	竞争对手列表
此规则会查找“竞争对手域”字典中的关键字（域），该字典是用户定义的。	

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

机密文档策略模板

此策略可检测有泄露风险的公司机密文档。

表 36-4 包含机密文档模板的规则

规则	类型	说明
已编制索引的机密文档	包括一个条件的简单IDM 规则	此规则会查找已注册为机密的特定文档中的内容；如果找到源文档 80% 或以上的内容，则返回一个匹配项。如果您尚未配置已编制索引的文档配置文件，则会丢弃此规则。 请参见第 377 页的 “关于实施索引文档匹配” 。

规则	类型	说明
机密文档	DCM 复合规则：附件/文件类型和关键字匹配。必须匹配所有条件，规则才能触发事件。	此规则会查找“机密关键字”列表中的关键字以及下列文件类型的组合： <ul style="list-style-type: none"> ■ Microsoft Excel 宏 ■ Microsoft Excel ■ Microsoft Works 电子表格 ■ SYLK 电子表格 ■ Corel Quattro Pro ■ Multiplan 电子表格 ■ 逗号分隔值 ■ Applix 电子表格 ■ Lotus 1-2-3 ■ Microsoft Word ■ Adobe PDF ■ Microsoft PowerPoint
专有文档	DCM 复合规则：附件/文件类型和关键字匹配	此复合规则查找“专有关键字”字典中的关键字和上面提及的文件类型的组合。
仅限内部使用的文档	DCM 复合规则：附件/文件类型和关键字匹配	此复合规则查找“仅限内部使用的关键字”字典中的关键字和上面提及的文件类型的组合。
不得分发的文档	DCM 复合规则：附件/文件类型和关键字匹配	此复合规则查找“不得散布字词”字典中的关键字和上面提及的文件类型的组合。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

信用卡号策略模板

此策略会检测指示有泄漏风险的信用卡号的模式。

DCM 规则

所有信用卡号

此规则会查找与信用卡号系统模式和“信用卡号关键字”字典中的关键字匹配的项。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

客户数据保护策略模板

此策略会检测有泄露风险的客户数据。

EDM 规则

用户名/密码组合

此规则使用以下三个或更多个字段查找用户名和密码组合：

- SSN
- 电话
- 电子邮件
- 名字
- 姓氏
- 银行卡号
- 帐号
- ABA 汇款路径号码
- 加拿大社会保险号
- 英国国家保险号码

但是，以下组合不是违规：

- 电话、电子邮件和姓氏
- 电子邮件、名字和姓氏
- 电话、名字和姓氏

EDM 规则

出生日期

此规则会查找下列任意三个数据字段组合：

- SSN
- 电话
- 电子邮件
- 名字
- 姓氏
- 银行卡号
- 帐号
- ABA 汇款路径号码
- 加拿大社会保险号
- 英国国家保险号码
- 出生日期

但是，以下组合不是违规：

- 电话、电子邮件和名字
- 电话、电子邮件和姓氏
- 电子邮件、名字和姓氏
- 电话、名字和姓氏

EDM 规则	确切 SSN 或 CCN 此规则会查找确切的社会安全号或银行卡号。
EDM 规则	客户目录 此规则会查找电话或电子邮件。
DCM 规则	美国社会安全号模式 此规则会查找与社会安全号数据标识符和“美国 SSN 关键字”字典中的关键字匹配的项。
DCM 规则	所有信用卡号 此规则会查找与信用卡号系统模式和“信用卡号关键字”字典中的关键字匹配的项。
DCM 规则	ABA 汇款路径号码 此规则会查找与 ABA 汇款路径号码数据标识符和“ABA 汇款路径号码关键字”字典中的关键字匹配的项。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

1998 年数据保护法案（英国）策略模板

1998 年数据保护法案（1984 年数据保护法案的替代法案）设定了在英国获取、拥有、使用或处理个人数据时必须满足的标准。1998 年数据保护法案涵盖个人信息的所有方面（例如，有关个人健康、就业、职业健康、金融、提供商和合同商的数据）。

表 36-5 英国数据保护法案 - 个人数据检测规则

说明	
<p>此 EDM 规则会查找以下三个数据列：</p> <ul style="list-style-type: none"> ■ NIN (国家保险号码) ■ 帐号 ■ PIN ■ 银行卡号 ■ 名字 ■ 姓氏 ■ 驾驶执照 ■ 密码 ■ 缴税 ID ■ 英国 NHS 号 ■ 出生日期 ■ 母亲的婚前姓 ■ 电子邮件地址 ■ 电话号码 	<p>但是，以下组合不是事件：</p> <ul style="list-style-type: none"> ■ 名字、姓氏、PIN ■ 名字、姓氏、密码 ■ 名字、姓氏、电子邮件 ■ 名字、姓氏、电话 ■ 名字、姓氏、母亲的婚前姓

表 36-6 1998 年数据保护法案策略模板中的其他检测规则

说明
<p>“英国选民登记号” 规则实施英国选民登记号数据标识符。</p> <p>请参见第 566 页的“英国选民登记号数据标识符”。</p>
<p>“英国国家保险号码” 规则实施英国国家保险号码数据标识符的小宽度版本。</p> <p>请参见第 569 页的“英国国家保险号码数据标识符”。</p>
<p>“英国税号” 规则实施英国税号数据标识符的小宽度版本。</p> <p>请参见第 573 页的“英国税号数据标识符”。</p>
<p>“英国驾照号” 规则实施英国驾照号数据标识符的小宽度版本。</p> <p>请参见第 564 页的“英国驾照号数据标识符”。</p>
<p>“英国护照号” 规则实施英国护照号数据标识符的小宽度版本。</p> <p>请参见第 571 页的“英国护照号数据标识符”。</p>
<p>“英国 NHS 号” 规则实施英国国民保健服务 (NHS) 号数据标识符的小宽度版本。</p> <p>请参见第 567 页的“英国国民保健服务 (NHS) 号数据标识符”。</p>
<p>请参见第 326 页的“选择确切数据配置文件”。</p>

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

数据保护规定（欧盟）策略模板

欧洲议会的 95/46/EC 指令涉及在个人数据的处理及自由转移方面的个人保护。此策略会检测特定于欧盟指令的个人数据。

EDM 规则

欧盟数据保护规定

此规则会查找以下任意两个数据列：

- 姓氏
- 银行卡号
- 驾驶执照号码
- 帐号
- PIN
- 医疗帐户号码
- 医疗 ID 卡号
- 用户名
- 密码
- ABA 汇款路径号码
- 电子邮件
- 电话
- 母亲的婚前姓

但是，下列组合不会创建匹配项：

- 姓氏、电子邮件
- 姓氏、电话号码
- 姓氏、帐号
- 姓氏、用户名

EDM 规则

欧盟数据信息 - 联系信息

此规则会查找以下任意两个数据列：姓氏、电话号码、帐号、用户名和电子邮件。

例外

欧盟内部电子邮件除外

此规则是接受者在欧盟内的例外。这会涵盖国家/地区代码来自“欧盟国家/地区代码”字典的接受者。

请参见第 326 页的“[选择确切数据配置文件](#)”。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

国防信息系统 (DMS) 的常规服务分类策略模板

国防信息系统机构为国防信息系统 (DMS) 常规服务 (GENSER) 邮件分类、类别和标记建立了准则。这些标准规定了如何根据美国标准来标记分类和敏感文档。此外还提供了与北约国家和其他美国盟国的互操作性。

GENSER 策略模板通过检测分类为机密的信息强制执行 GENSER 准则。模板包含四个简单的（一个条件）关键字匹配 (DCM) 检测规则。如果匹配任何规则条件，策略会报告事件。

检测规则“最高机密信息”（关键字匹配）会查找“最高机密信息”字典中的任何关键字。

表 36-7 检测规则：最高机密信息（关键字匹配）

方法	条件	配置
简单规则	内容匹配关键字 (DCM)	最高机密信息（关键字匹配）： <ul style="list-style-type: none">■ 关键字字典：TOP SECRET//■ 严重性：高度■ 检查是否存在。■ 查找信封、主题、正文和附件。■ 区分大小写。■ 全字匹配或部分匹配。

检测规则“机密信息”（关键字匹配）会查找“机密信息”字典中的任何关键字。

表 36-8 检测规则：机密信息（关键字匹配）

方法	条件	配置
简单规则	内容匹配关键字 (DCM)	机密信息（关键字匹配）： <ul style="list-style-type: none">■ 关键字字典：SECRET//■ 严重性：高度■ 检查是否存在■ 查看信封、主题、正文和附件■ 区分大小写■ 全字匹配或部分匹配。

检测规则“分类或限制信息”（关键字匹配）会查找“分类或限制信息”字典中的任何关键字。

表 36-9 检测规则：分类或限制信息（关键字匹配）

方法	条件	配置
简单规则	内容匹配关键字(DCM)	<p>分类或限制信息（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 关键字字典：CLASSIFIED//././RESTRICTED// ■ 严重性：高度 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 区分大小写。 ■ 全字匹配或部分匹配。

检测规则“其他敏感信息”会查找“其他敏感信息”字典中的任何关键字。

表 36-10 其他敏感信息检测规则

方法	条件	配置
简单规则	内容匹配关键字(DCM)	<p>其他敏感信息（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 关键字字典：FOR OFFICIAL USE ONLY、SENSITIVE BUT UNCLASSIFIED、DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION ■ 严重性：高度 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 区分大小写。 ■ 仅进行全字匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

设计文档策略模板

此策略会检测有泄露风险的各种类型的设计文档，如 CAD/CAM。

IDM 规则

已编制索引的设计文档

此规则会查找注册为专有内容的特定设计文档中的内容。如果引擎检测到源文档的 80% 或更多内容，则会返回匹配项。

DCM 规则

设计文档扩展名

此规则会查找在“设计文档扩展名”字典中找到的指定文件扩展名。

DCM 规则**设计文档**

此规则会查找下列指定的文件类型：

- cad_draw
- dwg

注意：由于该策略不检测所有所需文档的真实文件类型，因此要同时使用文件类型和文件扩展名。

请参见第 327 页的“[选择索引文档配置文件](#)”。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

员工数据保护策略模板

此策略会检测有泄露风险的员工数据。

EDM 规则**用户名/密码组合**

此规则使用以下任意三个数据字段查找用户名和密码组合。

- SSN
- 电话
- 电子邮件
- 名字
- 姓氏
- 银行卡号
- 帐号
- ABA 汇款路径号码
- 加拿大社会保险号
- 英国国家保险号码
- 出生日期

EDM 规则**员工目录**

此规则会查找电话或电子邮件。

DCM 规则**美国社会安全号模式**

此规则会查找与社会安全号数据标识符和“美国 SSN 关键字”字典中的关键字匹配的项。

DCM 规则	所有信用卡号
	此规则会查找与信用卡号系统模式和“信用卡号关键字”字典中的关键字匹配的项。
DCM 规则	ABA 汇款路径号码
	此规则会查找与 ABA 汇款路径号码数据标识符和“ABA 汇款路径号码关键字”字典中的关键字匹配的项。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

加密数据策略模板

此策略会通过多种方法（包括 S/MIME、PGP、GPG 和文件密码保护）来检测是否使用了加密。

DCM 规则	受密码保护的文件
	此规则会查找下列文件类型：encrypted_zip、encrypted_doc、encrypted_xls 或 encrypted_ppt。
DCM 规则	PGP 文件
	此规则会查找下列文件类型：pgp。
DCM 规则	GPG 文件
	此规则会查找“GPG 加密关键字”字典中的关键字。
DCM 规则	S/MIME
	此规则会查找“S/MIME 加密关键字”字典中的关键字。
DCM 规则	HushMail 传输
	此规则会从接受者 URL 列表中查找匹配项。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

出口管理条例 (EAR) 策略模板

美国商务部强制实施出口管理条例 (EAR)。这些条例主要包含商业和军事应用方面的技术和技术信息。这些技术也称为军民两用技术（例如化学、卫星、软件和计算机等）。

此出口管理条例 (EAR) 模板检测管制国家/地区以及受控技术中的违规情况。

检测规则“已编制索引的EAR商品管制列表项和接受者”查找接受者中来自“EAR国家/地区代码”字典的国家/地区代码和来自确切数据配置文件索引(EDM)的特定SKU。必须同时匹配这两个条件才能触发事件。

表 36-11 检测规则：已编制索引的 EAR 商品管制列表项和接受者

方法	条件	配置
复合规则	内容匹配确切数据(EDM)	请参见第 326 页的“ 选择确切数据配置文件 ”。
	内容匹配关键字(DCM)	

检测规则“EAR商品管制清单和接受者”会查找接受者中来自“EAR国家/地区代码”列表的国家/地区代码和来自“EAR CCL 关键字”字典中的关键字。必须同时匹配这两个条件才能触发事件。

表 36-12 检测规则：EAR 商品管制清单和接受者

方法	条件	配置
复合规则	接受者匹配模式(DCM)	EAR商品管制清单和接受者(接受者)： <ul style="list-style-type: none"> ■ 匹配：电子邮件地址或 URL 域后缀 ■ 严重性：高度。 ■ 检查是否存在。 ■ 必须至少匹配 1 个接受者。 ■ 与整个邮件匹配
	内容匹配关键字(DCM)	EAR商品管制清单和接受者(关键字匹配)： <ul style="list-style-type: none"> ■ 匹配：EAR CCL 关键字 ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

FACTA 2003 (红色标记规则) 策略模板

此策略有助于处理公平准确信用交易法案 (FACTA) 2003 的第 114 和 315 (或红色标记规则) 部分。这些规则指定，提供或维护涵盖帐户的金融机构或债权人必须制定和实施身份失窃预防计划。FACTA 旨在检测、预防和减少与开立涵盖帐户或任何现有涵盖帐户相关的身份失窃。

“用户名/密码组合”检测规则会检测已配置的数据库索引中是否同时存在用户名和密码。

表 36-13 用户名/密码组合检测规则

方法	条件	配置
简单规则	内容匹配确切数据 (EDM)	<p>此条件会检测包含以下两个数据项的确切数据：</p> <ul style="list-style-type: none"> ■ 用户名 ■ 密码 <p>请参见第 326 页的“选择确切数据配置文件”。</p>

“确切 SSN 或 CCN”检测规则会检测已配置的数据库中是否存在社会安全号或信用卡号。

表 36-14 确切 SSN 或 CCN 检测规则

方法	条件	配置
简单规则	内容匹配确切数据 (EDM)	<p>此条件会检测包含以下任一数据列的确切数据：</p> <ul style="list-style-type: none"> ■ 社会安全号 (纳税人 ID) ■ 银行卡号 <p>请参见第 326 页的“选择确切数据配置文件”。</p>

“客户目录”检测规则会检测已配置的数据库中是否存在电子邮件地址或电话号码。

表 36-15 客户目录检测规则

方法	条件	配置
简单规则	内容匹配确切数据 (EDM)	<p>此条件会检测包含以下任一数据列的确切数据：</p> <ul style="list-style-type: none"> ■ 电子邮件地址 ■ 电话号码 <p>请参见第 326 页的“选择确切数据配置文件”。</p>

“三个或更多数据列”检测规则会检测包含已配置的数据库索引中的三个或更多数据项的确切数据。

表 36-16 三个或更多数据列检测规则

方法	条件	配置
简单规则	内容匹配确切数据 (EDM)	<p>检测包含以下三个或更多数据项的确切数据：</p> <ul style="list-style-type: none"> ■ ABA 汇款路径号码 ■ 帐号 ■ 银行卡号 ■ 出生日期 ■ 电子邮件地址 ■ 名字 ■ 姓氏 ■ 国家保险号码 ■ 密码 ■ 电话号码 ■ 社会保险号 ■ 社会安全号 (纳税人 ID) ■ 用户名 <p>但是，以下组合不匹配：</p> <ul style="list-style-type: none"> ■ 电话号码、电子邮件和名字 ■ 电话号码、名字和姓氏 <p>请参见第 326 页的“选择确切数据配置文件”。</p>

“美国社会安全号模式”检测规则实现美国社会安全号 (SSN) 系统数据标识符的小宽度版本。

请参见第 577 页的“[美国社会安全号 \(SSN\) 数据标识符](#)”。

此数据标识符会检测 9 个数位的号码，该号码的模式为 DDD-DD-DDDD，以短横线或空格分隔或不使用分隔符。该号码必须处于指定的有效号码范围内。此条件会排除常见测试号码，例如 123456789 或数字全部相同的号码。此外，还要求存在社会安全号关键字。

表 36-17 美国社会安全号模式检测规则

方法	条件	配置
简单规则	内容匹配数据标识符 (DCM)	<ul style="list-style-type: none"> ■ 数据标识符：美国社会安全号 (SSN) 小宽度 请参见第 579 页的“美国社会安全号 (SSN) 小宽度”。 ■ 严重性：高度。 ■ 计算所有匹配项。 ■ 查找信封、主题、正文和附件。

所有信用卡号检测规则实现信用卡号系统数据标识符的小宽度版本。

请参见第 532 页的“[信用卡号数据标识符](#)”。

此数据标识符会检测以空格、短横线、句点分隔或不带分隔符的有效信用卡号。此条件会执行 Luhn 检查验证，包括 American Express、Diner's Club、Discover、Japan Credit Bureau (JCB)、MasterCard 和 Visa 格式。它会排除常见测试号码，包括保留供信用卡发行机构用于测试的号码。此外，还要求存在信用卡关键字。

表 36-18 所有信用卡号检测规则

方法	条件	配置
简单规则	内容匹配数据标识符 (DCM)	<ul style="list-style-type: none"> ■ 数据标识符：信用卡号小宽度 请参见第 535 页的“信用卡号小宽度”。 ■ 严重性：高度。 ■ 计算所有匹配项。 ■ 查找信封、主题、正文和附件。

“ABA 汇款路径号码”检测规则实现 ABA 汇款路径号码系统数据标识符的小宽度版本。

请参见第 522 页的“[ABA 汇款路径号码数据标识符](#)”。

此数据标识符会检测 9 个数位的号码。它使用最终检查数字验证号码。此条件会排除常见测试号码（例如 123456789）、保留供将来使用的号码范围，以及数字全部相同的号码。此条件还要求存在 ABA 关键字。

表 36-19 ABA 汇款路径号码检测规则

方法	条件	配置
简单规则	内容匹配数据标识符 (DCM)	<ul style="list-style-type: none"> ■ 数据标识符：ABA 汇款路径号码小宽度 请参见第 524 页的“ABA 汇款路径号码小宽度”。 ■ 严重性：高度。 ■ 计算所有匹配项。 ■ 查找信封、主题、正文和附件。

请参见第 317 页的“[从模板创建策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

金融信息策略模板

“金融信息”策略会检测金融数据和信息。

IDM 规则

已编制索引的金融信息

此规则会查找已注册为专有的特定金融信息文件中的内容；如果找到源文档 80% 或以上的内容，则返回一个匹配项。

DCM 规则

金融信息

此规则会查找特定文件类型、“金融关键字”字典中的关键字以及“机密/专有字词”字典中的关键字的组合。

指定的文件类型如下：

- excel_macro
- xls
- works_spread
- sylk
- quattro_pro
- mod
- csv
- applix_spread
- 123

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

请参见第 377 页的“[关于实施索引文档匹配](#)”。

禁止访问的网站策略模板

“禁止访问的网站”策略会检测对指定网站的访问。

DCM 规则

禁止访问的网站

此规则会查找“禁止访问的网站”字典中的任何关键字，该字典是用户定义的。

使“禁止访问的网站”策略正确处理 GET 请求

- 1 配置 Web 代理服务器以将 GET 请求转发到 Network Prevent (Web) 服务器。
- 2 将 Network Prevent (Web) 服务器上的“L7.processGets 高级设置”设置为 true (此为默认值)。
- 3 将 Network Prevent (Web) 服务器上的 L7.minSizeofGetURL 高级设置从默认值 100 减小为小于该策略指定的最短网站长度的字节 (字符) 数。

注意：减小 GET 的最小大小会增大必须处理的 URL 数目，这会增加服务器流量负载。一种方法是计算禁止访问 URL 列表中指定的最短 URL 的字符数，然后将最小大小设置为该数。另一种方法是将最小 URL 大小设置为 10 即可涵盖所有情况。

- 4 您可能需要在 Network Prevent Server 的 ICAP 配置中调整“忽略小于以下大小的请求”设置的默认值 4096 字节。此值会停止处理所含字节数少于指定字节数的传入网页。如果禁止访问的网站 URL 的页面小于该数，应相应减小该设置。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

赌博策略模板

此策略会检测对赌博的任何引用。

DCM 规则

可疑赌博关键字

此规则会查找“已确认的赌博关键字”字典中的 5 个关键字实例。

DCM 规则

可疑程度较低的赌博关键字

此规则会查找“可疑的赌博关键字”字典中的 10 个关键字实例。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

“金融服务法案”策略模板

金融服务法案 (GLB) 赋予客户限制金融机构对其信息进行某些共享的权利。

金融服务法案策略模板会检测客户数据的传输。

表 36-20 金融服务法案检测方法

检测方法	类型	说明
用户名/密码组合	简单规则： EDM	此规则会查找用户名和密码组合。 请参见第 326 页的 “选择确切数据配置文件” 。
确切 SSN 或 CCN	简单规则： EDM	此规则会查找 SSN 或信用卡号。
客户目录	简单规则： EDM	此规则会查找电话或电子邮件。
3个或更多关键客户字段	简单规则： EDM	<p>此规则会查找下列任意三个字段中的匹配项：</p> <ul style="list-style-type: none"> ■ 帐号 ■ 银行卡号 ■ 电子邮件地址 ■ 名字 ■ 姓氏 ■ PIN 号码 ■ 电话号码 ■ 社会安全号 ■ ABA 汇款路径号码 ■ 加拿大社会保险号 ■ 英国国家保险号码 ■ 出生日期 <p>但是，以下组合不匹配：</p> <ul style="list-style-type: none"> ■ 电话、电子邮件和名字 ■ 电话、电子邮件和姓氏 ■ 电子邮件、名字和姓氏 ■ 电话、名字和姓氏
ABA 汇款路径号码	简单规则： DCM (DI)	<p>此条件会检测 9 个数位的号码。它使用最终检查数字验证号码。此条件会排除常见测试号码（例如 123456789）、保留供将来使用的号码范围，以及数字全部相同的号码。此条件还要求存在与 ABA 相关的关键字。</p> <p>请参见第 524 页的“ABA 汇款路径号码小宽度”。</p>

检测方法	类型	说明
美国社会安全号	简单规则： DCM (DI)	此规则会查找社会安全号。为了使此规则匹配，必须具有一个符合美国 SSN 正则表达式模式的编号。还必须存在指示美国 SSN 和“美国 SSN 关键字”字典中的关键字是否存在的关键字或短语。包含关键字条件，以减少对可能匹配 SSN 格式的所有号码的误报。请参见第 579 页的 “美国社会安全号 (SSN) 小宽度” 。
信用卡号	简单规则： DCM (DI)	<p>此条件会检测以空格、短横线、句点分隔或不带分隔符的有效信用卡号。此条件执行 Luhn 检查验证并且包括下列信用卡格式：</p> <ul style="list-style-type: none"> ■ American Express ■ Diner's Club ■ Discover ■ Japan Credit Bureau (JCB) ■ MasterCard ■ Visa <p>此规则会排除常见测试号码（包括保留供信用卡发行机构用于测试的号码），此外，还要求存在与信用卡相关的关键字。</p> <p>请参见第 535 页的“信用卡号小宽度”。</p>

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

HIPAA 和 HITECH (包括 PHI) 策略模板

HIPAA 和 HITECH (包括 PHI) 策略严格强制实施美国医疗保险流通与责任法案 (HIPAA)。为了经济和临床健康的医疗保健信息科技法案 (HITECH) 是强制执行有关 PHI 的违反通知的第一部美国国家法律。

此策略模板结合使用受保护的医疗信息 (PHI) 来检测处方药、疾病和治疗相关数据。不受 HIPAA 约束的组织也可以使用此策略来控制 PHI 数据。

TPO (治疗、支付或医疗保健业务) 是面向医疗保健组织的服务提供商，对 HIPAA 信息限制具有例外。如果将受保护的信息发送给允许的合作伙伴之一，此策略不会触发事件。

表 36-21 在任何检测规则前进行评估。该模板要求您输入允许的电子邮件地址。

表 36-21 TPO 检测例外

方法和基数	条件类型	配置
简单检测例外	内容匹配关键字(DCM)	查找与“TPO电子邮件地址”关键字字典中的一个条目匹配的接受者电子邮件地址。

表 36-22 查找与已配置的患者数据数据库记录中的任何一列匹配的项。

表 36-22 患者数据检测规则

方法和基数	条件类型	配置
简单检测规则	内容匹配确切数据(EDM)	<p>患者数据(EDM):</p> <ul style="list-style-type: none"> ■ 姓氏 ■ 缴税 ID(SSN) ■ 电子邮件地址 ■ 帐号 ■ 身份证号 ■ 电话号码 <p>请参见第326页的“选择确切数据配置文件”。</p>

表 36-23 需要“患者数据”条件匹配项与“药品代码”数据标识符中的匹配项。

表 36-23 患者数据和药品代码检测规则

方法和基数	条件类型	配置
复合检测规则	内容匹配确切数据(EDM)	针对配置的患者数据数据库记录的任何一列查找匹配项。
	内容匹配数据标识符	请参见第556页的 “国家药品代码(NDC)数据标识符” 。

表 36-24 需要“患者数据”条件匹配项与“处方药品名称”关键字字典中关键字的组合。

表 36-24 患者数据和处方药品名称检测规则

方法和基数	条件类型	配置
复合检测规则	内容匹配确切数据(EDM)	针对配置的患者数据数据库记录的任何一列查找匹配项。
	内容匹配关键字(DCM)	

表 36-25 需要“患者数据”条件匹配项与“药物治疗关键字”关键字字典中关键字的组合。

表 36-25 患者数据和治疗关键字检测规则

方法和基数	条件类型	配置
复合检测规则	内容匹配确切数据(EDM)	针对配置的患者数据数据库记录的任何一列查找匹配项。
	内容匹配关键字(DCM)	

表 36-26 需要“患者数据”条件匹配项与“疾病名称”关键字字典中关键字的组合。

表 36-26 患者数据和疾病关键字检测规则

方法和基数	条件类型	配置
复合检测规则	内容匹配确切数据(EDM)	针对配置的患者数据数据库记录的任何一列查找匹配项。
	内容匹配关键字(DCM)	

表 36-27 使用美国社会安全号(SSN)系统数据标识符(小宽度)来查找社会安全号并查找“处方药品名称”关键字字典中的关键字。

表 36-27 SSN 和药品关键字检测规则

方法和基数	条件类型	配置
复合检测规则	内容匹配数据标识符	美国社会安全号(SSN)系统数据标识符(小宽度) 请参见第 577 页的“ 美国社会安全号(SSN)数据标识符 ”。
	内容匹配关键字	“处方药品名称”关键字字典

表 36-28 规则使用美国 SSN 系统数据标识符(小宽度)来查找社会安全号并查找“药物治疗关键字”关键字字典中的匹配项。

表 36-28 SSN 和治疗关键字检测规则

方法和基数	条件类型	配置
复合检测规则	内容匹配数据标识符	美国社会安全号 (SSN) 系统数据标识符 (小宽度) 请参见第 577 页的“ 美国社会安全号 (SSN) 数据标识符 ”。
	内容匹配关键字	“药物治疗关键字” 关键字字典

表 36-29 中的规则使用美国 SSN 系统数据标识符 (小宽度) 来查找社会安全号并查找“疾病名称”关键字字典中的匹配项。

表 36-29 SSN 和疾病关键字检测规则

方法和基数	条件类型	配置
复合检测规则	内容匹配数据标识符	美国社会安全号 (SSN) 系统数据标识符 (小宽度) 请参见第 577 页的“ 美国社会安全号 (SSN) 数据标识符 ”。
	内容匹配关键字	“疾病名称” 关键字字典

表 36-30 规则使用美国 SSN 系统数据标识符 (小宽度) 来查找社会安全号并使用“药品代码”系统数据标识符 (小宽度) 来查找药品代码。

表 36-30 SSN 和药品代码检测规则

方法和基数	条件类型	配置
复合检测规则	内容匹配数据标识符	美国 SSN 系统数据标识符 (小宽度) 请参见第 577 页的“ 美国社会安全号 (SSN) 数据标识符 ”。
	内容匹配关键字	“药品代码” 系统数据标识符 (小宽度) 请参见第 556 页的“ 国家药品代码 (NDC) 数据标识符 ”。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

1998 年人权法策略模板

1998 年人权法允许英国公民在英国法院和法庭依据《欧洲人权公约》来维护自己的权利。该法案声明 “so far as possible to do so, legislation must be read and given effect in a way which is compatible with convention rights (只要可以，必须阅读法案并在不与公约权利冲突的情况下使之生效)”。 “1998 年人权法” 策略通过确保英国公民的生活隐私来强制实施第 8 条。

EDM 规则	英国数据保护法案 - 个人数据 此复合规则结合使用“英国个人数据关键字”字典中的关键字来查找姓氏和选民登记号这两种数据类型。
DCM 规则	英国选民登记号 此规则会查找包含以下四个组成部分的单个复合条件： <ul style="list-style-type: none">■ “英国关键字”字典中的一个关键字■ 与英国选民登记号数据标识符的模式相匹配的模式■ “英国选民登记号字词”字典中的一个关键字■ “英国个人数据关键字”字典中的一个关键字

请参见第 326 页的“[选择确切数据配置文件](#)”。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

非法药品策略模板

此策略会检测有关非法药品和管制物的对话。

DCM 规则	市售毒品 此规则会查找“市售毒品名称”字典中的 5 个关键字实例。
DCM 规则	大量生产的管制物 此规则会查找“生产的管制物”字典中的 5 个关键字实例。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

个人纳税识别号 (ITIN) 策略模板

个人纳税识别号 (ITIN) 是由美国国税局 (IRS) 颁发的税务处理号。IRS 颁发 ITIN 以便跟踪无资格获取社会安全号 (SSN) 的个人。

DCM 规则 **ITIN**

此规则会查找与美国 ITIN 数据标识符和“美国 ITIN 关键字”字典中的关键字匹配的项。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

国际武器贸易条例 (ITAR) 策略模板

国际武器贸易条例 (ITAR) 由美国国务院强制实施。国防服务或相关技术数据的出口商需要向联邦政府注册，并且还可能需要具备出口许可证。此策略会根据国家/地区以及由 ITAR 指定的受控资产来检测潜在违规。

“已编制索引的 ITAR 军需品和接受者”检测规则查找接受者中来自“ITAR 国家/地区代码”字典的国家/地区代码和来自已编制索引的 EDM 文件的特定 SKU。

表 36-31 已编制索引的 ITAR 军需品和接受者检测规则

方法	条件 (必须同时满足两个条件)	配置
复合规则	接受者匹配模式 (DCM)	匹配来自“ITAR 国家/地区代码”列表的接受者电子邮件或 URL 域： <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 必须至少匹配 1 个接受者。
	内容匹配确切数据 (EDM)	请参见第 326 页的 “选择确切数据配置文件” 。

ITAR 军需品名单和接受者检测规则将查找接受者中来自“ITAR 国家/地区代码”字典的国家/地区代码和来自“ITAR 军需品名称”字典中的关键字。

表 36-32 ITAR 军需品名单和接受者检测规则

方法	条件（必须同时满足两个条件）	配置
复合规则	接受者匹配模式 (DCM)	<p>匹配来自“ITAR 国家/地区代码”列表的接受者电子邮件或 URL 域：</p> <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 必须至少匹配 1 个接受者模式。
	内容匹配关键字 (DCM)	<p>匹配来自 ITAR 军需品名单的任何关键字：</p> <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。 ■ 严重性：高度。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

媒体文件策略模板

“媒体文件”策略会检测各种类型的视频和音频文件（包括 mp3）。

DCM 规则	媒体文件
此规则会查找下列媒体文件类型：	
	<ul style="list-style-type: none"> ■ qt ■ riff ■ macromedia_dir ■ midi ■ mp3 ■ mpeg_movie ■ quickdraw ■ realaudio ■ wav ■ video_win ■ vrml

DCM 规则

媒体文件扩展名

此规则会从“媒体文件扩展名”字典中查找文件名扩展名。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

并购协议策略模板

并购协议策略模板可检测有关并购活动的合同和正式文档。

可以使用公司特定的代码字词修改此模板以便检测特定交易。

并购协议模板提供了一个复合检测规则。规则中的所有条件必须匹配，才能通过规则触发事件。

表 36-33 并购协议复合检测规则

条件	配置
合同特定关键字（关键字匹配）	<ul style="list-style-type: none">■ 匹配任何关键字：merger、agreement、contract、letter of intent、term sheet、plan of reorganization■ 严重性：高度。■ 检查是否存在。■ 查找信封、主题、正文和附件。■ 不区分大小写。■ 仅进行全字匹配。
收购公司结构关键字（关键字匹配）	<ul style="list-style-type: none">■ 匹配任何关键字：subsidiary、subsidiaries、affiliate、acquiror、merger sub、covenantor、acquired company、acquiring company、surviving corporation、surviving company■ 严重性：高度。■ 检查是否存在。■ 查找信封、主题、正文和附件。■ 不区分大小写。■ 仅进行全字匹配。

条件	配置
合并注意事项关键字 (关键字匹配)	<ul style="list-style-type: none"> ■ 匹配任何关键字: merger stock、merger consideration、exchange shares、capital stock、dissenting shares、capital structure、escrow fund、escrow account、escrow agent、escrow shares、escrow cash、escrow amount、stock consideration、break-up fee、goodwill ■ 严重性: 高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。
法律合同关键字 (关键字匹配)	<ul style="list-style-type: none"> ■ 匹配任何关键字: recitals、in witness whereof、governing law、Indemnify、Indemnified、indemnity、signature page、best efforts、gross negligence、willful misconduct、authorized representative、severability、material breach ■ 严重性: 高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

NASD 规则 2711 以及 NYSE 规则 351 和 472 策略模板

此策略保护参与即将进行的股票发行的任何公司的名称、股票发行的内部项目名称以及发行公司的股票代号。

已编制索引的 NASD 规则 2711 文档检测规则将查找作为敏感内容注册、并且已知符合 NASD 规则 2711 或 NYSE 规则 351 和 472 的特定文档中的内容。如果找到源文档 80% 或以上的内容，此规则会返回一个匹配项。

表 36-34 已编制索引的 NASD 规则 2711 文档检测规则

方法	条件	配置
简单规则	内容匹配文档 签名 (IDM)	<p>已编制索引的 NASD 规则 2711 文档 (IDM):</p> <ul style="list-style-type: none"> ■ 检测选定的已编制索引的文档配置文件中的文档 ■ 要求内容至少匹配 80%。 ■ 严重性: 高度。 ■ 检查是否存在。 ■ 查看正文和附件。 <p>请参见第 327 页的“选择索引文档配置文件”。</p>

NASD 规则 2711 以及 NYSE 规则 351 和 472 检测规则是包含发送者条件和关键字条件的复合规则。发送者条件基于用户定义的用户公司的研究分析师电子邮件地址列表（“分析师的电子邮件地址”字典）。关键字条件会查找任何即将进行的股票发行、股票发行的内部项目名称以及发行公司的股票代号（“NASD 2711 关键字”字典）。它与发送者条件一样，要求由用户来编辑。

表 36-35 NASD 规则 2711 以及 NYSE 规则 351 和 472 检测规则

方法	条件	配置
复合规则	发送者/用户匹 配模式 (DCM)	<p>NASD 规则 2711 以及 NYSE 规则 351 和 472 (发送者) :</p> <ul style="list-style-type: none"> ■ 匹配发送者模式 [research_analyst@company.com] (用 户定义) ■ 严重性: 高度。 ■ 与整个邮件匹配。
	内容匹配关键 字 (DCM)	<p>NASD 规则 2711 以及 NYSE 规则 351 和 472 (关键字匹 配) :</p> <ul style="list-style-type: none"> ■ 匹配 “[公司股票代号]”、 “[发行公司的名称]”、 “[发 行名称(内部名称)]”。 ■ 严重性: 高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

NASD 规则 3010 和 NYSE 规则 342 策略模板

NASD 规则 3010 和 NYSE 规则 342 要求券商监管某些涉足证券经纪业务的员工的通信情况。此策略会监控遵守这些法规的已注册负责人的通信情况。

股票推荐检测规则将查找“NASD 3010 股票关键字”字典和“NASD 3010 购买/销售关键字”字典中的关键字。此外，此规则要求存在某种股票推荐以及购买或销售行为的推荐。

表 36-36 股票推荐检测规则

方法	条件（必须满足所有条件）	配置
复合规则	内容匹配关键字 (DCM)	匹配关键字：“建议” <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。
	内容匹配关键字 (DCM)	匹配关键字：“购买”或“销售” <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。
	内容匹配关键字 (DCM)	匹配关键字：“股票、证券、股份” <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

NASD 规则 3010 和 NYSE 规则 342 关键字检测规则将查找“NASD 3010 常规关键字”字典中的关键字，这些关键字用于查找任何常见的股票经纪人活动和股票关键字。

表 36-37 NASD 规则 3010 和 NYSE 规则 342 关键字检测规则

方法	条件（必须同时满足两个条件）	配置
复合规则	内容匹配关键字 (DCM)	<p>匹配关键字：“授权”、“谨慎”、“保证”、“选项”</p> <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。
	内容匹配关键字 (DCM)	<p>匹配关键字：“股票、证券、股份”</p> <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

NERC 电气设备安全指导策略模板

保护可能敏感信息的北美电力可靠性委员会 (NERC) 指导描述如何保护和确保关键电力基础设施的安全。

此策略会为电力行业检测 NERC 安全指导中所列出的信息。

表 36-38 关键响应人员检测规则

检测方法	匹配条件	配置
简单规则	内容匹配确切数据 (EDM)	<p>匹配以下任何三个数据项：</p> <ul style="list-style-type: none"> ■ 名字 ■ 姓氏 ■ 电话 ■ 电子邮件 <p>请参见第 326 页的“选择确切数据配置文件”。</p>

表 36-39 网络基础架构图检测规则

检测方法	匹配条件	配置
简单规则	内容匹配索引文档 (IDM)	此规则要求精确的二进制匹配。 请参见第 327 页的“ 选择索引文档配置文件 ”。

敏感关键字和漏洞关键字检测规则将查找“敏感关键字”字典和“漏洞关键字”字典中的任何关键字匹配项。

表 36-40 敏感关键字和漏洞关键字检测规则

检测方法	匹配条件	配置
复合规则	内容匹配关键字 (DCM)	匹配任何敏感关键字： <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。
	内容匹配关键字 (DCM)	匹配任何漏洞关键字： <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

网络图策略模板

“网络图”策略会检测计算机网络图是否存在泄露风险。

IDM 规则	已编制索引的网络图
	此规则会查找作为机密内容注册的特定网络图中的内容。如果检测到源文档 80% 或更多内容，则此规则会返回一个匹配项。
DCM 规则	具有 IP 地址的网络图
	此规则会与 IP 地址数据标识符结合查找 Visio 文件类型。

DCM 规则**具有 IP 地址关键字的网络图**

此规则会与具有数据标识符的“IP 地址”的短语变体结合查找 Visio 文件类型。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

网络安全策略模板

“网络安全”策略会检测是否存在黑客工具和攻击计划。

DCM 规则**GoToMyPC 活动**

此规则会查找具有数据标识符的 GoToMyPC 命令格式。

DCM 规则**黑客关键字**

此规则会查找“黑客关键字”字典中的关键字。

DCM 规则**击键记录程序关键字**

此规则会查找“击键记录程序关键字”字典中的关键字。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

攻击性语言策略模板

“攻击性语言”策略会检测攻击性语言的使用。

DCM 规则**明显带有攻击性的语言**

此规则会查找“明显带有攻击性的语言”字典中的任何单一关键字。

DCM 规则**一般攻击性语言**

此规则会查找“一般攻击性语言”字典中的任何三个关键字实例。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

外国资产管制办公室 (OFAC) 策略模板

美国财政部的外国资产控制办公室负责管理和强制实施经济和贸易制裁。这些制裁根据美国针对某些国家/地区、个人和组织制定的对外策略和国家安全目标来确定。

“外国资产管制办公室 (OFAC)” 策略会检测涉及这些目标组的通信情况。

OFAC 策略包含两个主要部分。第一部分处理特别指定的国民名单 (SDN)，第二部分处理常规 OFAC 策略限制。

SDN 名单指符合贸易限制条件的特定人员或组织。美国财政部为这些个人和实体提供包含特定名称、上一个已知地址，以及已知别名的文本文件。财政部指明这些地址可能不正确或不是最新的，并且不同地点不会针对人员和组织更改限制。

在 OFAC 策略模板中，Symantec Data Loss Prevention 已经优化该名单以确保它更为适用。这包括从名称和别名列表中提取关键字和关键短语，因为名称并不总是和列表中显示的格式相同。另外，删除了常见的名称以减少误报。例如，SDN 名单中一个名为 SARA 的组织。将它留在名单中会造成误报率很高。“SARA 属性”是列表中的另一个条目。它用作模板中的关键短语，因为该短语的影响范围比 SARA 小得多。考虑名称和组织列表时，会将在 SDN 地址列表中通常找到的国家/地区考虑在内。再次删除比较容易找到的国家/地区之后，会考虑列表中的前 12 个国家/地区。该模板可查找将任何列出的国家/地区作为指定的国家/地区代码的收件人。该 SDN 名单在将误报率降至最低的同时，仍然可以检测与已知受限方之间进行的交易或通信。

OFAC 策略还提供了美国财政部下发的与特定国家/地区的常规贸易相关的限制指导。这与 SDN 名单不同，因为个人和组织在此并未指定。可以在下列位置找到常规制裁列表：

<http://www.treasury.gov/offices/enforcement/ofac/programs/index.shtml>

外国资产管制办公室 (OFAC) 模板可通过指定的国家/地区代码查找 OFAC 列出的国家/地区的接受者。

OFAC 特别指定的国民名单和接受者检测规则结合“特别指定的国民名单”字典中的关键字的匹配项，查找国家/地区代码与“OFAC SDN 国家/地区代码”规范中的条目匹配的接受者。

表 36-41 OFAC 特别指定的国民名单和接受者检测规则

方法	条件	配置
复合规则	接受者匹配模式 (DCM)	OFAC 特别指定的国民名单和接受者（接受者）： <ul style="list-style-type: none"> ■ 按 OFAC SDN 国家/地区代码匹配电子邮件或 URL 域。 ■ 严重性：高度。 ■ 检查是否存在。 ■ 必须至少匹配 1 个接受者。 ■ 与整个邮件匹配。
	内容匹配关键字 (DCM)	特别指定的国民名单（关键字匹配）： <ul style="list-style-type: none"> ■ 匹配来自特别指定的国民名单的关键字。 ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

与 OFAC 国家/地区的通信检测规则将查找国家/地区代码与“OFAC 国家/地区代码”列表中的条目匹配的接受者。

表 36-42 与 OFAC 国家/地区的通信检测规则

方法	条件	配置
简单规则	接受者匹配模式 (DCM)	与 OFAC 国家/地区的通信（接受者）： <ul style="list-style-type: none"> ■ 按 OFAC 国家/地区代码匹配电子邮件或 URL 域。 ■ 严重性：高度。 ■ 检查是否存在。 ■ 必须至少匹配 1 个接受者。 ■ 与整个邮件匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

OMB 备忘录 06-16 和 FIPS 199 条例策略模板

此策略会根据美国国家标准与技术研究院 (NIST) 的联邦信息处理标准 (FIPS) 出版物 199 中建立的准则，来检测分类为机密的信息。加强这些安全分类是遵从来自管理与预算办公室 (OMB) 的备忘录 06-16 的基础。

此模板包含三个简单的检测规则。如果任一规则报告匹配项，策略就会触发事件。

高度机密性指标检测规则将查找“高度机密”字典中的任何关键字。

表 36-43 高度机密性指标检测规则

方法	条件	配置
简单规则	内容匹配关键字	高度机密性指标（关键字匹配）： <ul style="list-style-type: none"> ■ 匹配“（机密性，高）”、“（机密性，高）” ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

中机密性指标检测规则将查找“中机密性”字典中的任何关键字。

表 36-44 中机密性指标检测规则

方法	条件	配置
简单规则	内容匹配关键字	中机密性指标（关键字匹配）： <ul style="list-style-type: none"> ■ 匹配“（机密性，中）”、“（机密性，中）” ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

低度机密性指标检测规则将查找“低度机密性”字典中的任何关键字。

表 36-45 低度机密性指标检测规则

方法	条件	配置
简单规则	内容匹配关键字	低度机密性指标（关键字匹配）： <ul style="list-style-type: none"> ■ 匹配“（机密性，低）”、“（机密性，低）” ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

密码文件策略模板

“密码文件”策略会检测密码文件的格式，例如 SAM、password 和 shadow。

DCM 规则	密码文件名
此规则会查找文件名 passwd 或 shadow。	
DCM 规则	/etc/passwd 格式
此规则会查找 /etc/passwd 格式的正则表达式模式。	
DCM 规则	/etc/shadow 格式
此规则会查找 /etc/shadow 格式的正则表达式模式。	
DCM 规则	SAM 密码
此规则会查找 SAM 格式的正则表达式模式。	

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

支付卡行业 (PCI) 数据安全标准策略模板

支付卡行业 (PCI) 数据安全标准由 Visa 和 MasterCard 联合确定，可通过维护个人可识别信息的安全来保护持卡人。Visa 的持卡人信息安全计划 (CISP) 和 MasterCard 的站点数据保护 (SDP) 计划都致力于强制实施这些标准。“支付卡行业 (PCI) 数据安全标准”策略会检测 Visa 和 MasterCard 的信用卡号数据。

“确切的卡号”检测规则会检测数据库或其他数据源中配置的确切信用卡号。

表 36-46 “确切的信用卡号”检测规则

方法	条件	配置
简单规则	内容匹配确切数据 (EDM)	此规则会检测信用卡号。 请参见第 326 页的“ 选择确切数据配置文件 ”。

“所有信用卡号”检测规则会使用信用卡号系统数据标识符检测信用卡号。

表 36-47 所有信用卡号检测规则

方法	条件	配置
简单规则	内容匹配数据标识符 (DCM)	所有信用卡号 (数据标识符) : <ul style="list-style-type: none"> ■ 数据标识符：信用卡号 (窄) 请参见第 532 页的“信用卡号数据标识符”。 ■ 严重性：高度。 ■ 计算所有匹配项。 ■ 查找信封、主题、正文和附件。

“信用卡的磁条数据”检测规则会使用信用卡磁条系统数据标识符检测信用卡磁条中的原始数据。

表 36-48 “信用卡的磁条数据”检测规则

方法	条件	配置
简单规则	内容匹配数据标识符 (DCM)	信用卡的磁条数据 (数据标识符) : <ul style="list-style-type: none"> ■ 数据标识符：信用卡磁条 (中) 请参见第 532 页的“信用卡号数据标识符”。 ■ 数据严重性：高。 ■ 计算所有匹配项。 ■ 查找信封、主题、正文和附件。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

PIPEDA 策略模板

加拿大的个人信息保护和电子文档法案(PIPEDA)保护由私营组织掌握的个人信息。此法案提供收集、使用和披露个人信息的准则。

PIPEDA 策略会检测 PIPEDA 条例保护的客户数据。

PIPEDA 检测规则用于查找两个数据项的匹配情况，在匹配时已排除特定数据组合。

表 36-49 PIPEDA 检测规则

检测方法类型	说明	已排除的组合
EDM 规则	<p>PIPEDA 检测规则匹配以下任意两个数据项：</p> <ul style="list-style-type: none"> ■ 姓氏 ■ 银行卡号 ■ 医疗帐户号码 ■ 医疗记录 ■ 代理人编号 ■ 帐号 ■ PIN ■ 用户名 ■ 密码 ■ SIN ■ ABA 汇款路径号码 ■ 电子邮件 ■ 电话 ■ 母亲的婚前姓 <p>请参见第 326 页的“选择确切数据配置文件”。</p>	<p>但是，下列组合不会创建匹配项：</p> <ul style="list-style-type: none"> ■ 姓氏、电子邮件 ■ 姓氏、电话号码 ■ 姓氏、帐号 ■ 姓氏、用户名

PIPEDA 联系信息检测规则用于查找两个数据项的匹配情况，在匹配时已排除特定数据组合。

表 36-50 PIPEDA 联系信息检测规则

检测方法类型	说明
EDM 规则	<p>此规则会查找以下任意两个数据列：</p> <ul style="list-style-type: none"> ■ 姓氏 ■ 电话 ■ 帐号 ■ 用户名 ■ 电子邮件 <p>请参见第 326 页的“选择确切数据配置文件”。</p>

表 36-51 加拿大社会保险号检测规则

检测方法类型	说明
DCM 规则	此规则实施加拿大社会保险号数据标识符的小宽度版本。 请参见第 528 页的“ 加拿大社会保险号小宽度 ”。

表 36-52 ABA 汇款路径号码检测规则

检测方法类型	说明
DCM 规则	此规则实施 ABA 汇款路径号码数据标识符的小宽度版本。 请参见第 524 页的“ ABA 汇款路径号码小宽度 ”。

表 36-53 所有信用卡号检测规则

检测方法类型	说明
DCM 规则	此规则实施信用卡号数据标识符的小宽度版本。 请参见第 535 页的“ 信用卡号小宽度 ”。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

价格信息策略模板

“价格信息”策略会检测有泄露风险的特定 SKU 和价格信息。

EDM 规则 价格信息

此规则会查找用户定义的库存单位(SKU)号与该 SKU 号的价格的组合。

注意：此模板包含一个 EDM 检测规则。如果您未配置 EDM 配置文件，或者使用的是 Symantec Data Loss Prevention Standard，则此策略模板将为空且不包含任何可配置的规则。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

项目数据策略模板

“项目数据”策略会检测对敏感项目的讨论。

IDM 规则

已编制索引的项目文档

此规则会查找已注册为专有内容的特定项目数据文件中的内容。如果引擎检测到源文档的 80% 或更多内容，则会返回匹配项。

DCM 规则

项目活动

此规则会查找用户定义的“敏感项目代码名称”字典中的任何关键字。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

请参见第 377 页的[“关于实施索引文档匹配”](#)。

专有媒体文件策略模板

“专有媒体文件”策略会检测有泄露风险且属于您组织的专有财产和知识产权的各种类型的视频和音频文件。

IDM 规则

已编制索引的媒体文件

此规则会查找已注册为专有内容的特定媒体文件中的内容。

DCM 规则

媒体文件

此规则会查找下列媒体文件类型：

- qt
- riff
- macromedia_dir
- midi
- mp3
- mpeg_movie
- quickdraw
- realaudio
- wav
- video_win
- vrml

DCM 规则

媒体文件扩展名

此规则会从“媒体文件扩展名”字典中查找文件名扩展名。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

请参见第 377 页的“[关于实施索引文档匹配](#)”。

出版文档策略模板

“出版文档”策略会检测有泄露风险的各种类型的出版文档，如 Adobe FrameMaker 文件。

IDM 规则

已编制索引的出版文档

此规则会查找注册为专有内容的特定出版文档中的内容。如果引擎检测到源文档的 80% 或更多内容，则会返回匹配项。

DCM 规则

出版文档

此规则会查找指定的文件类型：

- qxpress
- frame
- aldus_pagemaker
- publ

DCM 规则

出版文档, 扩展名

此规则会查找在“出版文档扩展名”字典中找到的特定文件扩展名。

注意：由于检测引擎不检测所有所需文档的真实文件类型，因此该策略要求同时使用文件类型和文件扩展名。同样，文件扩展名必须与文件类型结合使用。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

请参见第 377 页的“[关于实施索引文档匹配](#)”。

种族歧视语言策略模板

“种族歧视语言”策略会检测种族歧视语言的使用。

DCM 规则

种族歧视语言

此规则会查找“种族歧视语言”字典中的任何单一关键字。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

受限文件策略模板

“受限文件”策略会检测通常不适合发送到公司之外的各种文件类型，如 Microsoft Access 和可执行文件。

DCM 规则

MSAccess 文件和可执行文件

此规则会查找以下特定类型的文件：access、exe 和 exe_unix。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

受限接受者策略模板

“受限接受者”策略会检测与指定收件人（如前员工）之间的通信。

DCM 规则

受限接受者

此规则会查找发送给其电子邮件地址位于“受限接受者”字典中的收件人的邮件。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

简历策略模板

“简历”策略会检测活动的职位搜索。

EDM 规则

员工简历

此规则是包含两个条件的复合规则；必须同时满足这两个条件，才能触发事件。此规则包含 EDM 条件，用于查找用户提供的员工名字和姓氏。

此规则还用于查找小于 50KB 并且包含下列每本字典中的至少一个关键字的特定文件类型附件 (.doc)：

- 教育方面的职位搜索关键字
- 工作方面的职位搜索关键字
- 常规职位搜索关键字

DCM 规则

所有简历

此规则会查找小于 50 KB 并且与下列每本字典中的至少一个关键字匹配的指定类型 (.doc) 的文件：

- 教育方面的职位搜索关键字
- 工作方面的职位搜索关键字
- 常规职位搜索关键字

DCM 规则

职位搜索网站

此规则会查找在职位搜索中使用的网站的 URL。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

请参见第 356 页的“[关于实施确切数据匹配](#)”。

萨班斯-奥克斯利法案策略模板

美国萨班斯-奥克斯利法案(SOX)能够强制实施财务会计要求，包括保持数据完整性和创建审核跟踪。“萨班斯-奥克斯利”策略会检测敏感财务数据。

“已编制索引的萨班斯-奥克斯利法案文档”检测规则用于查找已注册为隶属于萨班斯-奥克斯利法案的特定文档中的内容。如果发现源文档的 80% 或更多内容，则此规则会返回一个匹配项。

表 36-54 “已编制索引的萨班斯-奥克斯利法案文档” 检测规则

方法	条件	配置
简单规则	内容匹配已编制索引的文档配置文件	请参见第 327 页的“ 选择索引文档配置文件 ”。

“SEC 公平披露规则”复合检测规则用于查找以下条件；必须满足所有条件，该规则才能触发事件：

- SEC 公平披露关键字指示可能会披露高级金融信息（“SEC 公平披露规则关键字”字典）。
- 属于常用文档或电子表格格式的附件类型或文件类型。检测到的文件类型有：Microsoft Word、Excel 宏、Excel、Works 电子表格、SYLK 电子表格、Corel Quattro Pro、WordPerfect、Lotus 123、Applix 电子表格、CSV、Multiplan 电子表格和 Adobe PDF。

- 公司名称关键字列表要求由用户来编辑。这可能包括任何名称、备用名称或可能表示公司的缩写。

表 36-55 “SEC 公平披露规则” 检测规则

方法	条件	配置
复合规则	内容匹配关键字	<p>SEC 公平披露规则（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 匹配关键字：earnings per share、forward guidance ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。 ■ 同一组件的匹配。 <p>关键字必须在通过该条件检测到的附件类型或文件类型中。</p>
	邮件附件类型或文件类型匹配	<p>SEC 公平披露规则（附件/文件类型）：</p> <ul style="list-style-type: none"> ■ 检测到的文件类型有：excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、123、doc、wordperfect 和 pdf。 ■ 严重性：高度。 ■ 匹配位置：附件和同一组件。
	内容匹配关键字	<p>SEC 公平披露规则（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 匹配 “[公司名称]” ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。 ■ 同一组件的匹配。 <p>关键字必须在通过该条件检测到的附件类型或文件类型中。</p>

“金融信息”检测规则用于查找包含“金融关键字”字典中的关键字和“机密/专有字词”字典中的关键字的特定文件类型。检测到的电子表格文件类型有：Microsoft Excel Macro、Microsoft Excel、Microsoft Works Spreadsheet、SYLK Spreadsheet、Corel Quattro Pro 等。

表 36-56 “金融信息” 检测规则

方法	条件	配置
复合规则	内容匹配已编制索引的文档配置文件	<p>金融信息（附件/文件类型）：</p> <ul style="list-style-type: none"> ■ 匹配文件类型：excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、Lotus 1-2-3 ■ 严重性：高度。 ■ 匹配位置：附件和同一组件。
	内容匹配关键字	<p>金融信息（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 匹配“accounts receivable turnover”、“adjusted gross margin”、“adjusted operating expenses”、“adjusted operating margin”、“administrative expenses”.... ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。 ■ 必须在附件（同一组件）中检测到关键字。
	内容匹配关键字	<p>金融信息（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 匹配“confidential”、“internal use only”、“proprietary”。 ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。 ■ 必须在附件（同一组件）中检测到关键字。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

SEC 公平披露规则策略模板

美国 SEC 选择性披露和内幕交易规则禁止上市公司在正式上市之前向分析人员和机构投资者选择性地披露重要信息。

“SEC 公平披露规则” 模板可检测表示披露重要财务信息的数据。

“已编制索引的 SEC 公平披露规则文档 (IDM)” 检测规则用于查找隶属于 SEC 公平披露规则的特定文档中的内容。如果发现源文档的 80% 或更多内容，则此规则会返回一个匹配项。

表 36-57 “已编制索引的 SEC 公平披露规则文档 (IDM)” 检测规则

方法	条件	配置
简单规则	内容匹配文档 签名 (IDM)	<p>已编制索引的 SEC 公平披露规则文档 (IDM):</p> <ul style="list-style-type: none">■ 检测选定的已编制索引的文档配置文件中的文档。 请参见第 327 页的“选择索引文档配置文件”。■ 按至少有 80% 的内容匹配的要求匹配文档。■ 严重性: 高度。■ 检查是否存在。■ 查看正文和附件。

“SEC 公平披露规则” 检测规则用于查找 “SEC 公平披露规则关键字” 字典中的关键字匹配项、属于常用文档或电子表格的附件类型或文件类型，以及 “公司名称关键字” 字典中的关键字匹配项。

必须同时满足这三个条件，才能通过规则触发事件：

- SEC 公平披露规则关键字指示可能会披露高级金融信息。
- 检测到的文件类型有：Microsoft Word、Excel 宏、Excel、Works 电子表格、SYLK 电子表格、Corel Quattro Pro、WordPerfect、Lotus 123、Applix 电子表格、CSV、Multiplan 电子表格和 Adobe PDF。
- 公司名称关键字列表要求由用户来编辑。这可能包括任何名称、备用名称或可能表示公司的缩写。

表 36-58 “SEC 公平披露规则” 检测规则

方法	条件	配置
复合规则	内容匹配关键字 (DCM)	<p>SEC 公平披露规则（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 匹配“earnings per share”、“forward guidance”。 ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 不区分大小写。 ■ 仅进行全字匹配。
	邮件附件类型或文件类型匹配 (DCM)	<p>SEC 公平披露规则（附件/文件类型）：</p> <ul style="list-style-type: none"> ■ 匹配文件类型：excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、123、doc、wordperfect、pdf ■ 严重性：高度。 ■ 匹配附件。 ■ 要求内容匹配项在同一组件中（附件）。
	内容匹配关键字 (DCM)	<p>SEC 公平披露规则（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 匹配 “[公司名称]”（用户定义） ■ 严重性：高度。 ■ 检查是否存在。 ■ 在信封、主题、正文、附件和同一组件中查找。 ■ 不区分大小写。 ■ 仅进行全字匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

下流语言策略模板

“下流语言”策略会检测粗俗和下流的语言内容。

DCM 规则	已确认的下流关键字
此规则会查找“已确认的下流关键字”字典中的任何单一关键字。	
DCM 规则	可疑的下流关键字
此规则会查找“可疑的下流关键字”字典中的任何三个关键字实例。	

DCM 规则	可能的下流关键字
此规则会查找“可能的下流关键字”字典中的任何三个关键字实例。	

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

源代码策略模板

“源代码”策略会检测有泄露风险的各种类型的源代码。

IDM 规则	源代码文档
此规则使用 IDM 查找用户提供的特定源代码。如果检测到源文档 80% 或更多内容，则此规则会返回一个匹配项。	
DCM 规则	源代码扩展名
此规则会从“源代码扩展名”字典中查找文件名扩展名。	
DCM 规则	Java 源代码
此规则会查找 Java 导入语句或 Java 类文件正则表达式。	
DCM 规则	C 源代码
此规则会查找 C 源代码正则表达式。	
DCM 规则	VB 源代码
此规则会查找 VB 源代码正则表达式。	
DCM 规则	PERL 源代码
此规则会查找三个不同的与 PERL 相关的系统模式和正则表达式。	

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

请参见第 377 页的[“关于实施索引文档匹配”](#)。

州数据隐私策略模板

美国的许多州都通过了要求保护数据和公开披露信息安全（个人的机密数据受到威胁）的法令。“州数据隐私”策略会检测这些违反机密性的行为。

首先会对“发送到附属机构的电子邮件”检测例外进行评估，该检测例外适用于向特定附属机构（允许这些机构合法接收州数据隐私条例中规定的信息）发送的电子邮件。

表 36-59 “发送到附属机构的电子邮件”检测例外

方法	条件	配置
简单例外	接受者匹配模式(DCM)	<p>发送到附属机构（接受者）的电子邮件：</p> <ul style="list-style-type: none"> ■ 匹配电子邮件：[affiliate1]、[affiliate2]。 “附属机构域”需要由用户来编辑。 ■ 必须至少匹配 1 个接受者。 ■ 与整个邮件匹配。

“州数据隐私-客户数据”检测规则用于查找基于任意三个数据项（特定组合除外）的完全匹配项。

表 36-60 “州数据隐私 - 客户数据”检测规则

方法	条件	配置
简单规则	内容匹配确切数据(EDM)	<p>此规则会查找基于任意三个数据项的匹配项：</p> <ul style="list-style-type: none"> ■ 名字 ■ 姓氏 ■ 缴税 ID ■ 银行卡号 ■ 帐户 ■ PIN ■ 州 ID ■ 驾驶执照 ■ 密码 ■ ABA 号码 ■ 出生日期 <hr/> <p>但是，以下组合不匹配：</p> <ul style="list-style-type: none"> ■ 名字、姓氏、PIN ■ 名字、姓氏、密码 <p>请参见第 326 页的“选择确切数据配置文件”。</p>

“美国社会安全号模式”检测规则会实施美国 SSN 小宽度系统数据标识符来检测社会安全号。

表 36-61 美国社会安全号模式检测规则

检测方法	条件类型	配置
简单规则	内容匹配数据标识符 (DCM)	<p>美国社会安全号模式：</p> <ul style="list-style-type: none"> ■ 请参见第 579 页的“美国社会安全号 (SSN) 小宽度”。 ■ 严重性：高度。 ■ 计算所有匹配项。 ■ 查找信封、主题、正文和附件。

“ABA 汇款路径号码”检测规则会实施 ABA 汇款路径号码数据标识符。

表 36-62 ABA 汇款路径号码检测规则

方法	条件	配置
简单规则	内容匹配数据标识符 (DCM)	<p>ABA 汇款路径号码：</p> <ul style="list-style-type: none"> ■ 请参见第 524 页的“ABA 汇款路径号码小宽度”。 ■ 严重性：高度。 ■ 计算所有匹配项。 ■ 查找信封、主题、正文和附件。

“所有信用卡号”检测规则用于查找“信用卡号关键字”字典中的关键字以及信用卡号系统模式。

表 36-63 所有信用卡号检测规则

方法	条件	配置
简单规则	内容匹配数据标识符 (DCM)	<p>所有信用卡号（数据标识符）：</p> <ul style="list-style-type: none"> ■ 信用卡号 请参见第 535 页的“信用卡号小宽度”。 ■ 严重性：高度。 ■ 计算所有匹配项。 ■ 查看信封、主题、正文和附件

“加利福尼亚驾驶执照号码”检测规则会查找符合加利福尼亚驾驶执照号码模式的匹配项、符合“驾驶执照”相关术语的数据标识符的匹配项以及“加利福尼亚关键字”字典中的关键字。

表 36-64 “加利福尼亚驾驶执照号码”检测规则

检测方法	条件类型	配置
简单规则	内容匹配数据标识符 (DCM)	请参见第 540 页的 “驾驶执照号码 - 加利福尼亚州数据标识符” 。

“纽约驾驶执照号码”检测规则会查找符合纽约驾驶执照号码模式的匹配项、符合“驾驶执照”相关术语的正则表达式的匹配项以及“纽约关键字”字典中的关键字。

表 36-65 “纽约驾驶执照号码”检测规则

检测方法	条件类型	配置
简单规则	内容匹配数据标识符 (DCM)	请参见第 545 页的 “驾驶执照号码 - 纽约州数据标识符” 。

“佛罗里达州、密歇根州和明尼苏达州驾驶执照号码”检测规则用于查找符合州驾驶执照号码模式的匹配项、符合“驾驶执照”相关术语的正则表达式的匹配项以及“字母/12 位数字的驾驶执照号码州字词”字典（即佛罗里达州、明尼苏达州和密歇根州）中的关键字。

表 36-66 “佛罗里达州、密歇根州和明尼苏达州驾驶执照号码”检测规则

方法	条件	配置
简单规则	内容匹配数据标识符 (DCM)	请参见第 541 页的 “驾驶执照号码 - 佛罗里达州、密歇根州和明尼苏达州数据标识符” 。

“伊利诺斯驾驶执照号码”检测规则用于查找符合伊利诺斯驾驶执照号码模式的匹配项、符合“驾驶执照”相关术语的正则表达式的匹配项以及“伊利诺斯关键字”字典中的关键字。

表 36-67 “伊利诺斯驾驶执照号码”检测规则

检测方法	条件类型	配置
简单规则	内容匹配数据标识符 (DCM)	请参见第 543 页的 “驾驶执照号码 - 伊利诺斯州数据标识符” 。

“新泽西驾驶执照号码”检测规则用于查找符合新泽西驾驶执照号码模式的匹配项、符合“驾驶执照”相关术语的正则表达式的匹配项以及“新泽西关键字”字典中的关键字。

表 36-68 “新泽西驾驶执照号码”检测规则

检测方法	条件类型	配置
简单规则	内容匹配数据标识符 (DCM)	<p>此条件实施“驾驶执照号码 - 新泽西州”中宽度系统数据标识符。</p> <p>请参见第 545 页的“驾驶执照号码 - 新泽西州中宽度”。</p>

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

SWIFT 代码策略模板

环球同业银行金融电讯协会(SWIFT)是依据比利时法律建立的合作组织，为其成员金融机构共同拥有。SWIFT 代码（也称为银行标识码(BIC)或 ISO 9362）使用标准格式来标识所涉及的银行、位置和分支机构。当在各银行之间转账（特别是跨国界转账）时，将会使用这些代码。

DCM 规则

SWIFT 代码正则表达式

此规则会查找与 SWIFT 代码正则表达式和“SWIFT 代码关键字”字典中的关键字匹配的项。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

Symantec DLP 感知与避免策略模板

“Symantec DLP 感知与避免”策略会检测引用 Symantec Data Loss Prevention 或数据泄露防护系统的任何通信和可能的检测避免。对于受监控的用户未广泛知晓的部署，Symantec DLP 感知与避免策略非常有用。

DCM 规则

Symantec DLP 感知

搜索“Symantec DLP 感知”字典中的关键字匹配项。

DCM 规则

Symantec DLP 避免

此规则是包含两个条件的复合规则；必须同时满足这两个条件，才能触发事件。此规则会查找“Symantec DLP 感知”字典中的关键字匹配项和“Symantec DLP 避免”字典中的关键字。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的“[将策略检测导出为模板](#)”。

英国驾照号策略模板

“英国驾照号”策略会使用英国内阁办公厅的英国政府标准的官方规范来检测英国驾照号。

DCM 规则

英国驾照号

此规则是具有以下条件的复合规则：

- “英国关键字”字典中的一个关键字
- 与英国驾照数据标识符的模式相匹配的模式
- 使用数据标识符的“驾照”短语的不同组合

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

英国选民登记号策略模板

“英国选民登记号”策略会使用英国内阁办公厅的英国政府标准的官方规范来检测英国选民登记号。

DCM 规则

英国选民登记号

此规则是具有以下条件的复合规则：

- “英国关键字”字典中的一个关键字
- 与英国选民登记号数据标识符匹配的模式
- “英国选民登记号字词”字典中的一个关键字

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

英国国民保健服务 (NHS) 号策略模板

“英国国民保健服务 (NHS) 号”策略会检测由英国国家卫生署 (NHS) 颁发的个人标识号码，用于进行医疗管理。

DCM 规则

英国 NHS 号

此规则会查找具有以下两个部分的一个复合条件：新型或旧型国民保健服务号和“英国 NHS 关键字”字典中的单个关键字。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

英国国家保险号码策略模板

国家保险号码由英国就业及退休金部和税务局 (DWP/IR) 颁发给个人，以便管理国家保险系统。“英国国家保险号码”策略会检测这些保险策略号。

DCM 规则

英国国家保险号码

此规则会查找与英国国家保险号码数据标识符以及“英国 NIN 关键字”字典中的关键字匹配的项。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

英国护照号策略模板

“英国护照号”策略会使用英国内阁办公厅的英国政府标准的官方规范来检测有效的英国护照。

DCM 规则

英国护照号（旧型）

此规则会查找“英国护照关键字”字典中的关键字以及与“英国护照号”（旧型）的正则表达式匹配的模式。

DCM 规则

英国护照号（新型）

此规则会查找“英国护照关键字”字典中的关键字以及与“英国护照号”（新型）的正则表达式匹配的模式。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

英国税号策略模板

“英国税号”策略会使用英国内阁办公室颁布的英国政府标准中的官方规范来检测英国税号。

DCM 规则 英国税号

此规则会查找与英国税号数据标识符以及“英国税号关键字”字典中的关键字匹配的项。

请参见第 330 页的[“配置策略”](#)。

请参见第 351 页的[“将策略检测导出为模板”](#)。

美国情报控制标记 (CAPCO) 和 DCID 1/7 策略模板

“美国情报控制标记 (CAPCO) 和 DCID 1/7”策略会检测已认可词汇，以便识别 Control Markings Register 中定义的美国联邦情报机构的分类信息，此信息由 Community Management Staff (CMS) 的 Controlled Access Program Coordination Office (CAPCO) 来维护。创建注册的目的是为了响应 Director of Central Intelligence Directive (DCID) 1/7。

此规则会查找 TOP SECRET 短语的关键字匹配项。

表 36-69 “最高机密信息”检测规则

方法	条件	配置
简单规则	内容匹配关键字 (DCM)	匹配 “TOP SECRET//” <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 区分大小写。 ■ 全字匹配或部分匹配。

此规则会查找 SECRET 短语的关键字匹配项。

表 36-70 “机密信息” 检测规则

方法	条件	配置
简单规则	内容匹配关键字 (DCM)	匹配 “SECRET//” <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 区分大小写。 ■ 全字匹配或部分匹配。

此规则会查找 CLASSIFIED 或 RESTRICTED 短语的关键字匹配项。

表 36-71 “分类或限制信息（关键字匹配）” 检测规则

方法	条件	配置
简单规则	内容匹配关键字 (DCM)	匹配 “CLASSIFIED//,//RESTRICTED//” <ul style="list-style-type: none"> ■ 严重性：高度。 ■ 检查是否存在。 ■ 查找信封、主题、正文和附件。 ■ 区分大小写。 ■ 全字匹配或部分匹配。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

美国社会安全号策略模板

“美国社会安全号” 策略会检测表明有泄露风险的社会安全号的模式。

DCM 规则

美国社会安全号模式

此规则会查找与社会安全号正则表达式和“美国 SSN 关键字”字典中的关键字匹配的项。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

暴力与武器策略模板

“暴力与武器”策略会检测暴力语言和有关武器的讨论。

DCM 规则

暴力与武器

此规则是包含两个条件的复合规则；必须同时满足这两个条件，才能触发事件。此规则会查找“暴力关键字”字典中的关键字和“武器关键字”字典中的关键字。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

Webmail 策略模板

Webmail 策略会检测多种 Webmail 服务（包括 Yahoo、Google 和 Hotmail）的使用情况。

表 36-72

名称	类型	条件	说明
Yahoo	复合检测规则	接受者匹配模式(DCM)	此条件会搜索 URL 域 mail.yahoo.com 。
		内容匹配关键字(DCM)	此条件会搜索关键字 ym/compose 。
Hotmail	复合检测规则	接受者匹配模式(DCM)	此条件会搜索 URL 域 hotmail.msn.com 。
		内容匹配关键字(DCM)	此条件会搜索关键字 compose?&curmbox 。
Go	复合检测规则	接受者匹配模式(DCM)	此条件会搜索 URL gomailus.go.com 。
		内容匹配关键字(DCM)	此条件会搜索关键字 compose 。
AOL	复合检测规则	接受者匹配模式(DCM)	此条件会搜索 URL 域 aol.com 。
		内容匹配关键字(DCM)	此条件会搜索关键字 compose 。

名称	类型	条件	说明
Gmail	复合检测规则	接受者匹配模式 (DCM)	此条件会搜索 URL 域 gmail.google.com 。
		内容匹配关键字 (DCM)	此条件会搜索关键字 gmail 。

请参见第 330 页的“[配置策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

Yahoo 留言板活动策略模板

“Yahoo 留言板”策略模板会检测 Yahoo 留言板活动。

“Yahoo 留言板”检测规则是查找发布到指定 Yahoo 留言板的留言的复合方法。

[表 36-73](#) 说明了其配置详细信息。

表 36-73 “Yahoo 留言板” 检测规则

方法	条件	配置
复合规则	内容匹配关键字 (DCM)	<p>Yahoo 留言板（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 不区分大小写。 ■ 匹配关键字： post.messages.yahoo.com/bbs。 ■ 仅进行全字匹配。 ■ 检查是否存在（不计算多个匹配项）。 ■ 查找信封、主题、正文和附件。 ■ 对于这两个条件来说，匹配都必须发生在同一组件中。
	AND	
	内容匹配关键字 (DCM)	<p>Yahoo 留言板（关键字匹配）：</p> <ul style="list-style-type: none"> ■ 不区分大小写。 ■ 匹配关键字： board=<enter board number>。 ■ 仅进行全字匹配。 ■ 检查是否存在（不计算多个匹配项）。 ■ 查找信封、主题、正文和附件。 ■ 对于这两个条件来说，匹配都必须发生在同一组件中。

“金融留言板 URL”检测规则会检测发布到 Yahoo 金融留言板的留言。

[表 36-74](#) 说明了其配置。

表 36-74

“金融留言板 URL”检测规则

方法	条件	配置
简单规则	内容匹配关键字 (DCM)	<p>金融留言板 URL (关键字匹配) :</p> <ul style="list-style-type: none"> ■ 不区分大小写。 ■ 匹配关键字: messages.finance.yahoo.com。 ■ 仅进行全字匹配。 ■ 检查是否存在 (不计算多个匹配项)。 ■ 查找信封、主题、正文和附件。

“板 URL”检测规则会检测发布到 Yahoo 留言板或 Yahoo 金融留言板的留言（通过二者中任意一个留言板的 URL）。

表 36-75 说明了其配置详细信息。

表 36-75

“板 URL”检测规则

方法	条件	配置
简单规则	接受者匹配模式 (DCM)	<p>板 URL (接受者) :</p> <ul style="list-style-type: none"> ■ 接受者 URL: messages.yahoo.com、 messages.finance.yahoo.com。 ■ 必须至少匹配 1 个接受者。 ■ 与整个消息匹配 (不可配置)。

请参见第 317 页的“[从模板创建策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

端口 80 上的 Yahoo 和 MSN Messenger 策略模板

“端口 80 上的 Yahoo 和 MSN Messenger”策略会检测端口 80 上的 Yahoo 和 MSN Messenger 活动。

Yahoo IM 检测规则会查找基于 ymsg 和 shttp.msg.yahoo.com 的关键字匹配项。

表 36-76 Yahoo IM 检测规则

方法	条件	配置
复合规则	内容匹配关键字 (DCM)	<p>Yahoo IM (关键字匹配) :</p> <ul style="list-style-type: none">■ 不区分大小写。■ 匹配关键字: ymsg。■ 仅进行全字匹配。■ 计算所有匹配项并对每个匹配项报告一个事件。■ 查找信封、主题、正文和附件中的匹配项。■ 对于规则中的两个条件来说，匹配都必须发生在同一组件中。
	AND	
复合规则	内容匹配关键字 (DCM)	<p>Yahoo IM (关键字匹配) :</p> <ul style="list-style-type: none">■ 不区分大小写。■ 匹配关键字: shttp.msg.yahoo.com。■ 仅进行全字匹配。■ 计算所有匹配项并对每个匹配项报告一个事件。■ 查找信封、主题、正文和附件中的匹配项。■ 对于规则中的两个条件来说，匹配都必须发生在同一组件中。

MSN IM 检测规则用于查找同一邮件组件中基于三个关键字的匹配项。

表 36-77 MSN IM 检测规则

方法	条件	配置
复合规则	内容匹配关键字 (DCM)	<p>MSN IM (关键字匹配) :</p> <ul style="list-style-type: none"> ■ 不区分大小写。 ■ 匹配关键字: msg。 ■ 仅进行全字匹配。 ■ 计算所有匹配项并对每个匹配项报告一个事件。 ■ 查找信封、主题、正文和附件中的匹配项。 ■ 对于规则中的所有条件来说，匹配都必须发生在同一组件中。
	AND	
	内容匹配关键字 (DCM)	<p>MSN IM (关键字匹配) :</p> <ul style="list-style-type: none"> ■ 不区分大小写。 ■ 匹配关键字: x-msn。 ■ 仅进行全字匹配。 ■ 计算所有匹配项并对每个匹配项报告一个事件。 ■ 查找信封、主题、正文和附件中的匹配项。 ■ 对于规则中的所有条件来说，匹配都必须发生在同一组件中。
复合规则	AND	
	内容匹配关键字 (DCM)	<p>MSN IM (关键字匹配) :</p> <ul style="list-style-type: none"> ■ 不区分大小写。 ■ 匹配关键字: charset=utf-8。 ■ 仅进行全字匹配。 ■ 计算所有匹配项并对每个匹配项报告一个事件。 ■ 查找信封、主题、正文和附件中的匹配项。 ■ 对于规则中的所有条件来说，匹配都必须发生在同一组件中。

请参见第 317 页的“[从模板创建策略](#)”。

请参见第 351 页的“[将策略检测导出为模板](#)”。

5

部分

配置策略响应

- 37. 响应策略违规
- 38. 配置和管理响应规则
- 39. 响应规则条件
- 40. 响应规则操作

响应策略违规

本章节包括下列主题：

- [关于响应规则](#)
- [关于响应规则操作](#)
- [所有检测服务器的响应规则](#)
- [端点检测的响应规则](#)
- [Network and Mobile Prevent for Web 检测的响应规则](#)
- [Network Protect 检测的响应规则](#)
- [分类服务器的响应规则](#)
- [关于响应规则执行类型](#)
- [关于“自动”响应规则](#)
- [关于智能响应规则](#)
- [关于响应规则条件](#)
- [关于响应规则操作的执行优先级](#)
- [关于响应规则创建权限](#)
- [实施响应规则](#)
- [响应规则最佳做法](#)

关于响应规则

出现违规时，您可以在策略中实施一个或多个响应规则，以提报、解决或排除事件。例如，如果违反了策略，响应规则会阻止传输包含敏感内容的文件。

请参见第 654 页的“[关于响应规则操作](#)”。

您可以独立于声明响应规则的策略创建、修改和管理这些响应规则。响应规则与策略的分离允许跨策略更新和重复使用响应规则。

请参见第 664 页的“[实施响应规则](#)”。

检测服务器将自动执行响应规则。或者，您可以配置智能响应规则，以供事件补救者手动执行。

请参见第 659 页的“[关于响应规则执行类型](#)”。

您可以实施条件来控制执行响应规则的方式和时间。

请参见第 661 页的“[关于响应规则条件](#)”。

您可以指定相同类型的响应规则的执行顺序。

请参见第 662 页的“[关于响应规则操作的执行优先级](#)”。

必须具有响应规则的创建权限才能创建和管理响应规则。

请参见第 664 页的“[关于响应规则创建权限](#)”。

关于响应规则操作

响应规则操作是在发生策略违规时执行操作的组件。响应规则操作是响应规则的必需组件。如果创建响应规则，则必须至少定义一个操作，才能让响应规则生效。

Symantec Data Loss Prevention 提供了多个响应规则操作。许多操作可用于所有类型的检测服务器，部分操作只能用于特定的检测服务器。

请参见第 664 页的“[实施响应规则](#)”。

只要发生策略违规，已部署策略的检测服务器就会执行响应规则操作。您也可以在配置响应规则条件时指定响应规则操作的执行时间。

请参见第 661 页的“[关于响应规则条件](#)”。

例如，只要出现违反策略的情况，就向违反策略的用户和管理员发送电子邮件。或者，如果策略违规严重性等级为“中”，则向用户显示屏幕警告。或者，如果严重性为“高”，则阻止文件复制到外部设备。

表 37-1 针对服务器类型制定的响应规则

服务器类型	说明
所有检测服务器	请参见第 655 页的“ 所有检测服务器的响应规则 ”。
端点检测服务器	请参见第 656 页的“ 端点检测的响应规则 ”。

服务器类型	说明
Network and Mobile Prevent for Web 检测服务器	请参见第 657 页的“ Network and Mobile Prevent for Web 检测的响应规则 ”。
Network Protect 检测服务器	请参见第 658 页的“ Network Protect 检测的响应规则 ”。
分类检测服务器	请参见第 658 页的“ 分类服务器的响应规则 ”。

所有检测服务器的响应规则

Symantec Data Loss Prevention 针对 Endpoint Prevent、Endpoint Discover、Network Prevent for Web、Network Prevent for Email、Mobile Prevent for Web 和 Network Protect 提供了一些响应规则操作。

表 37-2 面向所有检测服务器的可用响应规则

响应规则	说明
添加注释	为事件记录添加一个可供补救者在“事件快照”屏幕上对记录进行注释的字段。 请参见第 684 页的“ 配置“添加注释”操作 ”。
限制事件数据保留	丢弃或保留与事件记录匹配的数据。 请参见第 684 页的“ 配置“限制事件数据保留”操作 ”。
记录到 Syslog 服务器	将事件记录到 syslog 服务器。 请参见第 686 页的“ 配置“记录到 Syslog 服务器”操作 ”。
发送电子邮件通知	将您编写的电子邮件发送给指定的接受者。 请参见第 687 页的“ 配置“发送电子邮件通知”操作 ”。
服务器 FlexResponse	执行自定义服务器 FlexResponse 操作。 请参见第 689 页的“ 配置服务器 FlexResponse 操作 ”。 注意： 只有将一个或多个自定义服务器 FlexResponse 插件部署到 Symantec Data Loss Prevention 时，此响应规则操作才可用。 请参见第 968 页的“ 部署服务器 FlexResponse 插件 ”。
设置属性	将自定义值添加到事件记录。 请参见第 690 页的“ 配置“设置属性”操作 ”。

响应规则	说明
设置状态	将事件状态更改为指定值。 请参见第 691 页的“ 配置“设置状态”操作 ”。

请参见第 653 页的“[关于响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

端点检测的响应规则

Symantec Data Loss Prevention 针对 Endpoint Prevent 和 Endpoint Discover 提供了一些响应规则操作。

表 37-3 可用的端点响应规则

响应规则	说明
Endpoint: FlexResponse	使用 FlexResponse API 执行自定义操作。 请参见第 692 页的“ 配置“Endpoint: FlexResponse”操作 ”。
Endpoint Discover: 隔离文件	隔离发现的敏感文件。 请参见第 693 页的“ 配置“Endpoint Discover: 隔离文件”操作 ”。
Endpoint Prevent: 阻止	阻止违反策略的数据的传输。 例如，阻止将机密数据从端点计算机复制到 USB 闪存驱动器。 请参见第 694 页的“ 配置“Endpoint Prevent: 阻止”操作 ”。
Endpoint Prevent: 通知	转移机密数据时，将向端点用户显示屏幕通知。 请参见第 697 页的“ 配置“Endpoint Prevent: 通知”操作 ”。
Endpoint Prevent: 用户取消	允许用户取消机密文件的传输。该覆盖对时间敏感。 请参见第 699 页的“ 配置 Endpoint Prevent: 用户取消操作 ”。

请参见第 653 页的“[关于响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

Network and Mobile Prevent for Web 检测的响应规则

Symantec Data Loss Prevention 针对 Network Prevent for Web、Network Prevent for Email 和 Mobile Prevent for Web 提供了一些响应规则操作。

表 37-4 可用的网络响应规则

响应规则	说明
Network Prevent: 阻止 FTP 请求	阻止 FTP 传输。 请参见第 701 页的“ 配置“Network and Mobile Prevent for Web: 阻止 FTP 请求”操作 ”。 注意: 仅适用于 Network Prevent for Web。
Network Prevent: 阻止 HTTP/S	阻止 Web 发布。 请参见第 702 页的“ 配置“Network and Mobile Prevent for Web: 阻止 HTTP/S”操作 ”。 注意: 仅适用于 Network Prevent for Web。
Network Prevent: 阻止 SMTP 邮件 (仅限 Network Prevent)	阻止导致事件的电子邮件。 请参见第 703 页的“ 配置“Network Prevent: 阻止 SMTP 邮件”操作 ”。 注意: 仅适用于 Network Prevent for Email。
Network Prevent: 修改 SMTP 邮件 (仅限 Network Prevent)	修改敏感电子邮件。 例如，更改电子邮件主题以包括关于违规的信息。 请参见第 704 页的“ 配置“Network Prevent: 修改 SMTP 邮件”操作 ”。 注意: 仅适用于 Network Prevent for Email。
Network Prevent: 删除 HTTP/HTTPS 内容	从 Web 发布中删除机密内容。 请参见第 706 页的“ 配置“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”操作 ”。 注意: 仅适用于 Network Prevent for Web。

请参见第 653 页的“[关于响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

Network Protect 检测的响应规则

Symantec Data Loss Prevention 针对 Network Protect (Discover) 提供了一些响应规则操作。

表 37-5 可用的 Network Protect 响应规则

响应规则	说明
Network Protect: 复制文件	<p>将敏感文件复制到指定位置。</p> <p>请参见第 707 页的“配置“Network Protect: 复制文件”操作”。</p> <p>注意：仅适用于 Network Protect。</p>
Network Protect: 隔离文件	<p>隔离敏感文件。</p> <p>请参见第 708 页的“配置“Network Protect: 隔离文件”操作”。</p> <p>注意：仅适用于 Network Protect。</p>

请参见第 653 页的“[关于响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

分类服务器的响应规则

“对 Enterprise Vault 内容进行分类”响应规则使用分类服务器通过 Enterprise Vault for Microsoft Exchange 自动分类、存档或删除 Exchange 邮件。

注意：此响应规则仅与 Symantec Enterprise Vault 数据分类解决方案一起使用，该解决方案单独从 Symantec Data Loss Prevention 获得许可。您必须配置 Enterprise Vault 数据分类服务过滤器和分类服务器，使其相互通信。有关更多信息，请参见 *Enterprise Vault Data Classification Services Implementation Guide*（《Enterprise Vault 数据分类服务操作指南》）。

表 37-6 可用的分类响应规则

响应规则	说明
分类：对 Enterprise Vault 内容进行分类	定义 Symantec Enterprise Vault for Microsoft Exchange 用于以下用途的分类结果标记和保留类别：针对遵从审阅和 E-Discovery 搜索存档、删除或标记 Exchange 邮件。 分类服务器将保留类别和分类标记传送到已传送邮件供进行检测的 Enterprise Vault 数据分类过滤器。分类标记对应于执行了响应规则的策略的名称。

请参见第 653 页的“[关于响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

关于响应规则执行类型

Symantec Data Loss Prevention 提供了两种类型的策略响应规则：“自动”和“智能”。

用于报告策略违规的检测服务器执行的是“自动”响应规则。包括事件补救者在内的用户可根据需要通过 Enforce Server 管理控制台执行智能响应规则。

请参见第 82 页的“[关于建议的组织角色](#)”。

表 37-7 响应规则类型

响应规则执行类型	说明
自动响应规则	出现策略违规情况时，检测服务器将自动执行响应规则操作。 请参见第 659 页的“ 关于“自动”响应规则 ”。
智能响应规则	出现策略违规情况时，将由授权用户手动触发响应规则。 请参见第 660 页的“ 关于智能响应规则 ”。

请参见第 654 页的“[关于响应规则操作](#)”。

请参见第 664 页的“[实施响应规则](#)”。

关于“自动”响应规则

当检测引擎报告一个策略违规时，系统将执行“自动”响应规则。但如果实施响应规则条件，则必须先满足该条件，然后才能由系统执行响应规则。通过条件，可以控制响应规则操作的自动执行。

请参见第 661 页的“[关于响应规则条件](#)”。

例如，系统可以自动阻止特定的策略违规操作，如尝试传输重要的客户数据或敏感的设计文档。系统也可以将需要即时关注的事件汇报给工作流程管理系统。此外，您还可以对涉及 1000 个客户记录的事件与仅涉及 10 个记录的事件设置不同的严重性等级。

请参见第 664 页的“[实施响应规则](#)”。

关于智能响应规则

用户可以根据需要，通过 Enforce Server 管理控制台的“事件快照”屏幕执行智能响应规则来响应策略违规。

请参见第 654 页的“[关于响应规则操作](#)”。

出现需要人力补救的情况时，您可以创建智能响应规则。例如，可以创建智能响应规则来排除误报事件。事件补救者可以先查看事件，将匹配项确定为误报后即可排除该事件。

请参见第 670 页的“[关于配置智能响应规则](#)”。

只有部分响应规则可供手动执行。

表 37-8 可供手动执行的智能响应规则

智能响应规则	说明
添加注释	为事件记录添加一个可供补救者在“事件快照”屏幕上对记录进行注释的字段。 请参见第 684 页的“ 配置“添加注释”操作 ”。
记录到 Syslog 服务器	将事件记录到 syslog 服务器以便展开工作流程补救。 请参见第 686 页的“ 配置“记录到 Syslog 服务器”操作 ”。
发送电子邮件通知	将您编写的电子邮件发送给指定的接受者。 请参见第 687 页的“ 配置“发送电子邮件通知”操作 ”。
服务器 FlexResponse	执行自定义服务器 FlexResponse 操作。 请参见第 689 页的“ 配置服务器 FlexResponse 操作 ”。 注意： 只有将一个或多个自定义服务器 FlexResponse 插件部署到 Symantec Data Loss Prevention 时，此响应规则操作才可用。 请参见第 968 页的“ 部署服务器 FlexResponse 插件 ”。

智能响应规则	说明
设置状态	将事件状态设置为指定值。 请参见第 691 页的“ 配置“设置状态”操作 ”。

请参见第 664 页的“[实施响应规则](#)”。

关于响应规则条件

响应规则条件是可选的响应规则组件。条件定义了系统触发响应规则操作的方式和时间。条件提供了多种确定传入事件优先级的方式，以便进行重点补救并采取适当的响应。

请参见第 664 页的“[实施响应规则](#)”。

响应规则条件基于检测匹配条件来触发操作。例如，您可以将条件配置为在出现严重性为高的事件的情况下触发操作、在出现特定类型的事件的情况下触发操作，或者在出现指定数量的事件的情况下触发操作。

请参见第 670 页的“[配置响应规则条件](#)”。

条件不是必需的。如果响应规则未声明条件，则每次发生事件时都会执行响应规则操作。如果声明了条件，则必须满足该条件才能触发操作。如果声明了多个条件，则必须满足所有条件，才能由系统执行操作。

请参见第 669 页的“[配置响应规则](#)”。

表 37-9 可用的响应规则条件

条件类型	说明
端点位置	当端点与企业网络连接或断开连接时，触发响应操作。 请参见第 675 页的“ 配置“端点位置”响应条件 ”。
端点设备	在配置的端点设备上发生事件时，触发响应操作。 请参见第 676 页的“ 配置“端点设备”响应条件 ”。
事件类型	当指定类型的检测服务器报告匹配时，触发响应操作。 请参见第 677 页的“ 配置“事件类型”响应条件 ”。
事件匹配数	当策略违规数量超过某个阈值或范围时，触发响应操作。 请参见第 678 页的“ 配置“事件匹配数”响应条件 ”。
协议或端点监控	在指定的网络通信协议（如 HTTP）或端点目标（如 CD/DVD）上检测到事件时，触发响应操作。 请参见第 679 页的“ 配置“协议或端点监视”响应条件 ”。

条件类型	说明
严重性	当策略违规达到某个严重性等级时，触发响应操作。 请参见第 681 页的“ 配置“严重性”响应条件 ”。

关于响应规则操作的执行优先级

Symantec Data Loss Prevention 服务器根据系统定义的优先顺序来执行响应规则操作。不能修改不同类型的响应规则之间的执行顺序。

在所有情况下，当服务器对同一策略执行两项或两项以上不同的响应规则时，较高优先级的响应操作优先。

请注意以下示例：

- 一个端点响应规则允许用户取消复制文件的尝试，而另一个规则则阻止该尝试。
检测服务器将阻止文件复制。
- 一个网络响应规则操作可复制文件，而另一个操作则隔离该文件。
检测服务器将隔离文件。
- 一个网络响应规则操作修改电子邮件的内容，而另一个操作则阻止传输。
检测服务器将阻止电子邮件传输。

您不能更改不同响应规则操作类型的优先执行顺序，但可以修改类型相同但指令相冲突的响应规则操作的执行顺序。

请参见第 673 页的“[修改响应规则排序](#)”。

表 37-10 系统定义的响应规则执行优先级

执行优先级 (从高到低)	说明
Endpoint Prevent: 阻止	请参见第 694 页的“ 配置“Endpoint Prevent: 阻止”操作 ”。
Endpoint Prevent: 用户取消	请参见第 699 页的“ 配置 Endpoint Prevent: 用户取消操作 ”。
Endpoint: FlexResponse	请参见第 692 页的“ 配置“Endpoint: FlexResponse”操作 ”。
Endpoint Prevent: 通知	请参见第 697 页的“ 配置“Endpoint Prevent: 通知”操作 ”。
Endpoint Discover: 隔离文件	请参见第 693 页的“ 配置“Endpoint Discover: 隔离文件”操作 ”。
限制事件数据保留	请参见第 684 页的“ 配置“限制事件数据保留”操作 ”。

执行优先级 (从高到低)	说明
Network Prevent: 阻止 SMTP 邮件	请参见第 703 页的“配置“Network Prevent: 阻止 SMTP 邮件”操作”。
Network Prevent: 修改 SMTP 邮件	请参见第 704 页的“配置“Network Prevent: 修改 SMTP 邮件”操作”。
Network and Mobile Prevent for Web: 删除 HTTP/HTTPS 内容	请参见第 706 页的“配置“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”操作”。
Network and Mobile Prevent for Web: 阻止 HTTP/HTTPS	请参见第 702 页的“配置“Network and Mobile Prevent for Web: 阻止 HTTP/S”操作”。
Network and Mobile Prevent for Web: 阻止 FTP 请求	请参见第 701 页的“配置“Network and Mobile Prevent for Web: 阻止 FTP 请求”操作”。
Network Protect: 隔离文件	请参见第 708 页的“配置“Network Protect: 隔离文件”操作”。
Network Protect: 复制文件	请参见第 707 页的“配置“Network Protect: 复制文件”操作”。
对内容分类	
设置状态	请参见第 691 页的“配置“设置状态”操作”。
设置属性	请参见第 690 页的“配置“设置属性”操作”。
添加注释	请参见第 684 页的“配置“添加注释”操作”。
记录到 Syslog 服务器	请参见第 686 页的“配置“记录到 Syslog 服务器”操作”。
发送电子邮件通知	请参见第 687 页的“配置“发送电子邮件通知”操作”。
服务器 FlexResponse	请参见第 689 页的“配置服务器 FlexResponse 操作”。 注意： 服务器 FlexResponse 操作是自动响应规则的一部分，在 Enforce Server 上执行，而不是在检测服务器上执行。

请参见第 664 页的“实施响应规则”。

请参见第 667 页的“管理响应规则”。

关于响应规则创建权限

要管理和创建响应规则，必须分配具有响应规则创建权限的角色。要向策略添加响应规则，您必须具有策略创建权限。

请参见第 310 页的“[关于策略创建权限](#)”。

由于业务原因，您可能要将响应规则创建权限和策略创建权限授予同一个角色。或者，您可能要使这些角色各自独立。

请参见第 82 页的“[关于建议的组织角色](#)”。

如果以不具有响应规则创建权限的用户登录到系统，“管理” > “策略” > “响应规则” 屏幕将不可用。

请参见第 77 页的“[关于基于角色的访问控制](#)”。

实施响应规则

定义独立于策略的响应规则。

请参见第 653 页的“[关于响应规则](#)”。

必须具有响应规则的创建权限才能创建和管理响应规则。

请参见第 664 页的“[关于响应规则创建权限](#)”。

表 37-11 实施策略响应规则的工作流程

步骤	操作	说明
步骤 1	查看可用的响应规则。	<p>“管理” > “策略” > “响应规则” 屏幕显示了所有配置的响应规则。</p> <p>请参见第 667 页的“管理响应规则”。</p> <p>系统的解决方案软件包提供了配置的响应规则。可以使用策略中现有的这些响应规则，或者可以对其进行修改。</p> <p>请参见第 308 页的“关于解决方案软件包”。</p>
步骤 2	决定要实施的响应规则的类型：智能、自动和两者。	<p>根据企业要求决定响应规则的类型。</p> <p>请参见第 659 页的“关于响应规则执行类型”。</p>
步骤 3	确定要实施的操作的类型和任何触发条件。	<p>请参见第 661 页的“关于响应规则条件”。</p> <p>请参见第 654 页的“关于响应规则操作”。</p>

步骤	操作	说明
步骤 4	了解类型不同和相同的响应规则操作之间的优先顺序。	请参见第 662 页的“ 关于响应规则操作的执行优先级 ”。 请参见第 673 页的“ 修改响应规则排序 ”。
步骤 5	将 Enforce Server 与外部系统集成（如果响应规则需要这样做）。	有些响应规则可能需要与外部系统进行集成。其中包括： <ul style="list-style-type: none">■ 与“记录到 Syslog 服务器”响应规则集成的 SIEM 系统。■ 与“发送电子邮件通知”响应规则集成的 SMTP 电子邮件服务器■ 与 Network Prevent for Web 响应规则集成的 Web 代理主机。■ 与 Network Prevent for Email 响应规则集成的 MTA。
步骤 6	添加新的响应规则。	请参见第 668 页的“ 添加新的响应规则 ”。
步骤 7	配置响应规则。	请参见第 669 页的“ 配置响应规则 ”。
步骤 8	配置一个或多个响应规则条件（可选）。	请参见第 670 页的“ 配置响应规则条件 ”。
步骤 9	配置一个或多个响应规则操作（必需）。	必须为有效的响应规则至少定义一个操作。 请参见第 671 页的“ 配置响应规则操作 ”。 当报告策略违规或响应规则条件匹配时会执行操作。
步骤 10	向策略添加响应规则。	必须具有策略创建权限才能将响应规则添加到策略。 请参见第 352 页的“ 向策略添加自动响应规则 ”。

响应规则最佳做法

在实施响应规则时，请注意以下事项：

- 响应规则不是策略执行所必需的。通常，最好在实施响应规则之前实施和微调您的策略规则和例外。在获得所需的策略检测结果后，可以实施和完善响应规则。
- 响应规则需要至少一个规则操作；条件为可选。如果不实施条件，则在某个事件被报告出来时，系统会始终执行相关操作。如果配置多个响应规则条件，则必须在所有条件都匹配的情况下，才能触发响应规则操作。

请参见第 654 页的“[关于响应规则操作](#)”。

- 响应规则条件派生自策略规则。在配置响应规则条件时，请了解策略所实施的规则类型和例外条件。系统可根据策略规则的匹配计数方式来评估响应规则条件。
请参见第 290 页的“[检测规则简介](#)”。
- 在策略作者向策略添加响应规则时，系统仅显示响应规则名称供其选择。请确保提供一个便于策略作者识别响应规则用途的说明性名称。
请参见第 330 页的“[配置策略](#)”。
- 不能将“Endpoint Prevent: 通知”或“Endpoint Prevent: 阻止”响应规则操作与 EDM、IDM 或 DGM 检测方法组合在一起。如果您这样做，系统将显示一条指出策略配置有误的警告。
请参见第 347 页的“[管理和添加策略](#)”。
- 如果在单个策略中组合多个响应规则，请确保您了解响应规则之间的优先顺序。
请参见第 662 页的“[关于响应规则操作的执行优先级](#)”。
- 仅将智能响应规则用于适合人工干预的情形。
请参见第 670 页的“[关于配置智能响应规则](#)”。

配置和管理响应规则

本章节包括下列主题：

- [管理响应规则](#)
- [添加新的响应规则](#)
- [配置响应规则](#)
- [关于配置智能响应规则](#)
- [配置响应规则条件](#)
- [配置响应规则操作](#)
- [修改响应规则排序](#)
- [关于删除响应规则](#)

管理响应规则

“管理” > “策略” > “响应规则” 屏幕是管理响应规则的主页面，也是添加新响应规则的起点。

请参见第 653 页的“[关于响应规则](#)”。

您必须具有响应规则的创建权限，才能管理和添加响应规则。

请参见第 664 页的“[关于响应规则创建权限](#)”。

表 38-1 “响应规则” 屏幕的操作

操作	说明
添加响应规则	单击“添加响应规则”以定义新的响应规则。 请参见第 668 页的“ 添加新的响应规则 ”。

操作	说明
修改响应规则顺序	单击“修改响应规则顺序”修改响应规则的优先顺序。 请参见第 673 页的“ 修改响应规则排序 ”。
编辑现有响应规则	单击响应规则可以对其进行修改。 请参见第 669 页的“ 配置响应规则 ”。
删除现有响应规则	单击响应规则最右侧的红色 X 号图标可以删除响应规则。 删除之前必须确认该操作。 请参见第 674 页的“ 关于删除响应规则 ”。
刷新列表	单击“响应规则”屏幕右上方的刷新箭头图标，可以获取规则的最新状态。

表 38-2 “响应规则”屏幕的显示内容

显示列	说明
顺序	当配置了多个响应规则时，规则的优先级“顺序”。 请参见第 673 页的“ 修改响应规则排序 ”。
规则	响应规则的“名称”。 请参见第 669 页的“ 配置响应规则 ”。
操作	响应规则在响应事件时可采取的“操作”的类型（必需）。 请参见第 671 页的“ 配置响应规则操作 ”。
条件	触发响应规则的“条件”（如果有）。 请参见第 670 页的“ 配置响应规则条件 ”。

请参见第 664 页的“[实施响应规则](#)”。

添加新的响应规则

可以从“管理”>“策略”>“响应规则”>“新建响应规则”屏幕添加新的响应规则。

请参见第 653 页的“[关于响应规则](#)”。

添加新响应规则

- 1 在“管理”>“策略”>“响应规则”屏幕上单击“添加响应规则”。
请参见第 667 页的[“管理响应规则”](#)。
- 2 在“新建响应规则”屏幕上，选择以下选项之一：
 - **自动响应**
当服务器评估事件时，系统会自动执行响应操作（默认选项）。
请参见第 659 页的[“关于‘自动’响应规则”](#)。
 - **智能响应**
授权用户可从 Enforce Server 管理控制台的“事件快照”屏幕上执行响应操作。
请参见第 660 页的[“关于智能响应规则”](#)。
- 3 单击“下一步”以配置响应规则。
请参见第 669 页的[“配置响应规则”](#)。
请参见第 664 页的[“实施响应规则”](#)。

配置响应规则

可以在“管理”>“策略”>“响应规则”>“配置响应规则”屏幕上配置响应规则。
请参见第 653 页的[“关于响应规则”](#)。

配置响应规则

- 1 添加新的响应规则，或修改现有的响应规则。
请参见第 668 页的[“添加新的响应规则”](#)。
请参见第 667 页的[“管理响应规则”](#)。
- 2 输入响应的“规则名称”和“说明”。
3 或者，定义一个或多个“条件”来指明响应规则执行的时间。
请参见第 670 页的[“配置响应规则条件”](#)。
如果未声明条件，则出现匹配时始终执行响应规则操作（假设设置了相同的检测规则）。
如果选择了“智能响应”规则选项，则跳过此步骤。
请参见第 670 页的[“关于配置智能响应规则”](#)。

4 选择并配置一个或多个“操作”。必须至少定义一个操作。

请参见第 671 页的“[配置响应规则操作](#)”。

5 单击“保存”以保存响应规则定义。

请参见第 667 页的“[管理响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

关于配置智能响应规则

实施智能响应规则时，请注意以下情况：

- 智能响应规则最适合于授权用户查看以确定是否需要任何响应操作的事件。
如果不希望用户介入触发响应规则操作，请改用自动响应规则。
- 不能使用智能响应规则配置任何触发条件。
授权用户决定何时检测事件授权响应。
- 只能执行可以通过智能响应规则执行的操作（注释、日志、电子邮件和状态）。
如果需要阻止或修改操作，请使用自动响应规则。

请参见第 660 页的“[关于智能响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

配置响应规则条件

您可以向响应规则添加一个或多个条件。事件必须满足所有响应规则条件，系统才能执行相应的响应规则操作。

请参见第 661 页的“[关于响应规则条件](#)”。

配置响应规则条件

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

2 单击“添加条件”添加新的条件。

条件是可选的，且基于检测规则的匹配。每种类型的响应规则条件执行不同的功能。

请参见第 661 页的“[关于响应规则条件](#)”。

- 3 从“条件”列表中选择条件类型。

请参见第 661 页的[表 37-9](#)。

例如，选择“事件匹配数”条件和“大于”，然后在文本框中输入**15**。该条件会在出现 15 个策略违规匹配项后触发响应规则操作。

- 4 要添加其他条件，请单击“添加条件”并重复以上过程。

如果所有条件都不匹配，则不执行操作。

- 5 单击“保存”保存条件。

单击“取消”将不保存条件，并返回之前的屏幕。

单击条件旁边的红色**X**号图标将从响应规则中删除该条件。

请参见第 667 页的[“管理响应规则”](#)。

请参见第 664 页的[“实施响应规则”](#)。

配置响应规则操作

您必须为响应规则配置至少一个操作才能使之有效。您可以配置多个响应规则操作。每个操作会单独接受评估。

请参见第 664 页的[“实施响应规则”](#)。

定义响应规则操作

- 1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

- 2 从“操作”列表中选择操作类型，然后单击“添加操作”。

例如，将“所有:添加注释”操作添加到响应规则中。此操作使补救者能够为事件添加注释。

- 3 为所选操作类型指定期望的参数，配置操作类型。

请参见第 672 页的[表 38-3](#)。

- 4 对每个要添加的操作重复执行这些步骤。

如果添加其他操作，请考虑相似类型操作的执行顺序和可能的修改。

请参见第 673 页的[“修改响应规则排序”](#)。

- 5 单击“保存”保存响应规则。

请参见第 667 页的[“管理响应规则”](#)。

表 38-3 配置响应规则操作

事件类型	响应规则	说明
所有	添加注释	请参见第 684 页的 “配置“添加注释”操作” 。
所有	限制事件数据保留	请参见第 684 页的 “配置“限制事件数据保留”操作” 。
所有	记录到 Syslog 服务器	请参见第 686 页的 “配置“记录到 Syslog 服务器”操作” 。
所有	发送电子邮件通知	请参见第 687 页的 “配置“发送电子邮件通知”操作” 。
所有	服务器 FlexResponse	请参见第 689 页的 “配置服务器 FlexResponse 操作” 。
所有	设置属性	请参见第 690 页的 “配置“设置属性”操作” 。
所有	设置状态	请参见第 691 页的 “配置“设置状态”操作” 。
分类	对 Enterprise Vault 内容进行分类	
端点	FlexResponse	请参见第 692 页的 “配置“Endpoint: FlexResponse”操作” 。
Endpoint Discover	隔离文件	请参见第 693 页的 “配置“Endpoint Discover: 隔离文件”操作” 。
Endpoint Prevent	阻止	请参见第 694 页的 “配置“Endpoint Prevent: 阻止”操作” 。
Endpoint Prevent	通知	请参见第 697 页的 “配置“Endpoint Prevent: 通知”操作” 。
Endpoint Prevent	用户取消	请参见第 699 页的 “配置 Endpoint Prevent: 用户取消操作” 。
Network and Mobile Prevent for Web	阻止 FTP 请求	请参见第 701 页的 “配置“Network and Mobile Prevent for Web: 阻止 FTP 请求”操作” 。
Network and Mobile Prevent for Web	阻止 HTTP/S	请参见第 702 页的 “配置“Network and Mobile Prevent for Web: 阻止 HTTP/S”操作” 。
Network Prevent for Email	阻止 SMTP 邮件	请参见第 703 页的 “配置“Network Prevent: 阻止 SMTP 邮件”操作” 。
Network Prevent for Email	修改 SMTP 邮件	请参见第 704 页的 “配置“Network Prevent: 修改 SMTP 邮件”操作” 。
Network and Mobile Prevent for Web	删除 HTTP/S 内容	请参见第 706 页的 “配置“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”操作” 。
Network Protect	复制文件	请参见第 707 页的 “配置“Network Protect: 复制文件”操作” 。

事件类型	响应规则	说明
Network Protect	隔离文件	请参见第 708 页的“ 配置“Network Protect: 隔离文件”操作 ”。

请参见第 664 页的“[实施响应规则](#)”。

修改响应规则排序

您无法更改系统为不同类型的响应规则操作定义的执行优先级，但却可以修改类型相同、但指令存在冲突的响应规则操作之间的执行顺序。

请参见第 662 页的“[关于响应规则操作的执行优先级](#)”。

例如，请设想这样一种情形，一个策略中包含两个响应规则。每个响应规则实施一个“限制事件数据保留”操作。其中一个操作丢弃所有附件，而另一个操作仅丢弃那些非违规附件。在这种情况下，当违反策略时，检测服务器会查看响应规则的优先顺序，以确定优先执行哪个操作。这种类型的排序是可配置的。

修改响应规则操作排序

1 导航到“管理”>“策略”>“响应规则”屏幕。

请参见第 667 页的“[管理响应规则](#)”。

2 注意“顺序”列和每个配置的响应规则旁边的数字。

默认情况下，系统会按“顺序”列以降序方式从最高优先级(1)到最低优先级对响应规则列表进行排序。最初，系统按响应规则的创建顺序对其进行排序。您可以修改此顺序。

3 要启用修改模式，请单击“修改响应规则顺序”。

这时，“顺序”列会显示每个响应规则的下拉菜单。

4 要为每个需要重新排序的响应规则修改排序，请从下拉菜单选择所需的顺序优先级。

例如，对于顺序优先级为 2 的响应规则，可以将其修改为 1 (最高优先级)。

修改顺序号后，会将该响应规则移至修改后应在列表中所处的位置，并更新所有其他响应规则。

5 单击“保存”保存对响应规则排序所做的修改。

6 根据需要重复这些步骤以获得所需的结果。

请参见第 664 页的“[实施响应规则](#)”。

关于删除响应规则

可以在“管理”>“策略”>“响应规则”屏幕上删除响应规则。

请参见第 667 页的[“管理响应规则”](#)。

删除响应规则时，请注意以下事项：

- 用户必须具有响应规则创建权限才能删除现有的响应规则。
- 响应规则作者不能在其他用户修改现有的响应规则时删除该规则。
- 如果策略声明某个响应规则，则该响应规则的作者不能删除该响应规则。在这种情况下，必须先从声明响应规则的所有策略中删除该响应规则，才能删除它。

响应规则条件

本章节包括下列主题：

- 配置“端点位置”响应条件
- 配置“端点设备”响应条件
- 配置“事件类型”响应条件
- 配置“事件匹配数”响应条件
- 配置“协议或端点监视”响应条件
- 配置“严重性”响应条件

配置“端点位置”响应条件

出现违反端点策略的情况时，“端点位置”条件可根据DLP Agent的连接状态来触发响应规则操作。

请参见第 661 页的[“关于响应规则条件”](#)。

注意：此条件特定于端点事件。不应对“网络”事件或“发现”事件实施此条件。如果这样做，则响应规则操作不会执行。

配置“端点位置”条件

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

2 从“条件”列表中选择“端点位置”条件。

请参见第 670 页的[“配置响应规则条件”](#)。

3 选择触发操作所需的端点位置要求。

请参见第 676 页的[表 39-1](#)。

表 39-1 “端点位置”条件选项

限定符	条件	说明
为任一	在企业网络外	如果在端点与企业网络断开连接时发生某个事件，则此组合将触发响应规则操作。
都不是	在企业网络外	如果在端点与企业网络断开连接时发生某个事件，则此组合不会触发响应规则操作。
为任一	在企业网络内	如果在端点与企业网络处于连接状态时发生某个事件，则此组合将触发响应规则操作。
都不是	在企业网络内	如果在端点与企业网络处于连接状态时发生某个事件，则此组合不会触发响应规则操作。

请参见第 664 页的[“实施响应规则”](#)。

请参见第 667 页的[“管理响应规则”](#)。

配置“端点设备”响应条件

从一个或多个配置的端点设备检测到事件时，“端点设备”条件将触发响应规则操作。

请参见第 661 页的[“关于响应规则条件”](#)。

可以在“系统”>“代理”>“端点设备”屏幕上配置端点设备。

请参见第 470 页的[“关于端点设备检测”](#)。

注意：此条件特定于端点事件。不应对“网络”事件或“发现”事件实施此条件。如果这样做，则响应规则操作不会执行。

配置“端点设备”响应条件

- 1 在“配置响应规则”屏幕上配置响应规则。
请参见第 669 页的[“配置响应规则”](#)。
- 2 从“条件”列表中选择“端点设备”条件。
请参见第 670 页的[“配置响应规则条件”](#)。
- 3 选择检测或排除特定的端点设备。
请参见第 677 页的[表 39-2](#)。

表 39-2 “端点设备”条件参数

限定符	条件	说明
为任一	已配置的设备	在配置的端点设备上检测到事件时，触发响应规则操作。
都不是	已配置的设备	在配置的端点设备上检测到事件时，不触发（排除在执行之外）响应规则操作。

请参见第 664 页的[“实施响应规则”](#)。

请参见第 667 页的[“管理响应规则”](#)。

配置“事件类型”响应条件

“事件类型”条件可根据报告事件用的检测服务器的类型来触发响应规则操作。

请参见第 661 页的[“关于响应规则条件”](#)。

配置“事件类型”条件

- 1 在“配置响应规则”屏幕上配置响应规则。
请参见第 669 页的[“配置响应规则”](#)。
- 2 从“条件”列表中选择“事件类型”条件。
请参见第 670 页的[“配置响应规则条件”](#)。
- 3 选择一个或多个事件类型。
使用 `Ctrl` 键选择多个类型。
请参见第 678 页的[表 39-3](#)。

表 39-3 “事件类型” 条件参数

参数	服务器	说明
为任一	分类	不管分类服务器检测到何种事件，都会触发响应规则操作。
都不是		不管分类服务器检测到何种事件，都不触发响应规则操作。
为任一	发现	不管 Network Discover 检测到何种事件，都会触发响应规则操作。
都不是		不管 Network Discover 检测到何种事件，都不触发响应规则操作。
为任一	端点	不管 Endpoint Prevent 检测到何种事件，都会触发响应规则操作。
都不是		不管 Endpoint Prevent 检测到何种事件，都不触发响应规则操作。
为任一	网络或移动	不管 Network Prevent 检测到何种事件，都会触发响应规则操作。
都不是		不管 Network Prevent 检测到何种事件，都不触发响应规则操作。

请参见第 664 页的“[实施响应规则](#)”。

请参见第 667 页的“[管理响应规则](#)”。

配置“事件匹配数”响应条件

“事件匹配数”条件可根据已报告的策略违规数来触发响应规则操作。

请参见第 661 页的“[关于响应规则条件](#)”。

配置“事件匹配数”条件

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

2 从“条件”列表中选择“事件匹配数”条件。

请参见第 670 页的“[配置响应规则条件](#)”。

3 在文本字段中，请输入表示阈值（超过其值即触发响应规则）的数值。

例如，如果您输入 15，则响应规则会在检测到 15 个策略违规后触发。

请参见第 679 页的[表 39-4](#)。

表 39-4 “事件匹配数” 条件选项

参数	输入	说明
大于	用户指定的数	如果超过事件数的阈值，则会触发响应规则操作。
大于或等于	用户指定的数	如果满足或超过事件数的阈值，则会触发响应规则操作。
在两者之间	用户指定的数值对	当事件数处于指定的数值范围内时，则会触发响应规则操作。
小于	用户指定的数	如果事件数小于指定的数值，则会触发响应规则操作。
小于或等于	用户指定的数	当事件数等于或小于指定的数值时，则会触发响应规则操作。

请参见第 664 页的“[实施响应规则](#)”。

请参见第 667 页的“[管理响应规则](#)”。

配置“协议或端点监视”响应条件

“协议或端点监视”条件可根据发生策略违规的协议或端点目标、设备或者应用程序来触发操作。

请参见第 661 页的“[关于响应规则条件](#)”。

配置“协议或端点监视”条件

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

2 从“条件”列表中选择“协议或端点监视”条件。

请参见第 670 页的“[配置响应规则条件](#)”。

3 使用 Ctrl 键选择多个项，或使用 Shift 键选择一个范围。

请参见第 679 页的表 39-5。

系统会列出在“系统”>“设置”>“协议”屏幕上配置的任何其他网络协议。

表 39-5 “协议或端点目标” 条件选项

限定符	条件	说明
为任一	端点应用程序文件访问	如果已访问端点应用程序文件，则会触发操作。
都不是		如果已访问端点应用程序文件，则不会触发操作。

限定符	条件	说明
为任一	端点 CD/DVD	如果已写入端点 CD/DVD，则会触发操作。
都不是		如果已写入端点 CD/DVD，则不会触发操作。
为任一	端点剪贴板	如果已复制到端点剪贴板，则会触发操作。
都不是		如果已复制到端点剪贴板，则不会触发操作。
为任一	从端点复制到网络共享	如果敏感信息已复制到网络共享或从网络共享进行复制，则会触发操作。
都不是		如果敏感信息已复制到网络共享或从网络共享进行复制，则不会触发操作。
为任一	端点本地驱动器	如果在本地驱动器上发现敏感文件，则会触发操作。
都不是		如果在本地驱动器上发现敏感文件，则不会触发操作。
为任一	端点打印机/传真机	如果已发送到端点打印机或传真机，则会触发操作。
都不是		如果已发送到端点打印机或传真机，则不会触发操作。
为任一	端点可移动存储设备	如果敏感数据已复制到可移动存储设备，则会触发操作。
都不是		如果敏感数据已复制到可移动存储设备，则不会触发操作。
为任一	FTP	如果通过 FTP 复制敏感数据，则会触发操作。
都不是		如果通过 FTP 复制敏感数据，则不会触发操作。
为任一	HTTP	如果通过 HTTP 发送敏感数据，则会触发操作。
都不是		如果通过 HTTP 发送敏感数据，则不会触发操作。
为任一	HTTPS	如果通过 HTTPS 发送敏感数据，则会触发操作。
都不是		如果通过 HTTPS 发送敏感数据，则不会触发操作。
为任一	IM:AIM	如果通过 AIM 发送敏感数据，则会触发操作。
都不是		如果通过 AIM 发送敏感数据，则不会触发操作。
为任一	IM:MSN	如果通过 MSN 发送敏感数据，则会触发操作。
都不是		如果通过 MSN 发送敏感数据，则不会触发操作。
为任一	IM:Yahoo	如果通过 Yahoo IM 发送敏感数据，则会触发操作。
都不是		如果通过 Yahoo IM 发送敏感数据，则不会触发操作。

限定符	条件	说明
为任一	NNTP	如果通过 NNTP 发送敏感数据，则会触发操作。
都不是		如果通过 NNTP 发送敏感数据，则不会触发操作。
为任一	SMTP	如果通过 SMTP 发送敏感数据，则会触发操作。
都不是		如果通过 SMTP 发送敏感数据，则不会触发操作。

请参见第 664 页的[“实施响应规则”](#)。

请参见第 667 页的[“管理响应规则”](#)。

配置“严重性”响应条件

“严重性”条件会根据策略违规的严重性来触发响应规则操作。

请参见第 661 页的[“关于响应规则条件”](#)。

配置“严重性”条件

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

2 从“条件”列表中选择“严重性”条件。

请参见第 670 页的[“配置响应规则条件”](#)。

3 选择一个或多个严重性等级。

使用 Ctrl 键选择多个项；使用 Shift 键选择一个范围。

请参见第 681 页的[表 39-6](#)。

表 39-6 “严重性”条件匹配

参数	严重性	说明
为任一	高	与严重性设置为“高”的检测规则相匹配时，将会触发响应规则操作。
都不是	高	与严重性设置为“高”的检测规则相匹配时，不会触发响应规则操作。
为任一	中	与严重性设置为“中”的检测规则相匹配时，将会触发响应规则操作。

参数	严重性	说明
都不是	中	与严重性设置为“中”的检测规则相匹配时，不会触发响应规则操作。
为任一	低	与严重性设置为“低”的检测规则相匹配时，将会触发响应规则操作。
都不是	低	与严重性设置为“低”的检测规则相匹配时，不会触发响应规则操作。
为任一	信息	与严重性设置为“信息”的检测规则相匹配时，将会触发响应规则操作。
都不是	信息	与严重性设置为“信息”的检测规则相匹配时，不会触发响应规则操作。

请参见第 664 页的[“实施响应规则”](#)。

请参见第 667 页的[“管理响应规则”](#)。

响应规则操作

本章节包括下列主题：

- 配置“添加注释”操作
- 配置“限制事件数据保留”操作
- 配置“记录到 Syslog 服务器”操作
- 配置“发送电子邮件通知”操作
- 配置服务器 FlexResponse 操作
- 配置“设置属性”操作
- 配置“设置状态”操作
- 配置“Endpoint: FlexResponse”操作
- 配置“Endpoint Discover: 隔离文件”操作
- 配置“Endpoint Prevent: 阻止”操作
- 配置“Endpoint Prevent: 通知”操作
- 配置 Endpoint Prevent: 用户取消操作
- 配置“Network and Mobile Prevent for Web: 阻止 FTP 请求”操作
- 配置“Network and Mobile Prevent for Web: 阻止 HTTP/S”操作
- 配置“Network Prevent: 阻止 SMTP 邮件”操作
- 配置“Network Prevent: 修改 SMTP 邮件”操作
- 配置“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”操作
- 配置“Network Protect: 复制文件”操作

■ 配置“Network Protect: 隔离文件”操作

配置“添加注释”操作

“添加注释”响应规则操作允许事件响应人员输入有关特定事件的注释。例如，如果发生策略违规，系统将向事件响应人员显示响应人员可以添加注释的“注释”对话框。

请参见第 654 页的“[关于响应规则操作](#)”。

“添加注释”响应规则操作可用于所有类型的检测服务器。

请参见第 655 页的“[所有检测服务器的响应规则](#)”。

配置“添加注释”操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

2 从“操作”列表中添加“所有:添加注释”操作类型。

此时系统将显示“注释”字段。通常，将此字段留空，并允许补救者在评估事件时添加注释。但是，也可以在此配置级别上添加注释。

请参见第 671 页的“[配置响应规则操作](#)”。

3 单击“保存”保存配置。

请参见第 667 页的“[管理响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

配置“限制事件数据保留”操作

“限制事件数据保留”响应规则操作允许您修改检测服务器的默认事件数据保留行为。

请参见第 654 页的“[关于响应规则操作](#)”。

此响应规则可用于所有类型的检测服务器。

请参见第 655 页的“[所有检测服务器的响应规则](#)”。

配置事件数据保留

- 1 在“配置响应规则”屏幕上配置响应规则。
请参见第 669 页的[“配置响应规则”](#)。
- 2 从“操作”列表中添加操作类型“所有: 限制事件数据保留”。
请参见第 671 页的[“配置响应规则操作”](#)。
- 3 通过选择此选项来选择保留端点事件数据。
默认情况下，代理会丢弃有关端点事件的原始邮件和所有附件。
请参见第 685 页的[“保留端点事件的数据”](#)。
- 4 通过选择此选项来选择丢弃网络事件数据。
默认情况下，系统会保留有关网络事件的原始邮件和所有附件。
请参见第 686 页的[“丢弃网络事件的数据”](#)。
- 5 单击“保存”以保存响应规则配置。
请参见第 667 页的[“管理响应规则”](#)。
请参见第 664 页的[“实施响应规则”](#)。

保留端点事件的数据

默认情况下，系统会丢弃端点事件的原始文件（包括文件和附件）。可以实施限制事件数据保留响应规则操作以覆盖此默认行为并保留端点事件的原始邮件。

请参见第 684 页的[“配置“限制事件数据保留”操作”](#)。

表 40-1 保留端点事件的数据

参数	说明
所有端点事件 (包括 Endpoint Discover 事件)	选中此选项可以为所有 Endpoint Prevent 事件和 Endpoint Discover 使用端点目标捕获的事件保留原始邮件和文件附件。

如果在端点上将服务器端检测规则(EDM/IDM/DGM)和限制事件数据保留响应规则操作组合，请考虑网络带宽影响。当端点代理将内容发送至 Endpoint Server 进行分析时，它会根据检测要求发送文本数据或二进制数据。如果情况许可，Symantec DLP 代理会发送文本以减少带宽使用。保留端点事件的原始邮件时，系统会要求代理在任何情况下都将二进制数据发送到 Endpoint Server。这样一来，请确保网络能够在不降低性能的情况下处理端点代理和 Endpoint Server 之间增加的流量。

请考虑组合代理端检测规则（任何 DCM 规则，如关键字规则）的任何策略的系统行为。如果实施限制事件数据保留响应规则操作，带宽使用的增长情况取决于检测

引擎匹配的事件的数量。对于这些策略，端点代理不是将所有原始文件发送至 Endpoint Server，而是仅发送与确认的事件关联的原始事件。如果事件数量不多，则影响不大。

丢弃网络事件的数据

对于网络事件，默认情况下检测服务器保留触发事件的原始邮件和所有附件。

您可以实施限制事件数据保留响应规则操作以覆盖默认行为并丢弃原始邮件以及一些或所有附件。

请参见第 684 页的[“配置“限制事件数据保留”操作”](#)。

注意：网络事件的默认数据保留行为适用于 Network Prevent for Web 和 Network Prevent for Email 事件。该默认行为不适用于 Network Protect (Discover) 事件。对于 Network Discover 事件，系统在“事件快照”中提供指向违规文件原始位置的链接。Network Discover 的事件数据保留是不可配置的。

表 40-2 丢弃网络事件的数据

参数	说明
丢弃原始邮件	选中此选项可丢弃原始邮件。 当您只关心统计数据时，使用此配置可节省磁盘空间。
丢弃附件	选择“所有”可丢弃所有邮件附件。 选择“没有违规的附件”可仅保存相关邮件附件，即那些没有触发策略违规的邮件。 注意： 您必须为此操作选项选择“无”之外的选项。如果您选择了“无”且未选中“丢弃原始邮件”旁边的框，则此操作不会产生任何效果。这样的配置可复制网络服务器的默认事件数据保留行为。

配置“记录到 Syslog 服务器”操作

“记录到 Syslog 服务器”响应规则操作会将事件记录到 Syslog 服务器。如果使用安全信息和事件管理 (SIEM) 系统，则这些日志非常有用。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则操作可用于所有类型的检测服务器。

请参见第 655 页的[“所有检测服务器的响应规则”](#)。

必须将 Enforce Server 与 Syslog 服务器集成，才能实施此响应规则操作。

请参见第 134 页的“[启用 Syslog 服务器](#)”。

配置“记录到 Syslog 服务器”响应规则操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

2 从“操作”列表中添加“记录到 Syslog 服务器”操作类型。

请参见第 671 页的“[配置响应规则操作](#)”。

3 输入 Syslog 服务器的“主机”名称。

4 编辑 Syslog 服务器的“端口”（如有必要）。

默认端口为 **514**。

5 输入要记录在 Syslog 服务器上的“消息”文本。

6 从下拉列表中选择要应用至日志消息的“级别”。

提供以下选项：

- 0 - 内核严重错误
- 1 - 需要立即注意
- 2 - 严重情况
- 3 - 错误
- 4 - 警告
- 5 - 可能需要注意
- 6 - 信息
- 7 - 调试

7 “保存”响应规则。

请参见第 667 页的“[管理响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

配置“发送电子邮件通知”操作

“发送电子邮件通知”操作可向指定的接受者发送您撰写的电子邮件。

请参见第 654 页的“[关于响应规则操作](#)”。

此响应规则操作可用于所有类型的检测服务器。

请参见第 655 页的“[所有检测服务器的响应规则](#)”。

必须将 Enforce Server 与 SMTP 电子邮件服务器集成，才能实施此响应规则操作。

请参见第 135 页的“[配置 Enforce Server 以发送电子邮件警报](#)”。

配置“发送电子邮件通知”响应规则操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

2 从“操作”列表中添加“所有:发送电子邮件通知”操作类型。

请参见第 671 页的“[配置响应规则操作](#)”。

3 配置接受者、发送者、格式、事件包括的内容和每天邮件数。

请参见第 688 页的[表 40-3](#)。

4 配置电子邮件通知的“通知内容”：语言、主题、正文。

请参见第 689 页的[表 40-4](#)。

5 单击“保存”保存配置。

请参见第 667 页的“[管理响应规则](#)”。

表 40-3 发送者和接受者信息

参数	说明
收件人: 发送者	选择此选项可将电子邮件通知发送到电子邮件发送者。此接受者仅适用于电子邮件违规。
收件人: 数据所有者	选择此选项可将电子邮件通知发送到系统根据事件中电子邮件来识别的数据所有者。 请参见第 760 页的“ 发现事件快照 ”。
收件人: 其他电子邮件地址	此选项可以包括指定为电子邮件地址的所有自定义属性（例如 manager@email）。例如，如果您定义的自定义属性为电子邮件地址，或者通过查找插件检索一个自定义属性，则该地址将显示在可供选择的“收件人”字段中，以及“收件人: 发送者”和“收件人: 数据所有者”右侧。 请参见第 835 页的“ 配置自定义属性 ”。
自定义收件人	输入一个或多个以逗号分隔的特定电子邮件地址。
抄送	针对您想要抄送通知的收件人，输入一个或多个以逗号分隔的特定电子邮件地址。
自定义发件人	您可以指定邮件的发送者。 如果此字段为空，则邮件似乎来自系统电子邮件地址。

参数	说明
通知格式	选择 HTML 格式或纯文本格式。
包括原始邮件	选择此选项可包括生成具有电子邮件通知的事件的邮件。
每天最大值	输入一个数字以限制一天内系统发送的最大通知数。

表 40-4 通知内容

参数	说明
语言	从下拉菜单中，选择邮件使用的语言。
添加语言	单击该图标可为邮件添加多种语言。 请参见第 1153 页的“ 关于不同区域设置中的 Endpoint Prevent 响应规则 ”。
主题	输入简要说明邮件内容的邮件主题。
正文	输入邮件的正文。
插入变量	通过从“插入变量”列表中选择所需值，可以将一个或多个变量添加到电子邮件的主题或正文。 变量可以用于将文件名、策略名、接受者和发送者包括在电子邮件的主题和正文中。例如，要包括违反的策略和规则，请插入以下变量。 邮件违反了 \$POLICY\$ 中的以下规则：\$RULES\$

请参见第 664 页的“[实施响应规则](#)”。

配置服务器 FlexResponse 操作

通过“所有:服务器FlexResponse”操作，可以使用自定义服务器端FlexResponse 插件补救任何事件类型。可以为自动响应规则或智能响应规则配置服务器 FlexResponse 响应操作。

只有在您已授权了 Network Protect 并已将一个或多个服务器 FlexResponse 插件部署到 Symantec Data Loss Prevention 时，“所有:服务器 FlexResponse”操作才可用。

请参见第 968 页的“[部署服务器 FlexResponse 插件](#)”。

如果要部署 Python Script Bridge 这一服务器 FlexResponse 插件以实现一个用 Python 脚本编写语言编写的自定义插件，那么还需要执行其他一些步骤来配置此插件。请参见第 976 页的“[部署 Python Script Bridge 服务器 FlexResponse 插件](#)”。

配置服务器 FlexResponse 操作

- 1 登录到 Enforce Server 管理控制台。
- 2 为每个自定义服务器 FlexResponse 插件创建一个新的响应规则。
 - 单击“管理”>“策略”>“响应规则”。
- 3 单击“添加响应规则”。
- 4 选择“自动响应”或“智能响应”。单击“下一步”。
- 5 在“规则名称”字段中输入规则的名称。（对于智能响应规则，此名称显示在补救期间事件响应人员选择的按钮上作为标签。）
- 6 在“说明”字段中输入规则的可选说明。
- 7 在“操作(按显示顺序执行)”菜单中，选择“所有:服务器 FlexResponse”操作。
- 8 单击“添加操作”。
- 9 在“FlexResponse 插件”菜单中，选择要随此响应规则操作执行的已部署的服务器 FlexResponse 插件。

此下拉菜单中显示的名称是在配置属性文件或插件元数据类的 `display-name` 属性中指定的值。

请参见第 968 页的[“部署服务器 FlexResponse 插件”](#)。
- 10 单击“保存”。
- 11 重复此过程，为您部署的所有其他服务器 FlexResponse 插件添加响应规则。

配置“设置属性”操作

“设置属性”响应规则操作可将事件状态设置为指定值。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则操作可用于所有的检测服务器。

请参见第 655 页的[“所有检测服务器的响应规则”](#)。

“设置属性”操作基于在“系统”>“事件数据”>“属性”屏幕上定义的自定义属性。

请参见第 833 页的[“关于自定义属性”](#)。

配置“设置属性”操作

- 1 在“配置响应规则”屏幕上配置响应规则。
请参见第 669 页的[“配置响应规则”](#)。
- 2 从“操作”列表中添加“所有:设置属性”操作类型。
请参见第 671 页的[“配置响应规则操作”](#)。
- 3 从下拉列表中选择“属性”（如果定义了多个自定义属性）。
- 4 为选定的自定义属性输入事件状态“值”。
5 单击“保存”保存配置。
请参见第 667 页的[“管理响应规则”](#)。
请参见第 664 页的[“实施响应规则”](#)。

配置“设置状态”操作

“设置状态”响应规则操作可将事件状态设置为指定值。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则适用于所有检测服务器。

请参见第 655 页的[“所有检测服务器的响应规则”](#)。

此响应规则操作基于您在“系统”>“事件数据”>“属性”屏幕上配置的事件“状态值”。

请参见第 827 页的[“关于事件状态属性”](#)。

配置“设置状态”响应规则操作

- 1 在“配置响应规则”屏幕上配置响应规则。
请参见第 669 页的[“配置响应规则”](#)。
- 2 从“操作”列表中添加“所有:设置状态”操作类型。
- 3 请参见第 671 页的[“配置响应规则操作”](#)。
- 4 从列表中选择要分配给事件的“状态”。

以下是一些您可以从中进行配置和选择的事件状态示例：

- 新建
- 已提报
- 调查

- 已解决
- 已排除

5 单击“保存”保存配置。

请参见第 667 页的[“管理响应规则”](#)。

请参见第 664 页的[“实施响应规则”](#)。

配置“Endpoint: FlexResponse”操作

通过“Endpoint: FlexResponse”响应规则操作，您可以使用FlexResponse API实现一个或多个已开发的自定义响应。

请参见第 1163 页的[“关于 Endpoint FlexResponse”](#)。

此响应规则可用于 Endpoint Discover。

请参见第 656 页的[“端点检测的响应规则”](#)。

配置“Endpoint: FlexResponse”响应规则操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

2 从“操作”列表中添加“Endpoint: FlexResponse”操作类型。

请参见第 671 页的[“配置响应规则操作”](#)。

3 输入 FlexResponse 插件“名称”并配置其“参数”。

请参见第 692 页的[表 40-5](#)。

4 单击“保存”保存配置。

请参见第 667 页的[“管理响应规则”](#)。

表 40-5 “Endpoint: FlexResponse”响应规则操作参数

参数	说明
FlexResponse Python 插件	输入各软件包以句点(.)分隔的脚本模块名称
插件参数	单击“添加参数”将一个或多个参数添加到该脚本。 输入每个参数的“键/值”对。

参数	说明
凭据	<p>您可以添加凭据以便对插件进行访问。</p> <p>可以在“系统”>“设置”>“凭据”屏幕中添加和存储凭据。</p> <p>请参见第 121 页的“关于凭据存储”。</p>

请参见第 664 页的[“实施响应规则”](#)。

配置“Endpoint Discover: 隔离文件”操作

“Endpoint Discover: 隔离文件”响应规则操作将包含敏感信息的文件从不安全的位置删除，放到安全的位置。

请参见第 1145 页的[“关于端点隔离”](#)。

此响应规则操作特定于 Endpoint Discover 事件。此响应规则不适用于需要数据配置文件的双层检测方法。

请参见第 1143 页的[“如何实施 Endpoint Discover”](#)。

如果在单个策略中使用多个端点响应规则，请确保您了解这些规则的优先顺序。

请参见第 662 页的[“关于响应规则操作的执行优先级”](#)。

配置“Endpoint Discover: 隔离文件”响应规则操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

2 从“操作”列表添加“Endpoint Discover: 隔离文件”操作类型。

请参见第 671 页的[“配置响应规则操作”](#)。

3 输入“隔离路径”和“标记文件”设置。

请参见第 693 页的[表 40-6](#)。

4 单击“保存”保存配置。

请参见第 667 页的[“管理响应规则”](#)。

表 40-6 “Endpoint Discover: 隔离文件”响应规则操作参数

参数	说明
隔离路径	输入您要将文件放入的安全位置的路径。安全位置既可以在端点计算机的本地驱动器上，也可以在远程文件共享上。EFS 文件夹也可用作隔离位置。

参数	说明
访问模式	<p>如果您的安全位置位于远程文件共享，则必须选择 Symantec DLP Agent 访问该文件共享的方式。</p> <p>选择以下凭据访问类型之一：</p> <ul style="list-style-type: none"> ■ 匿名访问 ■ 使用保存的凭据 <p>在匿名模式下，Symantec DLP Agent 以 LocalSystem 用户身份运行来移动机密文件。您可使用匿名模式将文件移动到本地驱动器上的安全位置或移动到远程共享（如果其允许匿名访问）。</p> <p>注意：EFS 文件夹不接受匿名用户。</p> <p>指定的凭据可让 Symantec DLP Agent 扮演指定的用户来访问安全位置。凭据必须为以下格式：</p> <pre>domain\user</pre> <p>您必须通过“系统凭据”页面输入您要使用的指定凭据。</p> <p>请参见第 122 页的“配置端点凭据”。</p>
标记文件	选中“保留标记文件以替换补救的文件”复选框可创建替换机密文件的占位符文件。
标记文本	<p>指定要显示在标记文件中的文本。如果已选择用标记文件来替换补救的文件选项，则可以在标记文本中使用变量。</p> <p>要指定标记文本，请从“插入变量”列表中选择变量。</p> <p>例如，对于标记文本，您可以输入：</p> <p>邮件违反了 \$POLICY\$ 中的以下规则: \$RULES</p> <p>或者，您可以输入：</p> <p>\$FILE_NAME\$ 已移动到 \$QUARANTINE_PARENT_PATH\$</p>

请参见第 654 页的[“关于响应规则操作”](#)。

请参见第 656 页的[“端点检测的响应规则”](#)。

配置“Endpoint Prevent: 阻止”操作

“Endpoint Prevent: 阻止”响应规则操作可阻止移动端点计算机上的机密数据，并（可选）向端点用户显示屏幕通知。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则操作特定于 Endpoint Prevent 事件。此响应规则不适用于需要数据配置文件的双层检测方法。

请参见第 1143 页的[“如何实施 Endpoint Discover”](#)。

如果在单个策略中组合多个端点响应规则，请确保您了解这类规则的优先顺序。

请参见第 662 页的[“关于响应规则操作的执行优先级”](#)。

注意：将敏感数据复制到本地驱动器不会触发阻止操作。

配置“Endpoint Prevent: 阻止”响应规则操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

2 从“操作”列表添加“**Endpoint Prevent: 阻止**”操作类型。

3 请参见第 671 页的[“配置响应规则操作”](#)。

4 输入“端点通知内容”设置。

请参见第 695 页的[表 40-7](#)。

5 单击“保存”保存配置。

请参见第 667 页的[“管理响应规则”](#)。

表 40-7 “Endpoint Prevent: 阻止”响应规则操作的参数

参数	配置
语言	选择想让响应规则执行时使用的语言。单击“添加语言”可添加多种语言。 请参见第 1153 页的 “关于不同区域设置中的 Endpoint Prevent 响应规则” 。 请参见第 1154 页的 “设置不同区域设置的 Endpoint Prevent 响应规则” 。
显示在警报框的消息	此字段对于“端点阻止”操作是可选字段。选择“端点阻止”操作，以便在系统阻止尝试复制机密数据时向端点用户显示屏幕通知。 在文本框中输入通知消息。通过从“插入变量”框中选择适当的值，可以向邮件中添加变量。 或者，您可以配置屏幕通知以包括用户理由和用户输入其理由的选项。

参数	配置
插入变量	<p>选择要包括在系统阻止尝试复制机密数据时向端点用户显示的屏幕通知中的变量。</p> <p>您可以基于以下类型选择变量：</p> <ul style="list-style-type: none"> ■ 应用程序 ■ 内容名称 ■ 内容类型 ■ 设备类型 ■ 策略名称 ■ 协议
允许用户选择说明	<p>选择此选项最多可在屏幕通知中显示四条用户理由。当通知显示在端点计算机上时，用户需要选择其中一条理由。（如果选择“允许用户输入文本说明”，用户可以输入理由。）Symantec Data Loss Prevention 提供了四条默认理由，您可以根据需要对其进行修改或删除。</p> <p>理由：</p> <ul style="list-style-type: none"> ■ 用户培训 ■ 中断的业务流程 ■ 经管理员批准的 ■ 误报 <p>每条理由条目包括以下选项：</p> <ul style="list-style-type: none"> ■ 复选框 此选项指示是否在通知中包括相关理由。要删除某条理由，请清除旁边的复选框。要包括某条理由，请选中旁边的复选框。 ■ 理由 理由的系统标签。该值出现在报告（用于排序和过滤）中，但用户看不到它。您可以从下拉列表中选择所需的选项。 ■ 为最终用户提供选项 系统在通知中显示的理由文本。该值出现在具有理由标签的报告中。您可以根据需要修改默认文本。 <p>要添加一条新理由，请从下拉列表中选择“新理由”。在出现的“输入新理由”文本框中，输入理由名称。保存规则时，Symantec Data Loss Prevention 会将其作为选项（按字母顺序）包括在所有的“理由”下拉列表中。</p> <p>注意：应当有选择性地添加新理由。当前不支持删除新理由。</p>
允许用户输入文本说明	选择此选项可包括用户可在其中输入其各自理由的文本框。

请参见第 656 页的“[端点检测的响应规则](#)”。

配置“Endpoint Prevent: 通知”操作

当端点用户尝试复制或发送敏感文件时，“Endpoint Prevent: 通知”响应规则操作会向该用户显示屏幕通知。您可以提供通知的理由，并为端点用户提供给出操作理由的选项。

请参见第 654 页的“[关于响应规则操作](#)”。

此响应规则操作适用于 Endpoint Prevent。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

注意：将敏感数据复制到本地驱动器不会触发通知操作。

配置“Endpoint Prevent: 通知”操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

从“操作”列表中添加“**Endpoint Prevent: 通知**”操作类型。

请参见第 671 页的“[配置响应规则操作](#)”。

2 配置操作参数。

请参见第 697 页的[表 40-8](#)。

3 单击“保存”保存配置。

请参见第 667 页的“[管理响应规则](#)”。

表 40-8 “Endpoint Prevent: 通知” 响应规则操作参数

参数	说明
语言	选择想让响应规则执行时使用的语言。 单击“添加语言”可添加多种语言。 请参见第 1153 页的“ 关于不同区域设置中的 Endpoint Prevent 响应规则 ”。 请参见第 1154 页的“ 设置不同区域设置的 Endpoint Prevent 响应规则 ”。
显示在警报框的消息	此字段对于“端点通知”操作是必填字段。选择此选项可向端点用户显示屏幕通知。 在文本框中输入通知消息。通过从“插入变量”框中选择适当的值，可以向邮件中添加变量。 或者，您可以配置屏幕通知以包括用户理由和用户输入其理由的选项。

参数	说明
插入变量	<p>选择要在向端点用户显示的屏幕通知中包括的变量。</p> <p>您可以基于以下类型选择变量：</p> <ul style="list-style-type: none"> ■ 应用程序 ■ 内容名称 ■ 内容类型 ■ 设备类型 ■ 策略名称 ■ 协议
允许用户选择说明	<p>选择此选项最多可在屏幕通知中显示四条用户理由。当通知显示在端点计算机上时，用户需要选择其中一条理由。（如果选择“允许用户输入文本说明”，用户可以输入理由。）Symantec Data Loss Prevention 提供了四条默认理由，您可以根据需要对其进行修改或删除。</p> <p>可用理由：</p> <ul style="list-style-type: none"> ■ 中断的业务流程 ■ 误报 ■ 经管理员批准的 ■ 用户培训 ■ 自定义（新理由） <p>每条理由条目包括以下选项：</p> <ul style="list-style-type: none"> ■ 复选框 此选项指示是否在通知中包括相关理由。要删除某条理由，请清除旁边的复选框。要包括某条理由，请选中旁边的复选框。 ■ 理由 理由的系统标签。该值出现在报告（用于排序和过滤）中，但用户看不到它。您可以从下拉列表中选择所需的选项。 ■ 为最终用户提供选项 Symantec Data Loss Prevention 在通知中显示的理由文本。该值出现在具有理由标签的报告中。您可以根据需要修改默认文本。 <p>要添加一条新理由，请从相应的下拉列表中选择“新理由”。在出现的“输入新理由”文本框中，键入理由名称。保存规则时，系统会将新理由作为选项（按字母顺序）包括在所有的“理由”下拉列表中。</p> <p>注意：您应当有选择性地添加新理由。当前不支持删除新理由。</p>
允许用户输入文本说明	选择此选项可包括用户可在其中输入其各自理由的文本框。

请参见第 656 页的“[端点检测的响应规则](#)”。

配置 Endpoint Prevent: 用户取消操作

当出现策略违规时，“Endpoint Prevent: 用户取消”响应规则操作会向用户显示一条时效性通知。

请参见第 654 页的“[关于响应规则操作](#)”。

用户需要在限定时间内决定是否忽略该策略违规。如果忽略违规，将完成数据传输并创建一个事件。如果不忽略违规，将停止数据传输并创建一个事件。如果用户在给定时间内没有做出决定，将自动阻止数据传输并创建一个事件。您可以提供通知的理由，并为端点用户提供输入操作理由的选项。

此响应规则操作适用于 Endpoint Prevent。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

配置 Endpoint Prevent: 用户取消操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

从“操作”列表中添加“**Endpoint Prevent: 用户取消**”操作类型。

请参见第 671 页的“[配置响应规则操作](#)”。

2 配置“**Endpoint Prevent: 用户取消**”参数。

请参见第 699 页的[表 40-9](#)。

3 单击“保存”保存配置。

请参见第 667 页的“[管理响应规则](#)”。

表 40-9 Endpoint Prevent: 用户取消参数

参数	说明
语言	选择想让响应规则执行时使用的语言。 单击“添加语言”可添加多种语言。 请参见第 1153 页的“ 关于不同区域设置中的 Endpoint Prevent 响应规则 ”。 请参见第 1154 页的“ 设置不同区域设置的 Endpoint Prevent 响应规则 ”。
超时前警告	此字段是必填字段，用于通知用户他们需要在限定时间内响应该事件。 在文本框中输入通知消息。通过从“插入变量”框中选择适当的值，可以向邮件中添加变量。

参数	说明
超时后消息	<p>此字段用于通知用户可覆盖该策略的时间段已过期。已阻止数据传输。</p> <p>在文本框中输入通知消息。通过从“插入变量”框中选择适当的值，可以向邮件中添加变量。</p>
显示在警报框的消息	<p>此字段对于“端点用户取消”操作是必填字段。选择此选项可向端点用户显示屏幕通知。</p> <p>在文本框中输入通知消息。通过从“插入变量”框中选择适当的值，可以向邮件中添加变量。</p> <p>或者，您可以配置屏幕通知以包括用户理由和用户输入其理由的选项。</p>
插入变量	<p>选择要在向端点用户显示的屏幕通知中包括的变量。</p> <p>您可以基于以下类型选择变量：</p> <ul style="list-style-type: none">■ 应用程序■ 内容名称■ 内容类型■ 设备类型■ 策略名称■ 协议■ 超时计数器 <p>注意：必须使用超时计数器变量显示多长时间后将阻止数据传输。</p>

参数	说明
允许用户选择说明。	<p>选择此选项最多可在屏幕通知中显示四条用户理由。当通知显示在端点计算机上时，用户需要选择其中一条理由。（如果选择“允许用户输入文本说明”，用户可以输入理由。）Symantec Data Loss Prevention 提供了四条默认理由，您可以根据需要对其进行修改或删除。</p> <p>可用理由：</p> <ul style="list-style-type: none"> ■ 中断的业务流程 ■ 误报 ■ 经管理员批准的 ■ 用户培训 ■ 自定义（新理由） <p>每条理由条目包括以下选项：</p> <ul style="list-style-type: none"> ■ 复选框 此选项指示是否在通知中包括相关理由。要删除某条理由，请清除旁边的复选框。要包括某条理由，请选中旁边的复选框。 ■ 理由 理由的系统标签。该值出现在报告（用于排序和过滤）中，但用户看不到它。您可以从下拉列表中选择所需的选项。 ■ 为最终用户提供选项 Symantec Data Loss Prevention 在通知中显示的理由文本。该值出现在具有理由标签的报告中。您可以根据需要修改默认文本。 <p>要添加一条新理由，请从相应的下拉列表中选择“新理由”。在出现的“输入新理由”文本框中，键入理由名称。保存规则时，系统会将新理由作为选项（按字母顺序）包括在所有的“理由”下拉列表中。</p> <p>注意：您应当有选择性地添加新理由。当前不支持删除新理由。</p>
允许用户输入文本说明。	选择此选项可包括用户可在其中输入其各自理由的文本框。

请参见第 664 页的“[实施响应规则](#)”。

配置“Network and Mobile Prevent for Web: 阻止 FTP 请求”操作

“Network and Mobile Prevent for Web: 阻止 FTP 请求”响应规则操作会阻止任何从网络或移动设备上以 FTP 传输的文件。

请参见第 654 页的“[关于响应规则操作](#)”。

此响应规则仅适用于与代理服务器集成的 Network Prevent for Web 或既与 VPN 服务器集成又与代理服务器集成的 Mobile Prevent for Web。

请参见第 907 页的[“配置 Network Prevent for Web Server”](#)。

请参见第 1231 页的[“实施 Mobile Prevent”](#)。

配置 “Network and Mobile Prevent for Web: 阻止 FTP 请求” 响应规则操作

- 1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

- 2 从“操作”列表添加“**Network and Mobile Prevent for Web: 阻止 FTP 请求**”操作类型。

“阻止 FTP 请求”响应规则操作无需任何进一步配置。将响应规则部署到策略后，此操作将阻止任何 FTP 尝试。

请参见第 671 页的[“配置响应规则操作”](#)。

- 3 单击“保存”保存配置。

请参见第 667 页的[“管理响应规则”](#)。

请参见第 664 页的[“实施响应规则”](#)。

配置 “Network and Mobile Prevent for Web: 阻止 HTTP/S” 操作

“Network and Mobile Prevent for Web: 阻止 HTTP/S”响应规则操作会阻止 Network Prevent for Web 或 Mobile Prevent for Web 检测到的 Web 内容传输。此操作还会阻止基于 Web 的电子邮件和附件。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则操作会使用 Internet 内容修改协议 (ICAP) 阻止 Web 内容的传输。要实施此响应规则操作，必须将检测服务器与 Web 代理服务器相集成。对于 Mobile Prevent for Web，还必须与 VPN 服务器进行集成。

请参见第 907 页的[“配置 Network Prevent for Web Server”](#)。

请参见第 1231 页的[“实施 Mobile Prevent”](#)。

配置 “Network Prevent: 阻止 HTTP/S” 响应规则操作

- 1 将 Network Prevent for Web 或 Mobile Prevent for Web 与代理服务器集成，如有必要，再将其与 VPN 服务器集成。

请参见第 182 页的[“Network Prevent for Web Server - 基本配置”](#)。

- 2 在“配置响应规则”屏幕上配置响应规则。
请参见第 669 页的[“配置响应规则”](#)。
- 3 从“操作”列表添加“**Network and Mobile Prevent for Web: 阻止 HTTP/S**”操作类型。
请参见第 671 页的[“配置响应规则操作”](#)。
- 4 根据需要编辑“拒绝消息”。
当操作阻止内容时，系统会为用户的浏览器提供此消息。
例如，您可以包括一些要显示在浏览器中的 HTML 编码文本。

注意：如果请求客户端不希望收到 HTML 响应，客户端浏览器中可能不显示“拒绝消息”。例如，希望收到 Web 发布的 XML 响应的客户端可能仅指示 Javascript 错误。

- 5 单击“保存”保存响应规则的配置。

某些应用程序可能无法针对“Network and Mobile Prevent for Web: 阻止 HTTP/S”响应操作提供适当的响应。在 Yahoo! Mail 应用程序中，检测服务器在阻止文件上传时出现过这种情况。如果用户尝试上传电子邮件附件并且附件触发了“Network and Mobile Prevent for Web: 阻止 HTTP/S”响应操作，Yahoo!Mail 不会做出响应，也不会显示说明文件已被阻止的错误消息。相反，Yahoo! Mail 看上去仍在继续上传选择的文件，但是上传永远无法完成。用户必须在某个时间通过手动单击“取消”来取消上传。

其他应用程序可能存在这种情况，这取决于它们如何处理阻止请求。在这些情况下，即使应用程序没有发出这种指示，也会创建检测服务器事件，并阻止文件上传。

请参见第 664 页的[“实施响应规则”](#)。

配置“Network Prevent: 阻止 SMTP 邮件”操作

“Network Prevent: 阻止 SMTP 邮件”响应规则操作阻止在 Network Prevent (Email) 检测服务器上导致事件的 SMTP 电子邮件。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则操作仅适用于 Network Prevent for Email。

请参见第 657 页的[“Network and Mobile Prevent for Web 检测的响应规则”](#)。

必须将 Network Prevent for Email 检测服务器与邮件传输代理 (MTA) 集成，才能实施此响应规则操作。有关详细信息，请参考《Symantec Data Loss Prevention MTA 集成指南（适用于 Network Prevent (Email)）》。

配置“阻止 SMTP 邮件”响应规则操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

2 从“操作”列表中添加“**Network Prevent: 阻止 SMTP 邮件**”操作类型。

请参见第 671 页的[“配置响应规则操作”](#)。

3 配置“阻止 SMTP 邮件”操作参数。

请参见第 704 页的[表 40-10](#)。

4 单击“保存”保存响应规则。

请参见第 667 页的[“管理响应规则”](#)。

表 40-10 “Network Prevent: 阻止 SMTP 邮件”参数

参数	说明
将邮件退回发送者	输入希望在 Network Prevent (Email) 返回给 MTA 的 SMTP 错误中显示的文本。某些 MTA 在退回给发件人的邮件中显示此文本。 如果将此字段留空，邮件不会退回给发件人，但 MTA 会发送其自己的邮件。
将邮件重定向至该地址	如果您要将阻止的邮件重定向至特定地址（例如 Symantec Data Loss Prevention 管理员），请在此字段中输入该地址。 如果将此字段留空，退回的邮件只会转给发送者。

请参见第 664 页的[“实施响应规则”](#)。

配置“Network Prevent: 修改 SMTP 邮件”操作

可以通过“Network Prevent: 修改 SMTP 邮件”响应规则操作修改敏感电子邮件。例如，您可以使用该操作将电子邮件主题标题更改为包括策略违规类型的相关信息。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则操作仅适用于 Network Prevent for Email。

请参见第 657 页的[“Network and Mobile Prevent for Web 检测的响应规则”](#)。

配置“Network Prevent: 修改 SMTP 邮件”操作

- 1 在“配置响应规则”屏幕上配置响应规则。
请参见第 669 页的“[配置响应规则](#)”。
- 2 从“操作”列表中添加“**Network Prevent: 修改 SMTP 邮件**”操作类型。
请参见第 671 页的“[配置响应规则操作](#)”。
- 3 配置操作参数。
请参见第 705 页的[表 40-11](#)。
- 4 单击“保存”保存配置。
请参见第 667 页的“[管理响应规则](#)”。

表 40-11 “Network Prevent: 修改 SMTP 邮件”参数

参数	说明
主题	<p>从以下选项中选择要对邮件主题进行的修改类型：</p> <ul style="list-style-type: none"> ■ 不修改 – 不更改主题中的文本。 ■ 前缀 – 在主题开头添加新文本。 ■ 后缀 – 在主题末尾添加新文本。 ■ 替换为 – 将旧主题文本完全替换为新文本。 <p>如果当前修改主题文本，请指定新文本。</p> <p>例如，如果您想将 VIOLATION 放置在邮件主题之前，请选择“前缀”，并在文本字段中输入 VIOLATION。</p>
标头	为要添加到邮件中的每个标头（最多三个）输入一个唯一名称和一个值。
启用电子邮件隔离连接（需要 Symantec Messaging Gateway）	<p>选择此选项可启用与 Symantec Messaging Gateway 的集成。启用此选项后，Symantec Data Loss Prevention 会向邮件添加 x 个预配置标头，用于通知 Symantec Messaging Gateway 应隔离该邮件。</p> <p>有关详细信息，请参阅《Symantec Data Loss Prevention Email Quarantine Connect FlexResponse 操作指南》。</p>

请参见第 664 页的“[实施响应规则](#)”。

配置“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”操作

“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”响应操作会删除发布到 Web 邮件站点（如 Gmail）、博客（如 Blogspot）和其他站点的机密数据。此操作还会删除用户上传到网站或附加到 Web 邮件的所有文件中包含的机密数据。此操作仅适用于 HTTP/S POST 命令，而不适用于 GET 命令。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则操作仅适用于 Network Prevent for Web 和 Mobile Prevent for Web。

请参见第 657 页的[“Network and Mobile Prevent for Web 检测的响应规则”](#)。

Symantec Data Loss Prevention 可识别选定 Web 邮件、博客和社会网络站点的 Web 表单字段。如果 Network Prevent for Web 或 Mobile Prevent for Web 无法删除其识别的网站的机密数据，它会创建一个系统事件并执行已配置的备用选项。

注意：Symantec Data Loss Prevention 会删除所上传的文件的内容（对于 Network Prevent，还会删除 Web 邮件附件的内容），即使对于它未识别出需要删除 HTTP 内容的那些站点，也是如此。

配置“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”操作

1 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的[“配置响应规则”](#)。

2 从“操作”列表添加“Network and Mobile Prevent for Web: 删除 HTTP/S 内容”操作类型。

请参见第 671 页的[“配置响应规则操作”](#)。

3 配置操作参数。

请参见第 706 页的[表 40-12](#)。

4 单击“保存”保存配置。

请参见第 667 页的[“管理响应规则”](#)。

表 40-12 “Network and Mobile Prevent for Web: 删除 HTTP/S 内容”参数

字段	说明
删除消息	系统已从中删除机密信息的内容（Web 发布、Web 邮件或文件）中显示的消息。只有接受者能够看到此消息。

字段	说明
备用选项	<p>当 Network Prevent for Web 或 Mobile Prevent for Web 无法删除在 HTTP 或 HTTPS Post 请求中检测到的机密信息时采取的操作。</p> <p>可用选项包括“阻止”（默认）和“允许”。</p> <p>注意：Symantec Data Loss Prevention 会删除所上传的文件中的机密数据（对于 Network Prevent，还会删除 Web 邮件附件中的机密数据），即使对于它不在其中执行内容删除的站点，也是如此。只有在 Symantec Data Loss Prevention 在所识别的 Web 表单中检测到机密内容时，才会采用“备用选项”，但它不会删除这些内容。</p>
拒绝消息	<p>Network Prevent 或 Mobile Prevent 阻止 HTTP 或 HTTPS Post 请求时返回给客户端的消息。客户端 Web 应用程序可能会（也可能不会）显示拒绝消息，具体取决于该应用程序处理错误消息的方式。</p>

请参见第 664 页的“[实施响应规则](#)”。

配置“Network Protect: 复制文件”操作

“Network Protect: 复制文件”响应规则操作可将敏感文件复制到本地文件系统。

请参见第 654 页的“[关于响应规则操作](#)”。

此响应规则操作仅适用于已为 Network Protect 配置的 Network Discover。

请参见第 657 页的“[Network and Mobile Prevent for Web 检测的响应规则](#)”。

配置“Network Protect: 复制文件”响应规则操作

1 配置网络文件共享并指定要将文件复制到的位置。

请参见第 992 页的“[为文件共享配置 Network Protect](#)”。

2 在“配置响应规则”屏幕上配置响应规则。

请参见第 669 页的“[配置响应规则](#)”。

3 从“操作”列表中选择“**Network Protect: 复制文件**”操作类型。

此操作不要求您配置任何参数。

请参见第 671 页的“[配置响应规则操作](#)”。

4 单击“保存”保存配置。

请参见第 667 页的“[管理响应规则](#)”。

请参见第 664 页的“[实施响应规则](#)”。

配置“Network Protect: 隔离文件”操作

“Network Protect: 隔离文件”响应规则操作会隔离检测服务器标识为敏感或受保护的文件。

请参见第 654 页的[“关于响应规则操作”](#)。

此响应规则操作仅适用于已为 Network Protect 配置的 Network Discover。

请参见第 657 页的[“Network and Mobile Prevent for Web 检测的响应规则”](#)。

配置“Network Protect: 隔离文件”响应规则操作

1 在“配置响应规则”屏幕上配置响应规则

请参见第 669 页的[“配置响应规则”](#)。

2 从“操作”列表中选择“Network Protect: 隔离文件”操作类型。

请参见第 671 页的[“配置响应规则操作”](#)。

3 配置“Network Protect: 隔离文件”参数。

请参见第 708 页的[表 40-13](#)。

4 单击“保存”保存配置。

请参见第 667 页的[“管理响应规则”](#)。

表 40-13 “Network Protect: 隔离文件”配置参数

参数	说明
标记文件	<p>选择此选项可创建一个标记文本文件来替换原始文件。此操作会通知用户对文件执行了哪些操作，而不是隔离或删除文件而不提供任何说明。</p> <p>注意：只要原始文件是文本文件，标记文件就会具有与其相同的类型和名称。这类文件类型的一个示例是 Microsoft Word。如果原始文件为 PDF 或图像文件，则系统将创建纯文本标记文件。然后，系统将指定与原始文件相同的文件名，但在文件名结尾附加 .txt。例如，如果原始文件名是 accounts.pdf，则标记文件名是 accounts.pdf.txt。</p>
标记文本	<p>指定要显示在标记文件中的文本。如果已选择用标记文件来替换补救的文件选项，则可以在标记文本中使用变量。</p> <p>要指定标记文本，请从“插入变量”列表中选择变量。</p> <p>例如，对于标记文本，您可以输入：</p> <p>邮件违反了 \$POLICY\$ 中的以下规则: \$RULES</p> <p>或者，您可以输入：</p> <p>\$FILE_NAME\$ 已移动到 \$QUARANTINE_PARENT_PATH\$</p>

请参见第 664 页的[“实施响应规则”](#)。

6

部分

补救和管理事件

- 41. 补救事件
- 42. 补救网络事件
- 43. 补救端点事件
- 44. 补救移动事件
- 45. 补救发现事件
- 46. 使用分类事件
- 47. 管理和报告事件
- 48. 存档事件
- 49. 使用事件数据
- 50. 实施查找插件

补救事件

本章节包括下列主题：

- [关于事件补救](#)
- [补救事件](#)
- [执行智能响应规则](#)
- [事件补救操作命令](#)
- [响应操作变量](#)
- [Monitor 和 Prevent 事件变量](#)
- [移动事件变量](#)
- [发现事件变量](#)

关于事件补救

当系统中发生事件后，组织内的人员必须分析这些事件，确定其发生的原因，辨别趋势并补救问题。

Symantec Data Loss Prevention 提供一组丰富的功能，这些功能可用于建立有效的事件补救流程。准备好行动后，您可以在“事件快照”和“事件列表”页使用一系列事件命令。

由于“事件快照”页显示关于一个特定事件的详细信息，因此您可以选择一个命令来对显示的事件执行操作。

在“事件列表”页上，您可以同时对多个事件执行某个操作。您可以从该列表中选择多个事件，然后选择所需的命令。

[表 41-1](#) 对事件补救所涉及的选项进行了说明：

表 41-1 事件补救所涉及的选项

补救选项	说明
基于角色的访问控制	<p>可以通过基于角色的访问控制对访问 Symantec Data Loss Prevention 系统中的事件信息的行为进行严格控制。角色可以控制特定补救者可以对哪些事件采取操作，以及事件中的哪些信息可供补救者使用。例如，访问控制可用于确保给定补救者仅能对在特定业务单元中产生的事件进行操作。另外，访问控制可能会阻止该业务单元的员工看到高严重性事件，于是会将这些事件路由到安全部门。</p> <p>请参见第 77 页的“关于基于角色的访问控制”。</p>
严重性级别分配	<p>事件严重性是一种评定与特定事件相关的风险的方法。例如，包含 50 条客户记录的电子邮件可视为比包含 50 例可接受使用策略违规的电子邮件更严重。使用 Symantec Data Loss Prevention，您可以通过在策略规则级别对严重事件进行配置，指定构成严重事件的因素。然后，Symantec Data Loss Prevention 会使用事件的严重性来推动对该事件的后续响应。您可以通过此流程设置事件的优先级，并将手动补救资源投入到最需要的区域。</p>
自定义属性查找	<p>自定义属性查找是从 Enforce 和事件本身之外的数据源收集关于事件的其他信息的过程。例如，可以从公司 LDAP 服务器查询有关邮件发送者的其他信息，例如发送者的经理的姓名或业务单元。</p> <p>请参见第 834 页的“关于使用自定义属性”。</p> <p>例如，您可以将自定义属性用作后续自动响应的输入内容，以自动将策略违规情况通知给发送者的经理。</p> <p>请参见第 836 页的“手动设置自定义属性的值”。</p>
自动事件响应	<p>Enforce Server 的一个强大功能是能够在事件发生后自动对其作出响应。例如，您可以将系统配置为通过阻止或干扰通信来响应严重事件。您可以向发送者的经理发送电子邮件。您可以向安全事件管理系统发送警报。您可以将事件上报给安全部门。另外，可以通过向发送者发送电子邮件免除可接受的使用事件。然后您可以将该事件标记为关闭，无需执行进一步的操作。在这些极端情况之间，您可以建立一个自动对向商业合作伙伴传输的机密数据进行加密的策略。所有这些情景都可以自动处理，而无需用户干预。</p> <p>请参见第 671 页的“配置响应规则操作”。</p>

补救选项	说明
智能响应	<p>虽然自动响应是补救流程的重要部分，但 SmartResponse 通常必不可少，尤其是在出现更加严重的事件时。Symantec Data Loss Prevention 提供详细的事件快照，其中包含确定接下来采取哪些补救步骤的所有必要信息。您可以使用 SmartResponse 手动更新事件严重性、状态和自定义属性，并可以对事件添加注释。您可以通过补救工作流移动事件从而予以解决。</p> <p>请参见第 671 页的“配置响应规则操作”。</p> <p>下列标准 SmartResponse 操作可供使用：</p> <ul style="list-style-type: none"> ■ 添加注释 ■ 记录到 Syslog 服务器 ■ 发送电子邮件通知 ■ 设置状态 <p>请参见第 689 页的“配置服务器 FlexResponse 操作”。</p>
分发聚合的事件报告	您可以创建汇总的事件报告并自动分发给数据所有者，以进行补救。

Enforce Server 可处理所有这些步骤，“智能响应”除外。您可以完全自动处理事件。您只能对最严重的事件保留手动干预（智能响应）。

请参见第 727 页的“[网络事件快照](#)”。

请参见第 760 页的“[发现事件快照](#)”。

请参见第 736 页的“[端点事件快照](#)”。

补救事件

补救事件时，可以执行以下操作之一：

- 设置事件的状态或严重性。
- 将智能响应规则应用于事件。
- 设置事件的自定义属性。
- 向事件记录中添加注释。
- 执行一些操作组合。
- 可以通过转至事件列表或事件快照并选择要对一个或多个事件执行的操作来补救事件。

可以在安装期间导入解决方案包。解决方案包会在事件列表和事件快照中预先填入若干补救选项和自定义属性。有关所有解决方案软件包的完整说明（包括有关其中

所有补救选项和自定义属性的信息），请参考文档中解决方案软件包目录中的每个解决方案软件包的文档。

补救事件

1 访问事件列表或事件快照。

在事件列表中，Symantec Data Loss Prevention 会在“事件操作”下拉菜单中显示可用补救选项。当在列表中选择一个或多个事件时，该菜单会处于活动中（复选框为选中状态）。在事件快照中，Symantec Data Loss Prevention 还会显示可用补救选项。您可以在下拉菜单中设置“状态”或“严重性”。

请参见第 785 页的“[查看事件](#)”。

您还可以编辑“属性”并提供相关信息。

2 采取以下操作之一：

■ 查看事件列表时，请选择要补救的事件（选中相应的框）。您可以单独选择事件或者选择当前屏幕上的所有事件。然后从“事件操作”下拉菜单中选择想要执行的操作。例如，选择“事件操作”>“设置状态”>“已提报”。

您可以根据需要执行多项操作。

■ 查看事件快照时，可以在下拉菜单中设置“状态”和“严重性”。

如果以前设置了智能响应，则可以在补救栏中选择一个智能响应规则。

请参见第 653 页的“[关于响应规则](#)”。

例如，如果已安装了一个解决方案包，则可以在补救栏中选择“排除误报”。当出现“执行响应规则”屏幕时，单击“确定”。本智能响应规则会将事件状态从“新建”更改为“已排除”，并将“排除原因”属性设置为“误报”。

您可以根据需要执行多项补救操作。

执行智能响应规则

执行发送电子邮件的响应规则时，可手动编写电子邮件通知的内容。

注意：将电子邮件通知发送到发送者仅适用于 SMTP 事件。此外，基于自定义属性（如“管理员电子邮箱”）的通知地址只有在由属性查找插件填充时，才可正常工作。

编写电子邮件通知响应

- 1 在“抄送”字段中输入要发送副本的可选电子邮件地址。
- 2 选择语言。
- 3 编写或编辑电子邮件的主题和正文。
- 4 为事件中的字段插入变量。支持的变量会以链接的形式显示在可编辑的字段右侧。

例如，如果要包括违反的策略和规则，可输入：

```
A message has violated the following rules in $POLICY$:  
$RULES$
```

- 5 单击“确定”发送通知。

请参见第 668 页的“[添加新的响应规则](#)”。

请参见第 713 页的“[关于事件补救](#)”。

请参见第 718 页的“[响应操作变量](#)”。

事件补救操作命令

在事件列表中，使用“事件操作”下拉菜单选择补救操作。

下列事件操作适用于事件列表：

添加注释

向选定事件添加一个简短注释。每个选定事件的注释会显示在“事件快照”页面的“事件历史记录”选项卡上。

存档

选择下列存档操作之一以设置所选事件的存档状态：

- 存档事件 - 将所选事件标记为已存档。
- 还原事件 - 将所选事件还原为非存档状态。
- 不存档 - 禁止对所选事件进行存档。
- 允许存档 - 允许对所选事件进行存档。

请参见第 823 页的“[关于事件存档](#)”。

删除事件

从 Symantec Data Loss Prevention 系统中删除选定的事件。

删除事件时请务必谨慎。与事件关联的所有数据都会删除，而且此操作无法反转。

导出所选项: CSV

将选定事件导出为逗号分隔的 (.csv) 文件。

导出所选项: XML

将选定事件导出为 XML 文件。

查找属性	使用已配置的查找插件查找已配置的属性。
设置属性	显示“设置属性”页面，以便输入或编辑每个选定事件的属性值。
设置数据所有者	设置下列数据所有者属性： <ul style="list-style-type: none">■ 名称■ 电子邮件地址
设置严重性	将为选定事件设置的严重性更改为“设置严重性”下的选项之一。
设置状态	将选定事件的状态更改为“设置状态”下的选项之一。系统管理员可在“事件属性”页面上自定义此列表上显示的选项。 请参见第 827 页的 “关于事件状态属性” 。
运行智能响应	对选定事件执行所列出的响应之一。单击响应规则时，会显示“执行响应规则”页面。 只有当您具有补救权限时，才可使用这些手动响应规则。

请参见第 713 页的[“关于事件补救”](#)。

响应操作变量

响应操作变量可在响应规则中使用。

请参见第 716 页的[“执行智能响应规则”](#)。

Network Monitor 和 Network Prevent 事件的响应操作变量与 Network Discover 和 Network Protect 事件的响应操作变量是不相同的。

请参见第 718 页的[“Monitor 和 Prevent 事件变量”](#)。

请参见第 719 页的[“移动事件变量”](#)。

请参见第 720 页的[“发现事件变量”](#)。

Monitor 和 Prevent 事件变量

以下 Network Monitor 和 Network Prevent 变量可供使用：

\$BLOCKED\$

表示 Symantec Data Loss Prevention 是否阻止了邮件（是或否）。

\$DATAOWNER_NAME\$	负责补救事件的人员。必须手动设置或者使用某个查找插件来设置此字段。 系统可自动将报告发送给数据所有者以进行补救。
\$DATAOWNER_EMAIL\$	负责补救事件的人员的电子邮件地址。必须手动设置或者使用某个查找插件来设置此字段。
\$INCIDENT_ID\$	事件的 ID。
\$INCIDENT_SNAPSHOT\$	指向事件快照页面的完全限定的 URL。
\$MATCH_COUNT\$	事件匹配数。
\$POLICY_NAME\$	被违规的策略的名称。
\$POLICY_RULES\$	违规的一个或多个策略规则的列表（以逗号分隔）。
\$RECIPIENTS\$	一个或多个邮件收件人的列表（以逗号分隔）。
\$SENDER\$	邮件发送者。
\$SEVERITY\$	分配给事件的严重性。
\$SUBJECT\$	邮件的主题。

移动事件变量

以下 &pn.MobilePreventWeb 变量可供使用：

\$BLOCKED\$	表示 Symantec Data Loss Prevention 是否阻止了邮件（是或否）。
\$DATAOWNER_NAME\$	负责补救事件的人员。必须手动设置或者使用某个查找插件来设置此字段。 系统可自动将报告发送给数据所有者以进行补救。
\$DATAOWNER_EMAIL\$	负责补救事件的人员的电子邮件地址。必须手动设置或者使用某个查找插件来设置此字段。
\$DEVICE_INSTANCE_IDS\$	生成违规的移动设备的特定 ID。
\$ENDPOINT_MACHINES\$	生成违规的端点计算机的名称。
\$FILE_FULL_PATH\$	找到事件的文件的完整路径。
\$FILE_NAME\$	找到事件的文件的名称。
\$PARENT_DIRECTORY_PATH\$	找到事件的文件父目录的路径。

\$INCIDENT_SNAPSHOTS 事件的 ID。

\$INCIDENT_SNAPSHOT\$ 指向事件快照页面的完全限定的 URL。

\$MATCH_COUNT\$ 事件匹配数。

\$POLICY_NAME\$ 被违规的策略的名称。

\$POLICY_RULES\$ 违规的一个或多个策略规则的列表（以逗号分隔）。

\$PROTOCOL\$ 生成违规的协议、设备类型或者目标类型。

\$PARENT_DIRECTORY_PATH\$ 隔离文件的父目录的路径。

\$RECIPIENTS\$ 一个或多个邮件收件人的列表（以逗号分隔）。

\$SCAN_DATE\$ 找到事件的扫描的日期。

\$SENDER\$ 邮件发送者。

\$SEVERITY\$ 分配给事件的严重性。

\$SUBJECT\$ 邮件的主题。

\$TARGET\$ 找到事件的目标的名称。

发现事件变量

以下 Network Discover 和 Network Protect 事件变量可供使用：

\$DATAOWNER_NAME\$ 负责补救事件的人员。必须手动设置或者使用某个查找插件来设置此字段。

系统可自动将报告发送给数据所有者以进行补救。

\$DATAOWNER_EMAIL\$ 负责补救事件的人员的电子邮件地址。必须手动设置或者使用某个查找插件来设置此字段。

\$FILE_NAME\$ 找到事件的文件的名称。

\$INCIDENT_ID\$ 事件的 ID。

\$MATCH_COUNT\$ 事件匹配数。

\$FILE_PARENT_DIRECTORY_PATH\$ 找到事件的文件父目录的路径。

\$FILE_FULL_PATH\$ 找到事件的文件的完整路径。

\$POLICY_NAME\$ 被违规的策略的名称。

\$POLICY_RULES\$	违规的一个或多个策略规则的列表（以逗号分隔）。
\$QUARANTINE_PARENT_DIRECTORY_PATH\$	隔离文件的父目录的路径。
\$SCAN_DATE\$	找到事件的扫描的日期。
\$SEVERITY\$	分配给事件的严重性。
\$TARGET\$	找到事件的目标的名称。

补救网络事件

本章节包括下列主题：

- [网络事件列表](#)
- [网络事件列表 - 操作](#)
- [网络事件列表 - 列](#)
- [网络事件快照](#)
- [网络事件快照 - 标题和导航](#)
- [网络事件快照 - 常规信息](#)
- [网络事件快照 - 匹配项](#)
- [网络事件快照 - 属性](#)
- [网络摘要报告](#)

网络事件列表

网络事件列表显示了多个网络事件记录，以及有关事件的严重性、关联策略、匹配数和事件状态等信息。单击事件列表的某行可查看有关特定事件的更多详细信息。单击左侧的复选框可选择要修改或补救的特定事件（或事件组）。

注意：单击“全选”时要谨慎。此操作会选中报告中的所有事件（不只是当前页面的事件）。随后应用的任何事件命令会影响所有事件。如果只选择当前页面上的事件，可选择事件列表左上角的复选框。

事件信息分为多个列。单击任意列标题，可基于该列的数据按字母数字顺序对其进行排序。要按倒序进行排序，请再次单击该列标题。默认情况下，Symantec Data Loss Prevention 按日期对事件进行排序。

“类型”列显示了表示网络事件类型的图标。表 42-1 介绍了这些图标。

表 42-1 网络事件的类型

图标	说明
	SMTP
	添加第二个图标表示邮件附件。
	HTTP
	Symantec Data Loss Prevention 还会检测通过 HTTP 隧道传输的 Yahoo 和 MSN IM 通信。 添加第二个图标表示基于 Web 的电子邮件的附件。
	HTTPS
	FTP
	NNTP
	IM: MSN
	IM: AIM
	IM: Yahoo
	TCP:custom_protocol

此列还表示是阻止了通信还是更改了通信。表 42-2 显示了可能的值。

表 42-2 事件阻止或更改的状态

图标	说明
无图标。	如果没有阻止通信，该列为空白。
	表示 Symantec Data Loss Prevention 阻止了包含匹配文本的通信。

图标	说明
	表示 Symantec Data Loss Prevention 从 Web 发布或基于 Web 的电子邮件中删除了机密数据。此图标还可以表示文件已上传到网站或附加到基于 Web 的电子邮件。
	表示 Symantec Data Loss Prevention 添加或修改了生成事件的邮件的标头。

使用下列链接可了解有关网络事件列表页面的详细信息：

了解详细信息	参见此部分
事件列表表格中的列	请参见第 726 页的“ 网络事件列表 - 列 ”。
要对选定事件执行的操作	请参见第 725 页的“ 网络事件列表 - 操作 ”。
特定事件的详细信息	请参见第 727 页的“ 网络事件快照 ”。
查看所有网络事件的摘要	请参见第 731 页的“ 网络摘要报告 ”。
所有 Symantec Data Loss Prevention 报告的常见功能	请参见第 777 页的“ 关于事件报告 ”。 请参见第 801 页的“ 常见事件报告功能 ”。

网络事件列表 - 操作

您可以选择一个或多个事件，然后使用“事件操作”下拉列表中的命令对其进行补救。事件命令如下：

操作	说明
添加注释	选择此选项可打开一个对话框，键入注释，然后单击“确定”。
存档	选择下列存档操作之一以设置所选事件的存档状态： <ul style="list-style-type: none"> ■ 存档事件 - 将所选事件标记为已存档。 ■ 还原事件 - 将所选事件还原为非存档状态。 ■ 不存档 - 禁止对所选事件进行存档。 ■ 允许存档 - 允许对所选事件进行存档。 请参见第 823 页的“ 关于事件存档 ”。
删除事件	选择此选项可删除指定的事件。

操作	说明
导出所选项: CSV	选择此选项可将指定事件保存在可在多个常见应用程序（例如 Microsoft Excel）中显示的逗号分隔文本 (.csv) 文件或 XML 文件中。
导出所选项: XML	
查找属性	使用查找插件查找事件自定义属性。
运行智能响应	选择此选项可运行您或管理员配置的智能响应规则。（要配置智能响应规则，请导航至“策略”>“响应规则”，然后单击“添加响应规则”，并选择“智能响应”。）
设置属性	选择此选项可设置选定事件的属性。
设置数据所有者	设置数据所有者名称或电子邮件地址。数据所有者是负责补救事件的人员。 系统可自动将报告发送给数据所有者以进行补救。
设置严重性	选择此选项可设置严重性。
设置状态	选择此选项可设置状态。
请参见第 713 页的“关于事件补救”。	
请参见第 723 页的“网络事件列表”。	

网络事件列表 - 列

事件信息分为多个列。单击任意列标题，可基于该列的数据按字母数字顺序对其进行排序。要按倒序进行排序，请再次单击该列标题。默认情况下，Symantec Data Loss Prevention 会按日期列出事件。

报告包括以下列：

- 用于选择要补救的事件的复选框。

您可以选择一个或多个要应用列表顶部的“事件”下拉菜单中的命令的事件。

单击列顶部的复选框，选中当前页上的所有事件。（请注意，您也可以单击最右侧的“全选”，选择报告中的“全部”事件。）

- **类型**

检测匹配所使用的协议。

请参见第 723 页的“[网络事件列表](#)”。

- **主题/发送者/接受者**

邮件主题、发送者电子邮件地址或 IP 地址、接受者电子邮件地址或者 URL。

■ 发送时间

发送邮件的日期和时间。

■ ID/策略

Symantec Data Loss Prevention 事件 ID 号和记录事件所依据的策略。

■ 匹配项

事件中的匹配数。

■ 严重性

由事件所匹配规则的严重性设置确定的事件严重性。

可能的值如下：

图标	说明
	高
	中
	低
	信息

■ 状态

当前事件状态。

可能的值如下：

- 新建
- 进行中
- 已提报
- 误报
- 配置错误
- 已解决

您或管理员可在“属性设置”页面上添加新的状态标识。

请参见第 723 页的“[网络事件列表](#)”。

网络事件快照

事件快照提供有关特定事件的详细信息。快照中会显示常规事件信息、在拦截的文本中检测到的匹配项以及事件属性。通过快照还可以执行已配置的任何智能响应规则。

事件快照分为三个窗格，并带有导航和智能响应选项。单击链接可查看更多有关事件快照的帮助：

了解详细信息

导航和智能响应选项

常规事件信息（左侧窗格）

事件中的匹配项（中间窗格）

属性（右侧窗格）

参见以下部分

请参见第 728 页的“[网络事件快照 - 标题和导航](#)”。

请参见第 728 页的“[网络事件快照-常规信息](#)”。

请参见第 730 页的“[网络事件快照 - 匹配项](#)”。

请参见第 731 页的“[网络事件快照 - 属性](#)”。

网络事件快照 - 标题和导航

下列页面导航工具会显示在事件快照顶部附近：

上一个

显示源报告中的上一个事件。

下一个

显示源报告中的下一个事件。



返回至源报告（单击此链接可到达此屏幕）。



使用任意新数据更新快照，例如“历史记录”部分中的新注释或者修改后的状态。

如果配置了任何智能响应规则，Symantec Data Loss Prevention 会在页面顶部显示执行规则的响应选项。根据智能响应规则的数量，可能还会显示下拉菜单。

请参见第 727 页的“[网络事件快照](#)”。

网络事件快照 - 常规信息

快照的左侧部分显示常规事件信息。您可以单击许多值来查看根据该值过滤的事件列表。一个图标可能会显示在“状态”下拉列表旁边，指示对生成事件的请求进行了阻止还是对其进行修改。

请参见第 724 页的[表 42-2](#)。

事件的当前状态和严重性会显示在快照标题的右侧。要更改其中一个当前值，请单击该值并从下拉列表中选择另一个值。

常规信息窗格的其他部分被分成四个选项卡。

■ 关键信息

- 历史记录

- 注释

- 关联

此部分的信息会分为以下类别（并非会显示每个事件类型的所有类别）：

表 42-3 事件常规信息选项卡

选项卡名称	说明
关键信息	<p>“关键信息”选项卡显示事件中违反的策略。它也显示了策略匹配项以及每个策略规则匹配项的总数。单击策略名称以查看违反策略的所有事件的列表。单击“查看策略”可查看该策略的只读版本。</p> <p>此部分也列出了同一文件违反的其他策略。要查看与特定策略关联的事件的快照，请单击策略名称旁的“转至事件”。要查看该文件所创建的事件的列表，请单击“显示全部”。</p> <p>“关键信息”选项卡也包括下列信息：</p> <ul style="list-style-type: none">■ 记录该事件的检测服务器的名称。■ 邮件发送的日期和时间■ 发送者电子邮件或 IP 地址■ 接受者电子邮件或 IP 地址■ SMTP 标题或 NNTP 主题标题■ “已存档”字段显示事件的存档状态、事件是否可存档，以及允许您切换事件的“不存档”标志。■ 附件文件名。单击可打开或保存此文件。如果响应规则告知 Symantec Data Loss Prevention 放弃原始邮件，则您无法查看附件。■ 负责补救事件的人员（“数据所有者名称”）。此字段必须手动设置，或使用查找插件设置。系统可自动将报告发送给数据所有者以进行补救。如果单击显示为超链接的“数据所有者名称”，将会显示按“数据所有者名称”进行过滤后的事件列表。■ 负责补救事件的人员的电子邮件地址（“数据所有者电子邮件地址”）。此字段必须手动设置，或使用查找插件设置。如果单击“数据所有者电子邮件地址”超链接，将显示按“数据所有者电子邮件地址”过滤的事件列表。

选项卡名称	说明
历史记录	<p>查看对事件执行的操作。对于每个操作，Symantec Data Loss Prevention 会显示操作的日期和时间、参与者（用户或服务器）以及操作或注释。</p> <p>请参见第 716 页的“执行智能响应规则”。</p> <p>请参见第 667 页的“管理响应规则”。</p>
注释	<p>查看您或其他用户已添加到事件中的任何注释。单击“添加注释”可以添加注释。</p>
关联	<p>您可以查看共享当前事件属性的事件的列表。例如，可查看单个帐户生成的所有事件的列表。“关联”选项卡显示与单个属性匹配的关联的列表。单击属性值可以查看与这些值相关的事件的列表。</p> <p>要搜索具有相同属性的其他事件，请单击“查找类似项”。在显示的“查找类似事件”对话框中，请选择所需的搜索属性。然后单击“查找事件”。</p> <p>注意：关联的事件列表不会显示已存档的相关事件。</p>

请参见第 727 页的“[网络事件快照](#)”。

请参见第 823 页的“[关于事件存档](#)”。

网络事件快照 - 匹配项

在常规信息下，Symantec Data Loss Prevention 显示邮件内容（如果适用）和导致事件的匹配项。Symantec Data Loss Prevention 根据协议类型显示下列类型的邮件内容：

协议	邮件内容
SMTP	邮件正文
HTTP	HTTP 请求的名称值对
FTP	不显示任何内容
NNTP	邮件正文
IM（所有提供程序）	IM 对话
TCP	通过自定义协议传输的数据

匹配项以黄色突出显示，并根据在其中检测到这些匹配项的邮件组件（如标题、正文或附件）进行组织。Symantec Data Loss Prevention 显示每个邮件组件的相关匹配项总数。将按照原始文本中显示的顺序来显示匹配项。要查看触发匹配项的规则，请单击突出显示的匹配项。

请参见第 411 页的“[关于相似度阈值和相似度评分](#)”。

请参见第 727 页的“[网络事件快照](#)”。

网络事件快照 - 属性

注意: 只有系统管理员已配置自定义属性，此部分才会显示。

如果已指定，则可以查看自定义属性列表及其值。单击属性值以查看根据该值过滤的事件列表。要添加新值或编辑现有值，请单击“编辑”。在显示的“编辑属性”对话框中，键入新值并单击“保存”。

请参见第 836 页的“[手动设置自定义属性的值](#)”。

请参见第 727 页的“[网络事件快照](#)”。

网络摘要报告

网络摘要报告提供有关在您的网络中找到的事件的摘要信息。您可以使用一个或两个摘要条件组织报告。单摘要报告由一个摘要条件组织，例如与该事件相关的策略。双摘要报告由两个条件组织，例如策略和事件状态。

若要查看可供当前报告使用的主要条件和辅助摘要条件，请单击“高级过滤器和摘要”栏。该栏位于报告顶部附近。“摘要类型：”列表框显示主要条件和辅助摘要条件。在每个列表框中，Symantec Data Loss Prevention 都会以字母顺序显示所有独特的条件，后跟您的系统管理员已定义的任何自定义条件。摘要报告的名称取自主要摘要条件（首个列表框的值）。如果使用新条件重新运行报告，则报告名称也会相应改变。

摘要条目分为若干列。单击任意列标题，可基于该列的数据按字母数字顺序对其进行排序。要按倒序进行排序，请再次单击该列标题。

表 42-4 摘要报告列

列名	说明
<i>summary_criterion</i>	此列针对主要摘要条件命名。它列出主要和辅助摘要（针对双摘要）项目。在“策略摘要”中，此列的名称为“策略”，并列出多种策略。单击摘要项目以查看与此项目相关的事件列表。
总计	与摘要项目相关的事件的总数。在“策略摘要”中，此列提供了与每个策略相关的事件的总数。
高	与摘要项目相关的高严重性事件的数目。（所匹配规则的严重性设置确定事件的严重性。）
中	与摘要项目相关的中严重性事件的数目。
低	与摘要项目相关的低严重性事件的数目。
信息	与摘要项目相关的信息性事件的数目。
条形图表	与摘要项目相关的事件（所有严重性）的数目的直观表示。该条形图表分解为多个成比例的、带颜色的部分（代表各种严重性）。
匹配项	与摘要项目相关的匹配总数。

在包含总计的任意严重性列中，可以单击总计，查看所选严重性的事件的列表。

请参见第 801 页的“[常见事件报告功能](#)”。

请参见第 779 页的“[关于控制板报告和执行摘要](#)”。

请参见第 777 页的“[关于事件报告](#)”。

请参见第 789 页的“[保存自定义事件报告](#)”。

补救端点事件

本章节包括下列主题：

- 端点事件列表
- 端点事件快照
- 关于 Endpoint Prevent 响应规则的报告
- 端点事件目标或协议特定的信息
- 端点事件摘要报告
- 配置 Endpoint Server 文件过滤器

端点事件列表

端点事件列表会显示包含协议或目标、严重性、关联策略、匹配项数和状态等基本信息的端点事件。单击任意事件可查看包含更多事件详细信息的快照。还可以选择要修改或补救的特定事件（或事件组）。

注意：端点报告仅显示 Endpoint Prevent 捕获的事件。Endpoint Discover 捕获的事件会显示在 Network Discover 报告中。

事件信息分为多个列。单击任意列标题，可按该列的数据以字母数字顺序对事件信息进行排序。要按倒序进行排序，请再次单击该列标题。默认情况下，Symantec Data Loss Prevention 会按日期列出事件。

报告包括以下列：

- 用于您选择要补救的事件的复选框

您可以选择一个或多个要应用列表顶部的“事件”下拉菜单中的命令的事件。单击列顶部的复选框，选中当前页上的所有事件。（可以单击最右侧的“全选”来选择报告中的所有事件。）

表 43-1 端点事件的类型

图形	事件的类型
	CD/DVD 刻录机（例如，Windows Media 刻录机）
	可移动介质（例如，USB 闪存驱动器或 SD 卡）
	固定驱动器（例如，C:\drive）
	从端点复制到网络共享
	电子邮件/SMTP
	HTTP
	HTTPS
	FTP
	IM:AIM
	IM:MSN
	IM:Yahoo
	打印机/传真
	剪贴板
	应用程序文件访问

一个响应列，用于指示 Symantec Data Loss Prevention 是阻止了试图违规行为还是将机密数据策略违规通知了最终用户。

可能的值如下：

- 如果 Symantec Data Loss Prevention 没有阻止违规行为或通知最终用户，则该列为空白。
- 红色图标表示违规行为已由 Symantec Data Loss Prevention、用户阻止，或用于指示用户取消选项时间限制是否过期。
- 通知图标表示 Symantec Data Loss Prevention 将所违反的机密数据策略通知了最终用户。如果用户允许违规的数据传输，则还会出现通知图标。如果用户取消时间限制选项过期且默认操作设置为允许数据传输，也会出现此图标。

此部分的其他列显示如下：

表 43-2 端点事件列

列	定义
文件名/计算机/用户/主题/接受者	文件名、计算机、端点用户（域和登录名）、主题标题（如果出现电子邮件/SMTP 违规）以及与事件关联的接受者用户
发生日期	<ul style="list-style-type: none">■ 事件日期和时间■ 报告日期■ 报告事件的时间和日期。如果端点与公司网络断开连接，则在连接还原后会报告事件。
ID/策略	Symantec Data Loss Prevention 事件 ID 号和记录事件所依据的策略
匹配项	事件中的匹配数
严重性	<p>由事件所匹配规则的严重性设置确定的事件严重性。</p> <p>可能的值如下：</p> <ul style="list-style-type: none">■ 高■ 中■ 低■ 仅供参考

列	定义
状态	<p>当前事件状态</p> <p>可能的值如下：</p> <ul style="list-style-type: none">■ 新建■ 进行中■ 已提报■ 误报■ 配置错误■ 已解决

您或管理员可在“属性设置”页面上添加新的状态标识。

请参见第 736 页的“[端点事件快照](#)”。

请参见第 713 页的“[关于事件补救](#)”。

请参见第 777 页的“[关于事件报告](#)”。

请参见第 789 页的“[保存自定义事件报告](#)”。

端点事件快照

事件快照提供有关特定 Endpoint Prevent 事件的详细信息。快照中会显示常规事件信息、在拦截的文本中检测到的匹配数，以及属性、事件历史记录和违反策略的详细信息。您也可以在“关联”区域中搜索类似的事件。

注意：Endpoint Discover 事件在 Network Discover 报告中被捕获。

请参见第 763 页的“[发现事件列表](#)”。

快照标题下会显示当前状态和严重性。要更改其中一个当前值，请单击该值并从下拉列表中选择另一个值。如果任何操作图标与之关联，也将在此显示。

如果您已配置任何“智能响应”规则，Symantec Data Loss Prevention 会显示一个“补救”栏（在“状态”栏下方）。“补救”栏包括执行规则的选项。根据智能响应规则的数量，可能还会显示下拉菜单。

快照的顶部左侧显示常规事件信息。您可以单击大部分信息值以查看根据该值过滤的事件列表。此部分的信息会分为以下类别（并非会显示每个事件类型的所有类别）：

表 43-3 事件的类型

图标	事件类型
	CD/DVD 刻录机（例如，Windows Media 刻录机）
	可移动介质（例如，USB 闪存驱动器或 SD 卡）
	本地驱动器
	网络共享
	电子邮件/SMTP
	HTTP
	HTTPS/SSL
	FTP
	IM:AIM
	IM:MSN
	IM:Yahoo
	打印机/传真
	剪贴板
	应用程序文件访问

下表包含其他参考部分：

表 43-4 事件部分

部分	说明
服务器	对事件进行双层检测的 Endpoint Server 的名称。或者，是从 Symantec DLP Agent 接收事件的 Endpoint Server 的名称。
代理响应	<p>端点阻止、端点通知、端点隔离、Endpoint FlexResponse 或用户取消操作（如果有）。可能的值如下：</p> <ul style="list-style-type: none"> ■ 如果 Symantec Data Loss Prevention 没有阻止复制操作或通知最终用户，则为空白或不显示任何图标。 ■ 红色圆形图标表示 Symantec Data Loss Prevention 阻止了机密数据。 ■ 邮件图标表示 Symantec Data Loss Prevention 通知了最终用户该数据是机密数据。 <p>请参见“关于 Endpoint Prevent 响应规则的报告”。</p>
事件发生时间	事件发生的日期和时间。
事件报告日期	Endpoint Server 检测到事件的日期和时间。
已存档	显示事件的存档状态、事件是否可存档，以及用于切换事件的“不存档”标志。请参见第 823 页的“ 关于事件存档 ”。
用户	端点用户名（例如，MYDOMAIN\bsmit）。
用户理由	理由标签后跟屏幕通知上向最终用户展示的文本（例如，经理已批准：“我的经理批准了该数据的传输”）。Symantec Data Loss Prevention 将标签用于在报告中进行分类和过滤，但端点用户永远不会看到该标签。单击标签以查看最终用户在其中选择此理由的事件列表。
计算机名称	发生事件的计算机。
计算机 IP (公司)	违规计算机（如果该计算机当时位于公司网络上）的 IP 地址。
文件名	违反策略的文件的名称。仅针对固定驱动器事件显示的文件名字段。

部分	说明
隔离结果	如果已配置“Endpoint Discover: 隔离”响应规则，则可能会出现下列隔离情景之一： <ul style="list-style-type: none">■ 已隔离文件■ 隔离失败■ 隔离结果超时
隔离位置	显示发生文件移动的安全位置的文件路径。
隔离详细信息	显示隔离任务无法移动机密文件的原因。例如，操作可能会由于源文件丢失或访问安全位置的凭据不正确而失败。 如果隔离文件的状态因隔离结果超时事件而显示为“未知”，则隔离详细信息文件也会显示信息。
端点位置	指示事件发生时端点计算机是否连接到公司网络。
应用程序名称	导致事件发生的应用程序的名称。
目标	机密数据的目标位置或文件路径，具体取决于设备或协议。
目标 IP	机密数据的目标 IP 地址。目标 IP 地址仅针对特定网络事件而显示。
源	违规的原始文件或数据。源主要出现在文件传输型事件中。
发送者	网络违规的机密数据的发送者。
接受者	网络违规的机密数据的目标接受者。
FTP 用户名	违规 FTP 传输的源用户名。
附件	发送的相关文件或附件（针对网络事件）。 如果您的管理员已将 Symantec Data Loss Prevention 配置为保留端点事件数据，则您可以单击文件名来查看文件内容。
数据所有者	机密数据的指定所有者。
数据所有者电子邮件地址	机密数据所有者的电子邮件地址。

部分	说明
访问信息	可用的 ACL 信息。仅适用于 Endpoint Discover 和 Endpoint Prevent 本地驱动器监视。 请参见第 806 页的“ 事件快照访问信息部分 ”。

事件快照的其他部分对所有 Symantec Data Loss Prevention 产品均通用。通用部分包括：

- 事件快照匹配
请参见第 806 页的“[事件快照匹配项部分](#)”。
- 事件快照策略部分
请参见第 805 页的“[事件快照策略部分](#)”。
- 事件快照关联部分
请参见第 805 页的“[事件快照关联选项卡](#)”。
- 事件快照属性部分。（只有系统管理员已配置自定义属性，此部分才会显示。）
请参见第 805 页的“[事件快照策略部分](#)”。
- 事件快照历史记录部分
请参见第 804 页的“[事件快照历史记录选项卡](#)”。

端点事件快照还包含两个在其他产品线中不常见的部分。这两个部分是：

- 目标或协议特定的信息
请参见第 741 页的“[端点事件目标或协议特定的信息](#)”。
- 关于 Endpoint Prevent 响应规则的报告
请参见第 740 页的“[关于 Endpoint Prevent 响应规则的报告](#)”。

关于 Endpoint Prevent 响应规则的报告

如果在端点计算机上的用户活动触发了多个响应规则，Symantec Data Loss Prevention 会根据建立的优先顺序来确定要应用的策略。仅执行与现行策略相关联的响应规则。Symantec Data Loss Prevention 为违反的所有策略创建事件。它指示（在相关事件快照中）响应规则被取代。

请参见第 736 页的“[端点事件快照](#)”。

默认情况下，以下列表为 Endpoint Prevent 事件的主要优先顺序：

- 阻止
- 用户取消
- Endpoint FlexResponse

■ 通知

注意: 对于 Endpoint Discover, “隔离”事件总是优先于 Endpoint FlexResponse 事件。

请注意关于报告被取代事件的下列行为:

- 被取代的“端点阻止”或“用户取消”事件的快照仍显示“已阻止”图标，因为 Symantec Data Loss Prevention 确实阻止了所述的内容。此图标还可指示在用户选择阻止内容后，内容是否已阻止。或者，此图标会指示是否超出用户取消时间限制以及是否已阻止内容。
- 被取代的端点通知事件的快照不包含“通知”图标。“通知”图标不包括在内，因为 Symantec Data Loss Prevention 不显示在策略中配置的特定屏幕通知。
- 被取代的“端点隔离”事件的快照会显示“已阻止”图标，因为数据没有移出安全区域。此图标还可指示在用户选择阻止内容后，内容是否已阻止。或者，此图标会指示是否超出用户取消时间限制以及是否已阻止内容。事件快照的“历史记录”选项卡始终显示有关 Endpoint FlexResponse 规则是否成功的信息。
- 被取代的 Endpoint FlexResponse 事件的快照会显示“已阻止”图标，因为数据没有移出安全区域。此图标还可指示是否已激活“端点隔离”响应规则。

如果您已配置了 Endpoint Prevent 响应规则来显示屏幕上的通知，提示用户确认其操作，则下列陈述为真:

- Symantec Data Loss Prevention 在所有由包含被执行响应规则的策略生成的事件的快照中显示用户确认消息。
- Symantec Data Loss Prevention 在所有不包含已执行响应规则的被取代事件的快照中显示确认消息“被取代 - 是”。
- 如果没有用户输入确认信息（例如，如果用户访问远程计算机），则该确认信息为 N/A。

请参见第 727 页的“[网络事件快照](#)”。

请参见第 670 页的“[配置响应规则条件](#)”。

请参见第 777 页的“[关于事件报告](#)”。

请参见第 667 页的“[管理响应规则](#)”。

端点事件目标或协议特定的信息

根据事件类型，可以显示与事件快照关联的附加信息。

表 43-5 目标或协议特定的信息

目标或协议	说明
URL	对于网络事件，表示发生事件的 URL。
源 IP 和端口	对于网络事件，表示发生事件的端点计算机的 IP 地址或端口。仅当事件是在此端点计算机上创建时，才会显示该信息。
目标 IP 和端口	与事件关联的目标端点计算机的 IP 地址。仅当事件是在此端点计算机上创建时，才会显示该信息。
发件人/收件人电子邮件	对于电子邮件/SMTP 和 IM 事件，事件还包括发件人和收件人的电子邮件地址。仅当在发件人或收件人电子邮件地址上发生事件时，才显示发件人或收件人电子邮件地址。
主题	显示电子邮件/SMTP 邮件的主题行。
FTP 目标上的 FTP 用户名	对于 FTP 事件，显示 FTP 目标上的用户名。
服务器 IP	对于 FTP 事件，显示服务器 IP 地址。
文件名/位置	对于打印/传真事件，显示端点计算机上的文件名和文件位置。
打印作业名称	对于打印/传真事件，打印作业名称是生成事件的打印作业的文件名。
打印机名称/类型	对于打印/传真事件，仅当在无法通过“打印作业名称”命名文件或者文件是由 Internet 浏览器生成的时，才会显示打印机名称和类型。
应用程序窗口	对于剪贴板事件，应用程序窗口是从其获取剪贴板内容的应用程序名称。
标题栏	对于剪贴板事件，标题栏是从其复制数据的窗口。

请参见第 736 页的“[端点事件快照](#)”。

端点事件摘要报告

端点事件摘要报告提供有关那些按特定条件总结的端点事件的信息。您可以按一种或多种条件总结事件。单摘要报告由一个摘要条件组织，例如与该事件相关的策略。双摘要报告按两个或多个条件组织，例如策略和事件状态。

注意：端点报告仅显示 Endpoint Prevent 捕获的事件。来自 Endpoint Discover 的事件显示在 Network Discover 报告中。

要查看适用于报告的主要和次要摘要条件，请转至“摘要类型”链接。单击“编辑”。在“主要”和“次要”下拉菜单中，Symantec Data Loss Prevention 按字母顺序显示所有条件，其后为系统管理员定义的自定义条件。您可以从“主要”和“次要”下拉菜单中选择条件，然后单击“立即运行”创建新的摘要报告。摘要报告从主要摘要条件获取其名称。如果使用新条件重新运行报告，则报告名称也会相应改变。

请参见第 807 页的“[关于报告的过滤器和摘要选项](#)”。

摘要条目分为若干列。单击任意列标题，可基于该列的数据按字母数字顺序对其进行排序。要按倒序进行排序，请再次单击该列标题。

表 43-6 端点事件摘要报告详细信息

字段	说明
摘要条件	此列包含所选任意摘要条件的名称。如果同时选择了主要和次要摘要条件，则仅显示主要条件。
总计	与摘要项目相关的事件的总数。例如，在“策略摘要”中，此列提供了与每个策略相关的事件的总数。
高	与摘要项目相关的高严重性事件的数目。（所匹配规则的严重性设置确定严重性的级别。）
中	与摘要项目相关的中严重性事件的数目。
低	与摘要项目相关的低严重性事件的数目。
信息	与摘要项目相关的信息事件的数目。
条形图表	与摘要项目相关的事件（所有严重性）的数目的直观表示。该条形图表包含多个成比例的、带颜色的部分，代表各种严重性。

字段	说明
匹配项	与摘要项目相关的匹配总数。 在包含总计的任意严重性列中，可以单击总计，查看所选严重性的事件的列表。

配置 Endpoint Server 文件过滤器

可以为 Endpoint Server 监视器配置影响所监控内容类型的特定过滤器。Endpoint Server 过滤器仅影响文件类型。这些过滤器不会排除监视器。

Endpoint Server 过滤器页面分为以下三个部分：

- 过滤器操作
- 目标或协议
- 文件属性

“过滤器操作”部分允许您选择是否要过滤器监控以下属性。可以包含要监控的文件，也可以从相关协议或目标中排除文件。

可以选择以下选项之一：

- 监控
- 忽略(不监控)

“端点通道”部分允许您选择希望过滤的目标、协议或应用程序。必须至少选择一个选项。过滤器应用于所选的每个目标、协议或应用程序类型。

可以选择以下选项：

- 可移动存储
- CD/DVD
- 本地驱动器
- 应用程序文件访问
- 电子邮件附件
- HTTP/HTTPS 附件
- IM 文件传输
- FTP 传输
- 应用程序文件访问

“应用程序文件访问”选项允许您监控出现在“应用程序监控”页面上的所有应用程序。

请参见第 1207 页的“[关于应用程序监控](#)”。

“文件属性”部分中可以指定要应用的过滤器。

可以指定以下过滤器属性：

■ 大小

您可以指定要扫描的文件的最小、最大或基线大小。

■ 类型

指定要过滤的确切文件类型。此部分预先加载了常见文件类型。如果要指定任何其他文件类型，请在单独行上输入每个文件类型。

■ 目标上的文件路径

指定要分析的文件系统路径，每行键入一个。如果指定要包含任何路径，Symantec Data Loss Prevention 将仅监控这些路径下的文件。如果将此字段留空，Symantec Data Loss Prevention 将监控您可能已在别处指定的特定文件之外的所有文件。此过滤器仅适用于本地驱动器监控。

此部分只适用于本地驱动器上的监控。如果未在“目标或协议”部分中选择“本地驱动器”，则无法编辑“目标上的文件路径”属性。

端点监控过滤器总是按照其出现的顺序运行。可以对“顺序”字段重新编号来重新排列过滤器的运行顺序。

请参见第 1155 页的“[关于代理配置](#)”。

补救移动事件

本章节包括下列主题：

- [Mobile Prevent 事件报告](#)
- [Mobile Prevent 事件快照](#)
- [Mobile Prevent 事件列表](#)
- [Mobile Prevent 事件列表 - 操作](#)
- [Mobile Prevent 事件列表 - 列](#)
- [Mobile Prevent 事件快照 - 标题和导航](#)
- [Mobile Prevent 事件快照 - 常规信息](#)
- [Mobile Prevent 事件快照 - 匹配项](#)
- [Mobile Prevent 事件快照 - 属性](#)
- [Mobile Prevent 摘要报告](#)

Mobile Prevent 事件报告

使用 Mobile Prevent 事件报告可监视 Mobile Prevent 事件并对其做出响应。您可以保存、发送、导出或调度 Symantec Data Loss Prevention 报告。

在 Enforce Server 管理控制台中的“事件”菜单上，单击“移动设备”。此事件报告会显示所有目标为移动设备的所有事件。您可以选择针对以下内容的标准报告：所有事件、新事件、策略摘要、按策略的状态或高风险发送者。

摘要和过滤器选项可以选择要显示的事件。

请参见第 807 页的“[关于报告的过滤器和摘要选项](#)”。

您可以使用过滤器和摘要组合创建自定义报告来确定要补救的事件。

请参见第 786 页的“[关于自定义报告和控制板](#)”。

请参见第 748 页的“[Mobile Prevent 事件列表](#)”。

Mobile Prevent 事件快照

事件快照提供有关特定事件的详细信息。快照中会显示常规事件信息、在拦截的文本中检测到的匹配项以及事件属性。通过快照还可以执行已配置的任何智能响应规则。

事件快照分为三个窗格，并带有导航和智能响应选项。单击链接可查看更多有关事件快照的帮助：

了解详细信息

导航和智能响应选项

参见以下部分

请参见第 752 页的“[Mobile Prevent 事件快照 - 标题和导航](#)”。

常规事件信息（左侧窗格）

请参见第 752 页的“[Mobile Prevent 事件快照 - 常规信息](#)”。

事件中的匹配项（中间窗格）

请参见第 754 页的“[Mobile Prevent 事件快照 - 匹配项](#)”。

属性（右侧窗格）

请参见第 754 页的“[Mobile Prevent 事件快照 - 属性](#)”。

Mobile Prevent 事件列表

Mobile Prevent 事件列表可显示多条移动事件记录，这些记录包含事件的严重性、关联策略、匹配数和事件状态等信息。单击事件列表的某行可查看有关特定事件的更多详细信息。单击左侧的复选框可选择要修改或补救的特定事件（或事件组）。

注意：单击“全选”时要谨慎。此操作会选中报告中的所有事件（不只是当前页面的事件）。随后应用的任何事件命令会影响所有事件。如果只选择当前页面上的事件，可选择事件列表左上角的复选框。

事件信息分为多个列。单击任意列标题，可基于该列的数据按字母数字顺序对其进行排序。要按倒序进行排序，请再次单击该列标题。默认情况下，Symantec Data Loss Prevention 按日期对事件进行排序。

“类型”列显示了指示移动事件类型的图标。[表 44-1](#) 介绍了这些图标。

表 44-1 Mobile Prevent 事件的类型

图标	说明
	HTTP Symantec Data Loss Prevention 还会检测通过 HTTP 隧道传输的 Yahoo 和 MSN IM 通信。
	添加第二个图标表示基于 Web 的电子邮件的附件。
	HTTPS
	FTP

此列还表示是阻止了通信还是更改了通信。表 44-2 显示了可能的值。

表 44-2 Mobile Prevent 阻止或更改的状态

图标	说明
无图标。	如果没有阻止通信，该列为空白。
	表示 Symantec Data Loss Prevention 阻止了包含匹配文本的通信。
	表示 Symantec Data Loss Prevention 从 Web 发布或基于 Web 的电子邮件中删除了机密数据。此图标还可以表示文件已上传到网站或附加到基于 Web 的电子邮件。
	表示 Symantec Data Loss Prevention 添加或修改了生成事件的邮件的标头。

使用以下链接可了解有关 Mobile Prevent 事件列表页的详细信息：

了解详细信息

事件列表表格中的列

要对选定事件执行的操作

特定事件的详细信息

查看所有移动事件的摘要

所有 Symantec Data Loss Prevention 报告共同具有的功能

参见此部分

请参见第 750 页的“[Mobile Prevent 事件列表 - 列](#)”。

请参见第 750 页的“[Mobile Prevent 事件列表 - 操作](#)”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

请参见第 755 页的“[Mobile Prevent 摘要报告](#)”。

请参见第 777 页的“[关于事件报告](#)”。

请参见第 801 页的“[常见事件报告功能](#)”。

请参见第 789 页的“[保存自定义事件报告](#)”。

Mobile Prevent 事件列表 - 操作

您可以选择一个或多个事件，然后使用“事件操作”下拉列表中的命令对其进行补救。事件命令如下：

操作	说明
添加注释	选择此选项可打开一个对话框，键入注释，然后单击“确定”。
存档	选择下列存档操作之一以设置所选事件的存档状态： <ul style="list-style-type: none">■ 存档事件 - 将所选事件标记为已存档。■ 还原事件 - 将所选事件还原为非存档状态。■ 不存档 - 禁止对所选事件进行存档。■ 允许存档 - 允许对所选事件进行存档。
删除事件	请参见第 823 页的“ 关于事件存档 ”。
导出所选项: CSV	选择此选项可删除指定的事件。
导出所选项: XML	选择此选项可将指定事件保存于可在常用应用程序（例如 Microsoft Excel）中显示的逗号分隔文本 (.csv) 文件或 XML 文件中。
查找属性	使用查找插件查找事件自定义属性。
设置属性	选择此选项可设置选定事件的属性。
设置严重性	选择此选项可设置严重性。
设置状态	选择此选项可设置状态。

请参见第 713 页的“[关于事件补救](#)”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

Mobile Prevent 事件列表 - 列

事件信息分为多个列。单击任意列标题，可基于该列的数据按字母数字顺序对其进行排序。要按倒序进行排序，请再次单击该列标题。默认情况下，Symantec Data Loss Prevention 会按日期列出事件。

报告包括以下列：

- 用于选择要补救的事件的复选框。

您可以选择一个或多个要应用列表顶部的“事件”下拉菜单中的命令的事件。单击列顶部的复选框，选中当前页上的所有事件。（请注意，您也可以单击最右侧的“全选”，选择报告中的“全部”事件。）

■ **类型**

检测匹配所使用的协议。

■ **主题/发送者/接受者**

邮件主题、发送者电子邮件地址或 IP 地址、接受者电子邮件地址或者 URL。

■ **发送时间**

发送邮件的日期和时间。

■ **ID/策略**

Symantec Data Loss Prevention 事件 ID 号和记录事件所依据的策略。

■ **匹配项**

事件中的匹配数。

■ **严重性**

由事件所匹配规则的严重性设置确定的事件严重性。

可能的值如下：

图标	说明
	高
	中
	低
	仅供参考

■ **状态**

当前事件状态。

可能的值如下：

■ **新建**

■ **进行中**

■ **已提报**

■ **误报**

■ **配置错误**

■ **已解决**

您或管理员可在“属性设置”页面上添加新的状态标识。

Mobile Prevent 事件快照 - 标题和导航

下列页面导航工具会显示在事件快照顶部附近：

上一个	显示源报告中的上一个事件。
下一个	显示源报告中的下一个事件。
	返回至源报告（单击此链接可到达此屏幕）。
	使用任意新数据更新快照，例如“历史记录”部分中的新注释或者修改后的状态。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

Mobile Prevent 事件快照 - 常规信息

快照的左侧部分显示常规事件信息。您可以单击许多值来查看根据该值过滤的事件列表。一个图标可能会显示在“状态”下拉列表旁边，指示对生成事件的请求进行了阻止还是对其进行修改。

请参见第 724 页的[表 42-2](#)。

事件的当前状态和严重性会显示在快照标题的右侧。要更改其中一个当前值，请单击该值并从下拉列表中选择另一个值。

常规信息窗格的其他部分被分成四个选项卡。

- 关键信息
- 历史记录
- 注释
- 关联

此部分的信息会分为以下类别（并非会显示每个事件类型的所有类别）：

表 44-3 事件常规信息选项卡

选项卡名称	说明
关键信息	<p>“关键信息”选项卡显示事件中违反的策略。它也显示了策略匹配项以及每个策略规则匹配项的总数。单击策略名称以查看违反策略的所有事件的列表。单击“查看策略”可查看该策略的只读版本。</p> <p>此部分也列出了同一文件违反的其他策略。要查看与特定策略关联的事件的快照，请单击策略名称旁的“转至事件”。要看该文件所创建的事件的列表，请单击“显示全部”。</p> <p>“关键信息”选项卡也包括下列信息：</p> <ul style="list-style-type: none"> ■ 记录该事件的检测服务器的名称。 ■ 邮件发送的日期和时间。 ■ 发送者电子邮件或 IP 地址。 ■ 收件人的电子邮件或 IP 地址。 ■ SMTP 标题或 NNTP 主题标题。 ■ 附件文件名。单击可打开或保存此文件。 如果响应规则告知 Symantec Data Loss Prevention 放弃原始邮件，则您无法查看附件。 ■ 负责补救事件的人员（“数据所有者名称”）。此字段必须手动设置。系统可自动将报告发送给数据所有者以进行补救。 如果单击显示为超链接的“数据所有者名称”，将会显示按“数据所有者名称”进行过滤后的事件列表。 ■ 负责补救事件的人员的电子邮件地址（“数据所有者电子邮件地址”）。此字段必须手动设置。 如果单击“数据所有者电子邮件地址”超链接，将显示按“数据所有者电子邮件地址”过滤的事件列表。
历史记录	<p>查看对事件执行的操作。对于每个操作，Symantec Data Loss Prevention 会显示操作的日期和时间、参与者（用户或服务器）以及操作或注释。</p> <p>请参见第 716 页的“执行智能响应规则”。</p> <p>请参见第 667 页的“管理响应规则”。</p>
注释	查看您或其他用户已添加到事件中的任何注释。单击“添加注释”可以添加注释。

选项卡名称	说明
关联	<p>您可以查看共享当前事件属性的事件的列表。例如，可查看单个帐户生成的所有事件的列表。Symantec Data Loss Prevention 显示与单个属性匹配的关联的列表。单击属性值可以查看与这些值相关的事件的列表。</p> <p>要搜索具有相同属性的其他事件，请单击“查找类似项”。在显示的“查找类似事件”对话框中，请选择所需的搜索属性。然后单击“查找事件”。</p>

请参见第 748 页的[“Mobile Prevent 事件快照”](#)。

Mobile Prevent 事件快照 - 匹配项

在常规信息下，Symantec Data Loss Prevention 显示邮件内容（如果适用）和导致事件的匹配项。Symantec Data Loss Prevention 显示下列类型的邮件内容，具体取决于协议类型：

协议	邮件内容
HTTP/S	HTTP/S 请求的名称值对
FTP	不显示任何内容

匹配项以黄色突出显示，并根据在其中检测到这些匹配项的邮件组件（如标题、正文或附件）进行组织。Symantec Data Loss Prevention 显示每个邮件组件的所有相关匹配项。将按照原始文本中显示的顺序来显示匹配项。要查看触发匹配项的规则，请单击突出显示的匹配项。

请参见第 411 页的[“关于相似度阈值和相似度评分”](#)。

请参见第 748 页的[“Mobile Prevent 事件快照”](#)。

Mobile Prevent 事件快照 - 属性

注意：只有系统管理员已配置自定义属性，此部分才会显示。

如果已指定，则可以查看自定义属性列表及其值。单击属性值以查看根据该值过滤的事件列表。要添加新值或编辑现有值，请单击“编辑”。在显示的“编辑属性”对话框中，键入新值并单击“保存”。

请参见第 836 页的[“手动设置自定义属性的值”](#)。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

Mobile Prevent 摘要报告

Mobile Prevent 摘要报告提供有关在您的移动设备中生成的事件的摘要信息。您可以使用一个或两个摘要条件组织报告。单摘要报告由一个摘要条件组织，例如与该事件相关的策略。双摘要报告由两个条件组织，例如策略和事件状态。

要查看可供当前报告使用的主要条件和辅助摘要条件，请单击“**高级过滤器和摘要**”栏。该栏位于报告顶部附近。“**摘要类型：**”列表框显示主要条件和辅助摘要条件。在每个列表框中，Symantec Data Loss Prevention 都会以字母顺序显示所有检测条件，后跟您的系统管理员已定义的任何自定义条件。摘要报告的名称取自主要摘要条件（首个列表框的值）。如果使用新条件重新运行报告，则报告名称也会相应改变。

摘要条目分为若干列。单击任意列标题，可基于该列的数据按字母数字顺序对其进行排序。要按倒序进行排序，请再次单击该列标题。

表 44-4 摘要报告列

列名	说明
<i>summary_criterion</i>	此列针对主要摘要条件命名。它列出主要和辅助摘要（针对双摘要）项目。在“策略摘要”中，此列的名称为“策略”，并列出多种策略。单击摘要项目以查看与此项目相关的事件列表。
总计	与摘要项目相关的事件的总数。在“策略摘要”中，此列提供了与每个策略相关的事件的总数。
高	与摘要项目相关的高严重性事件的数目。（所匹配规则的严重性设置确定事件的严重性。）
中	与摘要项目相关的中严重性事件的数目。
低	与摘要项目相关的低严重性事件的数目。
信息	与摘要项目相关的信息性事件的数目。
条形图表	与摘要项目相关的事件（所有严重性）的数目的直观表示。该条形图表分解为多个成比例的、带颜色的部分（代表各种严重性）。
匹配项	与摘要项目相关的匹配总数。

在包含总计的任意严重性列中，可以单击总计，查看所选严重性的事件的列表。

请参见第 801 页的“[常见事件报告功能](#)”。

请参见第 779 页的“[关于控制板报告和执行摘要](#)”。

请参见第 777 页的“[关于事件报告](#)”。

请参见第 789 页的“[保存自定义事件报告](#)”。

补救发现事件

本章节包括下列主题：

- [关于 Network Discover 的报告](#)
- [关于 Network Discover 的事件报告](#)
- [发现事件报告](#)
- [发现事件快照](#)
- [解决 Firefox 浏览器中的链接访问问题](#)
- [发现事件列表](#)
- [Network Discover 事件操作](#)
- [Network Discover 事件条目](#)
- [发现摘要报告](#)

关于 Network Discover 的报告

Symantec Data Loss Prevention 具有用于事件、Network Discover 目标、扫描详细信息与扫描历史记录的报告。

Network Discover 事件报告包含关于暴露的机密数据的详细信息。

请参见第 962 页的“[关于 Network Discover 的事件报告](#)”。

如需 Network Discover 目标与扫描历史记录的相关信息，请转至“管理”>“发现扫描”>“发现目标”，然后从列表中选择其中一个发现目标。如需

&pN.NetworkDiscover 扫描详细信息的相关信息，请转至“管理”>“发现扫描”>“扫描历史记录”，然后从列表中选择其中一个发现扫描。

请参见第 943 页的“[管理 Network Discover 目标扫描](#)”。

表 45-1 列出了 Network Discover 报告。

表 45-1 Network Discover 报告

报告	导航
NetworkDiscover 目标	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“发现目标”上。 请参见第 944 页的 “关于 Network Discover 扫描目标列表” 。
扫描状态	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“发现服务器”上。 请参见第 953 页的 “查看 Network Discover 服务器状态” 。
扫描历史记录（单一目标）	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“发现目标”上。单击“扫描状态”列中的链接，以查看特定扫描目标的历史记录。 请参见第 947 页的 “关于 Network Discover 扫描历史记录” 。
扫描历史记录（所有目标）	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“扫描历史记录”上。 请参见第 947 页的 “关于 Network Discover 扫描历史记录” 。
扫描详细信息	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“扫描历史记录”上。单击“扫描状态”列中的链接，以查看扫描详细信息。 请参见第 950 页的 “关于 Network Discover 扫描详细信息” 。

关于 Network Discover 的事件报告

使用事件报告可追踪 Network Discover 事件并对其作出响应。您可以保存、发送、导出或调度 Symantec Data Loss Prevention 报告。

请参见第 775 页的[“关于 Symantec Data Loss Prevention 报告”](#)。

在 Enforce Server 管理控制台中的“事件”菜单上，单击“发现”。此事件报告将显示所有发现目标的所有事件。您可以选择针对以下内容的标准报告：所有事件、新事件、目标摘要、按目标的策略、按目标的状态或有风险的前几个共享。

摘要和过滤器选项可以选择要显示的事件。

请参见第 786 页的[“关于自定义报告和控制板”](#)。

请参见第 807 页的[“关于报告的过滤器和摘要选项”](#)。

您可以使用过滤器和摘要组合创建自定义报告来确定要补救的事件。

例如，您可以创建下列报告：

- 反映每个补救类别中的事件数量的摘要报告。
选择摘要“**保护状态**”。
- 已通过复制或隔离补救的所有事件的报告。
选择值为“**已复制文件**”和“**已隔离文件**”的过滤器“**保护状态**”。
- 以前未出现过的 Network Discover 事件的报告（用于标识这些事件并通知数据所有者对它们进行补救）。
选择过滤器“**出现过**”。将值设置为“**否**”。
- 仍然存在的 Network Discover 事件的报告（用于了解要提报补救哪些事件）。
选择过滤器“**出现过**”。将值设置为“**是**”。
- 使用摘要过滤器（如自首次检测后的月数）的报告。
选择摘要“**自首次检测后的月数**”。

发现事件报告

使用 Network Discover 事件报告可监控 Network Discover 事件并对其作出响应。您可以保存、发送、导出或调度 Symantec Data Loss Prevention 报告。

在 Enforce Server 管理控制台中的“事件”菜单上，单击“发现”。此事件报告将显示所有发现目标的所有事件。您可以选择针对以下内容的标准报告：所有事件、新事件、目标摘要、按目标的策略、按目标的状态或有风险的前几个共享。

摘要和过滤器选项可以选择要显示的事件。

请参见第 802 页的“[事件报告过滤器和摘要选项](#)”。

您可以使用过滤器和摘要组合创建自定义报告来确定要补救的事件。

请参见第 786 页的“[关于自定义报告和控制板](#)”。

Network Discover 具有以下类型的报告：

- 事件列表
请参见第 763 页的“[发现事件列表](#)”。
- 事件摘要
请参见第 767 页的“[发现摘要报告](#)”。
- 事件快照
请参见第 760 页的“[发现事件快照](#)”。

发现事件快照

事件快照提供有关特定事件的详细信息。快照中会显示常规事件信息、在截获的文本中检测到的匹配数，以及策略、属性和事件历史记录的详细信息。您也可以在“**关联**”区域中搜索类似事件。

快照标题下会显示当前状态和严重性。要更改其中一个当前值，请单击该值并从下拉列表中选择其他值。

可使用右上角的图标打印报告，或者通过电子邮件发送报告。要发送报告，您或管理员必须先在系统设置中启用报告分发功能。

请参见第 135 页的“[配置 Enforce Server 以发送电子邮件警报](#)”。

如果设置了任何智能响应规则，Symantec Data Loss Prevention 会显示一个补救栏，其中包括用于执行规则的按钮。根据智能响应规则的数量，可能还会显示下拉菜单。

请参见第 713 页的“[关于事件补救](#)”。

事件数据分为以下部分：

- “关键信息”选项卡

- 策略匹配项

请参见第 805 页的“[事件快照策略部分](#)”。

- 事件详细信息

包括以下详细信息：

服务器	检测到事件的发现服务器的名称。
目标	Network Discover 目标名称。
扫描	注册事件的扫描的日期和时间。
检测日期	检测到事件的日期和时间。
出现过	如果先前未曾检测到该事件，则为“否”。如果先前曾检测到该事件，则为“是”。
主题	集成的 Exchange 扫描的电子邮件主题。
发送者	集成的 Exchange 扫描的电子邮件发送者。
接受者	集成的 Exchange 扫描的电子邮件接受者。

文件位置	文件、存储库或项目的位置。 单击“转至文件”查看项目或文件，或者单击“转至目录”查看目录。如果查看 Endpoint Discover 事件，则不会看到“转至文件”或“转至目录”链接。 在 Firefox 浏览器中，如果不进行附加设置，这些链接不会起作用。 请参见第 762 页的“ 解决 Firefox 浏览器中的链接访问问题 ”。
已存档	显示事件的存档状态、事件是否可存档，并且您可以切换事件的“ 不存档 ”标志。请参见第 823 页的“ 关于事件存档 ”。
URL	对于 SharePoint，此 URL 是 SharePoint 服务器上的项目。单击此 URL 可转至 SharePoint 服务器上的项目。
文档名称	文件或项目名称
文件所有者	文件或项目的创建者。 对于 SharePoint 和 Exchange 事件快照，文件所有者被列为未知，因为它不适用于这些目标类型。
提取日期	运行自定义目标适配器的日期（仅适用于自定义目标）。
已扫描计算机	已扫描计算机的主机名。 对于 SharePoint，此名称是 Web 应用程序名称。
Notes 数据库	Lotus Notes 数据库的名称（仅适用于 Lotus Notes）。
文件创建时间	创建文件或项目的日期和时间。
上次修改时间	上次更改文件或项目的日期和时间。
上次访问时间	用户上次访问文件或项目的日期和时间。 对于 SharePoint，此日期无效。
数据所有者名称	负责补救事件的人员。此字段必须手动设置，或使用查找插件设置。 系统可自动将报告发送给数据所有者以进行补救。 如果单击“ 数据所有者名称 ”超链接，将显示按“ 数据所有者名称 ”过滤的事件列表。
数据所有者电子邮件地址	负责补救事件的人员的电子邮件地址。此字段必须手动设置，或使用查找插件设置。 如果单击“ 数据所有者电子邮件地址 ”超链接，将显示按“ 数据所有者电子邮件地址 ”过滤的事件列表。

■ 访问信息

请参见第 806 页的“[事件快照访问信息部分](#)”。

对于 SharePoint 事件快照，权限级别将显示 SharePoint 的权限，例如“参与讨论”或“设计”。事件快照中的列表仅显示前 50 个条目。所有 ACL 条目都可以导出为 CSV 文件。权限是以逗号分隔的。不记录或显示具有“受限访问”权限级别的用户或组。

■ 邮件正文

对于 SharePoint 列表项目，邮件正文在列表中显示名称和值对。

■ 匹配项和文件内容

请参见第 806 页的“[事件快照匹配项部分](#)”。

■ 属性

请参见第 804 页的“[事件快照属性部分](#)”。

■ 历史记录选项卡

请参见第 804 页的“[事件快照历史记录选项卡](#)”。

■ 注释选项卡

注释选项卡显示此事件的所有注释。

■ 关联选项卡

请参见第 805 页的“[事件快照关联选项卡](#)”。

请参见第 759 页的“[发现事件报告](#)”。

解决 Firefox 浏览器中的链接访问问题

在 Firefox 浏览器中，当您查看文件系统事件时，“文件位置”字段旁边的“转至文件”和“转至目录”链接不起作用。

要转至文件或目录，请采取以下操作之一：

右键单击“转至文件”和“转至目录”链接，然后选择“复制链接位置”。打开一个新的浏览器窗口（或选项卡）并将该 URL 粘贴到地址栏中。按 Enter。每次您要使用这些链接时，都必须执行此复制和粘贴操作。

在使用 Firefox 的计算机（而不是 Enforce Server 主机）上修改 Firefox 用户首选项。

修改 Firefox 用户首选项

- 1 转至 Firefox 用户首选项目录。

对于 Windows Vista、XP 或 2000，此目录为 C:\Documents and Settings\user_name\Application Data\Mozilla\Firefox\Profiles\xxxxxxx.default，其中 user_name 是您的用户名，xxxxxxx 是随机字符串。对于 Windows 95、98 或 ME，此目录为 C:\WINDOWS\Application Data\Mozilla\Firefox\Profiles\xxxxxxx.default。

- 2 查找 user.js 文件。如果不存在，则使用文本编辑器创建该文件。如果存在，请将其打开。（请注意，您可以使用 .txt 文件扩展名创建或重命名该文件，以便使用文本编辑器对其进行编辑。）
- 3 添加以下几行：

```
user_pref("capability.policy.policynames", "localfilelinks");
user_pref("capability.policy.localfilelinks.sites", "enforce_url");
user_pref("capability.policy.localfilelinks.checkloaduri.enabled",
          "allAccess");
```

其中 *enforce_url* 是在浏览器地址栏中显示的 Enforce Server URL，直到（但不包括）第一个斜杠（例如，<https://enforce.server.name>）。

- 4 保存文件（如果您为了编辑而对文件进行了更改，则使用 .js 文件扩展名重命名该文件），然后重新启动 Firefox。

发现事件列表

Network Discover 事件列表显示了在 Network Discover 扫描期间报告的事件（包括来自 Endpoint Discover 的事件）。各个事件记录包含严重性、关联策略、匹配数和状态等信息。

请参见第 765 页的“[Network Discover 事件条目](#)”。

可以单击任意事件以查看包含更多详细信息的快照。

您可以选择要修改或补救的特定事件（或事件组）。

请参见第 763 页的“[Network Discover 事件操作](#)”。

请参见第 759 页的“[发现事件报告](#)”。

Network Discover 事件操作

您可以选择一个或多个事件，然后使用“事件操作”下拉列表中的命令对其进行补救。

事件命令如下：

■ **添加注释**

选择此选项可打开一个对话框，键入注释，然后单击“确定”。

■ **存档**

选择下列存档操作之一以设置所选事件的存档状态：

■ **存档事件** - 将所选事件标记为已存档。

■ **还原事件** - 将所选事件还原为非存档状态。

■ **不存档** - 禁止对所选事件进行存档。

■ **允许存档** - 允许对所选事件进行存档。

请参见第 823 页的“[关于事件存档](#)”。

■ **删除事件**

选择此选项可删除指定的事件。

■ **设置属性**

选择此选项可设置选定事件的属性。

■ **导出所选项: CSV**

选择此选项可将指定事件保存在可在多个常见应用程序（例如 Microsoft Excel）中显示的逗号分隔文本 (.csv) 文件中。

■ **导出所选项: XML**

选择此选项可将指定事件保存在 XML 文件中，该 XML 文件可在多个常用应用程序中显示。

■ **查找属性**

使用查找插件查找事件自定义属性。

■ **设置数据所有者**

设置数据所有者名称或电子邮件地址。数据所有者是负责补救事件的人员。

系统可自动将报告发送给数据所有者以进行补救。

■ **设置严重性**

选择此选项可设置严重性。

■ **设置状态**

选择此选项可设置状态。

■ **运行智能响应**

选择此选项可运行您或管理员配置的智能响应规则。

请参见第 763 页的“[发现事件列表](#)”。

Network Discover 事件条目

事件信息分为多个列。

单击任意列标题，可基于该列的数据按字母数字顺序对其进行排序。要按倒序进行排序，请再次单击该列标题。

报告包括以下列：

- 用于选择要补救的事件的复选框。

您可以选择一个或多个要应用“事件操作”下拉菜单中的命令的事件。

单击列顶部的复选框，选中当前页上的所有事件。

可以单击最右侧的“全选”来选择报告中的所有事件。

注意：使用“全选”时要谨慎。单击此选项会选择报告中的所有事件（不只是当前页面中的事件），随后应用的任何事件命令将会影响所有事件。您可能需要配置 `maximum-incident-batch-size` 属性以限制服务器 FlexResponse 插件一次可处理的事件数。

请参见第 968 页的[“将服务器 FlexResponse 插件添加到插件属性文件”](#)。

■ 类型

在其中检测到匹配的目标类型。

每个图标代表一个目标类型。

如果应用了任何响应规则，此列还会显示补救图标。

可能的值如下：

如果没有应用响应规则，则为空白

 已复制

 已隔离

 补救错误

将服务器 FlexResponse 操作用于自动响应规则或智能响应规则时，可能会出现以下图标之一：

 此事件已使用服务器 FlexResponse 操作成功补救。

 正在执行服务器 FlexResponse 操作。

 服务器 FlexResponse 操作存在错误。

对于其他事件类型，也会出现这些相同的图标，您可以对这些事件执行服务器 FlexResponse 操作。

请参见第 689 页的“[配置服务器 FlexResponse 操作](#)”。

■ 位置/目标/扫描

存储库或文件位置、目标名称、最近一次扫描的日期和时间

■ 文件所有者

文件所有者的用户名（例如，MYDOMAIN\Administrator）

■ ID/策略

Symantec Data Loss Prevention 事件编号和记录事件所依据的策略

■ 匹配项

事件中的匹配数

■ 严重性

由事件所匹配规则的严重性设置确定的事件严重性

可能的值如下：



高



中



低



仅供参考

■ 状态

当前事件状态

可能的值如下：

■ 新建

■ 进行中

■ 已提报

■ 误报

■ 配置错误

■ 已解决

如果之前出现过此事件，则在状态附近可能会出现以下图标：



如果此事件具有以前连接的事件，则会显示此图标。

您或管理员可在“属性设置”页面上添加新的状态标识。

请参见第 835 页的“[配置自定义属性](#)”。

请参见第 763 页的“[发现事件列表](#)”。

发现摘要报告

发现摘要报告提供了有关发现扫描期间所找到的事件的摘要信息。

如果正在运行 Endpoint Discover，则发现摘要报告还会包括 Endpoint Discover 事件。

可以过滤或总结报告中的选项。

请参见第 802 页的“[事件报告过滤器和摘要选项](#)”。

可以使用选定的格式来提取报告信息。

可以单击突出显示的元素（如“总计”列中的条目）以进一步了解详细信息。

图标可以在较长的报告之间提供导航。

请参见第 801 页的“[事件报告中的页面导航](#)”。

请参见第 759 页的“[发现事件报告](#)”。

使用分类事件

本章节包括下列主题：

- [分类事件列表](#)
- [分类事件快照](#)
- [分类事件摘要报告](#)

分类事件列表

分类事件列表仅适用于已部署 Symantec Data Classification for Enterprise Vault 解决方案的部署。该解决方案使用 Symantec Data Loss Prevention 来分类电子邮件，并将其转发到 Symantec Enterprise Vault 进行存档或运行其他操作。该解决方案独立于 Symantec Data Loss Prevention 进行授权。只有当消息违反所配置的已激活“启用分类测试模式”选项的策略时，在分类事件列表中才会显示分类事件。分类测试模式仅适用于验证策略是否匹配。在普通生产操作期间，分类测试模式应该禁用。

表 46-1 描述了分类事件列表中显示的列。

表 46-1 分类事件列表列

列	定义
类型	“类型”列显示的图标可将事件标识为分类电子邮件事件。当电子邮件包含附件时，还会显示一个附加图标。
主题/发送者/接受者	显示电子邮件的发送者、主题行和接受者列表。
发送时间	显示发送电子邮件的日期与时间。

列	定义
ID/策略	Symantec Data Loss Prevention 事件 ID 号和记录事件所依据的策略。
匹配项	事件中的匹配数。
严重性	由事件所匹配规则的严重性设置确定的事件严重性。 可能的值如下： <ul style="list-style-type: none">■ 高■ 中■ 低■ 仅供参考
状态	当前事件状态 可能的值如下： <ul style="list-style-type: none">■ 新建■ 进行中■ 已提报■ 误报■ 配置错误■ 已解决 您或管理员可在“属性设置”页面上添加新的状态标识。

分类事件快照

事件分类提供有关特定事件的详细信息。快照中会显示常规事件信息、在拦截的文本中检测到的匹配数，以及属性、事件历史记录和违反策略的详细信息。您也可以在“关联”区域中搜索类似的事件。

分类测试模式仅适用于验证策略是否匹配。在普通生产操作期间，分类测试模式应该禁用。

请参见第 769 页的“[分类事件列表](#)”。

快照标题下会显示当前状态和严重性。要更改其中一个当前值，请单击该值并从下拉列表中选择另一个值。如果任何操作图标与之关联，也将在此显示。

[表 46-2](#)描述了快照中存在的事件信息。

表 46-2 事件常规信息选项卡

选项卡名称	说明
关键信息	<p>“关键信息”选项卡显示事件中违反的策略。它也显示了策略匹配项以及每个策略规则匹配项的总数。单击策略名称以查看违反策略的所有事件的列表。单击“查看策略”可查看该策略的只读版本。</p> <p>此部分也列出了同一文件违反的其他策略。要查看与特定策略关联的事件的快照，请单击策略名称旁的“转至事件”。要查看该文件所创建的事件的列表，请单击“显示全部”。</p> <p>“关键信息”选项卡也包括下列信息：</p> <ul style="list-style-type: none"> ■ 记录该事件的检测服务器的名称。 ■ 邮件发送的日期和时间 ■ 发送者电子邮件或 IP 地址 ■ 接受者电子邮件或 IP 地址 ■ SMTP 标题或 NNTP 主题标题 ■ “已存档”字段会显示事件的存档状态、事件是否可存档，并可切换事件的“不存档”标志。 ■ 附件文件名。单击可打开或保存此文件。 如果响应规则告知 Symantec Data Loss Prevention 放弃原始邮件，则您无法查看附件。
历史记录	查看对事件执行的操作。对于每个操作，Symantec Data Loss Prevention 会显示操作的日期和时间、参与者（用户或服务器）以及操作或注释。
注释	查看您或其他用户已添加到事件中的任何注释。单击“添加注释”可以添加注释。
关联	<p>您可以查看共享当前事件属性的事件的列表。例如，可查看单个帐户生成的所有事件的列表。“关联”选项卡显示与单个属性匹配的关联的列表。单击属性值可以查看与这些值相关的事件的列表。</p> <p>要搜索具有相同属性的其他事件，请单击“查找类似项”。在显示的“查找类似事件”对话框中，请选择所需的搜索属性。然后单击“查找事件”。</p> <p>注意：关联的事件列表不会显示已存档的相关事件。</p>

在常规信息下，Symantec Data Loss Prevention 显示邮件内容（如果适用）和导致事件的匹配项。

匹配项以黄色突出显示，并根据在其中检测到这些匹配项的邮件组件（如标题、正文或附件）进行组织。Symantec Data Loss Prevention 显示每个邮件组件的相关匹配项总数。将按照原始文本中显示的顺序来显示匹配项。要查看触发匹配项的规则，请单击突出显示的匹配项。

分类事件摘要报告

即将推出

管理和报告事件

本章节包括下列主题：

- [关于 Symantec Data Loss Prevention 报告](#)
- [关于使用报告的策略](#)
- [设置报告首选项](#)
- [关于事件报告](#)
- [关于控制板报告和执行摘要](#)
- [查看控制板](#)
- [创建控制板报告](#)
- [配置控制板报告](#)
- [选择要包括在控制板中的报告](#)
- [关于摘要报告](#)
- [查看摘要报告](#)
- [创建摘要报告](#)
- [查看事件](#)
- [关于自定义报告和控制板](#)
- [使用 IT Analytics 管理事件](#)
- [过滤报告](#)
- [保存自定义事件报告](#)
- [调度自定义事件报告](#)

- 事件和系统报告的交付日程表选项
- 控制板报告的交付日程表选项
- 使用日期工具调度报告
- 编辑自定义控制板和报告
- 导出事件报告
- Network Monitor 的导出字段
- Network Discover 的导出字段
- Mobile Prevent for Web 的导出字段
- Endpoint Discover 的导出字段
- 删除事件
- 删除自定义控制板和报告
- 常见事件报告功能
- 事件报告中的页面导航
- 事件报告过滤器和摘要选项
- 通过电子邮件发送事件报告
- 打印事件报告
- 事件快照历史记录选项卡
- 事件快照属性部分
- 事件快照关联选项卡
- 事件快照策略部分
- 事件快照匹配项部分
- 事件快照访问信息部分
- 自定义事件快照页面
- 关于报告的过滤器和摘要选项
- 报告的常规过滤器
- 事件报告的摘要选项
- 报告的高级过滤器选项

关于 Symantec Data Loss Prevention 报告

使用事件报告跟踪和响应事件。当检测到与策略规则的检测参数匹配的数据时，Symantec Data Loss Prevention 会报告事件。

此类数据可能包括特定文件内容、电子邮件发送者或接受者、附件文件属性，或许许多其他类型的信息。

每块匹配检测参数的数据称为一个匹配条目，一个事件可能包括任意数量的匹配条目。

您可以在事件上设置事件存档标志以表示已经存档该事件。默认情况下，已存档的事件不会出现在事件报告中，但是您可以借助设置报告上的“高级过滤器”，在报告中加入它们。在报告中包括已存档的事件，这可能减慢报告活动的速度。请参见第 823 页的“[关于事件存档](#)”。

Symantec Data Loss Prevention 会跟踪所有检测服务器的事件。这些服务器包括 Network Discover Server、Network Monitor Server、Network Prevent for Email Server、Network Prevent for Web Server、Server 和 Endpoint Server。

您可以指定 Symantec Data Loss Prevention 在导航面板中显示的报告。

请参见第 777 页的“[设置报告首选项](#)”。

Symantec Data Loss Prevention 将提供以下类型的事件报告：

- 事件列表会显示包含严重性、相关策略、匹配数和状态等信息的各个事件记录。可以单击任何事件以便查看包含更多详细信息的快照。还可以选择要修改或补救的特定事件或事件组。
Symantec Data Loss Prevention 针对事件提供了单独的报告，可通过选择“网络”、“端点”、“移动设备”或“发现”进行查看。
- 摘要会提供有关系统上的事件的摘要信息。它们使用一个或两个摘要条件进行组织。单摘要报告使用一个摘要条件（例如与每个事件关联的策略）进行组织。双摘要报告使用两个条件（例如策略和事件状态）进行组织。默认情况下，已存档的事件不会出现在以摘要报告显示的计数中，但是在您可以设置“高级过滤器”来加入已存档的事件（请参见第 823 页的“[关于事件存档](#)”。）
- 控制板会组合来自多个报告的信息。这些信息包括代表各种事件列表和摘要内容的图表和事件总计。图表有时包含高严重性事件列表或摘要组列表。您可以单击报告 portlet（包含报告数据的各 tile）进一步查看报告的详细版本。
Symantec Data Loss Prevention 附带有“网络”、“端点”、“移动设备”以及“发现”事件的执行摘要。
执行摘要与控制板非常类似。它们之间的区别是您可以自定义控制板，但是不能自定义执行摘要。

您可以创建和保存所有报告（执行摘要除外）的自定义版本供后续使用。

请参见第 786 页的“[关于自定义报告和控制板](#)”。

Symantec Data Loss Prevention 在“事件报告”屏幕的各个部分显示报告，如下所示：

- “保存的报告”部分显示与您当前角色相关的任何共享报告。仅当您或其他具有您当前角色的用户创建了已保存报告时，才会显示该部分。
请参见第 786 页的“[关于自定义报告和控制板](#)”。
- “网络”部分包含 Symantec 提供的网络事件的事件列表、摘要以及控制板。
- “移动设备”部分包含 Symantec 提供的端点事件的事件列表、摘要以及控制板。
- “端点”部分包含 Symantec 提供的端点事件的事件列表、摘要以及控制板。端点报告包括端点捕获的事件，例如“端点阻止”和“端点通知”事件。
Endpoint Discover 捕获的事件显示在“发现”报告中。
- “发现”部分包含 Symantec 提供的 Network Discover 和 Endpoint Discover 事件的事件列表、摘要以及控制板。

关于使用报告的策略

许多公司会配置其 Symantec Data Loss Prevention 报告以配合以下的基本角色：

- 负责降低整体风险的主管，他们必须监视风险趋势并制订高级计划来应对这些趋势。
他们必须监视控制板和摘要报告，以便对组织中的数据丢失趋势有一个大致的了解。主管还必须制订降低风险的方案与计划，并将这些信息传达给策略作者与事件响应人员。主管通常必须通过电子邮件或其他一些导出的格式报告来监视报告。
Symantec Data Loss Prevention 控制板和摘要报告可让您监视组织的风险趋势。这些报告会提供高级事件概述。执行董事和管理人员能够快速地评估风险趋势，并建议策略作者和事件响应人员如何应对这些风险趋势。您可以查看现有摘要报告和控制板，并创建这些报告的自定义版本。
请参见第 779 页的“[关于控制板报告和执行摘要](#)”。
请参见第 783 页的“[关于摘要报告](#)”。
- 监视和响应特定事件的事件响应人员，例如，信息安全分析师或信息安全管理員。
响应人员会监视事件报告和快照，以对与特定策略组、组织部门或地理位置相关的事件进行响应。响应人员也可以创建策略以降低风险。您可以根据风险降低管理员的说明，或是根据自己跟踪事件的经验来生成这些策略。
请参见第 713 页的“[关于事件补救](#)”。

设置报告首选项

可以指定 Symantec Data Loss Prevention 显示在每个报告类型的导航面板中的报告。也可以指定初始窗口中显示的报告。

您可以指定哪些报告显示在左侧的导航面板中，还可以指定以当前角色登录时显示的报告。

设置报告首选项

1 在 Enforce Server 管理控制台中的“事件”菜单上，单击“事件报告”。

2 在显示的“事件报告”屏幕上，单击“编辑首选项”。

“编辑报告首选项”屏幕列出所有保存的报告（针对所有分配的角色）。

该屏幕也会列出“网络”、“端点”、“移动设备”和“发现”报告。

3 要指定当前角色的默认报告，请找到“*current_role*的主页”下拉列表并选择一个报告。无论何时使用当前角色首次登录，Symantec Data Loss Prevention 都会显示该报告。

4 要显示该列表中的报告，请选中该报告对应的“是否显示报告”框。要从列表中删除某个报告，请清除该报告所对应的“是否显示报告”。

选定的报告列表显示在每种类型报告的左侧导航面板中。

例如，要查看“网络”报告的列表，请在“事件”菜单上，单击“网络”。

5 更改首选项后，单击“保存”。

请参见第 786 页的[“关于自定义报告和控制板”](#)。

关于事件报告

使用事件报告跟踪和响应网络上的事件。当 Symantec Data Loss Prevention 检测到与有效策略中的检测规则相匹配的数据时，会报告事件。此类数据可能包括特定文件内容、电子邮件发送者或接受者、附件文件属性，或许多其他类型的信息。每段与检测规则相匹配的数据称为一个匹配项，并且一个事件中可能包含任意数量的匹配项。

注意：您可以配置在导航面板中显示哪些报告。要执行该操作，请转至“所有报告”，然后单击“编辑首选项”。

Symantec Data Loss Prevention 提供以下类型的事件报告：

事件列表	这些列表显示包含严重性、关联策略、匹配数和状态等信息的各个事件记录。可以单击任意事件以查看包含更多详细信息的快照。还可以选择要修改或补救的特定事件或事件组。
摘要	这些摘要显示按特定事件属性（如状态或关联策略）组织的事件总计。例如，“策略摘要”包括与事件关联的所有策略的行。每行包括策略名称、相关事件总数以及按严重性排列的事件总计。可以通过单击任意严重性总计来查看相关事件的列表。
双摘要	这些摘要显示按两个事件属性组织的事件总计。例如，策略趋势摘要显示按策略和按星期组织的所有事件。与策略摘要类似，每个条目包括策略名称、关联事件总数以及按严重性排序的事件总计。另外，每个条目中每周单独成一行，显示本周的事件总计以及按严重性排列的事件。
控制板和执行摘要	这些是组合了来自多个报告的信息的快速参考控制板。这些信息包括代表各种事件列表、摘要和双摘要内容的图表和事件总计。有时，高严重性事件列表或摘要组列表旁边会有图表。您可以单击其中的报告名称来进一步查看显示在控制板上的报告。
	Symantec Data Loss Prevention 随附了“网络”、“端点”和“发现”报告的执行摘要，这些摘要无法自定义。
	您可以自己创建控制板，并按照需要对其进行自定义。
自定义	列出了与当前角色关联的共享报告。（只有在您或其他用户以您当前角色创建了这些报告的情况下，才会显示这些报告。）
网络	列出了网络事件报告。
端点	列出了端点事件报告。端点报告包括“端点阻止”和“端点通知”之类的事件。
	来自 Endpoint Discover 的事件包含在发现报告中。
Discover	列出了 Network Discover 和 Endpoint Discover 事件报告。 文件夹风险报告显示了按风险优先级顺序排列的文件共享文件夹。风险评分是根据来自 Symantec Data Loss Prevention 事件的相关信息以及来自 VML Management Server 的信息而评定的。
	请参见《Symantec Data Loss Prevention Data Insight 操作指南》。
移动	列出 Mobile Prevent for Web 事件报告。
	请参见第 786 页的“ 关于自定义报告和控制板 ”。
	请参见第 801 页的“ 常见事件报告功能 ”。
	请参见第 727 页的“ 网络事件快照 ”。
	请参见第 760 页的“ 发现事件快照 ”。
	请参见第 736 页的“ 端点事件快照 ”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

请参见第 723 页的“[网络事件列表](#)”。

请参见第 763 页的“[发现事件列表](#)”。

请参见第 733 页的“[端点事件列表](#)”。

请参见第 719 页的“[移动事件变量](#)”。

关于控制板报告和执行摘要

控制板和执行摘要是快速参考报告屏幕，这些屏幕用于显示来自多个事件报告的摘要信息。

Symantec Data Loss Prevention 为“网络”、“端点”“移动设备”和“发现”事件报告各随附了一个执行摘要。

请参见第 777 页的“[关于事件报告](#)”。

控制板和执行摘要有两列报告。左列显示一个饼图和事件总计栏。右列显示与左列中相同的信息类型。右列还显示最重要的事件列表或关联事件总计的摘要项目列表。可根据严重性和匹配数对最重要的事件进行排序。可以单击某个报告查看所代表的完整报告。

控制板最多包含 6 个 portlet，每个均为指定的报告提供快速摘要。

Symantec Data Loss Prevention 包括四个执行摘要（类似于控制板）：“执行摘要 - 网络”、“执行摘要 - 端点”、“执行摘要 - 移动设备”以及“执行摘要 - 发现”。（控制板和执行摘要拥有相同格式，但执行摘要不是可定制的）。

对于具有特定安全职责的用户，您可以创建自定义控制板。如果选择共享控制板，则创建控制板所用角色中的所有用户均可访问该控制板。（请注意，管理员用户无法创建共享控制板。）

控制板有两列报告 portlet（包含报告数据的 tiles）。左列中的 portlet 显示一个饼图和总计栏。右列中的 portlet 显示与左列中相同的信息类型。但是，它们还显示最有意义的事件列表或者摘要条件及相关事件列表。事件按严重性和匹配数排列。摘要条件突出显示了任何高严重性事件总计。您最多可以选择三个报告包括在左列和右列中。

要创建自定义控制板，请在显示的“[事件报告](#)”屏幕中的导航面板的顶部单击“[事件报告](#)”，然后单击“[创建控制板](#)”。管理员只能创建专用控制板，但是其他用户可以决定是共享新控制板还是将其保留为专用。

请参见第 786 页的“[关于自定义报告和控制板](#)”。

要编辑任意自定义控制板的内容，请转至所需的控制板并单击靠近屏幕顶部的“[自定义](#)”。

请参见第 782 页的“[配置控制板报告](#)”。

要在登录时显示自定义控制板，请将其指定为默认登录报告。

请参见第 777 页的“[设置报告首选项](#)”。

查看控制板

此过程为您显示如何查看控制板。

查看控制板

- 1 在 Enforce Server 管理控制台中的“事件”菜单上，单击“事件报告”。在“报告”下，单击控制板的名称。

控制板包含多达 6 个 portlet，每个均提供特定报告摘要。

例如，“执行摘要-网络”控制板包含“网络策略摘要”、“高风险发送者”、“协议摘要”、“前几个接受者域”、“按周的状态”和“事件-全部”的portlet。

- 2 要查看某个 portlet 的整个报告，请单击该 portlet。

Symantec Data Loss Prevention 会显示相应的事件列表或摘要报告。

- 3 浏览整个事件列表或摘要报告。

请参见第 785 页的“[查看事件](#)”。

请参见第 783 页的“[关于摘要报告](#)”。

创建控制板报告

可以创建自定义控制板和报告。

如果您以非管理员身份登录，Symantec Data Loss Prevention 允许您选择是共享控制板还是将其保留为专用。

创建控制板

- 1 在 Enforce Server 管理控制台中的“事件”菜单上，单击“事件报告”。
- 2 在显示的“事件报告”屏幕上，单击“创建控制板”。

将显示“配置控制板”屏幕。

- 3 选择是共享控制板还是将其保留为专用。

如果选择共享控制板，则分配有创建控制板所使用角色的所有用户均可访问该控制板。

如果您以管理员身份登录，则不会看到此选项。

注意：Symantec Data Loss Prevention 会将管理员创建的所有控制板自动指定为专用。

单击“下一步”。

- 4 在“常规”部分中，对于“名称”，键入控制板的名称。

- 5 对于“说明”，键入控制板的可选说明。

- 6 在“交付日程表”部分，您可以重新生成控制板报告并将其发送到指定的电子邮件帐户。

如果没有在您的 Enforce Server 上设置 SMTP，则看不到“交付日程表”部分。

如果您已将系统配置为发送警报和报告，则可以设置时间，以便重新生成控制板报告，并将其发送到指定的电子邮件帐户。

请参见第 135 页的[“配置 Enforce Server 以发送电子邮件警报”](#)。

如果未将 Symantec Data Loss Prevention 配置为发送报告，请跳至下一步。

要设置日程表，请找到“交付日程表”部分，从“日程表”下拉列表中选择一个选项。（或者，可以选择“无日程表”。）

例如，选择“每周发送，于”。

输入选择“日程表”所需的数据。必要信息包含一个或多个电子邮件地址（以逗号分隔）。它也可能包含日历日期、某一天的某个时间、某一周的某一天、某个月的某一天或者发送的最后日期。

请参见第 793 页的[“控制板报告的交付日程表选项”](#)。

- 7 对于“左列”，可选择要在饼图中显示的内容。对于“右列”，还可以选择一个信息表。

请参见第 783 页的[“选择要包括在控制板中的报告”](#)。

从三个“左列(仅图表)”下拉列表中选择报告。然后从三个“右列(图表与表格)”下拉列表中选择报告。

- 8 单击“保存”。
- 9 稍后您可以从“编辑报告首选项”屏幕编辑控制板。

要在登录时显示某个自定义控制板，请在“编辑报告首选项”屏幕上将其指定为默认登录报告。

请参见第 795 页的[“编辑自定义控制板和报告”](#)。

配置控制板报告

您可以针对具有特定角色的用户创建自定义控制板。

控制板最多包含 6 个 portlet，每个均为指定的报告提供快速摘要。

如果选择共享控制板，则分配有创建控制板所使用角色的所有用户均可访问该控制板。

注意：管理员用户无法创建共享控制板。

配置自定义控制板

- 1 在“常规”部分中，对于“名称”，键入控制板的名称。
- 2 对于“说明”，键入控制板的可选说明。
- 3 在“交付日程表”部分，您可以重新生成控制板报告并将其发送到指定的电子邮件帐户。

如果没有在您的 Enforce Server 上设置 SMTP，则看不到“交付日程表”部分。

如果您已将系统配置为发送警报和报告，则可以设置时间，以便重新生成控制板报告，并将其发送到指定的电子邮件帐户。

请参见第 135 页的[“配置 Enforce Server 以发送电子邮件警报”](#)。

如果未将 Symantec Data Loss Prevention 配置为发送报告，请跳至下一步。

要设置日程表，请找到“交付日程表”部分，从“日程表”下拉列表中选择一个选项。（或者，可以选择“无日程表”。）

例如，选择“每周发送，于”。

输入选择“日程表”所需的数据。必要信息包含一个或多个电子邮件地址（以逗号分隔）。它也可能包含日历日期、某一天的某个时间、某一周的某一天、某个月的某一天或者发送的最后日期。

请参见第 793 页的[“控制板报告的交付日程表选项”](#)。

- 4 对于“左列”，可选择要在饼图中显示的内容。对于“右列”，还可以选择一个信息表。

请参见第 783 页的[“选择要包括在控制板中的报告”](#)。

从三个“左列(仅图表)”下拉列表中选择报告。然后从三个“右列(图表与表格)”下拉列表中选择报告。

- 5 单击“保存”。

- 6 稍后您可以从“编辑报告首选项”屏幕编辑控制板。

要在登录时显示某个自定义控制板，请在“编辑报告首选项”屏幕上将其指定为默认登录报告。

请参见第 795 页的[“编辑自定义控制板和报告”](#)。

选择要包括在控制板中的报告

控制板中有两列报告 portlet。

左列中的 portlet 显示一个饼图。

右列中的 portlet 显示与左列相同的信息，另外还显示最重要的事件列表或摘要。事件按严重性和匹配数排列。您可以显示一个包括摘要条件以及突出显示了高严重性事件总计的关联事件的列表。

最多可以分别选择三个要包括在左列和右列中的报告。

选择要包括的报告

- 1 从三个“左列(仅图表)”下拉列表中选择报告。
- 2 从三个“右列(图表与表格)”下拉列表中选择报告。
- 3 配置控制板后，单击“保存”。

请参见第 782 页的[“配置控制板报告”](#)。

关于摘要报告

Symantec Data Loss Prevention 提供两种类型的摘要报告：单摘要和双摘要。

单摘要显示按特定事件属性（如状态或相关策略）组织的事件总计。例如，策略摘要中每个具有相关事件的策略成一行。每行包括策略名称、相关事件总数以及按严重性排列的事件总计。

双摘要显示按两个事件属性组织的事件总计。例如，策略趋势摘要显示使用策略和周组织的所有事件。和在策略摘要中一样，每个条目包括策略名称、相关事件总

数，以及按严重性排列的事件总计。另外，每个条目中每周单独成一行，显示本周的事件总计以及按严重性排列的事件。

请参见第 811 页的“[事件报告的摘要选项](#)”。

您可以从任意事件列表创建自定义摘要报告。

查看摘要报告

此过程为您显示如何查看摘要报告。

查看摘要报告

1 在 Enforce Server 管理控制台中的“事件”菜单上，选择其中一种报告类型。

例如，选择“网络”，然后单击“策略摘要”。

报告包括被划分成几个列的摘要条目（行）。第一列针对主要摘要条件命名。它列出主要和辅助摘要（针对双摘要）项目。例如，在“策略摘要”中，该列的名称为“策略”，并列出策略。每个条目中相关事件总数成一列。此外，它还包含显示严重性分别为高、中、低和信息的事件数量的列。最后，它还包括一个条形图表，表示按严重性排列的事件数量。

- 2 或者，您可以通过特定列的数据按字母数字顺序对报告进行排序。要执行此操作，请单击所需的列标题。要按倒序进行排序，请再次单击该列标题。
- 3 要确定潜在风险区域，请单击“高”列标题，显示按高严重性事件数量排列的摘要条目。
- 4 单击条目可查看相关事件的列表。在任意严重性列中，可以单击总计，查看所选严重性的事件的列表。

请参见第 785 页的“[查看事件](#)”。

创建摘要报告

此过程为您显示如何创建摘要报告。

从事件列表创建摘要报告

- 1 在 Enforce Server 管理控制台的“事件”菜单上，选择一种类型的报告，然后单击事件列表。

例如，选择“发现”，然后选择“事件-所有扫描”报告。

- 2 单击“高级过滤器和摘要”栏（在报告顶部附近）。

在显示的主要列表框和辅助列表框的“摘要类型”中，Symantec Data Loss Prevention 会按字母顺序显示 Symantec 提供的所有条件。此条件的优先级高于管理员定义的任何自定义条件。

请参见第 811 页的[“事件报告的摘要选项”](#)。

- 3 从主要列表框中选择一个条件，并从辅助列表框中选择一个可选条件。例如，先选择“策略组”，然后选择“策略”。（请注意，仅在从主要列表框中选择选项后，才会显示次要列表框中的选项。）

- 4 要创建摘要报告，请单击“应用”。

摘要报告从主要摘要条件获取其名称。如果使用新条件重新运行报告，则报告名称也会相应改变。

- 5 保存报告。

请参见第 789 页的[“保存自定义事件报告”](#)。

查看事件

Symantec Data Loss Prevention 事件列表显示包含事件相关信息的各个事件记录。可以单击任何事件以便查看包含更多详细信息的快照。还可以选择要修改或补救的特定事件或事件组。

Symantec Data Loss Prevention 为“网络”、“端点”和“发现”事件提供事件列表。

查看事件

- 1 在 Enforce Server 管理控制台中的“事件”菜单上，选择其中一种报告类型。

例如，选择“发现”。在左侧导航面板中，单击“事件-所有扫描”。

事件列表显示包含诸如严重性、关联的策略、匹配数及状态等信息的各个事件记录。

- 2 可以选择使用报告过滤器缩小事件列表。

请参见第 788 页的[“过滤报告”](#)。

3 要查看特定事件的更多详细信息，请单击事件。

将显示事件快照，快照中显示常规事件信息、在拦截的文本中检测到的匹配数，以及策略、属性和事件历史记录等详细信息。

您也可以在“**关联**”选项卡中搜索类似的事件。

4 还可以从上而下單击事件快照的每一部分，以便查看事件的更多相关信息。

以下列表说明通过快照访问更多信息的方式：

- 可以查找有关检测该事件的策略的信息。在“**关键信息**”选项卡上，“**策略匹配项**”部分显示策略名称。单击策略名称可查看与该策略关联的事件的列表。单击“**查看策略**”可查看该策略的只读版本。

此部分也列出了同一文件或邮件违反的其他策略。列出多个策略时，可以查看与特定策略关联的事件的快照。单击该策略名称旁边的“**转至事件**”。要查看该文件或邮件所创建的事件的列表，请单击“**显示全部**”。

- 可以查看与当前事件共享多个不同属性的事件的列表。“**关联**”选项卡显示与单个属性匹配的关联的列表。单击属性值可以查看与这些值相关的事件的列表。

例如，当前网络事件由一封来自特定电子邮件帐户的邮件触发。可以调出该帐户所创建的事件的列表。

- 对于大多数网络事件，可以访问与该网络邮件关联的任何附件。要访问附件，请找到快照的“**事件详细信息**”部分中的“**附件**”字段，然后单击附件的文件名。

有关事件快照以及可通过事件快照执行的操作的详细说明，请参见联机帮助。

5 查看完事件后，可以退出事件快照或事件列表，也可以选择一个或多个事件以进行补救。

请参见第 715 页的“[补救事件](#)”。

关于自定义报告和控制板

您可以过滤并总结报告，然后保存报告以备继续使用。保存自定义报告时，您可以配置 Symantec Data Loss Prevention，根据特定的日程表发送报告。

Symantec Data Loss Prevention 会在“**事件**”>“**事件报告**”下显示自定义报告的标题。

“**事件报告**”屏幕会显示适用于您的已分配角色的所有现成报告和自定义报告。该列表包括共享的自定义报告以及您或其他人以您当前角色所创建的控制板。Symantec Data Loss Prevention 提供了几个标准报告。

Symantec Data Loss Prevention 会显示每个报告的名称、关联产品和描述。对于自定义报告，Symantec Data Loss Prevention 会指明报告是共享还是专用，并显示报告生成和交付日程表。

您可以修改现有报告并将其另存为自定义报告，还可以创建自定义控制板。在导航面板的“保存的报告”部分会列出自定义报告和控制板。

您可以单击列表中的任意报告，以使用当前数据来重新运行该报告。

您可以查看和运行由具有分配给您的任何角色的用户所创建的自定义报告。但只能编辑或删除与当前角色关联的自定义报告。只有对管理员可见的自定义报告才是管理员用户创建的报告。

一组表将列出可用于过滤和总结报告的所有选项。

请参见第 783 页的“[关于摘要报告](#)”。

请参见第 811 页的“[事件报告的摘要选项](#)”。

请参见第 808 页的“[报告的常规过滤器](#)”。

请参见第 815 页的“[报告的高级过滤器选项](#)”。

创建控制板 允许您创建自定义控制板，用于显示来自您指定的多个报告的摘要数据。对于非管理员用户，此选项会转至“配置控制板”屏幕，从中可指定控制板为专用还是共享。所有管理员控制板都是专用的。

请参见第 780 页的“[创建控制板报告](#)”。

编辑首选项 允许您指定在登录时显示的报告，以及应在导航面板中显示的报告。

请参见第 795 页的“[编辑自定义控制板和报告](#)”。

与您的角色关联的已保存（自定义）报告会显示在屏幕顶部附近。

以下选项适用于您当前角色的自定义报告：

 单击报告旁边的该图标可显示“保存报告”或“配置控制板”屏幕。您可以更改名称、描述或日程表，或者（仅限控制板）更改要包括的报告。

请参见第 789 页的“[保存自定义事件报告](#)”。

请参见第 782 页的“[配置控制板报告](#)”。

 单击报告旁边的该图标可显示一个屏幕，在其中可更改此报告的调度。如果未显示该图标，则表示当前没有调度此报告。

请参见第 789 页的“[保存自定义事件报告](#)”。

 单击报告旁边的该图标可删除该报告。将出现一个对话框，提示您确认是否执行删除操作。删除报告后，将无法对其进行恢复。在删除报告之前，请确保其他角色成员都不需要该报告。

使用 IT Analytics 管理事件

IT Analytics Solution 是一种业务智能 (BI) 应用程序，用于对 Symantec Data Loss Prevention 提供的报告进行补充和扩展。它可以为 Symantec Management Platform 提供多维度分析及强大的图形报告功能。通过此功能，您无需精通数据库或第三方报告工具，即可创建实时即席报告。IT Analytics 通过数据透视表、预编译聚合来提供这一强大的实时即席报告功能，可快速回答通常运行时间较长的查询，并可方便地导出到 .PDF、Excel、.CSV 和 .TIF 文件。

有关详细信息，请参见 *Data Loss Prevention Pack for Altiris IT Analytics Solution 7.1 SP2 from Symantec User Guide*（《适用于 Altiris IT Analytics Solution 7.1 SP2 的 Symantec Data Loss Prevention Pack 安装使用指南》），您可以在以下 URL 找到该指南：

<http://www.symantec.com/business/support/index?page=content&id=DOC5526&key=56005>

过滤报告

您可以过滤选事件列表或摘要报告。

过滤事件列表

1 在 Enforce Server 管理控制台中的“事件”菜单上，选择其中一种报告类型。

例如，选择“网络”，然后单击“策略摘要”。

2 在“过滤器”区域中，会显示当前的过滤器以及用于添加和运行其他过滤器的选项。

3 根据需要修改默认过滤器。例如，从“状态”过滤器下拉列表中选择“等于”和“新建”。

对于“网络”、“移动”和“端点”报告，默认过滤器为“日期”和“状态”。

对于“发现”报告，默认过滤器为“状态”、“扫描”和“目标 ID”。

4 要添加新的过滤器，请从下拉列表中选择过滤器选项。单击“高级过滤器和摘要”以获得其他选项。对于其他过滤器选项，单击右边的“添加过滤器”。

就象写句子一样，从左到右选择过滤器类型和参数。例如，从高级过滤器的“添加过滤器”选项中，选择“策略”和“为任一”，然后在报告中选择一个或多个要查看的策略。按住 Ctrl 或 Shift 在列表框中选择多个项目。

5 单击“应用”以更新报告。

6 保存报告。

请参见第 789 页的“[保存自定义事件报告](#)”。

保存自定义事件报告

对报告进行摘要或过滤之后，您可以保存报告以便继续使用。保存自定义报告时，Symantec Data Loss Prevention 会在“事件报告”部分的“保存的报告”下显示报告标题。如果用户选择共享报告，Symantec Data Loss Prevention 仅显示属于与报告创建用户相同的角色的用户报告链接。

请参见第 786 页的“[关于自定义报告和控制板](#)”。

您可以稍后在“[编辑首选项](#)”屏幕中编辑报告。

请参见第 795 页的“[编辑自定义控制板和报告](#)”。

还可以选择将报告调度为定期自动运行。

请参见第 789 页的“[调度自定义事件报告](#)”。

保存自定义报告

1 设置自定义过滤报告或摘要报告。

请参见第 786 页的“[关于自定义报告和控制板](#)”。

单击“保存”>“另存为”。

2 输入唯一的报告名称并描述报告。报告名称最多可包括 50 个字符。

3 在“共享”部分，除管理员之外的用户可共享自定义报告。

注意：此部分不会向管理员显示。

“共享”部分允许您指定是将报告保留为专用还是将其与其他角色成员共享。此处的角色成员是指分配有同一角色的其他用户。要共享报告，请选择“[共享报告](#)”。现在所有角色成员都有权访问该报告，并且可以对其进行编辑或删除。如果您的帐户从系统中删除，共享报告仍然会保留在系统中。共享报告与角色相关联，而不是与特定用户帐户相关联。如果您不共享报告，则您是唯一可以访问该报告的用户。如果您的帐户从系统中删除，您的专用报告也会同时删除。如果您以其他角色登录，该报告在“事件报告”屏幕上可见，但您无法对其进行访问。

4 单击“保存”。

调度自定义事件报告

还可以选择将保存的报告调度为定期自动运行。

您也可以将报告调度为根据定期日程表通过电子邮件发送到指定地址或数据所有者。

请参见《Symantec Data Loss Prevention Data Insight 操作指南》。

调度自定义报告

- 1 单击“发送”>“日程表分发”。

如果尚未在 Enforce Server 上设置 SMTP，则不能选择“发送”菜单项发送报告。

请参见第 135 页的[“配置 Enforce Server 以发送电子邮件警报”](#)。

- 2 指定“交付详细信息”：

收件人： 选择是将报告发送到指定的电子邮件地址还是发送到数据所有者。

手动 - 发送到指定的电子邮件地址 在文本框中手动输入特定的电子邮件地址。

自动 - 发送到事件数据所有者 要将报告发送到数据所有者，必须启用“[通过电子邮件发送报告数据](#)”设置以显示此选项。

请参见第 135 页的[“配置 Enforce Server 以发送电子邮件警报”](#)。

如果选择将报告发送到事件数据所有者，则事件属性“[数据所有者电子邮件地址](#)”中的电子邮件地址是报告送达的地址。

此“[数据所有者电子邮件地址](#)”必须手动设置或使用查找插件设置。

请参见《Symantec Data Loss Prevention Data Insight 操作指南》。

可以向一个数据所有者最多分发 10000 个事件。

抄送： 在文本框中手动输入电子邮件地址。

主题： 使用默认主题或修改默认主题。

正文： 输入电子邮件的正文。

还可以在正文中输入响应操作变量。

请参见第 718 页的[“响应操作变量”](#)。

- 3 在“日程表交付”部分，指定交付日程表。

请参见第 791 页的[“事件和系统报告的交付日程表选项”](#)。

- 4 在“更改事件状态/属性”部分，可以实施工作流程。
必须设置“自动 - 将事件发送给数据所有者”选项，才能显示此部分。
请参见第 135 页的[“配置 Enforce Server 以发送电子邮件警报”](#)。
- 5 发送报告后，可以将事件的状态更改为任何有效值。从下拉列表中选择一个状态值。
- 6 还可以为任何自定义属性输入新值。
必须已经设置这些属性。
请参见第 827 页的[“关于事件状态属性”](#)。
- 7 从下拉列表中，选择其中一个自定义属性。
- 8 单击“添加”。
- 9 在文本框中，为此自定义属性输入新值。
发送报告后，所选的自定义属性将为报告中发送的事件设置新值。
- 10 单击“下一步”。
- 11 输入保存的报告的名称和说明。
- 12 单击“保存”。

事件和系统报告的交付日程表选项

可以通过“日程表交付”部分为报告设置日程表。

注意：如果未将 Enforce Server 配置为发送电子邮件，或者您无法发送报告，则不会显示“日程表交付”部分。

从列表中选择一个选项后，会显示附加字段。

要删除以前调度的报告的调度，请单击“删除”选项。

下表描述了列表中每个选项可用的附加字段。

交付详细信息

指定下列交付详细信息：

■ 收件人

指定“手动”以指定电子邮件地址。

指定“自动”以自动向数据所有者发送。

■ 收件人

输入一个或多个电子邮件地址。用逗号将其分隔开。

■ 抄送

输入一个或多个电子邮件地址。用逗号将其分隔开。

■ 主题

为电子邮件提供一个主题。

■ 正文

输入电子邮件的正文。使用项目变量，例如策略名称。

请参见第 718 页的“[响应操作变量](#)”。

一次

选择“一次”可将报告调度为将来运行一次，然后为该报告指定下列详细信息：

■ 时间

选择希望生成报告的时间。

■ 发送日期

输入希望生成报告的日期，或者单击日期工具并选择一个日期。

每日

选择“每日”可将报告调度为每天运行，然后为该报告指定下列详细信息：

■ 时间

选择希望生成报告的时间。

■ 截止日期

输入希望停止生成每日报告的日期，或者单击日期工具并选择一个日期，或者选择“不确定”。

每周

选择“每周，于”可将报告调度为每周运行，然后为该报告指定下列详细信息：

■ 时间

选择希望生成报告的时间。

■ 周中的某些天

单击选中一个或多个复选框，指明希望在一周的哪些天生成报告。

■ 截止日期

输入希望停止生成每周报告的日期，或者单击日期工具并选择日期，或者选择“不确定”。

每月 选择“每月，于”可将报告调度为每月运行，然后为该报告指定下列详细信息：

■ **时间**

选择希望生成报告的时间。

■ **月中的某日**

输入希望每月生成报告的日期。

■ **截止日期**

输入希望停止生成每月报告的日期，或者单击日期工具并选择一个日期，或者选择“不确定”。

请参见第 789 页的“[保存自定义事件报告](#)”。

请参见第 128 页的“[使用保存的系统报告](#)”。

控制板报告的交付日程表选项

可以通过“交付日程表”部分为报告设置日程表。

注意：如果未将 Enforce Server 配置为发送电子邮件，或者您无法发送报告，则不会显示“交付日程表”部分。

从“日程表”下拉列表中选择一个选项后，会显示附加字段。

下表描述了列表中每个选项可用的附加字段。

无日程表 选择“无日程表”可在不使用日程表的情况下保存报告。

一次 选择“一次”可将报告调度为将来运行一次，然后为该报告指定下列详细信息：

■ **日期**

输入希望生成报告的日期，或者单击日期工具并选择一个日期。

■ **时间**

选择希望生成报告的时间。

■ **收件人**

输入一个或多个电子邮件地址。用逗号将其分隔开。

每天发送	选择“每天发送”可将报告调度为每天运行，然后为该报告指定下列详细信息： <ul style="list-style-type: none">■ 时间 选择希望生成报告的时间。■ 截止日期 输入希望停止生成每日报告的日期，或者单击日期工具并选择一个日期，或者选择“不确定”。■ 收件人 输入一个或多个电子邮件地址。用逗号将其分隔开。
每周发送, 于	选择“每周发送, 于”可将报告调度为每周运行，然后为该报告指定下列详细信息： <ul style="list-style-type: none">■ 星期 单击选中一个或多个复选框，指明希望在一周的哪些天生成报告。■ 时间 选择希望生成报告的时间。■ 截止日期 输入希望停止生成每周报告的日期，或者单击日期工具并选择日期，或者选择“不确定”。■ 收件人 输入一个或多个电子邮件地址。用逗号将其分隔开。
每月发送, 于	选择“每月发送, 于”可将报告调度为每月运行，然后为该报告指定下列详细信息： <ul style="list-style-type: none">■ 每月的某天 输入希望每月生成报告的日期。■ 时间 选择希望生成报告的时间。■ 截止日期 输入希望停止生成每月报告的日期，或者单击日期工具并选择一个日期，或者选择“不确定”。■ 收件人 输入一个或多个电子邮件地址。用逗号将其分隔开。

请参见第 782 页的“[配置控制板报告](#)”。

使用日期工具调度报告

日期工具指定报告的日期。

日期工具为您输入日期。您可以单击“今天”来输入当前日期。

使用日期工具

- 1 单击日期工具。
- 2 单击月份两侧的向左箭头或向右箭头以更改月份。
- 3 单击年份两侧的向左箭头或向右箭头以更改年份。
- 4 在日历中单击所需的日期。

编辑自定义控制板和报告

可以编辑创建的任何自定义报告或控制板。

编辑自定义控制板或报告

- 1 在 Enforce Server 管理控制台中的“事件”菜单上，选择“事件报告”。
将显示“事件报告”控制板，控制板顶部附近显示“保存的报告”。
- 2 单击要编辑的报告或控制板旁边的“编辑”图标。
将显示“保存报告”屏幕或“保存控制板”屏幕。可以编辑任何自定义报告或控制板的名称、说明和日程表，并可为自定义控制板选择不同的报告组件。
请参见第 789 页的[“保存自定义事件报告”](#)。
- 3 完成编辑后，单击“保存”。

导出事件报告

可将报告导出为逗号分隔的文本 (.csv) 文件或导出为 XML 文件。

除逗号之外，您可以设置其他 CSV 分隔符。可以指定将哪些文件导出为 XML。必须先在配置文件中设置这些选项，然后再导出报告。

请参见第 54 页的[“编辑用户配置文件”](#)。

导出报告

- 1 单击“事件”，然后选择报告的类型。
- 2 导航至要导出的报告。根据需要，对报告中的事件进行过滤或总结。
请参见第 801 页的[“常见事件报告功能”](#)。

- 3 选中事件左侧的框以选择要导出的事件。
- 4 在“导出”下拉菜单中，选择“全部导出:CSV”或“全部导出:XML”

注意：导出报告的 XML 架构文件位于 `cc:\Vontu\Protect\tomcat\webapps\ProtectManager\WEB-INF\lib\reportingapi-schema.jar` 文件中。

有关各个 XML 元素的说明，请参见“报告 API 开发人员指南”。

- 5 单击“打开”或“保存”。如果选择“保存”，系统会打开“另存为”对话框，可指定位置和文件名。

请参见第 796 页的[“Network Monitor 的导出字段”](#)。

请参见第 798 页的[“Endpoint Discover 的导出字段”](#)。

请参见第 797 页的[“Network Discover 的导出字段”](#)。

请参见第 798 页的[“Mobile Prevent for Web 的导出字段”](#)。

请参见第 804 页的[“打印事件报告”](#)。

请参见第 803 页的[“通过电子邮件发送事件报告”](#)。

Network Monitor 的导出字段

会导出 Network Monitor 的下列字段：

类型	事件类型（例如 SMTP 、 HTTP 或 FTP ）。
邮件状态	该事件邮件的状态。
严重性	该事件的严重性（“高”、“中”或“低”）。
发送时间	发送邮件的日期和时间。
ID	该事件的唯一标识符。
策略	触发该事件的策略的名称。
匹配项	此项目与策略规则的检测参数匹配的次数。
主题	邮件的主题。
接受者	邮件的接受者。
状态	该事件的状态（“新建”、“已提报”、“已排除”或“已关闭”）。
带有附件	表示该邮件是否带有附件。

数据所有者名称 负责补救事件的人员。必须手动设置或者使用某个查找插件来设置此字段。
系统可自动将报告发送给数据所有者以进行补救。

数据所有者电子邮件地址 负责补救事件的人员的电子邮件地址。必须手动设置或者使用某个查找插件来设置此字段。

还将导出自定义属性。

Network Discover 的导出字段

会导出 Network Discover 的下列字段：

类型	目标类型（例如文件系统、Lotus Notes 或者 SQL 数据库）。
邮件状态	该事件邮件的状态。
严重性	该事件的严重性（“高”、“中”或“低”）。
检测日期	检测到事件的日期。
出现过	以前出现过此事件？值为“是”或“否”。
主题	集成的 Exchange 扫描的电子邮件主题。
发送者	集成的 Exchange 扫描的电子邮件发送者。
接受者	集成的 Exchange 扫描的电子邮件接受者。
ID	该事件的唯一标识符。
策略	触发该事件的策略的名称。
匹配项	此项目与策略规则的检测参数匹配的次数。
位置	该项目的位置（路径）。
状态	该事件的状态（“新建”、“已提报”、“已排除”或“已关闭”）。
目标	扫描目标的名称。
扫描	扫描文件的日期和时间。
文件所有者	文件的所有者。
上次修改日期	上次修改项目的日期和时间。
文件创建日期	创建项目的日期和时间。
上次访问日期	上次访问项目的日期和时间。

数据所有者名称 负责补救事件的人员。必须手动设置或者使用某个查找插件来设置此字段。
系统可自动将报告发送给数据所有者以进行补救。

数据所有者电子邮件 负责补救事件的人员的电子邮件地址。必须手动设置或者使用某个查找插件来设置此字段。

还将导出自定义属性。

Mobile Prevent for Web 的导出字段

以下是 Mobile Prevent for Web 的导出字段：

类型	事件类型（例如 HTTP/S 或 FTP ）。
邮件状态	该事件邮件的状态。
严重性	该事件的严重性（“高”、“中”或“低”）。
发送时间	发送邮件的日期和时间。
ID	该事件的唯一标识符。
策略	触发该事件的策略的名称。
匹配项	此项目与策略规则的检测参数匹配的次数。
主题	邮件的主题。
接受者	邮件的接受者。
状态	该事件的状态（“新建”、“已提报”、“已排除”或“已关闭”）。
带有附件	表示该邮件是否带有附件。
数据所有者名称	负责补救事件的人员。必须手动设置或者使用某个查找插件来设置此字段。 系统可自动将报告发送给数据所有者以进行补救。
数据所有者电子邮件	负责补救事件的人员的电子邮件地址。必须手动设置或者使用某个查找插件来设置此字段。

Endpoint Discover 的导出字段

会导出 Endpoint Discover 的下列字段：

类型 目标类型（例如“可移动存储”）。

严重性	该事件的严重性（“高”、“中”或“低”）。
发生时间	检测到事件的日期。
ID	该事件的唯一标识符。
策略	触发该事件的策略的名称。
匹配项	此项目与策略规则的检测参数匹配的次数。
状态	该事件的状态（“新建”、“已提报”、“已排除”或“已关闭”）。
文件名	违反策略的文件的名称。
文件路径	文件的路径。 注意： 仅针对固定驱动器事件显示的文件位置。
计算机	发生事件的计算机。
用户	端点用户名。
阻止状态	端点的状态（例如“已阻止操作”）。
主题	邮件的主题。
接受者	邮件的接受者。
带有附件	表示该邮件是否带有附件。
数据所有者名称	负责补救事件的人员。必须手动设置或者使用某个查找插件来设置此字段。 系统可自动将报告发送给数据所有者以进行补救。
数据所有者电子邮件	负责补救事件的人员的电子邮件地址。必须手动设置或者使用某个查找插件来设置此字段。 还将导出自定义属性。

删除事件

您可以删除事件，但无法恢复已删除的事件。因为删除是永久性操作，所以 Symantec Data Loss Prevention 提供了一些选项，这些选项仅删除触发事件的数据的某些部分。

删除事件

- 1 从下列删除选项中选择：

完全删除事件	永久删除事件及所有关联数据（例如，所有电子邮件和附件）。请注意，无法恢复已删除的事件。
保留事件，但删除消息数据	保留实际事件，但丢弃触发事件的数据的 Symantec Data Loss Prevention 副本。可以选择仅删除关联数据的某些部分。这样可保留数据的其余部分。
删除原始邮件	删除邮件内容（例如，电子邮件或 HTML 发布）。此选项仅适用于网络事件。
删除附件/文件	此选项针对文件（端点和发现事件）、电子邮件或邮寄的附件（网络事件）。选项为“全部”（这会删除所有附件）和“没有违规的附件”。例如，选择此选项可删除文件（端点和发现事件）或电子邮件附件（网络事件）。
	此选项仅删除 Symantec Data Loss Prevention 未在其中找到匹配项的附件。例如，当存在具有从压缩文件（端点和发现事件）或多个电子邮件附件（网络事件）中获取的各个文件的事件时，可选择此选项。

- 2 单击“取消”或“删除”。

“删除”会永久删除选定的事件。

删除自定义控制板和报告

可以删除创建的任何自定义报告或控制板。

删除自定义控制板或报告

- 1 在 Enforce Server 管理控制台中的“事件”菜单上，选择“事件报告”。
将显示“事件报告”控制板，控制板顶部附近显示“保存的报告”。
- 2 单击报告或控制板旁边的“删除”图标将其删除。
- 3 单击“确定”进行确认。
- 4 Symantec Data Loss Prevention 将删除报告，并从“事件报告”屏幕中将其删除。

常见事件报告功能

下列选项对事件报告列表通用：

- 报告中用于执行下列任务的图标：

- **Save (保存)**

您可以将当前报告另存为按自定义方式保存的报告。
请参见第 789 页的“[保存自定义事件报告](#)”。

- **发送**

您可以通过电子邮件发送报告或计划报告分发。
请参见第 789 页的“[保存自定义事件报告](#)”。

- **导出**

您可以将当前报告导出为 CSV 或 XML。
请参见第 795 页的“[导出事件报告](#)”。

- **删除报告**

如果此报告不是已保存的报告，则不会显示“[删除报告](#)”选项。

- 报告过滤器和摘要选项

请参见第 802 页的“[事件报告过滤器和摘要选项](#)”。

- 页面导航图标

请参见第 801 页的“[事件报告中的页面导航](#)”。

下列摘要报告可供各种事件使用：

- 网络

请参见第 731 页的“[网络摘要报告](#)”。

- 端点

请参见第 743 页的“[端点事件摘要报告](#)”。

- 发现

请参见第 767 页的“[发现摘要报告](#)”。

- 移动

请参见第 755 页的“[Mobile Prevent 摘要报告](#)”。

事件报告中的页面导航

除执行摘要外的所有报告均包含页面导航选项。Symantec Data Loss Prevention 显示总计报告事件中当前可见事件的数目（例如，1-19/19 或 1-50/315）。

超过 50 个事件的报告具有下列选项：

	显示报告的第一页。
	显示上一页。
	显示下一页。
	显示最后一页。
显示全部	显示单个页面上的所有项目。 当系统包含的事件超过500个时，请小心使用“事件列表”上的“显示全部”链接。如果“事件列表”页面上显示超过500个事件，则浏览器性能会显著降低。
全选	选择所有页面上的所有事件，以便您可以同时对其进行更新。（仅可用于“事件列表”。）单击“取消全选”以取消全部选中。 注意： 当选择“全选”时，请小心使用。此选项会选择报告中的所有事件（不仅是当前页面上的事件）。随后应用的任何事件命令都会影响所有事件。 如果只选择当前页面上的事件，可选择事件列表左上角的复选框。

请参见第 801 页的“[常见事件报告功能](#)”。

事件报告过滤器和摘要选项

过滤器分为常用过滤器、高级过滤器和摘要。

常用过滤器包括下列选项：

状态	选择“等于”、“为任一”或者“都不是”。然后选择状态值。按住 Ctrl 并单击以选择多个单独的状态值。按住 Shift 并单击以选择一个范围。
日期	使用下拉菜单选择一个日期范围，例如“上周”或“上个月”。默认值是“所有日期”。
网络和端点报告	
严重性	选中该框以选择严重性值。
扫描	对于发现报告，请选择要报告的扫描。您可以选择最近的扫描、初始扫描或正在进行的扫描。默认值是“所有扫描”。
发现报告	
目标 ID	对于发现报告，请选择要报告的目标名称。默认值是“所有目标”。

单击“高级过滤器和摘要”栏以展开具有过滤器和摘要选项的部分。

单击“添加过滤器”以添加高级过滤器。

为摘要选择一个主要选项和一个可选的辅助选项。单摘要报告使用一个摘要条件（例如与每个事件关联的策略）进行组织。双摘要报告使用两个条件（例如策略和事件状态）进行组织。

注意：如果您选择一个条件（在文本字段中输入要匹配的内容），则整个条目都必须完全匹配。例如，如果您输入 apples and oranges，指定组件中必须显示完全匹配的文本，才能将其视为匹配项。句子 Bring me the apples and the oranges 不被视为匹配项。

有关报告过滤器和摘要选项的完整列表，请参见《Symantec Data Loss Prevention 管理指南》。

请参见第 801 页的“[常见事件报告功能](#)”。

通过电子邮件发送事件报告

您可以将当前报告的副本发送到任何电子邮件地址。

若要发送报告，您的系统管理员必须配置SMTP服务器。管理员必须在“系统”>“设置”页面指定报告分发选项。您还必须为您的用户帐户指定一个电子邮件地址。

请参见第 135 页的“[配置 Enforce Server 以发送电子邮件警报](#)”。

发送报告

- 1 单击“事件”，然后选择报告的类型。
- 2 导航至要导出的报告。根据需要，对报告中的事件进行过滤或总结。
请参见第 801 页的“[常见事件报告功能](#)”。
- 3 单击右上角的“发送”。

此外，您也可以使用“发送”菜单（位于过滤器上方）。

请参见第 789 页的“[保存自定义事件报告](#)”。

- 4 在“发送报告”对话框中，指定下列选项：

收件人 输入一个或多个电子邮件地址（以逗号分隔）。

主题 为邮件输入一个主题。

消息 输入邮件正文。

- 5 单击“发送”或“取消”。

请参见第 804 页的“[打印事件报告](#)”。

请参见第 795 页的“[导出事件报告](#)”。

打印事件报告

可以将报告打印到任何可用的打印机。

打印报告

1 单击“事件”，然后选择报告的类型。

2 导航至要导出的报告。根据需要，对报告中的事件进行过滤或总结。

请参见第 801 页的“[常见事件报告功能](#)”。

3 单击右上角的“打印”。

4 报告的图像会显示在浏览器窗口中。

5 会显示打印机选择对话框，可选择一个打印机。

请参见第 803 页的“[通过电子邮件发送事件报告](#)”。

请参见第 795 页的“[导出事件报告](#)”。

事件快照历史记录选项卡

您可查看对事件执行的操作。对于每个操作，“历史记录”选项卡会显示操作的日期和时间、参与者（用户或服务器）以及操作或注释。单击“添加注释”以添加注释。

请参见第 760 页的“[发现事件快照](#)”。

请参见第 727 页的“[网络事件快照](#)”。

请参见第 736 页的“[端点事件快照](#)”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

事件快照属性部分

如果已指定，则可以查看自定义属性列表及其值。单击属性值以查看根据该值过滤的事件列表。要添加新值或编辑现有值，请单击“编辑”。在显示的“编辑属性”对话框中，键入新值并单击“保存”。过滤的列表中未显示已存档的事件。

注意：只有系统管理员已配置自定义属性，此部分才会显示。

请参见第 760 页的“[发现事件快照](#)”。

请参见第 736 页的“[端点事件快照](#)”。

请参见第 727 页的“[网络事件快照](#)”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

事件快照关联选项卡

您可以查看共享当前事件的各个属性的事件的列表。

例如，如果复制文件触发了当前事件，您可以生成与复制此文件相关的所有事件的列表。“关联”选项卡显示与单个属性匹配的关联的列表。单击属性值可以查看与这些值相关的事件的列表。

要搜索具有相同属性的其他事件，请单击“[查找类似项](#)”。在显示的“[查找类似事件](#)”对话框中，请选择所需的搜索属性。然后单击“[查找事件](#)”。搜索类似的事件时，不会显示已存档的事件。

请参见第 760 页的“[发现事件快照](#)”。

请参见第 736 页的“[端点事件快照](#)”。

请参见第 727 页的“[网络事件快照](#)”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

事件快照策略部分

“策略”区域显示事件中违规的策略并指示策略是否阻止了移动或通知了用户。它也显示了策略匹配项以及每个策略规则匹配项的总数。单击策略名称以查看违反策略的所有事件的列表。单击“[查看策略](#)”可查看该策略的只读版本。

您将看到描述下列信息的图标：

■ Symantec Data Loss Prevention 阻止了敏感信息的副本。

■ Symantec Data Loss Prevention 向用户通知了有关机密数据的副本的信息。

此部分还列出了在同一文件违规的其他策略。要查看与特定策略关联的事件的快照，请单击策略名称旁的“[转至事件](#)”链接。要查看与该文件相关的所有事件的列表，请单击“[显示全部](#)”。

请参见第 760 页的“[发现事件快照](#)”。

请参见第 736 页的“[端点事件快照](#)”。

请参见第 727 页的“[网络事件快照](#)”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

事件快照匹配项部分

在“匹配项”部分，Symantec Data Loss Prevention 显示导致事件的内容（如果适用）和匹配项。

匹配项以黄色突出显示。此部分显示总匹配数并按匹配项出现在原始内容中的顺序显示。要查看触发匹配项的规则，请单击突出显示的匹配项。

请参见第 760 页的“[发现事件快照](#)”。

请参见第 736 页的“[端点事件快照](#)”。

请参见第 727 页的“[网络事件快照](#)”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

请参见第 411 页的“[关于相似度阈值和相似度评分](#)”。

事件快照访问信息部分

事件快照的“访问信息”部分可显示对象的访问控制列表。

访问控制列表 (ACL) 是附加到某对象或部分数据的权限列表。该列表包含具有文件读写权限的所有用户的相关信息。使用该列表可查看哪些用户具有文件访问权限以及每个用户可执行哪些操作。并非每个用户或组的权限都是通过 Symantec Data Loss Prevention 设置的。管理员使用端点计算机上其他类型的程序为每个文件设置权限。权限通常在文件创建时设置。

例如，用户 1 具有访问文件 Example1.doc 的权限。用户 1 可以查看和编辑该文件。用户 2 也具有访问文件 Example1.doc 的权限。但用户 2 只能查看该文件，而没有更改文件的权限。在 ACL 中，会列出用户 1 和用户 2，以及授予他们的权限。

[表 47-1](#) 显示了用户及其权限。

表 47-1 访问控制列表示例

名称	权限
用户 1	授予读取权限
用户 1	授予写入权限
用户 2	授予读取权限

每授予一种权限，就会在 ACL 中添加一行。ACL 仅为用户 2 添加一行，因为用户 2 只有一种权限，即读取权限。用户 2 不能对文件进行任何更改。用户 1 具有两个条目，因为用户 1 拥有两种权限：读取权限和编辑权限。

您只能查看关于 Discover 和 Endpoint 本地驱动器事件快照的 ACL 信息。不能查看任何其他类型的事件上的 ACL 信息。

“访问信息”部分显示在事件快照的“关键信息”选项卡上。

请参见第 760 页的“[发现事件快照](#)”。

请参见第 736 页的“[端点事件快照](#)”。

请参见第 727 页的“[网络事件快照](#)”。

请参见第 748 页的“[Mobile Prevent 事件快照](#)”。

自定义事件快照页面

您可以自定义事件快照页面的外观。

自定义事件快照页面的外观

- 1 从事件快照中，单击“自定义布局”（位于右上角）。
- 2 选择要在事件快照中的每个选项卡上显示的信息。
“选项卡 1”始终包含“关键信息”，且不能更改。
- 3 对于事件快照屏幕上的每个区域，请选择要显示的信息。
- 4 单击“保存”。

关于报告的过滤器和摘要选项

您可以为 Symantec Data Loss Prevention 事件报告设置多个过滤器和摘要。

通过这些过滤器，可以采用不同方式查看事件和事件数据。

这组过滤器分别适用于网络、端点、移动和存储事件。

图 47-1 显示了用于过滤和总结报告的选项的位置。

图 47-1 过滤器和摘要选项



过滤器和摘要选项位于下列部分中：

常规过滤器

常规过滤器选项是最常用的选项。在事件列表报告中始终可以看见这些选项。

高级过滤器

高级过滤器提供了许多其他过滤器选项。必须单击“高级过滤器”栏，然后单击“添加过滤器”，才能查看这些过滤器选项。

摘要选项

摘要选项提供了在列表中总结事件的方式。必须单击“高级过滤器和摘要”栏才能查看这些摘要选项。

Symantec Data Loss Prevention 包含许多标准报告。您也可以创建自定义报告，或者保存报告摘要和过滤器选项以备重复使用。

请参见第 775 页的“[关于 Symantec Data Loss Prevention 报告](#)”。

报告的常规过滤器

报告的常规过滤器包括由几个常用过滤器组成的一组过滤器。

其中大多数过滤器适用于所有的产品。Network Discover 包含与存储扫描相关的一些常规过滤器。例如，您可以过滤特定扫描中的事件。这些过滤器不适用于 Network Prevent 或 Endpoint Prevent。

表 47-2 列出了报告状态值的常规过滤器选项。

您还可以创建自定义状态值。

请参见第 827 页的“[关于事件状态属性](#)”。

这些状态过滤器适用于网络、端点、移动和发现事件。

表 47-2 状态值的常规过滤器

名称	说明
等于	该状态等于在下一个下拉菜单中选择的字段。
为任一	该状态可以是在下一个下拉菜单中选择的任何一个字段。使用 Shift+单击操作选择多个字段。
都不是	该状态不是下一个下拉菜单中选择的字段的任意一个。使用 Shift+单击操作选择多个字段。

表 47-3 列出了按日期过滤的常规过滤器选项。

这些日期过滤器适用于网络、移动和端点事件。

表 47-3 按日期过滤的常规过滤器

名称	说明
所有日期	包含事件的所有日期。
当前月份	当前月份到今天为止报告的所有事件。
当前季度	当前季度到今天为止报告的所有事件。
当前星期	当前星期报告的所有事件。
当前年份	当前年份到今天为止报告的所有事件。
自定义	自定义时段。从日历菜单中选择要查看的日期。
最近 7 天	前七天报告的所有事件。
最近 30 天	前 30 天报告的所有事件。
上个月	前一日历月期间报告的所有事件。
上周	前一日历周期间报告的所有事件。
上个季度	前一季度报告的所有事件。
去年	上一日历年期间报告的所有事件。
今天	今天报告的所有事件。

名称	说明
昨天	昨天报告的所有事件。

表 47-4 列出了按严重性过滤的常规过滤器选项。选中要包括在过滤器中的严重性旁边的框。

这些严重性过滤器适用于网络、端点、移动和发现事件。

表 47-4 严重性值的常规过滤器

名称	说明
高	仅列出高严重性事件。显示事件列表中有多少个高严重性事件。
信息	只列出信息性事件。不对信息性事件指定任何其他严重性。显示事件列表中有多少个信息性事件。
低	仅列出低严重性事件。显示事件列表中有多少个低严重性事件。
中	仅列出中严重性事件。显示事件列表中有多少个中严重性事件。

表 47-5 列出了适用于 Network Discover 扫描的常规过滤器选项。此过滤器仅适用于发现事件。

表 47-5 用于扫描的常规过滤器

名称	说明
所有扫描	在已运行的所有扫描中报告的所有事件。
初始扫描	初始扫描中报告的所有事件。
进行中	当前正在进行的扫描中已报告的所有事件。
上次完成的扫描	上次完成的扫描中报告的所有事件。

您可以按“目标 ID”过滤发现事件。此过滤器仅适用于发现事件。

选择目标或选择“所有目标”。使用 Shift+单击操作选择多个字段。

表 47-6 列出了按发现事件的检测日期过滤的常规过滤器选项。

表 47-6 按日期过滤的常规过滤器

名称	说明
所有日期	包含事件的所有日期。
当前月份	当前月份到今天为止报告的所有事件。

名称	说明
当前季度	当前季度到今天为止报告的所有事件。
当前星期	当前星期报告的所有事件。
当前年份	当前年份到今天为止报告的所有事件。
自定义	自定义时段。从日历菜单中选择要查看的日期。
自定义始于	从特定日期到当前日期已连接到 Endpoint Server 的 Symantec DLP Agent。选择此过滤器的开始日期。
自定义早于	在特定日期之前已连接到 Endpoint Server 的 Symantec DLP Agent。选择此过滤器的最后日期。
最近 7 天	前七天报告的所有事件。
最近 30 天	前 30 天报告的所有事件。
上个月	前一日历月期间报告的所有事件。
上周	前一日历周期间报告的所有事件。
上个季度	前一季度报告的所有事件。
去年	上一日历年期间报告的所有事件。
今天	今天报告的所有事件。
昨天	昨天报告的所有事件。

事件报告的摘要选项

事件报告摘要为事件中包含的信息摘要提供选项。例如，您可以按状态或策略总结事件。

注意：除非“已存档”过滤器的“高级过滤器”选项设置为“显示存档和非存档的事件”，否则报告摘要中不包含已存档的事件。

请参见第 823 页的“[关于事件存档](#)”。

表 47-7 列出了事件报告的摘要选项。

表 47-7 摘要过滤器

名称	说明	适用的产品
代理配置	按关联的代理配置实体总结代理和事件。如果已配置多个代理配置实体，则可以按特定实体下拉菜单进行总结或过滤。如果默认的代理配置实体是唯一配置的实体，则不会显示下拉菜单。	端点
代理响应	按代理响应事件的方式总结事件。	端点
内容根目录	按内容根目录路径提供事件摘要。	发现
数据所有者电子邮件地址	负责补救事件的人员的电子邮件地址。此字段必须手动设置，或使用查找插件设置。	网络 端点 发现
数据所有者名称	负责补救事件的人员。此字段必须手动设置，或使用查找插件设置。 系统可自动将报告发送给数据所有者以进行补救。	网络 端点 发现 移动
目标 IP	按目标 IP 地址总结事件。	网络 端点
检测月份	按检测到事件的月份总结事件。	发现
检测季度	按检测到事件的日历季度总结事件。	发现
检测星期	按检测到事件的星期总结事件。	发现
检测年份	按检测到事件的年份总结事件。	发现
设备实例 ID	按创建违规的特定设备总结事件。	端点
域	按域名总结事件。	网络
电子邮件	按与违规关联的电子邮件总结事件。	移动
端点位置	按端点的位置总结事件。 可以是下列位置之一： ■ 在企业网络内 ■ 在企业网络外	端点
文件名	按与事件关联的文件名总结事件。	端点

名称	说明	适用的产品
文件所有者	按文件的所有者总结事件。	发现
调查状态	按当前状态总结代理。	端点 发现
位置	按事件的位置总结事件。	发现
日志级别	按代理的已配置日志级别汇总代理。	端点
计算机 IP (公司)	按企业网络中计算机的 IP 地址总结事件。	端点
计算机名称	按在其中创建事件的计算机的名称总结事件。	端点
月	按事件的创建月份总结事件。	网络 端点 移动
自首次检测后的月数	按首次检测到事件以来经过的月数总结事件。	发现
Network Prevent 操作	按 Network Prevent 中的操作总结事件。	网络
未选择主要摘要	用于表示尚未选择主要摘要的占位符选择。	网络 端点 发现
未选择辅助摘要	用于表示尚未选择摘要的占位符选择。	网络 端点 发现
策略	按事件的创建策略总结事件。	网络 端点 发现 移动
策略组	按事件所属的策略组总结事件。	网络 发现 移动

名称	说明	适用的产品
策略规则	由生成违规的策略规则总结事件。	移动
保护状态	按事件的网络状态总结事件。	发现
协议	按生成事件的协议总结事件。	网络 移动
协议或端点目标	按用于创建事件的协议或端点目标总结事件。	端点
隔离失败原因	按隔离响应操作失败的原因总结事件。	端点 发现
季度	按事件的创建季度总结事件。	网络 端点 移动
自首次检测后的季度数	按首次检测到事件以来经过的季度数总结事件。	发现
接受者	按接受者总结事件。	发现
扫描	按查找事件所用的扫描总结事件。	发现
已扫描计算机	按扫描的计算机总结事件。	发现
发送者	按发送者总结事件。	网络 端点 发现
服务器	按事件的创建服务器总结事件。	网络 端点 移动
源 IP	按事件的创建源 IP 地址总结事件。	网络 端点 移动
源文件	按违反策略的源文件总结事件。	端点

名称	说明	适用的产品
状态	按事件状态总结事件。	网络 端点 发现 移动
主题	按主题总结事件。	发现
Mobile Prevent 操作	按采取的响应规则操作总结事件。	移动
目标 ID	按目标扫描 ID 总结事件。	发现
目标类型	按在其中生成事件的目标的类型总结事件。	发现
用户理由	按用户输入的理由总结事件。	端点
用户名	按生成事件的用户总结事件。	端点
星期	按事件的创建星期总结事件。	网络 端点 移动
自首次检测后的周数	按首次检测到事件以来经过的星期数总结事件。	发现
年	按事件的创建年份总结事件。	网络 端点 移动
自首次检测后的年数	按首次检测到事件以来经过的年数总结事件。	发现

报告的高级过滤器选项

高级报告过滤器用于过滤与特定操作或文本字符串相关的事件。例如，您可以过滤与特定关键字相关的事件。或者，您可以过滤掉与特定操作相关的事件。这些过滤器将一组选择字段或文本框组合在一起，以创建高级过滤器。

[表 47-8](#)、[表 47-9](#) 和 [表 47-10](#) 列出了报告的高级过滤器选项。

表 47-8 高级过滤器，第一个字段

名称	说明	适用的产品
代理配置	按关联的代理配置实体总结代理和事件。如果已配置多个代理配置实体，则可以按特定实体下拉菜单进行总结或过滤。如果默认的代理配置实体是唯一配置的实体，则不会显示下拉菜单。	端点
代理配置状态	<p>按配置实体的状态总结代理。</p> <p>根据您是通过 Enforce 管理控制台还是通过 Symantec Management Platform (SMP) 控制台来实施代理配置模型，代理配置状态结果会有所不同。</p> <p>如果您通过 Enforce 控制台部署实体，则适用下列结果：</p> <ul style="list-style-type: none"> ■ 当前配置 代理上的配置与 Endpoint Server 上的配置相同。 ■ 过期的配置 代理上的配置与 Endpoint Server 上的配置不相同。 ■ 未知/已删除配置 代理不能报告已安装的配置，或代理上的配置已从 Endpoint Server 中删除。 <p>如果您通过 SMP 部署实体，则适用下列结果：</p> <ul style="list-style-type: none"> ■ 当前配置 Endpoint Server 上的指定配置自发送到代理之后未发生变化。 ■ 过期的配置 Endpoint Server 上的指定配置自发送到代理之后已发生变化。 ■ 未知/已删除配置 代理不能报告已安装的配置，或指定的配置已从系统中删除。 	端点
代理响应	按代理响应事件的方式过滤事件。	端点
应用程序名称	按生成事件的应用程序的名称过滤事件。	端点
应用程序窗口标题	按生成事件的窗口的标题中的字符串过滤事件。	端点
附件文件名	按与事件关联的附件的文件名过滤事件。	网络 移动

名称	说明	适用的产品
附件文件大小	按与事件关联的附件的大小过滤事件。	网络 移动
内容根目录	按内容根目录路径过滤事件。	发现
数据所有者电子邮件地址	负责补救事件的人员的电子邮件地址。此字段必须手动设置，或使用查找插件设置。	网络 端点 发现 移动
数据所有者名称	负责补救事件的人员。此字段必须手动设置，或使用查找插件设置。 系统可自动将报告发送给数据所有者以进行补救。	网络 端点 发现 移动
目标 IP	按生成事件的邮件的目标 IP 地址过滤事件。	网络 端点 移动
检测日期	按检测到事件的日期过滤事件。	发现
设备实例 ID	按创建违规的特定设备总结事件。	端点
文档名称	按违规文档的名称过滤事件。	发现
域	按与事件关联的域名过滤事件。	网络
电子邮件	按与事件关联的电子邮件地址过滤事件。	移动
端点位置	按端点位置过滤事件。 可以是下列位置之一： ■ 在企业网络内 ■ 在企业网络外	端点
文件上次修改日期	按上次修改文件的日期过滤事件。	端点 发现
文件位置	按违规文件的位置过滤事件。	端点
文件名	按违规文件的名称过滤事件。无通配符，但是可以指定部分匹配，例如 .pdf。	端点 发现

名称	说明	适用的产品
文件所有者	按违规文件的所有者过滤事件。	发现
文件大小	按违规文件的大小过滤事件。	端点 发现
事件历史记录发布者	按负责发行事件历史记录的用户过滤事件。	网络 端点 发现 移动
事件 ID	按事件 ID 过滤事件。	网络 端点 发现 移动
事件匹配数	按事件匹配项的数量过滤事件。	网络 端点 发现 移动
事件注释	按事件注释中的字符串过滤事件。	网络 端点 发现 移动
事件报告日期	按报告事件的日期过滤事件。	端点
调查状态	按调查状态过滤代理。可以选择以下选项之一： <ul style="list-style-type: none">■ 正在调查■ 不在调查	发现 端点
已存档	过滤已存档的事件。可以选择以下选项之一： <ul style="list-style-type: none">■ 显示存档的和非存档的事件■ 显示已存档的项 <p>请参见第 823 页的“关于事件存档”。</p>	网络 端点 发现 移动 分类

名称	说明	适用的产品
是否允许存档	根据“是否允许存档”标志的状态过滤事件。从第二个字段选择“为任一”运算符，然后从第三个字段选择“允许存档”或“不存档”选项。 请参见第 823 页的 “关于事件存档” 。	网络 端点 发现 移动 分类
上次连接时间	根据每个代理上次连接到 Endpoint Server 的时间过滤代理。	端点
位置	按事件的位置过滤事件。位置可以包括在其中生成事件的服务器。	发现
计算机 IP (公司)	按在其中创建事件的计算机的IP地址过滤事件。	端点
计算机名称	按创建事件的计算机名称过滤事件。	端点
最小相似度评分	按违规彼此之间的相似程度过滤事件。	移动
Network Prevent 操作	按 Network Prevent 中的操作过滤事件。	网络
策略	按事件的创建策略过滤事件。	网络 端点 发现 移动
策略组	按事件所属的策略组过滤事件。	网络 端点 发现 移动
策略规则	按生成事件的策略规则过滤事件。	网络 端点 发现 移动
保护状态	按事件的 Network Protect 状态过滤事件。	发现
协议	按事件所属的协议过滤事件。	网络 移动
协议或端点目标	按生成事件的协议或端点目标过滤事件。	端点

名称	说明	适用的产品
读取 ACL: 文件	按文件访问控制列表过滤事件。	端点 发现
读取 ACL: 共享	按共享访问控制列表过滤事件。	发现
接受者	按生成事件的消息的接受者名称过滤事件。	网络 端点 发现
已扫描计算机	按扫描的计算机过滤事件。	发现
出现过	依据是否存在以前连接的事件来过滤事件。	发现, 但不适用于 SQL 数据库事件 (其中“出现过” 始终为 False)
发送者	按发送者过滤事件。	网络 端点 发现
服务器	按事件的创建服务器过滤事件。	网络 端点 发现 移动
SharePoint ACL: 权限级别	根据 SharePoint 访问控制列表的权限级别过滤事件。	发现
SharePoint ACL: 用户/组	根据 SharePoint 访问控制列表中的用户或组过滤事件。	发现
源 IP	按事件的创建源 IP 地址过滤事件。	网络 移动
主题	按生成事件的邮件的主题行过滤事件。	网络 发现
被取代	按已被其他响应取代的事件响应过滤事件。	发现 端点
Mobile Prevent 操作	按采取的响应规则操作过滤事件。	移动
目标类型	按与事件关联的目标的类型过滤事件。	发现

名称	说明	适用的产品
自首次检测后的时间	按首次检测到事件以来经过的时间过滤事件。	发现，但并不适用于 SQL 数据库事件
URL	按发生违规的 URL 过滤事件。	发现
用户理由	按用户输入的理由过滤事件。	端点
用户名	按生成事件的用户过滤事件。	端点

高级过滤器中的第二个字段使您可以在过滤器中选择匹配类型。

表 47-9 高级过滤器，第二个字段

名称	说明
包含任一	允许您修改过滤器以在文本字符串中包括所有字词，或者允许您从第三个字段中的列表中进行选择。
包含，忽略大小写	允许您修改过滤器，以忽略特定的文本字符串。
不包含，忽略大小写	允许您修改过滤器，以过滤掉被忽略的文本字符串。
不完全匹配	允许您修改过滤器，以便与文本字符串的任意组合匹配。
结束于，忽略大小写	允许您修改过滤器，以便仅显示以被忽略的文本字符串结束的事件。
为任一	允许您修改过滤器，以使结果包括任一文本字符串，或者允许您从第三个字段中的列表中进行选择。
在两者之间	供您用来修改过滤器，以使数字结果在指定数字的范围内。
大于	供您用来修改过滤器，以使数字结果大于指定的数字。
小于	供您用来修改过滤器，以使数字结果小于指定的数字。
都不是	允许您修改过滤器，以使结果不包括任何文本字符串，或者允许您从第三个字段中的列表中进行选择。
完全匹配	允许您修改过滤器，以便与文本字符串完全匹配。
完全匹配，忽略大小写	允许您修改过滤器，以使过滤器必须与被忽略的文本字符串完全匹配。
始于，忽略大小写	允许您修改过滤器，以便仅显示以被忽略的文本字符串开始的事件。

高级过滤器中的第三个字段允许您从项列表中进行选择，或提供一个空框供您输入字符串。

第三个字段会因在第一个字段和第二个字段中选择的内容而有所不同。

对于项列表，请使用 Shift+单击操作选择多个项目。

对于字符串，不允许使用通配符，但是您可以输入部分字符串。

例如，您可以输入 .pdf 以选择任何 PDF 文件。

如果您不知道输入什么文本，请使用摘要选项来查看可能的文本值的列表。您还可以查看有关每个类别中的事件数量的摘要。

请参见第 811 页的“[事件报告的摘要选项](#)”。

表 47-10 列出了第三个字段中的某些选项。

表 47-10 高级过滤器，第三个字段

名称	说明
已阻止	阻止用户执行导致事件的操作。
已删除内容	已删除违规的内容。
无补救	尚未发生针对此事件的事件补救。
无	未针对导致事件的违规情况执行任何操作。
已复制保护文件	已将违规的文件复制到其他位置。
已隔离保护文件	已将违规的文件隔离到其他位置。
已通知用户	已通知用户发生了违规。

存档事件

本章节包括下列主题：

- [关于事件存档](#)
- [存档事件](#)
- [还原存档的事件](#)
- [禁止存档事件](#)
- [删除存档的事件](#)

关于事件存档

通过事件存档功能可将指定的事件标记为“已存档”。由于这些存档的事件被排除在常规事件报告之外，因此，通过存档不再相关的所有事件可以改善 Symantec Data Loss Prevention 部署的报告性能。存档的事件会保留在数据库中；不会移至其他表格、数据库、或其他类型的脱机存储设备。

您可以在 Enforce Server 管理控制台中对事件报告设置过滤器，以便仅显示存档的事件或同时显示存档的事件和非存档的事件。使用这些报告，您可以使用“存档”选项（选择一个或多个事件并单击“事件操作”按钮时会这些选项可用）将一个或多个事件标记为已存档。“存档”选项包括：

- **存档事件** - 将所选事件标记为已存档。
- **还原事件** - 将所选事件还原为非存档状态。
- **不存档** - 禁止对所选事件进行存档。
- **允许存档** - 允许对所选事件进行存档。

事件的存档状态显示在 Enforce Server 管理控制台的事件快照屏幕中。事件快照的“历史记录”选项卡在每次为事件设置“不存档”或“允许存档”标志时都会创建一个相应条目。

请参见第 788 页的“[过滤报告](#)”。

能否访问存档功能受角色控制。您可以对角色设置下列用户权限来控制访问权限：

- **存档事件** - 向用户授予存档事件的权限。
- **还原存档事件** - 向用户授予还原存档事件的权限。
- **补救事件** - 向用户授予设置“**不存档**”或“**允许存档**”标志的权限。

请参见第 77 页的“[关于基于角色的访问控制](#)”。

请参见第 824 页的“[存档事件](#)”。

请参见第 824 页的“[还原存档的事件](#)”。

请参见第 825 页的“[禁止存档事件](#)”。

存档事件

存档事件

- 1 打开 Enforce Server 管理控制台并导航至事件报告。
 - 2 选择您要存档的事件，方法是手动选择事件或通过设置过滤器或高级过滤器来返回您要存档的事件集。
 - 3 单击“事件操作”按钮并选择“存档”>“存档事件”。
- 所选择的事件便会存档。

还原存档的事件

还原存档的事件

- 1 打开 Enforce Server 管理控制台并导航至事件报告。
 - 2 选择“高级过滤器和摘要”链接。
 - 3 单击“添加过滤器”按钮。
 - 4 选择第一个下拉列表中的“已存档”。
 - 5 从第二个下拉列表选择“显示已存档的项”。
 - 6 选择您要还原的事件，方法是手动选择事件或通过设置过滤器或高级过滤器来返回您要还原的事件集。
- 所选择的事件便会还原。

禁止存档事件

您可以使用事件报告或事件快照来禁止存档事件。

使用事件报告禁止存档事件

- 1 打开 Enforce Server 管理控制台并导航至事件报告。
- 2 选择您要禁止存档的事件。您可以手动选择事件，也可以通过设置过滤器或高级过滤器来返回您要禁止存档的事件集。
- 3 单击“事件操作”按钮并选择“存档”>“不存档”。
系统便会禁止存档所选择的事件。

注意：按以下方法操作可允许存档您已禁止存档的事件：选择相应事件，然后从“事件操作”按钮选择“存档”>“允许存档”。

使用事件快照禁止存档事件

- 1 打开 Enforce Server 管理控制台并导航至事件报告。
- 2 单击某个事件以打开事件快照。
- 3 在“关键信息”选项卡的“事件详细信息”部分，单击“不存档”。

注意：按以下方法可以允许存档您已禁止存档的事件：打开事件快照，然后单击“事件详细信息”部分中的“允许存档”。

删除存档的事件

删除存档的事件

- 1 打开 Enforce Server 管理控制台并导航至事件报告。
- 2 单击“高级过滤器和摘要”链接。
- 3 单击“添加过滤器”。
- 4 选择第一个下拉列表中的“已存档”。
- 5 从第二个下拉列表选择“显示已存档的项”。
- 6 选择您要删除的事件。您可以手动选择事件，也可以通过设置过滤器或高级过滤器来返回您要删除的事件集。
- 7 单击“事件操作”按钮并选择“删除事件”。

8 选择以下删除选项之一：

- | | |
|---------------------|---|
| 完全删除事件 | 永久删除事件及所有关联数据（例如，所有电子邮件和附件）。
请注意，无法恢复已删除的事件。 |
| 保留事件，但删除消息数据 | 保留实际事件，但丢弃触发事件的数据的 Symantec Data Loss Prevention 副本。可以选择仅删除关联数据的某些部分。这样可保留数据的其余部分。 |
| 删除原始邮件 | 删除邮件内容（例如，电子邮件或 HTML 发布）。此选项仅适用于网络事件。 |
| 删除附件/文件 | 此选项针对文件（端点和发现事件）、电子邮件或邮寄的附件（网络事件）。选项为“全部”（这会删除所有附件）和“没有违规的附件”。例如，选择此选项可删除文件（端点和发现事件）或电子邮件附件（网络事件）。 |
| | 此选项仅删除 Symantec Data Loss Prevention 未在其中找到匹配项的附件。例如，当存在具有从压缩文件（端点和发现事件）或多个电子邮件附件（网络事件）中获取的各个文件的事件时，可选择此选项。 |

9 单击“删除”按钮。

使用事件数据

本章节包括下列主题：

- [关于事件状态属性](#)
- [配置状态属性和值](#)
- [配置状态组](#)
- [导出 Web 存档](#)
- [导出 Web 存档 - 创建存档](#)
- [导出 Web 存档 - 所有最近事件](#)
- [关于自定义属性](#)
- [关于使用自定义属性](#)
- [如何填充自定义属性](#)
- [配置自定义属性](#)
- [手动设置自定义属性的值](#)

关于事件状态属性

事件状态属性通过“属性”屏幕（“系统”>“事件数据”>“属性”）进行指定和配置。

此屏幕上列出的任何状态属性均可分配给任意给定的事件，方法是从事件快照的“状态”下拉菜单中选择它。

系统属性页面包含下列可协助进行事件补救的属性：

- 状态值

“状态值”部分列出了可分配给给定事件的当前事件状态属性。使用此部分可创建新的状态属性，对其进行修改并更改每个属性出现在下拉菜单中的顺序。请参见第 829 页的“[配置状态属性和值](#)”。

■ 状态组

“状态组”部分列出了当前事件状态组及其构成。使用此部分可创建新的状态组，对其进行修改并更改组在下拉菜单中的顺序。

请参见第 829 页的“[配置状态组](#)”。

■ “自定义属性”选项卡上的“自定义属性”

“自定义属性”选项卡提供所有当前已定义的自定义事件属性的列表。自定义属性提供有关事件的或与事件关联的信息。例如，导致事件的人员的电子邮件地址、该人员的经理、排除此事件的原因等。使用此选项卡，可以添加、配置、删除自定义事件属性并对其进行排序。

请参见第 833 页的“[关于自定义属性](#)”。

处理事件的过程需要经历从发现到解决的几个阶段。每个阶段标识为不同的状态属性，如“新建”、“调查”、“已提报”和“已解决”。这样，您可以追踪整个工作流程中事件的进度，并按事件状态过滤列表和报告。

您安装 Symantec Data Loss Prevention 时安装的解决方案软件包提供了一组初始默认的状态属性和状态属性组。您可以创建新的状态属性，也可以修改现有的状态属性。您使用的状态属性值和状态组应该以组织用来处理事件的工作流程为依据。例如，您可以将全部新事件的状态都分配为“新建”。之后，您可以将该状态更改为“已分配”、“调查”或“已提报”。最后，大部分事件将标记为“已解决”或“已排除”。

对于列表和报告过滤，您也可以创建状态组。

根据组织的偏好以及在行业内常用的技术，您可以：

- 自定义状态属性的名称以及添加新的状态属性。
- 自定义状态组的名称以及添加新的状态组。
- 设置状态属性出现在事件的“状态”下拉列表中的顺序。
- 指定自动分配给新事件的默认状态属性。

请参见第 829 页的“[配置状态属性和值](#)”。

请参见第 777 页的“[关于事件报告](#)”。

请参见第 713 页的“[关于事件补救](#)”。

请参见第 833 页的“[关于自定义属性](#)”。

配置状态属性和值

由于处理事件涉及从发现到解决的整个过程，所以每个阶段都可以标记为一种不同的状态。状态使您能够追踪整个工作流程中事件的进展。根据组织的偏好以及在行业内常用的技术，您可以定义希望用于工作流程追踪的不同的状态。

“状态值”部分列出了可分配给给定事件的可用事件状态属性。状态属性在此列表中的顺序决定了它们在用于设置事件状态的下拉菜单中的顺序。您可以从“状态值”部分执行下列操作：

操作	过程
创建新事件状态属性。	单击“添加”按钮。
删除事件状态属性。	单击属性的红色 X，然后确认您的决定。
更改事件状态属性。	单击您想更改的属性，输入新名称，然后单击“保存”。 要更改现有状态的名称，请单击该状态的铅笔图标，输入新名称，然后单击“保存”。
将事件状态属性设置为默认值。	针对某一属性单击“设置为默认值”，使其成为所有新事件的默认状态。
更改事件状态属性在下拉菜单重的顺序。	■ 单击“上移”可按顺序向上移动属性。 ■ 单击“下移”可按顺序向下移动属性。

创建新事件状态属性

1 转至“属性”屏幕（“系统”>“事件数据”>“属性”）屏幕。

单击“状态”选项卡。

2 单击“状态值”部分中的“添加”按钮。

3 输入新状态属性的名称。

4 单击“保存”。

请参见第 829 页的“[配置状态组](#)”。

请参见第 827 页的“[关于事件状态属性](#)”。

配置状态组

事件状态属性可分配给与组织的工作流程相匹配的状态组。例如，“打开”状态组可能包括“新建”、“调查”和“已提报”状态属性。然后，您可以基于其状态组

过滤事件列表和报告。例如，您可以列出带有属于“打开”状态组的状态属性的所有事件。

导航至“系统”>“事件数据”>“属性”，会出现“状态组”。

为了方便起见，您可以对事件状态进行分组，以与组织的工作流程匹配。您可使用“状态组”添加或修改状态组的名称，并指定要包含在组中的状态值。

“状态组”部分列出了可用于过滤事件的可用事件状态组。对于每个组，将列出组中包含的状态属性。您可以从“状态值”部分执行下列操作：

操作	过程
创建新事件状态组。	单击“添加状态组”按钮。
删除事件状态组。	单击组的红色 X，然后确认您的决定。
更改组的名称或事件状态属性。	单击要更改的组。然后单击铅笔图标。更改名称，选中或取消选中属性，然后单击“保存”。
更改状态组在下拉菜单中的顺序。	<ul style="list-style-type: none">■ 单击“上移”可按顺序向上移动组。■ 单击“下移”可按顺序向下移动组。

定义新状态组

1 转至“属性”屏幕（“系统”>“事件数据”>“属性”）屏幕。

单击“状态”选项卡。

2 单击“状态组”部分中的“添加状态组”按钮。

3 输入新状态组的名称。

4 单击您希望包含在此组中的状态属性的相应复选框。

状态属性是使用“状态值”部分中的“添加”按钮定义的。

请参见第 829 页的[“配置状态属性和值”](#)。

5 单击“保存”。

请参见第 829 页的[“配置状态属性和值”](#)。

请参见第 827 页的[“关于事件状态属性”](#)。

导出 Web 存档

使用此屏幕可将事件列表报告另存为 HTML 页面存档。通过存档，无法直接访问 Symantec Data Loss Prevention 的用户也可了解事件数据，并根据需要进一步了解各个事件。

当您以 Web 存档形式导出事件时，该存档会放置到
\SymantecDLP\Protect\archive\webarchive 目录中。

注意：不能存档摘要报告或控制板。

导出事件时，请注意下列事项：

- 不能像普通报告那样对存档提取摘要。
- 存档不包含过滤器，因此很难在包含大量事件的存档中定位某个特定的事件。
- 导出事件的存档不会将对应的事件从管理控制台中删除。
- 每次只能导出一个存档。

“导出 Web 存档”是必须分配给某个角色的用户权限。仅当您的角色提供对该功能的访问权限时，才能导出 Web 存档。由于角色访问权限还能确定事件报告中包含的信息，因此它还适用于存档这些事件报告。在您创建的存档中包含的信息与原始事件报告中包含的信息相同。

请参见第 81 页的“[关于配置角色和用户](#)”。

“导出 Web 存档”屏幕分为以下两个部分：

请参见第 831 页的“[导出 Web 存档 - 创建存档](#)”。

请参见第 832 页的“[导出 Web 存档 - 所有最近事件](#)”。

导出 Web 存档 - 创建存档

在“[创建存档](#)”部分，完成下列信息：

字段	说明
存档名称	使用普通 Windows 命名约定为创建的存档指定名称。

字段	说明
要导出的报告	从下拉列表中选择要存档的报告。您创建的所有报告都将提供默认报告选项。 “网络” 选项如下： <ul style="list-style-type: none">■ 事件 - 周, 当前 - 当前周的网络事件。■ 事件 - 全部 - 所有网络事件。■ 事件 - 新建 - 状态为“新建”的网络事件。 “端点” 选项如下： <ul style="list-style-type: none">■ 事件 - 周, 当前 - 当前周的端点事件。■ 事件 - 全部 - 所有端点事件。■ 事件 - 新建 - 仅状态为“新建”的端点事件。 “发现” 选项如下： <ul style="list-style-type: none">■ 事件 - 上次扫描 - 上次完成的扫描中的发现事件。（不包括当前活动扫描中的事件。）■ 事件 - 正在进行扫描 - 当前扫描中的发现事件。■ 事件 - 所有扫描 - 所有发现事件。■ 事件 - 新建 - 状态为“新建”的发现事件。 “移动” 选项如下： <ul style="list-style-type: none">■ 事件 - 周, 当前 - 当前周的网络事件。■ 事件 - 全部 - 所有网络事件。■ 事件 - 新建 - 状态为“新建”的网络事件。 “分类” 选项如下： <ul style="list-style-type: none">■ 事件 - 所有

在完成这些字段后, 请单击“创建”编译存档。

请参见第 830 页的[“导出 Web 存档”](#)。

导出 Web 存档 - 所有最近事件

“所有最近事件”部分显示与该存档相关的事件列表。（该列表仅在单击“创建”以创建该存档之后显示。）事件条目显示下列信息：

- 事件类型（错误、警告或系统信息）。
- 事件日期和时间

■ 事件的简要说明

若要查看任意事件的详细信息，请单击列表中相应的事件条目。若要查看该存档的完整“事件报告”，请单击“显示全部”。

请参见第 830 页的[“导出 Web 存档”](#)。

关于自定义属性

“自定义属性”是用于提供一种捕获和存储附加事件信息的方法的事件数据字段。自定义属性中包含的附加数据可以：

- 用于驱动工作流程。
- 执行事件响应操作。
- 用于报告衡量标准。
- 使事故响应团队更快地对事件采取操作。
- 启用增加的补救和报告自动化。

您可以针对这些目的创建所需的自定义属性。自定义属性提供有关事件的或与事件关联的信息；例如，导致事件的人员的电子邮件地址、该人员的经理、排除此事件的原因等。

“属性”屏幕（“系统”>“事件数据”>“属性”）的“自定义属性”选项卡用于处理自定义属性。“属性”屏幕包含下列选项卡：

- **状态。**“状态”选项卡提供了所有当前已定义的事件状态属性和状态属性组的列表。使用此选项卡，可以添加、配置、删除事件状态属性和事件状态组并对其进行排序。

请参见第 827 页的[“关于事件状态属性”](#)。

- **自定义属性。**“自定义属性”选项卡提供所有当前已定义的自定义事件属性的列表。使用此选项卡，可以添加、配置、删除自定义事件属性并对其进行排序。

您安装 Symantec Data Loss Prevention 时加载的解决方案软件包提供了一组初始默认的自定义属性。“自定义属性”选项卡提供可应用于任何事件的所有当前已定义的自定义属性的列表。此选项卡用于以整体方式创建、修改和删除安装的自定义属性。可以通过事件快照或使用查找插件，将任意这些自定义属性或属性值应用于单个事件。

在“自定义属性”选项卡上，可以执行以下功能：

操作

创建新自定义属性。

过程

单击“添加”按钮。

操作	过程
删除自定义属性。	单击属性的红色 X，然后确认您的决定。 请注意，您不能删除当前分配给一个或多个事件的自定义属性。必须先为受影响的事件分配其他属性，之后才能成功删除该自定义属性。
更改属性的名称、电子邮件状态或属性组。	单击要更改的属性，更改其参数，然后单击“保存”。
更改下拉菜单中的属性顺序。	<ol style="list-style-type: none">1 单击“上移”可按顺序向上移动属性。2 单击“下移”可按顺序向下移动属性。
重新加载查找插件	单击“重新加载查找插件”以重新加载已由系统卸载的所有自定义属性插件。 重新加载查找插件会对所有的事件产生影响。如果下列任何情况属实，则您可能需要重新加载查找插件： <ul style="list-style-type: none">■ 插件有问题并且系统已将其卸载，但是现在该问题已得到解决。■ 由于某种原因网络已关闭或断开连接，但是现在运行正常。■ 插件在高速缓存中存储数据，而您想要手动更新该高速缓存。
请参见第 827 页的“ 关于事件状态属性 ”。	
请参见第 835 页的“ 配置自定义属性 ”。	
请参见第 836 页的“ 手动设置自定义属性的值 ”。	

关于使用自定义属性

当创建事件时，Enforce Server 会检索关于该事件的数据。某些此类数据采用“属性”的形式。有关事件属性的更多信息，请参见《Symantec Data Loss Prevention 管理指南》。

“自定义属性”是一种特殊的属性类型，用于捕获和存储附加数据。此数据与事件相关，例如相关经理的姓名或相关部门的名称。您可创建所需的自定义属性。

自定义属性中包含的附加数据可以用于：

- 启用工作流程
- 执行事件响应操作

- 包含在报告衡量标准中
- 使事故响应团队更快地对事件采取操作
- 启用增加的补救和报告自动化

如何填充自定义属性

对于每个事件，可以通过以下方式填充自定义属性（其值可在事件数据中设置）：

- 通过查找插件在检测到事件时自动填入（如本指南所述）。
- 通过自动响应规则在检测到事件时自动填入。
- 用户执行“智能响应规则”时自动填入。
- 检测后由特定用户手动填入（通过数据条目）

还可以通过单击“事件快照”屏幕的“属性”部分的“查找”选项自动重新填充自定义属性。此操作会使用新查找返回的值替换自定义属性字段中存储的现有值。

注意：如果新查找针对任何自定义属性字段返回 null 或空值，则这些空值会覆盖现有值。

配置自定义属性

使用“配置自定义属性”屏幕添加或修改自定义属性。

可以将自定义属性分成属性组（与将状态分成状态组的方式类似），以便以一种有用的方式组织信息。常用属性组的示例包括“员工信息”、“管理员信息”和“补救信息”。所有自定义属性均可用于所有事件。

创建自定义属性并将其添加到组中

- 1 在 Enforce Server 上，单击“系统”>“事件数据”>“属性”>“自定义属性”。请注意，在安装期间所选择的解决方案软件包已为您定义和加载了大量自定义属性。所有现有自定义属性均在“自定义属性”窗口中列出。
- 2 要创建新的自定义属性，请单击“添加”选项。
- 3 在“名称”框中键入自定义属性的名称。如果适用，请选中“是电子邮件地址”框。

您为自定义属性提供的名称无关紧要。但您创建的自定义属性的结构必须与相应的外部数据源的结构相同。例如，假设外部源按照单独地理位置和部门名称存储部门信息。在这种情况下，您必须创建相应的位置和部门名称自定义属性。您无法创建组合位置和部门名称的单个部门 ID 自定义属性。

- 4 从“属性组”下拉列表中选择属性组。如果需要，请创建新的属性组。从下拉列表中选择“创建新的属性组”，然后在所显示的文本框中键入新的组名称。
- 5 单击“保存”选项。
- 6 生成一个新事件或查看现有事件并验证其是否包含新的自定义属性。

在您定义了自定义属性之后，它们可用于每个事件。每个事件都会接收其自己的自定义属性集（但某些名称值对可能为空，这取决于具体情况）。可以独立于其他事件填充或更改某个事件的自定义属性值。

如果您已经被分配了包含自定义属性的编辑访问权限的角色，则可以编辑自定义属性值。如果要更新一组事件，则可以在事件列表页面上选择这些事件。然后，从“事件操作”菜单中选择“设置属性”命令。您可以选择“查找属性”，以查找自定义属性的值。请注意，仅当至少定义一个自定义属性时，“事件快照”页面上的“设置属性”命令和“属性”部分才可用。

请参见第 835 页的“[配置自定义属性](#)”。

请参见第 827 页的“[关于事件状态属性](#)”。

请参见第 829 页的“[配置状态组](#)”。

请参见第 829 页的“[配置状态属性和值](#)”。

手动设置自定义属性的值

您可以使用自定义属性的值手动指定事件补救状态或工作流程进度。

注意：要自动填充自定义属性值，请使用一个或多个查找插件。请参见第 837 页的“[关于查找插件](#)”。

设置自定义属性的值

- 1 显示事件快照。
- 2 单击事件快照的“属性”部分中的“编辑”选项。
- 3 要设置自定义属性的值，请在相应属性字段中输入值。
- 4 完成值的设置后，单击“保存”。

实施查找插件

本章节包括下列主题：

- [关于查找插件](#)
- [实施和测试查找插件](#)
- [配置 CSV 查找插件](#)
- [配置 LDAP 查找插件](#)
- [配置脚本查找插件](#)
- [配置迁移的自定义（旧版）查找插件](#)

关于查找插件

通过查找插件可将 Enforce Server 连接到外部系统，以检索与事件有关的附加数据。数据将存储为属性。通过查找插件可向事件添加其他上下文，以改善补救工作流程。例如，考虑触发事件的电子邮件。查找插件可用于根据电子邮件发件人的地址，从目录服务器检索和显示发件人的管理员的名称和电子邮件地址。

查找插件使用相互协同作用的属性和自定义属性。如果违反了某条策略规则，系统就会生成事件属性。您可以为自定义事件数据定义自定义属性。继续该示例，在检测到事件时，系统会生成事件属性 `sender-email`，并用发件人的电子邮件地址填充它。查找插件使用此“键-值”对从 LDAP 服务器查找自定义属性“管理员名称”和“管理员电子邮件”的值。该插件会填充自定义属性，并在“事件快照”中显示这些属性。

请参见第 833 页的“[关于自定义属性](#)”。

请参见第 834 页的“[关于使用自定义属性](#)”。

请参见第 835 页的“[如何填充自定义属性](#)”。

查找插件的类型

Symantec Data Loss Prevention 提供了几种类型的查找插件，包括 CSV、LDAP、脚本、Data Insight 和自定义（旧版）。下表更详细地介绍了每种类型的查找插件。

请参见第 837 页的“[关于查找插件](#)”。

表 50-1 查找插件的类型

类型	说明
CSV	CSV 查找插件用于从上传到 Enforce Server 的逗号分隔值 (CSV) 文件检索事件数据。您可以为每一个 Enforce Server 实例分别配置一个 CSV 查找插件。 请参见第 838 页的“ 关于 CSV 查找插件 ”。
LDAP	LDAP 查找插件用于从 Microsoft Active Directory、Novell LDAP、Oracle Directory Server（以前称为 Sun ONE）或 IBM LDAP 等目录服务器检索事件数据。您可以配置多个 LDAP 查找插件实例。 请参见第 839 页的“ 关于 LDAP 查找插件 ”。
脚本	脚本查找插件用于编写从任意外部资源检索事件数据的脚本。例如，您可以使用脚本查找插件从外部资源（例如，代理日志文件或 DNS 系统）检索事件数据。您可以配置多个脚本查找插件实例。 请参见第 839 页的“ 关于脚本查找插件 ”。
Data Insight	Data Insight 查找插件可让您从 Symantec Data Insight 检索事件数据，这样，您便可以查找并管理有风险的数据。您可以为每一个 Enforce Server 实例分别配置一个 Data Insight 查找插件。 请参见第 839 页的“ 关于 Data Insight 查找插件 ”。
自定义（旧版）	自定义（旧版）查找插件用于使用 Java 代码从任意外部资源检索事件数据。 请参见第 840 页的“ 关于自定义（旧版）查找插件 ”。 注意： 顾名思义，自定义（旧版）查找插件是为旧版 Java 插件保留的。要开发新的自定义插件，您必须使用一种其他类型的查找插件。

关于 CSV 查找插件

CSV 查找插件会提取存储在 Enforce Server 上的逗号分隔值 (CSV) 文件中的数据。插件会使用来自 CSV 文件的数据，在生成事件时，填入事件的自定义属性。

CSV 查找插件会收到来自 Enforce Server 的一组查找参数，其中包含事件的相关数据。将组中的一个或多个查找参数映射到 CSV 文件中的列的标题。例如，`sender-email` 查找参数可能会映射到 CSV 文件中的 `Email` 列。查找参数中的值可用作查找相应 CSV 列中匹配值的关键字。当找到匹配时，包含匹配值的 CSV 行会提供返回到 Enforce Server 的数据。Enforce Server 使用此行中的数据来填充该事件的自定义属性。例如，如果 `sender-email` 查找参数包含值 `mary.smith@mycompany.com`，则插件会在 `Email` 列中搜索包含

mary.smith@mycompany.com 的行。然后，使用该行以提供要填充此事件的自定义属性的数据。

CSV 查找插件会使用内存中的数据库处理大文件。

请参见第 854 页的“[配置 CSV 查找插件](#)”。

关于 LDAP 查找插件

LDAP 查找插件会从实时 LDAP 系统（例如 Microsoft Active Directory、Novell LDAP、Oracle LDAP（先前为 Sun ONE）或 IBM LDAP）提取数据。然后在事件生成时，该插件使用此数据来填充事件的自定义属性。

LDAP 查找插件会收到来自 Enforce Server 的一组查找参数，其中包含事件的相关数据。这些查找参数可用于 LDAP 查询，以从现有 LDAP 目录中提取数据。例如，`sender-email` 查找参数的值也许可以与 `email` 属性的值进行比较。如果 `sender-email` 查找参数包含 `mary.smith@mycompany.com`，则可以将查询构造为搜索 `email` 属性包含 `mary.smith@mycompany.com` 的记录。搜索返回的记录中的数据会插入到事件的自定义属性中。

请参见第 862 页的“[配置 LDAP 查找插件](#)”。

关于脚本查找插件

您可以编写一个或多个脚本查找插件来查询数据存储库中的属性值。例如，您可以编写用于在 DNS 服务器中查询事件涉及的发送者的相关信息的脚本。脚本查找插件可使用此类脚本的输出来填充事件记录中的自定义属性。

与 CSV 或 LDAP 查找插件不同，脚本查找插件不会使用内联属性映射来指定如何查找参数键，而是您根据需要将此功能编入每个脚本中。

若要实现脚本查找插件，您可以使用读取标准输入(`stdin`)和写入标准输出(`stdout`)的任何脚本语言。用户界面及本文档中的示例使用的都是 Python 2.6 版。

请参见第 853 页的“[配置高级插件属性](#)”。

关于 Data Insight 查找插件

Symantec Data Insight 查找插件会从 Symantec Data Insight Management Server 检索数据，并在生成事件时，使用该数据填充 Network Discover 事件的属性。Data Insight 查找插件将 Symantec Data Loss Prevention 连接至 Symantec Data Insight 以检索属性值。Data Insight 可用于提供事件的粒度上下文，包括最新的数据所有者信息。事件属性的值是在“事件快照”屏幕中查看和填充。

Data Insight 查找插件需要一个不同于 Symantec Data Loss Prevention 授权许可的 Data Insight 许可证。如果您的系统未获得 Data Insight 许可，Data Insight 查找插件将不可用。如果您已获得 Data Insight 授权，请参阅《Symantec Data Loss Prevention Data Insight 操作指南》，了解有关与 Data Insight 集成的详细信息。

关于自定义（旧版）查找插件

您可以使用自定义（旧版）查找插件，将旧版的自定义 Java 查找插件迁移至 Enforce Server 管理控制台。自定义 Java 查找插件不再是创建新插件的首选方法，因此，会提供存在于此处的信息来支持将旧版自定义 Java 查找插件迁移至 Symantec Data Loss Prevention 11.6 版的用户界面。请考虑使用脚本查找插件或其中一种其他支持的查找插件（例如 CSV 或 LDAP）来重写此类插件，作为迁移旧版自定义 Java 查找插件的替代方案。

请参见第 838 页的“[查找插件的类型](#)”。

注意：自定义（旧版）查找插件仅能用于迁移使用查找 Java API 所实施的旧版查找插件。已弃用对新自定义 Java 查找插件的支持。

请参见第 876 页的“[配置迁移的自定义（旧版）查找插件](#)”。

关于查找参数

创建事件时，Enforce Server 会生成事件属性，并在这些属性中填入从事件捕获的数据。您要使用一个或多个事件属性作为查找参数键来检索外部数据，并将自定义属性填入已从外部系统检索的值。您在“[查找参数](#)”屏幕中，选择要用于查找插件的查找参数。在外部数据源中必须至少存在一个查找参数，才能运行查找。

一些属性是针对所有事件类型创建的，而另一些属性则专属的于事件类型。例如，事件属性 `sender-email` 专属于 SMTP 事件。专属于端点和发现事件的属性以标识符开头，例如 `discover-name` 和 `endpoint-machine-name`。为了方便管理，查找参数进行了分组。事件会在所启用的每个查找参数组中公开所有查找参数。查找时，该组中的某些名称/值对可能毫无用处（视事件类型而定）。例如，`sender-email` 参数的属性值对于发现事件而言为 `null` (`sender-email=null`)。

查找插件不会更改系统定义的查找参数值。插件仅使用这些参数作为关键字来执行查找，并填入自定义属性。例如，如果查找插件使用 `subject` 查找参数，此属性的值就不会由外部数据源中此属性的值所更改；Enforce Server 会在进行查找之后，忽略该值。不过有两个例外：`data-owner-name` 和 `data-owner-email`。这些系统定义的事件属性的工作方式如同自定义属性，且其值会由检索的值填入。

当您将关键字映射至数据源时，插件会依序搜索关键字，直到找到第一个相符的值为止。找出匹配的值之后，插件就会停止搜索关键字。插件将使用包含第一个匹配值的行中的数据来填充相关自定义属性。因此，关键字值不会结合使用，而是将找到的第一个值作为关键字。由于插件在找到第一个匹配值后将停止搜索，因此属性映射中的 `keys` 的排列顺序非常重要。对于查找插件属性映射语法间的细微差别，请参阅个别的属性映射主题和示例。

若要执行查找，您必须将至少一个查找参数键映射到外部数据源中的字段。您启用的每个查找参数组都是利于 Enforce Server 执行的独立数据库查询。在开始查找

前，会针对每个事件执行所有数据库查询。为了避免不需要的数据库查询所带来的性能影响，请仅启用查找插件所需要的属性组。

因为插件在找到第一个匹配的查找参数键值对后会停止搜索，因此，属性映射中列出 keys 的顺序非常关键。请参阅实施的特定目标类型的插件类型的属性映射范例。

请参见第 846 页的“[选择查找参数](#)”。

关于插件部署

查找插件是以通过用户界面启用的方式进行部署。您必须启用每个插件，即使只有一个查找插件，也不例外。如果启用多个插件，您要将这些插件链接在一起，然后指定其执行顺序。

选择的查找参数键全局适用于所有部署的查找插件。如果重新加载插件，则也会重新加载所有部署的插件。

每个 Enforce Server 实例只能部署一个 CSV 查找插件和一个 Data Insight 查找插件。

请参见第 850 页的“[启用查找插件](#)”。

关于插件链接

当您创建查找插件时，您要将查找参数键和自定义属性映射到外部数据源中的字段。所有部署的查找插件都会收到相同属性映射的引用。这可让插件依序链接在一起执行。

在查找插件链中，第一个插件使用 Enforce Server 传递给它的查找参数来查找属性值。第二个插件使用第一个插件传递给它的数据，包含查找参数以及上一个查找所创建的任何变量。这会依序或依链接中的所有插件继续。

当必须从不同的源提取信息以填充事件的自定义属性时，插件链非常有用。另外，在解锁正确数据所需的关键字之间存在差异或依赖关系时，插件链也非常有用。

例如，请考虑下列插件链：

1. 脚本查找插件会使用一个或多个参数执行 DNS 查找。
2. CSV 查找插件会使用脚本查找的结果，从 CSV 文件检索提取自资产管理系统的事件数据。
3. LDAP 查找插件会使用 CSV 查找的结果，从公司的 LDAP 目录获取数据。

请参见第 850 页的“[链接查找插件](#)”。

请参见第 872 页的“[链接多个脚本查找插件](#)”。

关于升级查找插件

在 Symantec Data Loss Prevention 11.6 版之前，查找插件是使用属性文件手动实现的，没有用来配置查找插件的用户界面。查找插件用户界面是 11.6 版的新功能。

如果您升级到 11.6 版，现有的查找插件会自动升级到新的框架并添加到用户界面中以便进行配置和部署。另外，升级之后，插件状态将保持不变；也就是说，如果在升级之前，某个插件处于启用状态，则升级之后，它应该在用户界面中处于打开状态。

如果查找插件的升级不成功，系统会显示下列错误消息：

```
INFO: IN PROCESS: Errors detected in lookup plugin configuration.  
Your lookup plugins may require manual configuration after the upgrade.
```

在此情况下，请在“系统”>“查找插件”屏幕检查该插件，然后按照该文档提供的说明，进行手动配置。有关查找插件升级的相关已知问题，请参阅 11.6 版的《Symantec Data Loss Prevention 版本说明》。

实施和测试查找插件

下表介绍了用于实施和测试查找插件的工作流程。链接部分更详细地介绍了这些步骤。

表 50-2 实施和测试查找插件

步骤	说明
1	确定要提取并作为自定义属性加载到事件中的外部数据。 请参见第 834 页的“ 关于使用自定义属性 ”。
2	确定从哪些源获得自定义属性数据，以及适合用于检索此信息的查找插件。 请参见第 838 页的“ 查找插件的类型 ”。
3	为要在事件快照和报告中的外部数据的各个块分别创建一个自定义属性。 请参见第 835 页的“ 配置自定义属性 ”。
4	确定哪些查找参数组包括从外部源提取相关数据所需的特定查找参数。 请参见第 840 页的“ 关于查找参数 ”。

步骤	说明
5	<p>对插件进行配置，使其从外部数据源提取数据并填充自定义属性。</p> <p>请参见第 854 页的“配置 CSV 查找插件”。</p> <p>请参见第 862 页的“配置 LDAP 查找插件”。</p> <p>请参见第 867 页的“配置脚本查找插件”。</p> <p>请参见第 876 页的“配置迁移的自定义（旧版）查找插件”。</p>
6	<p>在 Enforce Server 上启用插件。</p> <p>请参见第 850 页的“启用查找插件”。</p>
7	<p>设置多个插件的执行顺序。</p> <p>请参见第 850 页的“链接查找插件”。</p>
8	<p>验证权限。最终用户必须具有“查找属性”权限，才能使用查找插件查找属性值。</p> <p>请参见第 85 页的“配置角色”。</p>
9	<p>生成事件。该事件所属的类型必须显示一个或多个您已指定作为参数键的事件属性。</p> <p>请参见第 330 页的“配置策略”。</p>
10	<p>查看事件详细信息。对于您生成的事件，请转到“事件快照”屏幕。在“属性”部分，您应该能够看到自己创建的自定义属性。请注意，这些属性尚未填充数据（即还没有值）。如果您看不到自定义属性，请确认权限以及是否已创建自定义属性。</p>
11	<p>如果查找插件正确实施，您会看到“查找”按钮在“事件快照”的“属性”部分可用。单击“查找”，您就会看到每个自定义属性填充了值。首次查找后，连接状态保持不变并且后续事件的自定义属性会由该查找插件自动进行填充；因此，补救者不需要对后续事件单击“查找”。如果需要，您可以重新加载插件。</p> <p>请参见第 851 页的“排除查找插件故障”。</p> <p>请参见第 851 页的“重新加载查找插件”。</p>

管理和配置查找插件

“系统”>“查找插件”屏幕是用于创建、配置和管理查找插件的主页面。查找插件用于补救以便从外部数据源检索事件相关数据并填充事件属性。

请参见第 837 页的“[关于查找插件](#)”。

您可以在“**查找插件列表页面**”中创建和配置查找插件。

表 50-3 创建和配置查找插件

操作	说明
新建插件	选择此选项可创建新插件。 请参见第 845 页的“ 创建新的查找插件 ”。
修改插件链	选择此选项可启用（部署）插件并设置多个插件的查找顺序。 请参见第 850 页的“ 启用查找插件 ”。
查找参数	选择此选项可选择要使用哪些查找参数组作为键，以便从外部数据源填充属性字段。 请参见第 846 页的“ 选择查找参数 ”。
重新加载插件	选择此选项可在更改已启用的插件后或外部数据更新时刷新系统。此操作将按顺序自动执行已启用的查找，并在创建事件时填充事件。 请参见第 851 页的“ 重新加载查找插件 ”。

对每一个配置的查找插件，系统会在“[查找插件列表页面](#)”中显示以下信息。您可以使用此信息来管理查找插件。

表 50-4 管理查找插件

显示字段	说明
执行顺序	此字段显示系统执行查找插件的顺序。 请参见第 850 页的“ 启用查找插件 ”。
名称	此字段显示每个查找插件的用户定义名称。 单击“名称”链接可编辑该插件。 请参见第 845 页的“ 创建新的查找插件 ”。
类型	此字段显示查找插件的类型。每一个 Enforce Server 实例可以配置一个 CSV 和一个 DataInsight 查找插件。您可以配置 LDAP、脚本和自定义（旧版）查找插件的多个实例。 请参见第 838 页的“ 查找插件的类型 ”。
说明	此字段显示每个查找插件的用户定义说明。 请参见第 842 页的“ 实施和测试查找插件 ”。
状态	此字段显示每个查找插件的状态：“打开”（绿色）或“关闭”（红色）。若要编辑插件的状态，请单击“修改插件链”。 请参见第 850 页的“ 启用查找插件 ”。

对于每一个配置的查找插件，您可以在“[查找插件列表页面](#)”中执行以下管理功能。

表 50-5 对查找插件进行排序和分组

操作	说明
编辑	单击“操作”列中的铅笔图标可编辑插件。
删除	单击“操作”列中的 X 图标可删除插件。该操作的执行取决于您确认还是取消它。
排序	按升序或降序对所选显示列进行排序。
分组	根据所选显示列对插件进行分组。例如，假设您有多个插件，将它们按照“类型”或“状态”进行分组可能很有用。

创建新的查找插件

您必须具有服务器管理员权限才能创建和配置查找插件。

请参见第 85 页的[“配置角色”](#)。

创建新的查找插件

- 1 导航至 Enforce Server 管理控制台的“系统”>“查找插件”。
- 2 在“[查找插件列表页面](#)”屏幕上，单击“新建插件”。
- 3 选择您要创建并配置的查找插件类型。

CSV

请参见第 854 页的[“配置 CSV 查找插件”](#)。

LDAP

请参见第 862 页的[“配置 LDAP 查找插件”](#)。

脚本

请参见第 867 页的[“配置脚本查找插件”](#)。

Data Insight

自定义 (旧版)

请参见第 876 页的[“配置迁移的自定义（旧版）查找插件”](#)。

4 单击“保存”应用查找插件配置。

如果插件成功保存，系统会显示成功（绿色）消息；如果插件配置错误且无法保存，则会显示错误（红色）消息。

请参见第 851 页的“[排除查找插件故障](#)”。

5 单击“修改插件链”，然后启用查找插件并链接多个插件。

请参见第 850 页的“[启用查找插件](#)”。

请参见第 850 页的“[链接查找插件](#)”。

选择查找参数

“系统”>“查找插件”>“编辑查找插件参数”页面会列出您选择要触发查找属性值的“查找参数键”。查找参数键会组织成属性组。在此屏幕所做的选择会应用到 Enforce Server 上已部署的所有查找插件中。

若要执行查找，您必须将至少一个查找参数键映射到外部数据源中的字段。您启用的每个查找参数组都是利于 Enforce Server 执行的独立数据库查询。在开始查找前，会针对每个事件执行所有数据库查询。为了避免不需要的数据库查询所带来的性能影响，请仅启用查找插件所需要的属性组。

因为插件在找到第一个匹配的查找参数键值后会停止搜索，因此，属性映射中列出 keys 的顺序非常关键。请参阅实施的特定插件类型的属性映射示例，以取得详细信息。

请参见第 840 页的“[关于查找参数](#)”。

启用一个或多个查找参数键

- 1 导航至 Enforce Server 管理控制台的“系统”>“查找插件”。
- 2 在“查找插件列表页面”上单击“查找参数”。
- 3 在“编辑查找插件参数”页面选择“检查”一个或多个属性组。

单击“视图属性”以查看该属性组的所有键。

- 附件 [表 50-6](#)
- 事件 [表 50-7](#)
- 消息 [表 50-8](#)
- 策略 [表 50-9](#)
- 接受者 [表 50-10](#)
- 发送者 [表 50-11](#)
- 服务器 [表 50-12](#)

■ 监视 [表 50-13](#)

■ 状态 [表 50-14](#)

■ ACL [表 50-15](#)

4 保存配置。

验证成功消息，以表示所有启用的插件都已重新加载。

表 50-6 附件查找参数

查找参数关键字	说明和注释
attachment-nameX	附加文件的名称，其中 X 是区分多个附件的唯一索引，例如：attachment-name1、attachment-size1；attachment-name2、attachment-size2 等。
attachment-sizeX	附加文件的原始大小，其中 X 是区分多个附件的唯一索引。请参阅以上示例。

表 50-7 事件查找参数

查找参数关键字	说明
date-detected	检测到事件的日期和时间，例如：date-detected=Tue May 15 15:08:23 PDT 2012。
incident-id	Enforce Server 分配的事件 ID。在事件报告中可以看到相同的 ID。例如：incident-id=35。
protocol	用于传输违规邮件的网络协议的名称，如 SMTP、HTTP 等。例如：protocol=Email / SMTP。
data-owner-name	负责补救事件的人员。系统不会填入此属性。相反，此属性是在“事件快照”屏幕的“事件详细信息”部分中手动设置，或使用查找插件自动设置。 可自动将基于此属性的报告发送给数据所有者以进行补救。
data-owner-email	负责补救事件的人员的电子邮件地址。系统不会填入此属性。相反，此属性是在“事件快照”屏幕的“事件详细信息”部分中手动设置，或使用查找插件自动设置。

表 50-8 邮件查找参数

查找参数关键字	说明
date-sent	发送邮件的日期和时间（如果是电子邮件）。例如：date-sent=Mon Aug 15 11:46:55 PDT 2011。
subject	邮件主题（如果是电子邮件事件）。

查找参数关键字	说明
file-create-date	文件在其当前位置创建的日期，无论它是最初就在此处创建还是从其他位置复制而来。从操作系统检索。
file-access-date	检查文件的日期。
file-created-by	将文件置于端点计算机的用户。
file-modified-by	针对发生违规复制操作的计算机的完全限定用户凭据。
file-owner	用户名或违规文件所在计算机的名称。
discover-content-root-path	导致发现事件的文件的根路径。
discover-location	导致发现事件的文件的完整路径。
discover-name	违规文件的名称。
discover-extraction-date	发现扫描时从封装文件中提取子文件的日期。
discover-server	要扫描的存储库名称。
discover-notes-database	适用于 Lotus Notes 存储库发现扫描的特定属性。
discover-notes-url	适用于 Lotus Notes 存储库发现扫描的特定属性。
endpoint-volume-name	发生端点事件的本地驱动器的名称。
endpoint-dos-volume-name	发生端点事件的本地驱动器的 Windows 名称。
endpoint-application-name	最近用来打开（或创建）违规文件的应用程序的名称。
endpoint-application-path	用于创建或打开违规文件的应用程序的路径。
endpoint-file-name	违规文件的名称。
endpoint-file-path	文件被复制到的位置。

表 50-9 策略查找参数

查找参数关键字	说明和注释
policy-name	违规策略的名称，例如：policy-name=Keyword Policy。

表 50-10 接受者查找参数

查找参数关键字	说明
recipient-emailX	接受者的电子邮件地址，其中 X 是区分多个接受者的唯一索引，例如：recipient-email1、recipient-ip1、recipient-url1；recipient-email2、recipient-ip2、recipient-url2 等。
recipient-ipX	接受者的 IP 地址，其中 X 是区分多个接受者的唯一索引。请参阅以上示例。
recipient-urlX	接受者的 URL，其中 X 是区分多个接受者的唯一索引。请参阅以上示例。

表 50-11 发件人查找参数

查找参数关键字	说明
sender-email	针对适用于电子邮件(SMTP)的 Network Prevent 事件的发件人电子邮件地址。
sender-ip	针对通过 SMTP 之外协议的端点和网络事件的发件人 IP 地址。
sender-port	针对通过 SMTP 之外协议的网络事件的发件人端口。
endpoint-user-name	发生违规时，已登录端点计算机的用户。
endpoint-machine-name	违规文件所在端点计算机的名称。

表 50-12 服务器查找参数

查找参数关键字	说明和注释
server-name	报告事件的检测服务器的名称。此名称是在部署检测服务器时，由用户定义及输入。例如：server-name=My Network Monitor。

表 50-13 监视查找参数

查找参数关键字	说明
monitor-name	报告事件的检测服务器的名称。此名称是在部署检测服务器时，由用户定义及输入。例如：server-name=My Network Monitor。
monitor-host	报告事件的检测服务器的 IP 地址。例如：monitor-host=127.0.0.1
monitor-id	检测服务器的系统定义数字标识符。例如：monitor-id=1。

表 50-14 状态查找参数

查找参数关键字	说明和注释
incident-status	事件的当前状态。例如：incident-status=incident.status.New。

表 50-15 ACL 查找参数

查找参数关键字	说明
acl-principalX	字符串，指示应用 ACL 的用户或组。
acl-typeX	字符串，指示 ACL 是应用于文件还是应用于共享。
acl-grant-or-denyX	字符串，指示 ACL 将授予还是拒绝权限。
acl-permissionX	字符串，指示 ACL 表示读取访问还是写入访问。

启用查找插件

若要启用查找插件，您必须将其状态从“关闭”（配置查找插件后的初始状态）更改为“打开”。您可在“系统”>“查找插件”>“修改查找插件执行链”启用查找插件。

请参见第 841 页的[“关于插件部署”](#)。

启用查找插件

- 1 导航至 Enforce Server 管理控制台的“系统”>“查找插件”。
- 2 在“查找插件列表页面”上，单击“修改插件链”。
- 3 在“专用操作”字段中，选择（勾选）“打开”选项。
- 4 单击“保存”应用配置。

如果无法加载插件，系统将会报告错误，而且插件状态将保持“关闭”。在此情况下，请检查最新 Tomcat 日志文件中的错误。

请参见第 851 页的[“排除查找插件故障”](#)。

链接查找插件

通过“系统”>“查找插件”>“修改查找插件执行链”可以启用查找插件，并指定部署多个查找插件时的执行顺序。

请参见第 850 页的[“启用查找插件”](#)。

如果启用多个查找插件，则必须指定其执行顺序。当插件链接在一起时，来自前一个插件的输入会当作后续查找插件的属性使用。

请参见第 841 页的[“关于插件部署”](#)。

链接多个查找插件

- 1 导航至 Enforce Server 管理控制台的“系统”>“查找插件”。
- 2 在“查找插件列表页面”上，单击“修改插件链”。
- 3 在“执行顺序”字段中，从下拉菜单选取执行顺序。
- 4 单击“保存”以应用链接配置。

重新加载查找插件

如果您更改了查找插件的配置，或外部数据已更改，则需要重新加载查找插件。重新加载插件会刷新系统并且自动按顺序执行已启用的查找，然后在检测到事件时填充事件属性。

此外，进行更改时会重新加载插件，如果下列任何情况属实，您可能也需要重新加载查找插件：

- 插件有问题并且系统已将其卸载，但是现在该问题已得到解决。
- 由于某种原因网络已关闭或断开连接，但是现在运行正常。
- 插件在高速缓存中存储数据，而您想要手动更新该高速缓存。

重新加载查找插件

- 1 导航至 Enforce Server 管理控制台的“系统”>“查找插件”。
- 2 单击“重新加载插件”以重新加载所有启用的插件。

注意：管理员也可以从“系统”>“事件数据”>“属性”屏幕的“自定义属性”选项卡中，重新加载查找插件。

排除查找插件故障

Symantec Data Loss Prevention 提供查找插件特定的日志记录和错误消息。最常见的错误涉及因为一个或多个错误配置而导致无法加载插件。如果查找插件无法加载，系统会将异常记录为系统事件屏幕和 Tomcat 日志中的警告。另外，属性映射和插件执行链也会记录在 Tomcat 日志中。

对查找插件错误进行故障排除

- 1 导航到“系统”>“服务器”>“概述”屏幕，然后在页面底端的“最近的错误和警告事件”表格中查找所有警告。
- 2 在 Enforce Server 主机上，打开日志文件
`\SymantecDLP\protect\Enforce\logs\tomcat\localhost.<date>.log`。

- 3 对 Tomcat localhost 日志文件中显示的错误进行故障排除。

表 50-16

- 4 如果插件失败，但没有日志记录错误，请配置查找插件的详细日志记录。

请参见第 852 页的“[配置查找插件的详细记录](#)”。

- 5 请参阅特定插件的故障排除主题。

请参见第 859 页的“[测试 CSV 查找插件并进行故障排除](#)”。

请参见第 865 页的“[测试和故障排除 LDAP 查找插件](#)”。

请参见第 873 页的“[脚本查找插件教程](#)”。

表 50-16 排除查找插件故障

问题	解决方案
查找插件无法加载	<p>如果插件无法加载，请在日志文件中搜索类似以下的消息：</p> <pre>SEVERE [com.vontu.enforce.workflow.attributes.AttributeLookupLoader] Error loading plugin [<Plugin_Name>]</pre> <p>请注意，此错误消息类型后面的 Cause 部分。任何这类条目将说明为何插件无法加载。</p>
查找未填入属性	如果插件加载，但没有填入属性，则查看日志中的属性映射。验证值是否填入，包括您启用的查找参数的值。为此，请搜索已启用的查找参数键，例如 <code>sender-email</code> 。

配置查找插件的详细记录

系统为查找插件提供了详细日志记录配置。可以在“系统”>“日志”>“配置”选项卡中配置查找插件的日志记录级别。通过配置查找插件的日志，可在 Tomcat localhost 日志中提供更详细的消息。

请参见第 851 页的“[排除查找插件故障](#)”。

配置和收集查找插件的日志

- 1 导航至“系统”>“服务器”>“日志”屏幕。
- 2 选择“配置”选项卡。
- 3 对于**EnforceServer**，从“诊断日志记录设置”下拉菜单中选择“自定义属性查找日志记录”条目。
- 4 单击“配置日志”。
- 5 在“收集”选项卡中，针对 Enforce Server 选择以下“调度”和“跟踪日志”。

- 6 单击“收集日志”。
- 7 在页面底部，单击“下载”下载日志。使用“刷新”按钮刷新页面。此时日志将打包到一个 ZIP 文件中。
- 8 打开该 ZIP 文件，或者将其保存到文件系统，然后解压缩。
- 9 导航至目录 \SymantecDLPLogs.zip\Enforce\logs\tomcat。
- 10 使用文本编辑器打开文件 localhost.<date>.log。打开具有最新日期的文件。
- 11 搜索查找插件的名称。您应该会看到多条消息。
- 12 根据需要，验证文件 \Protect\config\ManagerLogging.properties 中的查找插件日志记录属性。

```
com.vontu.logging.ServletLogHandler.level=FINEST
com.vontu.enforce.workflow.attributes.CustomAttributeLookup.
level=FINEST
com.vontu.lookup.level=FINEST
```

配置高级插件属性

\<SymantecDLP_Home>\protect\config\Plugins.properties 文件中包含用于配置查找插件的多个高级属性。一般情况下，不需要修改这些属性，除非根据以下说明有必要修改时才进行修改。

表 50-17 查找插件的高级属性

属性	默认值	说明
AttributeLookup. output.parameters	<i>data-owner-name,</i> <i>data-owner-email</i>	<p>“属性查找输出参数”属性是一个用逗号分隔的列表，其中指定了查找插件可以修改的参数。一般情况下，查找参数键的值是在创建事件时由系统设置的。由于这些参数用于查找自定义属性值，因此，如果它们与系统定义的值不同，则不会被查找的值所修改。</p> <p>不过，通过此属性可根据检索的值来修改“数据所有者名称”和“数据所有者电子邮件”属性的输出。这些参数是在查找插件配置和脚本中指定的，使用的语法与自定义属性相同。这两个属性均通过选择“事件”属性组来启用。</p> <p>您可以通过删除其中一个属性或同时删除这两个属性来禁用此功能。如果删除，则其中任何一个参数的输出都不会被查找的值所更改。</p>

属性	默认值	说明
AttributeLookup.timeout	60000	<p>为避免系统因意外查找问题而冻结，Enforce Server 会限制指定给每个查找插件的时间量。此超时在 Plugins.properties 文件的 com.vontu.api.incident.attributes.AttributeLookup.timeout 属性中进行配置。</p> <p>如果查找超过 60 秒默认超时，事件属性框架会卸载关联的插件。如果存在失控查找，Enforce Server 将无法针对任何后续事件执行该特定的查找。如果插件经常超时，您可以延长超时时长，方法是修改超时时长（以毫秒为单位）。</p> <p>注意：请注意，由于属性查找速度缓慢，增大此值可能会导致事件处理速度变慢。</p>
AttributeLookup.auto	true	<p>自动查找属性指定当检测到新事件时，是否应自动触发查找。在执行初始查找之后，此属性会使用已部署的查找插件自动填充事件属性。</p> <p>若要禁用自动查找，您可以将属性值更改为 false。如果禁用此属性，补救者必须为每一个事件单击“查找”。</p>
AttributeLookup.reload	false	自动插件重新加载属性指定是否应在每天凌晨 3:00 自动重新加载所有插件。更改为 true 可启用此功能。

配置 CSV 查找插件

每一个 Enforce Server 实例只能配置一个 CSV 查找插件。

请参见第 838 页的“[关于 CSV 查找插件](#)”。

表 50-18 配置 CSV 查找插件

步骤	操作	说明
1	创建自定义属性。	<p>针对您要查找的信息定义自定义属性。</p> <p>请参见第 836 页的“手动设置自定义属性的值”。</p>
2	创建 CSV 数据源文件。	<p>该 CSV 文件中包含要用于填充事件补救的自定义属性的数据。</p> <p>请参见第 855 页的“创建 CSV 文件的要求”。</p>
3	创建新的 CSV 插件。	请参见第 845 页的“ 创建新的查找插件 ”。
4	命名并说明插件。	名称字符串不得超过 100 个字符。建议您输入查找插件的说明。
5	指定文件路径。	<p>提供 CSV 文件的路径。CSV 文件必须是 Enforce Server 的本地文件。</p> <p>请参见第 856 页的“指定 CSV 文件路径”。</p>

步骤	操作	说明
6	选择文件分隔符。	指定 CSV 文件中使用的分隔符。建议您使用管道分隔符 []。 请参见第 856 页的“ 选择 CSV 文件分隔符 ”。
7	选择文件编码。	例如：UTF-8 请参见第 857 页的“ 选择 CSV 文件字符集 ”。
8	映射属性。	将系统和自定义属性映射到 CSV 文件列标题，并定义用于提取自定义属性数据的键。键映射到列标题，而非自定义属性。 语法如下： <code>attr.attribute_name=column_head</code> <code>keys=column_head_first:column_head_next:column_head_3rd</code> 请参见第 857 页的“ 将属性和参数键映射至 CSV 字段 ”。
9	保存插件。	验证是否显示了插件的正确保存消息。
9	选择查找参数键。	定义用于提取自定义属性数据的键。 请参见第 846 页的“ 选择查找参数 ”。
10	启用查找插件。	必须在 Enforce Server 上启用 CSV 查找插件。 请参见第 850 页的“ 启用查找插件 ”。
11	对插件进行故障排除。	请参见第 859 页的“ 测试 CSV 查找插件并进行故障排除 ”。
11	测试查找插件。	

创建 CSV 文件的要求

CSV 查找插件需要存储在 Enforce Server 上的 CSV 文件。

当创建 CSV 文件时，请谨记以下要求：

- CSV 文件的第一个数据行必须包含列标题。
- 列标题字段不能是空白的。
- 确保列标题字段的结尾没有空格。
- 确保所有行有相同列数。
- 文件的每一行必须是单独、无间断的行。
- 文件中的一个或多个列都可用作数据查找的关键字字段。您应在列标题用作关键字字段的属性映射中指定。您也可以指定关键字字段搜索顺序。常见关键字字段通常包括电子邮件地址、域\用户名（针对端点事件）和用户名（针对存储事件）。

- 关键字字段列中的数据值必须是唯一的。如果将多个列用作关键字字段（例如，`EMP_EMAIL` 和 `USER_NAME`），则每行中的值的组合必须是唯一的。
- 数据行中的字段（列标题行除外）可以为空，但每行中必须至少一个关键字字段包含数据。
- 在列标题和数据行中，必须对所有值使用相同类型的分隔符。
- 如果 CSV 文件是只读的，请确保 CSV 文件在文件的尾端有新的一行。系统将尝试在执行插件时，将新的一行加入到文件中，但是如果文件是只读的，系统就无法执行此操作，因此插件将不会加载。
- 对于发现扫描事件，`file-owner` 查找参数不包括域。要将 `file-owner` 用作关键字，与 `file-owner` 对应的 CSV 文件列应为 `owner` 格式。格式 `DOMAIN\owner` 会导致查找失败。此限制只适用于发现事件，其他类型的事件可以包括域。
例如，列标题行和以竖线分隔的 CSV 文件的数据行可能如下所示：

```
email|first_name|last_name|domain_user_name|user_name|department|manager|manager_email
jsmith@acme.com|John|Smith|CORP\jsmith1|jsmith1|Accounting|Mei Wong|m Wong@acme.com
```

- 如果在 CSV 文件中超过 10% 的行违反上述任一要求，则插件不会加载。
- 为了准确地进行查找，CSV 文件需要保持最新。

请参见第 838 页的“[关于 CSV 查找插件](#)”。

指定 CSV 文件路径

若要配置 CSV 查找插件，您必须为 CSV 文件的位置指定“**CSV 文件路径**”属性。CSV 文件必须保存在 Enforce Server 本地。

您可以输入文件的绝对路径，也可以输入文件的相对路径。例如：

- `../../../../vontu_csv_lookup_file/senders2.csv`
- `C:/vontu_csv_lookup_file/senders2.csv`

在 Windows 上，您可以使用正斜线或反斜线。例如：

`C:/Vontu/Protect/plugins/employees.csv` 或

`C:\Vontu\Protect\plugins\employees.csv`。在 Linux 上，您只能使用正斜线。

当您保存配置时，系统会验证文件路径。如果系统找不到文件，则会报告一个错误，而且不会让您保存配置。请确保 CSV 文件未打开，且存储在 Enforce Server 本地。

选择 CSV 文件分隔符

使用“**分隔符**”属性指定 CSV 文件的分隔符。

支持以下分隔符：

- 逗号
- 坚线
- 制表符
- 分号

建议的做法是使用坚线字符（“|”）作为分隔符。不建议使用以逗号分隔符，因为数据字段中的数据通常包含逗号。例如，街道地址可能会包含逗号。

选择 CSV 文件字符集

您必须为 CSV 文件指定字符集。默认值为 UTF-8。

所有支持的字符集都列在了下拉菜单中。

将属性和参数键映射至 CSV 字段

若要配置CSV查找插件，您要在“属性映射”字段中输入执行代码。此代码会将查找参数键和自定义属性映射至 CSV 文件中的列标题。一个或多个属性/列对用来将事件属性映射至列标题。属性映射中的 keys 属性会标识要用于查找的列。

下面是 CSV 文件属性映射的示例：

```
attr.Store-ID=store-id
attr.Store\ Address=store_address
attr.incident-id=incident-id-key
attr.sender-email=sender-email-key
keys=sender-email-key:incident-id-key
```

将属性映射至 CSV 文件数据时，请记住此示例，并遵从下列语法规则。

表 50-19 CSV 文件的属性映射语法

示例和语法	说明
attr.Store-ID=store-id attr.attribute_name=column_head	属性会映射至属性/列对中的列标题名称。 此处， Store-ID 为自定义属性，而 store-id 则是 CSV 文件中的列标题名称。
attr.Store\ Address=store_address attr.attribute\ name=column\ head	在等号(=)前后允许使用空格 (LDAP 查找插件除外)。 属性和列名称中的空格前面必须加上反斜线。 此处，自定义属性名称为 Store Address 。

示例和语法	说明
<pre>attr.Store-ID=store-id attr.Store\ Address=store_address attr.attribute_name=column_head attr.attribute_name=column_head</pre>	每个属性/列对都是在独立的一行输入。
<pre>attr.Store\ Address=STORE_ADDRESS</pre>	所有语法均区分大小写。 标识符 attr. 必须是小写。 事件属性必须精确匹配系统定义字符串。
<pre>attr.incident-id=incident-id-key attr.sender-email=sender-email-key attr.attribute_name=column_head</pre>	系统属性会映射至列标题名称。列名称不必匹配系统属性，也不需要 key 这个字。
<pre>keys=sender-email-key:incident-id-key keys=<column_name_1st>:<column_name_2nd></pre>	关键字会将列名称标题映射至您要用来查找属性值的事件属性关键字。关键字会映射至列标题名称，而非事件属性名称。外观的顺序会决定优先级。一旦第一个事件位于 CSV 文件之后，就会填入其他属性。

CSV 属性映射示例

请考虑 CSV 查找插件的另一个映射示例。

```
attr.sender-email = Email
attr.endpoint-user-name = Username
attr.file-owner = File-owner
attr.sender-ip = IP

attr.First\ Name = FIRST_NAME
attr.Last\ Name = LAST_NAME
attr.Business\ Unit = Org
attr.Manager\ Email = Mgr_email
attr.Employee\ ID = EMPLOYEE_NUMBER
attr.Phone\ Number = Phone
attr.Manager\ Last\ Name = Mgr_lastname
attr.Manager\ First\ Name = Mgr_firstname
attr.Employee\ Email = Emp_email

keys = Email:Username:File-owner:IP
```

关于此示例，请注意下列几项：

- 前 4 行会将查找参数映射到列标题。
- 剩下的 9 行会将自定义属性映射到列标题。
- 在属性或列名称的每一个空格字符实例的前面加上反斜线。在本示例中，`attr.Employee\ Email = Emp_email` 会将 **Employee Email** 自定义属性映射到 **emp_email** 列标题。
- `keys` 属性会标识并排序用于提取自定义属性数据的关键字。每个关键字会以冒号分隔。关键字的排列顺序将决定搜索次序。在 `keys = Email:Username:File-owner:IP` 示例中，插件会先搜索 `Email` 列，查找与已传递到插件的 `sender-email` 的查找参数值相匹配的值。如果未找到相匹配的值，插件会接着搜索 `Username` 列，查找与 `endpoint-user-name` 查找参数相匹配的值。如果在该列中也没有找到匹配值，插件会继续搜索下一个关键字 (`File-owner`)，依此类推。
- 插件会在找到第一个匹配的参数键/值对后停止搜索。因此，您列出 `keys` 列标题的顺序非常关键。

测试 CSV 查找插件并进行故障排除

如果插件未加载，或者插件加载，但无法按所查找的值填入自定义属性，请如下进行故障排除：

测试 CSV 查找插件并进行故障排除

- 1 验证 CSV 文件是否符合要求。如果在 CSV 文件中超过 10% 的行违反上述 CSV file 文件任何要求，则查找插件不会加载。
请参见第 855 页的“[创建 CSV 文件的要求](#)”。
- 2 验证所选择的分隔符与 CSV 文件中使用的相同。请注意系统默认为逗号，但建议使用竖线符号。
请参见第 856 页的“[选择 CSV 文件分隔符](#)”。
- 3 检查属性映射。不会对属性映射提供验证。请确保属性映射遵循语法。
常见的语法错误包括：
 - 属性映射字段中的每个条目均区分大小写。
 - 必须由反斜线标识属性和列名的间隔。
 - 对于每个“属性=列”对，在等号 (=) 右边的数据必须是列标题名称。
 - 键是列标题名称，不是事件属性。
- 4 如果插件无法加载，或插件无法返回查找的值，请检查文件
`\SymantecDLP\Protect\logs\tomcat\localhost.<latest-date>.log`。

- 检查数据库和表格是否已创建，且 CSV 文件已加载该表格。若要验证，请查找类似以下的数据行：

```
INFO [com.vontu.lookup.csv.CsvLookup]
creating database
create table using SQL
importing data from file into table LOOKUP having columns
```

注意：要处理大文件，CSV 查找插件会使用内存内数据库(Apache Derby)。每一台 Enforce Server 只能运行一个 Derby 实例。如果上一个实例正在运行，CSV 查找插件就不会加载。如果数据库和表格没有创建，请重新启动 Vontu Manager 服务并重新加载插件。

5 如果插件无法返回查找的值，请检查文件

\SymantecDLP\Protect\logs\tomcat\localhost.<latest-date>.log。

查找指出“SQL query did not return any results”的警告消息。在这种情况下，请确保属性映射匹配 CSV 列标题，如有进行更改，则重新加载插件。

请参见第 851 页的[“排除查找插件故障”](#)。

CSV 查找插件教程

本教程提供实施简单 CSV 查找插件的说明。本教程的目的是从实机操作方式，为您介绍查找插件的功能。如果您已有生成事件、创建自定义属性和实施查找插件等经验，则本教程可能过于简单。

请参见第 838 页的[“关于 CSV 查找插件”](#)。

实施简单 CSV 查找插件

1 在“系统”>“属性”>“自定义属性”创建下列自定义属性：

- 管理员
- 部门
- 电子邮件地址

2 创建包含下列数据、以竖线分隔的 CSV 文件。

SENDER|MGR|DEPT|EMAIL
emp@company.com|Merle Manager|Engineering|rmanager@company.com

- 3 将 CSV 文件保存到安装 Enforce Server 的同一卷磁盘机。

例如: C:\SymantecDLP\Protect\plugins\lookup\csv_lookup_file.csv。

- 4 创建一项基本关键字策略。

请参见第 330 页的“[配置策略](#)”。

- 5 生成电子邮件事件。

若要触发此示例的查找，事件应该是 SMTP 事件，而发件人的电子邮件地址为 emp@company.com。更改 CSV 中的发件人的值，使其匹配电子邮件发件人的实际值。

- 6 在“系统”>“查找插件”>“新建插件”创建新的 CSV 查找插件。

- 7 配置查找插件的方法如下:

- 名称: *CSV Lookp Plug-in*
- 说明: *Look up manager of email sender from CSV file.*
- CSV 文件路径: *C:\SymantecDLP\Protect\plugins\lookup\csv_lookup_file.csv*
- 分隔符: *Pipe []*
- 文件编码: *UTF-8*
- 属性映射

对单独的行映射系统定义的属性、自定义属性和查找参数键如下:

```
attr.sender-email=SENDER
attr.Manager=MGR
attr.Department=DEPT
attr.Email\ Address=EMAIL
keys=SENDER
```

attr.sender-email = SENDER 来自“发件人”组的查找参数键。它映射到 CSV 文件中相应的列标题。

attr.Manager = MGR 步骤 1 中定义的自定义属性。它映射到 CSV 文件中相应的列标题。

attr.Department = DEPT 步骤 1 中定义的自定义属性。它映射到 CSV 文件中相应的列标题。

attr.Email\ Address = EMAIL 步骤 1 中定义的空格分隔自定义属性。它映射到 CSV 文件中相应的列标题。

keys = SENDER 该行声明要执行查找的一个键。一旦找到第一个键，查找即停止，并且会填入属性值。

- 8 保存插件配置。

9 选择“系统”>“查找插件”>“查找参数”，并选择下列查找参数键组：

发送者 此组包含 `sender-email` 键。

10 选择“系统”>“查找插件”>“修改插件链”，然后启用插件。

11 打开在步骤 4 中生成的事件的“事件快照”。

12 验证您在步骤 1 中创建的未填入自定义属性，是否出现在屏幕右侧的“属性”窗格中。

如果没有这样做，请完成步骤 1。

13 验证“查找”按钮是否出现在自定义属性上方的“属性”窗格中。

如果没有，请验证“查找属性”权限是否授予用户。

在进行任何更改之后，单击“重新加载插件”。

14 单击“查找”按钮。

自定义属性应该填入从 CSV 文件中查找并且提取的值。

15 根据需要，对插件进行故障排除。

请参见第 859 页的[“测试 CSV 查找插件并进行故障排除”](#)。

配置 LDAP 查找插件

要配置一个或多个 LDAP 查找插件，请完成以下任务。

表 50-20 配置 LDAP 查找插件

步骤	操作	说明
1	创建自定义属性。	请参见第 835 页的 “配置自定义属性” 。
2	配置到 LDAP 服务器的连接。	必须建立到 LDAP 服务器的正常连接。 请参见第 863 页的 “LDAP 服务器连接的要求” 。 可从 LDAP 查找插件中的链接配置与 LDAP 服务器的连接。 请参见第 116 页的 “配置目录服务器连接” 。
3	创建新的 LDAP 查找插件。	请参见第 845 页的 “创建新的查找插件” 。

步骤	操作	说明
4	映射属性。	<p>将属性映射到相应的 LDAP 目录字段。语法如下：</p> <pre>attr.CustomAttributeName = search_base: (search_filter=\$variable\$): ldapAttribute</pre> <p>请参见第 863 页的“将属性映射到 LDAP 数据”。</p> <p>请参见第 864 页的“LDAP 的属性映射示例”。</p>
5	保存并启用插件。	<p>必须在 Enforce Server 上启用 LDAP 查找插件。</p> <p>请参见第 850 页的“启用查找插件”。</p>
6	测试并对 LDAP 查找插件进行故障排除。	请参见第 851 页的“ 排除查找插件故障 ”。

LDAP 服务器连接的要求

为了使 Symantec Data Loss Prevention 与 LDAP 目录之间建立连接，必须满足下列条件：

- LDAP 目录必须在 Enforce Server 可以访问的主机上运行。
- 必须存在一个可供 Symantec Data Loss Prevention 使用的 LDAP 帐户。此帐户必须具有只读访问权限。您必须知道此帐户的用户名和密码。
- 您必须知道 LDAP 服务器的完全限定域名称 (FQDN) (无法使用 IP 地址) 。
- 您必须知道 Enforce Server 用来与 LDAP 服务器进行通信的 LDAP 服务器上的端口。默认值为 389。

您可以使用 LDAP 查找工具（如 Softerra LDAP 浏览器）确认您是否有正确的凭据来连接 LDAP 服务器。还要确认是否已定义正确的字段来填充自定义属性。

请参见第 839 页的“[关于 LDAP 查找插件](#)”。

将属性映射到 LDAP 数据

您需要将系统和自定义属性映射到“属性映射”字段中的 LDAP 数据。输入时，每个映射占单独的一行。这些映射条目的显示顺序无关紧要。

LDAP 查找插件的属性映射语法如下所示：

```
attr.CustomAttributeName = search_base:  
  (search_filter=$variable$):  
    ldapAttribute
```

下表更加详细地介绍了此语法。

表 50-21 LDAP 映射语法详细信息

元素	说明
<i>CustomAttributeName</i>	自定义属性的名称，如 Enforce Server 中所定义。 注意： 如果属性名称包含空格字符，则必须在每个空格字符前加上反斜杠。空格字符指的是空格或 Tab。例如，您需要将 Business Unit 自定义属性输入为 attr.Business\ Unit 请参见第 835 页的“ 配置自定义属性 ”。
<i>search_base</i>	标识 LDAP 目录。
<i>search_filter</i>	LDAP 属性（字段）的名称，该名称与从 Enforce Server 传递给插件的查找参数（或其他变量）相对应。
<i>variable</i>	查找参数的名称，该查找参数包含一个值，将使用该值作为关键字来在 LDAP 目录中查找正确数据。 如果多个插件链接在一起，该参数可能是由上一个插件传递给 LDAP 查找插件的变量。
<i>ldapAttribute</i>	数据值将返回给 Enforce Server 的 LDAP 属性。此值用于填充在条目的第一个元素中指定的自定义属性。

请参见第 839 页的“[关于 LDAP 查找插件](#)”。

LDAP 的属性映射示例

下列映射提供了 LDAP 查找插件的其他属性映射示例。

下列属性映射示例会搜索 hr.corp LDAP 目录，以查找具有 mail 属性，且值与 sender-email 查找参数值匹配的记录。它还会将该记录的 givenName 属性值返回给 Enforce Server。

```
attr.First\ Name = dc=corp,dc=hr:(mail=$sender-email$):givenName
```

在以下属性映射示例中，会以不同的行输入每个要填入的自定义属性。另外，请注意使用 TempDeptCode 临时变量。要从 LDAP 层次结构获得部门名称，需要部门代码。但是，只有部门名称需要存储为自定义属性。TempDeptCode 变量就是为此而创建的。

```
attr.First\ Name = cn=users:(email=$sender-email$):firstName
attr.Last\ Name = cn=users:(email=$sender-email$):lastName
attr.TempDeptCode = cn=users:(email=$sender-email$):deptCode
attr.Department = cn=departments:(deptCode=$TempDeptCode$):name
attr.Manager = cn=users:(email=$sender-email$):manager
```

测试和故障排除 LDAP 查找插件

完成这些步骤以解答 LDAP 查找插件实施的疑难。

请参见第 839 页的“[关于 LDAP 查找插件](#)”。

故障排除 LDAP 查找插件

- 1 如果插件没有正确保存，请验证配置。

在使用 LDAP 查找插件之前，您应该测试到 LDAP 服务器的连接。您可以使用查找工具（例如 Softerra LDAP Browser）来帮助确认是否已定义了正确的字段。

请参见第 116 页的“[配置目录服务器连接](#)”。

- 2 请确保已启用插件。

- 3 请确保您已创建“自定义属性”定义。

特别是，请检查属性映射。属性名称必须相同。

- 4 如果您已进行更改，或者已编辑查找参数键，请重新加载插件。

请参见第 851 页的“[重新加载查找插件](#)”。

- 5 针对您要用来检测事件的检测服务器，选择“事件”>“所有事件”。

- 6 选择（勾选）多个事件，然后从“事件操作”下拉菜单选择“查找属性”。
(此操作会针对该形式的检测，查找所有事件的属性值。)

- 7 检查事件的“事件快照”屏幕。验证“查找”自定义属性填满从 LDAP 查询检索的项。

- 8 如果没有填入正确的值，或者在您已经定义的自定义属性中没有值，请确保在事件的“历史记录”选项卡中没有记录任何连接错误。

- 9 检查 Tomcat 日志文件。

请参见第 851 页的“[排除查找插件故障](#)”。

LDAP 查找插件教程

本教程提供实施简易 LDAP 查找插件的步骤。

实施 LDAP 查找插件

- 1 在“系统”>“属性”>“自定义属性”创建下列自定义属性：

LDAP givenName

LDAP telephoneNumber

- 2 在“系统”>“组目录”中，创建 Active Directory 服务器的目录连接。

例如：

- 主机名称：**enforce.dlp.company.com**
- 端口：**389**
- 基准 DN：**dc=enforce,dc=dlp,dc=com**
- 加密：无
- 验证：已验证
- 用户名：**userName**
- 密码：**password**

- 3 测试连接。系统会指出连接是否成功。

- 4 在“系统”>“查找插件”>“新建插件”>**LDAP** 中，创建新的 LDAP 插件。

名称：**LDAP 查找插件**

说明：**LDAP 插件说明。**

- 5 选择在步骤 2 中创建的目录连接。

- 6 将属性映射到 LDAP 元数据。

```
attr.LDAP\ givenName = cn=users:(|(givenName=$endpoint-username$)(mail=$sender-email$)(streetAddress=$discoverserver$)):givenName
attr.LDAP\ telephoneNumber = cn=users:(|(givenName=$endpointuser-name$)(mail=$sender-email$)(streetAddress=$discoverserver$)):telephoneNumber
```

- 7 保存插件。验证是否显示了插件的正确保存消息。

- 8 在“系统”>“查找插件”>“查找参数”页面中，启用下列关键字。

■ 事件

■ 消息

■ 发送者

- 9 创建生成其中一个查找参数的事件。例如，电子邮件事件将会公开发件人电子邮件属性。在 Active Directory 服务器中必须有一些相应的信息。
- 10 打开事件的“事件快照”。
- 11 单击“查找”按钮，然后验证在步骤 1 中创建的自定义属性是否已填入正确的面板中。

配置脚本查找插件

完成这些步骤以实施一或多个脚本查找插件，以查找外部信息。

请参见第 868 页的[“编写脚本查找插件”](#)。

表 50-22 配置脚本查找插件

步骤	操作	说明
1	创建自定义属性。	请参见第 835 页的“配置自定义属性”。
2	创建脚本。	请参见第 868 页的“编写脚本查找插件”。
3	定义查找参数键。	选择用于提取自定义属性数据的键。 请参见第 846 页的“选择查找参数”。
4	创建新的脚本插件。	请参见第 845 页的“创建新的查找插件”。
5	输入脚本命令。	此值是脚本引擎可执行文件在 Enforce Server 主机上的本地路径。 请参见第 869 页的“指定脚本命令”。
6	指定参数。	该值将用于属性查找及任何命令行参数的 Python 脚本的路径。以 -u 参数作为脚本路径的开头，可改善查找性能。 请参见第 869 页的“指定参数”。
7	启用 stdin 和 stdout 选项。	同时启用两个选项有助于防止脚本注入攻击。 请参见第 870 页的“启用 stdin 和 stdout 选项”。
8	或者，也可以启用协议过滤。	您可以指定传递属性值的事件类型（按协议）以查找脚本。 请参见第 870 页的“对脚本启用事件协议过滤”。
9	或者，也可以启用并加密证书。	您可以将脚本连接到外部系统所需的凭据加密并传递出去。 请参见第 871 页的“启用和加密脚本凭据”。
9	保存插件。	验证是否显示了插件的正确保存消息。 请参见第 845 页的“创建新的查找插件”。

步骤	操作	说明
10	启用查找插件。	您可以将各脚本链接在一起，也可以将脚本与其他查找插件链接在一起。
11	测试查找插件。	测试查找插件。 请参见第 851 页的“ 排除查找插件故障 ”。

编写脚本查找插件

如果您要使用脚本查找插件，则必须编写提取数据并填入每个事件的自定义属性的脚本。脚本查找插件会将属性传递到脚本作为关键字/值对。反之，脚本必须使用标准输出 (stdout) 来输出一组关键字/值对。插件会使用这些关键字/值对来填入自定义属性。

在编写用于脚本查找插件的脚本时，请遵循下列语法要求和调用约定，包括脚本插件如何将参数传递至脚本，以及所请求的脚本输出格式。

表 50-23 脚本插件调用约定

惯例	语法	说明
输入	attribute_name=attribute_value	脚本查找插件会以 key=value 格式，将属性传递至脚本作为命令行参数。
输出	stdout	要与插件和填充属性结合使用，脚本必须将一组关键字/值对输出到标准输出 (stdout)。 必须使用换行符分隔输出的关键字/值对。例如： host-name=mycomputer.company.corp username=DOMAIN\bsmith
退出代码	0	脚本必须以退出代码 0 退出。如果脚本以其他代码退出，Enforce Server 会认为在执行脚本过程中发生了错误并终止属性查找。
错误处理	stderr 至文件	脚本不会打印出错误或调试信息。重定向 stderr 至文件。在 Python 中，这将会是： fsock = open("C:\error.log", "a") sys.stderr = fsock

请参见第 874 页的“[脚本示例](#)”。

指定脚本命令

“脚本命令”字段指定执行之脚本引擎的路径。这些是 Python 指定的说明。

指定脚本命令

- 1 下载并安装 Python 2.6 版到 Enforce Server 主机（如果尚未执行此操作）。
- 2 输入 python.exe 可执行文件的本地路径。

例如：

- Windows: c:\python26\python.exe
- Linux: /usr/local/bin/python

- 3 输入参数。

请参见第 869 页的“[指定参数](#)”。

指定参数

“参数”字段指定脚本的路径以及任何其他的命令行参数。这些是 Python 指定的说明。

指定参数

- 1 在编写脚本后，请将它复制到 Enforce Server 主机，或复制到 Enforce Server 可访问的文件共享。
- 2 确保对目录和脚本文件正确设置了权限。
`protect` 用户必须可读取和可执行目录和文件。
- 3 在“参数”字段中输入 `-u` 参数。
此命令会强制 `stdin`、`stdout` 和 `stderr` 完全取消缓冲，以改进查找的性能。
- 4 输入脚本文件的完全限定路径。

例如：

- Windows: -u,c:\python26\scripts\ip-lookup.py
- Linux: -u,/opt/python26/scripts/ip-lookup.py

注意：系统不会验证文件位置。

- 5 保存插件配置。

启用 stdin 和 stdout 选项

当您配置脚本查找插件时，可以选择“启用 **stdin**”和“启用 **stdout**”。如果启用这些选项，系统会检查脚本输入和输出中是否存在不安全的字符，例如可能由 UNIX 或 Windows Shell 造成安全漏洞的命令分隔符和逻辑运算符。

由于您在安装 Enforcer Server 的主机上运行脚本，您应该启用这两个选项，除非您确定脚本是安全的。如果启用，日志将指出无效的和未经转义的字符。

请参见第 870 页的[表 50-24](#)。

表 50-24 属性名称的无效字符

无效的字符	说明
空字符串	不允许空字符串。
@	如果启用 stdin 和 stdout 选项，在处理期间，包含这些字符的属性将被忽略。
-	
+	
=	
:	
/	
\	
)	
(
-	
+	
-	
\$	如果 \$ 和 % 字符正确使用反斜线转义，则允许使用包含这些字符的属性。
%	

对脚本启用事件协议过滤

您可以选择指定将属性值传递到查找脚本的事件类型（按协议）。如果不启用协议过滤，您的脚本查找插件将应用于所有事件。

例如，您可以限制将属性值传送给通过 HTTP 检测到的那些事件。当您按协议过滤时，Enforce Server 仍会捕获通过其他协议检测到的事件。但它不会通过脚本查找插件使用属性值来填充这些事件。

启用协议过滤

- 1 导航至 Enforce Server 管理控制台中的“系统”>“查找插件”>“编辑脚本查找插件”屏幕。
请参见第 867 页的[“配置脚本查找插件”](#)。
- 2 在“脚本查找插件”屏幕中，选择（勾选）“启用协议过滤”选项。
此操作将显示可供过滤的所有协议。请注意，这些协议是检测服务器特定的。

注意：网络协议和移动协议在“系统”>“设置”>“协议”屏幕进行配置。端点协议在“系统”>“代理”>“代理配置”屏幕进行配置。发现协议在“策略”>“发现扫描”>“发现目标”进行配置。此外，事件生成后，该事件的协议值就会显示在“事件快照”屏幕的顶部。

- 3 指定要在查找中包含的协议。
如果启用协议过滤，您必须至少选择一个协议过滤依据。
- 4 保存插件配置。

启用和加密脚本凭据

如果您的脚本连接到需要凭据的外部系统，您可以启用脚本中的凭据。如果是通过用户界面选项启用凭据，则必须将它们加密。Symantec Data Loss Prevention 提供凭据实用程序，可让您加密凭据并使用它们来对外部数据源进行身份验证。

当 Enforce Server 调用脚本查找插件时，该插件会在运行时解密所有凭据并将其作为属性传递给脚本。然后就可以在脚本中使用这些凭据了。凭据实用程序使用的平台加密密钥与保护 Symantec Data Loss Prevention 系统中的用户帐户和事件信息所用的平台加密密钥相同。

请参见第 871 页的[表 50-25](#)。

如果选择以明文形式使用凭据，必须将它们硬编码到您的脚本中。在这种情况下，Enforce Server 会将导出的值传递给明文的凭据文件。这些值按以下格式传递：
key=value。

表 50-25 启用和加密凭据

步骤	操作	说明
1	创建包含脚本访问相应外部系统所需的凭据的文本文件。	此文件的格式为 <i>key=value</i> ，其中 <i>key</i> 是凭据的名称。 例如： <code>username=msantos password=esperanza9</code>

步骤	操作	说明
2	将此凭据文件保存到 Enforce Server 的本地文件系统。	该文件必须暂时保存到 Enforce Server 中。 例如: C:\temp\MyCredentials.txt。
3	在 Enforce Server 上, 打开一个 Shell 或命令提示符, 并将目录更改为 <\SymantecDLP_home>\Protect\bin。	Enforce Server 上的这个目录包含凭据生成器实用程序。
4	发出命令以生成加密的凭据文件。	命令语法如下: <pre>CredentialGenerator.bat in-cleartext-filepathout-encrypted-filepath</pre> 例如, 在 Windows 上您可以发出下列命令: <pre>CredentialGenerator.bat C:\temp\MyCredentials.txt C:\temp\MyCredentialsEncrypted.txt</pre> 您可以在文本编辑器中打开这个文件, 以验证它是否已经加密。
5	选择“启用凭据”。	在“系统”>“查找插件”>“编辑脚本查找插件”页面上, 选择(选中)“启用凭据”选项。
6	输入“凭据文件路径”。	输入加密凭据文件的完全限定路径。例如: C:\temp\MyCredentialsEncrypted.txt。
7	保存插件。	您现在可以使用加密的凭据对外部系统进行验证。
8	安全的明文凭据文件。	如果要保存明文凭据文件, 请将其移到安全位置。如果打算稍后对其进行更新和重新加密, 保存该文件会非常有用。如果不保存该文件, 请立刻将其删除。
9	重新加载查找插件。	请参见第 843 页的 “管理和配置查找插件” 。

链接多个脚本查找插件

所有查找插件都会收到对同一属性映射的引用。此引用可让您链接查找插件。插件链是否需要填充自定义属性会根据情况而变化。请考虑以下示例情景。

获取网络电子邮件事件的正确关键字通常很容易。邮件发送者的电子邮件地址会作为 `sender-email` 查找参数被自动捕获。该查找参数可以用作解锁有关外部源中存储的发送者信息的关键字。在这种情况下, 不需要链接多个插件。

对于 Web 或 FTP 事件, 可能需要插件链。针对这些种类的事件捕获的查找参数是原始主机的IP地址。但是IP地址通常不是类似电子邮件地址的静态标识符。因此, 您可能需要连续查找以获得可用作信息关键字的静态标识符。

您可以编写脚本，将 `sender-ip` 查找参数传递至 DNS 服务器以取得主机名称。然后，您可以编写另一个脚本以将该主机名称传递到资产管理系统。从资产管理系统，您可以获得使用该计算机的人员的用户名或电子邮件。然后，该用户名或电子邮件可用作解锁其余数据的“关键字”。此插件链将有三个链接：

1. 使用 IP 地址返回主机名称的脚本查找插件。
2. 使用主机名称返回用户名或电子邮件的脚本查找插件。
3. 使用用户名或电子邮件返回其余自定义属性数据的 CSV 查找插件。

在此示例中，您必须创建新的 `Host_Name` 临时变量以存储主机名称信息。此临时变量及其值然后就可用于第二个脚本和后续插件。

脚本查找插件教程

完成下列教程可实施脚本查找插件。本教程假设对实施查找插件具有基本的实务熟悉程度。要达到此熟悉程度，请完成“CSV 查找插件教程”。

请参见第 860 页的“[CSV 查找插件教程](#)”。

要实施脚本查找插件

- 1 下载 Python 2.6 并将其安装到已安装 Enforce Server 的系统中。
例如：C:\python26。
- 2 将本章提供的“脚本示例”复制到一个文本文件中，并将文件保存到 Enforce Server 主机上的一个目录中，保存名称为 `Script-Plugin.py`。
例如：C:\python26\scripts\Script-Plugin.py。
请参见第 874 页的“[脚本示例](#)”。
- 3 在 Python IDE 中（如 Wing IDE）打开此脚本（位于 <http://www.wingware.com/>）。
- 4 查看此脚本中的注释并运行它。
 - 对第 18 行添加注释。
 - 运行脚本。这样会返回“`Script-attribute=script value`”。
 - 取消对第 18 行的注释，这样便不会处理该行。
- 5 创建以下自定义属性：`Script-attribute`。
- 6 选择“新建插件”>“脚本”来创建新的脚本查找插件。
请参见第 845 页的“[创建新的查找插件](#)”。
- 7 配置脚本查找插件。
请使用以下参数：

- 脚本命令: C:\python26\python.exe
- 参数: -u,C:\python26\scripts\Script-Plugin.py

- 8 保存插件，并确保插件如系统消息所示成功加载。
- 9 启用下列查找参数：“事件”、“消息”和“发送者”。
- 10 生成会传递 date-sent 属性的事件。
- 11 转至新事件的“事件快照”，然后单击“查找”。
- 12 验证 script-attribute 自定义属性填入 script value 的值。
- 13 如果自定义属性没有填入，请检查日志文件
C:\SymantecDLP\Protect\logs\tomcat\localhost.<latest_date>.log。
如果 script-attribute=null，请检查脚本。查看提供的脚本中的注释，并确保 attribute=value 对之间没有空格。
请参见第 851 页的“[排除查找插件故障](#)”。
- 14 浏览启用脚本查看插件的选项属性，包括 stdin/stdout、协议过滤和凭据。
请参见第 870 页的“[启用 stdin 和 stdout 选项](#)”。
请参见第 870 页的“[对脚本启用事件协议过滤](#)”。
请参见第 872 页的“[链接多个脚本查找插件](#)”。

脚本示例

以下提供的脚本作为脚本查找插件的示例。这是使用 Python 2.6 编写的。此脚本的目的是提供使用 Python 编写脚本的基本工作示例，该脚本可以用于脚本查找插件。

此脚本包含 date-sent 查找参数键，并且会返回 script-attribute 自定义属性的“脚本值”。

请参见第 873 页的“[脚本查找插件教程](#)”。

注意：由于 Python 对缩进要求十分严格，如果您复制/粘贴此脚本示例，则可能需要重新格式化，以使外观与此处显示完全相同。

```
__name__ = "__main__"

import sys, os, traceback
import commands

# Switch this to 0 when in production mode.
debugMode = 1

def main(args):

    try:

        attributeMap = parseInput(args)

        # This is the lookup parameter key.
        # Comment-out this line for testing the script standalone.
        dateSent = attributeMap["date-sent"]

        # "Script-attribute" is the custom attribute.
        # "script value" is the return value.
        # You cannot have a space between the custom attribute and the
        # attribute value. For example, "Script-attribute = script value"
        # Does not work for Script Lookup Plugins.
        print "Script-attribute=script value"
        return

    except:
        error()
        print "something went wrong!"
        return "something went wrong!"

def parseInput(args):

    # Input data is a list of key value pairs seperated by carraige return
    # Create a python dictionary to create the attribute map
    attributeMap = {}
    delimiter = "="
    for item in args:
        if delimiter in item:
            tuple = item.split(delimiter)
            attributeMap[tuple[0]] = tuple[1]
    return attributeMap

def error():
    # "SCRIPT PROCESSING ERROR"
    if(debugMode):
```

```
#print "Script Processing Error"
traceback.print_exc(file=sys.stdout)
return ""

#-----
# DOS-style shells (for DOS, NT, OS/2):
#-----
def getstatusoutput(cmd):
    """ Return (status, output) of executing cmd in a
    shell."""

    pipe = os.popen(cmd + ' 2>&1', 'r')
    text = pipe.read()
    sts = pipe.close()
    if sts is None: sts = 0
    if text[-1:] == '\n': text = text[:-1]
    return sts, text

#-----
# Entry Point
#-----

if __name__ == "__main__":
    if(len(sys.argv) == 0):
        error()
    else:
        main(sys.argv)
```

配置迁移的自定义（旧版）查找插件

这些步骤假定您已经将现有的自定义 Java 查找插件部署至 11.6 版之前的 Symantec Data Loss Prevention，而且您已经将系统升级至 Symantec Data Loss Prevention 11.6 版。在此情况下，自定义 Java 查找插件将迁移至自定义（旧版）查找插件，而且将会出现在验证和测试的用户界面中。

请参见第 840 页的“[关于自定义（旧版）查找插件](#)”。

注意：有关实施自定义 Java 查找插件的相关信息，请参阅《Symantec Data Loss Prevention 查找插件指南》。

表 50-26 实施自定义 (旧版) 查找插件

步骤	操作	说明
1	创建自定义属性。	创建您的自定义 (旧版) 查找插件将会检索其值的自定义属性。 请参见第 834 页的“ 关于使用自定义属性 ”。
2	编辑自定义 (旧版) 插件。	成功升级应该将自定义 (旧版) 查找插件导入用户界面，您可以在此处启用该插件。 如有需要，您可以更新名称和说明。 请参见第 845 页的“ 创建新的查找插件 ”。
3	验证“插件类别”。	升级后，应该从 <code>Plugins.properties</code> 文件填入类别名称。
4	验证“所需的 JAR”。	升级后，先前复制到 Enforce Server 的 JAR 文件应会出现在此字段中。
5	启用插件。	“打开”插件。 请参见第 850 页的“ 启用查找插件 ”。
6	启用参数查找关键字。	选择关键字来触发属性查找。 请参见第 846 页的“ 选择查找参数 ”。
7	创建策略，并生成插件预期类型的事件。	例如，创建一个关键字策略，并生成传递 <code>sender-name</code> 属性的 SMTP 网络事件。
8	确认已更新自定义属性。	检查“事件快照”中填入的属性。 请参见第 851 页的“ 排除查找插件故障 ”。

7

部分

监视和防止网络中的数据丢失

- 51. 实施 Network Monitor
- 52. 实施 Network Prevent for Email
- 53. 实施 Network Prevent for Web

实施 Network Monitor

本章节包括下列主题：

- 实施 Network Monitor
- 选择网络数据包捕获方法
- 关于数据包捕获软件的安装和配置
- 配置 Network Monitor Server
- 对 Network Monitor 启用 GET 处理
- 为 Network Monitor 创建策略
- 测试 Network Monitor

实施 Network Monitor

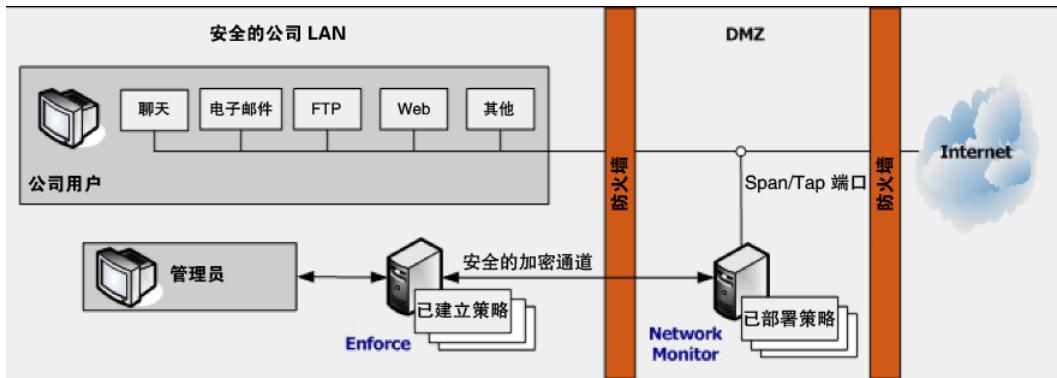
Network Monitor 可捕获和分析网络上的流量，检测所指定协议之上的机密数据和重要的流量元数据。例如，SMTP、FTP、HTTP 和各种 IM 协议。您可以对 Network Monitor Server 进行配置以监视自定义协议并使用各种过滤器（按协议）滤除低风险流量。

要监视网络流量，Network Monitor Server 要求具有：

- 网络交换端口分析器 (SPAN) 或网络 TAP，用来获取目标网络上的流量。
- Network Monitor Server 主机上的卡，用来捕获从 SPAN 或 TAP 获取的网络流量。可以使用网络接口卡 (NIC) 或高速数据包捕获适配器 (Endace 或 Napatech)（请注意，除此流量捕获卡之外，还需要一张单独的 NIC，负责 Network Monitor Server 和 the Enforce Server 之间的通信。为了达到此目的，必须有 WinPcap。）

- 数据包捕获软件。使用 NIC 进行数据包捕获时，必须在 Network Monitor Server 主机上安装数据包捕获软件。当您使用高速数据包捕获适配器（Endace 或 Napatech）时，该适配器必须使用正确的驱动程序。
请参见第 883 页的“[选择网络数据包捕获方法](#)”。

图 51-1 基本 Network Monitor 设置



要实施数据包捕获并设置 Network Monitor，请执行以下高级任务：

- 1 安装并设置捕获网络流量的网络 TAP 或 SPAN。
- 2 选择捕获网络流量的方法。

请参见第 883 页的“[选择网络数据包捕获方法](#)”。

- 3 按照卡文档说明，在 Network Monitor 上安装所需的 NIC 卡或高速数据包捕获适配器（Endace 或 Napatech）。还可以参考适当的《Symantec Data Loss Prevention 安装指南》（Windows 或 Linux）。该 NIC 或高速数据包捕获适配器（Endace 或 Napatech）必须运行于混合模式下，以便可以收集所有入站和所有出站流量。

如需所支持的高速数据包捕获适配器和驱动程序的相关信息，请参阅《Symantec Data Loss Prevention 系统要求和兼容性指南》。

- 4 在 Windows 平台上，安装 WinPcap（如果尚未安装）。

请参见第 884 页的“[在 Windows 平台上安装 WinPcap](#)”。

- 5 若有必要，请更新高速数据包捕获适配器的驱动程序。

请参见第 885 页的“[更新 Endace 卡驱动程序](#)”。

请参见第 885 页的“[安装和更新 Napatech 网络适配器和驱动程序软件](#)”。

- 6 禁用用于监视网络流量的 NIC 的校验和卸载。对于 Linux 平台，请使用以下命令在 eth0 界面上禁用接收数据和已传输数据的校验和卸载。

```
ethtool -K eth0 tx off  
ethtool -K eth0 rx off
```

要查看校验和卸载的当前状态，请使用 ethtool -k eth0 命令。

注意：某些校验和算法通过修改网络数据包和添加空校验和来运行。空校验和可能会导致网络捕获驱动程序丢弃数据包，在此情况下，Network Monitor 不会评估这些数据包。

- 7 使用 Wireshark 之类的协议分析器验证 TAP 或 SPAN 上流入到 NIC 卡或高速数据包捕获适配器（Endace 或 Napatech）的流量。
- 8 配置 Network Monitor Server。
请参见第 886 页的“[配置 Network Monitor Server](#)”。
- 9 创建和部署 Network Monitor 测试策略。
请参见第 888 页的“[为 Network Monitor 创建策略](#)”。
- 10 针对测试策略生成事件，以测试系统。
请参见第 889 页的“[测试 Network Monitor](#)”。

选择网络数据包捕获方法

可以使用以下三种不同的方法来捕获 SPAN 或 TAP 获取的网络流量：

- Windows 平台上的 NIC。使用 NIC 进行数据包捕获的 Windows 平台要求 Network Monitor Server 主机上具有 WinPcap 库。如果 Network Monitor Server 主机上未安装 WinPcap，则必须安装该软件。有关 WinPcap 库的支持版本的信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。
请参见第 884 页的“[在 Windows 平台上安装 WinPcap](#)”。
- Linux 平台上的 NIC。使用 NIC 的 Linux 平台使用 Linux 自带的数据包捕获，该捕获方式要求内核支持 PACKET_MMAP。默认情况下，受支持的 Linux 内核中包含对 PACKET_MMAP 的支持。
- Windows 或 Linux 平台上的高速数据包提取适配器。您可以在 Windows 32 位和 Linux 32 及 64 位平台上使用 Endace DAG 网络测量卡，以便在高流量环境中提供网络数据包捕获。或者，也可以使用 Napatech 网络适配器卡来提供网络数据包捕获。如需所支持的高速数据包捕获适配器和驱动程序的相关信息，请参阅《Symantec Data Loss Prevention 系统要求和兼容性指南》。

表 51-1 数据包捕获选择

数据包捕获类型	平台	软件
NIC	Windows	WinPcap
	Linux	自带
高速数据包捕获适配器	Windows 32 位	Endace
	Windows 64 位	Napatech
	Linux (32 位)	Endace
	Linux (64 位)	Endace Napatech

关于数据包捕获软件的安装和配置

当安装和配置数据包捕获软件时，应考虑下列要求：

- 在 Windows 平台上，如果尚未安装 WinPcap 软件，则需要安装该软件才能运行数据包捕获。
- 在 Linux 平台上，PACKET_MMAP 可执行数据包捕获。PACKET_MMAP 是标准的 Linux 组件，不需要进行安装或修改。但是，您还需要 apr-util、apr、expat 和其他第三方软件包才能在 Linux 上运行 Network Monitor Server。有关更多信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。
- 如果您使用高速数据包捕获适配器（Endace 或 Napatech），您将需要安装或更新适配器驱动程序软件。

请参见第 884 页的“[在 Windows 平台上安装 WinPcap](#)”。

请参见第 885 页的“[更新 Endace 卡驱动程序](#)”。

请参见第 885 页的“[安装和更新 Napatech 网络适配器和驱动程序软件](#)”。

在 Windows 平台上安装 WinPcap

如果 Windows 平台上尚未安装 WinPcap 软件，您必须安装该软件。有关 WinPcap 库的支持版本的信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。可以在《Symantec Data Loss Prevention 安装指南》中找到其他详细信息。

请参见第 173 页的“[关于管理 Symantec Data Loss Prevention 服务器](#)”。

在 Network Monitor 检测服务器上安装 WinPcap：

- 1 将 WinPcap 文件复制到本地驱动器。
- 2 执行 WinPcap 可执行文件，并遵循安装命令进行操作。
- 3 通过运行 `pcapstart.reg` 来重置 Windows 注册表设置，并遵循显示的命令进行操作。

更新 Endace 卡驱动程序

如果要将 Network Monitor Server 升级到当前版本，可能需要更新 Endace 卡驱动程序。有关支持的 Endace 卡和驱动程序的信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。

更新 Endace 驱动程序

- 1 按照 Endace 文档所述，安装新的驱动程序。
- 2 重新配置 Network Monitor 以使用新的驱动程序。
请参见第 886 页的“[配置 Network Monitor Server](#)”。

安装和更新 Napatech 网络适配器和驱动程序软件

本主题提供有关安装 Napatech 高速数据包捕获适配器的说明。有关支持的 Napatech 卡和驱动程序版本的信息，请参考《Symantec Data Loss Prevention 系统要求和兼容性指南》。

表 51-2 安装和更新 Napatech 网络适配器

步骤	操作	说明
1	安装支持的 Napatech 高速数据包捕获适配器。	有关安装和配置说明，请访问 Napatech 网站 (http://www.napatech.com/products/capture_adapters/4x1g_std_nt4e-std.html)。有关支持的 Napatech 卡版本，请参考《Symantec Data Loss Prevention 系统要求和兼容性指南》。
2	安装 Napatech 驱动程序。	有关支持的 Napatech 驱动程序版本，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。

步骤	操作	说明
3	验证 Napatech 安装。	<p>对于 Windows:</p> <ul style="list-style-type: none">■ 确保 Napatech 库文件 CommonLib.dll 位于目录 <code>\<windows_installation_drive>\Windows\System32\</code> 中。 <p>对于 Linux:</p> <ul style="list-style-type: none">■ Napatech 驱动程序必须是在安装 Napatech 软件包过程（请参见上述步骤 2）中从源编译的。■ 在捕获数据包之前，必须使用脚本 <code>/opt/napatech/bin/load_driver.sh</code> 为每个计算机引导程序加载一次 Napatech 驱动程序。请注意，对于 RHEL Linux，应编辑文件 <code>/etc/rc.d/rc.local</code> 以附加 <code>/opt/napatech/bin/load_driver.sh</code>，然后重新启动系统。■ 验证 Napatech 库文件 libntcommoninterface.so 是否位于目录 <code>\<nt_installation_directory>/lib\</code> 中。
4	配置 Network Monitor 检测服务器。	<p>部署 Network Monitor 检测服务器，并配置“高级服务器”设置:</p> <ul style="list-style-type: none">■ 通过将以下标志设置为 true，启用 Napatech pack 数据包捕获：<code>PacketCapture.IS_NAPATECH_ENABLED</code>。■ 通过在以下条目的字段中输入 Napatech 驱动程序工具目录的路径，将值更新为此路径：<code>PacketCapture.NAPATECH_TOOLS_PATH</code>。<ul style="list-style-type: none">■ 例如，在 Windows 上，Napatech 工具二进制文件包含在 Napatech 软件包中：<code>\vtcapackage_windows_\version\tools\vt_tools_windows_\version\zip\tools\binary\Tools\architecture\</code>■ 对于 Linux，Napatech 工具是在 Napatech 软件包安装过程中从源编译的：<code>\<nt_installation_directory>/bin/</code> <p>请参见第 195 页的“高级服务器设置”。</p>

配置 Network Monitor Server

可以通过选择用于流量捕获的网络接口（NIC 或 Endace 卡）来配置 Network Monitor Server。还必须选择要监控的协议。

配置 Network Monitor Server

1 在 Enforce Server 管理控制台中，转至“系统”>“服务器”>“概述”，然后单击 Network Monitor Server。将显示“服务器详细信息”屏幕。

如果您不使用高速数据包捕获适配器 (Endace 或 Napatech) 进行流量捕获，请跳至步骤 6。

2 如果您使用高速数据包捕获适配器 (Endace 或 Napatech)，请单击“服务器设置”。

3 在以下字段中输入适当的值：

PacketCapture.ENDACE_BIN_PATH	键入 Endace \bin 目录的路径。 此目录默认位于 <i>endace_home\daq-version\bin</i> (例如，在 Windows 平台上，位于 c:\Program Files\Endace\daq-3.2.2\bin)。请注意， 在此处所列的任何字段中，均不能 使用变量 (例如 %ENDACE_HOME%)。
PacketCapture.ENDACE_LIB_PATH	键入 Endace \lib 目录的路径。
PacketCapture.ENDACE_XILINX_PATH	键入 Endace \xilinx 目录的路径。
PacketCapture.IS_ENDACE_ENABLED	将值更改为 true。

- 4 停止并重新启动 Network Monitor Server。Symantec Data Loss Prevention 将在 Network Monitor Server 的“配置服务器”屏幕中的“网络接口”字段中显示 Endace 卡。
- 5 转至“系统”>“服务器”>“概述”，然后再次单击 Network Monitor Server。
- 6 在“服务器详细信息”屏幕上，请单击“配置”。您可以如后续步骤所述，在最上方的“常规”部分和“数据包捕获”选项卡中，确认或修改设置。
- 7 保留“源文件夹覆盖”字段为空以接受默认目录，从而在 Network Monitor Server 处理网络流之前先缓冲网络流。（此为建议设置。）要指定自定义缓冲目录，请键入该目录的完整路径。
- 8 保留“存档文件夹”字段为空。
- 9 选择 Network Monitor Server 应通过其捕获流量的一个或多个“网络接口”(NIC 或 Endace 卡)。
- 10 在“协议”部分中，选择要监控的一个或多个协议。例如，选中 SMTP、HTTP 和 FTP 的复选框。要让协议显示在此部分中，必须已经在 Enforce Server 中的全局“协议”屏幕上配置了该协议。

请参见与“配置服务器”屏幕关联的联机帮助。

Symantec Data Loss Prevention 对于列表中的每个协议都有标准设置。要修改协议的设置，请单击相应协议旁的“铅笔”图标。有关修改协议设置的详细信息，请参见联机帮助。

- 11 单击“保存”。
- 12 停止并重新启动 Network Monitor Server。单击“服务器详细信息”屏幕中“状态”条目旁的“循环”。

在选择了网络接口和协议后，您可能希望创建测试策略来测试您的部署。

请参见第 889 页的[“测试 Network Monitor”](#)。

请参见第 888 页的[“对 Network Monitor 启用 GET 处理”](#)。

请参见第 888 页的[“为 Network Monitor 创建策略”](#)。

对 Network Monitor 启用 GET 处理

默认情况下，Network Monitor 不会处理 HTTP GET 命令。GET 处理已被禁用，因为其流量过高，而且敏感数据很少会在 GET 命令中丢失。如果您需要 GET 处理且 Network Monitor Server 可以处理增加的负载，请按照此过程配置 Network Monitor 以处理 GET 命令。

启用 GET 处理

- 1 确保 Network Monitor Server 的 **L7.processGets** 高级服务器设置必须为 **true**（此为默认值）。
- 2 将 Network Monitor Server 上的 **PacketCapture.DISCARD_HTTP_GET** 高级服务器设置从默认设置 **true** 更改为 **false**。
- 3 减小 Network Monitor Server 的 **L7.minSizeofGetURL** 高级设置的大小，从默认值 100 减小为小于最短 URL（您要从其处理 GET 命令）长度的字节数。如果最小 URL 大小为 10，将处理所有情况。但是请注意，减小 GET 的最小大小会增大必须处理的请求数，这会增加服务器流量负载。

请参见第 914 页的[“为 Network Prevent for Web 启用 GET 处理”](#)。

为 Network Monitor 创建策略

对于 Network Monitor，可以创建包含任意标准响应规则的策略。要设置响应规则操作，请转至“管理”>“策略”>“响应规则”，然后单击“添加响应规则”。

请参见第 314 页的[“实施策略”](#)。

创建 Network Monitor 的测试策略

- 1 在 Enforce Server 管理控制台中，创建其中一个操作应用于 Network Monitor 的响应规则。例如，创建包含“所有：设置状态”操作的响应规则。
请参见第 669 页的“[配置响应规则](#)”。
- 2 创建包含在上一步中配置的响应规则的策略。
例如，按如下所示创建称为“测试策略”的策略：
 - 包括按照关键字 `test_vontu_secret_keyword` 进行匹配的“[内容匹配关键字](#)”检测规则。
 - 包括“[所有：设置状态](#)”响应规则。
 - 将它与“[默认](#)”策略组相关联。
请参见第 329 页的“[添加新的策略或策略模板](#)”。
请参见第 330 页的“[配置策略](#)”。

测试 Network Monitor

可以通过发送违反测试策略的电子邮件来对 Network Monitor 进行测试。

测试系统

- 1 访问通过 MTA 路由邮件的电子邮件帐户。
- 2 发送包含机密数据的电子邮件。例如，发送一封包含关键字 `test_vontu_secret_keyword` 的电子邮件。
- 3 在 Enforce Server 管理控制台中，转至“事件”>“网络”并单击“事件 - 新建”。查找生成的事件。例如，搜索包括适当的时间戳和策略名称的事件条目。
- 4 单击相关事件条目来查看完整的事件快照。

请参见第 775 页的“[关于 Symantec Data Loss Prevention 报告](#)”。

请参见第 886 页的“[配置 Network Monitor Server](#)”。

请参见第 888 页的“[为 Network Monitor 创建策略](#)”。

实施 Network Prevent for Email

本章节包括下列主题：

- [实施 Network Prevent for Email](#)
- [关于邮件传输代理 \(MTA\) 集成](#)
- [针对反射或转发模式配置 Network Prevent for Email Server](#)
- [指定一个或多个上游邮件传输代理 \(MTA\)](#)
- [为 Network Prevent for Email 创建策略](#)
- [关于策略违规数据标头](#)
- [启用策略违规数据标头](#)
- [测试 Network Prevent for Email](#)

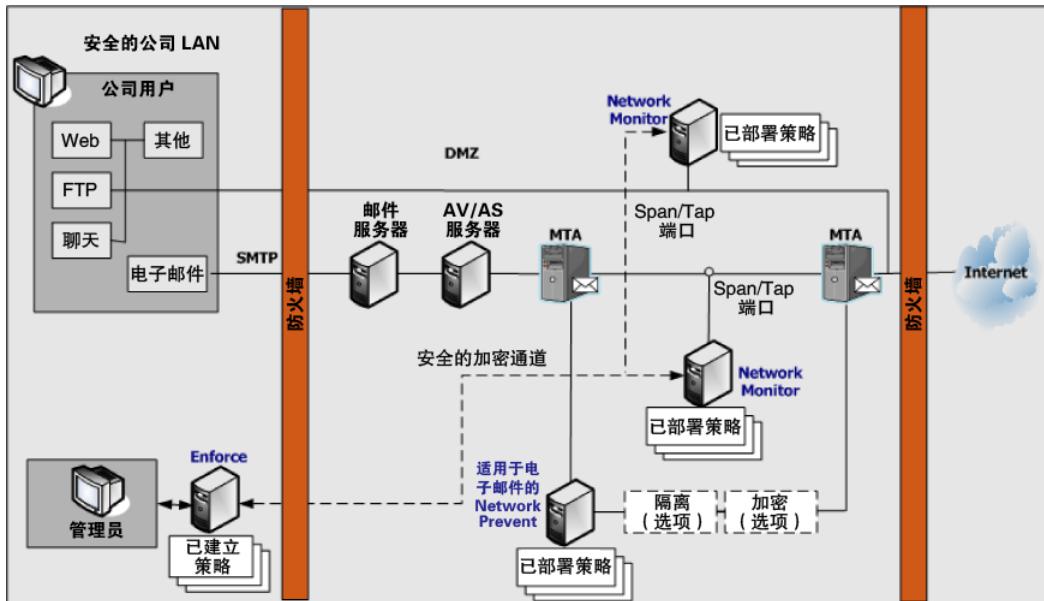
实施 Network Prevent for Email

Network Prevent for Email 可监视和分析内联出站电子邮件流量，并（可选）按照策略中指定的方式阻止、重定向或修改电子邮件。Network Prevent for Email 与行业标准的邮件传输代理(MTA)和托管电子邮件服务相集成，可让您通过 SMTP 监视和阻止数据丢失事件。Network Prevent for Email Server 上部署的策略可指导集成 Prevent 的 MTA 或托管的电子邮件服务器。集成 Prevent 的电子邮件服务器基于特定内容或其他电子邮件属性阻止、重新路由和更改电子邮件。

注意：继续进行实施之前，请查看《Symantec Data Loss Prevention MTA 集成指南（适用于 Network Prevent for Email）》，以确定您首选的集成架构。

图 52-1 显示 Network Prevent for Email Server 与在网络中管理的下一跳 MTA 的集成。作为替代方案，可以将 Network Prevent for Email Server 与位于防火墙外部的托管电子邮件服务器相集成。

图 52-1 基本 Network Prevent for Email 设置



首先，您需要了解实施 Network Prevent for Email 所需的高级步骤。有关更多详细信息，请查看交叉引用章节。

实施 Network Prevent for Email

- 1 选择集成架构，并将邮件传输代理(MTA)配置为与 Network Prevent for Email Server 一起使用。
请参见第 893 页的“[关于邮件传输代理 \(MTA\) 集成](#)”。
- 2 将 Network Prevent for Email Server 配置为在所选集成架构内工作。
请参见第 893 页的“[针对反射或转发模式配置 Network Prevent for Email Server](#)”。
- 3 如果计划加密或隔离电子邮件，请配置必要的第三方加密服务器或存档服务器。有关详细信息，请参见产品文档。

4 创建和部署 Network Prevent for Email 策略。

请参见第 900 页的“[为 Network Prevent for Email 创建策略](#)”。

5 针对测试策略生成事件，以测试系统。

请参见第 902 页的“[测试 Network Prevent for Email](#)”。

关于邮件传输代理 (MTA) 集成

选择集成架构，并将邮件传输代理 (MTA) 配置为与 Network Prevent for Email Server 一起使用。

查看《Symantec Data Loss Prevention MTA 集成指南（适用于 Network Prevent for Email）》。自行熟悉兼容的集成架构。

Network Prevent for Email Server 在反射或转发模式中均可与 MTA 一起运行：

- 反射模式。在反射模式中，Network Prevent for Email Server 会收到来自 MTA 的邮件。它会对这些邮件进行分析，然后将其返回到同一 MTA（并提供阻止邮件或在下游处理它们的指示）。事实上，服务器会将邮件返回至它们所发出的同一 IP 地址。
- 转发模式。在转发模式中，Network Prevent for Email Server 会收到来自上游 MTA 的邮件。分析这些邮件，然后将其发送到下游 MTA 或托管电子邮件服务提供商。您可以在 Network Prevent for Email Server 配置中为下一跳邮件服务器指定一系列 IP 地址或主机名。

您也可以将单个 Network Prevent for Email Server 配置为与多个 MTA 一起使用。

请参见第 899 页的“[指定一个或多个上游邮件传输代理 \(MTA\)](#)”。

针对反射或转发模式配置 Network Prevent for Email Server

使用下列说明将 Network Prevent for Email Server 配置为在反射模式或转发模式下运行。

配置 Network Prevent for Email Server

- 1 登录到您要配置的 Symantec Data Loss Prevention 系统的 Enforce Server 管理控制台。
- 2 选择“系统”>“服务器”>“概述”以显示已配置的服务器列表。
- 3 单击要配置的 Network Prevent for Email Server 名称。
- 4 单击“配置”。

- 5 取消选择“试用模式”以阻止违反了 Symantec Data Loss Prevention 策略的电子邮件。

6 通过修改下列字段来配置反射模式或转发模式：

字段	说明
下一跳配置	选择“反射”以在反射模式下运行Network Prevent for Email Server。选择“转发”以在转发模式下运行。 注意： 如果选择“转发”，则还必须选择“启用 MX 查找”或“禁用 MX 查找”，以配置用于确定下一跳 MTA 的方法。
启用 MX 查找	此选项仅适用于转发模式配置。 选择“启用 MX 查找”来根据域名执行 DNS 查询，以获取服务器的邮件交换(MX)记录。Network Prevent for Email Server 使用返回的 MX 记录来选择下一跳邮件服务器的地址。 如果选择“启用 MX 查找”，则同时在“输入域”文本框中添加一个或多个域名。例如： companyname.com Network Prevent for Email Server 会对您指定的域名执行 MX 记录查询。 注意： “输入域”文本框中必须至少包含一个有效条目，才可成功配置转发模式行为。

字段	说明
禁用 MX 查找	<p>此字段仅适用于转发模式配置。</p> <p>如果您要指定一个或多个下一跳 MTA 的确切主机名或 IP 地址，请选择“禁用 MX 查找”。Network Prevent for Email Server 将使用您指定的主机名或地址，且不会执行 MX 记录查找。</p> <p>如果选择“禁用 MX 查找”，请同时在“输入主机名”文本框中添加一个或多个下一跳 MTA 的主机名或 IP 地址。可以通过将每个条目放在单独的一行来指定多个条目。例如：</p> <pre>smtp1.companyname.com smtp2.companyname.com smtp3.companyname.com</pre> <p>Network Prevent for Email Server 总是尝试代理到您在列表中指定的第一个 MTA。如果该 MTA 不可用，Network Prevent for Email Server 会尝试代理到列表中下一个可用的条目。</p> <p>注意：“输入主机名”文本框中必须至少包含一个有效条目，才可成功配置转发模式行为。</p>

7 单击“保存”。

8 单击“服务器设置”验证或配置下列高级设置：

字段	说明
RequestProcessor.ServerSocketPort	确保此值与上游 MTA 向其发送电子邮件的 SMTP 倾听程序端口号相符。默认值为 10025。 注意： 许多 Linux 系统会限制只有根用户才能访问低于 1024 的端口。Network Prevent for Email 不能绑定到这些受限端口。如果计算机在受限端口（例如，端口 25）上收到要进行检查的邮件，请重新配置计算机以将流量从受限端口路由到非受限 Network Prevent for Email 端口（默认情况下为端口 10025）。 请参见第 898 页的“ 将 Linux IP 表配置为从受限端口重新路由流量 ”。
RequestProcessor.MTAResubmitPort	确保此值与上游 MTA 上 Network Prevent for Email Server 向其返回邮件的 SMTP 倾听程序端口号相符。默认值为 10026。
RequestProcessor.AddDefaultHeader	默认情况下，Network Prevent for Email Server 使用标头来标识所有处理过的电子邮件。标头和值在 RequestProcessor.DefaultPassHeader 字段中指定。 如果您不想向每封邮件添加标头，请将此字段的值更改为 false。
RequestProcessor.AddDefaultPassHeader	此字段将指定 Network Prevent for Email Server 添加到所处理的每封电子邮件的标头和值。默认的标头和值为 X-CFilter-Loop: Reflected。如果要向每封处理过的邮件添加不同的标头，请更改此字段的值。 如果您不想向每封电子邮件添加标头，请将 AddDefaultPassHeader 字段设为 False。

注意：无论是实施反射模式还是转发模式，都要配置 **RequestProcessor.ServerSocketPort** 和 **RequestProcessor.MTAResubmitPort**。如果实施转发模式，**RequestProcessor.ServerSocketPort** 会指定上游 MTA 向其发送电子邮件的

检测服务器上的 SMTP 倾听程序端口。**RequestProcessor.MTAResubmitPort** 是检测服务器将向其发送电子邮件的下游 MTA 上的 SMTP 倾听程序端口。

- 9 单击“保存”。
- 10 单击“完成”。
- 11 如果您的电子邮件交付系统在转发模式下使用 TLS 通信，则代理链中的每个下一跳邮件服务器必须支持 TLS，并且必须向上一跳邮件服务器验证自己的身份。这意味着 Network Prevent for Email Server 必须向上游 MTA 验证自己的身份，而下一跳 MTA 必须向 Network Prevent for Email Server 验证自己的身份。适当的身份验证需要每个邮件服务器都在其本地 Keystore 文件中为下一跳邮件服务器存储公钥证书。

请参见第 899 页的“[指定一个或多个上游邮件传输代理 \(MTA\)](#)”。

请参见第 900 页的“[为 Network Prevent for Email 创建策略](#)”。

请参见第 902 页的“[测试 Network Prevent for Email](#)”。

将 Linux IP 表配置为从受限端口重新路由流量

许多 Linux 系统会限制只有根用户才能访问低于 1024 的端口。Network Prevent for Email 不能绑定到这些受限端口。

如果计算机在受限端口（例如，端口 25）上收到要进行检查的邮件，则使用 `iptables` 命令将该流量路由到非受限端口（例如 Network Prevent for Email 默认端口 10025）。然后确保 Network Prevent for Email 在非受限端口上进行侦听以检查电子邮件。

使用以下说明将 Linux 系统配置为从端口 25 路由到端口 10025。如果使用其他受限端口或 Network Prevent for Email 端口，则请在 `iptables` 命令中输入正确的值。

配置将流量从端口 25 路由到端口 10025

- 1 如有必要，将 Network Prevent for Email 配置为使用默认端口 10025。
请参见第 893 页的“[针对反射或转发模式配置 Network Prevent for Email Server](#)”。
- 2 在 Network Prevent for Email 计算机的终端窗口中，请输入以下命令，将流量从端口 25 重新路由到端口 10025：

```
iptables -N Vontu-INPUT
iptables -A Vontu-INPUT -s 0/0 -p tcp --dport 25 -j ACCEPT
iptables -I INPUT 1 -s 0/0 -p tcp -j Vontu-INPUT
iptables -t nat -I PREROUTING -p tcp --destination-port 25 -j REDIRECT --to-ports=10025
iptables-save > /etc/sysconfig/iptables
```

注意：如果只想使用 Telnet 测试端口之间的本地 IP 路由，则使用命令：

```
iptables -t nat -I OUTPUT -o lo -p tcp --destination-port 25 -j
REDIRECT --to-ports=10025
```

如果稍后决定删除 IP 表条目，则使用命令：

```
iptables -t nat -D OUTPUT -o lo -p tcp --destination-port 25 -j REDIRECT --to-ports=10025
```

指定一个或多个上游邮件传输代理 (MTA)

默认情况下，Network Prevent for Email Server 可接受网络上任何系统与 ESMTP 服务端口的连接。为安全起见，您可以将 Network Prevent for Email Server ESMTP 通信限制为一组指定的邮件传输代理(MTA)。创建授权的系统的“白名单”。如果将一个或多个系统列入白名单，则不在白名单内的其他系统便不能连接到 Network Prevent for Email Server ESMTP 服务端口。

请注意，MTA 白名单可能会受 **RequestProcessor.BindAddress** 设置影响。默认情况下，**RequestProcessor.BindAddress** 设置为 0.0.0.0，而侦听程序会绑定到所有可用的地址。如果 RequestProcessor.BindAddress 指示侦听程序绑定到特定 IP，则已列入白名单的 MTA 也必须能够接入到侦听程序地址。

创建允许与 Network Prevent for Email Server 通信的系统的白名单：

- 1 转至“系统”>“服务器”>“概述”，并单击所需的 Network Prevent for Email Server。
- 2 在显示的“服务器详细信息”屏幕上，单击“服务器设置”。

3 向下滚动至 **RequestProcessor.AllowHosts** 字段。

默认情况下，**RequestProcessor.AllowHosts** 设为 `any`，表示网络上所有其他系统都能够与此 Network Prevent for Email Server 进行通信。

4 您可以限制能够与此 Network Prevent for Email Server 连接的系统。删除 `any`，然后输入想要授权的系统 IP 地址或 FQDN。请以逗号分隔多个地址。例如：123.14.251.31,smtp_1.corp.mycompany.com,123.14.223.111。仅使用逗号分隔地址；不要包含空格。

5 单击“保存”。

对此设置所做的更改在您重新启动服务器之后才会生效。

为 Network Prevent for Email 创建策略

可以创建包含任意标准响应规则的策略。例如，添加注释、限制事件数据保留、记录到 Syslog 服务器、发送电子邮件通知和设置状态。

请参见第 314 页的“[实施策略](#)”。

也可以加入以下 Network Prevent for Email 所特有的规则：

■ 网络：阻止 SMTP 邮件

阻止包含机密数据或重要元数据的电子邮件（按策略中所定义）。可以配置 Symantec Data Loss Prevention 退回邮件或将邮件重定向至指定地址。

重定向功能通常用于将邮件重新路由至邮箱或邮件列表的地址。管理员使用该邮箱或列表来查看和释放邮件。这些邮箱在 Symantec Data Loss Prevention 系统之外。

■ 网络：修改 SMTP 邮件

修改包含机密数据或重要元数据的电子邮件（按策略中所定义）。可以使用该操作来修改邮件主题，或添加特定的 RFC-2822 邮件标头，以便触发进一步的后续处理。例如，邮件加密、邮件隔离或邮件存档。

有关设置任意响应规则操作的详细信息，请打开联机帮助。转至“管理”>“策略”>“响应规则”，然后单击“添加响应规则”。

有关使用“网络：修改 SMTP 邮件”操作来触发下游处理（如邮件加密）的详细信息，请参见《Symantec Data Loss Prevention MTA 集成指南（适用于 Network Prevent）》。

即使不在策略中加入响应规则，只要策略包含检测规则，Network Prevent for Email 也会捕获事件。如果想要查看 Symantec Data Loss Prevention 捕获的事件类型并在之后优化策略，则该功能十分有用。

创建 Network Prevent for Email 的测试策略

- 1 在 Enforce Server 管理控制台中创建包含 Network Prevent for Email 特有操作之一的响应规则。例如，创建包括“**网络：阻止 SMTP 邮件**”操作的响应规则。

请参见第 669 页的[“配置响应规则”](#)。

- 2 创建包含在上一步中配置的响应规则的策略。

例如，按如下所示创建称为“测试策略”的策略：

- 包括按照关键字 secret 进行匹配的“**内容匹配关键字**”检测规则。
- 包括“**网络：阻止 SMTP 邮件**”响应规则。
- 将它与“**默认**”策略组相关联。

请参见第 330 页的[“配置策略”](#)。

请参见第 901 页的[“关于策略违规数据标头”](#)。

关于策略违规数据标头

一封邮件可能会违反多个策略。对于用于报告邮件所违反的策略数目与严重性的传出邮件，您可以为其添加特殊标头。您可使用下列三种不同种类的违规数据标头：

- **违反的策略数目**-一种可添加的标头，用于报告邮件违反的策略的总数。
- **最高严重性**-一种可添加的标头，用于报告邮件违反的所有策略中单个的最高严重性级别（“高”、“中”、“低”或“信息”）。
- **累计严重性评分**-一种可添加的标头，用于报告严重性总评分，该评分是所有策略违规的数字总和。为此，严重性级别指定为如下数值：高=4、中=3、低=2以及信息=1。因此，同时违反“低(2)”与“中(3)”严重性策略的消息，其严重性评分为 5。

可以使用标头触发基于违规数目或违规严重性的下游响应。例如：

- 违反单个策略的邮件会被路由到一个隔离邮箱。违反多个策略的邮件则会被路由到第二个邮箱。违反超过指定数量的策略的邮件，则会被路由到第三个邮箱。
- 对于违反多个策略的邮件，可以根据最严重的违规严重性级别，以不同的方式对其进行处理。
- 对于违反多个策略的邮件，可以根据邮件的严重性评分，以不同的方式对其进行处理。

请参见第 902 页的[“启用策略违规数据标头”](#)。

启用策略违规数据标头

可以组合使用三种多策略标头。

启用策略违规邮件标头：

- 1 转至“系统”>“服务器”>“概述”，并单击所需的 Network Prevent for Email Server。
- 2 在显示的“服务器详细信息”屏幕上，单击“服务器设置”。
- 3 向下滚动至下列三个 **RequestProcessor** 设置之一。默认情况下，这些设置值为 **false**。
- 4 将值更改为 **true**。
- 5 单击“保存”。

对这些设置所做的更改在您重新启动服务器之后才会生效。

三个 **RequestProcessor** 高级设置可启用不同种类的多策略违规邮件标头：

- **RequestProcessor.TagPolicyCount**。
设置设为 **true** 时，Network Prevent 会添加标头，报告该邮件违反的策略总数。例如，如果邮件违反 3 个策略，就会添加名为 X-DLP-Policy-Count: 3 的标头。
- **RequestProcessor.TagHighestSeverity**。
设置设为 **true** 时，Network Prevent 会添加标头，报告所违反的策略中最高的严重性。例如，如果邮件违反三个策略，其中一个的严重性为“中”，而另外两个的严重性为“低”，就会添加名为 X-DLP-Max-Severity: MEDIUM 的标头。
- **RequestProcessor.TagScore**。
设置设为 **true** 时，Network Prevent 会添加标头，报告违反的所有策略的累计评分。使用以下公式计算分数：高=4，中=3，低=2，信息=1。例如，如果邮件违反了三项策略，其中一个的严重性为“中”，其他两个的严重性为“低”，就会添加名为 X-DLP-Score: 7 的标头。

将值设为 **true**，会使相应的标头自动添加到所处理的每封传出邮件。即使该邮件只违反了一个策略也是如此。

请参见第 901 页的“[关于策略违规数据标头](#)”。

测试 Network Prevent for Email

可以通过发送违反测试策略的电子邮件来对 Network Prevent for Email 进行测试。

测试系统

- 1 访问通过 Network Prevent for Email Server 集成的 MTA 路由邮件的电子邮件帐户。
- 2 发送包含机密数据的电子邮件。例如，发送包含 *Secret* 一词的电子邮件。
- 3 在 Enforce Server 管理控制台中，转至“事件”>“网络”，并单击“事件 - 全部”。查找生成的事件。例如，搜索包括适当的时间戳和策略名称的事件条目。
- 4 单击相关事件条目来查看完整的事件快照。

请参见第 775 页的[“关于 Symantec Data Loss Prevention 报告”](#)。

实施 Network Prevent for Web

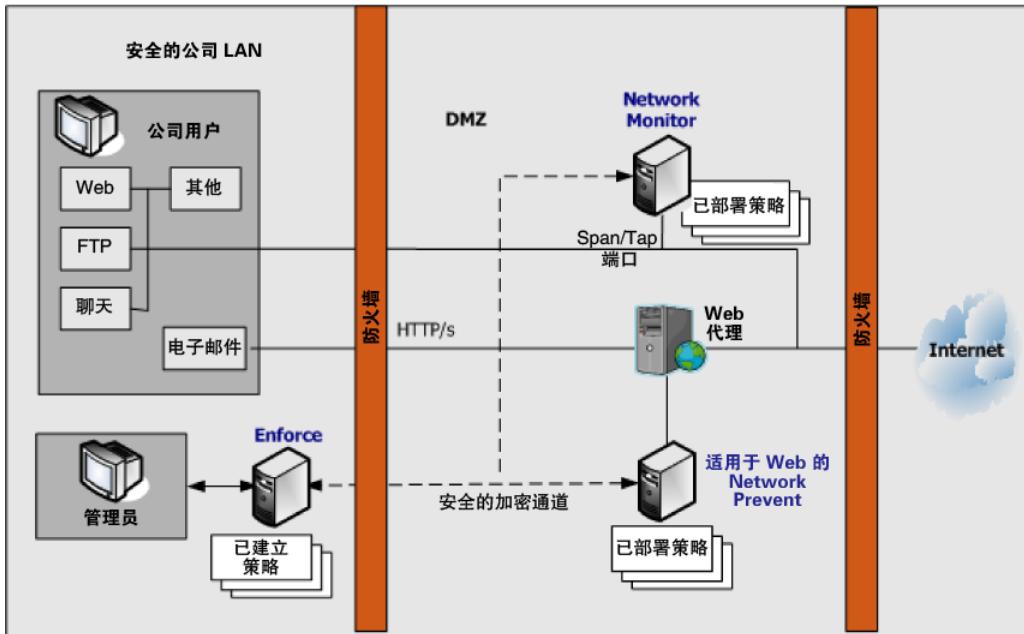
本章节包括下列主题：

- 实施 Network Prevent for Web
- 配置 Network Prevent for Web Server
- 关于代理服务器配置
- 指定一个或多个代理服务器
- 为 Network Prevent for Web 启用 GET 处理
- 为 Network Prevent for Web 创建策略
- 测试 Network Prevent for Web
- Network Prevent for Web Server 的故障排除信息

实施 Network Prevent for Web

Network Prevent for Web Server 可使用 ICAP 与 HTTP、HTTPS 或 FTP 代理服务器相集成，以进行内置活动 Web 请求管理。如果它在 Web 内容中检测到机密数据，便会使代理依策略规定拒绝请求，或删除 HTML 内容。

图 53-1 基本 Network Prevent for Web 设置



首先，您需要了解实施 Network Prevent for Web 所需的高级步骤。有关更多详细信息，请查看交叉引用章节。

实施 Network Prevent for Web

- 1 请确保 Network Prevent for Web Server 已配置为与 HTTP 代理服务器通信。
也可以视需要配置检测服务器过滤流量。
请参见第 907 页的“[配置 Network Prevent for Web Server](#)”。
- 2 将 HTTP 代理服务器配置为与 Network Prevent for Web Server 协同工作。
请参见第 910 页的“[关于代理服务器配置](#)”。
- 3 创建和部署 Network Prevent for Web 策略。
请参见第 914 页的“[为 Network Prevent for Web 创建策略](#)”。
- 4 针对测试策略生成事件，以测试系统。
请参见第 916 页的“[测试 Network Prevent for Web](#)”。
- 5 如有需要，请对实施问题进行故障排除。
请参见第 916 页的“[Network Prevent for Web Server 的故障排除信息](#)”。

Network Prevent 授权许可

Network Prevent 有多种不同的部署方案。可以将 Network Prevent 作为一个独立产品进行部署，也可以将其与 Mobile Prevent for Web 一起部署。

Symantec Data Loss Prevention 的用户界面因您购买的许可证而异。屏幕上显示的内容可能与 Symantec Data Loss Prevention 文档中的描述略有差异。该文档假设您是将 Mobile Prevent 与 Network Prevent 一起部署的。

例如，您创建了一个响应规则来阻止通过 HTTP 协议传输敏感信息。如果您已将 Network Prevent 作为一个独立产品进行部署，那么“**阻止 HTTP/HTTPS**”响应规则操作就会显示在 **Network Prevent** 标题下方。如果您将 Mobile Prevent 与 Network Prevent 一起部署，那么该响应规则操作就会显示在 **Network and Mobile Prevent for Web** 标题下方。

请参见第 1231 页的“[实施 Mobile Prevent](#)”。

配置 Network Prevent for Web Server

您可以使用 Network Prevent for Web Server 的多个配置选项。例如，您可以将服务器配置为：

- 忽略小型 HTTP 请求或响应。
- 忽略特定主机或域（例如企业子公司的域）的请求或响应。
- 忽略用户搜索引擎查询。

修改 Network Prevent for Web Server 配置

- 1 转至“系统”>“服务器”>“概述”，然后单击 Network Prevent for Web Server。
- 2 在显示的“服务器详细信息”屏幕上，单击“配置”。
如后续步骤中所述，您可以验证或修改 **ICAP** 选项卡上的设置。该选项卡分为如下几个部分：“请求过滤”、“响应过滤”和“连接”。
- 3 验证或修改“试用模式”设置。“试用模式”让您无需实时阻止请求即可测试阻止功能。如果选择“试用模式”，则 Symantec Data Loss Prevention 会检测事件并指出其阻止了 HTTP 通信，但它并没有阻止该通信。

4 针对来自 HTTP 客户端（用户代理）的请求验证或修改过滤器选项。“请求过滤”部分的选项如下：

忽略小于以下大小的请求

指定要检查的HTTP请求的最小正文大小。
(默认为4096个字节。)例如，在搜索引擎(如Yahoo或Google)中键入的搜索字符串通常很短。通过调整该值，您可以将这些搜索排除在检查范围之外。

忽略没有附件的请求

让服务器只检查包含附件的请求。如果您主要涉及一些计划发布敏感文件的请求，该选项非常有用。

忽略向主机或域的请求

让服务器忽略您指定的主机或域的请求。如果预期公司总部和分公司之间有大量HTTP流量，则该选项非常有用。您可以键入一个或多个主机或域名(例如www.company.com)，每个域名各自一行。

忽略来自用户代理的请求

让服务器忽略来自您指定的用户代理(HTTP客户端)的请求。如果组织使用频繁发送HTTP请求的程序或语言(如Java)，则该选项非常有用。您可以键入一个或多个用户代理值(例如java/1.4.2_xx)，每个值各自一行。

- 5 针对来自 Web 服务器的响应验证或修改过滤器选项。“**响应过滤**”部分的选项如下：

忽略小于以下大小的响应 指定该服务器所检查的 HTTP 响应的最小正文大小。（默认为 4096 字节。）

检查内容类型 指定响应中 Symantec Data Loss Prevention 应监视的 MIME 内容类型。默认情况下，该字段包含 Microsoft Office、PDF 以及纯文本格式的内容类型值。要添加其他值，请每行键入一个 MIME 内容类型。例如，键入 `application/wordperfect5.1` 让 Symantec Data Loss Prevention 分析 WordPerfect 5.1 文件。

注意，在 Web 代理层指定 MIME 内容类型通常更加高效。

忽略来自主机或域的响应 让服务器忽略来自您指定的主机或域的响应。您可以键入一个或多个主机或域名（例如 `www.company.com`），每个域名各自一行。

忽略对用户代理的响应 让服务器忽略对您指定的用户代理（HTTP 客户端）的响应。您可以键入一个或多个用户代理值（例如 `java/1.4.2_xx`），每个值各自一行。

- 6 验证或修改 HTTP 代理服务器和 Web Prevent Server 之间 ICAP 连接的设置。“连接”选项如下：

TCP 端口	指定该服务器用来侦听 ICAP 请求的 TCP 端口号。该端口号必须与在将 ICAP 请求发送至该服务器的 HTTP 代理上配置的值一样。建议值为 1344。
最大请求数	指定来自 HTTP 代理的最大并行 ICAP 请求连接数。默认值为 25。
最大响应数	指定来自 HTTP 代理的最大并行 ICAP 请求响应数。默认值为 25。
连接积压	指定允许的等待连接数。等待连接即等待来自浏览器的 HTTP 响应的用户。最小值为 1。如果 HTTP 代理收到太多请求（或响应），则代理会根据代理配置来处理这些请求或响应。您可以将 HTTP 代理配置为阻止大于该值的任何请求（或响应）。

- 7 单击“保存”退出“配置服务器”屏幕，然后单击“完成”退出“服务器详细信息”屏幕。

关于代理服务器配置

您必须至少配置一部 HTTP 代理服务器，以便将 Web 请求或响应转发到 Mobile Prevent for Web Server。HTTP 代理充当 Network Prevent for Web Server 的 ICAP 客户端。Symantec Data Loss Prevention 同时支持 ICAP 的请求修改 (REQMOD) 和响应修改 (RESPMOD) 模式。如果想要分析请求和响应，请使用其中一个 Network Prevent for Web Server 分析请求。使用另一个 Network Prevent for Web Server 分析响应。

请注意，大多数代理服务器均提供以 REQMOD 模式及 RESPMOD 模式过滤转发到 Network Prevent for Web Server 的内容的方法。有关详细信息，请参考代理服务器的文档。

请参见第 913 页的“[指定一个或多个代理服务器](#)”。

请参见第 910 页的“[代理服务器与 Network Prevent for Web 的兼容性](#)”。

请参见第 912 页的“[配置请求与响应模式服务](#)”。

代理服务器与 Network Prevent for Web 的兼容性

Network Prevent for Web Server 使用 ICAP 协议，而且可与以下代理一起操作：

表 53-1 Network Prevent for Web 支持的代理服务器

代理	支持的协议	配置信息
适用于 Network Prevent for Web 的 Blue Coat ProxySG 4.2.1、5.2.4.8、5.5.2.1 和 5.5.3.1 版本	HTTP、HTTPS、FTP over HTTP 或 FTP 代理	Blue Coat 产品文档
适用于 Mobile Prevent 或使用 Network Prevent for Web 部署的 Mobile Prevent 的 Blue Coat ProxySG 5.5.3.1 版本		
Cisco IronPort S-Series 6.0、7.1.2 版本	HTTP、HTTPS 和 FTP over HTTP	Cisco IronPort 产品文档
Microsoft ISA 2004, 2006 Standard 和 Enterprise 版本	HTTP 和受限制的 FTP over HTTP	请参见 <i>Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server</i> (《Symantec Data Loss Prevention 集成指南（适用于 Microsoft Internet Security and Acceleration Server）》)
Microsoft Windows 2008 R2 SP1 Enterprise 或 Standard Edition 上的 Microsoft TMG 2010 (不含 Service Pack, 或含 SP1 或 SP2)	HTTP、HTTPS、受限制的 FTP over HTTP/S	请参见《Symantec Data Loss Prevention 集成指南（适用于 Microsoft Threat Management Gateway）》
Secure Computing Secure Web (Webwasher) 6.8.x 和 6.9.1 版本	HTTP、HTTPS、FTP over HTTP 或 FTP 代理	Secure Web 文档 (特别是说明使用 DLP 解决方案设置 Secure Web 的章节)
Squid Web Proxy 3.0 和 3.1.11 Stable 18 版本 (仅限 Linux)	HTTP	请参见 <i>Symantec Data Loss Prevention Integration Guide for Squid Web Proxy</i> (《Symantec Data Loss Prevention 集成指南（适用于 Squid Web 代理）》)
Symantec Web Gateway 5.0 和 5.0.2.8 版本	HTTP、HTTPS	请参见 <i>Symantec Web Gateway 5.0 Implementation Guide</i> (《Symantec Web Gateway 5.0 操作指南》)

代理	支持的协议	配置信息
Websense Appliance V5000 和 V10000, 含 Websense Web Security 7.6.0 版 (11.1.1 和以上版本)	HTTP、HTTPS	<p>不支持编辑。</p> <p>仅支持“阻止 HTTP/HTTPS”。</p> <p>不支持 RESPMOD。</p> <p>仅当 Symantec Data Loss Prevention 拒绝消息（在响应规则中）的大小超过 512 字节时，Websense 才会阻止通信。如果拒绝消息小于 512 字节，则会生成一个事件，但不会阻止网络流量。</p>

请参见第 913 页的“[指定一个或多个代理服务器](#)”。

请参见第 910 页的“[关于代理服务器配置](#)”。

配置请求与响应模式服务

有关配置代理服务器的详细信息，请参考代理服务器产品文档，或联系代理服务器管理员。

配置代理服务器：

- 1 REQMOD。在代理服务器上，创建将请求转发至 Mobile Prevent for Web Server 的 ICAP REQMOD 服务。如果代理服务器支持不同的协议，请将其配置为处理所需的协议。

对于 REQMOD 模式，代理服务器上的 ICAP 服务应类似如下所示：

```
icap://ip_address|FQDN[:port]/reqmod
```

- 2 RESPMOD。在代理服务器上，创建将响应转发至 Mobile Prevent for Web Server 的 ICAP RESPMOD 服务。如果代理服务器支持不同的协议，请将其配置为处理所需的协议。

对于 RESPMOD 模式，代理服务器上的 ICAP 服务应类似如下所示：

```
icap://ip_address|FQDN[:port]/respmod
```

其中：

- *ip_address|FQDN* 使用 IP 地址或完全限定域名标识 Mobile Prevent for Web Server。

- *Port* 是 Mobile Prevent for Web Server 倾听的端口号。使用默认的 ICAP 端口 (1344) 时，指定端口号为可选步骤。
- 要在 REQMOD 模式中正确工作，必须使用 /reqmod。
- 要在 RESPROMD 模式中正确工作，必须使用 /respmmod。

示例：

```
icap://10.66.194.45/reqmod
icap://10.66.194.45:1344/reqmod
icap://netmonitor1.company.com/reqmod
icap://10.66.194.45/respmmod
icap://10.66.194.45:1344/respmmod
icap://netmonitor1.company.com/respmmod
```

请注意，代理上的 ICAP 服务定义中指定的端口，必须与 Mobile Prevent for Web Server 倾听的端口匹配。

请参见第 910 页的“[代理服务器与 Network Prevent for Web 的兼容性](#)”。

请参见第 910 页的“[关于代理服务器配置](#)”。

指定一个或多个代理服务器

默认情况下，Network Prevent for Web Server 可接受网络上任何系统与 ICAP 服务端口的连接。为安全起见，您可以将 ICAP 连接限制为仅应用于指定的系统（或“白名单”）。将一个或多个系统添加白名单后，不在白名单上的系统则不能连接至 Network Prevent for Web Server ICAP 服务端口。

请注意，**Icap.BindAddress** 设置会影响代理服务器白名单。默认情况下，**Icap.BindAddress** 设置为 0.0.0.0，而侦听程序会绑定到所有可用地址。如果**Icap.BindAddress** 指示侦听程序绑定到特定 IP，则白名单列出的代理也必须能够接入到该侦听程序地址。

创建允许连接至 Network Prevent for Web Server ICAP 服务端口的系统白名单：

- 1 转至“系统”>“服务器”>“概述”，并单击所需的 Network Prevent for Web Server。
- 2 在显示的“服务器详细信息”屏幕上，单击“服务器设置”。
- 3 向下滚动至 **Icap.AllowHosts** 设置。

默认情况下，**Icap.AllowHosts** 设置为 any，表示网络上的所有其他系统均可与此 Network Prevent for Web Server 进行通信。

- 4 您可以限制能够与此 Network Prevent for Web Server 连接的系统。删除 any，输入您要授权的系统 IP 地址或完全限定域名称 (FQDN)。

请以逗号分隔多个地址。例如：

123.14.251.31,webcache.corp.mycompany.com,123.14.223.111。仅使用逗号分隔多个条目；不要包含空格。

- 5 单击“保存”。

对此设置所做的更改在您重新启动服务器之后才会生效。

请参见第 910 页的“[代理服务器与 Network Prevent for Web 的兼容性](#)”。

请参见第 910 页的“[关于代理服务器配置](#)”。

为 Network Prevent for Web 启用 GET 处理

默认情况下，Mobile Prevent for Web 不处理 HTTP GET 命令，因为这类命令的流量很高。按照此过程可使服务器处理 GET 命令。

为 Network Prevent for Web 启用 GET 处理

- 1 配置 Web 代理服务器将 GET 请求传送至 Network Monitor Server，如代理服务器文档中所述。
- 2 确保 Network Monitor Server 的 **L7.processGets** 高级服务器设置必须为 true（此为默认值）。
- 3 减小 Network Monitor Server 上 **L7.minSizeofGetURL** 高级设置的大小。从默认值 100 减小为小于最短网站 URL（您要从其处理 GET 命令）长度的字节数。如果将最小 URL 大小设为 10，将处理所有情况。但是请注意，减小 GET 的最小大小会增大必须处理的请求数，这会增加服务器流量负载。
- 4 调整 Network Prevent for Web 的“服务器详细信息”页面 ICAP 部分中的“忽略小于以下大小的请求”设置。从默认的 4096 字节减少为将使请求接受 DLP 检查的较小值。但是请注意，减少此值会增加服务器流量负载。

请参见第 888 页的“[对 Network Monitor 启用 GET 处理](#)”。

为 Network Prevent for Web 创建策略

可以创建包含任意标准响应规则的策略。例如，添加注释、限制事件数据保留、记录到 Syslog 服务器、发送电子邮件通知和设置状态。

请参见第 775 页的“[关于 Symantec Data Loss Prevention 报告](#)”。

也可以加入以下 Network Prevent for Web Server 所特有的规则：

- **Network Prevent: 阻止 HTTP/HTTPS**

阻止包含机密数据的发布（按策略中所定义）。这包括 Web 发布、基于 Web 的电子邮件、上传到网站或附加到基于 Web 的电子邮件的文件。

注意：某些应用程序可能不会对“**Network Prevent: 阻止 HTTP/HTTPS**”响应操作做出适当响应。在 Yahoo! Mail 应用程序中，检测服务器在阻止文件上传时出现过这种情况。如果用户尝试上传电子邮件附件并且附件触发了“**Network Prevent: 阻止 HTTP/HTTPS**”响应操作，Yahoo! Mail 不会做出响应，也不会显示说明文件已被阻止的错误消息。相反，Yahoo! Mail 看上去仍在继续上传选择的文件，但是上传永远无法完成。用户必须在某个时间通过手动单击“取消”来取消上传。

其他应用程序可能也存在这种情况，这取决于它们如何处理阻止请求。在这些情况下，即使应用程序没有发出这种指示，也会创建检测服务器事件，并阻止文件上传。

■ **Network Prevent: 删除 HTTP/HTTPS 内容**

从包含机密数据的发布中删除机密数据（按策略中所定义）。这包括基于 Web 的电子邮件以及上传到网站或附加到基于 Web 的电子邮件的文件。请注意，“**删除 HTTP/HTTPS 内容**”操作仅对请求有效。

■ **Network Prevent: 阻止 FTP 请求**

阻止包含机密数据的 FTP 传输（按策略中所定义）。

有关设置任意响应规则操作的详细信息，请打开联机帮助。转至“管理”>“策略”>“响应规则”，然后单击“添加响应规则”。

即使不在策略中加入响应规则，只要策略包含检测规则，Network Prevent for Web 也会捕获事件。可以设置此类策略，在实施阻止或删除内容的策略之前监视网络上的 Web 和 FTP 活动。

如果已将代理配置为同时转发 HTTP/HTTPS 请求和响应，则策略对二者均有效。例如，策略同时适用于网站的上传和下载内容。

创建 Network Prevent for Web 的测试策略

- 1 在 Enforce Server 管理控制台中创建包含 Network Prevent for Web 特有操作之一的响应规则。例如，创建包含“**Network Prevent: 阻止 HTTP/HTTPS**”操作的响应规则。

请参见第 669 页的“[配置响应规则](#)”。

- 2 创建包含在上一步中配置的响应规则的策略。

例如，按如下所示创建称为“测试策略”的策略：

- 包括按照关键字 secret 进行匹配的“**内容匹配关键字**”检测规则。

- 包括“Network Prevent: 阻止 HTTP/HTTPS”响应规则。

- 将它与“默认”策略组相关联。

请参见第 330 页的[“配置策略”](#)。

测试 Network Prevent for Web

您可以通过发送一封违反测试策略的 Web 电子邮件来测试 Network Prevent for Web。

测试系统

- 1 打开通过 HTTP 代理服务器访问 Internet 的浏览器。
- 2 在浏览器中，访问测试 Web 电子邮件帐户，并发送一封附件含有机密数据的电子邮件。例如，访问 Hotmail 帐户，并发送一封附件含有 *Secret* 一词及更多文本段落的电子邮件。
- 3 在 Enforce Server 管理控制台中，转至“事件”>“网络”，然后单击“事件 - 全部”。查找生成的事件。例如，搜索包括适当的时间戳和策略名称的事件条目。
- 4 单击相关事件条目来查看完整的事件快照。

请参见第 776 页的[“关于使用报告的策略”](#)。

Network Prevent for Web Server 的故障排除信息

下表描述了使用 Network Prevent for Web Server 时的常见问题并提出了可能的解决方案。

表 53-2 故障排除

问题	可能的解决方案
“网络”报告中会显示事件，但 Symantec Data Loss Prevention 不执行相关响应规则中指定的操作。	当 Network Prevent for Web Server 运行于试用模式（默认设置）时，预计会出现该行为。如果不想在试用模式中运行，请更改设置。 请参见第 907 页的 “配置 Network Prevent for Web Server” 。

8

部分

发现机密数据的存储位置

- 54. 关于 Network Discover
- 55. 设置和配置 Network Discover
- 56. Network Discover 扫描目标配置选项
- 57. 管理 Network Discover 目标扫描
- 58. 管理 Network Discover 事件报告
- 59. 使用服务器 FlexResponse 插件补救事件
- 60. 设置文件共享扫描
- 61. 设置 Lotus Notes 数据库扫描
- 62. 设置 SQL 数据库扫描
- 63. 设置 SharePoint 服务器扫描
- 64. 设置 Exchange Server 扫描
- 65. 关于 Network Discover 扫描程序
- 66. 设置文件系统扫描
- 67. 设置 Microsoft Exchange Server 扫描
- 68. 设置 SharePoint 2007 服务器扫描

- 69. 设置 SharePoint 2003 服务器扫描
- 70. 设置 Web 服务器扫描
- 71. 设置 Documentum 存储库扫描
- 72. 设置 Livelink 存储库扫描
- 73. 为自定义扫描目标设置 Web 服务

关于 Network Discover

本章节包括下列主题：

- [关于 Network Discover](#)
- [Network Discover 的工作原理](#)

关于 Network Discover

Network Discover 通过扫描大量企业数据存储库找到暴漏的机密数据。这些数据存储库包括文件服务器、数据库、Microsoft SharePoint、Lotus Notes、Documentum、LiveLink、Microsoft Exchange、Web 服务器及其他数据存储库。

Network Discover 可以扫描以下数据源：

- 网络文件共享 (CIFS、NFS 或 DFS)
请参见第 985 页的“[设置文件系统扫描](#)”。
- Windows 台式机和便携式计算机上的本地文件系统
Windows、Linux、AIX 和 Solaris 服务器上的本地文件系统
请参见第 1049 页的“[设置文件系统扫描](#)”。
- Lotus Notes 数据库
请参见第 995 页的“[设置 Lotus Notes 数据库扫描](#)”。
- SQL 数据库
请参见第 1003 页的“[设置 SQL 数据库扫描](#)”。
- SharePoint 2007 和 2010 服务器
请参见第 1011 页的“[设置 SharePoint 服务器扫描](#)”。
- Microsoft Exchange Server
请参见第 1023 页的“[使用 Exchange Web 存储连接器设置 Exchange 2003 和 2007 存储库的扫描](#)”。

请参见第 1032 页的“[设置使用 Exchange Web 服务扫描 Exchange 2007 SP2 和 2010 存储库](#)”。

■ Documentum

请参见第 1103 页的“[设置 Documentum 存储库扫描](#)”。

■ Livelink

请参见第 1111 页的“[设置 Livelink 存储库扫描](#)”。

■ Web 服务器（网站和基于 Web 的应用程序）

请参见第 1093 页的“[设置 Web 服务器扫描](#)”。

■ Microsoft Exchange

请参见第 1061 页的“[设置 Microsoft Exchange Server 扫描](#)”。

■ SharePoint 2007

请参见第 1075 页的“[设置 SharePoint 2007 服务器扫描](#)”。

■ SharePoint 2003

请参见第 1085 页的“[设置 SharePoint 2003 服务器扫描](#)”。

■ Web 服务

Web 服务暴漏自定义集成点。您可以写入自定义代码来扫描任何存储库。自定义代码检索存储库，并将内容提供给 Network Discover Server 进行扫描。自定义应用程序和存储库可以使用 Web 服务扫描。

请参见第 1119 页的“[为自定义扫描目标设置 Web 服务](#)”。

■ 自定义

可以写入自定义应用程序，以便从存储库中提取内容和元数据，并将其他们提供给 Network Discover。建议的用于自定义集成的 Network Discover 接口是 Web 服务。

Endpoint Discover 可以扫描 Windows 台式机和便携式计算机上的文件系统。

Endpoint Discover 在 Windows 台式机和便携式计算机上包括一个代理，可以扫描本地文件系统。

请参见第 1127 页的“[关于 Endpoint Discover 和 Endpoint Prevent](#)”。

在事件补救期间，Symantec Data Insight 可帮助组织解决由于不完整或不准确的元数据或跟踪信息所导致的识别信息的数据所有者和责任方的问题。

使用 Symantec Data Insight，用户可以监控文件访问，以根据访问历史记录自动识别文件的数据用户。随后使用信息将自动填入违反 Symantec Data Loss Prevention 策略的文件的事件详细信息中。此方法可以使用户识别敏感数据，还可以使责任用户补救和数据管理更高效。

请参见《[Symantec Data Loss Prevention Data Insight 操作指南](#)》。

FlexResponse 平台允许为使用 Symantec Data Loss Prevention Network Discover 发现的文件创建全面的自定义补救操作。FlexResponse 支持 Symantec 和第三方文

件安全解决方案，包括企业数字版权管理和加密。FlexResponse 是 Network Protect 产品的扩展，实现 FlexResponse 功能需要 Network Protect 产品。

有关可用插件的列表，请参见 *Symantec Data Loss Prevention FlexResponse Developers Guide* (《Symantec Data Loss Prevention FlexResponse 开发人员指南》) 或联系 Symantec Data Loss Prevention 专业服务人员。

在事件补救期间，可以使用已安装的 FlexResponse 插件来补救事件。

请参见第 967 页的“[使用服务器 FlexResponse 自定义插件补救事件](#)”。

Network Discover 的工作原理

Network Discover Server 可以查找大量暴露的机密数据。它可以与 Enforce Server 进行通信，获取有关策略和扫描目标的信息。它可以将找到的有关暴露的机密数据的信息发送到 Enforce Server 以进行报告和补救。

[图 54-1](#) 可在公司 LAN 内部安全地显示 Network Discover Server。

Network Discover Server 连接到 Enforce Server，并且每个服务器都执行与查找暴露的机密数据相关的任务。

为了将工作分散开，可以设置多个 Network Discover Server。

请参见第 187 页的“[添加检测服务器](#)”。

Network Discover Server 将扫描选定的目标，读取文件或存储库，并检测机密信息是否存在。

Enforce Server 包含用于执行下列任务的用户界面：

- 设置目标扫描。
- 选择目标存储库。
- 定义用于扫描的过滤器。
- 调度扫描。

请参见第 926 页的“[添加新的 Network Discover 目标](#)”。

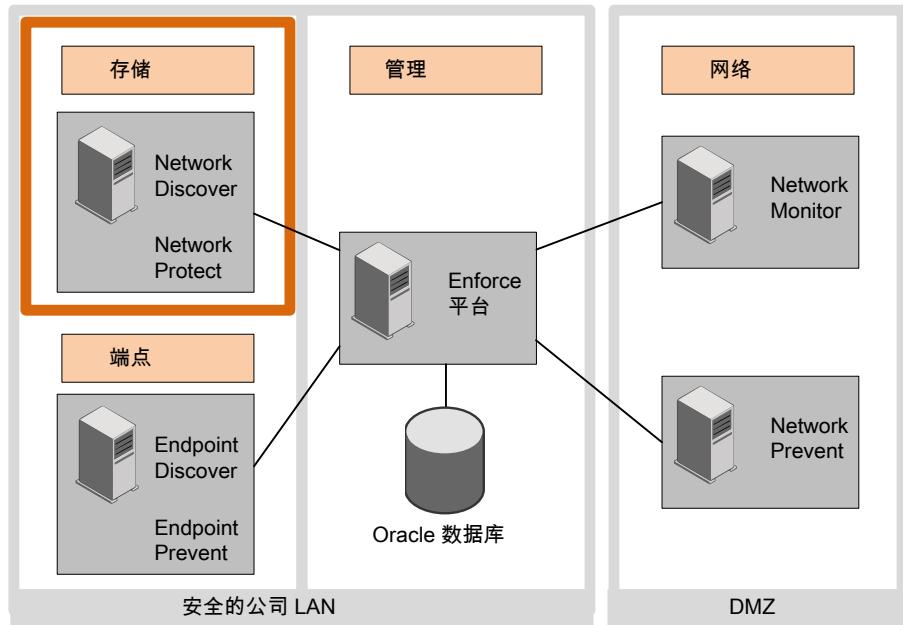
Enforce Server 还管理在 Network Discover Server 上运行的扫描并在用户界面中显示扫描的状态。

请参见第 943 页的“[管理 Network Discover 目标扫描](#)”。

扫描完成后，您可以在 Enforce Server 上显示暴露的机密数据的报告。

请参见第 961 页的“[关于 Network Discover 的报告](#)”。

图 54-1 Network Discover



设置和配置 Network Discover

本章节包括下列主题：

- [设置和配置 Network Discover](#)
- [修改 Network Discover Server 配置](#)
- [关于 Linux Network Discover Server](#)
- [添加新的 Network Discover 目标](#)
- [编辑现有的 Network Discover 目标](#)

设置和配置 Network Discover

设置 Network Discover 扫描目标包括几个步骤。正确进行 Network Discover 目标扫描需要运行每个步骤。

表 55-1 设置和配置 Network Discover

步骤	操作	详细信息
1	如果需要，请修改 Network Discover Server 配置。	请参见第 924 页的“ 修改 Network Discover Server 配置 ”。
2	创建策略组。	转至“系统”>“服务器”>“策略组”。 在显示的“策略组列表”屏幕上，单击“添加策略组”。 请参见第 349 页的“ 创建和修改策略组 ”。

步骤	操作	详细信息
3	创建策略。	<p>转至 Enforce Server 上的“管理”>“策略”>“策略列表”。</p> <p>选择“添加空白策略”。</p> <p>将规则添加至策略中。</p> <p>请参见第 330 页的“配置策略”。</p>
4	将 Network Protect 用于文件共享发现目标之前，请创建响应规则。使用 Network Protect 是可选步骤。	请参见第 653 页的 “关于响应规则” 。
5	创建 Network Discover 目标。	<p>转至 Enforce Server 上的“管理”>“发现扫描”>“发现目标”。</p> <p>单击“新建目标”，然后使用下拉菜单选择特定的目标类型。</p> <p>请参见第 926 页的“添加新的 Network Discover 目标”。</p>
6	设置目标的选项。	请参见第 929 页的 “Network Discover 扫描目标配置选项” 。
7	设置报告。	请参见第 775 页的 “关于 Symantec Data Loss Prevention 报告” 。

修改 Network Discover Server 配置

安装 Network Discover Server 并向 Enforce Server 注册之后，就可以修改 Network Discover Server 配置。

如果在 Linux 系统上安装 Network Discover Server，请注意与在 Windows 系统上安装 Network Discover Server 的区别。

请参见第 926 页的[“关于 Linux Network Discover Server”](#)。

Network Discover Server 可以安装在虚拟机上。有关受支持的虚拟机类型，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。

如果已配置了增量扫描，增量扫描索引会自动分发到所有发现服务器，包括所有新的发现服务器。

请参见第 956 页的[“关于增量扫描”](#)。

修改 Network Discover Server 配置

- 1 在 Enforce Server 管理控制台中，转至“系统”>“服务器”>“概述”。然后单击要修改的服务器。

这样会出现相应的“服务器详细信息”屏幕，并显示常规服务器信息、配置信息、已部署的索引，以及最近的服务器事件。

- 2 单击“配置”。

将显示“配置服务器”屏幕，并显示用于服务器类型的配置选项。

- 3 修改服务器配置。

下列配置选项位于“常规”选项卡上：

■ 名称

检测服务器的名称（用于在 Enforce Server 管理控制台中显示）。更改现有检测服务器的这项设置会影响 Symantec Data Loss Prevention 报告中的过滤器选项。Network Discover Server 是检测服务器。

■ 主机

检测服务器用于侦听与 Enforce Server 连接的检测服务器的主机名或 IP 地址。当您更换 Network Discover Server 主机计算机时，可能需要修改此设置。

■ 端口

检测服务器使用端口号接受来自 Enforce Server 的连接。此值必须大于 1024，并且必须与检测服务器的 `Communication.properties` 文件中 `listenPort` 属性的值匹配。此文件位于 `DLP_home\Protect\config`（例如 `c:\SymantecDLP\Protect\config`）中。如果更改此设置，请在修改 `Communication.properties` 文件中的 `listenPort` 值之后，重新启动检测服务器。安装成功之后，应该不需要更改此设置。

请参见第 175 页的“[服务器控件](#)”。

- 4 用于并行扫描的配置位于“发现”选项卡上。输入要在该 Network Discover Server 上运行的并行扫描数目。默认值为 1。

可以随时增大最大计数。增大该值之后，就会启动可在该 Network Discover Server 上运行的任何排队扫描。

只有在 Network Discover Server 没有运行中的扫描时，才能减小该计数。减小该计数之前，请暂停或停止 Network Discover Server 上的所有扫描。

支持并行扫描服务器与扫描程序目标类型。不支持并行扫描端点文件系统。

请参见第 958 页的“[配置 Network Discover 目标的并行扫描](#)”。

- 5 完成服务器配置修改之后，单击“保存”退出“配置服务器”屏幕，然后单击“完成”退出“服务器详细信息”屏幕。
- 6 若要查看此 Network Discover Server 上使用中的扫描，请转至“策略”>“发现扫描”>“发现服务器”。

请参见第 943 页的[“管理 Network Discover 目标扫描”](#)。

关于 Linux Network Discover Server

如果在 Linux 系统上安装 Network Discover Server，请注意下列与 Windows 系统上的 Network Discover Server 的区别。

- 扫描文件后，无法重置该文件的“上次访问时间”日期。
- 无法检索违规文件的“所有者”和“上次访问时间”日期，但可以正确检索访问控制列表 (ACL)。
- 您无法扫描 Microsoft Outlook 个人文件夹 (.pst) 文件。
- 不支持 SFTP 扫描。
- Linux 上的 Network Discover Server 使用限于单线程的 jCIFS。与在 Windows Network Discover Server 上相比，扫描速度可能会慢一些。

请参见第 923 页的[“设置和配置 Network Discover”](#)。

添加新的 Network Discover 目标

在添加 Network Discover 目标之前，必须完成 Network Discover Server 设置。

请参见第 923 页的[“设置和配置 Network Discover”](#)。

添加 Network Discover 目标

- 1 在EnforceServer管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击“新建目标”，然后使用下拉菜单选择特定的目标类型。
- 3 在“常规”选项卡上，输入 Network Discover 目标的名称。将显示此名称，用于管理扫描。

请参见第 943 页的[“管理 Network Discover 目标扫描”](#)。
- 4 输入其余的必需参数。输入策略组。输入 Network Discover Server。

请参见第 930 页的[“为 Network Discover 目标配置必填字段”](#)。

5 继续添加新目标，以及特定于该目标类型的条目。

网络文件共享 (CIFS、NFS、DFS)	请参见第 985 页的“ 设置文件系统扫描 ”。
Lotus Notes 数据库	请参见第 995 页的“ 设置 Lotus Notes 数据库扫描 ”。
SQL 数据库	请参见第 1003 页的“ 设置 SQL 数据库扫描 ”。
Windows 台式机和便携式计算机上的本地文件系统	请参见第 1049 页的“ 设置文件系统扫描 ”。
Windows、Linux、AIX 和 Solaris 服务器上的本地文件系统	
Microsoft Exchange	请参见第 1061 页的“ 设置 Microsoft Exchange Server 扫描 ”。
SharePoint	请参见第 1075 页的“ 设置 SharePoint 2007 服务器扫描 ”。
	请参见第 1085 页的“ 设置 SharePoint 2003 服务器扫描 ”。
Documentum	请参见第 1103 页的“ 设置 Documentum 存储库扫描 ”。
Livelink	请参见第 1111 页的“ 设置 Livelink 存储库扫描 ”。
Web 服务器 (网站和基于 Web 的应用程序)	请参见第 1093 页的“ 设置 Web 服务器扫描 ”。

6 配置可选的 Network Discover 目标参数。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

编辑现有的 Network Discover 目标

要设置各种配置选项，请编辑 Network Discover 目标的配置。

您还可以添加一个新的 Network Discover 目标，并在此时设置选项。

请参见第 926 页的“[添加新的 Network Discover 目标](#)”。

编辑 Network Discover 目标

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击列表中的扫描目标之一，以打开要编辑的目标。
- 3 编辑所需的选项。

请参见第 929 页的[“Network Discover 扫描目标配置选项”](#)。

Network Discover 扫描目标配置选项

本章节包括下列主题：

- [Network Discover 扫描目标配置选项](#)
- [为 Network Discover 目标配置必填字段](#)
- [调度 Network Discover 扫描](#)
- [为 Network Discover 扫描的内容提供密码身份验证](#)
- [加密配置文件中的密码](#)
- [设置发现过滤器以在扫描中包括或排除项目](#)
- [按项目大小过滤发现目标](#)
- [根据上次访问或修改日期过滤发现目标](#)
- [使用 Network Discover 扫描限制优化资源](#)
- [创建未受保护的敏感数据的位置的库存](#)

Network Discover 扫描目标配置选项

使用“常规”、“扫描的内容”和“高级”选项卡配置 Network Discover 扫描目标。

“常规”选项卡可用于所有目标类型。

“扫描的内容”和“高级”选项卡仅可用于某些目标类型。

请参见第 927 页的[“编辑现有的 Network Discover 目标”](#)。

有关特定于某种目标类型的其他配置信息，请参考该目标类型所对应的章节。

请注意，如果提供值，会使用 AND 将所有过滤器组合在一起。添加或修改扫描过滤器时，请考虑所有过滤器值，以避免不慎在扫描中包括所有项目或排除所有项目。

对于添加或编辑目标时的配置，请选择以下选项：

可选任务	扫描目标的选项 卡	任务说明
配置所需字段。 添加新目标后，需要设置这些必填字段。	常规	请参见第 930 页的“ 为 Network Discover 目标配置必填字段 ”。
调度 Network Discover 扫描。	常规	请参见第 931 页的“ 调度 Network Discover 扫描 ”。
配置增量扫描。	常规	请参见第 957 页的“ 使用增量扫描来扫描新的或修改过的项 ”。
提供身份验证，并设置凭据。	扫描的内容	请参见第 933 页的“ 为 Network Discover 扫描的内容提供密码身份验证 ”。
在扫描中包括或排除储存库。	扫描的内容	请参见第 935 页的“ 设置发现过滤器以在扫描中包括或排除项目 ”。
按文件大小过滤目标。	扫描的内容	请参见第 937 页的“ 按项目大小过滤发现目标 ”。
根据上次访问或修改日期过滤目标。	扫描的内容	请参见第 938 页的“ 根据上次访问或修改日期过滤发现目标 ”。
使用扫描限制优化资源。	高级	请参见第 940 页的“ 使用 Network Discover 扫描限制优化资源 ”。
创建未受保护的敏感数据位置的库存。	高级	请参见第 941 页的“ 创建未受保护的敏感数据的位置的库存 ”。
使用 Network Protect 移动或隔离网络文件共享中的文件。	保护	请参见第 992 页的“ 为文件共享配置 Network Protect ”。

为 Network Discover 目标配置必填字段

对于新目标，请输入目标的名称、策略组和可以运行扫描的发现服务器。

添加新目标后，需要设置这些必填字段。

为目标输入必填字段

1 在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“发现目标”。

2 单击“新建目标”，然后使用下拉菜单选择特定的目标类型。

3 在“常规”选项卡上，输入此发现目标的“名称”。

输入目标的唯一名称，或编辑现有名称，最多为 255 个字符。

4 选择“策略组”。

如果未选择其他任何策略组，则会使用默认策略组。要应用策略组，请选择要用于此目标的策略组。您可以将多个策略组分配给一个目标。

管理员会在“策略组列表”页面上定义策略组。如果要使用的策略组未显示在列表中，请联系您的 Symantec Data Loss Prevention 管理员。

5 选择允许运行扫描的一个或多个发现服务器。

如果您选择多个服务器，则 Symantec Data Loss Prevention 会在扫描开始时自动选择其中一个服务器。

列表中仅显示配置为发现服务器的检测服务器。如果网络上只有一个发现服务器，则会自动指定该发现服务器的名称。在配置目标之前，应先配置发现服务器。在对此目标运行扫描之前，必须至少指定一台服务器。

6 在“扫描的内容”选项卡上，必须输入要扫描的项目。有关此条目的其他信息，请参考各种目标类型的相关文档。

请参见第 919 页的“[关于 Network Discover](#)”。

7 您可以为此目标配置其他选项。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

调度 Network Discover 扫描

Network Discover 扫描可以设置为定期运行，例如在晚上或周末。扫描还可以设置为在指定时间内暂停，例如，资源通常忙于其他任务的时候。

对于文件共享、Lotus Notes 或 SQL 数据库，可使用“**扫描日程表**”的参数完整指定扫描日程表。

对于扫描程序目标（例如 SharePoint 或 Exchange），还必须从安装了扫描程序的计算机中调度扫描。您必须手动管理发现目标和扫描程序应用程序之间的扫描日程表。扫描程序已在 Enforce Server 和 Network Discover Server 之外进行安装、配置和运行。例如，可以将扫描程序调度为使用主机的本机日程表自动运行。您可以创建 UNIX cron 作业，或者向 Windows 调度程序添加扫描程序。扫描程序应调度为在调度的 Network Discover 扫描之前运行，以便 Network Discover 扫描有信息可用。

如果您要选择启动或暂停扫描的特定时间，则需使用 Enforce Server 的时区。
您可以为此目标配置其他选项。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

设置扫描日程表

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击要调度的扫描的名称。
- 3 单击“常规”选项卡。
- 4 选择“按日程表提交扫描作业”项目。

选中此复选框以设置扫描指定目标的日程表时，可以使用“日程表”下拉列表。在“日程表”下拉列表中选择一个选项后，会显示附加字段。

- 5 选择以下附加字段之一：

无定期日程表	保存目标而不使用日程表。
扫描一次	于指定时间与日期运行一次扫描。
每日扫描	每天于指定的开始时间扫描目标。选中“直到”可以在特定日期后停止每日扫描。
每周扫描	每周扫描目标。选中“直到”可以在特定日期后停止每月扫描。
每月扫描	每月扫描目标。选中“直到”可以在特定日期后停止每月扫描。

- 6 单击“保存”。

在指定时间内暂停扫描

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击要在指定时间内暂停的扫描的名称。
- 3 单击“常规”选项卡。
- 4 选择“暂停扫描时间间隔”项目。

5 选择暂停选项。

此选项会在指定的时间间隔内自动暂停扫描。您可以转至“发现目标”屏幕，并单击目标项的启动图标来覆盖目标的暂停窗口。暂停窗口保持不变，并依指定暂停与扫描窗口相抵触的所有日后的运行的扫描。您也可以单击目标项中的继续图标，来重新启动暂停的扫描。

注意：如果在目标暂停期间修改了目标配置，则修改后的配置不会应用到已扫描的项目。暂停然后重新启动扫描时，扫描会从暂停扫描时所创建的检查点重新启动。修改后的配置可用于从该检查点扫描的项目。

6 单击“保存”。

为 Network Discover 扫描的内容提供密码身份验证

在“扫描的内容”选项卡上，输入用于进行身份验证的配置选项。

您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

在身份验证凭据中，避免使用特殊字符。身份验证凭据不得包括以下任何一种字符，否则扫描会失败：

- 竖线字符
- &号字符
- 引号（单或双）

为扫描的内容提供密码身份验证

1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。

2 单击扫描名称以提供密码身份验证。

3 单击“扫描的内容”选项卡。

4 您可以通过多种方式输入身份验证信息：

- 使用已存储的凭据。

如果有已存储的凭据，请从“使用保存的凭据”中的下拉列表中选择已命名的凭据。

- 可以为此目标中的所有共享提供全局扫描凭据。

在“使用这些凭据”中输入用户名和密码。

- 可以为列表中的每个共享提供单独的身份验证凭据。

如果提供了单独凭据，则将单独凭据取代全局扫描凭据。

单击“添加”或“编辑”为列表中的每个共享提供凭据。

在“添加”框中，使用以下语法输入共享和凭据：

path[, [username, password][, [depth][, remediation-username, remediation-password]]]]

对于忽略的项目，提供一个包含连续逗号的空条目。

- 5 凭据的格式取决于扫描类型。有关各种目标类型的凭据的特定格式和示例，请参见各目标类型的相关主题。

请参见第 919 页的“[关于 Network Discover](#)”。

- 6 可以在“扫描的内容”选项卡上设置其他选项。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

可以在“保护”选项卡上设置补救凭据。

请参见第 992 页的“[为文件共享配置 Network Protect](#)”。

加密配置文件中的密码

使用应用程序 `EncryptPassword.exe` 加密配置文件中的密码。

加密配置文件中的密码

- 1 导航至扫描程序计算机中扫描程序安装的 `bin` 目录。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

- 2 运行实用程序 `EncryptPassword.exe`。

该实用程序可加密扫描程序配置文件中提供的密码。

- 3 当实用程序要求您输入密码时，请输入密码。

- 4 单击加密选项。

- 5 将加密的密码放入 `Vontuscanter_typeScanner.cfg` 文件中的 `Password=` 设置中。

请参见第 1066 页的“[Exchange 扫描程序的配置选项](#)”。

请参见第 1089 页的“[SharePoint 2003 扫描程序的配置选项](#)”。

请参见第 1097 页的“[Web 服务器扫描程序的配置选项](#)”。

请参见第 1107 页的“[Documentum 扫描程序的配置选项](#)”。

请参见第 1116 页的“[Livelink 扫描程序的配置选项](#)”。

设置发现过滤器以在扫描中包括或排除项目

排除和包括过滤器可减少要扫描的项目或存储库的数量。

使用“包括过滤器”字段可以指定 Symantec Data Loss Prevention 应该处理的项目。如果将“包括过滤器”字段保留为空白，则 Symantec Data Loss Prevention 会匹配所选目标中的所有项目。如果在字段中输入了任何值，则 Symantec Data Loss Prevention 仅扫描匹配过滤器的那些项目。

使用“排除过滤器”字段可以指定 Symantec Data Loss Prevention 应该处理的项目。如果将“排除过滤器”字段保留为空白，则 Symantec Data Loss Prevention 会匹配所选目标中的所有项目。如果在字段中输入了任何值，则 Symantec Data Loss Prevention 仅扫描不匹配过滤器的那些项目。

要优化扫描，可以使用包括和排除过滤器来限制扫描。例如，可以排除二进制项目。二进制项目包含策略违规的可能性较小。

请参见第 953 页的[“关于 Network Discover 扫描优化”](#)。

请注意，如果提供值，会使用 AND 将所有过滤器组合在一起。添加或修改扫描过滤器时，请考虑所有的过滤器值（例如大小和日期）。请避免不慎在扫描中包括所有项目或排除所有项目。

当包括过滤器和排除过滤器都存在时，会优先使用排除过滤器。

您可以为此目标配置其他选项。

请参见第 929 页的[“Network Discover 扫描目标配置选项”](#)。

设置包括过滤器或排除过滤器

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击要添加包括过滤器或排除过滤器的扫描的名称。
- 3 单击“扫描的内容”选项卡。
- 4 将文件名或路径输入到“包括过滤器”和“排除过滤器”，以选择 Symantec Data Loss Prevention 应该处理的项目子集。请使用逗号分隔各条目，但不能含有空格。路径过滤器区分大小写。

当包括过滤器和排除过滤器都存在时，会优先使用排除过滤器。

“包括过滤器”和“排除过滤器”文件名是相对于文件系统根目录的名称。根据需要指定完整的路径或子目录。允许使用某些通配符。

[表 56-1](#) 显示了过滤器的语法。

如果“排除过滤器”的条目超出 1024 个字符的限制，可以创建一个包含要排除的文件名的排除文件。

- 5 单击“保存”。

创建排除文件

- 1 在 Symantec Data Loss Prevention 配置目录中创建名为 excludeFiles 的目录，例如 \SymantecDLP\Protect\config\excludeFiles\。对于具有多个发现服务器的配置，每个发现服务器上均必须有此目录和文件的副本。
- 2 在此目录中，为要排除的每一组项目创建一个文本文件。例如，您可以为要扫描的每一个 UNIX 系统创建一个文件。将文件命名为 *hostname.txt*，其中，*hostname* 是要扫描的系统名称（如目标配置中所提供）。此文本文件中的 *hostname* 必须与发现目标中的名称完全匹配。
- 3 在每个文件中，列出您要排除于扫描范围之外的路径（每行一个路径）。路径可以是文件、目录、符号链接或已装载目录。每个路径必须以 / 或 \ 分隔符开头，其后为共享名称、目录名称及文件名称。例如，有效路径为 \excludeshare\excludedir\excludefile。

表 56-1 显示了过滤器的语法。

表 56-1 包括过滤器和排除过滤器的语法

* (星号)	使用此通配符匹配任意字符序列，包括 null。
? (问号)	使用此通配符匹配位于特定位置的任意一个字符。
, (逗号)	代表逻辑运算符 OR。使用逗号分隔条目，但不要使用空格。
正斜杠 (/) 和反斜杠 (\)	这些字符是等效的。通常代表目录分隔符，但是在 Linux 上，反斜杠是文件名称的有效字符。
模式开头与结尾的空白	忽略模式开头与结尾的空白。分隔条目的逗号前后不要使用空格。
转义字符	匹配进程不支持转义字符，因此无法显式匹配问号、逗号或星号。通常，过滤器项目中不支持特殊字符。

“包括过滤器”的以下示例仅匹配扩展名为 .txt 或 .doc 的文件或文档，忽略其他所有内容：

`*.txt, *.doc`

“包括过滤器”的以下示例仅匹配扩展名为单个字符的文件或文档。此示例会匹配诸如 hello.1 和 hello.2 等文件，不会匹配 hello.doc 或 hello.html 文件：

`*.?`

您也可以使用过滤器来匹配文件共享的特定子目录。例如，要仅匹配名为 documentation 和 specs 两个子目录中包括的文件，请输入以下包括过滤器：

`*/documentation/*, */specs/*`

“SQL 数据库”一节中包括了 SQL 数据库扫描的语法和示例。

请参见第 1004 页的“[配置并运行 SQL 数据库扫描](#)”。

SharePoint 扫描的语法和示例在 SharePoint 部分中进行了介绍。

请参见第 1015 页的“[配置和运行 SharePoint 服务器扫描](#)”。

Endpoint Discover 扫描的语法和示例在“端点”部分中进行了介绍。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

按项目大小过滤发现目标

使用大小过滤器从基于项目大小的匹配进程中排除项目。

大小过滤器仅可用于文件共享中的文件、端点文件、Lotus Notes 文档、SharePoint 项目及 Exchange 项目。

您可以为此目标配置其他选项。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

根据项目大小排除项目

- 1 在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击要根据项目大小过滤的扫描的名称。
- 3 单击“扫描的内容”选项卡。
- 4 在项目大小过滤器下输入可选值。

Symantec Data Loss Prevention 仅包括与您所指定的大小过滤器匹配的项目。如果将此字段留空，Symantec Data Loss Prevention 将对所有大小的项目执行匹配。

请注意，如果提供值，会使用 AND 将所有过滤器组合在一起。添加或修改扫描过滤器时，请考虑所有的过滤器值（例如包括、排除和日期）。请避免不慎在扫描中包括所有项目或排除所有项目。

- 5 要排除小于特定大小的项目，请在“忽略小于以下大小的文件”旁的字段中输入数字。然后从其旁边的下拉列表中选择适合的文件大小单位（字节、KB 或 MB）。
- 6 要排除大于特定大小的项目，请在“忽略大于以下大小的文件”旁的字段中输入数字。然后从其旁边的下拉列表中选择适合的文件大小单位（字节、KB 或 MB）。
- 7 单击“保存”将所有更新保存到此目标。

根据上次访问或修改日期过滤发现目标

指定日期过滤器可根据项目的日期从匹配的进程中排除项目。仅会包括与所指定的日期过滤器匹配的项目。

“日期过滤器”仅可用于文件共享中的文件、端点文件及 Lotus Notes 文档。

增量扫描和差异扫描可用于某些 Network Discover 目标类型。

请参见第 957 页的“[使用增量扫描来扫描新的或修改过的项](#)”。

请参见第 958 页的“[使用差异扫描来扫描新的或修改过的项](#)”。

您可以为此目标配置其他选项。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

请注意，如果提供值，会使用 AND 将所有过滤器组合在一起。添加或修改扫描过滤器时，请考虑所有的过滤器值（例如包括、排除和大小）。请避免不慎在扫描中包括所有项目或排除所有项目。

根据上次访问或修改日期排除项目

- 1 在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击“扫描的内容”选项卡。
- 3 在“文件日期过滤器”下输入可选值。
- 4 选择“仅扫描上次完整扫描后添加或修改的文件”进行差异扫描。

请参见第 958 页的“[使用差异扫描来扫描新的或修改过的项](#)”。

此选项仅扫描上次完整扫描后添加或修改（以两者中时间较晚者为准）的项目。

如果不选择此项，则 Symantec Data Loss Prevention 不会使用日期过滤器。它会对指定目标中所有日期的项目执行匹配。

第一次扫描必须是完整扫描。如果您在 Symantec Data Loss Prevention 第一次扫描此目标之前选择此选项，则会进行完整扫描。

当选择此选项时，还可以选择“下一次扫描执行完整扫描”选项。如果选择此选项，将禁用“仅扫描添加或修改的文件”和“仅扫描上次访问的文件”的日期过滤器。下一次扫描将是完整扫描（如果之前未完成完整扫描）。后续的扫描仅针对完整扫描后添加或修改的项目。Symantec Data Loss Prevention 执行完整扫描后，会自动取消选中此复选框。

此选项对文件系统（文件共享）目标不可用。请改用增量扫描。

请参见第 956 页的“[关于增量扫描](#)”。

请参见第 955 页的“[关于增量扫描和差异扫描之间的区别](#)”。

5 选择“仅扫描添加或修改的文件”可以根据添加或修改的日期来包括文件。

Symantec Data Loss Prevention 仅扫描在指定的“晚于”日期之后、指定的“早于”日期之前或指定的日期之间的项目。

请注意，如果“晚于”日期晚于“早于”日期，则不会扫描任何项目。如果“早于”日期与“晚于”日期相同，也不会扫描任何项目。不会扫描任何项目的原因是“早于”参数的假设时间为凌晨零时，而“晚于”为午夜 24 时。

如果选择此选项，还可以选择以下选项：

■ 晚于

要包括于特定日期之后创建或修改（两者中时间较新的）的项目，请键入日期。您也可以单击日期工具并选择日期。

■ 早于

要包括于特定日期之前创建或修改（两者中时间较早的）的项目，请键入日期。您也可以单击日期工具并选择日期。

6 选择“仅扫描上次访问的文件”可以根据上次访问的日期来包括文件。

Symantec Data Loss Prevention 仅扫描在指定的“晚于”日期之后、指定的“早于”日期之前或指定的日期之间的项目。

仅 CIFS 共享的 Windows Network Discover Server 扫描支持“仅扫描上次访问的文件”功能。

请注意，如果“晚于”日期晚于“早于”日期，则不会扫描任何项目。如果“早于”日期与“晚于”日期相同，也不会扫描任何项目。不会扫描任何项目的原因是“早于”参数的假设时间为凌晨零时，而“晚于”为午夜 24 时。

如果选择此选项，还可以选择以下选项：

■ 晚于

要包括于特定日期之后访问的项目，请输入日期。您也可以单击日期工具并选择日期。

■ 早于

要包括于特定日期之前访问的项目，请输入日期。您也可以单击日期工具并选择日期。

注意：默认装载进程使用 CIFS 客户端。如果默认装载不能工作，则通过在属性文件 `Crawler.properties` 中设置 `filesystemcrawler.use.jcifs=true`，装载任务可使用基于 Java 的 CIFS 客户端。

7 单击“保存”将所有更新保存到此目标。

使用 Network Discover 扫描限制优化资源

对于以下扫描目标，您可以在目标的“高级”选项卡上设置限制选项：

- 文件共享
- 端点文件
- Lotus Notes 文档
- SQL 数据库

对于扫描程序，必须通过编辑扫描程序计算机上的配置文件来设置限制。

注意：使用项目限制会显著降低扫描速率。扫描速率预计会降为原始扫描速率的一半或更低。

您还可以设置其他选项来优化扫描。

请参见第 953 页的“[关于 Network Discover 扫描优化](#)”。

为文件共享、Lotus Notes 文档或 SQL 数据库设置扫描限制

- 1 在EnforceServer管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击扫描目标名称以打开要编辑的目标。
- 3 在“高级”选项卡上，设置限制选项。
- 4 输入每分钟要处理的最大文件数或行数，或每分钟要处理的最大字节数。

如果同时选择这两个选项，则扫描速率会低于这两个选项。

文件限制

指定每分钟要处理的文件、文档（在Lotus Notes 中）或行（在SQL数据库中）的上限。

字节限制

指定每分钟要处理的字节的上限。

从下拉列表中指定测量单位。选项包括：字节、KB（千字节）或 MB（兆字节）。

为扫描程序设置项目限制

- 1 在安装了扫描程序的计算机上，找到扫描程序配置文件(`scanner-type.cfg`)。
 - 2 在扫描程序配置文件中，修改 `ImportPoliteness` 参数和 `BatchSize` 参数。

设置项目限制时，扫描程序会将 `BatchSize` 个项目提取至本地存储，然后在处理每个所提取的项目之间等待 `ImportPoliteness` 毫秒。

任何扫描程序都不支持字节限制。
 - 3 要从存储库实现项目限制，请将 `BatchSize` 参数设为较小的值。从而 `ImportPoliteness` 值的作用会更大。设置 `BatchSize=1` 时，在提取文档方面可实现最佳限制效果。
- 例如，如果您设置 `BatchSize=25` 和 `ImportPoliteness=5000`（5 秒），则扫描程序将下载 25 个文档，在处理每个文档之间暂停 5 秒的时间。

创建未受保护的敏感数据的位置的库存

要审核目标是否含有机密数据，而不扫描整个目标，请使用“库存模式”进行扫描。如果每个位置上的事件存在的重要性大于事件数目的重要性，则库存模式就很有用。

以库存模式执行扫描也能够改进扫描大量计算机或大量数据时的性能。设置事件阈值可通过跳至下一个要扫描的内容根目录（而非扫描所有内容）来提升扫描性能。内容根目录是在“扫描的内容”选项卡上指定的一行（文件共享、Domino 服务器或 SQL 数据库）。

您可以为扫描项目设置事件数目上限。扫描项目可以是文件共享或物理计算机。

在达到事件阈值之后，将停止对此内容根目录的扫描，并继续扫描下一个内容根目录。由于进程不是同步的，因此所创建的事件可能会略高于事件阈值所指定的数目。

下列基于服务器的扫描目标都支持存库存式扫描：

- 文件共享

如果是文件共享，则您也可以指定是否要按照内容根目录或按照计算机来计算事件。内容根目录是在“扫描的内容”选项卡中指定的列表上的一个文件共享。在“事件计数基于”字段中指定此项。

- Lotus Notes 数据库

根据内容根目录（“扫描的内容”选项卡上列表中的 Domino 服务器）对事件阈值进行计数。

- SQL 数据库

根据内容根目录（“扫描的内容”选项卡上列表中的 SQL 数据库）对事件阈值进行计数。

可以利用事件阈值参数来设置库存模式。可以在新建目标或编辑现有目标时设置库存模式。

找出敏感数据后，可以设置其他选项以运行目标为这些位置的完全扫描。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

创建敏感数据的库存

- 1 在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击扫描目标名称以打开要编辑的目标。
- 3 在“高级”选项卡上，可以使用“库存模式”扫描来优化扫描。
- 4 设置“事件阈值”。

输入在转至下一个内容根目录（在“扫描的内容”选项卡上指定）之前要生成事件的数目。

- 5 设置“事件计数基于”选项。

对于文件共享夹，您也可选择以下方式为事件计数：

- 内容根目录（默认）

内容根目录是“扫描的内容”选项卡上列表中的一个文件共享。
达到事件阈值之后，扫描将转至下一个文件共享。

- 计算机

选择此选项可以通过计算机（从计算机上指定的共享）进行计数。
达到事件阈值时，扫描将转至列表上的下一个内容根目录进行扫描。如果该内容根目录与上一个项目位于同一台物理计算机，则会忽略该内容根目录。

请注意，对于要跳过的内容根目录，计算机名称必须完全相同。例如，
\\localhost\myfiles 和 \\127.0.0.1\myfiles 会视为不同的计算机，即使它们的逻辑名称相同。

管理 Network Discover 目标扫描

本章节包括下列主题：

- 管理 Network Discover 目标扫描
- 管理 Network Discover 目标
- 管理 Network Discover 扫描历史记录
- 管理 Network Discover 服务器
- 关于 Network Discover 扫描优化
- 关于增量扫描和差异扫描之间的区别
- 关于增量扫描
- 使用增量扫描来扫描新的或修改过的项
- 关于管理增量扫描
- 使用差异扫描来扫描新的或修改过的项
- 配置 Network Discover 目标的并行扫描

管理 Network Discover 目标扫描

Network Discover 目标扫描的管理任务分为四大类别：管理 Network Discover 目标、管理 Network Discover 扫描历史记录、管理 Network Discover 服务器以及优化扫描。

请参见第 944 页的“[管理 Network Discover 目标](#)”。

请参见第 946 页的“[管理 Network Discover 扫描历史记录](#)”。

请参见第 952 页的“[管理 Network Discover 服务器](#)”。

请参见第 953 页的“[关于 Network Discover 扫描优化](#)”。

管理 Network Discover 目标

若要管理发现扫描目标，您可以运行以下操作：

- 启动、停止和暂停目标扫描。
- 在目标扫描运行时监视状态。
- 选择要查看其详细信息的目标。
- 编辑或删除目标。
- 管理多个目标。
- 排序并过滤目标，以简化目标管理。
- 指定要显示的目标数量。

请参见第 944 页的“[关于 Network Discover 扫描目标列表](#)”。

请参见第 945 页的“[使用 Network Discover 扫描目标](#)”。

请参见第 946 页的“[删除 Network Discover 扫描目标](#)”。

关于 Network Discover 扫描目标列表

您可以通过“发现目标”屏幕，管理 Network Discover 的扫描目标。目标列表上方的工具栏，包括创建新的扫描目标的下拉菜单、用于启动、停止和暂停扫描的按钮；以及过滤列表中项目的图标。您可以将操作应用到多个目标。

您可以单击大多数的列标题，以便按该列的数据将列表排序。

您可以使用“操作”列上方的下拉菜单，选择要在“发现目标”列表中显示的条目数。

请参见第 943 页的“[管理 Network Discover 目标扫描](#)”。

[表 57-1](#) 列出了每个目标扫描的各列。

表 57-1 **发现目标**

目标信息	说明
目标名称	目标扫描的名称。
目标类型	扫描的目标类型（例如，文件系统或 SharePoint）。
策略组	列出这个目标分配给哪些策略组。

目标信息	说明
服务器	列出分配给这个目标的服务器。
上次修改时间	指定上次修改目标的日期和时间。
扫描状态	显示扫描的状态。单击此列中的链接，以查看此目标的已过滤扫描历史记录页面。
下次扫描	显示这个目标的下次调度扫描（如果适用）。
操作	单击“编辑目标”图标以编辑目标定义。 单击“删除”图标以删除目标。

过滤“发现目标”列表

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击“过滤器”。在“发现目标”列表的每个列标题中，会出现文本字段或下拉列表。
- 3 将下面其中一个过滤器应用至列表：
 - **目标名称：**在文本字段中，输入目标名称。
 - **目标类型：**从下拉列表中选择目标类型。
 - **策略组：**在文本字段中，键入策略组的名称。
 - **服务器：**在文本字段中，键入服务器的名称。
 - **上次修改时间：**从下拉列表中选择范围。
 - **扫描状态：**从下拉列表中选择扫描状态。
 - **上次扫描时间：**从下拉列表中选择范围。
- 4 若要清除过滤器，请清除相关文本字段或下拉列表中的值，或者单击“过滤器”。

使用 Network Discover 扫描目标

您可以使用扫描目标执行以下任务：

启动、停止和暂停 Network Discover 扫描

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 选择您要启动、停止或暂停的扫描。
- 3 单击目标列表工具栏上的“启动”、“停止”或“暂停”图标。

编辑 Network Discover 扫描目标

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 针对要编辑的目标，单击“编辑目标”按钮。
- 3 在“编辑目标”页上进行所需的更改。

请参见第 929 页的[“Network Discover 扫描目标配置选项”](#)。

删除 Network Discover 扫描目标

在删除扫描目标之前，请检查正在运行或排入队列的扫描。

请参见第 943 页的[“管理 Network Discover 目标扫描”](#)。

若要删除扫描目标，请执行以下操作：

- 从 Enforce Server 中删除扫描目标。
- 从安装扫描程序所在的计算机卸载该扫描程序（如果适用）。

删除扫描目标

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 针对您要删除的目标，单击“删除”图标。

删除 Windows 系统上的扫描程序

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 针对您要删除的目标，单击“删除”图标。
- 3 在具有扫描程序的系统上，以管理员身份登录并单击 Windows “开始”图标。
- 4 选择“程序”>“Vontu 扫描程序”>“*scanner_name*”>“卸载程序”。

删除 UNIX 系统上的扫描程序

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 针对您要删除的目标，单击“删除”图标。
- 3 在具有扫描程序的系统上，以根用户身份登录，并键入下列文本：

```
# /opt/scanner/uninstall
```

管理 Network Discover 扫描历史记录

若要管理 Network Discover 扫描历史记录，您可以运行以下操作：

- 查看有关运行中或已完成扫描的统计信息。
- 以逗号分隔的值 (CSV) 格式下载扫描历史记录信息。
- 查看扫描详细信息。
- 查看事件报告。
- 删除扫描历史记录。
- 管理多个扫描历史记录。
- 排序并过滤扫描历史记录以简化管理。
- 指定要显示的扫描历史记录数量。

请参见第 947 页的“[关于 Network Discover 扫描历史记录](#)”。

请参见第 949 页的“[使用 Network Discover 扫描历史记录](#)”。

请参见第 949 页的“[删除 Network Discover 扫描](#)”。

请参见第 950 页的“[关于 Network Discover 扫描详细信息](#)”。

请参见第 952 页的“[使用 Network Discover 扫描详细信息](#)”。

关于 Network Discover 扫描历史记录

您可以在“扫描历史记录”屏幕上管理您的 Network Discover 扫描历史记录。若要查看所有发现目标的扫描历史记录列表，请在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“扫描历史记录”。

您可以单击任意列标头，依照该列中的数据，以字母数字顺序对列表进行排序。

您可以使用“操作”列上方的下拉菜单，选择要在“发现目标”列表中显示的条目数。

如需扫描的其他详细信息，请单击“扫描状态”列中的链接，以显示“扫描详细信息”屏幕。

请参见第 950 页的“[关于 Network Discover 扫描详细信息](#)”。

请参见第 943 页的“[管理 Network Discover 目标扫描](#)”。

[表 57-2](#) 列出了为每次扫描所显示的字段。

表 57-2 **扫描历史记录**

扫描历史记录	说明
目标名称	目标扫描的名称。

扫描历史记录	说明
目标类型	扫描的目标类型（例如，文件系统或 SharePoint）。
已启动扫描	扫描开始的日期与时间。
扫描状态	扫描的当前状态：“运行中”、“已暂停”、“已完成”、“已停止”。
扫描类型	扫描类型：“增量”、“差异”或“完整”。
事件计数	在扫描中找到的事件的数目。
运行时间	扫描经过的时间（采用 dd:hh:mm:ss 格式）。
已扫描的字节数/已扫描的项目数	目标中已扫描的字节数，以及已扫描的项目数。
错误数	扫描期间的错误数。
操作	<p>单击“查看事件”图标来查看扫描的事件摘要报告。 请参见第 962 页的“关于 Network Discover 的事件报告”。 请参见第 759 页的“发现事件报告”。 单击“删除”图标可删除扫描。删除基本扫描前，请确定先删除差异扫描。 请参见第 949 页的“删除 Network Discover 扫描”。</p>

过滤“扫描历史记录”列表

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“扫描历史记录”。
- 2 单击“过滤器”。文字字段或下拉列表便会在“扫描历史记录”列表的列标题中。
- 3 将下面其中一个过滤器应用至列表：
 - **目标名称：**在文本字段中，输入目标名称。
 - **目标类型：**从下拉列表中选择目标类型。
 - **已启动扫描：**从下拉列表中选择一个范围。
 - **扫描状态：**从下拉列表中选择扫描状态。

■ 扫描类型：从下拉列表中选择扫描类型。

- 4 若要清除过滤器，请清除相关文本字段或下拉列表中的值，或者单击“过滤器”。

使用 Network Discover 扫描历史记录

您可以使用扫描历史记录执行以下任务：

导出 Network Discover 扫描历史记录

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“扫描历史记录”。
- 2 选择您要导出的扫描。
- 3 单击“导出”。此时会出现“文件下载”对话框。
- 4 单击“打开”查看已导出的数据，或者单击“保存”保存文件。
- 5 若要取消导出操作，请单击“取消”。

查看特定扫描的事件

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“扫描历史记录”。
- 2 针对要查看的扫描，单击“查看事件”图标。此时会出现“发现事件”屏幕。

删除 Network Discover 扫描

您可以从扫描历史记录删除特定扫描。

删除扫描

- 1 在Enforce Server管理控制台中，转至“管理”>“发现扫描”>“扫描历史记录”。
- 2 在删除该目标的基本完整扫描之前，请先删除所有差异扫描。
不必对增量扫描执行此步骤。
- 3 选择要删除的扫描，然后单击“操作”列中的删除图标。
若要删除多个扫描，请标记您要删除扫描的复选框，然后单击工具栏上的“删除”。

关于 Network Discover 扫描详细信息

您可以查看关于每个 &pn.NetworkDiscover 扫描的详细信息，包含常规扫描信息、扫描统计数据、最近的错误以及扫描活动。您也可以针对扫描统计数据、最近的错误以及扫描活动，下载 CSV 格式的报告。

若要查看扫描详细信息，请转至“管理”>“发现扫描”>“扫描历史记录”。选择扫描，然后单击“状态”列中的链接。

请参见第 943 页的[“管理 Network Discover 目标扫描”](#)。

[表 57-3](#) 显示了“常规”部分，其中提供关于扫描的信息。

表 57-3 常规扫描详细信息

常规扫描详细信息	说明
目标类型	所扫描的目标的类型及图标。
目标名称	目标的名称。
状态	扫描的状态。 如果正在运行扫描，则会显示运行当前扫描的 Network Discover Server 的名称。
扫描类型	扫描类型，例如增量扫描或完整扫描。
开始时间	扫描开始的日期与时间。
结束时间	扫描完成的日期与时间。

[表 57-4](#) 显示了“扫描统计信息”部分，其中提供关于扫描的详细信息。

表 57-4 扫描统计信息

扫描统计信息	说明
已处理	所扫描的项目数。如果扫描仍在运行，此字段会提供对扫描进度的对照基准测评。
运行时间 (dd:hh:mm:ss)	扫描完成所需的时间。如果仍在运行扫描，则显示已运行扫描的时间。总时间并不包括任何扫描暂停期间的时间。
已扫描的项目数	已扫描的项目数。
已扫描的字节数	已扫描的字节数。

扫描统计信息	说明
错误数	扫描期间发生的错误数。将在“最新扫描错误”部分中显示错误列表。
检测到的事件总数	当前扫描期间所检测到的事件的总数。
当前的事件总数	在当前扫描期间检测到的事件总数，少于任何已删除的事件。您可以单击此数目，查看此次扫描的事件列表。

“最新扫描错误”部分列出的是扫描期间发生的错误。

如果扫描中发生了许多错误，“扫描详细信息”屏幕并不会将它们全部显示出来。要查看扫描期间所出现错误的完整列表，请单击“[下载完整错误报告](#)”。

[表 57-5](#) 显示了“最新扫描错误”报告中的信息，其中提供关于每项错误的信息。

表 57-5 最新扫描错误

最新扫描错误详细信息	说明
日期	在扫描期间发现错误的日期与时间。
路径	扫描期间发现错误的文件的位置目录路径。
错误	错误消息。

“最新扫描活动”会显示扫描期间所发生的重大事件的最新日志条目。

如果在一次扫描中生成了许多活动消息，“扫描详细信息”屏幕并不会将它们全部显示出来。要查看扫描活动消息的完整列表，请单击“[下载完整活动报告](#)”。

[表 57-6](#) 显示了“最新扫描活动”报告，其中提供关于每项活动的信息。

表 57-6 最新扫描活动

最新扫描活动详细信息	说明
日期/时间	所记录的事件的发生日期与时间。
级别	事件的严重性。
消息	所记录的关于事件的消息。

[表 57-7](#) 说明了“扫描详细信息”屏幕上的选项。

表 57-7 “扫描详细信息”屏幕上的选项

扫描详细信息的选项	说明
下载完整统计信息报告	下载 CSV 格式的报告以及所有扫描统计数据。
下载完整错误报告	下载 CSV 格式的报告以及所有扫描错误。
下载完整活动报告	下载 CSV 格式的报告以及所有扫描活动。

使用 Network Discover 扫描详细信息

您可以使用扫描详细信息执行以下任务：

查看扫描详细信息

- 1 在 Enforce Server 管理控制台中，单击“管理”>“发现扫描”>“扫描历史记录”
- 2 在“扫描历史记录”页上，针对要查看其详细信息的扫描，单击“扫描状态”列中的链接。

将扫描详细信息导出到 CSV 文件

- 1 在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“扫描历史记录”
- 2 在“扫描历史记录”页上，针对要查看其详细信息的扫描，单击“扫描状态”列中的链接。
- 3 在“扫描详细信息”页上，单击以下按钮之一：
 - 下载完整统计信息报告
 - 下载完整错误报告
 - 下载完整活动报告

管理 Network Discover 服务器

您可以查看每台发现服务器的 Network Discover 扫描状态和扫描详细信息。

请参见第 953 页的“[查看 Network Discover 服务器状态](#)”。

查看 Network Discover 服务器状态

“发现服务器”屏幕列出了在您网络上配置的 Network Discover 或 Endpoint Discover 的检测服务器。此屏幕显示了有关每个检测服务器上的扫描的详细信息。

若要查看“发现服务器”，请在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“发现服务器”。

请参见第 943 页的[“管理 Network Discover 目标扫描”](#)。

[表 57-8](#) 列出了每个服务器的信息。

表 57-8 发现服务器

服务器信息	说明
服务器名称	服务器的名称。括号内是检测服务器的类型，可以是“发现”或“端点”。
运行中扫描	当前正在此服务器上运行的扫描列表。
已排队的扫描	要在此服务器上运行的已排队扫描列表。
调度扫描	调度为以后在此服务器上运行的扫描列表。
暂停的扫描	此服务器上暂停的扫描列表。

从 Network Discover 服务器查看扫描详细信息

- 1 在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“发现服务器”
- 2 在“发现服务器”页面上，单击您要查看其详细信息的扫描的名称。

请参见第 950 页的[“关于 Network Discover 扫描详细信息”](#)。

关于 Network Discover 扫描优化

根据扫描的类型、要扫描数据的数量和格式，以及硬件和网络速度，Network Discover 目标扫描可能需要数小时或数天才能完成。要优化对大量信息的扫描，以获得较高质量，请遵循本部分中的建议。

要帮助优化您的 Network Discover 扫描，请考虑使用下面的一些方法：

- 首先，仅扫描最常访问和使用最广泛的文件共享或存储库（例如访客或公共访问）。从较小的文件共享或存储库开始，在增加扫描的信息量之前确认准确性。通过初始扫描达到满意的性能之后，针对处理您的机密数据的业务单位增加扫描。

- 在网络上安装多个 Network Discover Server。
- 将大规模的扫描拆分成数次较小的扫描。创建独立的扫描目标，并使用过滤器来拆分要扫描的集合。

您可以使用包括、排除、大小与日期等过滤器来拆分扫描。
请参见第 935 页的“[设置发现过滤器以在扫描中包括或排除项目](#)”。
请参见第 937 页的“[按项目大小过滤发现目标](#)”。
请参见第 938 页的“[根据上次访问或修改日期过滤发现目标](#)”。
- 先扫描非二进制文件。二进制文件包含策略违规的可能性较小。

例如，您可以对以下列表设置“排除过滤器”来扫描非二进制文件：

```
*.exe, *.lib, *.bin, *.dll, *.cab, *.dat  
*.au, *.avi, *.mid, *.mov, *.mp, *.mp3, *.mp4, *.mpeg, *.wav, *.wma
```

要扫描其余的文件，则将这项过滤器用作其他扫描目标的“包括过滤器”。
请参见第 935 页的“[设置发现过滤器以在扫描中包括或排除项目](#)”。
- 对于文件系统目标，可以配置增量扫描以只检查尚未扫描过的那些文件。

请参见第 957 页的“[使用增量扫描来扫描新的或修改过的项](#)”。
请参见第 955 页的“[关于增量扫描和差异扫描之间的区别](#)”。
- 在一个扫描目标中扫描新建或最近修改的项目，而在另一个扫描目标中扫描较旧的项目。

使用数据过滤器，按日期值、按早于某时点的文件或晚于某时点的文件拆分扫描。
请参见第 938 页的“[根据上次访问或修改日期过滤发现目标](#)”。
- 在初始扫描之后运行差异扫描，以便只检查自从上次完整扫描之后添加或修改的项目。

请参见第 958 页的“[使用差异扫描来扫描新的或修改过的项](#)”。
请参见第 955 页的“[关于增量扫描和差异扫描之间的区别](#)”。
- 在一个扫描目标中扫描较小的文件，而在另一个目标中则扫描较大的文件。扫描许多小文件会比扫描少量大文件需要更多的开销。

使用大小过滤器来按大小拆分扫描。
请参见第 937 页的“[按项目大小过滤发现目标](#)”。
- 在独立的扫描目标中扫描压缩文件。

可使用“包括过滤器”来扫描压缩文件。例如，使用以下列表：

```
*.zip, *.gzip
```

要扫描其余的文件，则将这项过滤器用作其他扫描目标的“排除过滤器”。
请参见第 935 页的“[设置发现过滤器以在扫描中包括或排除项目](#)”。

- 在独立的扫描目标中扫描数据库或电子表格文件。

使用 SQL 数据库目标来扫描数据库文件。

请参见第 1004 页的“[配置并运行 SQL 数据库扫描](#)”。

使用“包括过滤器”来扫描电子表格文件：

`*.xls`

设置独立的扫描目标，并使用“排除过滤器”来扫描剩下的所有文件。

请参见第 935 页的“[设置发现过滤器以在扫描中包括或排除项目](#)”。

- 排除应用程序内部文件夹。例如，在 DFS 共享扫描中，排除内部 `DfsrPrivate` 文件夹。在 NetApp 文件管理器上的共享扫描中，排除 `.snapshot` 文件夹。

请参见第 987 页的“[排除内部 DFS 文件夹](#)”。

请参见第 988 页的“[配置与运行文件系统的扫描](#)”。

- 使用“库存模式”扫描，以便在达到某个事件阈值后移到下一个扫描项目。“库存模式”扫描可审核存储机密数据的位置，但不会运行完全扫描。

请参见第 941 页的“[创建未受保护的敏感数据的位置的库存](#)”。

- 尽可能分配多的硬件资源供扫描使用。例如，您可以挂起或退出在服务器上运行的任何其他程序。

- 使用“暂停扫描”以自动在工作时间挂起扫描。

- 运行并行扫描。

请参见第 958 页的“[配置 Network Discover 目标的并行扫描](#)”。

- 使用限制功能来减少网络负载。

请参见第 940 页的“[使用 Network Discover 扫描限制优化资源](#)”。

- 更新服务器硬件。

您可以使用最多 12 GB 的内存、四核心 CPU、极快速的硬盘，以及网卡来处理任何硬件上的瓶颈问题。

关于增量扫描和差异扫描之间的区别

通过增量扫描和差异扫描可以只扫描新增或修改的项，从而优化扫描性能。增量扫描可从上次停止扫描的任何点开始继续扫描，而不管第一次扫描是否为完整扫描。差异扫描只扫描上次完整扫描后添加或修改的项：必须对您的扫描目标运行至少一次完整扫描，才能使用差异扫描。

请参见第 956 页的“[关于增量扫描](#)”。

请参见第 957 页的“[使用增量扫描来扫描新的或修改过的项](#)”。

请参见第 958 页的“[使用差异扫描来扫描新的或修改过的项](#)”。

表 57-9 对增量扫描与差异扫描进行了比较。

表 57-9 增量扫描和差异扫描之间的区别

增量扫描	差异扫描
<p>以下目标支持增量扫描：</p> <ul style="list-style-type: none"> ■ “服务器” > “文件系统” ■ “服务器” > SharePoint 	<p>以下目标支持差异扫描：</p> <ul style="list-style-type: none"> ■ “服务器” > Lotus Notes ■ “服务器” > Exchange ■ “端点” > “文件系统”
<p>部分扫描会保留已扫描项目的信息。</p> <p>如果文件、共享或其他项目由于无法访问而没有被扫描，则接下来的增量扫描会自动扫描遗漏的项目。</p>	<p>差异扫描从发现目标的完整扫描开始。此完整扫描称为基本扫描。</p> <p>部分扫描不能用作基本扫描。</p>
<p>后续扫描将扫描之前未扫描的所有项目，包括新项目或修改的项目。</p>	<p>后续扫描将扫描自最近一次完整（基本）扫描完成日期以来添加或修改的所有项目。</p>
<p>增量扫描索引会一直跟踪已经扫描的项目。</p>	<p>根据基本扫描的日期，最近一次完成的基本扫描可充当要扫描项目的参照。</p>

关于增量扫描

通过增量扫描可以只扫描新增或修改的项，从而优化扫描性能。增量扫描可从上次停止扫描的任何点开始继续扫描，而不管第一次扫描是否为完整扫描。

请参见第 953 页的“[关于 Network Discover 扫描优化](#)”。

只有某些目标类型支持增量扫描。

请参见第 955 页的“[关于增量扫描和差异扫描之间的区别](#)”。

增量扫描会保留已扫描项目的信息。

例如，由于某些文件已锁定或正在使用，则扫描过程会跳过这些文件。可能会因为无法访问数据而不能完成扫描，例如，在服务器或设备脱机时。会在此目标的后续扫描中扫描这些遗漏的文件。

增量扫描索引会一直跟踪以前扫描过的项目。此索引会在多个发现服务器之间进行同步。

有关调整增量扫描索引要求的信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。

使用增量扫描来扫描新的或修改过的项

通过增量扫描可以从上次未扫描的项目开始继续 Network Discover 扫描。增量扫描仅扫描以前未扫描的项目。

请参见第 955 页的“[关于增量扫描和差异扫描之间的区别](#)”。

设置增量扫描

- 1 转至“管理”>“发现扫描”>“发现目标”。
- 2 单击下拉菜单“新建目标”，然后选择“文件系统”或 SharePoint 目标类型或选择列表中的一个文件系统扫描目标或 SharePoint 扫描目标进行编辑。
- 3 单击“常规”选项卡。
- 4 在“扫描类型”下，选择“仅扫描新项目或修改的项目(增量扫描)”。此选项为新目标的默认选项。

如果更改了现有扫描的策略或其他定义，您可能希望将下一次扫描设置为完整扫描，以确保策略的完全覆盖。选择下列选项：

“下一次扫描所有项目。后续扫描将为增量扫描。”

如果想要始终扫描此目标中的所有项目，请选择下列选项：

始终扫描所有项目(完整扫描)

- 5 完成设置或修改发现目标的其他步骤并运行扫描。

请参见第 930 页的“[为 Network Discover 目标配置必填字段](#)”。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

请参见第 985 页的“[设置文件系统扫描](#)”。

- 6 要管理增量扫描并诊断问题，请参考以下主题：

请参见第 957 页的“[关于管理增量扫描](#)”。

关于管理增量扫描

运行增量扫描时，请注意下列事项：

- 如果您的安装有多个发现服务器，则增量扫描索引将自动与该目标的所有其他发现服务器同步。
- 当您将增量扫描设置从“仅扫描新项目或修改的项目(增量扫描)”更改为“下一次扫描所有项目。后续扫描将为增量扫描”，在开始扫描之前清除该目标的增量扫描索引。后续扫描为增量扫描。
- 要扫描所有项目，请为发现目标设置“始终扫描所有项目(完整扫描)”。

- 如果选择了“**始终扫描所有项目(完整扫描)**”设置，则在开始扫描之前清除该目标的任何以前索引条目。不会在扫描期间重新填充索引。
如果要扫描所有项目，然后继续进行增量扫描，请选择“**下一次扫描所有项目。后续扫描将为增量扫描**”选项。
- 删除发现目标时，不会自动删除增量扫描索引。

使用差异扫描来扫描新的或修改过的项

为节省资源，差异扫描仅扫描上次完整扫描之后添加或修改过的项。

有关在版本升级过程中目标（配置为进行差异扫描）如何升级的信息，请参见《Symantec Data Loss Prevention 升级指南》。

请参见第 955 页的“[关于增量扫描和差异扫描之间的区别](#)”。

设置差异扫描

- 1 转至“管理”>“发现扫描”>“发现目标”。
- 2 单击下拉式“新建目标”，然后选择目标类型或者在列表中选择其中一个扫描目标以进行编辑。
- 3 单击“扫描的内容”选项卡。
- 4 选择差异扫描的日期选项。
请参见第 938 页的“[根据上次访问或修改日期过滤发现目标](#)”。
- 5 运行完整扫描。初始的扫描必须是完整扫描。
- 6 在初始扫描完成之后，下一次的扫描就会只扫描自从上次完整扫描之后添加或修改的项目。

配置 Network Discover 目标的并行扫描

您可以在同一 Network Discover Server 上，对不同目标同时运行多个扫描。

支持并行扫描服务器与扫描程序目标类型。不支持并行扫描端点文件系统。不支持从同一 Network Discover Server 并行扫描其中包含不同凭据的相同 CIFS 服务器或共享。

您可以控制（暂停、继续或停止）扫描，而不会影响 Network Discover Server 上的其他扫描。将会分别维护和报告每个扫描的状态。

当扫描开始时，如果选择了多个 Network Discover Server，则会针对此扫描选择其中之一。会将扫描分配为在运行最少扫描任务的服务器上运行。服务器是从目标中指定的服务器组选择的。

扫描开始之后，就会持续在同一台服务器上运行，直到扫描完成、中止或暂停为止。继续运行扫描时，可能会分配到不同的服务器上运行。

不支持自动负载平衡。如果 Network Discover Server 执行完所有的扫描，则其他服务器的扫描也不会迁移到无负载的服务器。不过，暂停并重新启动扫描即可手动迁移扫描。

要在同一 Network Discover Server 上运行多个扫描程序目标，则必须为每个扫描程序配置不同端口。新扫描程序的默认端口是尚未由任何扫描目标使用的值。

请参见第 1042 页的“[排除扫描程序故障](#)”。

配置并行扫描

- 1 在 Enforce Server 管理控制台中，转至“系统”>“服务器”>“概述”。
- 2 选择要配置的 Network Discover Server，然后单击服务器名称。
- 3 单击顶部的“配置”选项。
- 4 接着选择“发现”选项卡。
- 5 设置要在该 Network Discover Server 上运行的最大并行扫描数。

“最大并行扫描数”的默认值为 1。可以随时增大最大计数。增大该值之后，就会启动可在 Network Discover Server 上运行的任何排队扫描。只有在 Network Discover Server 没有运行中的扫描时，才能减小该计数。减小该计数之前，请暂停或停止 Network Discover Server 上的所有扫描。

- 6 单击“保存”。
- 7 单击“完成”。
- 8 您可以查看每个 Network Discover Server 上正在运行、排入队列、调度或暂停的扫描。在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“发现服务器”。

请参见第 943 页的“[管理 Network Discover 目标扫描](#)”。

管理 Network Discover 事件报告

本章节包括下列主题：

- [关于 Network Discover 的报告](#)
- [关于 Network Discover 的事件报告](#)

关于 Network Discover 的报告

Symantec Data Loss Prevention 具有用于事件、Network Discover 目标、扫描详细信息与扫描历史记录的报告。

Network Discover 事件报告包含关于曝露的机密数据的详细信息。

请参见第 962 页的“[关于 Network Discover 的事件报告](#)”。

如需 Network Discover 目标与扫描历史记录的相关信息，请转至“管理”>“发现扫描”>“发现目标”，然后从列表中选择其中一个发现目标。如需

&pn.NetworkDiscover 扫描详细信息的相关信息，请转至“管理”>“发现扫描”>“扫描历史记录”，然后从列表中选择其中一个发现扫描。

请参见第 943 页的“[管理 Network Discover 目标扫描](#)”。

[表 45-1](#) 列出了 Network Discover 报告。

表 58-1 Network Discover 报告

报告	导航
Network Discover 目标	<p>此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“发现目标”上。</p> <p>请参见第 944 页的“关于 Network Discover 扫描目标列表”。</p>

报告	导航
扫描状态	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“发现服务器”上。 请参见第 953 页的 “查看 Network Discover 服务器状态” 。
扫描历史记录（单一目标）	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“发现目标”上。单击“扫描状态”列中的链接，以查看特定扫描目标的历史记录。 请参见第 947 页的 “关于 Network Discover 扫描历史记录” 。
扫描历史记录（所有目标）	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“扫描历史记录”上。 请参见第 947 页的 “关于 Network Discover 扫描历史记录” 。
扫描详细信息	此报告位于 Enforce Server 管理控制台“管理”菜单的“发现扫描”>“扫描历史记录”上。单击“扫描状态”列中的链接，以查看扫描详细信息。 请参见第 950 页的 “关于 Network Discover 扫描详细信息” 。

关于 Network Discover 的事件报告

使用事件报告可追踪 Network Discover 事件并对其作出响应。您可以保存、发送、导出或调度 Symantec Data Loss Prevention 报告。

请参见第 775 页的[“关于 Symantec Data Loss Prevention 报告”](#)。

在 Enforce Server 管理控制台中的“事件”菜单上，单击“发现”。此事件报告将显示所有发现目标的所有事件。您可以选择针对以下内容的标准报告：所有事件、新事件、目标摘要、按目标的策略、按目标的状态或有风险的前几个共享。

摘要和过滤器选项可以选择要显示的事件。

请参见第 786 页的[“关于自定义报告和控制板”](#)。

请参见第 807 页的[“关于报告的过滤器和摘要选项”](#)。

您可以使用过滤器和摘要组合创建自定义报告来确定要补救的事件。

例如，您可以创建下列报告：

■ 反映每个补救类别中的事件数量的摘要报告。

选择摘要“保护状态”。

■ 已通过复制或隔离补救的所有事件的报告。

选择值为“已复制文件”和“已隔离文件”的过滤器“保护状态”。

- 以前未出现过的 Network Discover 事件的报告（用于标识这些事件并通知数据所有者对它们进行补救）。
选择过滤器“出现过”。将值设置为“否”。
- 仍然存在的 Network Discover 事件的报告（用于了解要提报补救哪些事件）。
选择过滤器“出现过”。将值设置为“是”。
- 使用摘要过滤器（如自首次检测后的月数）的报告。
选择摘要“自首次检测后的月数”。

使用服务器 FlexResponse 插件补救事件

本章节包括下列主题：

- [关于服务器 FlexResponse 平台](#)
- [使用服务器 FlexResponse 自定义插件补救事件](#)
- [部署服务器 FlexResponse 插件](#)
- [查找事件进行手动补救](#)
- [使用服务器 FlexResponse 插件的操作手动补救事件](#)
- [验证事件响应操作的结果](#)
- [对服务器 FlexResponse 插件进行故障排除](#)
- [部署 Python Script Bridge 服务器 FlexResponse 插件](#)

关于服务器 FlexResponse 平台

服务器 FlexResponse 应用程序编程接口 (API) 为事件补救提供了一个灵活的平台。利用该平台，Symantec Data Loss Prevention 用户能够自动或手动调用自定义服务器 FlexResponse 操作来保护数据。Symantec 提供了一组插件，这些插件用于执行各种补救，例如隔离敏感数据、复制文件和应用数字版权保护或加密。

开发人员也可以使用此 API 和 Java 编程语言编写用于执行自定义事件补救的服务器 FlexResponse 插件。开发人员还可以编写 Python 脚本来执行补救。可通过安装一个称作 Python Script Bridge 的服务器 FlexResponse 插件来启用 Python 脚本编写。此插件可对 Java API 进行转换以便在 Python 脚本编写过程中使用，此插件的部署方式与其他的服务器 FlexResponse 插件相同。请参见第 976 页的“[部署 Python Script Bridge 服务器 FlexResponse 插件](#)”。

用户可以对识别的事件执行一系列 Network Protect 操作来辅助补救。补救操作由一个自定义程序来执行。使用服务器 FlexResponse API，您可以构建插件，用于实现在自动响应规则和智能响应规则中使用的事件响应。

以下是您可以通过开发服务器 FlexResponse 插件来实施的 Network Protect 操作的示例：

- 更改文件的访问控制列表 (ACL)。例如，您可以删除对选定文件的访客访问权限。
- 手动隔离文件。手动处理允许在实施补救前对事件进行验证。
- 手动从隔离中释放选定的文件。如果用户确认文件使用合法，您可以将文件移回其原始位置。
- 应用数字版权管理 (DRM)。例如，您可以对文档应用数字版权，这样外部单位对敏感材料的访问便会受到限制。这些数字版权可以包括“禁止转发”或“禁止打印”。
- 加密文件。
- 将文件迁移到 SharePoint。该自定义保护操作可以将文件从共享移动到 SharePoint 存储库，然后应用 DRM 和 ACL。
- 执行补救响应的工作流程和自动化。
- 使用 Symantec Workflow 业务流程自动化工作流程。

构建、部署和使用服务器 FlexResponse 插件时会涉及下列步骤：

- 使用 Java API 开发插件。此阶段涉及对插件和补救操作进行设计和代码编写。
请参见第 970 页的“[创建用于配置服务器 FlexResponse 插件的属性文件](#)”。
- 将插件添加到插件配置属性文件。
请参见第 968 页的“[将服务器 FlexResponse 插件添加到插件属性文件](#)”。
- 在 Enforce Server 上部署自定义插件。
请参见第 968 页的“[部署服务器 FlexResponse 插件](#)”。
- 加载插件（包括插件元数据）。
- 为事件的智能响应操作创建响应规则。
- 使用插件操作补救事件。
请参见第 973 页的“[使用服务器 FlexResponse 插件的操作手动补救事件](#)”。
- 验证服务器 FlexResponse 插件操作的结果。
请参见第 974 页的“[验证事件响应操作的结果](#)”。

注意：为 Symantec Data Loss Prevention 版本 10 创建的服务器 FlexResponse 插件与 Symantec Data Loss Prevention 版本 11 兼容。

以下各节说明如何部署和配置预制的 FlexResponse 插件，以及如何在 Symantec Data Loss Prevention 策略中使用自定义插件操作。可直接从 Symantec 获取某些服务器 FlexResponse 插件。还可以使用服务器 FlexResponse API 开发自己的自定义插件。关于如何使用 Java API 开发插件的信息，请参见《Symantec Data Loss Prevention 服务器 FlexResponse 平台开发人员指南》。关于如何使用 Python 开发插件的信息，请参见 *Python Script Bridge Server Plug-in Developers Guide*（《Python Script Bridge 服务器插件开发人员指南》），您在安装 Python Script Bridge 插件时可以获得此指南。

使用服务器 FlexResponse 自定义插件补救事件

您可以使用服务器 FlexResponse 插件操作自动或手动补救 Network Discover 事件。

要制定自定义补救操作，请参见 *Symantec Data Loss Prevention Server FlexResponse Platform Developers Guide*（《Symantec Data Loss Prevention 服务器 FlexResponse 平台开发人员指南》）。

要使用自定义服务器 FlexResponse 插件自动或手动补救事件，必须执行下列步骤：

表 59-1

步骤	操作	说明
1	将服务器 FlexResponse 插件部署到 Enforce Server 计算机。	必须先将每个服务器 FlexResponse 插件部署到 Enforce Server 计算机，然后才能在 Symantec Data Loss Prevention 策略中使用插件操作。 请参见第 968 页的“ 部署服务器 FlexResponse 插件 ”。
2	创建使用自定义服务器 FlexResponse 事件响应操作的响应规则。	请参见第 689 页的“ 配置服务器 FlexResponse 操作 ”。
3	(可选) 使用服务器 FlexResponse 插件来手动补救事件。	如果在智能响应规则中使用服务器 FlexResponse 插件操作，则必须手动查找事件并执行 FlexResponse 操作。 请参见第 973 页的“ 查找事件进行手动补救 ”。 请参见第 973 页的“ 使用服务器 FlexResponse 插件的操作手动补救事件 ”。 如果配置自动响应规则来执行服务器 FlexResponse 操作，则不需要此步骤。使用自动响应规则，创建触发自动响应规则的事件还会执行已配置的 FlexResponse 操作。
4	验证结果。	请参见第 974 页的“ 验证事件响应操作的结果 ”。

部署服务器 FlexResponse 插件

为服务器 FlexResponse API 启用插件。

部署服务器 FlexResponse 插件

- 1 将已完成的服务器 FlexResponse 插件 JAR 文件复制到插件目录：

DLP_home\Protect\plugins

- 2 配置有属性文件的插件。

请参见第 970 页的“[创建用于配置服务器 FlexResponse 插件的属性文件](#)”。

- 3 将每个插件的属性文件复制到放置 JAR 文件的目录中：

DLP_home\Protect\plugins

- 4 在 *DLP_home\Protect\config\Plugins.properties* 文件中，将插件添加到列表中，然后输入插件的属性。

请参见第 968 页的“[将服务器 FlexResponse 插件添加到插件属性文件](#)”。

- 5 确保 Symantec Data Loss Prevention protect 用户对插件 JAR 文件和插件属性文件都具有读取和执行访问权限。

- 6 要加载插件，请停止 Vontu Incident Persister 和 Vontu Manager 服务，然后重新启动这两个服务。

将服务器 FlexResponse 插件添加到插件属性文件

将服务器 FlexResponse 插件添加到 *Plugins.properties* 文件。并修改插件需要的所有参数。

将服务器 FlexResponse 插件添加到属性文件

1 编辑 `Plugins.properties` 文件。

所有插件的常规值都在此文件中，另外还包括所有已实施的插件的列表。

请参见第 969 页的[表 59-2](#)。

此文件位于以下目录中：

`DLP_home\Protect\config`

2 在文件中找到以下行，此行指定了要在加载时构建的插件的 JAR 文件：

```
# Incident Response Action configuration parameters.  
  
com.symantec.dlp.flexportresponse.Plugin.plugins =  
plugin1.jar,plugin2.jar
```

如有必要，删除此行开头的注释标记，并使用要部署的插件 JAR 文件名替换 `plugin1.jar,plugin2.jar`。请使用逗号分隔多个 JAR 文件。

3 编辑此文件中的任何附加参数。

[表 59-2](#) 介绍了 `Plugins.properties` 文件中的服务器 FlexResponse API 的附加属性。

4 停止 Vontu Incident Persister 和 Vontu Manager 服务，然后重新启动这两个服务。这样会加载新插件和此文件中的其他参数。

如果您稍后更改了 `Plugins.properties` 文件，则必须重新启动 Vontu Incident Persister 和 Vontu Manager 服务才能应用更改。

在 [表 59-2](#) 中，`plugin-id` 是插件在此属性文件内的唯一标识符，例如 `test1`。

表 59-2 Plugins.properties 文件中的参数

属性名称	说明
<code>protect.plugins.directory</code>	所有 Symantec Data Loss Prevention 插件的安装目录。

属性名称	说明
com.symantec.dlp.x.flexresponse.Plugin.plugins	<p>要在服务器 FlexResponse 插件容器中加载的 JAR 文件（或 JAR 标题）的逗号分隔列表。</p> <p>该列表中的每个插件都将对应 Enforce Server 管理控制台中的响应规则操作。</p> <p>在其中部署 JAR 文件的容器包括所有公共 JRE 类，这些类由随 Symantec Data Loss Prevention 安装的 JVM 提供。容器还包括本文档中介绍的所有 FlexResponse API 类（com.symantec.dlp.x 软件包层次机构中的类）。FlexResponse 插件代码可能与不是由插件容器提供的其他 JAR 文件具有依赖关系。将所需的任何外部 JAR 文件置于部署 FlexResponse 插件的 Enforce Server 的 \plugins 目录中。然后引用该属性中的 JAR。</p>
com.vontu.enforce.incidentresponseaction.IncidentResponseActionInvocationService.maximum-incident-batch-size	<p>对于一个服务器 FlexResponse 智能响应规则调用，可以从事件列表报告中选择的最大事件数。</p> <p>默认值为 100。</p> <p>在此版本中，此参数的最大值不能超过 1000。</p>
com.vontu.enforce.incidentresponseaction.IncidentResponseActionInvocationService.keep-alive-time	<p>不要更改此参数的值。此参数保留供开发和调试使用。</p> <p>使用单个插件属性文件中的 timeout 属性可以设置插件的执行线程超时。</p>
com.vontu.enforce.incidentresponseaction.IncidentResponseActionInvocationService.serial-timeout	<p>串行线程执行器的执行线程超时（全局）。</p> <p>有关详细信息，请参见单个插件属性文件中的 is-serialized 属性。</p>

创建用于配置服务器 FlexResponse 插件的属性文件

每个服务器 FlexResponse 插件的特定信息和参数都位于 *plug-in-name.properties* 文件中。

每个插件必须有一个单独的属性文件。

如果插件满足下列条件，则不需要单独的插件属性文件：

- 不需要自定义属性。
- 在插件元数据类的实现中提供显示名称和插件标识符。
- 不需要存储凭据。

配置服务器 FlexResponse 插件

- 1 创建包含每个服务器 FlexResponse 插件的属性的文本文件。

每个 JAR 文件有一个与该 JAR 文件具有相同基本名称的可选关联属性文件。这些文件位于 *DLP_home\Protect\plugins* 目录中。

例如，如果有一个 *plugin1.jar* 文件，则应该创建一个 *plugin1.properties* 文件。

- 2 在此文件中，请输入插件的所有参数的密钥和值：

```
display-name=plugin 1
plugin-identifier=IncidentResponseAction1
```

要更新属性，必须停止 Vontu Manager 和 Vontu Incident Persister 服务，然后重新启动它们才能加载新值。

请参见第 971 页的 [表 59-3](#)。

- 3 确保 Symantec Data Loss Prevention protect 用户对插件属性文件具有读取和执行访问权限。

[表 59-3](#) 描述了 *plug-in-name.properties* 文件中的属性。

表 59-3 自定义插件属性文件中的参数

属性名称	说明
display-name	<p>此插件的名称。</p> <p>在智能响应规则或自动响应规则中选择“所有：服务器 FlexResponse”操作时，此名称会显示在下拉菜单“选择插件”中。</p> <p>最佳做法是在插件属性文件中定义此属性。</p> <p>如果在加载插件后在属性文件中更改此名称的值，则必须重新启动 Vontu Incident Persister 和 Vontu Manager 服务，以加载新名称。</p> <p>或者，可以在元数据类中指定此值。</p> <p>此值是必选的，必须至少在一个位置指定此值，在配置属性文件中，或者在插件元数据类中。</p> <p>对于国际环境，此显示名称可以使用本地语言。</p>

属性名称	说明
plugin-identifier	<p>此插件的标识符。此标识符对于此 Enforce Server 上的所有服务器 FlexResponse 插件应该是唯一的。</p> <p>最佳做法是在插件属性文件中定义此属性。</p> <p>或者，可以在元数据类中指定此值。</p> <p>此值是必选的，必须至少在一个位置指定此值，在配置属性文件中，或者在插件元数据类中。</p> <p>如果将任何响应规则分配给此服务器 FlexResponse 插件，请不要在属性文件中更改此标识符。</p>
<i>credential-reference. credential</i>	<p>指定对用于验证访问权限的已命名凭据的引用，例如，对库存数据库的引用。此属性的值必须引用在 Enforce Server 上定义的已命名凭据。属性名称中的 credential-reference 提供了一种用于区分属性文件中的多个凭据的方法。</p> <pre>inventory-credential. credential= InventoryDB1</pre>
自定义名称 示例： <code>test1.value.1</code> <code>test1.value.2</code>	需要这些可选自定义参数才能将信息传递给您的插件。会将这些参数传递给插件的每个调用，且可以选择在构建此插件时使这些参数可用。
timeout	<p>一个可选参数，表示此插件的执行线程的超时值（以毫秒计）。</p> <p>默认值为 60000（一分钟）。</p> <p>如果已达到超时值，用户界面会将服务器 FlexResponse 插件状态显示为失败，并且会使用一条超时消息来更新事件历史记录。</p> <p>如果在插件加载后在属性文件中更改此属性的值，则必须停止 Vontu Incident Persister 和 Vontu Manager 服务，然后重新启动这些服务。</p>
maximum-thread-count	<p>一个可选参数，表示可用于执行此插件的并行线程的数量。如果设置了 is-serialized，则会忽略此参数。</p> <p>默认值为 2。</p> <p>如果在插件加载后在属性文件中更改此属性的值，则必须停止 Vontu Incident Persister 和 Vontu Manager 服务，然后重新启动这些服务。</p>

属性名称	说明
is-serialized	<p>此参数的值可以是 <code>true</code> 或 <code>false</code>。如果必须序列化此插件执行（一次一个线程），请将此可选参数设置为 <code>true</code>。所有序列化插件共享单个执行线程。如果设置了此参数，则会忽略 <code>timeout</code> 和 <code>maximum-thread-count</code>。</p> <p>默认值为 <code>false</code>。</p> <p>如果在插件加载后在属性文件中更改此属性的值，则必须停止 Vontu Incident Persister 和 Vontu Manager 服务，然后重新启动这些服务。</p>

查找事件进行手动补救

要手动执行在智能响应规则中配置的插件操作，请使用 Enforce Server 中的报告选择事件进行补救。

查找事件进行手动补救

- 1 登录到 Enforce Server 管理控制台。
 - 2 单击“事件”>“发现”。
 - 3 选择一个事件（或多个事件）进行补救。您可以使用标准报告或报告过滤器来缩小事件列表的范围。
 - 4 您可以选择一组事件或一个事件来进行补救：
 - 在事件列表中，选中每个事件左侧的框，以选择该事件进行补救。您可以选择多个事件。
 - 在事件列表中，通过单击报告标头左侧的复选框选择此页面上的所有事件。
 - 在事件列表中，通过单击报告右上方的“全选”选项选择报告中的所有事件。
 - 单击某个事件以显示“事件详细信息”，并选择某个事件进行可能的补救。
 选择要补救的事件之后，可以手动对它们进行补救。
- 请参见第 973 页的[“使用服务器 FlexResponse 插件的操作手动补救事件”](#)。

使用服务器 FlexResponse 插件的操作手动补救事件

选择要修补的一个事件或一组事件后，可以调用智能响应规则的操作。此操作使用自定义服务器 FlexResponse 插件来手动补救事件。

修补单个事件

- 1 熟悉可用于手动修补事件的响应规则。

单击“策略”>“响应规则”。
“条件”列指示哪些规则可以手动执行。
- 2 选择单个事件，并显示“事件详细信息”。

请参见第 973 页的[“查找事件进行手动补救”](#)。
- 3 在“事件详细信息”屏幕的事件编号上方，显示补救选项。这些选项显示您的响应规则的名称。
- 4 单击一个服务器 FlexResponse 插件补救图标以执行补救操作。
- 5 查看补救操作。单击“确定”。
- 6 验证补救是否已完成。某些补救操作可能会花费很长时间，例如，加密大的文件。要查看用户界面更新，请单击报告右上角的刷新图标。刷新页面，直到在事件详细信息中看到绿色成功图标或红色失败图标。

请参见第 974 页的[“验证事件响应操作的结果”](#)。

补救选定的事件组

- 1 从事件列表报告中选择事件。选中选定事件左侧的框。

或者，您可以选择一个页面或一个报告中的所有事件。
请参见第 973 页的[“查找事件进行手动补救”](#)。
- 2 “事件操作”将成为下拉菜单。
- 3 从“事件操作”下拉菜单中，选择“运行智能响应”，然后选择自定义的服务器 FlexResponse。
- 4 查看补救操作。单击“确定”。
- 5 验证补救是否已完成。某些补救操作可能会花费很长时间，特别是在选择了多个事件时尤为如此。要查看用户界面更新，请单击报告右上角的刷新图标。刷新页面，直到在事件详细信息中看到绿色成功图标或红色失败图标。

请参见第 974 页的[“验证事件响应操作的结果”](#)。

验证事件响应操作的结果

您可以使用事件的“历史记录”选项卡验证补救操作是否已完成。

验证对单个事件执行事件响应操作的结果

- 1 登录到 Enforce Server 管理控制台。
- 2 单击“事件”>“发现”。
查找事件报告中的绿色成功图标或红色失败图标。
- 3 有关结果的其他信息，请单击一个事件以显示“事件详细信息”。
- 4 单击“历史记录”选项卡。
- 5 查看插件中的补救消息。应显示两条消息，一条消息说明已调用插件，另一条消息反映成功或失败情况。可能还会显示其他消息，以及状态结果或补救结果。

验证对事件组执行事件响应操作的结果

- 1 登录到 Enforce Server 管理控制台。
- 2 单击“事件”>“发现”。
- 3 使用报告过滤器和摘要显示事件的保护或阻止状态。
请参见第 785 页的“[查看事件](#)”。
还可以创建自定义报告，以显示保护或阻止状态，或自定义属性的值。
请参见第 786 页的“[关于自定义报告和控制板](#)”。

对服务器 FlexResponse 插件进行故障排除

表 59-4 包含诊断服务器 FlexResponse 问题的故障排除问题和建议。

表 59-4 故障排除建议

问题	建议
在创建智能响应规则的过程中，下拉菜单不显示“所有：服务器 FlexResponse”操作。	发生此问题的原因是您的插件未加载。在 Plugins.properties 文件的末尾，在插件列表中输入您的插件 JAR 文件的名称。确保此行未被注释掉。
在创建自动响应规则的过程中，下拉菜单不显示“所有：服务器 FlexResponse”操作。	重新启动 Vontu Incident Persister 和 Vontu Manager 服务加载您的插件。
有多个插件时，您的插件名称不显示在“所有：服务器 FlexResponse”下拉菜单中。	您的插件属性文件和插件代码可能未正确匹配。请查看 Tomcat 日志查找错误。 名为 localhost.date.log。位于 DLP_home\Protect\logs\tomcat 中。 要验证是否已加载插件，请查找 Enforce 系统事件 (2122)。此事件列出了已加载的所有插件。
您的插件未成功执行。	检查插件和插件框架的消息的事件快照历史记录。 对于智能响应，请查看 Tomcat 日志查找错误。此日志位于 DLP_home\Protect\logs\tomcat 中。名为 localhost.date.log。 对于智能响应，请查看 VontuIncidentPersister.log 调试日志文件。请参见《Symantec Data Loss Prevention 管理指南》。

部署 Python Script Bridge 服务器 FlexResponse 插件

您可通过安装 Python Script Bridge 服务器 FlexResponse 插件，部署使用 Python 脚本语言编写的服务器 FlexResponse 插件。表 59-5 介绍了如何部署和配置此插件以及如何引用 Python 脚本。关于使用 Python 编写和配置服务器 FlexResponse 插件的更多信息，请参见 *Python Script Bridge Server FlexResponse Plug-in Developers Guide* (《Python Script Bridge 服务器 FlexResponse 插件开发人员指南》)。

表 59-5 部署 Python Script Bridge FlexResponse 插件的步骤

步骤	操作	说明
1	安装 Python。	在承载 Enforce Server 的计算机上安装 Python 2.5.4 版。可从 http://www.python.org/download/releases/2.5.4/ 获取 Python 2.5.4

步骤	操作	说明
2	安装 Python Script Bridge 插件。	安装 Python Script Bridge 插件，以便能够使用 Python 编写服务器 FlexResponse 插件代码。 请参见第 977 页的“ 安装 Python Script Bridge 插件 ”。
3	将 Python 脚本复制到 <code>plugins\PythonScriptBridge</code> 目录。	将包含插件的 Python 文件（使用 .py 扩展名的 Python 文件）复制到以下目录中： <code>DLP_home\Protect\plugins\PythonScriptBridge</code>
4	(可选) 创建在插件中使用的凭据和配置参数。	您可以引用插件中存储的凭据。您可以在 Enforce Server 管理控制台中定义这些凭据，然后在插件的属性文件中引用这些凭据。您也可添加仅应用至该插件的配置参数。 请参见第 980 页的“ Python Script Bridge 的属性文件 ”。
5	配置 Python Script Bridge。	每个插件都必须有一个用于配置该插件的属性文件，您可编辑全局 Plugins.properties 文件以引用该插件。 请参见第 980 页的“ Python Script Bridge 的属性文件 ”。 请参见第 978 页的“ 为您的 Python 插件配置 Python Script Bridge 插件 ”。 请参见第 980 页的“ 配置多个 Python Script Bridge 插件 ”。
6	创建响应规则。	响应规则用于定义针对事件进行补救的措施。 请参见第 983 页的“ 为 Python Script Bridge FlexResponse 插件创建响应规则 ”。
7	将响应规则分配至策略。	策略及其关联的检测规则决定着敏感数据何时违反规则并创建事件。 请参见第 983 页的“ 为 Python Script Bridge FlexResponse 插件创建响应规则 ”。

安装 Python Script Bridge 插件

要在 Python 中创建 FlexResponse 插件，必须安装并配置 Python Script Bridge 插件。使用此插件可从服务器 FlexResponse 插件 API 的 Java 实现转换成 Python API。然后，您便可以将 Python Script Bridge 插件配置为调用您的插件。

注意：安装多个插件时，需在以下过程的基础上做一些变化。请参见第 980 页的“[配置多个 Python Script Bridge 插件](#)”。

安装用于部署单个插件的 Python Script Bridge 插件

- 1 从 Symantec FileConnect 网站上下载 Symantec_DLP_版本_Server_FlexResponse_Plugins.zip 文件。
- 2 将此 ZIP 文件解压缩到 Enforce Server 主机上的一个临时目录中。
- 3 在该临时目录中找到 Symantec_DLP_Plugin_Python_Script_Bridge_1.0.0.0.exe 安装程序文件。
- 4 双击此安装程序可执行文件以运行它。
- 5 当安装程序提示指定目标目录时，请输入 Enforce Server 主机上的一个临时目录的路径。（默认情况下，安装程序会将文件解压缩到桌面上一个名为 FlexResponseFiles 的目录中。）
- 6 将以下文件从该临时目录中复制到 `DLP_home\Protect\plugins` 目录中：
 - `PythonScriptBridge.jar`
 - `PythonScriptBridge.properties`
 - `PythonScriptBridge` 目录及其内容。
- 7 将您的 Python 插件的 Python 脚本复制到 `PythonScriptBridge` 子目录中。

注意：默认情况下，Python Script Bridge 插件包含一个预先配置好的 Hello World 示例 Python 插件。

为您的 Python 插件配置 Python Script Bridge 插件

安装 Python Script Bridge 插件并将文件复制到 plug-in 目录中后，您需要对该插件进行配置。配置多个插件时，需在以下过程的基础上做一些变化。请参见第 980 页的“[配置多个 Python Script Bridge 插件](#)”。

配置 Python Script Bridge 插件

- 1 将您的插件的 Python 文件（.py 文件）复制到以下目录中：

`DLP_home\Protect\plugins\PythonScriptBridge`

此目录还包含示例插件文件 `hello_world.py` 和 `hello_world_init.py`，以及 `examples` 目录的内容。对于生产环境，您可以删除这些文件。

- 2 使用文本编辑器打开以下文件：

`DLP_home\Protect\plugin\PythonScriptBridge.properties`

- 3 更改下列属性：

■ `python-script = myPythonActionScript.py`

■ `python-initialization-script = myPythonInitializationScript.py`

其中：

`myPythonActionScript.py` 是为执行补救操作而应调用的 Python 脚本的名称。如果您的插件需要其他脚本，应使用 `python-script` 属性从您定义的脚本中调用这些脚本。

`myPythonInitializationScript.py` 是您的插件的初始化脚本的名称。初始化脚本是可选的，因此可以省略此属性。

- 4 将 `display-name` 属性更改为描述插件功能的名称。例如：

```
display-name = MyCustomFlexResponse
```

`display-name` 属性控制在创建使用“**所有：服务器 FlexResponse**”操作的响应规则时显示的插件名称。

- 5 将 `plugin-identifier` 属性更改为一个描述性的唯一名称。例如：

```
plugin-identifier = my-new-plugin
```

您可以为 `display-name` 和 `plugin-identifier` 属性选用任何唯一名称。

- 6 添加任何配置参数或引用您的插件所需的任何凭据。请参见第 981 页的表 59-6。

- 7 您的插件可能还需要其他的插件配置，例如超时值、线程处理、调试和本地化。请参见第 981 页的表 59-6。

- 8 使用文本编辑器打开以下文件：

```
DLP_home\Protect\config\Plugins.properties
```

- 9 找到以 `#com.symantec.dlp.flexportresponse.Plugin.plugins =` 开头的行。如果该行以 `#` 注释字符开头，请删除 `#` 字符。该行可能包含其他已配置插件的逗号分隔列表；如果未配置任何插件，该行可能为空白。

- 10 将 `PythonScriptBridge.jar` 文件添加到此属性引用的插件列表中。

例如：

```
com.symantec.dlp.flexportresponse.Plugin.plugins = Copy.jar,  
PythonScriptBridge.jar
```

- 11 将以下每个文件的权限设置为允许 Symantec Data Loss Prevention 的 protect 用户对其进行“读取”和“执行”：

■ `DLP_home\Protect\plugins\PythonScriptBridge.jar`

■ `DLP_home\Protect\config\Plugins.properties`

■ `DLP_home\Protect\plugins\PythonScriptBridge.properties`

- *DLP_home\Protect\plugins\PythonScriptBridge* 目录及该目录中的所有 .py 文件。

12 如果 Enforce Server 正在运行, 请重新启动 **VontuManger** 和 **VontuIncident Persister** 服务以注册您所做的配置更改。

配置多个 Python Script Bridge 插件

当您需要安装多个 Python Script Bridge 插件时, 安装过程和配置过程会略有变化。

配置多个 Python Script Bridge 插件

1 请遵照安装说明操作, 同时进行以下替换:

解压缩文件后, 将 `PythonScriptBridge.jar` 和
`PythonScriptBridge.properties` 文件重命名为能够代表您的插件的新名称。
对每个文件使用相同的基本名称。例如:

`myNewPlugin.jar` 和 `myNewPlugin.properties`

请参见第 977 页的“[安装 Python Script Bridge 插件](#)”。

2 按照配置步骤操作, 同时在需要的位置用新的文件名进行替换。

请参见第 978 页的“[为您的 Python 插件配置 Python Script Bridge 插件](#)”。

注意: 配置多个 Python Script Bridge 插件时, `.properties` 文件和 `.jar` 文件的名称必须相同 (`.jar` 或 `.properties` 扩展名除外)。这种命名方式可以将配置与 `jar` 文件关联起来。

Python Script Bridge 的属性文件

属性文件定义了 Python 脚本的名称, 以及有关插件如何运行的其他详细信息。

表 59-6 说明了您可以在此文件中设置的属性。安装 Python Script Bridge 插件后, 属性文件位于以下位置:

DLP_home\Protect\plugins\PythonScriptBridge.properties

如果您配置了多个插件, `plugins` 目录中将有根据其他插件进行命名的其他属性文件。

注意: 当您更改在表 59-6 中列出且在“是否需要重新启动”列中显示“是”的任何属性后, 您必须在承载 Enforce Server 的计算机上重新启动 **VontuManger** 和 **VontuIncidentPersister** 服务。

表 59-6 Python Script Bridge 的属性

属性	是否需要重新启动?	说明
display-name	是	<p>在配置响应规则的过程中，此属性是在您选择“所有:服务器 FlexResponse”操作时“FlexResponse 插件”下拉列表中显示的名称。</p> <p>例如： <code>display-name=Python Bridge</code></p>
plugin-identifier	是	<p>该插件的唯一标识符。此值在 Symantec Data Loss Prevention 部署中必须是唯一的。</p> <p>例如： <code>plugin-identifier=python-bridge</code></p>
timeout	是	<p>以毫秒为单位的时间，经过此时间后，如果线程尚未完成其工作，该插件将停止执行。</p> <p>如果 <code>is-serialized</code> 属性设置为 <code>true</code>，则会忽略此属性。</p> <p>例如： <code>timeout = 600000</code></p>
maximum-thread-count	是	<p>可用来执行此插件的并行线程数目。</p> <p>如果 <code>is-serialized</code> 属性设置为 <code>true</code>，则会忽略此属性。</p> <p>例如： <code>maximum-thread-count = 2</code></p>
is-serialized	是	<p>如果此插件的执行顺序必须是串行的（一次执行一个），则设置为 <code>true</code>。</p> <p>此属性与 <code>timeout</code> 和 <code>maximum-thread-count</code> 属性互斥（并且，如果指定了所有这些属性，则此属性优先）。</p> <p>请注意，所有串行执行的插件共用一个执行线程。此执行线程的超时由 <code>Plugins.properties</code> 文件中的 <code>serial-timeout</code> 属性进行设置。</p> <p>例如： <code>is-serialized = false</code></p>
python-initialization-script	否	<p>可选的 Python 初始化脚本名称。此脚本仅在此插件加载时或 Enforce Server 启动时执行一次。</p> <p>例如： <code>python-initialization-script = hello_world_init.py</code></p>

属性	是否需要重新启动?	说明
python-script	否	<p>执行补救操作的事件响应Python脚本的名称。每次触发使用服务器 FlexResponse 操作的响应规则时都会执行此脚本。这种响应规则可能由策略违规行为触发或者在用户调用智能响应规则时触发。</p> <p>例如:</p> <pre>python-script = hello_world.py</pre>
python-import-path	否	<p>其他的 Python 导入路径 (如果有)。</p> <p>例如:</p> <pre>python-import-path = c:\python_scripts</pre>
debug-mode	否	<p>将此属性设置为 true 可允许使用 Wing IDE 进行调试。</p> <p>例如:</p> <pre>debug-mode = true</pre>
自定义配置参数	否	<p>您可以在属性文件中指定可供您在 Python 脚本中作为名称-值对使用的自定义配置参数。例如:</p> <pre>myParameter = myValue</pre> <p>注意: 请勿用单引号或双引号将此配置参数值引起来。</p> <p>可以在 Python 脚本中引用此配置参数, 方法是在全局 <code>parameters</code> 对象中调用 <code>ConfigurationParameters</code> 类的 <code>getStringValue()</code> 方法。例如, 下面的代码检索 <code>myParameter</code> 配置参数的值:</p> <pre>value_1 = parameters.getStringValue("myParameter")</pre>

属性	是否需要重新启动?	说明
凭据	否	<p>您可以通过在属性文件中创建引用所存储凭据的凭据参数来引用存储在 Enforce Server 上的凭据。请在凭据参数名称后追加 .credential，然后将该参数的值设置为所保存的凭据的名称。</p> <p>例如，下面的属性创建一个配置参数，该参数引用一个已存储且名为 MyEnforceCredential 的凭据：</p> <pre>myCredParam.credential = myEnforceCredential</pre> <p>您可以通过在全局 parameters 对象中调用 getCredentialValue() 方法在 Python 脚本中引用此凭据。</p> <p>例如，下面的代码检索由 MyCredParam 凭据参数定义的已存储的 myEnforceCredential 凭据：</p> <pre>cp = parameters.getCredentialValue("MyCredParam") myCredName = cp.getName() myCredUsername = cp.getUsername() myCredPassword = cp.getPassword()</pre> <p>注意：当您引用此凭据参数时，请省略此参数的 .credential 部分。</p>

为 Python Script Bridge FlexResponse 插件创建响应规则

响应规则定义了用于针对策略违规行为进行补救的操作。要使用 FlexResponse 插件，需要配置引用 Python Script Bridge FlexResponse 插件的操作。

创建响应规则

- 1 打开 Enforce Server 管理控制台。
- 2 导航至“管理”>“响应规则”。
- 3 单击“添加响应规则”。
- 4 选择“自动响应”或“智能响应”。
- 5 单击“下一步”。
- 6 在“规则名称”字段中为此响应规则输入一个名称。如果要配置智能响应规则，此规则名称定义在 Enforce Server 管理控制台中查看事件时用于调用智能响应规则的按钮或菜单项的标签。
- 7（可选）在“说明”字段中输入对此响应规则的说明。

8 (可选, 且仅限于自动响应规则) 单击“添加条件”以添加限制何时触发响应操作的条件。请参见《Symantec Data Loss Prevention 管理指南》。

9 在“添加操作”按钮旁的下拉列表中, 选择“所有:服务器 FlexResponse”操作。

10 单击“添加操作”。

随即便会显示一个包含已配置的 FlexResponse 插件的下拉列表。

11 从该下拉列表中选择相应插件。

该列表中显示的名称由 `PythonScriptBridge.properties` 文件中的 `display-name` 属性决定。

12 单击“保存”。

设置文件共享扫描

本章节包括下列主题：

- [设置文件系统扫描](#)
- [支持的文件系统目标](#)
- [自动发现开放文件共享](#)
- [排除内部 DFS 文件夹](#)
- [配置 Microsoft Outlook 个人文件夹 \(.pst 文件\) 扫描](#)
- [配置与运行文件系统的扫描](#)
- [优化文件系统目标扫描](#)
- [为文件共享配置 Network Protect](#)

设置文件系统扫描

Network Discover 会扫描网络文件服务器和共享资源（“共享”）（例如驱动器或目录）来发现机密数据。Network Discover 使用 CIFS、NFS、DFS 或者其他任何客户端来支持与 CIFS 兼容的文件服务器和文件共享。Network Discover 也可以扫描网络文件共享上的 Microsoft Outlook 个人文件夹 (.pst 文件)。

要设置文件系统扫描，请完成下列过程：

表 60-1 设置网络文件系统扫描

步骤	操作	说明
1	验证网络文件系统是否位于支持的目标列表中。	请参见第 986 页的“ 支持的文件系统目标 ”。

步骤	操作	说明
2	转至“管理”>“发现扫描”>“发现目标”，为文件系统创建新目标，并配置文件系统的扫描。	请参见第988页的“ 配置与运行文件系统的扫描 ”。
3	设置所有其他扫描目标配置选项。 对于 Microsoft Outlook 个人文件夹的扫描，请验证是否设置了此选项。	请参见第929页的“ Network Discover 扫描目标配置选项 ”。 请参见第988页的“ 配置 Microsoft Outlook 个人文件夹 (.pst 文件) 扫描 ”。
4	要自动移动或隔离文件，请配置 Network Protect。	请参见第992页的“ 为文件共享配置 Network Protect ”。
5	启动文件系统扫描。 转至“管理”>“发现扫描”>“发现目标”。	从目标列表中选择扫描目标，然后单击“开始”图标。
6	验证扫描是否正在顺利进行。	请参见第944页的“ 关于 Network Discover 扫描目标列表 ”。

支持的文件系统目标

文件系统目标支持扫描下列网络文件系统：

支持的文件服务器：

- 仅限 CIFS 服务器

支持的文件共享：

- Windows 上的 CIFS
- Linux 上的 NFS
- DFS 扫描（在 Windows 2003 和 2008 上）。

注意：使用 Network Protect 时，不支持 DFS。

此外，文件系统目标支持扫描以下文件类型：

- 使用 Outlook 1997-2002、2003 和 2007 创建的 Microsoft Outlook 个人文件夹 (.pst) 文件。

扫描此目标的 Network Discover Server 必须运行 Windows 操作系统，且必须在该系统上安装 Outlook 2003 SP3 或更新版本。

请参见第 988 页的“[配置 Microsoft Outlook 个人文件夹 \(.pst 文件\) 扫描](#)”。

- UNIX 系统上的文件系统（即使这些系统不是当作 CIFS 或 NFS 共享公开）。使用 SFTP 协议提供与文件共享扫描类似的方法。还可通过列出内容根目录中的路径名的方式扫描 Linux Network Discover Server 上的本地文件系统。例如，您可输入 /home/myfiles。

自动发现开放文件共享

Symantec Data Loss Prevention 可以自动发现指定 CIFS 服务器上的开放共享。指定 UNC 路径或 SMB URL 后，Symantec Data Loss Prevention 会自动查找并扫描该服务器上的开放文件共享。

请参见第 988 页的“[设置新的文件系统目标](#)”。

您可以对自动发现加以限制，使其仅发现与逻辑驱动器对应的管理共享，例如 C\$ 或 D\$。

将自动发现限制在管理共享

- 1 在 Enforce Server 管理控制台中，转至“系统”>“服务器”>“概述”。此时会出现“概述”页。
- 2 单击 Network Discover 服务器的名称。此时会出现“服务器详细信息”页。
- 3 单击“服务器设置”。此时会出现“服务器详细信息 - 高级设置”页。
请参见第 195 页的“[高级服务器设置](#)”。
- 4 将 Discover.FileSystem.OnlyAutoDiscoverAdministrativeShares 属性设置为 true。

排除内部 DFS 文件夹

默认情况下，DFS 文件共享扫描包含动态内部 DFS 文件夹，您不需要扫描这些文件夹。若要从 DFS 文件共享扫描排除这些文件夹，请遵从以下程序：

排除 DFS 内部文件夹

- 1 在 Enforce Server 管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击要向其中添加 DFS 内部文件夹的排除过滤器的扫描的名称。
- 3 单击“扫描的内容”选项卡。
- 4 在“排除过滤器”字段中，输入 /DfsrPrivate/*。
- 5 单击“保存”。

配置 Microsoft Outlook 个人文件夹 (.pst 文件) 扫描

您可以扫描文件共用上的 Microsoft Outlook 个人文件夹 (.pst 文件)。扫描支持使用 Outlook 1997-2002、2003 和 2007 创建的 Microsoft Outlook 个人文件夹 (.pst 文件)。

请参见第 988 页的“[配置与运行文件系统的扫描](#)”。

以下是与扫描 .pst 文件相关的说明：

- 扫描此目标的 Network Discover Server 必须运行 Windows 操作系统，且必须在该系统上安装 Outlook 2003 SP3 或更新版本。
如果用于扫描的 Network Discover Server 运行 32 位 Windows 操作系统，则必须安装 32 位 Outlook。
如果用于扫描的 Network Discover Server 运行 64 位 Windows 操作系统，则必须安装 64 位 Outlook。
- Outlook 必须是扫描此目标的 Network Discover Server 上的默认电子邮件客户端。
- Network Protect 不支持 .pst 文件，即使文件位于 CIFS 共享上也是一样。
- 运行初始基本扫描之后，如果上次修改日期发生变化，增量扫描会扫描整个 .pst 文件。
- 日期过滤器及大小过滤器适用于整个 .pst 文件，而不适用于单独的电子邮件或文件中的其他项目。
- 不能并行扫描 .pst 文件。如果并行运行的扫描开始扫描 .pst 文件，则这些扫描将转为串行扫描。

配置 Microsoft Outlook 个人文件夹扫描

- 1 在 EnforceServer 管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 设置包含 Microsoft Outlook 个人文件夹的文件共享扫描。
请参见第 988 页的“[配置与运行文件系统的扫描](#)”。
- 3 在“高级”选项卡上，选中“扫描PST文件”框。（此框默认为勾选状态。）

配置与运行文件系统的扫描

在运行扫描之前，您必须使用以下过程设置目标。

设置新的文件系统目标

- 1 在 EnforceServer 管理控制台中，转至“管理”>“发现扫描”>“发现目标”。
- 2 单击“新建目标”，然后使用下拉菜单选择特定的目标类型。

3 在“常规”选项卡上，键入此发现目标的“名称”。

键入目标的唯一名称，最多为 255 个字符。

4 选择“策略组”。

如果未选择其他任何策略组，则会使用默认策略组。要应用策略组，请选择要用于此目标的策略组。您可以将多个策略组分配给一个目标。

您可以在“策略组列表”页面上定义策略组。

5 选择希望运行扫描的一或多个发现服务器。

如果您选择多个服务器，则 Symantec Data Loss Prevention 会在扫描开始时自动选择其中一个服务器。

列表中仅显示配置为发现服务器的检测服务器。如果网络上只有一个发现服务器，则会自动指定该发现服务器的名称。在配置目标之前，应先配置发现服务器。在对此目标运行扫描之前，必须至少指定一台服务器。

6 在“扫描类型”下，选择“仅扫描新项目或修改的项目(增量扫描)”。此选项为新目标的默认选项。

■ 如果已更改了现有扫描中的策略或其他定义，则可以将下一次扫描设置为完整扫描。选择下列选项：

“下一次扫描所有项目。后续扫描将为增量扫描。”

■ 如果想要始终扫描此目标中的所有项目，请选择下列选项：
始终扫描所有项目(完整扫描)

7 指定调度选项。

选择“按日程表提交扫描作业”以设置扫描指定目标的日程表。从“日程表”下拉列表中选择选项以显示其他字段。选择“暂停扫描时间间隔”以在指定的时间间隔内自动暂停扫描。您可以转至“发现目标”屏幕，并单击目标项的启动图标来覆盖目标的暂停窗口。暂停窗口保持不变，之后任何针对此窗口运行的扫描都可以依指定暂停。您也可以单击目标项的继续图标，来重新启动暂停的扫描。

8 在“扫描的内容”选项卡上，选择或键入凭据。

您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

您可以指定用来访问所有文件系统的默认用户名。

密码不得包含引号字符。如果任何密码包含引号字符，将不会装载这些文件系统以供扫描。

如果需要在密码中使用引号字符，可以使用JCIFS。默认装载进程使用CIFS客户端。如果默认装载不能工作，则通过在属性文件 Crawler.properties 中设置 filesystemcrawler.use.jcifs=true，装载任务可使用基于 Java 的 CIFS 客户端。

9 在“内容根目录”下，输入要扫描的项目。

从下面选择一种方法来输入文件系统：

■ 从上传的文本文件扫描内容根目录

创建并保存列出您要扫描的服务器的纯文本文件(.txt)。然后单击“浏览”以查找列表，接着单击“立即上传”将其导入。使用 ASCII 文本编辑器创建一个文件，并在每一行键入一个文件服务器或共享。请勿包括用户名和密码。默认情况下，Symantec Data Loss Prevention 会将这些信息解译为服务器消息块 (SMB) 路径。如果要指定 NFS 路径，请在路径中包括 nfs。

```
\server\marketing
nfs:\share\marketing
//server/engineering/documentation
/home/protect/mnt/server/share/marketing
c:\share\engineering
```

■ 扫描内容根目录

单击“添加”以使用行编辑器来指定要扫描的服务器或共享。此处所输入的信息会优先于默认值，且只会应用至指定的路径。

```
\server\share
\server.company.com
smb://server.company.com
\\10.66.23.34
```

10 指定路径过滤器。

使用“**包括过滤器**”和“**排除过滤器**”指定 Symantec Data Loss Prevention 应处理或跳过的文件。请注意，您必须指定绝对路径。如果字段空白，Symantec Data Loss Prevention 会对文件共享中的所有文件进行比对。如果您在“**包括过滤器**”中输入任何值，则 Symantec Data Loss Prevention 只会扫描与过滤器匹配的文件或文档。使用逗号分隔条目，但不要使用空格。当“**包括过滤器**”和“**排除过滤器**”都存在时，会优先使用“**排除过滤器**”。

请参见第 935 页的[“设置发现过滤器以在扫描中包括或排除项目”](#)。

在扫描 DFS 共享时，请排除内部 DFS 文件夹。

请参见第 987 页的[“排除内部 DFS 文件夹”](#)。

在带有快照应用程序的 NetApp 文件管理器上扫描共享时，请排除 .snapshot 文件夹。此文件夹通常位于文件系统或网络共享的根部，例如 \\myshare\\.snapshot。

11 指定日期过滤器。

日期过滤器允许您根据日期在比对进程中包括文件。所有匹配指定日期过滤器的文件都会接受扫描。

12 指定大小过滤器。

使用大小过滤器，您可以基于大小从匹配进程排除文件。Symantec Data Loss Prevention 仅包含匹配指定的大小过滤器的文件。如果将此字段保留空白，则 Symantec Data Loss Prevention 会对所有大小的文件或文档进行比对。

13 选择选项的“高级”选项卡以优化扫描。

请参见第 991 页的[“优化文件系统目标扫描”](#)。

优化文件系统目标扫描

若要优化“文件系统”扫描目标的扫描，您可以配置限制选项、设置事件阈值进行扫描（“库存扫描”），还可以忽略或选择扫描项目。

限制文件系统目标扫描

- 1 转至目标定义的“高级”选项卡。
- 2 在“文件限制”字段中，键入每分钟要处理的最大文件数。
- 3 在“字节限制”字段中，键入每分钟要处理的最大数据量。从下拉列表中选择字节、千字节 (KB) 或兆字节 (MB)。

设置事件阈值

- 1 转至目标定义的“高级”选项卡。
- 2 在“事件阈值”字段中，键入要从单个文件共享（“内容根目录”）或服务器（“计算机”）创建的最大事件数。
- 3 选择“事件计数基于”：“内容根目录”或计算机。

“内容根目录”是“扫描的内容”选项卡上列表中的一个文件共享。达到事件阈值时，扫描会转至下一个文件共享。

“计算机”是一台物理计算机。达到事件阈值时，扫描会转至列表中下一个要扫描的项目。如果该项目位于与上一个项目相同的物理计算机上，则会忽略此项目。此物理计算机的名称在要针对 Network Discover 进行扫描的项目列表中必须完全相同，这样才能将其标识为同一计算机。例如，`\localhost\myfiles` 和 `\127.0.0.1\myfiles` 会视为不同的计算机，即使它们的逻辑名称相同。

如果您使用自动发现扫描指定文件服务器上的开放共享，则“内容根目录”与“计算机”为同一对象。

您也可以设置 Outlook .pst 文件的扫描。

请参见第 988 页的[“配置 Microsoft Outlook 个人文件夹 \(.pst 文件\) 扫描”](#)。

为文件共享配置 Network Protect

使用 Network Protect 可自动将公开共享上所发现的机密文件复制或隔离到安全位置。

Network Protect 仅可用于 CIFS 共享基于服务器的扫描。Network Protect 不支持 .pst 文件。

在启用 Network Protect 的情况下，“添加文件系统目标”页面上会显示一个选项卡，其中包含 Network Protect 补救选项。要使用 Network Protect，您必须在 Enforce Server 管理控制台中同时配置策略和响应规则。此外，扫描凭据（用户名和密码）也必须存在于此目标的“扫描的内容”选项卡上。

以下过程提供过程概述。

为文件共享设置 Network Protect

- 1 创建具有响应规则的策略。转至“管理”>“策略”>“响应规则”，然后单击“添加响应规则”。
- 2 请参见第 653 页的[“关于响应规则”](#)。

3 单击“下一步”。

4 对于“操作”，选择“NetworkProtect: 复制文件”或“NetworkProtect: 隔离文件”。

对于“隔离文件”操作，通过选中“标记文件”复选框，您可以选择保留标记文件来替换删除的文件。在“标记文本”框中，键入标记文本。标记文件是文本文件。标记文本可以包含替代变量。在“标记文本”框内单击可看到插入变量的列表。

如果原始文件属于其他文件类型，则原始文件会移动到隔离区域。标记文件包括原始文件名称加上.txt扩展名。属性文件protectRemediation.properties中会列出保留的默认文件扩展名。保留的文件扩展名包括txt、doc、xls、ppt、java、c、cpp、h和js。例如，名为myfile.pdf的文件会有标记文件名myfile.pdf.txt。

您可以基于每次扫描为隔离文件创建新的子目录（默认）。您可以更改默认设置，并将扫描信息附加到一个隔离目录中的文件名（版本）。编辑属性文件ProtectRemediation.properties以更改默认设置。

单击“保存”。

5 新建策略或编辑现有策略。

请参见第330页的[“配置策略”](#)。

6 单击“响应”选项卡。

7 在下拉菜单中，选择之前创建的响应规则之一。

8 单击“添加响应规则”。

然后，此响应规则会指定当此策略在扫描文件期间触发事件时的自动响应。

一个策略可以存在多个具有不同条件的响应规则。

9 创建新文件系统 Network Discover 目标，或编辑现有目标。

请参见第988页的[“配置与运行文件系统的扫描”](#)。

10 在许可证中已启用 Network Protect 的情况下，“文件系统目标”页面上会出现“保护”选项卡，其中包含 Network Protect 补救选项。

在“允许的保护补救”下，选择是复制还是隔离（移动）文件以保护信息。

此选择必须匹配响应规则中的“操作”选择。

此外，具有该操作（复制或隔离）的响应规则应该存在于针对此文件系统目标所选择的其中一个策略内。

11 在“隔离/复制共享”下，指定隔离或复制文件所在的共享位置。

您也可以从“使用保存的凭据”下拉菜单中的凭据库选择已命名的凭据。

12 在“保护凭据”下，为已扫描文件的位置指定写入权限凭据。

要在补救期间移动隔离文件，Network Discover 目标定义必须对隔离位置和原始文件位置均具有写入权限。指定复制或隔离文件的路径（位置）。键入该位置的写入权限用户名和密码。

通常，已扫描的共享只需读取权限凭据（例如，如果选择了“复制”选项）。

指定共享写入权限凭据（如果与读取权限凭据不同）。

您也可以从“使用保存的凭据”下拉菜单中的凭据库选择已命名的凭据。

设置 Lotus Notes 数据库扫描

本章节包括下列主题：

- [设置 Lotus Notes 数据库扫描](#)
- [支持的 Lotus Notes 目标](#)
- [配置与运行 Lotus Notes 扫描](#)
- [配置 Windows 服务器上的 Lotus Notes 本机模式配置扫描选项](#)
- [配置 Lotus Notes DIOP 模式配置扫描选项](#)
- [在 Linux 服务器上配置 Lotus Notes 本机模式扫描配置选项](#)

设置 Lotus Notes 数据库扫描

您可以配置对 Lotus Notes 存储库的扫描。

请参见第 997 页的“[配置与运行 Lotus Notes 扫描](#)”。

要设置 Lotus Notes 数据库扫描，请完成下列过程：

表 61-1 设置 Lotus Notes 数据库扫描

步骤	操作	说明
1	验证 Lotus Notes 数据库是否在支持的目标列表上。	请参见第 996 页的“ 支持的 Lotus Notes 目标 ”。

步骤	操作	说明
2	配置 Lotus Notes 本机或 DIIOP 模式的扫描。	请参见第 999 页的“ 配置 Windows 服务器上的 Lotus Notes 本机模式配置扫描选项 ”。 请参见第 1000 页的“ 配置 Lotus Notes DIIOP 模式配置扫描选项 ”。
3	单击“管理”>“发现扫描”>“发现目标”以创建 Lotus Notes 目标并配置 Lotus Notes 数据库扫描。	请参见第 997 页的“ 配置与运行 Lotus Notes 扫描 ”。
4	为 Lotus Notes 目标设置所有其他扫描选项。	请参见第 929 页的“ Network Discover 扫描目标配置选项 ”。
5	启动 Lotus Notes 数据库扫描。 单击“管理”>“发现扫描”>“发现目标”。	从列表中选择扫描目标，然后单击“开始”图标。
6	验证扫描是否正在顺利进行。	请参见第 943 页的“ 管理 Network Discover 目标扫描 ”。

支持的 Lotus Notes 目标

Lotus Notes 目标支持扫描以下版本：

- Lotus Notes 6.5
- Lotus Notes 7.0
- Lotus Notes 8.0
- Lotus Notes 8.5.1

在 Network Discover 32 位服务器上，建议使用本机配置，且 Network Discover Server 上必须安装 32 位的 Lotus Notes 客户端。

64 位的 Windows Server 支持 DIIOP 配置选项。但是，只有已在 Network Discover Server 上安装 32 位 Lotus Notes 客户端的 32 位 Network Discover Windows Server，才支持本机配置选项。

在 DIIOP 和本机配置中使用 Linux 32 位 Network Discover Server 时，支持 Lotus Notes 8.5 扫描目标。

文件 Notes.jar 和 NCSO.jar 位于 Lotus Notes 客户端安装目录。仅 DIIOP 模式需要 NCSO.jar 文件。这些文件的清单版本号取决于 Domino 服务器的版本。

- 版本 7 的 JAR 文件中的清单版本为 1.4.2

- 版本 8 的 JAR 文件中的清单版本为 1.5.0

配置与运行 Lotus Notes 扫描

在运行扫描之前，您必须设置目标。

设置新目标以进行 Lotus Notes 数据库扫描

- 1 将 Lotus Notes 扫描的内容根目录指定为一个 Domino 服务器或一个 Domino 服务器列表。

指定要扫描的数据库，如下所示：

- 个别

单击“添加”以指定要扫描的服务器。此处所输入的服务器凭据信息会优先于默认值，且只会应用至指定的服务器。

```
[hostname,username,password]
```

对于本机模式配置，可以使用 Domino 服务器列表中的名称 local。如果指定 local，则仅在扫描中包括客户端可见的本地数据库。例如，输入以下文本，而不是 URI：

```
local
```

- 上传服务器列表

创建并保存您要扫描的服务器的纯文本文件 (.txt)。此文本文件中不能指定服务器凭据。将使用“添加 Lotus Notes 目标”页面的“扫描的内容”选项卡中的用户名和密码。

列表中前面几个 Domino 服务器的示例：

```
dominoserver1.company.com
dominoserver2.company.com
dominoserver3.company.com
```

- 2 选择路径过滤器。

使用“包括过滤器”和“排除过滤器”字段来指定 Symantec Data Loss Prevention 应该作为目标的 Lotus Notes 数据库名称。过滤器会匹配数据库 URI 的完整路径。如果字段空白，Symantec Data Loss Prevention 会扫描所有指定 Domino 服务器中的所有数据库。用逗号分隔条目。如果某个数据库 URI 同时与包括过滤器和排除过滤器相匹配，则排除过滤器优先级更高，不会扫描该数据库。

请参见第 935 页的“[设置发现过滤器以在扫描中包括或排除项目](#)”。

3 选择日期过滤器。

指定日期过滤器以根据日期排除不扫描的 Lotus Notes 文档。仅会包括与所指定的日期过滤器匹配的文档。

4 选择调度选项。

选择“按日程表提交扫描作业”以设置扫描指定目标的日程表。从“日程表”下拉列表中选择选项以显示其他字段。选择“暂停扫描时间间隔”以在指定的时间间隔内自动暂停扫描。您可以转至“发现目标”屏幕，并单击目标项的启动图标来覆盖目标的暂停窗口。暂停窗口保持不变，之后任何针对此窗口运行的扫描都可以依指定暂停。您也可以单击目标项的继续图标，来重新启动暂停的扫描。

5 选择差异扫描（可选）。

选择“仅扫描上次完整扫描后添加或修改的文件”以使 Symantec Data Loss Prevention 扫描自上次扫描之后添加或修改的文档。如果在 Symantec Data Loss Prevention 第一次扫描此目标之前选择此选项，则第一次扫描会以完整扫描来运行。

6 选择大小过滤器。

指定大小过滤器，以根据大小从目标中排除文档。Symantec Data Loss Prevention 仅包括与您指定的大小过滤器匹配的文档。如果您将此字段保留空白，Symantec Data Loss Prevention 会包括所有文档。

7 输入凭据（默认和覆盖）。

您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

您可以指定默认用户名和密码以访问目标中指定的所有 Domino 服务器。您可以在 Domino 服务器列表中编辑单个条目，来覆盖服务器的凭据。只有以个别输入服务器名称的方式创建列表时，才有可能覆盖单个条目的凭据。在包括服务器列表的上传文本文件中，便不能覆盖单个条目的凭据。

8 选择选项的“高级”选项卡以优化扫描。在“高级”选项卡上，您可以配置限制选项或“库存模式”进行扫描。

■ 限制选项

输入每分钟要处理的最大文档数，或每分钟要处理的最大字节数。对于字节数，请从下拉列表中指定度量单位。选项包括：字节、KB（千字节）或 MB（兆字节）。

■ 库存扫描

输入在转至下一个 Domino 服务器（在“扫描的内容”选项卡中指定）之前要生成事件的数目。要审核目标上是否有机密数据，而不扫描整个目标，

请设置“库存模式”进行扫描。设置事件阈值可通过跳至下一个要扫描的服务器，而非全部扫描来提高扫描性能。

请参见第 941 页的“[创建未受保护的敏感数据的位置的库存](#)”。

配置 Windows 服务器上的 Lotus Notes 本机模式配置扫描选项

在文件 `Crawler.properties` 中，当 `lotusnotescrawler.use.diiop` 设为 `false` 时，Network Discover Server 将会通过本地 Lotus Notes 客户端直接访问 Domino 服务器。此模式称为“本机”模式。Lotus Notes 客户端必须安装在 Network Discover Server 上。从性能和安全性考虑，建议使用本机模式。

Lotus Notes 扫描目标也可配置为以 DIIOP 模式扫描。在 DIIOP 模式下，不需要本地客户端。

请参见第 1000 页的“[配置 Lotus Notes DIIOP 模式配置扫描选项](#)”。

配置 Windows 服务器上的 Lotus Notes 本机扫描选项

- 1 仅将 Lotus Notes Java 库文件 `Notes.jar` 复制到 `DLP_home\Protect\plugins` 目录。

可以在 Lotus Notes 客户端安装的安装目录中找到这个文件。

在 Lotus Notes 8 客户端默认安装中，此 JAR 文件位于以下位置：

`C:\Program Files\IBM\lotus\notes\jvm\lib\ext\Notes.jar`

在 Lotus Notes 7 客户端默认安装中，此 JAR 文件位于以下位置：

`C:\Program Files\lotus\notes\jvm\lib\ext\Notes.jar`

在 Lotus Notes 6.5 客户端默认安装中，此 JAR 文件位于以下位置：

`C:\Program Files\lotus\notes\Notes.jar`

使用与 Lotus Notes 客户端版本对应的 `Notes.jar` 文件版本。

请参见第 996 页的“[支持的 Lotus Notes 目标](#)”。

- 2 在 `DLP_home\Protect\config\Crawler.properties` 文件中，设置下列属性：

`lotusnotescrawler.use.diiop = false`

- 3 将 Lotus Notes 客户端安装在 Network Discover Server 上。

- 4 向 Symantec Data Loss Prevention 服务用户授予对 Lotus Notes 主安装目录中 notes.ini 文件的写入权限。

Symantec Data Loss Prevention 服务用户名默认为 protect。

要在 Lotus Notes 客户端上更改此文件的权限, 请右键单击文件 c:\Program Files\lotus\notes\notes.ini。选择“属性”选项。选择“安全”选项卡。在“组或用户名”部分, 选择或添加 protect 用户。在权限部分, 选择“允许”列中的“写入”复选框。单击“确定”。

- 5 将 Lotus Notes 主目录 (如 c:\Program Files\lotus\notes) 添加到系统的 PATH 系统变量。

单击“开始”>“控制面板”。双击“系统”。在“系统属性”窗口中, 单击“高级”选项卡, 然后单击“环境变量”。编辑变量 PATH 并在变量值的末尾添加一个分号和 Lotus Notes 路径 (如 c:\Program Files\lotus\notes)。单击“确定”关闭每个对话框。

- 6 将执行扫描的用户的 user.id 用户凭据文件 (令牌) 复制到 Network Discover Server 上客户端安装的 Lotus Notes 目录 Program Files\lotus\notes\ 中。在 user.id 文件名中, user 是实际用户名。

授予此文件的权限决定对 Lotus Notes Domino 服务器的访问权限以及扫描操作是否成功。Lotus Notes 管理员必须确保 user.id 具有适当的权限来访问所有要扫描的数据库。

- 7 将执行扫描的用户设置为本地安装的 Lotus Notes 客户端的默认用户 (通过 Lotus Notes 客户端用户界面)。必须具有 user.id 用户凭据文件 (令牌), 以供用户在客户端安装的 Program Files\lotus\notes\data 目录中执行扫描时使用。(此路径在 notes.ini 文件中指定。) 在扫描期间, 会忽略在目标配置中指定的用户名, 并且会使用密码来对此默认用户进行身份验证。

- 8 重新启动 Network Discover Server。

单击 Enforce Server 的“系统”菜单。单击 Network Discover Server 以获得“服务器详细信息”。单击“重新启动”来重新启动 Network Discover Server。

配置 Lotus Notes DIIOP 模式配置扫描选项

在文件 Crawler.properties 中, 当 lotusnotescrawler.use.diiop 设为 true 时, 将会使用 DIIOP (CORBA) 来扫描 Domino 服务器。扫描程序会使用 HTTP 和 DIIOP 直接连接至 Domino 服务器。

Lotus Notes 扫描目标也可配置为以本机模式扫描。从性能和安全性考虑, 建议使用本机模式。

请参见第 999 页的“[配置 Windows 服务器上的 Lotus Notes 本机模式配置扫描选项](#)”。

配置 Lotus Notes DIIOP 模式扫描配置

- 1 将 Lotus Notes Java 库文件 Notes.jar 和 NCSO.jar 复制到 *DLP_home/Protect/plugins* 目录。

可以在 Lotus Notes 客户端或安装了 Domino Designer 的 Lotus Domino 服务器的安装目录中找到这些文件。

Notes.jar 文件位于以下 Lotus Notes 客户端默认安装目录：

■ Lotus Notes 8

C:\Program Files\IBM\lotus\notes\jvm\lib\ext\Notes.jar

■ Lotus Notes 7

C:\Program Files\lotus\notes\jvm\lib\ext\Notes.jar

■ Lotus Notes 6.5

C:\Program Files\lotus\notes\Notes.jar

使用与 Lotus Notes 客户端版本对应的 JAR 文件版本。

请参见第 996 页的“[支持的 Lotus Notes 目标](#)”。

安装 Domino Designer 时，NCSO.jar 文件位于以下 Lotus Domino 服务器默认安装目录：

■ Lotus Notes 8

C:\Program Files\IBM\lotus\Notes\Data\domino\java\NCSO.jar

■ Lotus Notes 7

C:\Program Files\lotus\notes\data\domino\java\NCSO.jar

■ Lotus Notes 6.5

C:\Program Files\lotus\notes\data\domino\java\NCSO.jar

- 2 在 Crawler.properties 文件中设置下列属性：

lotusnotescrawler.use.diiop = true

- 3 启动 Domino 服务器上的 HTTP 服务。

- 4 启动 Domino 服务器上的 DIIOP 服务。

- 5 在 Domino 服务器上，将“允许 HTTP 连接以浏览数据库”设置设为 true。
- 6 创建目标时，请输入具有 Internet 密码的用户的凭据。您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

在 Linux 服务器上配置 Lotus Notes 本机模式扫描配置选项

您可以通过 Linux 32 位 Network Discover Server 以本机模式扫描 Lotus Notes 8.5 目标。若要在 Linux 上扫描 Lotus Notes 目标，请执行以下附加任务：

在 Linux 服务器上配置 Lotus Notes 本机模式扫描选项

- 1 确保 notes.ini 和 names.nsf 文件可供 Network Protect 用户写入，并且位于 Lotus Notes 客户端主安装目录 /opt/ibm/lotus/notes 中
- 2 确保 User ID 文件可供 Network Protect 用户写入，并且位于 Lotus Notes 主安装目录中：

```
/opt/ibm/lotus/notes/data
```

- 3 在 Crawler.properties 文件中设置下列属性：

```
lotusnotescrawler.use.dliop = false
```

- 4 将文件 /opt/ibm/lotus/notes/jvm/lib/ext/Notes.jar 复制到 Symantec Data Loss Prevention 插件目录中：

```
/opt/SymantecDLP/Protect/plugins
```

- 5 在 /home/protect/.bash_profile 文件中，设置以下属性：

```
LD_LIBRARY_PATH="/opt/ibm/lotus/notes/data:/opt/ibm/lotus/notes:  
$LD_LIBRARY_PATH"
```

- 6 在 /opt/ibm/lotus/notes/notes.ini 文件中，设置以下属性：

```
KeyFileName=user.id
```

- 7 重新启动 Network Discover Server 以应用所做的配置更改。

设置 SQL 数据库扫描

本章节包括下列主题：

- [设置 SQL 数据库扫描](#)
- [支持的 SQL 数据库目标](#)
- [配置并运行 SQL 数据库扫描](#)
- [为 SQL 数据库目标安装 JDBC 驱动程序](#)
- [SQL 数据库扫描配置属性](#)

设置 SQL 数据库扫描

您可以配置对 Oracle、SQL Server 或 DB2 数据库的扫描。

请参见第 1004 页的“[配置并运行 SQL 数据库扫描](#)”。

要设置 SQL 数据库扫描，请完成以下过程：

表 62-1 设置 SQL 数据库扫描

步骤	操作	说明
1	验证 SQL 数据库是否在支持的目标列表中。	请参见第 1004 页的“ 支持的 SQL 数据库目标 ”。
2	单击“管理”>“发现扫描”>“发现目标”以创建 SQL 数据库目标并配置 SQL 数据库扫描。	请参见第 1004 页的“ 配置并运行 SQL 数据库扫描 ”。
3	为 SQL 数据库目标设置所有其他扫描选项。	请参见第 929 页的“ Network Discover 扫描目标配置选项 ”。

步骤	操作	说明
4	为 SQL 数据库安装 JDBC 驱动程序（如果需要）。	请参见第 1007 页的“ 为 SQL 数据库目标安装 JDBC 驱动程序 ”。
5	启动 SQL 数据库扫描。 单击“管理”>“发现扫描”>“发现目标”。	从目标列表中选择扫描目标，然后单击“开始”图标。
6	验证扫描是否正在顺利进行。	请参见第 943 页的“ 管理 Network Discover 目标扫描 ”。

支持的 SQL 数据库目标

下列 SQL 数据库已经过 Network Discover 目标扫描的测试：

- Oracle 10g (*vendor_name* 是 oracle)
- SQL Server 2005 (*vendor_name* 是 sqlserver)
- DB2 9 (*vendor_name* 是 db2)

有关扫描任何其他 SQL 数据库的信息，请联系 Symantec Data Loss Prevention 支持部门。

配置并运行 SQL 数据库扫描

可以配置并运行针对 SQL 数据库的扫描，以识别哪些数据库包括机密数据，或是找出机密数据存在不当的情况。

会针对特定的一组列数据类型进行 SQL 数据库扫描。SQL 数据库扫描会提取以下 Java 数据库连接 (JDBC) 类型的数据：CLOB、BLOB、BIGINT、CHAR、LONGVARCHAR、VARCHAR、TINYINT、SMALLINT、INTEGER、REAL、DOUBLE、FLOAT、DECIMAL、NUMERIC、DATE、TIME 和 TIMESTAMP。这些列类型与特定数据库列类型之间的映射取决于为扫描实施的 JDBC 驱动程序。

您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

设置 SQL 数据库的扫描

1 选择以下其中一个方法来输入数据库：

- 上传带有数据库列表的文件

创建并保存您要扫描的服务器的纯文本文件(.txt)。单击“浏览”找出列表，然后单击“立即上传”进行导入。系统会使用“添加 SQL 数据库目标”页面的“扫描的内容”选项卡上指定的用户名和密码。

使用以下语法输入数据库。供应商名称可以是oracle、db2或sqlserver。数据源是该驱动程序和数据库的 JDBC 连接字符串的子名称。JDBC 驱动程序的文档提供此子名称的说明。您可以选择输入数据库中每个表扫描的最大行数。

```
vendor_name:datasource[, maximum-rows-to-scan]
```

例如：

```
oracle:@//oracleserver.company.com:1521/mydatabase  
db2://db2server.company.com:50000/mydatabase,300
```

对于某些 SQL Server，还必须指定 SQL 实例名称，如以下示例所示：

```
sqlserver://sqlserver.company.com:1433/mydatabase;  
instance=myinstance
```

■ 手动将数据库输入到用户界面中

单击“添加”选项，以使用行编辑器指定要扫描的数据库。此处所输入的 SQL 数据库信息会优先于默认值，且只会应用于指定的数据库。您可以选择输入数据库中每个表扫描的最大行数。

使用以下语法：

```
vendor-name:datasource[, [username, password]  
[, maximum-rows-to-scan]]
```

2 输入可选的包括和排除过滤器。

使用“包括过滤器”和“排除过滤器”指定 Symantec Data Loss Prevention 应处理或跳过的 SQL 数据库和表。

同时使用“包括过滤器”和“排除过滤器”时，会优先使用“排除过滤器”。任何匹配“包括过滤器”的表都会被扫描，除非它也匹配“排除过滤器”（此时不会扫描）。

如果“包括过滤器”字段为空，Symantec Data Loss Prevention 会对所有表进行匹配。从目标SQL数据库的表查询会返回这些表。如果在此字段中输入任何值，则 Symantec Data Loss Prevention 只会扫描匹配过滤器的数据库和表。

语法为数据库的模式、一条竖线和表名称的模式。多个模式可使用逗号分隔。可应用标准模式匹配。例如，? 匹配单个字符。

由于对于许多数据库而言，表名称匹配不区分大小写，因此会进行大写转换。模式中的表名称和匹配所基于的表名称都会在匹配之前转换成大写。

以下示例将会匹配所有数据库中的员工表。

```
*|employee
```

以下示例将会匹配所有 Oracle 数据库中的所有表。

```
oracle:/*|*
```

对于 SQL Server 2005 和 DB2，默认表查询会返回格式为 *schema_name.table_name* 的表名称。SQL Server 和 DB2 的“包括过滤器”和“排除过滤器”应该匹配此格式。

请参见以下示例：

```
sqlserver:/*|HRSchema.employee  
sqlserver:/*|*.employee
```

3 选择调度选项。

选择“按日程表提交扫描作业”以设置扫描指定目标的日程表。从“日程表”下拉列表中选择选项以显示其他字段。选择“暂停扫描时间间隔”以在指定的时间间隔内自动暂停扫描。您可以转至“发现目标”屏幕，并单击目标项的启动图标来覆盖目标的暂停窗口。暂停窗口保持不变，之后任何针对此窗口运行的扫描都可以依指定暂停。您也可以单击目标项中的继续图标，来重新启动暂停的扫描。

4 选择选项的“高级”选项卡以优化扫描。在“高级”选项卡上，您可以配置限制选项或“库存模式”进行扫描。

■ 限制选项

输入每分钟要处理的最大行数，或每分钟要处理的最大字节数。如果同时选择这两个选项，则扫描速率会低于这两个选项。扫描速率会低于指定的每分钟扫描的行数和指定的每分钟扫描的字节数。对于字节数，请从下拉列表中指定度量单位。选项包括：字节、KB（千字节）或MB（兆字节）。

■ 库存扫描

输入要生成的事件数后，才会继续下一个要扫描的项目。下一个项目是“扫描的内容”选项卡的列表中的下一个数据库。要审核目标上是否有机密数据，而不扫描整个目标，请设置“库存模式”进行扫描。设置事件阈值可通过跳至下一个要扫描的项目，而非全部扫描来提高扫描性能。

请参见第 941 页的“[创建未受保护的敏感数据的位置的库存](#)”。

为 SQL 数据库目标安装 JDBC 驱动程序

必须为要扫描的每种数据库类型安装 JDBC 驱动程序。

安装 JDBC 驱动程序

1 获取相关 JDBC 驱动程序。

■ Oracle 驱动程序已随 Network Discover Server 一起安装在默认 SQL 驱动程序目录 `Protect/lib/jdbc` 中。

JDBC 驱动程序是 Oracle JDBC 驱动程序版本 10.2.0.3.0。

■ 对于 Microsoft SQL Server，开源驱动程序 jTDS 可从 Source Forge 获取，网址为：<http://jtds.sourceforge.net/>。

jTDS JDBC 驱动程序版本 1.2.2 已经过 Network Discover 的测试。

■ 对于 DB2，IBM 驱动程序 JAR 文件位于 IBM DB2 分发的 java 文件夹下。可以从 IBM 获得这些文件，网址为：<http://www.ibm.com/db2>。

IBM JDBC 驱动程序版本 1.4.2 已经过 Network Discover 的测试。

2 将驱动程序文件复制到默认 SQL 驱动程序目录 `Protect/lib/jdbc`。

- 3 更改 JDBC 驱动程序文件的权限，以便 Protect 用户至少具有读取权限。
- 4 可能也需要修改 `sqldatabasecrawler.properties` 文件，以便为所选驱动程序指定正确的 JAR 名称。

请参见第 1008 页的“[SQL 数据库扫描配置属性](#)”。

SQL 数据库扫描配置属性

可以在 Network Discover Server 上的 `sqldatabasecrawler.properties` 配置文件中编辑以下配置属性：

■ `driver_class.vendor_name`

指定要使用的 JDBC 驱动程序的类名。该驱动程序的 JAR 文件必须包含于 `sqldrivers.dir` 中所指定的目录，并且必须被命名为

`driver_jar.vendor_name`。

示例：

```
driver_class.sqlserver = net.sourceforge.jtds.jdbc.Driver
```

■ `driver_subprotocol.vendor_name`

指定 JDBC 连接字符串的子协议部分。

示例：

```
driver_subprotocol.sqlserver = jtds:sqlserver
```

■ `driver_jar.vendor_name`

指定驱动程序所需的 JAR 文件的列表。JAR 文件存储于 `sqldrivers.dir` 中所指定的目录。

请参见第 1007 页的“[为 SQL 数据库目标安装 JDBC 驱动程序](#)”。

示例：

```
driver_jar.sqlserver = jtds-1.2.2.jar  
driver_jar.db2 = db2jcc.jar, db2jcc_license_cu.jar
```

■ `driver_table_query.vendor_name`

指定返回要扫描的表的列表所需要执行的查询。通常，查询应返回数据库中的所有用户表。请注意，执行该查询的数据库帐户需要由数据库管理员授予其适当的权限。

必须使用一个帐户来执行扫描，以便在 `sqldatabasecrawler.properties` 中运行 `driver_table_query` 查询，并返回结果。可以通过使用 `sqlplus` 以扫描用户身份登录，并运行查询来测试扫描配置。如果获得了结果，就有权限完成扫描。如果没有获得结果，则必须更改查询，或者更改扫描用户的权限。

示例：

```
driver_table_query.sqlserver = SELECT table_schema
+ '.' + table_name FROM information_schema.tables
```

■ **driver_row_selector.vendor_name**

指定从表中选择行时要使用的查询格式。该供应商名称根据数据库而变化。对于最常用的数据库，示例包含于 `sqlbasecrawler.properties` 配置文件中。

查询中使用以下替代变量：

```
0=TABLENAME
1=COLUMNS
2=ROWNUM
```

示例：

```
driver_row_selector.sqlserver = SELECT TOP {2} {1} FROM {0}
```

■ **quote_table_names.vendor_name**

指定是否在创建行选择查询前将表名引起来。启用该功能允许扫描使用数字名称的表。例如，将名称引起来后，`Payroll.1` 会变为 “`Payroll`” . “`1`”。

示例：

```
quote_table_names.sqlserver=true
```

■ **sqldrivers.dir**

指定放置 JDBC 驱动程序 JAR 文件的目录的位置。

1010 | 设置 SQL 数据库扫描
SQL 数据库扫描配置属性

设置 SharePoint 服务器扫描

本章节包括下列主题：

- [设置 SharePoint 服务器扫描](#)
- [关于 SharePoint 服务器扫描](#)
- [支持的 SharePoint 服务器目标](#)
- [SharePoint 2007 和 2010 扫描的访问权限](#)
- [关于备用访问映射集合](#)
- [配置和运行 SharePoint 服务器扫描](#)
- [在服务器场的 Web 前端上安装 SharePoint 解决方案](#)
- [将 SharePoint 扫描设置为使用 Kerberos 身份验证](#)
- [排除 SharePoint 扫描故障](#)

设置 SharePoint 服务器扫描

要设置 SharePoint 服务器扫描，请完成以下过程：

表 63-1 设置 SharePoint 服务器扫描

步骤	操作	说明
1	验证 SharePoint 服务器是否位于支持的目标列表中。	请参见第 1014 页的“ 支持的 SharePoint 服务器目标 ”。

步骤	操作	说明
2	验证是否具有足够的权限在服务器场的 Web 前端上安装 SharePoint 解决方案。 此外，还要验证扫描用户是否有权限运行 SharePoint 服务器的扫描。	请参见第 1014 页的“ SharePoint 2007 和 2010 扫描的访问权限 ”。 请参见第 1018 页的“ 在服务器场的 Web 前端上安装 SharePoint 解决方案 ”。 请参见第 1015 页的“ 配置和运行 SharePoint 服务器扫描 ”。
3	在服务器场的 Web 前端上安装 SharePoint 解决方案。	请参见第 1018 页的“ 在服务器场的 Web 前端上安装 SharePoint 解决方案 ”。
4	单击“管理”>“发现扫描”>“发现目标”以创建 SharePoint 目标并配置 SharePoint 服务器的扫描。	请参见第 1015 页的“ 配置和运行 SharePoint 服务器扫描 ”。
5	为 SharePoint 目标设置所有其他扫描选项。	请参见第 929 页的“ Network Discover 扫描目标配置选项 ”。
6	启动 SharePoint 服务器扫描。	单击“管理”>“发现扫描”>“发现目标”。 从目标列表中选择扫描目标，然后单击“开始”图标。
7	验证扫描是否正在顺利进行。	请参见第 943 页的“ 管理 Network Discover 目标扫描 ”。

关于 SharePoint 服务器扫描

Network Discover Server 可以查找 SharePoint 服务器上的大量暴露的机密数据。它可以与 Enforce Server 进行通信，获取有关策略和扫描目标的信息。它可以将找到的有关暴露的机密数据的信息发送到 Enforce Server 以进行报告和补救。

下列类型的 SharePoint 项目会接受扫描：

- Wiki 页面
- 博客
- 日历条目
- 任务
- 项目任务

- 讨论条目
- 联系人列表
- 公告
- 链接
- 调查
- 问题跟踪
- 自定义列表
- 文档库中的文档

注意：仅最新版本的文档会接受扫描。

发现服务器和 SharePoint Web 前端 (WFE) 之间的通信是基于 SOAP 的。

当 SharePoint Web 站点配置为使用 SSL 时，通信是安全的。

对于 HTTPS，默认情况下不会验证服务器 SSL 证书。要启用服务器 SSL 证书的验证，请打开高级设置 `Discover.ValidateSSLCertificates`。然后将服务器 SSL 证书导入到发现服务器。

请参见第 195 页的“[高级服务器设置](#)”。

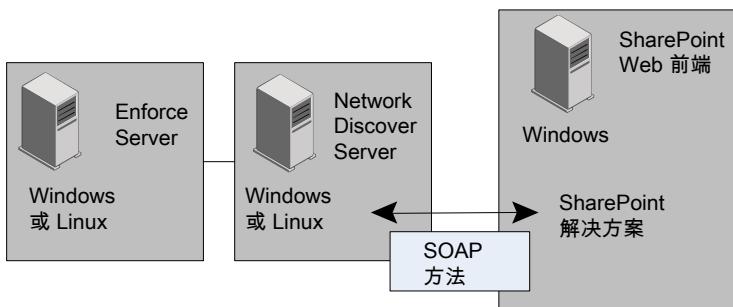
请参见第 190 页的“[将 SSL 证书导入到 Enforce Server 或发现服务器](#)”。

如果将指定的 SharePoint 站点配置为在某个端口上，但不是默认端口 (80)，请确保 SharePoint 服务器允许发现服务器在所需端口上进行通信。

SharePoint 解决方案使用 Windows SharePoint Services (WSS) 应用程序编程接口。用户对内容的访问权限基于 SharePoint 中指定用户的权限。配置 SharePoint 扫描时，请输入用户凭据以指定该用户。您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

请参见第 1015 页的“[配置和运行 SharePoint 服务器扫描](#)”。

图 63-1 SharePoint 与发现服务器的通信



支持的 SharePoint 服务器目标

支持以下 SharePoint 服务器目标：

- Windows Server 2003 32 位上的 Microsoft Office SharePoint Server 2003
SharePoint 2003 仅受 SharePoint 扫描程序的支持。
- Windows Server 2003 32 位上的 Microsoft Office SharePoint Server 2007
- Windows Server 2003 32 位或 64 位，或 Windows Server 2008 R1 32 位或 64 位上的 Microsoft Office SharePoint Server 2007
- Windows Server 2008 R2 64 位上的 Microsoft Office SharePoint Server 2010

请参见第 1076 页的“[支持的 SharePoint 扫描程序目标](#)”。

SharePoint 2007 和 2010 扫描的访问权限

要执行 SharePoint 扫描，用户帐户应具有足够的权限才能访问和浏览 SharePoint 站点内容。用户帐户还必须具有调用 Web 服务和获取访问控制列表(ACL)的权限。

这些权限对应于低级 SharePoint 权限：“浏览目录”、“使用远程接口”和“枚举权限”。有关 SharePoint 权限和权限级别的详细信息，请参考 Microsoft SharePoint 文档。如果用户帐户不具有“枚举权限”，则不会为 SharePoint 内容获取 ACL。

SharePoint 中的下列权限级别已定义这些权限：

- 完全控制（包括“浏览目录”、“使用远程接口”和“枚举权限”）
- 设计（包括“浏览目录”和“使用远程接口”权限）
- 分配（包括“浏览目录”和“使用远程接口”权限）

关于备用访问映射集合

SharePoint 要求在管理中心中将用于访问 Web 应用程序所有 URL 均定义为内部或公共，并且 Symantec SharePoint 解决方案要求用户提供其中一个定义的 URL 作为扫描目标。使用 SharePoint 的备用访问映射集合可以定义用于扫描的 Web 应用程序 URL。有关配置备用访问映射集合的信息，请参见 <http://technet.microsoft.com/en-us/library/cc288609%28office.12%29.aspx>。

配置和运行 SharePoint 服务器扫描

在运行扫描之前，您必须使用以下过程设置目标。

必须在服务器场的 Web 前端上安装 SharePoint 解决方案。

请参见第 1018 页的“[在服务器场的 Web 前端上安装 SharePoint 解决方案](#)”。

设置新目标以进行 SharePoint 服务器扫描

- 1 单击“管理”>“发现扫描”>“发现目标”>“新建目标”>“服务器”>**SharePoint**。
- 2 在“常规”选项卡上，输入该扫描目标的名称。
- 3 选择包含此目标扫描的策略的策略组。
- 4 选择此目标扫描可在其中运行的发现服务器。
- 5 选择调度选项。

选择“按日程表提交扫描作业”以设置扫描指定目标的日程表。从“日程表”下拉列表中选择选项以显示其他字段。

选择“暂停扫描时间间隔”以在指定的时间间隔内自动暂停扫描。您可以转至“发现目标”屏幕，并单击目标项的启动图标来覆盖目标的暂停窗口。暂停窗口保持不变，之后任何针对此窗口运行的扫描都可以依指定暂停。您也可以单击目标项的继续图标，来重新启动暂停的扫描。

请参见第 931 页的“[调度 Network Discover 扫描](#)”。

6 在“扫描的内容”选项卡上，输入该扫描的凭据。

您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

您可以指定默认用户名，以用于访问除了使用“添加”编辑器所指定的那些 SharePoint 站点以外的所有 SharePoint 站点。

如果使用“添加”编辑器指定 SharePoint 站点，则可以为每个站点指定单独的凭据。

用户帐户必须具有 SharePoint 的“浏览目录”权限才能执行扫描。要检索权限，用户帐户必须具有 SharePoint 的“枚举权限”权限级别。

请参见第 1014 页的[“SharePoint 2007 和 2010 扫描的访问权限”](#)。

7 指定要扫描的 SharePoint 站点。

对于每个站点，请输入要扫描的 SharePoint Web 应用程序、站点集合或站点的目标 URL。会扫描其子站点中的所有项目。

对于 Web 应用程序，按如下所示进行指定：<http://www.sharepoint.com:2020>

对于站点集合，按如下所示进行指定：

<http://www.sharepoint.com:2020/Sites/collection>

对于站点或子站点，按如下所示进行指定：

<http://www.sharepoint.com:2020/Sites/mysharepoint/sub/mysite>

对于 SharePoint 站点，请使用公用 URL，而不是内部 URL。

以下语法适用于每行上的 URL 和凭据。

URL, [username, password]

选择用于输入 SharePoint 服务器位置的以下方法之一：

■ 上传的文件

选择“从上传的文件扫描站点”。创建并保存列出您要扫描的服务器的纯文本文件(.txt)。使用 ASCII 文本编辑器创建文件，并在每一行输入一个 URL。然后单击“浏览”在列表中查找文件。单击“立即上传”导入文件。

■ 单个条目

选择“扫描站点”。单击“添加”以使用行编辑器来指定要扫描的服务器。此处所输入的服务器信息会优先于默认值，且只会应用至指定的路径。

8 选择路径过滤器。

使用“包括过滤器”和“排除过滤器”可指定 Symantec Data Loss Prevention 应处理或忽略的项目。如果该字段为空，Symantec Data Loss Prevention 会对所有项目执行匹配。如果为“包括过滤器”输入了任何值，则 Symantec Data Loss Prevention 仅扫描匹配过滤器的那些项目。使用逗号分隔条目，但不要使用空格。

可以使用正则表达式或相对于 SharePoint 站点位置的路径提供过滤器。过滤器可以包括站点集合、站点、子站点、文件夹、文件名或者文件扩展名。路径过滤器不应用于项目的附件，例如，列表项目的 .doc 附件。

所有路径过滤器都是区分大小写的。

对于“包括过滤器”，正则表达式匹配适用于文件，但不适用于文件夹。

对于“排除过滤器”，正则表达式匹配同时适用于文件和文件夹。

匹配文件夹或文件时，仅考虑第一个？或者 * 之前的那段路径。

当所有指定的路径过滤器都为相对时，会忽略匹配文件夹，且扫描统计信息不包括忽略的文件夹中的项目。

请参见第 935 页的[“设置发现过滤器以在扫描中包括或排除项目”](#)。

9 选择日期过滤器。

日期过滤器允许您根据项目日期在匹配进程中包括项目。所有匹配指定日期过滤器的项目都会接受扫描。

请参见第 938 页的[“根据上次访问或修改日期过滤发现目标”](#)。

10 选择大小过滤器。

使用大小过滤器，您可以基于项目大小从匹配进程中排除项目。Symantec Data Loss Prevention 仅包含匹配指定的大小过滤器的项目。如果将此字段留空，Symantec Data Loss Prevention 将对所有大小的项目或文档执行匹配。

请参见第 937 页的[“按项目大小过滤发现目标”](#)。

- 11 在“扫描类型”下，选择“仅扫描新项目或修改的项目(增量扫描)”。此选项为新目标的默认选项。

如果已更改了现有扫描中的策略或其他定义，则可以将下一次扫描设置为完整扫描。选择下列选项：

“下一次扫描所有项目。后续扫描将为增量扫描。”

如果想要始终扫描此目标中的所有项目，请选择下列选项：

始终扫描所有项目(完整扫描)

- 12 选择选项的“高级”选项卡以优化扫描。在“高级”选项卡上，您可以配置限制选项并设置“库存模式”进行扫描。

■ 限制选项

指定每分钟要处理的最大项目数，或指定每分钟要处理的最大字节数。对于字节数，请从下拉列表中指定度量单位。选项包括：字节、KB(千字节)或MB(兆字节)。

注意：提取每个项目后才会应用字节限制。因此，实际网络流量可能不完全匹配设置的字节限制。

■ 库存扫描

输入要生成的事件数后，才会继续下一个要扫描的站点（“扫描的内容”选项卡中的 URL）。要审核目标上是否有机密数据，而不扫描整个目标，请设置“库存模式”进行扫描。设置事件阈值可通过跳至下一个要扫描的站点，而非全部扫描来提高扫描性能。

达到事件阈值之后，便会停止扫描此站点，继续扫描下一个站点。由于进程不是同步的，因此所创建的事件可能会略高于事件阈值所指定的数目。

在服务器场的 Web 前端上安装 SharePoint 解决方案

要使用 Network Discover 扫描 SharePoint 目标，您必须在服务器场的 Web 前端上安装 Symantec SharePoint 解决方案。

在 Network Discover 上运行的 SharePoint 目标与 SharePoint 解决方案进行通信，并在通过 SharePoint 验证后提取内容。如果在 Network Discover 和 SharePoint 服务器之间需要安全的数据传输，则可以将应用程序配置为使用 SSL。

SharePoint 解决方案安装过程需要特定的权限。

请参见第 1014 页的“[SharePoint 2007 和 2010 扫描的访问权限](#)”。

Symantec SharePoint 解决方案已创建版本，并且不向后兼容。如果您要从 Symantec Data Loss Prevention 11.5 版或更低版本升级，您必须升级您的 SharePoint 解决方

案。表 63-2 列出了与 Symantec Data Loss Prevention 版本兼容的 SharePoint 解决方案版本。

表 63-2 Symantec SharePoint 解决方案版本的兼容性

Symantec SharePoint 解决方案的版本	兼容的 Symantec Data Loss Prevention 版本
没有版本号	11.0 至 11.5
11.5.1	11.5.1
11.6	11.6

安装 Symantec SharePoint 解决方案

- 1 将 SharePoint 解决方案安装程序 Symantec_DLP_Solution.exe 复制到 SharePoint Web 前端上的一个临时目录。此文件位于 *DLP_Home\Symantec_DLP_11_Win\Third_Party\SharePoint* 或 *DLP_Home\Symantec_DLP_11_Lin\Third_Party\SharePoint* 目录中，其中 *DLP_Home* 是将 Symantec Data Loss Prevention 软件解压缩到的目录的名称。
- 2 在 SharePoint 服务器上启动 Windows SharePoint Services 管理服务。在 SharePoint 服务器上，单击“开始”>“所有程序”>“管理工具”>“**SharePoint 管理中心**”。
- 3 双击 Symantec_DLP_Solution.exe 文件。此时将启动 Symantec Data Loss Prevention 解决方案安装程序。
- 4 单击“下一步”，安装程序将执行多个初步检查。
如果其中一个检查失败，请更正问题并重新启动安装程序。
单击“下一步”。
- 5 接受 Symantec 授权许可协议，然后单击“下一步”。
- 6 安装程序会复制文件，并将解决方案部署到 SharePoint 服务器场中的所有 Web 应用程序。
- 7 安装后，验证 SharePoint 解决方案是否已正确部署到服务器或服务器场。
- 8 连接到“**SharePoint 管理中心**”。在 SharePoint 服务器上，转至“开始”>“所有程序”>“系统管理工具”>“**SharePoint 管理中心**”。
- 9 对于 SharePoint 2007，单击“操作”选项卡。在“全局配置”部分中，选择“**解决方案管理**”。
- 10 对于 SharePoint 2010，单击“**系统设置**”。然后选择“**管理场解决方案**”。

- 11 验证部署。如果正确安装了解决方案，列表将包括 **symantec_dlp_solution.wsp**。
- 12 如果必须删除解决方案，请使用 SharePoint 的“收回”和“取消部署”功能。

将 SharePoint 扫描设置为使用 Kerberos 身份验证

SharePoint 扫描可有选择地使用 Kerberos 身份验证。

SharePoint 必须已设置为与 Kerberos 身份验证配合使用。

必须将发现服务器配置为与密钥分发中心 (KDC) 和 SharePoint 服务器进行通信。

配置发现服务器以进行 Kerberos 身份验证

- 1 创建一个名为 `krb5.conf` 的文件，其中包含区域和 KDC 信息。在 Windows 中，此文件通常被命名为 `krb5.ini`。示例文件位于文件夹 `C:\SymantecDLP\Protect\config`（在 Windows 默认 Symantec Data Loss Prevention 安装中）。

请参见第 98 页的“[创建 Active Directory 集成的配置文件](#)”。

- 2 将此文件复制到发现服务器的文件夹 `c:/SymantecDLP/jre/lib/security/`（在 Windows 默认 Symantec Data Loss Prevention 安装中）。
- 3 更新此文件中的默认区域和目录服务器参数（区域）。

```
[libdefaults]
    default_realm = ENG.COMPANY.COM

[realms]
ENG.COMPANY.COM = {
    kdc = engADserver.emg.company.com
}
MARK.COMPANY.COM = {
    kdc = markADserver.emg.company.com
}
```

请参见第 98 页的“[创建 Active Directory 集成的配置文件](#)”。

- 4 在发现服务器上，更新文件夹 `C:\SymantecDLP\Protect\config` 中的 `Protect.properties` 文件（在 Windows 默认 Symantec Data Loss Prevention 安装中）。更新指向已更新的 `krb5.ini` 文件的属性。

```
# Kerberos Configuration Information
java.security.krb5.conf=C:/SymantecDLP/jre/lib/security/krb5.ini
```

排除 SharePoint 扫描故障

表 63-3 为排除 SharePoint 扫描的故障提供建议。

表 63-3 排除 SharePoint 扫描故障

问题	建议的步骤
如果指定了内部 SharePoint URL，则仅扫描默认的站点集合。	为 SharePoint 站点指定公用 URL。会扫描所有站点集合。
当发现服务器和 SharePoint 站点位于不同的域时，不会扫描站点集合或者仅扫描默认的站点集合。	使用完全限定的域名指定站点集合/站点/Web 应用程序 URL。 要从发现服务器验证访问，请尝试从浏览器访问 SharePoint URL。 如果短名称不起作用，请尝试使用完全限定的域名。 如果 Web 应用程序 URL 不包含完全限定的域名，则仅扫描默认的站点集合。
报告为已扫描的字节数与内容中的字节数不匹配。	为提高性能，扫描统计信息不包含跳过（过滤掉）的文件夹中的项目。 动态内容（如 .aspx 文件）可以更改大小。 您可以设置高级服务器设置 Discover.countAllFilteredItems 以获取更准确的扫描统计信息。 请参见第 195 页的“ 高级服务器设置 ”。

1022 | 设置 SharePoint 服务器扫描
排除 SharePoint 扫描故障

设置 Exchange Server 扫描

本章节包括下列主题：

- 使用 Exchange Web 存储连接器设置 Exchange 2003 和 2007 存储库的扫描
- 关于 Exchange 2003 和 2007 服务器扫描
- 支持的 Exchange Server Web 存储连接器目标
- 提供扫描所有邮箱和公用文件夹的访问权限
- 配置 Exchange 2003 和 2007 服务器扫描
- Exchange 2003 和 2007 扫描的配置和使用案例示例
- 解答 Exchange 2003 和 2007 扫描的疑难
- 设置使用 Exchange Web 服务扫描 Exchange 2007 SP2 和 2010 存储库
- 关于 Exchange 2007 SP2 和 2010 服务器扫描
- 支持的 Exchange Server Web 服务连接器目标
- 配置 Exchange 2007 SP2 和 2010 服务器扫描
- Exchange 2007 SP2 和 2010 扫描的配置示例和使用情况
- 故障排除 Exchange 2007 SP2 和 2010 扫描问题

使用 Exchange Web 存储连接器设置 Exchange 2003 和 2007 存储库的扫描

您可以使用 Exchange Web 存储连接器扫描 Exchange 2003 和 2007（所有版本）服务器。若要设置使用 Exchange Web 存储连接器扫描 Exchange 2003 和 2007 服务器，请完成下列过程：

表 64-1 设置 Exchange Server 扫描

步骤	操作	说明
1	确认您的 Exchange Server 可提供 Outlook Web Access 且启用 WebDAV。	
2	如果您需要在发现服务器和 Exchange Server 或 LDAP 服务器之间进行安全访问，请设置 HTTPS 和 LDAPS。	请参见第 1026 页的“ 配置 Exchange 2003 和 2007 服务器扫描 ”。
3	如果要扫描所有邮箱和公用文件夹，请确保授予特定用户访问权限。用户也需要对域控制器的访问权限。	请参见第 1026 页的“ 提供扫描所有邮箱和公用文件夹的访问权限 ”。
4	转至“管理”>“发现扫描”>“发现目标”以创建 Exchange 目标并配置 Exchange Server 扫描。	请参见第 1026 页的“ 配置 Exchange 2003 和 2007 服务器扫描 ”。
5	为 Exchange 目标设置所有其他扫描选项。	请参见第 929 页的“ Network Discover 扫描目标配置选项 ”。
6	启动 Exchange Server 扫描。	转至“管理”>“发现扫描”>“发现目标”。 从目标列表中选择扫描目标，然后单击“开始”图标。
7	验证扫描是否正在顺利进行。	请参见第 943 页的“ 管理 Network Discover 目标扫描 ”。

关于 Exchange 2003 和 2007 服务器扫描

Network Discover Server 在 Exchange Server 上查找许多暴露的机密数据，包括电子邮件、日历项目、联系人、日志和标记项目。

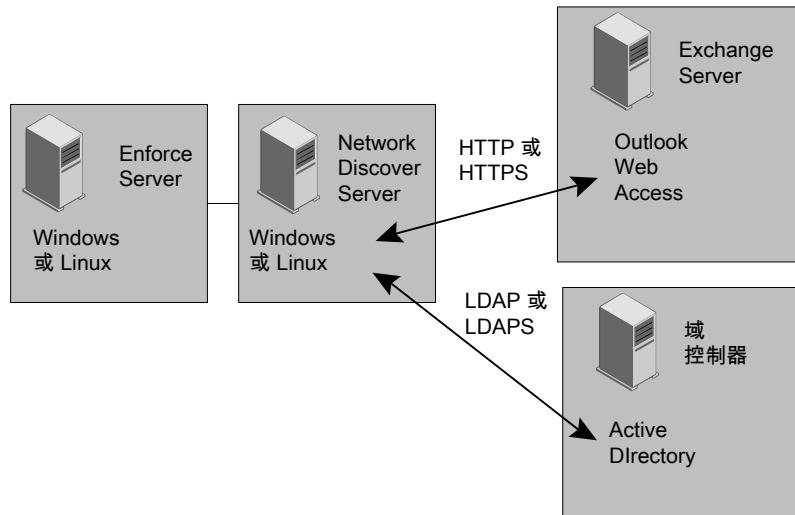
在将 Exchange Server 配置为使用 SSL (HTTPS) 时，通信非常安全。在将 LDAP Server 配置为使用 LDAPS 时，与它通信非常安全。

对于 HTTPS，默认情况下不会验证服务器 SSL 证书。要启用服务器 SSL 证书的验证，请打开高级设置 `Discover.ValidateSSLCertificates`。然后将服务器 SSL 证书导入到发现服务器。

请参见第 195 页的“[高级服务器设置](#)”。

请参见第 190 页的“[将 SSL 证书导入到 Enforce Server 或发现服务器](#)”。

图 64-1 Exchange 扫描配置



支持的 Exchange Server Web 存储连接器目标

Exchange Web 存储连接器支持下列 Exchange Server 目标：

- Microsoft Exchange Server 2003

- Microsoft Exchange Server 2007

对于 Exchange 2007 SP2 服务器，您可以使用 Exchange Web 存储连接器或 Exchange Web 服务连接器。

如果要使用 Exchange Web 存储连接器，必须配置 Outlook Web Access，还必须启用 WebDAV。

Exchange 扫描内容包括用户邮箱中的电子邮件文本和电子邮件文件附件。

您可以扫描存储在公用文件夹内的数据对象，例如：

- 电子邮件
- 邮件附件
- Microsoft Word 文档
- Excel 电子表格

但是，Exchange 扫描不会扫描保存在“个人文件夹”（.pst 文件）或离线文件夹（.ost 文件）中的邮件，这些文件夹不在 Exchange Server 上。要扫描文件共享中的 .pst 文件，请使用共享文件系统目标。

请参见第 988 页的“[配置 Microsoft Outlook 个人文件夹 \(.pst 文件\) 扫描](#)”。

提供扫描所有邮箱和公用文件夹的访问权限

如果要扫描所有邮箱和公用文件夹，请确保授予特定用户访问权限。

支持基本身份验证、NTLM 身份验证和基于表单的身份验证。还支持 Kerberos（如果安装了它）。

对于 Exchange 2007，设置对所有邮箱和公用文件夹的访问权限。

- 1 在 Exchange 控制台中，运行下列命令以启用对所有邮箱的访问权限：

```
Get-Mailbox | Add-MailboxPermission -User specific_user
-Accessright Fullaccess -InheritanceType All
```

- 2 默认情况下，应启用对公用文件夹的访问权限。验证访问权限。
- 3 重新启动 Microsoft Exchange Information Store 服务以立即传播更改。

注意：这些更改将自动传播，但可能需要 15 分钟或更长的时间。

对于 Exchange 2003，设置对所有邮箱和公用文件夹的访问权限。

- 1 打开 Exchange Server Manager。
- 2 选择“服务器”>*server_name* 并确保允许特定用户的访问权限。在“属性”对话框的“安全”选项卡下，查找各个邮箱存储和公用文件夹存储。通常，会授予“代理接收”和“代理发送”以外的所有访问权限。
- 3 添加“代理接收”和“代理发送”访问权限。
- 4 重新启动 Microsoft Exchange Information Store 服务以传播更改。

注意：这些更改将自动传播，但可能需要 15 分钟或更长的时间。

配置 Exchange 2003 和 2007 服务器扫描

在运行扫描之前，您必须使用以下过程设置目标。

如果要进行从发现服务器到 Exchange Server 的安全访问，请为 Exchange Server 设置 HTTPS。如果要进行从发现服务器到域服务器的安全访问，请为域服务器设置

LDAP。对 Enforce Server 和扫描 Exchange Server 的每台发现服务器使用相同的过程。

请参见第 190 页的“[将 SSL 证书导入到 Enforce Server 或发现服务器](#)”。

注意：eml 字符串专用于 Exchange Server 扫描，因为 Exchange 中的文件具有.eml 扩展名。查看您的策略，例如文件匹配，避免在 Exchange 扫描的匹配中使用 eml。此外，还要避免在 Exchange 扫描的包括或排除过滤器中使用此字符串。

设置新目标以进行 Exchange Server 扫描

- 1 转至“管理”>“发现扫描”>“发现目标”>“新建目标”>“服务器”>**Exchange**。
- 2 在“常规”选项卡上，输入该扫描目标的名称。
- 3 选择包含此目标扫描的策略的策略组。
- 4 选择此目标扫描可在其中运行的 Network Discover 服务器。
- 5 选择调度选项。

选择“按日程表提交扫描作业”以设置扫描指定目标的日程表。从“日程表”下拉列表中选择选项以显示其他字段。

选择“暂停扫描时间间隔”以在指定的时间间隔内自动暂停扫描。您可以转至“发现目标”屏幕，并单击目标项的启动图标来覆盖目标的暂停窗口。暂停窗口保持不变，之后任何针对此窗口运行的扫描都可以依指定暂停。您也可以单击目标项的继续图标，来重新启动暂停的扫描。

请参见第 931 页的“[调度 Network Discover 扫描](#)”。
- 6 在“扫描的内容”选项卡上，输入该扫描的凭据。

您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

所有 Exchange 用户名都必须包括域名，例如：

DOMAIN_NAME\user_name

您可以指定默认的用户名来访问 Exchange 站点。

请参见第 933 页的“[为 Network Discover 扫描的内容提供密码身份验证](#)”。
- 7 输入要扫描的 Exchange Server 的目标 URL。

注意：只能为每个发现目标指定一个 Exchange Server。

选择以下某种项目输入方法，以对 Exchange Server 进行扫描：

■ 目录服务器上的所有用户

若要使用此选项，请选择您已经指定的目录服务器连接，或者单击“创建新的目录连接”链接以配置新的目录连接。

请参见第 116 页的[“配置目录服务器连接”](#)。

■ 目录组和用户

如果目录用户组可用，则选择要包含在此目标中的组。

要使用此选项，必须建立目录组。如果没有建立目录组，请单击链接“[创建新的用户组](#)”跳转到相应页面以配置目录用户组。

请参见第 487 页的[“创建或修改用户组”](#)。

■ 指定要包括在此目标中的用户邮箱

输入特定的邮箱。允许在邮箱名称中使用字母数字字符和下列特殊字符：

! # \$ ' - ^ _ ` { }

您可以将该选项与“目录组和用户”组合使用。用户邮箱选项不需要目录组。

■ 公用文件夹

选择此选项可扫描 Exchange Server 上的所有公用文件夹。具有指定凭据的用户必须有对这些公用文件夹的访问权限。

除“目录服务器上的所有用户”或“目录组和用户”之外，您还可以选择此选项。

8 选择路径过滤器。

使用“包括过滤器”和“排除过滤器”可指定 Symantec Data Loss Prevention 应处理或忽略的项目。如果该字段为空，Symantec Data Loss Prevention 会对所有项目执行匹配。如果为“包括过滤器”输入了任何值，则 Symantec Data Loss Prevention 仅扫描匹配过滤器的那些项目。使用逗号分隔条目，但不要使用空格。

可以使用正则表达式或相对于 Exchange 站点位置的路径提供过滤器。过滤器可以包括文件夹名称或文件名。所有路径过滤器都是区分大小写的。

Exchange 可以将电子邮件标识符附加到路径的末尾。要匹配过滤器，请在末尾添加通配符。例如，要过滤“示例公用文件夹项目”，请使用以下过滤器：

```
*/folder/*/*sample public folder item*
```

可以使用正则表达式或相对于 Exchange 站点位置的路径提供过滤器。过滤器可以包括站点集合、站点、子站点、文件夹、文件名或者文件扩展名。所有路径过滤器都是区分大小写的。

对于“包括过滤器”，正则表达式匹配适用于文件，但不适用于文件夹。

对于“排除过滤器”，正则表达式匹配同时适用于文件和文件夹。

匹配文件夹或文件时，仅考虑第一个？或者*之前的那段路径。

当所有指定的路径过滤器都为相对时，会忽略匹配文件夹，且扫描统计信息不包括忽略的文件夹中的项目。

请参见第 935 页的“[设置发现过滤器以在扫描中包括或排除项目](#)”。

9 选择大小过滤器。

使用大小过滤器，您可以基于项目大小从匹配进程中排除项目。Symantec Data Loss Prevention 仅包含匹配指定的大小过滤器的项目。如果将此字段留空，Symantec Data Loss Prevention 将对所有大小的项目执行匹配。

请参见第 937 页的“[按项目大小过滤发现目标](#)”。

10 选择差异扫描（可选）。

选择“仅扫描上次完整扫描后添加或修改的文件”以使 Symantec Data Loss Prevention 仅扫描自上次完整扫描之后添加或修改的项目或文档。第一次的扫描必须是完全（初始基础）扫描。如果您在 Symantec Data Loss Prevention 第一次扫描此目标之前选择此选项，则会进行完整扫描。

11 选择日期过滤器。

日期过滤器允许您根据项目日期在匹配进程中包括项目。所有匹配指定日期过滤器的项目都会接受扫描。

请参见第 938 页的“[根据上次访问或修改日期过滤发现目标](#)”。

12 选择选项的“高级”选项卡以优化扫描。在“高级”选项卡上，您可以配置限制选项并设置“库存模式”进行扫描。

■ 限制选项

指定每分钟要处理的最大项目数，或指定每分钟要处理的最大字节数。对于字节数，请从下拉列表中指定度量单位。选项包括：字节、KB（千字节）或 MB（兆字节）。

■ 库存扫描

输入在完成此扫描前要生成的事件数。要审核目标上是否有机密数据，而不扫描整个目标，请设置“库存模式”进行扫描。

达到事件阈值后，扫描会停止。由于进程不是同步的，因此所创建的事件可能会略高于事件阈值所指定的数目。

Exchange 2003 和 2007 扫描的配置和使用案例示例

表 64-2 列出了配置 Exchange 目标过程中可在“扫描的内容”选项卡中选择的选项。

表 64-2 Exchange 2003 和 2007 扫描使用案例

用例	说明
扫描所有用户邮箱和公用文件夹。	在用户界面中选择下列选项： ■ 目录服务器上的所有用户 ■ 公用文件夹 凭据必须包括同时具有对邮箱和域控制器（用于检索用户列表）的访问权限的用户。 请参见第 1026 页的“ 提供扫描所有邮箱和公用文件夹的访问权限 ”。
扫描所有用户邮箱（但不扫描公用文件夹）。	在用户界面中选择选项“目录服务器上的所有用户”。 凭据必须包括同时具有对邮箱和域控制器（用于检索用户列表）的访问权限的用户。 请参见第 1026 页的“ 提供扫描所有邮箱和公用文件夹的访问权限 ”。
扫描所有公用文件夹。	在用户界面中选择“公用文件夹”选项。 凭据必须包含拥有对公用文件夹的访问权限的用户。

用例	说明
扫描所有属于指定组的用户邮箱。	<p>在用户界面中选择“目录组和用户”选项。 然后从列表的组中选择“目录组”。组中的所有用户邮箱都会接受扫描。 凭据必须包括同时具有对邮箱和域控制器（用于检索用户列表）的访问权限的用户。 请参见第 1026 页的“提供扫描所有邮箱和公用文件夹的访问权限”。</p>
扫描单个用户邮箱。	<p>在用户界面中选择“目录组和用户”选项。 然后输入此单个用户邮箱的名称。 凭据必须包括对指定用户邮箱的访问权限。</p>
扫描不在 Exchange 的默认存储区上的用户邮箱。	<p>在 Exchange Server 上，用户邮箱可能位于不同于默认存储区的其他存储区中。 使用此表中的任一方法指定包含到备用存储区的路径的 Exchange URL，具有对邮箱的访问权限的凭据以及要扫描的邮箱。</p>
扫描不在 Exchange 的默认存储区上的公用文件夹。	<p>在 Exchange Server 上，公用文件夹可能位于不同于默认存储区的其他存储区中。 指定包含到公用文件夹的路径的 Exchange URL 以及具有对公用文件夹的访问权限的凭据。 在用户界面中选择“公用文件夹”选项。</p>

解答 Exchange 2003 和 2007 扫描的疑难

表 64-3 为排除 Exchange 扫描的故障提供建议。

表 64-3 解答 Exchange 2003 和 2007 扫描的疑难

问题	建议的步骤
已创建某个邮箱，但从未登录。未扫描该邮箱。	登录到该邮箱。然后，会扫描该邮箱。
在 Exchange 日志中，扫描了 Exchange 服务器的用户在用户活动中被报告为“上次登录的用户”。	此日志条目指示上次使用邮箱的用户，该用户可能是扫描了邮箱的用户。
报告为已扫描的字节数与内容中的字节数不匹配。	<p>为提高性能，扫描统计信息不包含跳过（过滤掉）的文件夹中的项目。 您可以在“服务器详细信息”>“高级服务器设置”中设置 Discover.countAllFilteredItems 以获取更准确的扫描统计信息。 请参见第 195 页的“高级服务器设置”。</p>

问题	建议的步骤
与 Exchange 服务器的连接超时，未扫描任何项目。	<p>与 Exchange 服务器的连接超时的默认值是 5 分钟（300000 毫秒）。</p> <p>要增大该值，请在配置文件 <code>crawler.properties</code> 中添加并设置该属性。例如，要将超时值设置为 10 分钟，请添加或修改以下行：</p> <pre>crawler.exchange.serverTimeout = 600000</pre>
如果在 Exchange 扫描策略中，文件类型检测规则设置为检测 Outlook Express 项目，则所有项目都将触发事件。	从文件类型检测规则中删除 Outlook Express。

设置使用 Exchange Web 服务扫描 Exchange 2007 SP2 和 2010 存储库

您可以使用 Exchange Web 服务爬网 Exchange 2007 SP2（及更高版本）和 2010 服务器。

表 64-4 设置 Exchange Server 扫描

步骤	操作	说明
1	验证 Exchange Web 服务和 Autodiscover 服务已在 Exchange Server 上启用，且 Network Discover 服务器可以访问这些服务。	有关 Exchange Web 服务和 Autodiscover 服务的相关信息，请参阅 Microsoft Exchange 文档。
2	如果您需要在发现服务器和 Exchange Web 服务或 Active Directory 服务器之间进行安全访问，请设置 HTTPS 和 LDAPS。	<p>默认情况下，Symantec Data Loss Prevention 只允许对 Active Directory 服务器和 Exchange Web 服务进行 HTTPS 连接。若要允许 HTTP 连接，请在“服务器详细信息”>“高级服务器设置”上将 <code>Discover.Exchange.UseSecureHttpConnections</code> 设置设为 <code>false</code>。</p> <p>请参见第 195 页的“高级服务器设置”。</p>
3	确保您的 Exchange 用户凭据可模拟您要扫描的任何邮箱。	有关启用用户凭据的模拟相关信息，请参阅 Microsoft Exchange 文档。
4	转至“管理”>“发现扫描”>“发现目标”以创建 Exchange 目标并配置 Exchange Server 扫描。	请参见第 1034 页的“ 配置 Exchange 2007 SP2 和 2010 服务器扫描 ”。
5	为 Exchange 目标设置所有其他扫描选项。	请参见第 929 页的“ Network Discover 扫描目标配置选项 ”。

步骤	操作	说明
6	启动 Exchange Server 扫描。	转至“管理”>“发现扫描”>“发现目标”。 从目标列表中选择扫描目标，然后单击“开始”图标。
7	验证扫描是否正在顺利进行。	请参见第 943 页的“ 管理 Network Discover 目标扫描 ”。

关于 Exchange 2007 SP2 和 2010 服务器扫描

您可以使用 Exchange Web 服务连接器扫描 Exchange 2007 SP2（及更高版本）和 2010 服务器。对于 Exchange 2007 SP2 服务器，您可以使用 Exchange Web 存储连接器或 Exchange Web 服务连接器。Exchange Web 服务连接器不需要在 Exchange Server 安装代理，也不会搜索每台 Exchange Server。使用 Exchange Autodiscover 功能时，会从 Active Directory 提取 Exchange Server 和邮箱信息，然后使用简单对象访问协议（SOAP）直接从适当的 Exchange Server 提取数据。有关 Exchange Autodiscover 功能的详细信息，请参阅 <http://technet.microsoft.com/en-us/library/bb124251.aspx>。

Network Discover Server 在 Exchange Server 上查找许多暴露的机密数据，包括电子邮件、日历项目、联系人、日志和标记项目。

在将 Exchange Server 配置为使用 SSL (HTTPS) 时，通信非常安全。如果将其配置为使用 LDAPS，则与 Active Directory 服务器的通信将是安全的。

对于 HTTPS，默认情况下不会验证服务器 SSL 证书。要启用服务器 SSL 证书的验证，请打开高级设置 `Discover.ValidateSSLCertificates`。然后将服务器 SSL 证书导入到发现服务器。

默认情况下，Network Discover 会使用与 Exchange 和 Active Directory 服务器间的安全连接。您可以在“服务器详细信息”>“高级服务器设置”中，将 `Discover.Exchange.UseSecureHttpConnections` 设置设为 `false`，来禁用安全访问 Exchange 和 Active Directory。

请参见第 195 页的“[高级服务器设置](#)”。

请参见第 190 页的“[将 SSL 证书导入到 Enforce Server 或发现服务器](#)”。

支持的 Exchange Server Web 服务连接器目标

Exchange Web 服务连接器支持下列 Exchange Server 目标：

- Microsoft Exchange Server 2007 SP2 或更高版本

对于 Exchange 2007 SP2 服务器，您可以使用 Exchange Web 服务连接器或 Exchange Web 存储连接器。

- Microsoft Exchange Server 2010

如果要使用 Exchange Web 服务连接器，必须在 Exchange Server 上启用 Exchange Web 服务和 Autodiscover 服务，而且 Network Discover 服务器可以访问这些服务。

您可以扫描存储在公用文件夹内的数据对象，例如：

- 电子邮件
- 邮件附件
- Microsoft Word 文档
- Excel 电子表格

Exchange 扫描也会将 Exchange 2010 个人存档中存储的邮件列为目标。

配置 Exchange 2007 SP2 和 2010 服务器扫描

在运行扫描之前，您必须使用以下过程设置目标。

设置新目标以使用 Exchange Web 服务扫描 Exchange Server

- 1 转至“管理”>“发现扫描”>“发现目标”>“新建目标”>“服务器”>**Exchange**。
- 2 在“常规”选项卡上，输入该扫描目标的名称。
- 3 选择包含此目标扫描的策略的策略组。
- 4 选择此目标扫描可在其中运行的 Network Discover 服务器。
- 5 选择调度选项。

选择“按日程表提交扫描作业”以设置扫描指定目标的日程表。从“日程表”下拉列表中选择选项以显示其他字段。

选择“暂停扫描时间间隔”以在指定的时间间隔内自动暂停扫描。您可以转至“发现目标”屏幕，并单击目标项的启动图标来覆盖目标的暂停窗口。暂停窗口保持不变，之后任何针对此窗口运行的扫描都可以依指定暂停。您也可以单击目标项的继续图标，来重新启动暂停的扫描。

请参见第 931 页的“[调度 Network Discover 扫描](#)”。

6 在“扫描的内容”选项卡上，输入该扫描的凭据。

您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

所有 Exchange 用户名都必须包括域名，例如：

DOMAIN_NAME\user_name

确保您提供的用户凭据可以模拟您要扫描的所有邮箱。有关配置 Exchange 模拟的相关信息，请参阅 <http://msdn.microsoft.com/en-us/library/bb204095%28v=exchg.80%29.aspx>。请参见第 933 页的“[为 Network Discover 扫描的内容提供密码身份验证](#)”。

7 输入 Microsoft Active Directory 服务器的目标 URL。

注意：只能为每个发现目标指定一个 Active Directory 服务器。

8 选择“公用文件夹”可扫描 Exchange Server 上的所有公用文件夹。具有指定凭据的用户必须有对这些公用文件夹的访问权限。

注意：在同时部署 Exchange 2007 和 2010 服务器的混合 Exchange 环境中，Network Discover 只会扫描您在 Exchange Network Discover 目标中输入凭据所指定版本中的公用文件夹。若要在混合环境中跨 2007 版和 2010 版扫描公用文件夹，请针对每个版本创建其单独所属的 Network Discover 目标。

除“目录服务器上的所有用户”或“目录组和用户”之外，您还可以选择此选项。

9 选择“邮箱”以扫描 Exchange Server 上的用户信箱。选择以下某种项目输入方法，以对 Exchange Server 进行扫描：

■ 目录服务器上的所有用户

如果目录服务器可用，则从下拉列表中选择“**目录服务器**”。

若要使用此选项，请选择您已指定的目录服务器连接，或者单击“**创建新的目录连接**”链接来配置另一个目录连接。

请参见第 116 页的“[配置目录服务器连接](#)”。

■ 目录组和用户

如果目录用户组可用，则选择要包含在此目标中的组。

要使用此选项，必须建立目录组。如果没有建立目录组，请单击链接“**创建新的用户组**”跳转到相应页面以配置目录用户组。

请参见第 487 页的“[创建或修改用户组](#)”。

■ 指定要包括在此目标中的用户邮箱

输入特定的邮箱。允许在邮箱名称中使用字母数字字符和下列特殊字符：

! # \$ ' - ^ _ ` { }

您可以将该选项与“目录组和用户”组合使用。用户邮箱选项不需要目录组。

■ 个人存档

选择此选项可扫描您指定的用户的 Exchange 2010 个人存档信箱。

10 选择路径过滤器。

使用“**包括过滤器**”和“**排除过滤器**”指定 Symantec Data Loss Prevention 应处理或跳过的项目。如果该字段为空，Symantec Data Loss Prevention 会对所有项目执行匹配。如果为“**包括过滤器**”输入了任何值，则 Symantec Data Loss Prevention 仅扫描匹配过滤器的那些项目。使用逗号分隔条目，但不要使用空格。

可以使用正则表达式或相对于 Exchange 站点位置的路径提供过滤器。过滤器可以包括文件夹名称或文件名。所有路径过滤器都是区分大小写的。

Exchange 可以将电子邮件标识符附加到路径的末尾。要匹配过滤器，请在末尾添加通配符。例如，要过滤“示例公用文件夹项目”，请使用以下过滤器：

`*/folder/*/*sample public folder item*`

可以使用正则表达式或相对于 Exchange 站点位置的路径提供过滤器。过滤器可以包括站点集合、站点、子站点、文件夹、文件名或者文件扩展名。所有路径过滤器都是区分大小写的。

对于“**包括过滤器**”，正则表达式匹配适用于文件，但不适用于文件夹。

对于“**排除过滤器**”，正则表达式匹配同时适用于文件和文件夹。

匹配文件夹或文件时，仅考虑第一个？或者*之前的那段路径。

当所有指定的路径过滤器都为相对时，会忽略匹配文件夹，且扫描统计信息不包括忽略的文件夹中的项目。

请参见第 935 页的“[设置发现过滤器以在扫描中包括或排除项目](#)”。

11 选择大小过滤器。

使用大小过滤器，您可以基于项目大小从匹配进程中排除项目。Symantec Data Loss Prevention 仅包含匹配指定的大小过滤器的项目。如果将此字段留空，Symantec Data Loss Prevention 将对所有大小的项目执行匹配。

请参见第 937 页的“[按项目大小过滤发现目标](#)”。

12 选择差异扫描（可选）。

选择“仅扫描上次完整扫描后添加或修改的文件”以使 Symantec Data Loss Prevention 仅扫描自上次完整扫描之后添加或修改的项目或文档。第一次的扫描必须是完全（初始基础）扫描。如果您在 Symantec Data Loss Prevention 第一次扫描此目标之前选择此选项，则会进行完整扫描。

13 选择日期过滤器。

日期过滤器允许您根据项目日期在匹配进程中包括项目。所有匹配指定日期过滤器的项目都会接受扫描。

请参见第 938 页的“[根据上次访问或修改日期过滤发现目标](#)”。

14 选择选项的“高级”选项卡以优化扫描。在“高级”选项卡上，您可以配置限制选项并设置“库存模式”进行扫描。

■ 限制选项

您可以使用限制来限制扫描消耗的带宽，或限制 Exchange Server 的负载。指定每分钟要处理的最大项目数，或指定每分钟要处理的最大字节数。对于字节数，请从下拉列表中指定度量单位。选项包括：字节、KB（千字节）或 MB（兆字节）。

■ 库存扫描

输入在完成此扫描前要生成的事件数。要审核目标上是否有机密数据，而不扫描整个目标，请设置“库存模式”进行扫描。

达到事件阈值后，扫描会停止。由于进程不是同步的，因此所创建的事件可能会略高于事件阈值所指定的数目。

Exchange 2007 SP2 和 2010 扫描的配置示例和使用情况

表 64-5 列出了配置 Exchange 目标过程中可在“扫描的内容”选项卡中选择的选项。

确保您提供的用户凭据可以模拟您要扫描的所有邮箱。有关配置 Exchange 模拟的相关信息，请参阅

<http://msdn.microsoft.com/en-us/library/bb204095%28v=exchg.80%29.aspx>。

表 64-5

Exchange 2007 SP2 和 2010 扫描使用情况

用例	说明
扫描所有用户邮箱和公用文件夹。	在用户界面中选择下列选项： ■ 公用文件夹 ■ “邮箱” > “目录服务器上的所有用户” 凭据必须具有模拟您要扫描之所有邮箱的权限。
扫描所有用户邮箱（但不扫描公用文件夹）。	在用户界面中选择“目录服务器上的所有用户”。 凭据必须具有模拟您要扫描之所有邮箱的权限。
扫描所有公用文件夹。	在用户界面中，选择“公用文件夹”。
扫描指定组或用户。	在用户界面中，选择“邮箱” > “目录组和用户”。 若要扫描目录组，请从列表的组中选择目录组。组中的所有用户邮箱都会接受扫描。您可以单击“创建新的用户组”来创建一个新的目录组。 若要扫描特定用户，请输入用户信箱名称的以逗号分隔的列表。 凭据必须具有模拟您要扫描之所有邮箱的权限。
扫描 Exchange 2010 个人存档。	在用户界面中，选择“邮箱” > “目录服务器上的所有用户” > “个人存档” 或 “邮箱” > “目录组和用户” > “个人存档”。如有必要，请指定要扫描哪些邮箱。Network Discover 会扫描与指定邮箱相关联的个人存档。

故障排除 Exchange 2007 SP2 和 2010 扫描问题

如果遇到 Exchange 2007 SP2 和 2010 扫描问题，可以在此处查找更多信息：

- `FileReader0.log`: 此文件记录在 `&pn.NetworkDiscover` 与 Exchange Web 服务之间的所有 SOAP 请求和响应。

若要配置文件读卡器日志列出 SOAP 请求，请如下编辑
`FileReaderSettings.properties` 文件：

```
java.util.logging.FileHandler.level = FINEST
org.apache.cxf.interceptor.LoggingInInterceptor.level = FINEST
net.entropysoft.eci.exchangewebservices.schema.SchemaHelper.level = WARNING
net.entropysoft.eci.exchangewebservices.schema.PropertyManagersReader.level
org.apache.commons.beanutils.converters.level = WARNING
net.entropysoft.eci.exchangewebservices.AutodiscoverHelper.level = FINEST
net.entropysoft.eci.exchangewebservices.ExchangeWebServicesHelper= FINEST
net.entropysoft.eci.exchangewebservices.level = FINE
```

请参见第 234 页的“操作日志文件”。

- Exchange 日志：您也许可以在 Microsoft Exchange Server 创建的日志中找到有用故障排除信息。

关于 Network Discover 扫描程序

本章节包括下列主题：

- [Network Discover 扫描程序的工作原理](#)
- [排除扫描程序故障](#)
- [扫描程序进程](#)
- [扫描程序安装目录结构](#)
- [扫描程序配置文件](#)
- [扫描程序控制器配置选项](#)

Network Discover 扫描程序的工作原理

扫描程序是一种单机应用程序，可收集存储库中的内容和元数据，并将其发送到 Network Discover 进行处理。

例如，[图 65-1](#) 显示的是一个双层式配置。此配置具备 Enforce Server 与 Network Discover Server，后者连接至已安装扫描程序的 SharePoint 服务器。

您可以在这种配置的计算机上执行下列任务：

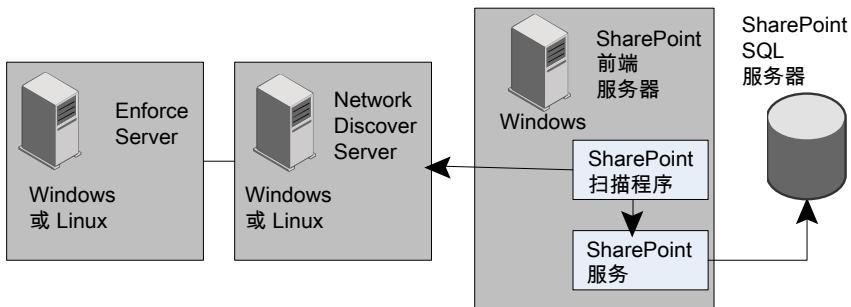
- 在 Enforce Server 上定义扫描目标（例如此示例中的 SharePoint）。
- 在 SharePoint 服务器上安装 SharePoint 扫描程序，配置扫描程序以将内容发布到 Network Discover Server，然后启动（或停止）扫描程序。
- 在 Enforce Server 上启动或停止目标扫描（使用“开始”图标），然后查看事件报告。

扫描程序系统使用 HTTP 协议与 Network Discover Server 通信。

当扫描程序运行时，它会执行下列任务：

- 从本机连接到存储库，检索存储库以便读取内容和元数据。
- 提取文本和一些元数据。
- 将提取的该信息发布到 Network Discover Server。
- Network Discover 使用文本和元数据并应用检测。

图 65-1 SharePoint 扫描程序配置示例



请参见第 919 页的“[关于 Network Discover](#)”。

排除扫描程序故障

扫描启动后，将从存储库中提取内容和元数据。然后将该内容传给扫描控制器和 Network Discover Server。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

如果扫描程序似乎未在处理项目，请使用下列建议：

表 65-1 扫描程序故障排除建议

问题	建议
扫描程序似乎未在运行。	验证是否适当安装了扫描程序。每扫描程序都有自己的安装程序。 在安装了扫描程序的系统中，确保扫描程序进程正在运行。 请参见第 1043 页的“ 扫描程序进程 ”。
报告中没有出现事件。	验证是否适当设置了扫描目标。扫描程序只能向同一类型的目标发送内容。同一类型的多个扫描程序可以为该类型的 Network Discover 扫描提供内容。 检查扫描未被停止。

问题	建议
扫描似乎没有启动。	<p>查看 outgoing 文件夹。</p> <p>请参见第 1044 页的“扫描程序安装目录结构”。</p> <p>如果特定扫描程序无法将内容发送到 Network Discover（这些内容在 /outgoing 文件夹中排队等候）。</p> <p>该文件夹中出现又消失的项目指示进展正常。</p>
扫描似乎已停止。	<p>如果扫描程序无法将内容发送给 Network Discover，则扫描程序内容在扫描程序系统上排队等候。扫描程序系统必须具有 Network Discover Server 的访问权限。安装之前，两个系统上都应出现诸如磁盘空间不足或服务已关闭等系统警告。</p> <p>要验证 Network Discover Server 上接收的内容，请查看扫描的扫描统计信息页面。要查看扫描统计信息，请单击目标扫描列表中运行的扫描。</p> <p>通过检查日志和临时目录验证扫描信息是否贯穿扫描进程。</p> <p>请参见第 1044 页的“扫描程序安装目录结构”。</p> <p>如果看上去扫描已停止，请检查扫描程序计算机上的以下位置来诊断问题：</p> <ul style="list-style-type: none">■ /logs 文件夹<ul style="list-style-type: none">/scanner_typeScanner/logs 文件夹中有扫描程序的启动状态、停止状态以及与 Network Discover 的连接状态。相似的信息位于控制台窗口。检查日志文件以验证扫描程序是否正在正常运行。■ /failed 文件夹<ul style="list-style-type: none">/failed 文件夹中出现的项目指示“新建目标”和扫描程序之间的扫描程序类型不匹配。例如，如果在“新建目标”中指定 Exchange 扫描程序，但是扫描程序为 SharePoint，则项目会出现在 /failed 文件夹中。■ /outgoing 文件夹<ul style="list-style-type: none">该文件夹中出现又消失的项目指示进展正常。如果项目存留在该文件夹中而不被消耗（不消失），则指示文本和元数据的提取存在问题。如果特定扫描程序无法将内容发送到 Network Discover，这些内容会在 /outgoing 文件夹中排队等候。■ /scanner_typeScanner/scanner 目录中有扫描程序与存储库之间的连接状态、存储库检索信息以及所提取的数据。

扫描程序进程

表 65-2 提供了关于 Windows 操作系统上 Network Discover 扫描程序进程的相关信息。

表 65-2 发现进程

进程	可执行文件	说明
ScannerController	scanner_typeScanner_Console.exe 或 scanner_typeScanner_Service.exe	配置与控制连接器、将内容发送至 Network Discover Server 以及将扫描结束消息发送至 Network Discover 的进程。
Connector	scanner_typeScanner.exe	从存储库中提取文档和元数据的进程。
ImportModule	ImportSlave.exe	从连接器下载的文档中提取文本和元数据的进程。
KeyView	KVoop.exe	KeyView 进程是从已知文档类型提取文本和元数据。
Binslave	BinSlave.exe	尝试从未知文档类型提取文本的进程。

扫描程序安装目录结构

表 65-3 说明了 Network Discover 扫描程序配置文件的目录结构。

表 65-3 安装目录结构

路径	说明
/scanner_typeScanner	
....../bin	运行、启动和停止扫描程序的文件。
......./Clean.exe	清除 /scanner 目录下的所有临时文件及日志。
......./EncryptPassword.exe	可用于加密置于 scanner_typeScanner.cfg 文件中的用户名及密码。
......./scanner_typeScanner_Console.exe	将扫描程序作为控制台应用程序（含窗口）启动。键入 CTRL+C 可以停止扫描程序。

路径	说明
...../scanner_typeScanner_Service.exe	将扫描程序作为应用程序（无窗口）启动。通常，仅在扫描程序已注册且作为 Windows 或 UNIX 服务运行时，才会使用此启动。
.... /config	配置文件位于此目录中。
..... /ScannerController.properties	ScannerController 的配置文件。
..... /ScannerControllerLogging.properties	扫描程序记录的属性文件。
..... /scanner_typeScanner.cfg	连接器的配置文件。在启动子进程前，会将此文件复制到 /scanner 目录中。
.... /logs	包含 ScannerController 进程的日志文件。
.... /outgoing	在将包括内容和元数据的 XML 文件发送至 Network Discover Server 前，会在此文件夹中将这些文件排成队列。
.... /scanner	此目录下包括二进制文件、日志文件及临时文件。
..... /outgoing	不能将某些连接器（例如，Exchange 和 SharePoint2003）配置为将 .idx 文件写入 ./outgoing 文件夹中。相反，这些连接器会将其写入 ./scanner/outgoing 文件夹中，ScannerController 会将其移动至 ./outgoing 目录，以便可以发送至 Network Discover Server。
..... /failed	如果 Network Discover Server 无法解析 XML，并返回错误代码 500，则 ScannerController 会将违规的 XML 文档移动至 ./failed 文件夹。

扫描程序配置文件

通过编辑扫描程序系统上的以下文件，可以在安装之后及启动扫描之前编辑配置选项：

文件名	配置任务
ScannerController.properties	<p>在 ScannerController.properties 文件中，您可以配置以下选项：</p> <ul style="list-style-type: none"> ■ 定义 Network Discover Server 连接信息。 ■ 提供内容压缩以减少网络负载。 ■ 打开或关闭增量扫描。在 Vontusscanner_typeScanner.cfg 文件中可能需要其他配置。 <p>请参见第 1046 页的“扫描程序控制器配置选项”。</p>
ScannerControllerLogging.properties	<p>在 ScannerControllerLogging.properties 文件中，您可以配置以下选项：</p> <ul style="list-style-type: none"> ■ 从 .level = INFO 到 .level = FINEST 指定日志记录级别。
Vontusscanner_typeScanner.cfg	<p>在 Vontusscanner_typeScanner.cfg 文件中，您可以配置以下选项：</p> <ul style="list-style-type: none"> ■ 指定多个作业（按顺序运行）。 ■ 定义访问凭据。 请参见第 934 页的“加密配置文件中的密码”。 ■ 定义过滤器。 ■ 定义限制。 ■ 特定设置也适用于每个扫描类型。

扫描程序控制器配置选项

初始扫描程序配置是在安装期间发生的。安装之后，您就可以修改或指定其他扫描设置。

表 65-4 提供了对 ScannerController.properties 文件中通常会修改的参数的说明。

表 65-4 ScannerController.properties 中通常会修改的参数

参数	默认值	说明
discover.host	localhost	扫描程序路由内容至此的目标 Network Discover Server 的主机名称或 IP 地址。在配置此值之前，应将 Network Discover Server 添加至 Enforce Server，并从已验证的扫描程序对其进行访问。
discover.port	8090	扫描程序将数据路由到的目标 Network Discover 端口。

参数	默认值	说明
discover.compress	true	指定是否要先压缩内容，再将内容路由至 Network Discover Server。进行压缩可降低网络负载，但是会消耗扫描程序计算机与 Network Discover Server 上的额外 CPU 资源。
discover.retry.interval	1000	扫描程序在中断连接或上次失败之后，重试连接到 Network Discover Server 之前应该等待的时间（毫秒）。
scanner.send.endofscanmarker	true	如果将此参数设为 false，扫描程序将会一直运行，直到在 Enforce Server 控制台中手动停止为止。当扫描到达扫描列表结尾处，就会从头重新开始。
scanner.incremental	false	如果是 true，则扫描程序只会扫描其创建或修改日期晚于上次完整扫描日期的文档。如果是 false，则每当扫描运行时，就会扫描所有文件。
dre.fake.port	disabled http://localhost:19821	只能由某些扫描程序用于防止内容被误导向至错误的进程。还必须使用 <i>scanner_typeScanner.cfg</i> 文件中的 DREHost 值和 ACIPort 值来修改。 <i>dre.fake.port</i> 可指定 ScannerController 所绑定到的端口。它可确保连接器不会尝试将内容发送到其他一些进程。
queue.folder.path	disabled ./scanner/outgoing	只能由某些扫描程序用于桥接 .idx 文件的写入位置与预期位置之间的差异。此参数适用于 Exchange 与 SharePoint 2003 扫描程序。

设置文件系统扫描

本章节包括下列主题：

- [设置文件系统扫描](#)
- [支持的文件系统扫描程序目标](#)
- [安装文件系统扫描程序](#)
- [启动文件系统扫描](#)
- [从命令行以静默方式安装文件系统扫描程序](#)
- [文件系统扫描程序的配置选项](#)
- [扫描 Windows 计算机上的 C 驱动器的配置示例](#)
- [在 UNIX 上扫描 /usr 目录的配置示例](#)
- [使用包括过滤器进行扫描的配置示例](#)
- [使用排除过滤器进行扫描的配置示例](#)
- [使用包括和排除过滤器进行扫描的配置示例](#)
- [使用日期过滤进行扫描的配置示例](#)
- [使用文件大小过滤进行扫描的配置示例](#)
- [在 UNIX 系统中跳过符号链接的扫描的配置示例](#)

设置文件系统扫描

扫描不是文件共享的文件系统是通过多计算机安装来完成的。在具有文件系统的计算机上，扫描软件会将数据发送到 Network Discover Server 进行处理。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

对于文件共享，请使用服务器文件系统目标。

请参见第 985 页的“[设置文件系统扫描](#)”。

要设置文件系统扫描，请完成下列过程：

表 66-1 [设置文件系统扫描程序](#)

步骤	操作	说明
1	验证文件系统是否位于支持的目标列表中。 文件系统扫描程序可在远程 Windows、Linux、AIX 和 Solaris 服务器上扫描本地文件系统。	请参见第 1050 页的“ 支持的文件系统扫描程序目标 ”。
2	在包含文件系统的服务器上，安装文件系统扫描程序。 扫描文件系统设置需要在文件系统所在的计算机上安装扫描程序软件。 在 Linux、AIX 和 Solaris 上，根用户必须安装该扫描程序。	请参见第 1051 页的“ 安装文件系统扫描程序 ”。 请参见第 1054 页的“ 从命令行以静默方式安装文件系统扫描程序 ”。
3	通过编辑配置文件和属性文件执行所有手动配置。	请参见第 1055 页的“ 文件系统扫描程序的配置选项 ”。
4	在 Enforce Server 中，添加新的扫描程序文件系统目标。	请参见第 926 页的“ 添加新的 Network Discover 目标 ”。
5	启动文件系统扫描。 启动扫描程序计算机上的扫描程序，并在 Enforce Server 上启动扫描。	请参见第 1053 页的“ 启动文件系统扫描 ”。
6	验证扫描是否正在顺利进行。	请参见第 1042 页的“ 排除扫描程序故障 ”。

支持的文件系统扫描程序目标

可扫描下列远程 Windows 系统：

- Windows 2000
- Windows 2003 (32 位)
- Windows XP, 32 位

可扫描下列 Linux 文件系统：

- x86 32 位, Red Hat Enterprise Linux AS 4 U5

可扫描下列 AIX 文件系统：

■ AIX 5.3

AIX 需要以下 C 运行时库以及 Java 1.5:

- `xlc.aix50.rte (v8.0.0.0+)`
- `xlc.rte (v8.0.0.0+)`

可扫描下列 Solaris 文件系统:

- Solaris 8 (SPARC 平台)
- Solaris 9 (SPARC 平台)
- Solaris 10 (SPARC 平台)

对于该扫描程序, Solaris 要求以下修补程序级别:

- Solaris 8, 111308-05
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-111308-05-1>
- Solaris 9, 115697-01
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-115697-02-1>

也可使用 SFTP 协议扫描 UNIX 系统上的文件系统。此协议提供类似于基于共享的文件扫描的方法, 而不使用文件系统扫描程序。有关详细信息, 请联系 Symantec 专家服务。

安装文件系统扫描程序

必须在具有要扫描的文件系统的计算机上安装文件系统扫描程序。

在 Linux、AIX 和 Solaris 上, 根用户必须安装该扫描程序。

如果除安装扫描程序的用户以外的其他用户想要运行该扫描程序, 必须更改权限。

在 Linux、AIX 和 Solaris 上, 必须向目录和文件授予适当的权限。

安装文件系统扫描程序

- 1 在具有要扫描的文件系统的计算机上, 将相关安装文件下载或复制 (作为二进制文件) 到临时目录。该文件位于 `DLP_Home\Symantec_DLP_11_Win\Scanners` 或 `DLP_Home\Symantec_DLP_11_Lin\Scanners` 目录中, 其中, `DLP_Home` 是您先前将 Symantec Data Loss Prevention 软件解压缩到的目录名称。

文件的文件名为以下之一:

- `FileSystemScanner_windows_x32_11.6.exe`

注意: 此扫描程序应该仅安装在 32 位 Windows 服务器上。

- `FileSystemScanner_Aix_11.6.sh`

- FileSystemScanner_Unix_11.6.sh (适用于 Linux 系统)
- FileSystemScanner_Solaris_11.6.sh

2 启动扫描程序安装程序。

使用 -c 标志，通过控制台命令（而不是 GUI）来安装扫描程序。

Windows GUI:

```
FileSystemScanner_windows_x32_11.6.exe
```

Linux GUI:

```
./FileSystemScanner_Unix_11.6.sh
```

Linux 控制台:

```
./FileSystemScanner_Unix_11.6.sh -c
```

- 3 选择安装的“目标目录”（想要将 SymantecDLP 文件系统扫描程序安装到的目录）。
- 4 对于 Windows，选择开始菜单文件夹（“开始”菜单中的快捷方式）。默认值为 **Vontu FileSystem Scanner**。
- 5 输入 Network Discover Server 的以下连接信息：
 - 发现主机（Network Discover Server 的 IP 或主机名）
 - 发现端口
- 6 通过输入以下信息来配置文件系统扫描程序：
 - 扫描目录
要扫描的目录的列表。使用逗号分隔（不含空格）。
 - 路径包括过滤器
仅扫描包含此处指定的所有字符串的路径。使用逗号分隔（不含空格）。
 - 路径排除过滤器
扫描除包含此处指定的字符串的目录以外的所有内容。使用逗号分隔条目，但不要使用空格。
请注意，“包括过滤器”和“排除过滤器”文件名是相对于文件系统根目录的名称。根据需要指定完整的路径或子目录。
- 7 安装扫描程序。
- 8 选择 Startup Mode。

在最初测试或验证扫描程序是否可成功运行时，不要选择这些选项，而是手动启动扫描程序。

可以选择以下选项之一（或不选）：

- 作为 Windows 系统上的服务安装。
- 安装后启动。

- 9 扫描程序计算机上的文件扫描程序安装完成。
- 10 通过编辑配置文件和属性文件执行所有手动配置。
请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。
请参见第 1044 页的“[扫描程序安装目录结构](#)”。
请参见第 1045 页的“[扫描程序配置文件](#)”。
- 11 在 Enforce Server 上，为扫描程序“文件系统”类型创建一个新目标。
- 12 在扫描程序计算机和 Enforce Server 上同时启动扫描。
请参见第 1053 页的“[启动文件系统扫描](#)”。

启动文件系统扫描

确保在目标计算机上安装并配置扫描程序，并在 Enforce Server 上添加新目标。

请参见第 1051 页的“[安装文件系统扫描程序](#)”。

然后，您可以启动扫描。

下列每种情景对应的过程是不同的：

- 一个目标对应一个扫描程序（第一个过程）。
- 一个目标对应多个扫描程序（第二个过程）。

启动文件系统扫描（一个目标对应一个扫描程序）

- 1 登录到 Enforce Server。
转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。
- 2 从目标列表中选择扫描目标，然后单击“开始”图标。
- 3 在扫描程序计算机上，启动文件系统扫描程序。
在 Windows 上，选择“开始”>**Vontu FileSystem Scanner > Vontu FileSystem Scanner Console**。
在 UNIX 上，输入下列命令：

```
/opt/FileSystemScanner/bin/FileSystemScanner_Console
```

- 4 扫描程序启动扫描数据进程。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

- 5 如果扫描不能正常进行，您可以对其进行故障排除。

请参见第 1042 页的“[排除扫描程序故障](#)”。

- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

启动文件系统扫描（一个目标对应多个扫描程序）

- 1 在每台扫描程序计算机上，启动此计算机上的文件系统扫描程序。

在 Windows 上，选择“开始”>**Vontu FileSystem Scanner > Vontu FileSystem Scanner Console**。

在 UNIX 上，输入下列命令：

```
/opt/FileSystemScanner/bin/FileSystemScanner_Console
```

确保每个扫描程序都已启动并且都已发布信息。检查每台计算机上的 outgoing 文件夹。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

- 2 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

- 3 从目标列表中选择扫描目标，然后单击“开始”图标。

- 4 扫描程序启动扫描数据进程。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

- 5 如果扫描不能正常进行，您可以对其进行故障排除。

请参见第 1042 页的“[排除扫描程序故障](#)”。

- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

从命令行以静默方式安装文件系统扫描程序

要自动安装，可以使用安装选择预先配置文本文件 varfile，然后从命令行启动安装。

安装扫描程序的另一个方法是采用交互式安装。

请参见第 1051 页的“[安装文件系统扫描程序](#)”。

自动进行文件扫描程序安装

- 1 创建一个文本文件，例如 FileSystemScanner.varfile。
- 2 输入您的特定参数，并将文件保存到与扫描程序安装相关 Shell 脚本相同的位置。

```

sys.programGroup.allUsers$Boolean=true
discover.host=test-server.test.lab
discover.port=8090
sys.service.selected.417$Boolean=true
job.0.excludeFilters=
sys.languageId=en
sys.programGroup.linkDir=/usr/local/bin
installService$Boolean=false
sys.installationDir=/opt/FileSystemScanner
sys.programGroup.enabled$Boolean=true
job.0.includeFilters=
job.0.directory=/home/text_files/text_scan/text
sys.service.startupType.417=auto
startAfterInstall$Boolean=false

```

- 3 要使用 varfile 运行安装，请键入以下命令（适用于 Linux）：

```
# ./FileSystemScanner_Unix_11.6.sh
-varfile FileSystemScanner.varfile -q
```

参数 -q 可执行静默安装。

文件系统扫描程序的配置选项

表 66-2 提供了 VontuFileSystemScanner.cfg 文件中主要参数的说明。

表 66-2 VontuFileSystemScanner.cfg 文件中的参数

类型	参数	说明
扫描的内容	DirectoryPathCSVs	要扫描的目录的列表（以逗号分隔）。
扫描的内容	DirectoryCantHaveCSVs	路径的排除过滤器。使用逗号分隔条目，但不要使用空格。

类型	参数	说明
扫描的内容	DirectoryMustHaveCSVs	路径的包括过滤器。使用逗号分隔条目，但不要使用空格。
扫描的内容	DirectoryAfterDate	日期过滤器（相对于今天的天数）。
扫描的内容	DirectoryBeforeDate	日期过滤器（相对于今天的天数）。
扫描的内容	DirectoryFileMatch	对于 Solaris 或 Linux 系统上没有扩展名的扫描文件，将此参数设置为以下值： DirectoryFileMatch=*
扫描的内容	ImportPreImportMinLength	文件的最小大小。
扫描的内容	ImportPreImportMaxLength	文件的最大大小。
限制	ImportPoliteness	指定导入模块在两个文档之间应等待的时间（毫秒）。
限制	PollingMaxNumber	在文件导入至每个发送到 Network Discover 的 XML 文件之前聚合的文件数。 请参见第 940 页的“ 使用 Network Discover 扫描限制优化资源 ”。

扫描 Windows 计算机上的 C 驱动器的配置示例

扫描 Windows 计算机上的 C 驱动器。

该配置位于文件 VontuFileSystemScanner.cfg 中。

请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。

```
DirectoryPathCSVs=C:\  
DirectoryMustHaveCSVs=  
DirectoryCantHaveCSVs=
```

在 UNIX 上扫描 /usr 目录的配置示例

在 UNIX 计算机上扫描 /usr 目录。

该配置位于文件 VontuFileSystemScanner.cfg 中。

请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。

```
DirectoryPathCSVs=/usr
DirectoryMustHaveCSVs=
DirectoryCantHaveCSVs=
```

使用包括过滤器进行扫描的配置示例

使用包括过滤器扫描所选的文件和目录。

该配置位于文件 VontuFileSystemScanner.cfg 中。

请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。

仅包括目录 C:\Windows 下路径中包含 temp 的文件。

```
DirectoryPathCSVs=C:\Windows
DirectoryMustHaveCSVs=*/temp/*
DirectoryCantHaveCSVs=
```

仅包括路径中以扩展名 tmp 结尾或目录名称中包含 xml 的文件。

```
DirectoryPathCSVs=C:\Windows
DirectoryMustHaveCSVs=*/xml/*, *.tmp
DirectoryCantHaveCSVs=
```

仅包括 UNIX 目录 /home/data 下以扩展名 txt 结尾的文件。

```
DirectoryPathCSVs=/home/data
DirectoryMustHaveCSVs=*.txt
DirectoryCantHaveCSVs=
```

使用排除过滤器进行扫描的配置示例

使用排除过滤器扫描所选的文件和目录。

该配置位于文件 VontuFileSystemScanner.cfg 中。

请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。

排除目录 C:\Windows 下扩展名为 exe 的所有文件。

```
DirectoryPathCSVs=C:\Windows
DirectoryMustHaveCSVs=
DirectoryCantHaveCSVs=*.exe
```

排除 UNIX 目录 /home/data 下以扩展名 tmp 结尾或目录名称中包含 bin 的所有文件。

```
DirectoryPathCSVs=/home/data  
DirectoryMustHaveCSVs=  
DirectoryCantHaveCSVs=*/bin/*, *.tmp
```

使用包括和排除过滤器进行扫描的配置示例

结合使用包括和排除过滤器扫描所选的文件和目录。

该配置位于文件 `VontuFileSystemScanner.cfg` 中。

请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。

扫描路径中包含 `temp` 或以 `pdf` 结尾的所有目录。排除目录 `C:\data` 中位于 `bin` 目录或以 `tmp` 结尾的所有文件。

```
DirectoryPathCSVs=C:\data  
DirectoryMustHaveCSVs=*/temp/*, *.pdf  
DirectoryCantHaveCSVs=*/bin/*, *.tmp
```

使用日期过滤进行扫描的配置示例

您可以通过参数 `DirectoryBeforeDate` 和 `DirectoryAfterDate` 指定一个日期范围，文档必须在此范围内得到修改以便扫描程序处理。

使用参数 `DirectoryAfterDate` 输入相对于当前日期的天数，在此日期后，必须对文档进行修改。负数将指定过去的日期。

使用参数 `DirectoryBeforeDate` 输入相对于当前日期的天数，在此日期之前，必须对文档进行修改。

在该实例中，需要结合使用 `DirectoryBeforeDate` 和 `DirectoryAfterDate`。

该配置位于文件 `VontuFileSystemScanner.cfg` 中。

请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。

扫描过去六个月中修改的所有 `pdf` 文件。

```
DirectoryMustHaveCSVs=*.pdf  
DirectoryAfterDate=-180  
DirectoryBeforeDate=0
```

扫描过去 60 天到 360 天之间修改的所有文件。

```
DirectoryAfterDate=-360  
DirectoryBeforeDate=-60
```

使用文件大小过滤进行扫描的配置示例

使用文件大小过滤扫描文件以限制扫描内容。

该配置位于文件 VontuFileSystemScanner.cfg 中。

请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。

扫描大小范围在 3000 到 4000 个字节的所有文件。不要导入该大小范围外的任何文件。

```
ImportPreImportMinLength=3000
ImportPreImportMaxLength=4000
ImportEmptyFiles=false
```

扫描大于 4 KB 的所有 doc 文件。

```
DirectoryMustHaveCSVs=*.doc
ImportPreImportMinLength=4096
ImportEmptyFiles=false
```

在 UNIX 系统中跳过符号链接的扫描的配置示例

扫描 UNIX 系统，但是跳过所有符号链接。

指定一个包含扫描程序应扫描的所有文件的文件。在运行过程中仅扫描这些文件。将此文件放在扫描程序安装目录外。在该示例中，将此文件命名为 /opt/test/filenames.txt。

该配置位于文件 VontuFileSystemScanner.cfg 中。

请参见第 1055 页的“[文件系统扫描程序的配置选项](#)”。

请务必对 DirectoryPathCSVs 和相关参数添加注释。并且，确保参数 PollingMethod 在配置文件中仅出现一次。

```
PollingMethod=1
FilePollFilename=/opt/test/filenames.txt
```


设置 Microsoft Exchange Server 扫描

本章节包括下列主题：

- [设置 Microsoft Exchange Server 扫描](#)
- [支持的 Exchange 扫描程序目标](#)
- [检查 Exchange 邮箱存储权限](#)
- [安装 Exchange 扫描程序](#)
- [Exchange 扫描程序的配置选项](#)
- [对配置文件名进行配置](#)
- [配置 DNMailbox 的设置](#)
- [启动 Microsoft Exchange 扫描](#)
- [扫描 Exchange 存档公用文件夹的配置示例](#)
- [扫描 Exchange 收件箱的配置示例](#)
- [扫描其他用户收件箱的配置示例](#)
- [扫描所有 Exchange 邮箱的配置示例](#)

设置 Microsoft Exchange Server 扫描

Exchange 扫描程序是一个独立实用程序，可以用来从 Microsoft Exchange 提取数据并将数据发送至 Network Discover 进行内容处理。

Exchange 扫描程序使用连接的 Outlook 客户端访问 Exchange Server 上的客户端邮箱。

Exchange 扫描程序允许您指定应使用哪个 MAPI 配置文件从 Exchange 结构中提取数据。Exchange 扫描程序使用配置文件通过 MAPI 接口连接至 Exchange Server，然后将文件发布到 Discover。

可以使用 Exchange 扫描程序执行以下任务：

- 使用特定帐户扫描公用文件夹以查找机密数据。
- 使用可以访问所有邮箱的管理员帐户扫描所有邮箱。
- 使用管理员帐户扫描特定用户的邮箱。
- 在知道用户名和密码的情况下扫描单个用户的邮箱。

要设置 Microsoft Exchange Server 扫描，请完成以下过程：

表 67-1 设置 Exchange 扫描程序

步骤	操作	说明
1	确认您的 Exchange Server 是 2003 版还是 2007 版。	请参见第 1062 页的“ 支持的 Exchange 扫描程序目标 ”。
2	在安装了 Microsoft Outlook 2003 或 2007 并配置了有效 Outlook 配置文件的任何计算机上安装 Exchange 扫描程序。	请参见第 1064 页的“ 安装 Exchange 扫描程序 ”。
3	配置 ProfileName 以及 DNMailbox 的设置。	请参见第 1069 页的“ 对配置文件名进行配置 ”。 请参见第 1069 页的“ 配置 DNMailbox 的设置 ”。
4	通过编辑配置文件和属性文件执行所有手动配置。	请参见第 1066 页的“ Exchange 扫描程序的配置选项 ”。
5	在 Enforce Server 上，添加新的 Exchange 目标。	请参见第 926 页的“ 添加新的 Network Discover 目标 ”。
6	启动 Exchange 扫描。 启动扫描程序计算机上的扫描程序，并在 Enforce Server 上启动扫描。	请参见第 1053 页的“ 启动文件系统扫描 ”。
7	验证扫描是否正在顺利进行。	请参见第 1042 页的“ 排除扫描程序故障 ”。

支持的 Exchange 扫描程序目标

Exchange 扫描程序支持扫描下列目标：

■ Microsoft Exchange Server 2003

■ Microsoft Exchange Server 2007

必须配置附带有效 Outlook 配置文件的 Outlook 2003 或 Outlook 2007。Exchange 扫描程序使用 Outlook 连接到 Exchange Server 并提取数据。Outlook 2003 或 2007 必须安装在运行扫描程序的计算机上。必须对 Outlook 进行配置，使其与要扫描的 Exchange Server 进行通信。

有关设置 Outlook 2003 或 Outlook 2007 的步骤，请参考以下链接。

<http://support.microsoft.com/kb/829918>

Exchange 扫描包括客户端邮箱中的电子邮件文件格式的 Exchange 项目 (.EML 文件) 和文件附件，并会扫描压缩文件的内容。

可以扫描存储在公用文件夹内的数据对象。

但是，Exchange 扫描程序不会扫描存储在“个人文件夹” (.pst 文件) 或脱机文件夹 (.ost 文件) 中的邮件。对于扫描 .pst 文件，请使用共享文件系统目标。

请参见第 988 页的“[配置 Microsoft Outlook 个人文件夹 \(.pst 文件\) 扫描](#)”。

Exchange 扫描程序不会监控使用 MAPI、SMTP、POP3 或 HTML Web 邮件发送的入站或出站邮件。可使用 Symantec Data Loss Prevention 的其他产品来处理 POP3 或 HTML Web 邮件扫描类型。

注意：此扫描程序应该仅安装在 32 位 Windows 服务器上。

请参见第 881 页的“[实施 Network Monitor](#)”。

请参见第 891 页的“[实施 Network Prevent for Email](#)”。

检查 Exchange 邮箱存储权限

Exchange 扫描程序会扫描 Outlook 配置文件具有权限的邮箱或公用文件夹。例如，可以使用 Windows 管理员凭据和管理级别的 Outlook 配置文件登录客户端。然后即可扫描该配置文件具有访问权限的所有邮箱或公用文件夹。如果使用用户 A 的配置文件登录，则只能扫描用户 A 具有访问权限的条目，通常是用户 A 的个人邮箱。

当使用管理帐户扫描其他用户的邮箱时，该帐户必须具有所有邮箱的访问权限。该帐户也必须具有对 Exchange Server 的“邮箱存储”对象的访问权限。

检查 Exchange 2003 的邮箱存储权限

- 1 打开“[Exchange 系统管理器](#)”。
- 2 查找“邮箱存储”对象并右键单击该对象。

- 3 选择“属性”
- 4 选择“安全”选项卡。

检查 Exchange 2007 的邮箱存储权限

- 1 打开 Exchange Management Shell。

Microsoft 的 [Exchange Management Shell](#) 信息。

运行下列命令：

```
Add-ExchangeAdministrator -Role ViewOnlyAdmin -Identity MyDomain\My_User
```

- 2 打开 **Exchange Management Console**。
- Microsoft 的 [Exchange Management Console](#) 信息。
- 3 在“组织配置”>“**Exchange 管理员**”>“操作”下，选择“添加 **Exchange 管理员**”。
- 4 选择作为 Exchange 管理员添加的用户或组。选择角色“**Exchange 仅查看管理员角色**”。

安装 Exchange 扫描程序

在安装了 Microsoft Outlook 2003 或 Outlook 2007 并具有有效 Outlook 配置文件的任何 Windows 计算机上安装 Exchange 扫描程序。

在运行 Exchange 扫描程序的计算上必须安装 [Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package ATL 安全更新](#)。如果未安装此运行时库，则 Exchange 扫描程序无法启动。

使用 IndexAllAccounts=true 时，必须使用具有所有邮箱的读取权限的用户的配置文件。检查您对 Exchange “邮箱存储”的权限。

请参见第 1063 页的“[检查 Exchange 邮箱存储权限](#)”。

安装 Exchange 扫描程序

- 1 使用对所有文件具有完全访问权限的 Windows 管理员帐户登录要安装 Exchange 扫描程序的计算机。
该计算机应正在运行具有有效 Outlook 配置文件的 Microsoft Outlook 2003 或 Outlook 2007，并且可以访问 Exchange Server。
- 2 将安装程序 (ExchangeScanner_windows_x32_11.6.exe) 下载或复制（作为二进制文件）到临时目录。该文件位于 *DLP_Home\Symantec_DLP_11_Win\Scanners* 中，其中 *DLP_Home* 是解压缩 Symantec Data Loss Prevention 软件的目录的名称。

注意：此扫描程序应该仅安装在 32 位 Windows 服务器上。

- 3 运行 Exchange 扫描程序安装程序，并按照屏幕上的说明进行操作。
- 4 在 Welcome 屏幕中，单击 **Next**。
- 5 选择 Destination Directory（想要将 Vontu Exchange Scanner 安装到的文件夹）。
默认值为 `c:\Program Files\ExchangeScanner\`。
单击 **Next**。
- 6 选择开始菜单文件夹（“开始”菜单中的快捷方式）。
默认值为 **Vontu Exchange Scanner**。
单击 **Next**。
- 7 输入 Network Discover Server 的以下连接信息：
 - 发现主机（Network Discover Server 的 IP 或主机名）
 - 发现端口。
单击 **Next**。
- 8 输入以下信息来配置与 Exchange Server 的连接。
 - Profile Name
用于连接到 Exchange Server 以进行扫描的 MAPI 配置文件（及关联的权限）
 - Start Folder
要扫描的文件夹（仅在默认情况 `IndexAllAccounts=false` 时才适用）。
单击 **Next**。
- 9 安装扫描程序。

10 选择 Startup Mode。

扫描程序必须以拥有在配置文件中指定的配置文件的相同用户身份运行。

在最初测试或验证扫描程序是否可成功运行时，不要选择这些选项，而是手动启动扫描程序。

可以选择以下选项之一（或不选）：

- 作为 Windows 系统上的服务安装。

要作为服务运行，在安装完成后，需要为名为 **Vontu ExchangeScanner Service** 的服务设置适当的凭据。

在安装了扫描程序的计算机上，请打开“开始”>“设置”>“控制面板”>“管理工具”>“服务”。查找名为 **VontuExchangeScannerService** 的本地服务。右键单击此服务，选择“属性”。单击“登录”选项卡。选择“此帐户”。然后输入具有适当凭据的用户的用户名和密码。

- 安装后启动。

11 单击 **Next**，然后单击 **Finish**。

12 打开文件 `VontuExchangeScanner.cfg` 进行编辑。

请参见第 1066 页的“[Exchange 扫描程序的配置选项](#)”。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

`Job0.log` 文件中的 `Exchange` 文件夹结构有助于确定用于 `StartFolder` 的值。要查看 `Exchange` 文件夹结构，请在启动扫描程序之前将 `ShowFolderStructure` 参数设置为 `true`。

13 保存所做的更改并关闭配置文件。

14 在 Web 浏览器中打开 Enforce Server 管理控制台，并添加新的 Exchange 目标。

请参见第 929 页的“[Network Discover 扫描目标配置选项](#)”。

15 在扫描程序计算机和 Enforce Server 上同时启动扫描。

请参见第 1069 页的“[启动 Microsoft Exchange 扫描](#)”。

Exchange 扫描程序的配置选项

表 67-2 提供了 `VontuExchangeScanner.cfg` 文件的说明。

表 67-2 VontuExchangeScanner.cfg 文件中的参数

类型	参数	说明
扫描的内容 (公用文件夹或单个邮箱)	ProfileName	<p>要连接至 Microsoft Exchange Server 的 Microsoft Outlook 配置文件的名称。配置文件名称可能与用户名不同。</p> <p>请参见第 1069 页的“对配置文件名进行配置”。</p>
扫描的内容 (公用文件夹或单个邮箱)	StartFolder	<p>从中开始提取数据的文件夹。StartFolder 值区分大小写。</p> <p>StartFolder 值不允许以斜杠结尾。使用 IPM_SUBTREE\Inbox，而不是 IPM_SUBTREE\Inbox\。</p> <p>要扫描的文件夹仅在 IndexAllAccounts=false 时才适用。</p> <p>Exchange 文件夹结构位于 Job0.log 文件中。此文件夹结构有助于确定用于 StartFolder 参数的值。</p> <p>配置中的 StartFolder 值取决于为配置文件配置的“缓存 Exchange 模式”。 “缓存 Exchange 模式”是 Microsoft Outlook 内的一种设置，会影响从 Microsoft Exchange Server 收集数据的方式。以缓存模式运行会阻止 Outlook 持续从服务器请求新信息。请参见 http://office.microsoft.com/en-us/outlook/CH010045991033.aspx</p> <p>在 Outlook 配置文件中，如果“缓存 Exchange 模式”为 false (未选中)，则“信息存储的顶部”是邮箱的顶部文件夹。在这种情况下，收件箱的 StartFolder 值是 StartFolder=Top of Information Store\Inbox。</p> <p>如果“缓存 Exchange 模式”设置为 true (已选中)，则 IPM_SUBTREE 是根目录。在这种情况下，收件箱的 StartFolder 值是 StartFolder=IPM_SUBTREE\Inbox。</p>
扫描的内容 (公用文件夹或单个邮箱)	Password	<p>MAPI 配置文件的密码。</p> <p>如果密码存储在配置文件中，应当对其进行加密。</p> <p>请参见第 934 页的“加密配置文件中的密码”。</p>

类型	参数	说明
扫描的内容 (公用文件夹或单个邮箱)	ShowFolderStructure	<p>如果为 true, 会将 Exchange Server 文件夹结构输出到 Job0.log 文件 (仅在 IndexAllAccounts=false 时才适用)。</p> <p>ShowFolderStructure 的默认值是 false。</p> <p>此文件夹结构有助于确定用于 StartFolder 参数的值。</p> <p>如果公用文件夹的结构过大, 则将整个树结构写入到日志文件中可能需要几个小时。另一种选择是用 Microsoft Exchange Server MAPI Editor 来确定 StartFolder 值。请参见 http://www.microsoft.com/downloads/details.aspx?FamilyID=55fdffd7-1878-4637-9808-1e21abb3ae37&displaylang=en</p> <p>在大多数情况下, 确定文件夹结构后, 应将 ShowFolderStructure 设为 false。</p>
扫描的内容 (公用文件夹或单个邮箱)	Incremental	<p>如果为 true, 则只会扫描自上次扫描之后的新邮件。必须同时在 ScannerController.properties 文件中设置 scanner.incremental=true。</p> <p>为了使增量模式扫描程序能够正常运行, 扫描程序先前的运行必须都已成功完成。如果在完成前中止了运行, 则无法使用 Incremental 参数。</p>
扫描的内容 (所有邮箱)	IndexAllAccounts	<p>如果为 true, 则扫描所有邮箱。通过 DNMailbox 所指定的帐户必须具有足够的权限。您必须使用对所有邮箱具有读取权限的用户的配置文件。此用户不需要是管理员。</p> <p>检查您对 Exchange “邮箱存储”的权限。</p> <p>请参见第 1063 页的“检查 Exchange 邮箱存储权限”。</p>
扫描的内容 (所有邮箱)	DNMailbox	<p>用于登录服务器的邮箱或帐户的判别名 (仅在 IndexAllAccounts = true 时才适用)。</p> <p>请参见第 1069 页的“配置 DNMailbox 的设置”。</p>
扫描的内容 (所有邮箱)	Mailbox	邮箱的判别名。忽略以扫描所有邮箱。
限制和扫描控制	BatchSize	将文件导入发送到 Network Discover 的每个 XML 文件之前已聚合的文件数量。 请参见第 940 页的“ 使用 Network Discover 扫描限制优化资源 ”。

对配置文件名进行配置

Exchange 扫描程序使用配置的 Outlook 配置文件来扫描 Exchange Server。

对配置文件名进行配置

- 1 导航至“控制面板”>“邮件”>“显示配置文件”。
- 2 找到针对您的 Exchange 配置的 MAPI 配置文件。
- 3 在 VontuExchangeScanner.cfg 文件中输入 ProfileName 的值。

请参见第 1066 页的“[Exchange 扫描程序的配置选项](#)”。

配置 DNMailbox 的设置

找到 DNMailbox 的值，并配置 VontuExchangeScanner.cfg 文件中的参数。

配置 DNMailbox 的设置

- 1 从下列位置下载 Active Directory Services Interface (ADSI) Edit 支持工具。
<http://technet2.microsoft.com/windowsserver/en/library/eBCA3324-5427-471a-bc19-9aa1decd3d401033.mspx?mfr=true>
- 2 安装 ADSI Edit 支持工具。
ADSI Edit 支持工具通常安装于以下位置：
`c:\Program Files\Support Tools\adsiedit.msc`
- 3 要查找 DNMailbox 值的设置，请打开 ADSI Edit 应用程序并找到 DNMailbox 值。
例如，该值为“管理员用户”的 legacyExchangeDN 属性值。在 Exchange 配置中的位置可能不同。
请注意，DNMailbox 值区分大小写。
- 4 在 VontuExchangeScanner.cfg 文件中输入 DNMailbox 值。
请参见第 1066 页的“[Exchange 扫描程序的配置选项](#)”。

启动 Microsoft Exchange 扫描

确保在目标计算机上安装并配置扫描程序，并在 Enforce Server 上添加新目标。

请参见第 1064 页的“[安装 Exchange 扫描程序](#)”。

然后，您可以启动扫描。

下列每种情景对应的过程是不同的：

- 一个目标对应一个扫描程序（第一个过程）。
- 一个目标对应多个扫描程序（第二个过程）。

启动 Exchange 扫描（一个目标对应一个扫描程序）

- 1 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

- 2 从目标列表中选择扫描目标，然后单击“开始”图标。
- 3 在扫描程序计算机上，启动 Exchange 扫描程序。

单击“开始”>**Vontu Exchange Scanner > Vontu Exchange Scanner Console**。

要作为控制面板运行，请使用有效的用户帐户登录计算机，或在启动扫描程序时使用 run as 命令。

- 4 扫描程序启动扫描数据进程。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

- 5 如果扫描不能正常进行，您可以对其进行故障排除。
- 请参见第 1042 页的“[排除扫描程序故障](#)”。

- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

启动 Exchange 扫描（一个目标对应多个扫描程序）

- 1 在每台扫描程序计算机上，启动 Microsoft Exchange Scanner。

单击“开始”>**Vontu Exchange Scanner > Vontu Exchange Scanner Console**。

要作为控制面板运行，请使用有效的用户帐户登录计算机，或在启动扫描程序时使用 run as 命令。

确保每个扫描程序都已启动并且都已发布信息。检查每台计算机上的 outgoing 文件夹。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

- 2 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

- 3 从目标列表中选择扫描目标，然后单击“开始”图标。

- 4 扫描程序启动扫描数据进程。
请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。
- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的“[排除扫描程序故障](#)”。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

扫描 Exchange 存档公用文件夹的配置示例

扫描存档公用文件夹。

该配置位于 VontuExchangeScanner.cfg 文件中。

请参见第 1066 页的“[Exchange 扫描程序的配置选项](#)”。

```
//#####
//# Jobs
//#####
[Jobs]
Number=1
0=Job0

[Job0]
ProfileName=Administrator
Password=mypassword
StartFolder=IPM_SUBTREE\Archive
```

扫描 Exchange 收件箱的配置示例

扫描某个用户配置文件的收件箱。

该配置位于 VontuExchangeScanner.cfg 文件中。

请参见第 1066 页的“[Exchange 扫描程序的配置选项](#)”。

```
//#####
//# Jobs
//#####
[Jobs]
Number=1
0=Job0

[Job0]
```

```
ProfileName=some-user
Password=some-password
StartFolder=IPM_SUBTREE\Inbox
```

扫描其他用户收件箱的配置示例

使用管理员配置文件扫描用户 TEST2 的收件箱。

检查您对 Exchange “邮箱存储”的权限。

请参见第 1063 页的“[检查 Exchange 邮箱存储权限](#)”。

该配置位于 VontuExchangeScanner.cfg 文件中。

请参见第 1066 页的“[Exchange 扫描程序的配置选项](#)”。

```
//#####
//# Jobs
//#####
[Jobs]
Number=1
0=Job0

[Job0]
ProfileName=Administrator
Password=mypassword

IndexAllAccounts = true
DNMailbox=/o=Dar Test Lab/ou=First Administrative Group
/cn=Recipients/cn=Administrator

Mailbox=/O=DAR TEST LAB
/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS
/CN=TEST2
StartFolder=Top of Information Store\Inbox
```

扫描所有 Exchange 邮箱的配置示例

扫描所有的邮箱。

检查您对 Exchange “邮箱存储”的权限。

请参见第 1063 页的“[检查 Exchange 邮箱存储权限](#)”。

该配置位于 VontuExchangeScanner.cfg 文件中。

请参见第 1066 页的“[Exchange 扫描程序的配置选项](#)”。

```
//#####
//# Jobs
//#####
[Jobs]
Number=1
0=Job0

[Job0]
IndexAllAccounts=true
ProfileName=Administrator
Password=mypassword
DNMailbox=/o=Dar Test Lab/ou=First Administrative Group
/cn=Recipients/cn=Administrator
```

1074 | 设置 Microsoft Exchange Server 扫描
扫描所有 Exchange 邮箱的配置示例

设置 SharePoint 2007 服务器扫描

本章节包括下列主题：

- [设置 SharePoint 2007 服务器扫描](#)
- [支持的 SharePoint 扫描程序目标](#)
- [SharePoint 2007 扫描的访问权限](#)
- [安装 SharePoint 2007 扫描程序](#)
- [启动 SharePoint 2007 扫描](#)
- [SharePoint 2007 扫描程序的配置选项](#)
- [扫描特定站点集合的配置示例](#)
- [扫描特定网站的配置示例](#)
- [扫描 Web 应用程序中所有网站的配置示例](#)
- [扫描服务器上所有 Web 应用程序中所有网站的配置示例](#)
- [调度 SharePoint 2007 扫描](#)

设置 SharePoint 2007 服务器扫描

SharePoint 2007 扫描程序会扫描文档的最新修订并列出 Windows SharePoint Services 3.0 或 Microsoft Office SharePoint Server 2007 中的项目。然后，扫描程序将文件转换为标准格式并将其发送到 Network Discover Server 进行内容处理。

SharePoint 2007 扫描程序通过 Microsoft API 与 SharePoint 服务器通信。由于 Microsoft API 限制了通过 API 与 SharePoint 服务器通信的能力，因此必须在其中

一个 SharePoint 2007 Web 前端 (WFE) 服务器上安装扫描程序。只能通过直接安装在 SharePoint 服务器上的组件进行通信。

请参见第 1076 页的“[支持的 SharePoint 扫描程序目标](#)”。

请参见第 1077 页的“[SharePoint 2007 扫描的访问权限](#)”。

要设置 SharePoint 2007 服务器扫描，请完成以下过程：

表 68-1 设置 SharePoint 2007 扫描程序

步骤	操作	说明
1	验证 SharePoint 2007 服务器是否在支持的目标列表中。	请参见第 1076 页的“ 支持的 SharePoint 扫描程序目标 ”。
2	安装 SharePoint 2007 扫描程序。 扫描 SharePoint 2007 服务器的设置要求在 SharePoint 2007 部署的其中一个 Web 前端 (WFE) 服务器上安装扫描程序软件。	请参见第 1078 页的“ 安装 SharePoint 2007 扫描程序 ”。
3	设置允许 SharePoint 扫描的访问权限。	请参见第 1077 页的“ SharePoint 2007 扫描的访问权限 ”。
4	通过编辑配置文件和属性文件执行所有手动配置。	请参见第 1081 页的“ SharePoint 2007 扫描程序的配置选项 ”。
5	在 Enforce Server 上，添加新的扫描程序 SharePoint 2007 目标。	请参见第 926 页的“ 添加新的 Network Discover 目标 ”。
6	启动 SharePoint 2007 扫描。 启动 SharePoint 服务器上的扫描程序，并在 Enforce Server 上启动扫描。	请参见第 1079 页的“ 启动 SharePoint 2007 扫描 ”。
7	验证扫描是否正在顺利进行。	请参见第 1042 页的“ 排除扫描程序故障 ”。

支持的 SharePoint 扫描程序目标

扫描程序支持以下 SharePoint 目标：

- Windows Server 2003 32 位操作系统上的 Microsoft Office SharePoint 2007 Server

单独扫描程序安装可用于 SharePoint 2007 32 位服务器。对于 SharePoint 2007 32 位服务器，请使用下列 SharePoint 扫描程序安装文件：

`SharePoint2007Scanner_windows_x32_11.6.exe`

请参见第 1075 页的“[设置 SharePoint 2007 服务器扫描](#)”。

扫描程序必须安装在 SharePoint 2007 32 位服务器场的其中一个 Web 前端 (WFE) 服务器上。

Microsoft Visual C++ 2005 SP1 (32 位) Redistributable Package 必须安装在此计算机上。

[Microsoft 32 位下载链接。](#)

- Windows Server 2003 32 位或 64 位, 或 Windows 2008 R1 32 位或 64 位上的 Microsoft Office SharePoint 2007 Server。

单独扫描程序安装可用于 SharePoint 2007 64 位服务器。对于 SharePoint 2007 64 位服务器, 请使用下列 SharePoint 扫描程序安装文件。

SharePoint2007Scanner_windows_x64_11.6.exe

请参见第 1075 页的“[设置 SharePoint 2007 服务器扫描](#)”。

扫描程序必须安装在 SharePoint 2007 64 位服务器场的其中一个 Web 前端 (WFE) 计算机上。

Microsoft Visual C++ 2005 SP1 (64 位) Redistributable Package 必须安装在此计算机上。

[Microsoft 64 位下载链接。](#)

- SharePoint 2003

请参见第 1085 页的“[设置 SharePoint 2003 服务器扫描](#)”。

确保为您的 SharePoint 版本安装正确的 SharePoint 扫描程序。

SharePoint 2007 扫描的访问权限

此扫描程序进程必须在对 SharePoint 服务器具有适当访问权限的帐户下运行:

SharePoint 2007 扫描程序帐户向扫描程序提供 Windows 服务的权限。此帐户用于提供对带有 Windows SharePoint Services API 的 SharePoint 内容的访问权限, 并进行标准 WSS API 对象模型代码调用, 以在只读操作中枚举和检索 SharePoint 内容。

Microsoft 在与以下 Microsoft Technet 文章中指定的所有 Windows 或控制台应用程序进行交互时, 需要这些提升权限:

<http://support.microsoft.com/kb/935751/en-us>

在大多数 Sharepoint 环境中, 可以使用应用程序池帐户。

要扫描整个 SharePoint 2007 服务器, 请确保运行 SharePoint 2007 扫描程序的用户帐户具有以下权限:

- 本地和场管理员权限
- 数据库所有者对内容和 SharePoint 2007 的数据库配置的权限
- 站点集合管理员权限, 或完全控制所有 Web 应用程序的权限

- 对 SharePoint 2007 服务器上的所有资源的访问权限

安装 SharePoint 2007 扫描程序

此扫描程序必须安装在 SharePoint 2007 部署的其中一个 Web 前端 (WFE) 服务器上。

验证先决条件是否均已满足。

请参见第 1076 页的“[支持的 SharePoint 扫描程序目标](#)”。

安装并部署 SharePoint 2007 扫描程序

- 1 验证 SharePoint 存储库及前端的版本。

确保为您的 SharePoint 版本安装正确的 SharePoint 扫描程序。

请参见第 1076 页的“[支持的 SharePoint 扫描程序目标](#)”。

- 2 验证运行 SharePoint 2007 扫描程序的扫描程序进程是否具有适当的访问权限。

请参见第 1077 页的“[SharePoint 2007 扫描的访问权限](#)”。

- 3 在具有 SharePoint 2007 WFE 的计算机上，下载扫描程序安装文件。

对于 32 位 SharePoint 2007 服务器，将文件

`SharePoint2007Scanner_windows_x32_11.6.exe` 下载或复制（作为二进制文件）到临时目录。该文件位于 `DLP_Home\Symantec_DLP_11_Win\Scanners` 中，其中 `DLP_Home` 是解压缩 Symantec Data Loss Prevention 软件的目录的名称。

对于 64 位 SharePoint 2007 服务器，请使用文件

`SharePoint2007Scanner_windows_x64_11.6.exe`。

- 4 在 SharePoint 2007 WFE 上启动扫描程序安装程序。

- 5 查看 Welcome 屏幕，然后单击 **Next**。

- 6 选择安装 Destination Directory，即要安装 SharePoint 2007 扫描程序的文件夹。

默认值为 `c:\Program Files\SharePoint2007Scanner\`。

单击 **Next**。

- 7 选择开始菜单文件夹（“开始”菜单中的快捷方式）。

默认值为 **Vontu SharePoint2007 Scanner**。

单击 **Next**。

- 8 输入 Network Discover Server 的以下连接信息：

- 发现主机（Network Discover Server 的 IP 或主机名）

■ 发现端口。

9 单击 **Next**。

10 输入以下信息来配置 SharePoint 2007 扫描程序：

■ 包括过滤器

SharePoint 对象的 URL 必须包括此处所指定的字符串，才能提取以供扫描。过滤器仅适用于列表 URL 之前（包括列表 URL）的 URL 部分。使用逗号分隔条目，但不要使用空格。

■ 排除过滤器

如果某 SharePoint 对象的 URL 中出现其中任何一个字符串，则不会提取该对象。使用逗号分隔条目，但不要使用空格。

11 安装扫描程序。

12 选择 **Startup Mode**。

在最初测试或验证扫描程序是否可成功运行时，不要选择这些选项，而是手动启动扫描程序。

可以选择以下选项之一（或不选）：

■ 作为 Windows 系统上的服务安装。

■ 安装后启动。

默认值为手动启动扫描程序。

13 SharePoint 2007 WFE 上的 SharePoint 2007 扫描程序安装完成。

14 通过编辑配置文件和属性文件执行所有手动配置。

请参见第 1081 页的“[SharePoint 2007 扫描程序的配置选项](#)”。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

请参见第 1045 页的“[扫描程序配置文件](#)”。

15 在 Enforce Server 上，为扫描程序 SharePoint 2007 类型创建一个新目标。

请参见第 926 页的“[添加新的 Network Discover 目标](#)”。

16 在扫描程序计算机和 Enforce Server 上同时启动扫描。

请参见第 1079 页的“[启动 SharePoint 2007 扫描](#)”。

启动 SharePoint 2007 扫描

确保在目标计算机上安装并配置扫描程序，并在 Enforce Server 上添加新目标。

请参见第 1078 页的“[安装 SharePoint 2007 扫描程序](#)”。

然后，您可以启动扫描。

下列每种情景对应的过程是不同的：

- 一个目标对应一个扫描程序（第一个过程）。
- 一个目标对应多个 SharePoint 扫描程序（第二个过程）。

启动 SharePoint 2007 扫描（一个目标对应一个扫描程序）

- 1 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

- 2 从目标列表中选择扫描目标，然后单击“开始”图标。
- 3 在扫描程序计算机上，启动 SharePoint 2007 扫描程序。

单击“开始”>**Vontu SharePoint2007 Scanner**>**Vontu SharePoint2007 Scanner Console**。

运行 SharePoint 2007 扫描程序的用户必须具有适当的权限。

请参见第 1076 页的[“支持的 SharePoint 扫描程序目标”](#)。

- 4 扫描程序启动扫描数据进程。
请参见第 1041 页的[“Network Discover 扫描程序的工作原理”](#)。
- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的[“排除扫描程序故障”](#)。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

启动 SharePoint 2007 扫描（一个目标对应多个 SharePoint 扫描程序）

- 1 在每台扫描程序计算机上，启动 SharePoint 2007 扫描程序。

单击“开始”>**Vontu SharePoint2007 Scanner**>**Vontu SharePoint2007 Scanner Console**。

运行 SharePoint 2007 扫描程序的用户必须具有适当的权限。

请参见第 1076 页的[“支持的 SharePoint 扫描程序目标”](#)。

确保每个扫描程序都已启动并且都已发布信息。检查每台计算机上的outgoing 文件夹。

请参见第 1044 页的[“扫描程序安装目录结构”](#)。

- 2 登录到 Enforce Server。
转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。
- 3 从目标列表中选择扫描目标，然后单击“开始”图标。

- 4 扫描程序启动扫描数据进程。
请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。
- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的“[排除扫描程序故障](#)”。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

SharePoint 2007 扫描程序的配置选项

[表 68-2](#) 提供了 VontuSharePoint2007Scanner.cfg 文件的说明。

表 68-2 VontuSharePoint2007Scanner.cfg 文件中的参数

类型	参数	说明
扫描的内容	FetchMode	<p>指定要扫描的文档集。</p> <p>0 - 提取单个站点集合（由 StartURL 指定）中的信息。</p> <p>1 - 提取 Web 应用程序（由 StartURL 指定）中所有站点的信息。</p> <p>2 - 提取所有 Web 应用程序中的所有信息。</p>
扫描的内容	StartURL	指定启动扫描程序作业的 Web 应用程序或站点集合的 URL。
扫描的内容	SingleSiteName	如果指定了此参数，将只提取其“标题”与此字符串匹配的站点。
扫描的内容	MustHaveCSVs	<p>该参数是“包括过滤器”。如果某 SharePoint 对象的 URL 中没有出现其中任何一个字符串，则不会提取该对象。此过滤器仅适用于列表 URL 之前（包括列表 URL）的 URL 部分。</p> <p>使用逗号分隔条目，但不要使用空格。</p>
扫描的内容	CanHaveCSVs	<p>该参数是“排除过滤器”。如果某 SharePoint 对象的 URL 中出现其中任何一个字符串，则不会提取该对象。</p> <p>使用逗号分隔条目，但不要使用空格。</p>
扫描的内容	MaximumJobTime	在扫描程序作业停止之前，允许其运行的最大秒数。当该作业停止时，其状态将写入状态文件。

类型	参数	说明
限制	ImportPoliteness	指定导入模块在两个导入文档之间应等待的时间（毫秒）。
限制	BatchSize	将文件导入发送到 Network Discover 的每个 XML 文件之前已聚合的文件数量。 请参见第 940 页的“ 使用 Network Discover 扫描限制优化资源 ”。

扫描特定站点集合的配置示例

扫描特定站点集合。

该配置位于文件 VontuSharePoint2007Scanner.cfg 中。

请参见第 1081 页的“[SharePoint 2007 扫描程序的配置选项](#)”。

```
FetchMode=0
StartURL=http://sp2007/sites/Site1
SingleSiteName=Site_Title
```

扫描特定网站的配置示例

扫描特定网站。

该配置位于文件 VontuSharePoint2007Scanner.cfg 中。

请参见第 1081 页的“[SharePoint 2007 扫描程序的配置选项](#)”。

```
FetchMode=0
StartURL=http://sp2007/sites/Site1
SingleSiteName=Site_Title
```

扫描 Web 应用程序中所有网站的配置示例

扫描 Web 应用程序 sp2007:3856 中的所有网站。

该配置位于文件 VontuSharePoint2007Scanner.cfg 中。

请参见第 1081 页的“[SharePoint 2007 扫描程序的配置选项](#)”。

```
FetchMode=1
StartURL=http://sp2007:3856
```

扫描服务器上所有 Web 应用程序中所有网站的配置示例

扫描服务器上所有 Web 应用程序中的所有网站。

该配置位于文件 VontuSharePoint2007Scanner.cfg 中。

请参见第 1081 页的“[SharePoint 2007 扫描程序的配置选项](#)”。

```
FetchMode=2
```

调度 SharePoint 2007 扫描

以下示例显示如何调度 SharePoint 2007 扫描。

调度 SharePoint 2007 扫描

- 1 将参数 MaximumJobTime 添加到 Job0 部分（使用您希望作业运行的秒数）。
- 2 根据需要设置 ImportPoliteness。
- 3 要运行示例作业，请将以下内容输入到文件 VontuSharePoint2007Scanner.cfg 中。此作业最多运行五个小时，导入每个文档之间的时间限制设置为 15 秒，批处理大小为 10。

请参见第 1081 页的“[SharePoint 2007 扫描程序的配置选项](#)”。

```
FetchMode=2  
MaximumJobTime=18000  
ImportPoliteness=15000  
BatchSize=10
```

- 4 编辑 **Vontu SharePoint2007Scanner** 服务的凭据，以使用管理员凭据。
- 5 使用以下内容创建批处理文件：

```
net stop "Vontu SharePoint2007Scanner Service" &  
net start "Vontu SharePoint2007Scanner Service"
```
- 6 将扫描程序设置为以增量模式运行，方法是在 ScannerController.properties 文件中将参数 scanner.incremental 值设置为 true。
请参见第 1046 页的“[扫描程序控制器配置选项](#)”。
- 7 使用 Windows Scheduled Task 将任务调度为在每天的所需时间运行批处理文件。
- 8 将 Enforce Server 上的发现目标调度为在同一时间启动。

1084 | 设置 SharePoint 2007 服务器扫描
调度 SharePoint 2007 扫描

设置 SharePoint 2003 服务器扫描

本章节包括下列主题：

- [设置 SharePoint 2003 服务器扫描](#)
- [安装 SharePoint 2003 扫描程序](#)
- [启动 SharePoint 2003 扫描](#)
- [SharePoint 2003 扫描程序的配置选项](#)
- [扫描所有 SharePoint 2003 站点的配置示例](#)
- [扫描一个 SharePoint 2003 站点的配置示例](#)

设置 SharePoint 2003 服务器扫描

SharePoint 2003 扫描程序会扫描文档的最新修订并列出 SharePoint 2003 部署中的项目。

请参见第 1076 页的“[支持的 SharePoint 扫描程序目标](#)”。

要设置 SharePoint 2003 服务器扫描，请完成以下过程：

表 69-1 设置 SharePoint 2003 扫描程序

步骤	操作	说明
1	验证 SharePoint 2003 服务器是否在支持的目标列表中。	请参见第 1076 页的“ 支持的 SharePoint 扫描程序目标 ”。

步骤	操作	说明
2	安装 SharePoint 2003 扫描程序。 扫描 SharePoint 2003 服务器的设置要求在 SharePoint 2003 部署的其中一个前端计算机上安装扫描程序软件。	请参见第 1086 页的“ 安装 SharePoint 2003 扫描程序 ”。
3	通过编辑配置文件和属性文件执行所有手动配置。	请参见第 1089 页的“ SharePoint 2003 扫描程序的配置选项 ”。
4	在 Enforce Server 上，添加新的扫描程序 SharePoint 2003 目标。	请参见第 926 页的“ 添加新的 Network Discover 目标 ”。
5	启动 SharePoint 2003 扫描。 启动扫描程序计算机上的扫描程序，并在 Enforce Server 上启动扫描。	请参见第 1088 页的“ 启动 SharePoint 2003 扫描 ”。
6	验证扫描是否正在顺利进行。	请参见第 1042 页的“ 排除扫描程序故障 ”。

安装 SharePoint 2003 扫描程序

此扫描程序必须安装在 SharePoint 2003 部署的其中一个前端计算机上。

验证先决条件是否均已满足。

请参见第 1076 页的“[支持的 SharePoint 扫描程序目标](#)”。

此扫描程序进程必须在对 SharePoint 站点具有适当访问权限的帐户下运行。

安装并部署 SharePoint 2003 扫描程序

1 验证 SharePoint 存储库及前端的版本。

请参见第 1076 页的“[支持的 SharePoint 扫描程序目标](#)”。

2 在具有 SharePoint 2003 前端的计算机上，下载安装文件。将 SharePoint2003Scanner_windows_x32_11.6.exe 文件下载或复制（作为二进制文件）到临时目录。该文件位于 *DLP_Home\Symantec_DLP_11_Win\Scanners* 中，其中 *DLP_Home* 是解压缩 Symantec Data Loss Prevention 软件的目录的名称。

3 在 SharePoint 2003 前端上启动扫描程序安装程序。

SharePoint2003Scanner_windows_x32_11.6.exe

注意：此扫描程序应该仅安装在 32 位 Windows 服务器上。

- 4 查看 Welcome 屏幕，然后单击 **Next**。
- 5 选择安装 Destination Directory，即要安装 SharePoint 2003 扫描程序的文件夹。

默认值为 `c:\Program Files\SharePoint2003Scanner\`。

单击 **Next**。
- 6 选择开始菜单文件夹（“开始”菜单中的快捷方式）。

默认值为 **Vontu SharePoint2003 Scanner**。

单击 **Next**。
- 7 输入 Network Discover Server 的以下连接信息：
 - 发现主机（Network Discover Server 的 IP 或主机名）
 - 发现端口。
- 8 单击 **Next**。
- 9 输入以下信息来配置 SharePoint 2003 扫描程序：
 - 包括过滤器

SharePoint 对象的 URL 必须包括此处所指定的字符串，才能提取以供扫描。使用逗号分隔条目，但不要使用空格。
 - 排除过滤器

如果此处指定的字符串在 SharePoint 对象的 URL 中没有出现，则不会提取该对象以供扫描。使用逗号分隔条目，但不要使用空格。
- 10 安装扫描程序。
- 11 选择 Startup Mode。

在最初测试或验证扫描程序是否可成功运行时，不要选择这些选项，而是手动启动扫描程序。

可以选择以下选项之一（或不选）：

 - 作为 Windows 系统上的服务安装。
 - 安装后启动。

默认值为手动启动扫描程序。
- 12 扫描程序计算机上的 SharePoint 2003 扫描程序安装完成。
- 13 通过编辑配置文件和属性文件执行所有手动配置。

请参见第 1089 页的“[SharePoint 2003 扫描程序的配置选项](#)”。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

请参见第 1045 页的“[扫描程序配置文件](#)”。

- 14 在 Web 浏览器中打开 Enforce Server 管理控制台，并为扫描程序 SharePoint 2003 类型创建一个新目标。
- 15 在扫描程序计算机和 Enforce Server 上同时启动扫描。

请参见第 1088 页的“[启动 SharePoint 2003 扫描](#)”。

启动 SharePoint 2003 扫描

确保在目标计算机上安装并配置扫描程序，并在 Enforce Server 上添加新目标。

请参见第 1086 页的“[安装 SharePoint 2003 扫描程序](#)”。

然后，您可以启动扫描。

下列每种情景对应的过程是不同的：

- 一个目标对应一个扫描程序（第一个过程）。
- 一个目标对应多个扫描程序（第二个过程）。

启动 SharePoint 2003 扫描（一个目标对应一个扫描程序）

- 1 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

- 2 从目标列表中选择扫描目标，然后单击“开始”图标。
- 3 在扫描程序计算机上，启动 SharePoint 2003 扫描程序。

单击“开始”>**Vontu SharePoint2003 Scanner > Vontu SharePoint2003 Scanner Console**。

注意：此扫描程序进程必须在具有 SharePoint 站点的适当访问权限的帐户下运行。

- 4 扫描程序启动扫描数据进程。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

- 5 如果扫描不能正常进行，您可以对其进行故障排除。

请参见第 1042 页的“[排除扫描程序故障](#)”。

- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

启动 SharePoint 2003 扫描 (一个目标对应多个扫描程序)

1 在每台扫描程序计算机上，启动 SharePoint 2003 扫描程序。

单击“开始”>Vontu SharePoint2003 Scanner>Vontu SharePoint2003 Scanner Console。

注意：此扫描程序进程必须在具有 SharePoint 站点的适当访问权限的帐户下运行。

确保每个扫描程序都已启动并且都已发布信息。检查每台计算机上的outgoing文件夹。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

2 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

3 从目标列表中选择扫描目标，然后单击“开始”图标。

4 扫描程序启动扫描数据进程。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

5 如果扫描不能正常进行，您可以对其进行故障排除。

请参见第 1042 页的“[排除扫描程序故障](#)”。

6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

SharePoint 2003 扫描程序的配置选项

表 69-2 提供了 VontuSharePoint2003Scanner.cfg 文件的说明。

表 69-2 VontuSharePoint2003Scanner.cfg 文件中的参数

类型	参数	说明
扫描的内容	SharePointServer	SharePoint 服务器的 URL
扫描的内容	FetchMode	指定要扫描的文档集。 0 - 一个站点（由 SingleSiteName 参数指定） 1 - 所有站点

类型	参数	说明
扫描的内容	SingleSiteName	指定要扫描的文档的 SharePoint 站点名称。
扫描的内容	MustHaveCSVs	包含路径的包括过滤器的列表。使用逗号分隔条目，但不要使用空格。
扫描的内容	CanHaveCSVs	包含路径的排除过滤器的列表。使用逗号分隔条目，但不要使用空格。
扫描的内容	FileExtensionCSVs	文件扩展名列表。使用逗号分隔条目，但不要使用空格。
身份验证	Username	可以从 SharePoint 下载文档的用户的 Windows 用户名。
身份验证	Password	Username 参数中指定的用户的密码。加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。
身份验证	Domain	Username 参数中指定的用户的域。
限制	BatchSize	将文件导入发送到 Network Discover 的每个 XML 文件之前已聚合的文件数量。 请参见第 940 页的“ 使用 Network Discover 扫描限制优化资源 ”。

扫描所有 SharePoint 2003 站点的配置示例

使用过滤功能扫描所有站点。

该配置位于文件 VontuSharePoint2003Scanner.cfg 中。

请参见第 1089 页的“[SharePoint 2003 扫描程序的配置选项](#)”。

```
//#####
//# Jobs
//#####
[Jobs]
Number=1
0=Job0
[Job0]
SharePointServer = http://sharepoint_name.domain
MustHaveCSVs      = Document Library
```

```
CantHaveCSVs    = _catalogs
FetchMode = 1
```

扫描一个 SharePoint 2003 站点的配置示例

扫描一个站点。

该配置位于文件 VontuSharePoint2003Scanner.cfg 中。

请参见第 1089 页的“[SharePoint 2003 扫描程序的配置选项](#)”。

```
//#####
//# Jobs
//#####
[Jobs]
Number=1
0=Job0
[Job0]
SharePointServer = http://sharepoint_name.domain
FetchMode = 0
SingleSiteName = TestSite
```


设置 Web 服务器扫描

本章节包括下列主题：

- [设置 Web 服务器扫描](#)
- [支持的 Web 服务器（扫描程序）目标](#)
- [安装 Web 服务器扫描程序](#)
- [启动 Web 服务器扫描](#)
- [Web 服务器扫描程序的配置选项](#)
- [不使用身份验证的网站扫描的配置示例](#)
- [使用基本身份验证的网站扫描的配置示例](#)
- [使用基于表单的身份验证的网站扫描配置示例](#)
- [使用 NTLM 的网站扫描的配置示例](#)
- [网站扫描的 URL 过滤示例](#)
- [网站扫描的日期过滤示例](#)

设置 Web 服务器扫描

Web 服务器扫描程序可以检索网站文档。

Web 服务器扫描程序使用爬网程序查找和处理网页，以获得内容和到其他网站的链接。爬网程序从网站检索完文档后，Web 服务器扫描程序会将爬网程序检索到的内容导入到索引文件格式 (IDX) 文件。然后，扫描程序会将 IDX 文件发布到 Network Discover 进行内容处理。Web 服务器扫描程序可以从各种文档类型（包括 Web 文档、Word、Excel 和 PDF 文件）检索内容。

Web 服务器扫描程序会抓取网页以获得链接和内容。爬网程序处理页面内容，然后接受或拒绝该页面以进行检索。如果接受该页面，则爬网程序会查找页面中的链

接、过滤链接并将已接受的链接排入队列进行爬网程序处理。如果拒绝该页面，则只有将爬网程序配置为访问已拒绝页面上的链接时，爬网程序才会查找这些链接。在向爬网程序队列添加这些链接之前，会对其进行过滤。然后，爬网程序会检索已接受页面的页面内容。爬网程序会请求其队列中的下一个链接，并重复执行此过程。

要设置 Web 服务器扫描，请完成以下过程：

表 70-1 设置 Web 服务器扫描程序

步骤	操作	说明
1	Web 服务器扫描程序可以扫描网站。 该扫描程序已经过 IIS 和 Apache Web 服务器的测试。	请参见第 1094 页的“ 支持的 Web 服务器（扫描程序）目标 ”。
2	在对网站具有读取访问权限的服务器上，安装 Web 服务器扫描程序。	请参见第 1094 页的“ 安装 Web 服务器扫描程序 ”。
3	通过编辑配置文件和属性文件执行所有手动配置。	请参见第 1097 页的“ Web 服务器扫描程序的配置选项 ”。
4	在 Enforce Server 中，添加新的扫描程序文件系统目标。	请参见第 926 页的“ 添加新的 Network Discover 目标 ”。
5	启动文件系统扫描。 启动扫描程序计算机上的扫描程序，并在 Enforce Server 上启动扫描。	请参见第 1096 页的“ 启动 Web 服务器扫描 ”。
6	验证扫描是否正在顺利进行。	请参见第 1042 页的“ 排除扫描程序故障 ”。

支持的 Web 服务器（扫描程序）目标

Web 服务器扫描程序支持扫描静态 HTTP 网站。

安装 Web 服务器扫描程序

Web 服务器扫描程序必须安装在有权访问要扫描的网站的计算机上。

安装 Web 服务器扫描程序

- 1 在有权访问要扫描的网站的计算机上，将安装文件下载或复制（作为二进制文件）到临时目录。该文件位于 *DLP_Home\Symantec_DLP_11_Win\Scanners* 或 *DLP_Home\Symantec_DLP_11_Lin\Scanners* 目录中，其中，*DLP_Home* 是您先前将 Symantec Data Loss Prevention 软件解压缩到的目录名称。

如果在 Windows 计算机上安装 Web 服务器扫描程序，请使用以下文件：

`WebServerScanner_windows_x32_11.6.exe`

注意：此扫描程序应该仅安装在 32 位 Windows 服务器上。

如果在 Linux 计算机上安装 Web 服务器扫描程序，请使用以下文件：

`WebServerScanner_Unix_11.6.sh`

- 2 启动扫描程序安装。
- 3 选择安装的 **DestinationDirectory**（希望安装 Web 服务器扫描程序的目录）。单击 **Next**。
- 4 选择开始菜单文件夹（“开始”菜单中的快捷方式）。默认值为 **Vontu WebServer Scanner**。
单击 **Next**。
- 5 输入 Network Discover Server 的以下连接信息：
 - 发现主机（Network Discover Server 的 IP 或主机名）
 - 发现端口单击 **Next**。
- 6 通过输入以下信息来配置 Web 服务器扫描程序：
 - 起始 URL
输入扫描开始处的 URL。
 - 包括过滤器
仅扫描包含此处指定的所有字符串的路径。使用逗号分隔条目，但不要使用空格。支持通配符。
 - 路径排除过滤器
扫描除包含此处所指定字符串的路径以外的所有内容。使用逗号分隔条目，但不要使用空格。支持通配符。单击 **Next**。
- 7 安装扫描程序。

8 选择 Startup Mode。

在最初测试或验证扫描程序是否可成功运行时，不要选择这些选项，而是手动启动扫描程序。

可以选择以下选项之一（或不选）：

- 作为 Windows 系统上的服务安装。
- 安装后启动。

单击 **Next**。

单击 **Finish**。

9 完成 Web 服务器扫描程序在扫描程序计算机上的安装。

10 通过编辑配置文件和属性文件执行所有手动配置。

请参见第 1097 页的“[Web 服务器扫描程序的配置选项](#)”。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

请参见第 1045 页的“[扫描程序配置文件](#)”。

11 在 Enforce Server 上，为扫描程序 Web 服务器类型创建一个新目标。

12 在扫描程序计算机和 Enforce Server 上同时启动扫描。

请参见第 1096 页的“[启动 Web 服务器扫描](#)”。

启动 Web 服务器扫描

确保在目标计算机上安装并配置扫描程序，并在 Enforce Server 上添加新目标。

请参见第 1094 页的“[安装 Web 服务器扫描程序](#)”。

然后，您可以启动扫描。

下列每种情景对应的过程是不同的：

- 一个目标对应一个扫描程序（第一个过程）。
- 一个目标对应多个扫描程序（第二个过程）。

启动 Web 服务器扫描（一个目标对应一个扫描程序）

1 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

2 从目标列表中选择扫描目标，然后单击“开始”图标。

- 3 在扫描程序计算机上，启动 Web 服务器扫描程序。
单击“开始”>**Vontu WebServer Scanner**>**Vontu WebServer Scanner Console**。
- 4 扫描程序启动扫描数据进程。
请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。
- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的“[排除扫描程序故障](#)”。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

启动 Web 服务器扫描（一个目标对应多个扫描程序）

- 1 在每台扫描程序计算机上，启动 Web 服务器扫描程序。
单击“开始”>**Vontu WebServer Scanner**>**Vontu WebServer Scanner Console**。
确保每个扫描程序都已启动并且都已发布信息。检查每台计算机上的outgoing 文件夹。
请参见第 1044 页的“[扫描程序安装目录结构](#)”。
- 2 登录到 Enforce Server。
转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。
- 3 从目标列表中选择扫描目标，然后单击“开始”图标。
- 4 扫描程序启动扫描数据进程。
请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。
- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的“[排除扫描程序故障](#)”。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

Web 服务器扫描程序的配置选项

表 70-2 提供了 VontuWebServerScanner.cfg 文件的说明。

表 70-2 VontuWebServerScanner.cfg 文件中的参数

类型	参数	说明
扫描的内容	URL	爬网程序开始的有效 URL。如果您要检索多个页面，则起始网页必须包含到其他网页的链接。在配置参数中必须包括以 http:// 开头的 URL。
扫描的内容	NavDirAllowCSVs	包含路径的包括过滤器的列表。页面 URL 必须包含此列表中的字符串，扫描程序才能处理页面。使用参数 NavDirCheck 指定扫描程序如何以及何时检查这些字符串。 使用 * 表示通配符。使用逗号分隔条目，但不要使用空格。
扫描的内容	NavDirDisallowCSVs	包含路径的排除过滤器的列表。页面 URL 不得包含此列表中的字符串，否则扫描程序无法处理页面。使用参数 NavDirCheck 指定扫描程序如何以及何时检查这些字符串。 使用 * 表示通配符。使用逗号分隔条目，但不要使用空格。
扫描的内容	NavDirCheck	用于确定扫描程序何处以及如何检查 NavDirAllowCSVs 字符串和 NavDirDisallowCSVs 字符串的按位掩码号。如果页面的 URL 不包含任意一个 NavDirAllowCSVs 字符串或不包含任意一个 NavDirDisallowCSVs 字符串，则扫描程序不处理该页面。 请参见第 1101 页的“ 网站扫描的 URL 过滤示例 ”。
扫描的内容	扩展名	输入文件扩展名以限制扫描程序可以抓取的文档类型。要输入多个扩展名，请以逗号分隔。使用*表示通配符。逗号前后不含空格。 仅提取扩展名为 .doc 或 .html 的文档的示例： Extensions=* .doc,* .html*
扫描的内容	MaxLinksPerPage	一个页面可以包含的最大链接数。具有许多链接的页面通常是导航页面，可以使用此参数将其过滤掉。

类型	参数	说明
扫描的内容	StayOnSite	您可以将爬网程序配置为停留在开始的网站，或者允许爬网程序在起始网站之外的域中跟踪外部网站链接。默认情况下，爬网程序停留在起始网站域内。
扫描的内容	AfterDate	超过此天数后，在保存页面之前必须对页面进行修改。输入相对于当前日期的天数。负数将指定过去的日期。
扫描的内容	BeforeDate	在此天数之前，在保存页面之前必须对页面进行修改。输入相对于当前日期的天数。负数将指定过去的日期。
身份验证	LoginMethod	站点的身份验证方法。值必须是 AUTHENTICATE、FORMPOST 或 FORMGET。 请参见第 1100 页的“ 使用基本身份验证的网站扫描的配置示例 ”。 请参见第 1100 页的“ 使用基于表单的身份验证的网站扫描配置示例 ”。
身份验证	LoginURL	包括登录表单的页面。
身份验证	LoginUserName	供身份验证使用的用户名（纯文本或加密的文本）。
身份验证	LoginPassValue	供身份验证使用的密码。加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。
身份验证	LoginUserField	用户名表单字段（适用于 FORMPOST 或 FORMGET 登录方式）的名称。
身份验证	LoginPassField	密码表单字段（适用于 FORMPOST 或 FORMGET 登录方式）的名称。加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。
代理	ProxyHost	代理服务器的主机名或 IP 地址。
代理	ProxyPort	代理服务器的端口号。
代理	ProxyUsername	代理服务器的用户名（纯文本或加密）。
代理	ProxyPassword	代理服务器的密码。加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。
限制	PageDelay	下载一个页面和请求下一个页面之间的秒数。

类型	参数	说明
限制	BatchSize	聚合到发送至 Network Discover 的每个 XML 文件的文件数量。

不使用身份验证的网站扫描的配置示例

扫描不使用身份验证的网站。

该配置位于文件 `VontuWebServerScanner.cfg` 中。

请参见第 1097 页的“[Web 服务器扫描程序的配置选项](#)”。

```
//#####
//#   Jobs
//#####
URL=http://www.cnn.com
```

使用基本身份验证的网站扫描的配置示例

扫描使用标准身份验证进行保护的网站。

该配置位于文件 `VontuWebServerScanner.cfg` 中。

请参见第 1097 页的“[Web 服务器扫描程序的配置选项](#)”。

```
//#####
//#   Jobs
//#####
URL=http://site.domain.com
LoginURL=http://domain.server.com/login.html
LoginMethod=AUTHENTICATE
LoginUserValue=some_user
LoginPassValue=9sfIy8vw
```

使用基于表单的身份验证的网站扫描配置示例

扫描使用基于表单的身份验证进行保护的网站。

该配置位于文件 `VontuWebServerScanner.cfg` 中。

请参见第 1097 页的“[Web 服务器扫描程序的配置选项](#)”。

```
//#####
//#   Jobs
```

```
//#####
URL= http://wiki.symantec.corp/dashboard.action

LoginMethod=FORMPOST
LoginURL=http://wiki.symantec.corp/login.action

LoginUserField=os_username
LoginUserValue=some_user

LoginPassField=os_password
LoginPassValue=9sfIy8vw
```

使用 NTLM 的网站扫描的配置示例

扫描使用 NTLM 进行保护的网站。

确保 NTLMUsername 的格式为域\用户名。

该配置位于文件 VontuWebServerScanner.cfg 中。

请参见第 1097 页的“[Web 服务器扫描程序的配置选项](#)”。

```
//#####
//#    Jobs
//#####
URL=http://some_site
NTLMUsername=Some_Domain\some_domain_user
NTLMPassword=9sfIy8vw
```

网站扫描的 URL 过滤示例

使用参数 NavDirCheck 来确定扫描程序检查 NavDirAllowCSVs 字符串和 NavDirDisallowCSVs 字符串的位置和方式。

通过添加以下某些数字之和来创建 NavDirCheck 数：

参数	值	说明
URL	1	要使扫描程序检查页面的 URL 是否包含在参数 NavDirAllowCSVs 或 NavDirDisallowCSVs 中指定的任意字符串，必须输入 1。
不区分大小写	64	如果将 URL 值加 64，扫描程序会检查页面的 URL 是否与在参数 NavDirAllowCSVs 或 NavDirDisallowCSVs 中指定的字符串匹配。此匹配不区分大小写。

参数	值	说明
下载之前	128	如果将 URL 值加 128，扫描程序会在下载页面之前检查 URL 是否含有任意 NavDirAllowCSVs 或 NavDirDisallowCSVs 字符串。
有效站点结构	512	如果将 URL 值加 512，扫描程序会重新检查站点的 NavDirAllowCSVs 和 NavDirDisallowCSVs 值，以确保该站点在其更新之前仍然有效。如果不包含此设置，则永远不会检查对这些值的更改。如果站点无效，则不会对其进行下载。

在以下示例中，扫描程序会检查 URL 是否与字符串 archive 或 test 匹配。此匹配不区分大小写，且可匹配部分词或整个词。如果 URL 包含以下字符串之一，则不会处理页面。

```
NavDirDisallowCSVs=*archive*,*test*
NavDirCheck=65
```

在以下示例中，扫描程序会检查 URL 是否与字符串 news 或 home 匹配。此匹配不区分大小写，且可匹配部分词或整个词。如果 URL 不包含这些字符串之一，则不会处理页面。

```
NavDirAllowCSVs=*news*,*home*
NavDirCheck=65
```

网站扫描的日期过滤示例

下列示例检索在当前日期之前的第 365 天修改的文档和在当前日期之后的第 7 天修改的文档。

```
AfterDate=-365
BeforeDate=7
```

设置 Documentum 存储库扫描

本章节包括下列主题：

- [设置 Documentum 存储库扫描](#)
- [支持的 Documentum（扫描程序）目标](#)
- [安装 Documentum 扫描程序](#)
- [启动 Documentum 扫描](#)
- [Documentum 扫描程序的配置选项](#)
- [扫描 Documentum 存储库中所有文档的配置示例](#)

设置 Documentum 存储库扫描

Documentum 扫描程序会扫描 Documentum 存储库。

要设置 Documentum 存储库扫描，请完成以下过程：

表 71-1 设置 Documentum 扫描程序

步骤	操作	说明
1	验证 Documentum 存储库是否位于支持的目标列表中。	请参见第 1104 页的“ 支持的 Documentum（扫描程序）目标 ”。
2	在连接至托管 Documentum Document Broker 的计算机的任何计算机上，均可安装 Documentum 扫描程序。	请参见第 1104 页的“ 安装 Documentum 扫描程序 ”。

步骤	操作	说明
3	通过编辑配置文件和属性文件执行所有手动配置。	请参见第 1107 页的“ Documentum 扫描程序的配置选项 ”。
4	在 Enforce Server 上，添加新的扫描程序 Documentum 目标。	请参见第 926 页的“ 添加新的 Network Discover 目标 ”。
5	启动 Documentum 扫描。 启动扫描程序计算机上的扫描程序，并在 Enforce Server 上启动扫描。	请参见第 1106 页的“ 启动 Documentum 扫描 ”。
6	验证扫描是否正在顺利进行。	请参见第 1042 页的“ 排除扫描程序故障 ”。

支持的 Documentum (扫描程序) 目标

Documentum 扫描程序支持扫描 Documentum Content Server 5.3.x 存储库。

安装 Documentum 扫描程序

在连接至托管 Documentum Document Broker 的计算机的任何计算机上，均可安装 Documentum 扫描程序。

安装和部署 Documentum 扫描程序

- 1 在通过网络与托管 Documentum Document Broker 的计算机相连接的计算机上，下载安装文件。将 DocumentumScanner_windows_x32_11.6.exe 文件下载或复制（作为二进制文件）到临时目录。该文件位于 *DLP_Home\Symantec_DLP_11_Win\Scanners* 中，其中 *DLP_Home* 是解压缩 Symantec Data Loss Prevention 软件的目录的名称。
- 2 启动此计算机上的扫描程序安装程序。

DocumentumScanner_windows_x32_11.6.exe

注意：此扫描程序应该仅安装在 32 位 Windows 服务器上。

- 3 查看 Welcome 屏幕，然后单击 **Next**。

4 选择安装的 Destination Directory，也就是要安装 Documentum 扫描程序的文件夹。

默认值为 c:\Program Files\DocumentumScanner\。

单击 **Next**。

5 选择开始菜单文件夹（“开始”菜单中的快捷方式）。

默认值为 **Vontu Documentum Scanner**。

单击 **Next**。

6 输入 Network Discover Server 的以下连接信息：

■ 发现主机（Network Discover Server 的 IP 或主机名）

■ 发现端口

7 单击 **Next**。

8 输入扫描程序的下列 Documentum 配置值：

Doc Broker Host 存储 DocBase 存储库的服务器的名称。

Doc Base 您希望 Documentum 扫描程序检索的存储库的名称。

User Name 指定对您希望扫描的 Documentum 文件具有完全访问权限的帐户。

Password 帐户的密码。在配置文件中，此密码是纯文本。

WebTop Host Documentum 内容存储库的 Web 接口的主机名。

WebTop Port Web 接口的端口号。

9 单击 **Next**。

10 安装扫描程序。

11 选择 Startup Mode。

在最初测试或验证扫描程序是否可成功运行时，不要选择这些选项，而是手动启动扫描程序。

可以选择以下选项之一（或不选）：

■ 作为 Windows 系统上的服务安装。

■ 安装后启动。

默认值为手动启动扫描程序。

12 扫描程序计算机上的 Documentum 扫描程序安装完成。

13 通过编辑配置文件和属性文件执行所有手动配置。

请参见第 1107 页的“[Documentum 扫描程序的配置选项](#)”。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

请参见第 1045 页的“[扫描程序配置文件](#)”。

14 安装 Documentum 扫描程序之后，请将 dmc140.dll 文件从 Documentum 安装 bin 目录复制到扫描程序安装目录的 \DocumentumScanner\scanner 文件夹中。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

15 在 Enforce Server 上，为扫描程序 Documentum 类型创建一个新目标。

16 在扫描程序计算机和 Enforce Server 上同时启动扫描。

请参见第 1106 页的“[启动 Documentum 扫描](#)”。

启动 Documentum 扫描

确保在目标计算机上安装并配置扫描程序，并在 Enforce Server 上添加新目标。

请参见第 1104 页的“[安装 Documentum 扫描程序](#)”。

然后，您可以启动扫描。

下列每种情景对应的过程是不同的：

- 一个目标对应一个扫描程序（第一个过程）。
- 一个目标对应多个扫描程序（第二个过程）。

启动 Documentum 扫描（一个目标对应一个扫描程序）

1 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

2 从目标列表中选择扫描目标，然后单击“开始”图标。

3 在扫描程序计算机上，启动 Documentum 扫描程序。

单击“开始”>**Vontu Documentum Scanner**>**Vontu Documentum Scanner Console**。

4 扫描程序启动扫描数据进程。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的“[排除扫描程序故障](#)”。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

启动 Documentum 扫描 (一个目标对应多个扫描程序)

- 1 在每台扫描程序计算机上，启动 Documentum 扫描程序。
单击“开始”>**Vontu Documentum Scanner**>**Vontu Documentum Scanner Console**。
确保每个扫描程序都已启动并且都已发布信息。检查每台计算机上的outgoing文件夹。
请参见第 1044 页的“[扫描程序安装目录结构](#)”。
- 2 登录到 Enforce Server。
转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。
- 3 从目标列表中选择扫描目标，然后单击“开始”图标。
- 4 扫描程序启动扫描数据进程。
请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。
- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的“[排除扫描程序故障](#)”。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

Documentum 扫描程序的配置选项

表 71-2 提供了 VontuDocumentumScanner.cfg 文件的说明。

表 71-2 VontuDocumentumScanner.cfg 文件中的参数

参数	说明
DocBase	您希望 Documentum 检索的存储库名称。
UserName	指定对您希望扫描的 Documentum 文件具有访问权限的帐户。
Password	UserName 中所指定的帐户的密码。加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。

参数	说明
ExtensionCSVs	<p>要扫描的文件类型（包括过滤器）列表，例如：</p> <pre>ExtensionCSVs=*.doc,*.htm,*.ppt,*.xls</pre> <p>使用逗号分隔（不含空格）。</p>
ImportRefReplaceWithCSVs	<p>用于建构所扫描文档的 URL 的一个或两个值的列表（以逗号分隔）。</p> <p><i>first_value,second_value</i></p> <p>如果 Documentum 接口客户端是 Windows 桌面或桌面客户端，则会将第一个值连接至 document-id 的左侧，将第二个字符串连接至右侧，例如：</p> <p><i>first_value</i><i>document_id</i><i>second_value</i></p> <p>如果 Documentum Webtop（基于 Web）接口是您的客户端接口，则只需要一个值，例如：</p> <pre>ImportRefReplaceWithCSVs= http://documentum-server.mycompany.com:8080/ webtop/component/drl?objectId=</pre>
AfterDate	<p>扫描自此日期之后的文档。例如，如果您将 AfterDate 设置为 5 天，则只扫描时间不超过五天的文档。</p> <p>AfterDate 会查看上次修改日期。</p> <p>您可以输入以下其中一个值：</p> <p><i>N</i> 小时</p> <p><i>N</i> 天</p> <p><i>N</i> 周</p> <p><i>N</i> 个月</p> <p>Documentum 扫描程序不支持自动增量扫描，但是，您可以通过设置 AfterDate 和 BeforeDate 参数手动执行增量扫描。</p>

参数	说明
BeforeDate	扫描自此日期之后的文档。例如，如果您将AfterDate 设置为 5 天，则只扫描时间不超过五天的文档。AfterDate 会查看上次修改日期。 您可以输入以下其中一个值： N 小时 N 天 N 周 N 个月
FolderCSVs	指定从中提取文档的存储库文件夹。所有条目必须以斜杠开头，但不能只包括斜杠。将条目保留为空白可以指定所有文件夹。将压缩文件视为文件夹。例如： FolderCSVs=/support,/clients,/marketing,/finance

表 71-3 显示了 dmcl.ini 文件中的主机参数。

```
[DOCBROKER_PRIMARY]
host = documentum-server.mycompany.com
```

在 Symantec Data Loss Prevention 扫描程序安装期间，会在 dmcl.ini 文件中设置主机参数。如果稍后 Documentum Document Broker（服务器）发生更改，则必须编辑此文件，以指向新服务器。

表 71-3 dmcl.ini 文件

参数	说明
host	托管 Documentum Document Broker（服务器）的计算机。

扫描 Documentum 存储库中所有文档的配置示例

扫描存储库中的所有文档。

该配置位于文件 VontuDocumentumScanner.cfg 中。

请参见第 1107 页的“[Documentum 扫描程序的配置选项](#)”。

```
//#####
//#    Jobs
//#####
```

```
[JOBS]
NUMBER=1
0=Job0
[Job0]
DocBase=Vontu_1
UserName=Administrator
Password=mypassword
ImportRefReplaceWithCSVs=
    http://documentum-server.mycompany.com:8080/webtop/
    component/drl?objectId=
LogFile = Job0.log
```

设置 Livelink 存储库扫描

本章节包括下列主题：

- [设置 Livelink 存储库扫描](#)
- [持的 Livelink 扫描程序目标](#)
- [为 SQL Server 创建 ODBC 数据源](#)
- [安装 Livelink 扫描程序](#)
- [启动 Livelink 扫描](#)
- [Livelink 扫描程序的配置选项](#)
- [扫描 Livelink 数据库的配置示例](#)

设置 Livelink 存储库扫描

Livelink 扫描程序可扫描 Livelink 数据库。

要设置 Livelink 存储库扫描，请完成以下过程：

表 72-1 设置 Livelink 扫描程序

步骤	操作	说明
1	验证 Livelink 存储库是否位于支持的目标列表中。	请参见第 1112 页的“ 持的 Livelink 扫描程序目标 ”。
2	为 SQL Server 创建 ODBC 数据源。 安装 Livelink 扫描程序。	请参见第 1112 页的“ 为 SQL Server 创建 ODBC 数据源 ”。 请参见第 1113 页的“ 安装 Livelink 扫描程序 ”。

步骤	操作	说明
3	通过编辑配置文件和属性文件执行所有手动配置。	请参见第 1116 页的“ Livelink 扫描程序的配置选项 ”。
4	在 Enforce Server 上，添加新的扫描程序 Livelink 目标。	请参见第 926 页的“ 添加新的 Network Discover 目标 ”。
5	启动 Livelink 扫描。 启动扫描程序计算机上的扫描程序，并在 Enforce Server 上启动扫描。	请参见第 1115 页的“ 启动 Livelink 扫描 ”。
6	验证扫描是否正在顺利进行。	请参见第 1042 页的“ 排除扫描程序故障 ”。

持的 Livelink 扫描程序目标

Livelink 扫描程序支持扫描以下目标：

- Livelink Server 9.x

为 SQL Server 创建 ODBC 数据源

此过程假设 Livelink 数据库是 SQL Server 数据库。如果您有 Oracle Livelink 数据库，请联系 Symantec Data Loss Prevention 支持以获得特定说明。

为 SQL Server 创建 ODBC 数据源

- 1 转至“控制面板”>“管理工具”>“数据源(ODBC)”。
- 2 单击“系统 DSN”选项卡。
- 3 单击“添加”。
- 4 选择 SQL Server。
- 5 为其命名（例如 Livelink）。VontuLiveLinkScanner.cfg 文件中引用了此名称。
- 6 单击“下一步”。
- 7 选择“使用用户输入的登录 ID 和密码的 SQL Server 身份验证”。
- 8 选中“连接到 SQL Server”选项，以获取其他配置选项的默认设置，并输入 SQL Server凭据。您提供的凭据必须同时拥有对扫描目标的读取权限和写入属性权限。您需要有写入属性权限，才能更新“上次访问”日期。

9 单击“下一步”。接受默认设置。

10 单击“下一步”。接受默认设置。

11 单击“完成”。

安装 Livelink 扫描程序

在可以访问 Livelink 数据库的计算机上安装 Livelink 扫描程序。

安装 Livelink 扫描程序

1 为 SQL Server 创建 ODBC 数据源。

请参见第 1112 页的“[为 SQL Server 创建 ODBC 数据源](#)”。

2 在可以访问 Livelink 数据库的计算机上，下载安装文件。将 *LivelinkScanner_windows_x32_11.6.exe* 文件下载或复制（作为二进制文件）到临时目录。该文件位于 *DLP_Home\Symantec_DLP_11_Win\Scanners* 中，其中 *DLP_Home* 是解压缩 Symantec Data Loss Prevention 软件的目录的名称。

3 启动此计算机上的扫描程序安装程序。

LivelinkScanner_windows_x32_11.6.exe

注意：此扫描程序应该仅安装在 32 位 Windows 服务器上。

4 查看 Welcome 屏幕，然后单击 **Next**。

5 选择安装的 Destination Directory，也就是要安装 Livelink 扫描程序的文件夹。

默认值为 *c:\Program Files\LivelinkScanner*。

单击 **Next**。

6 选择开始菜单文件夹（“开始”菜单中的快捷方式）。

默认值为 **Vontu Livelink Scanner**。

单击 **Next**。

7 输入 Network Discover Server 的以下连接信息：

■ 发现主机（Network Discover Server 的 IP 或主机名）

■ 发现端口

单击 **Next**。

8 输入扫描程序的下列 Livelink 配置值：

LiveLink Host	Livelink 服务器的主机名称或 IP 地址。
LiveLink Port	Livelink 服务器的 HTTP 端口。
LiveLink User Name	扫描时要使用的用户名。
LiveLink Password	扫描时要使用的密码。 加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。
LiveLink Connection Name	Livelink API 连接名称。此名称是 Livelink 服务器上 opentext.ini 文件中的 dbconnection。
LiveLink API Port	除非已在 Livelink 服务器上的 opentext.ini 文件中对此端口进行更改，否则应为 2099。默认值为 2099。
ODBC DSN	运行 Livelink 扫描程序的计算机上的 ODBC 数据源的名称。
SQL User Name	用于连接至 ODBC 数据源的用户名。
SQL Password	用于连接至 ODBC 数据源的密码。 加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。

单击 **Next**。

9 安装扫描程序。

10 选择 Startup Mode。

在最初测试或验证扫描程序是否可成功运行时，不要选择这些选项，而是手动启动扫描程序。

可以选择以下选项之一（或不选）：

- 作为 Windows 系统上的服务安装。
- 安装后启动。

默认值为手动启动扫描程序。

11 扫描程序计算机上的 Livelink 扫描程序安装完成。

12 通过编辑配置文件和属性文件执行所有手动配置。

请参见第 1116 页的“[Livelink 扫描程序的配置选项](#)”。

请参见第 1044 页的“[扫描程序安装目录结构](#)”。

请参见第 1045 页的“[扫描程序配置文件](#)”。

13 将下列文件从 Livelink 安装复制到 \LivelinkScanner\scanner 文件夹：

- LAPI_ATTRIBUTES.dll
- LAPI_BASE.dll
- LAPI_DOCUMENTS.dll
- LAPI_USERS.dll
- LLKERNEL.dll

14 为 Livelink 使用的数据库实例创建 ODBC 数据源。VontuLivelinkScanner.cfg 文件中引用了此数据源。

请参见第 1112 页的“[为 SQL Server 创建 ODBC 数据源](#)”。

15 在 Enforce Server 上，为扫描程序 Livelink 类型创建一个新目标。

16 在扫描程序计算机和 Enforce Server 上同时启动扫描。

请参见第 1115 页的“[启动 Livelink 扫描](#)”。

启动 Livelink 扫描

确保在目标计算机上安装并配置扫描程序，并在 Enforce Server 上添加新目标。

请参见第 1113 页的“[安装 Livelink 扫描程序](#)”。

然后，您可以启动扫描。

下列每种情景对应的过程是不同的：

- 一个目标对应一个扫描程序（第一个过程）。
- 一个目标对应多个扫描程序（第二个过程）。

启动 Livelink 扫描（一个目标对应一个扫描程序）

1 登录到 Enforce Server。

转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。

2 从目标列表中选择扫描目标，然后单击“开始”图标。

3 在扫描程序计算机上，启动 Livelink 扫描程序。

单击“开始”>**VontuLivelinkScanner**>**VontuLivelinkScanner Console**。

4 扫描程序启动扫描数据进程。

请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。

- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的“[排除扫描程序故障](#)”。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

启动 Livelink 扫描（一个目标对应多个扫描程序）

- 1 在每台扫描程序计算机上，启动 Livelink 扫描程序。
单击“开始”>**Vontu Livelink Scanner > Vontu Livelink Scanner Console**。
确保每个扫描程序都已启动并且都已发布信息。检查每台计算机上的 outgoing 文件夹。
请参见第 1044 页的“[扫描程序安装目录结构](#)”。
- 2 登录到 Enforce Server。
转到“管理”>“发现扫描”>“发现目标”以导航至目标列表。
- 3 从目标列表中选择扫描目标，然后单击“开始”图标。
- 4 扫描程序启动扫描数据进程。
请参见第 1041 页的“[Network Discover 扫描程序的工作原理](#)”。
- 5 如果扫描不能正常进行，您可以对其进行故障排除。
请参见第 1042 页的“[排除扫描程序故障](#)”。
- 6 每次更改配置文件后，请停止并重新启动扫描程序。要停止扫描程序，请在控制台窗口中键入 Control-C 字符。

Livelink 扫描程序的配置选项

表 72-2 提供了 `VontuLiveLinkScanner.cfg` 文件的说明。

表 72-2 VontuLiveLinkScanner.cfg 文件中的参数

类型	参数	说明
连接性	<code>OpenTextServer</code>	Livelink 服务器的主机名称或 IP 地址。
连接性	<code>OpenTextPort</code>	Livelink 服务器的 HTTP 端口。
连接性	<code>OpenTextUsername</code>	扫描时要使用的用户名。
连接性	<code>OpenTextPassword</code>	扫描时要使用的密码。加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。

类型	参数	说明
连接性	LLConnection	Livelink API 连接名称。此参数是 Livelink 服务器上 opentext.ini 文件中 dbconnection 的名称。
连接性	LLApiPort	除非已在 Livelink 服务器上的 opentext.ini 文件中对此值进行更改，否则应为 2099。
连接性	DSN	运行 Livelink 扫描程序的计算机上 ODBC 数据源的名称。
连接性	SQLUserName	用于连接至 ODBC 数据源的用户名。
连接性	SQLPassWord	用于连接至 ODBC 数据源的密码。加密此密码。 请参见第 934 页的“ 加密配置文件中的密码 ”。
限制	BatchSize	将文件导入发送到 Network Discover 的每个 XML 文件之前已聚合的文件数量。 请参见第 940 页的“ 使用 Network Discover 扫描限制优化资源 ”。

扫描 Livelink 数据库的配置示例

扫描 Livelink 数据库中的所有属性。

该配置位于文件 VontuLiveLinkScanner.cfg 中。

请参见第 1116 页的“[Livelink 扫描程序的配置选项](#)”。

```
//#####
//#    Jobs
//#####
[JOBS]
Number=1
0=Job0
[Job0]
OpenTextServer=mydatabase-livelink.test.lab
OpenTextPort=80
OpenTextUsername=Admin
OpenTextPassword=livelink
LLConnection=LivelinkDB
LLApiPort=2099
```

```
DSN=livelink  
SQLUserName=lldbuser  
SQLPassWord=livelink
```

为自定义扫描目标设置 Web 服务

本章节包括下列主题：

- [为自定义扫描目标设置 Web 服务](#)
- [关于设置 Web 服务定义语言 \(WSDL\)](#)
- [Web 服务 Java 客户端的示例](#)
- [Web 服务示例的示例 Java 代码](#)

为自定义扫描目标设置 Web 服务

“Web 服务” 目标类型可让客户编写自定义扫描程序。这些自定义扫描程序将内容和元数据作为简单对象访问协议 (SOAP) 请求发送至 Network Discover。Network Discover Server 成为 Web 服务主机。

请参见第 1120 页的[“关于设置 Web 服务定义语言 \(WSDL\)”](#)。

提供了 Java SOAP 客户端示例。

请参见第 1120 页的[“Web 服务 Java 客户端的示例”](#)。

要为 Network Discover 设置自定义 Web 服务，请完成以下过程：

表 73-1 设置自定义扫描目标

步骤	操作	说明
1	添加 “Web 服务” 目标类型。	请参见第 926 页的 “添加新的 Network Discover 目标” 。

步骤	操作	说明
2	启动扫描。	从目标列表中选择扫描目标，然后单击“开始”图标。 请参见第 943 页的“ 管理 Network Discover 目标扫描 ”。
3	保存并修改 WSDL，然后创建客户端（例如 Java 客户端）或 SOAP 请求。	请参见第 1120 页的“ 关于设置 Web 服务定义语言 (WSDL) ”。 提供了 Java 客户端示例。 请参见第 1120 页的“ Web 服务 Java 客户端的示例 ”。
4	运行此客户端，并验证结果。	请参见第 1120 页的“ Web 服务 Java 客户端的示例 ”。

关于设置 Web 服务定义语言 (WSDL)

“Web 服务”目标运行时，您可以从以下 URL 下载具体的 Web 服务定义语言 (WSDL)。下列端口为默认端口。输入 Network Discover Server 的位置和端口号。

`http://discover_server:8090/?wsdl`

有关“Web 服务”示例 WSDL 及“Web 服务”示例 SOAP 请求的信息，请参见联机帮助。

Web 服务 Java 客户端的示例

下列过程和代码提供了 Web 服务的示例。此示例会将某个文件夹中的所有文件的内容和元数据发送到 Network Discover Server。

创建并运行 Web 服务 Java 客户端

1 登录 Enforce Server 并创建 Network Discover Web 服务目标类型。

请参见第 926 页的“[添加新的 Network Discover 目标](#)”。

使用默认设置。记下扫描程序端口号；默认值为 8090。

2 启动扫描。

3 浏览到下列 URL:

```
http://discover_server:8090/?wsdl
```

以名为 DiscoverSOAPTarget.wsdl 的 WSDL 文件将该页面另存在某个文件夹（例如 sample_folder）中。

如果在步骤 1 中扫描程序端口号不同，则请编辑 URL 以替换端口号 8090。

4 安装 Java 开发工具包 (JDK)（如果该工具包在系统中不可用）。

5 将 Java 主目录设置为安装 JDK 的文件夹。

```
JAVA_HOME=jdk_install_dir
```

6 安装开源服务框架 Apache CXF。

请参见 <http://cxf.apache.org/>

7 将 WSDL 转换为 Java 代码。

```
apache-cxf-installdir\bin\wsdl2java  
-client sample_folder\DiscoverSOAPTarget.wsdl
```

Java 源文件会在 com.vontu.discover 和 com.vontu.wsdl.discoversoaptarget 软件包下自动创建。

8 编辑 sample_folder 中名为 DiscoverSOAPClient.java 的文件，并插入 Java 代码。在此文件的开头放置新代码。根据需要更改常数。

请参见第 1121 页的“[Web 服务示例的示例 Java 代码](#)”。

9 使用下列命令编译 Java 代码：

```
javac DiscoverSOAPClient.java
```

10 使用下列命令运行程序：

```
java DiscoverSOAPClient
```

11 在 Enforce Server 上，验证是否已在步骤 1 中创建的 Network Discover 目标报告了预计的项目数。

Web 服务示例的示例 Java 代码

在名为 DiscoverSOAPClient.java 的文件开头输入下列源代码。

请参见第 1120 页的“[Web 服务 Java 客户端的示例](#)”。

```
import javax.xml.datatype.DatatypeFactory;
import javax.xml.namespace.QName;
import java.io.ByteArrayOutputStream;
import java.io.File;
import java.io.FileInputStream;
import java.net.URL;
import java.util.Date;

import com.vontu.discover.ComponentContentType;
import com.vontu.discover.ComponentType;
import com.vontu.discover.DocumentType;
import com.vontu.discover.ProcessDocumentsType;
import com.vontu.wsdl.discoversoaptarget.DiscoverSOAPTargetPortType;
import com.vontu.wsdl.discoversoaptarget.DiscoverSOAPTargetService;
import com.sun.org.apache.xerces.internal.impl.dv.util.Base64

public class DiscoverSOAPClient

{
    private static final QName SERVICE_NAME = new QName(
        "http://www.vontu.com/wsdl/DiscoverSOAPTarget.wsdl",
        "DiscoverSOAPTarget_Service");
    private static final String OWNER = "DiscoverSOAPClient";
    private static final String BODY = "This is the body";
    private static final String TYPE = "Text";
    private static final String ENCODING = "base64";

    //Change this value according to your needs
    private static final String TEST_FOLDER_NAME = "c:\\temp\\data";

    //Change this based on your discover host name and scanner port
    private static final String WSDL_PATH =
        "http://localhost:8090/?wsdl";

    public static void main(String []args)
    {
        try
        {
            URL wsdl = new URL(WSDL_PATH);
            File folder = new File(TEST_FOLDER_NAME);
            DiscoverSOAPTargetService service =
                new DiscoverSOAPTargetService(wsdl, SERVICE_NAME);
            DiscoverSOAPTargetPortType client = service.getDiscoverPort();
```

```
for(File file : folder.listFiles())
{
    if(file.isDirectory())
    {
        //only files in the test folder are sent to Discover
        continue;
    }
    System.out.println(file);
    ProcessDocumentsType processDocumentsType =
        new ProcessDocumentsType();
    DocumentType documentType = new DocumentType();
    processDocumentsType.getDocument().add(documentType);
    documentType.setOwner(OWNER);
    documentType.setURI(file.toString());
    GregorianCalendar time = new GregorianCalendar();
    time.setTime(new Date(file.lastModified()));
    documentType.setLastModifiedDate(
        DatatypeFactory.newInstance().
        newXMLGregorianCalendar(time));
    documentType.setLastModifiedDate(
        DatatypeFactory.newInstance().
        newXMLGregorianCalendar(time));

    //create a component
    ComponentType body = new ComponentType();
    documentType.setComponent(body);
    body.setName(file.getName());

    //add body
    ComponentContentType bodyContent =
        new ComponentContentType();
    body.setComponentContent(bodyContent);
    bodyContent.setType(TYPE);
    bodyContent.setContent(BODY);

    ComponentType attachment = new ComponentType();
    body.getComponent().add(attachment);
    attachment.setName(file.getName());

    //add some content to the component
    ComponentContentType attachmentContent =
        new ComponentContentType();
    attachment.setComponentContent(attachmentContent);
```

```
attachmentContent.setContentType(ENCODING);

ByteArrayOutputStream bytes =
    new ByteArrayOutputStream();
FileInputStream in = new FileInputStream(file);
byte[] buf = new byte[1024];

for(;;)
{
    int len = in.read(buf);
    if(len == -1)
    {
        break;
    }
    bytes.write(buf,0,len);
}

attachmentContent.setContent(
    Base64.encode(bytes.toByteArray()));

//make the SOAP call
client.processDocuments(processDocumentsType);
}

}catch(Exception e)
{
}
}
```

发现和防止端点计算机上的数据丢失

- 74. 使用 Endpoint Discover 和 Endpoint Prevent
- 75. 实施 Endpoint Discover
- 76. 实施 Endpoint Prevent
- 77. 使用代理配置
- 78. 使用 Endpoint FlexResponse
- 79. 实施 Symantec DLP Agent
- 80. 管理 Symantec DLP Agent
- 81. 关于应用程序监控
- 82. 使用 Endpoint Server 工具

使用 Endpoint Discover 和 Endpoint Prevent

本章节包括下列主题：

- [关于 Endpoint Discover 和 Endpoint Prevent](#)
- [关于 Endpoint Prevent 监视](#)
- [关于 Endpoint Discover 监视](#)
- [关于端点计算机的策略](#)
- [关于为 Endpoint Prevent 创建策略](#)
- [关于规则结果缓存 \(RRC\)](#)
- [关于端点报告](#)

关于 Endpoint Discover 和 Endpoint Prevent

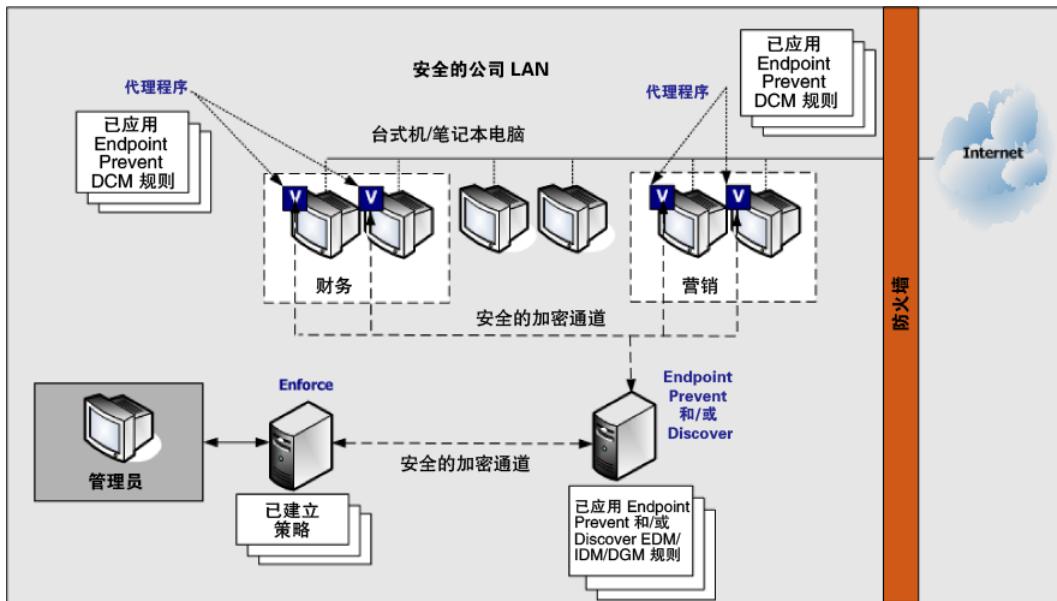
Endpoint Discover 和 Endpoint Prevent 是直接在端点计算机上运行的相关产品。Endpoint Discover 和 Endpoint Prevent 均应用数据泄漏防护策略来保护敏感数据或危险数据。敏感数据或危险数据可以包括信用卡号或姓名、地址、身份证号。可以视为敏感数据的数据类型不受限制。必须通过一系列的策略来定义敏感信息类型。

请参见第 314 页的“[实施策略](#)”。

Endpoint Discover 会扫描端点计算机以查找已定义为危险或敏感的信息。Endpoint Prevent 可阻止敏感数据从端点计算机移出。例如，Endpoint Prevent 会停止将含有信用卡号的文件传输到 eSATA、USB 或 FireWire 已连接的介质。不过，Endpoint Discover 会检查本地固定驱动器，并找出含有这些匹配策略的信用卡号的每一个文件。这两种产品已配置，可识别含有敏感数据的文件并保护该数据。

Endpoint Discover 和 Prevent 都使用 Symantec Data Loss Prevention 代理及 Endpoint Server 部署。

图 74-1 安全的公司 LAN



Endpoint Discover 的工作原理

Endpoint Discover 允许您检查组织的本地驱动器中是否包括任何具有潜在风险的数据。Endpoint Discover 会在发现违反策略的文件时通知您，并确定该文件在端点系统上的位置。Endpoint Discover 可以扫描与端点计算机连接的任何本地驱动器，但无法扫描 CD/DVD 驱动器或可移动介质设备（例如 eSATA 驱动器、USB 闪存驱动器或 SD 卡）。

请参见第 1135 页的“[关于 Endpoint Discover 监视](#)”。

Endpoint Prevent 的工作原理

Endpoint Prevent 策略与检查离开端点计算机的不同路由的策略组相关联。Endpoint Server 可以将策略推送到 Symantec DLP Agent，或将策略直接应用于由 Symantec DLP Agent 发送的文件。根据创建的策略类型，该策略会由 Symantec DLP Agent 直接应用或由 Endpoint Server 应用。当 Symantec DLP Agent 或 Endpoint Server 检测到违反策略规则的活动时，便会生成一个事件。该事件会出现在端点事件列表中。您可以通过发送警报、通知端点用户等方式对事件做出响应。

注意：分配到 Endpoint Server 的策略组同样地应用于所有连接的代理。

Endpoint Prevent 可以各种方式在端点上检测违规，其中包括：

- 应用程序监控
- CD/DVD 事件
- 剪贴板事件
- eSATA 事件（写入 eSATA 可移动驱动器）
- 网络事件（HTTP/HTTPS、即时消息传送、电子邮件和 FTP）
- 网络共享事件
- 打印/传真事件
- USB 事件（闪存卡和 SD 卡）

请参见第 1130 页的“[关于 Endpoint Prevent 监视](#)”。

请参见第 1129 页的“[关于 Symantec DLP Agent](#)”。

请参见第 314 页的“[实施策略](#)”。

关于 Endpoint Server

Endpoint Server 会将端点计算机上部署的所有 Symantec DLP Agent 连接到 Enforce Server。Endpoint Server 也包括 Endpoint Discover 的检测策略。

Endpoint Server 同时连接 Endpoint Discover 和 Endpoint Prevent。

根据许可证的不同，本指南中讨论的部分主题可能对您不适用。例如，如果您已授权了 Endpoint Prevent，则必须配置 Endpoint Server，以允许使用监视和防止功能。然而，如果您仅授权 Endpoint Discover，则不需要配置网络功能。

请参见第 1127 页的“[关于 Endpoint Discover 和 Endpoint Prevent](#)”。

关于 Symantec DLP Agent

您可以在要进行扫描的每台端点计算机上部署 Symantec DLP Agent。Enforce Server 会控制 Symantec DLP Agent 并应用该 Endpoint Server 的策略和规则。您不能对 Symantec DLP Agent 进行个别更改。

Symantec DLP Agent 包括加密的数据存储区，称为“代理存储区”。它可作为供 Symantec DLP Agent 发送至 Endpoint Server 的事件和文件使用的缓冲区或保留空间。如果 Symantec DLP Agent 从 Endpoint Server 断开，则在重新创建连接前，代理存储区会保留这些事件和文件。代理存储区的大小是受限制的（默认为 5% 的磁盘空间）。如果达到大小上限，Symantec DLP Agent 会从代理存储区逐出文件和事件。逐出策略会先瞄准最早的文件，然后再瞄准最早的事件。由于文件可能包

括或不包括 Endpoint Server 必须分析的敏感数据，所以会先瞄准文件。然而，事件是对策略的直接违规，如果可能的话，必须保留该违规的记录。

有关可以安装 Symantec DLP Agent 的端点计算机操作系统的信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。

请参见第 1180 页的“[关于 Symantec DLP Agent 的安装前步骤](#)”。

关于 Endpoint Prevent 监视

您可以使用 Endpoint Prevent 执行多种不同类型的监控。这些不同类型的监控合在一起就创建了 Endpoint Prevent 产品。下表提供了可以执行的监控类型的参考。

表 74-1 Endpoint Prevent 监控

监控类型
关于可移动存储监控
关于端点网络监视
关于 CD/DVD 监视
关于打印/传真监视
关于网络共享监视
关于剪贴板监视
关于应用程序监控

Endpoint Prevent 无论是否连接到 Endpoint Server，均可在端点计算机上监控活动。如果端点计算机与网络断开，且无法连接到 Endpoint Server，则 Endpoint Prevent 将继续监控端点计算机。所有事件都会存储在代理存储区，直到计算机重新连接至 Endpoint Server 为止。如果代理存储区超出指定的大小限制，则在达到大小限制之前会弹出旧文件，Endpoint Prevent 不会停止监控端点计算机。

请参见第 1129 页的“[关于 Symantec DLP Agent](#)”。

关于可移动存储监控

Endpoint Prevent 允许您阻止将数据从硬盘驱动器传输到可移动介质。可移动介质包括下列设备：

- 压缩闪存卡
- eSATA 可移动驱动器
- 由 FireWire 连接的设备

- SD 卡
- USB 闪存驱动器

在 Symantec DLP Agent 检测到发生违规时，不会传输数据。此时会创建一个事件，并将其发送给 Endpoint Server。发生违规时，Symantec DLP Agent 会对用户显示弹出式通知，以通知用户发生了违规。通知消息也会请求对文件传输进行确认。此项确认会出现在事件快照中。

请参见第 777 页的“[设置报告首选项](#)”。

例如，用户 1 从端点计算机复制一个含有医疗记录的 Microsoft Word 文件到 USB 闪存驱动器。Symantec DLP Agent 会禁止该文件传输到闪存驱动器中。当文件被禁止时，会在用户的屏幕上显示弹出式通知，指出文件传输违反了某项特定策略。弹出式通知也会包括一个确认组件，用于用户确认要将文件移动到闪存驱动器上。用户输入弹出式窗口中的确认消息可在此次事件的事件快照中看到。

请参见第 1130 页的“[关于 Endpoint Prevent 监视](#)”。

关于 CD/DVD 监视

CD/DVD 监视与 Windows Server 2003、XP、Vista 和 Windows 7 32 位和 64 位操作系统上运行的所有主要 CD/DVD 刻录应用程序兼容。

端点 CD/DVD 监视旨在监视特定文件类型。性能过滤器位于代理配置部分。可使用它们来指定 Endpoint Prevent 监视的文件类型。也可以在 CD/DVD 刻录应用程序中控制监视的效果。

要启用 CD/DVD 保护，必须选中 Endpoint Server 配置页的“代理监视”选项卡中的 CD/DVD 状态切换按钮。此外，还可以为复制到 CD/DVD 刻录机的文件创建策略。创建将 CD/DVD 作为目标的“协议”或“端点目标”规则。必须为该策略指定内容条件。可以使用 AND/OR 布尔条件来创建策略。仅在策略生成器中使用 AND 条件来指定内容条件。

例如，想要创建阻止含有关键字 Farallon 的文件刻录到 DVD 的策略。DVD 刻录应用程序为 Roxio 9。创建一项带有协议或设备类型规则的空白策略。选择 CD/DVD 设备类型，并且匹配“内容匹配关键字”规则。输入 Farallon 作为关键字。完成该规则及“端点阻止”响应规则的创建。保存策略之后，Symantec DLP Agent 会阻止包含关键字 Farallon 的所有文件刻录到 DVD。

通过选择 CD/DVD 设备类型，即已指定这项策略仅影响刻录到 CD/DVD 的文件。端点的硬盘和通过 USB 连接的介质不受影响。通过组合使用设备类型和关键字匹配规则，可保证 Symantec DLP Agent 仅阻止含有指定关键字的文件。代理不会阻止发送到 CD/DVD 应用程序的所有文件。如果创建 CD/DVD 阻止规则而不创建关联的关键字规则，则策略会阻止发送到刻录应用程序的每个文件。如果创建关键字阻止规则而不创建关联的 CD/DVD 规则，则策略会阻止端点的硬盘和通过 USB 连接的介质中含有关键字的文件。

注意：根据使用的CD/DVD刻录应用程序，含有机密信息的文件会被阻止或修改。修改后的文件不包含敏感数据。如果将修改后的文件写入光盘，则该特定 CD 或 DVD 不能重复使用。

注意：小于 64 字节的小文件在由 CD/DVD 监视读取时不会被检测到。通常会检测大小超过 64 字节的文件。

请参见第 1136 页的“[关于端点计算机的策略](#)”。

请参见第 1130 页的“[关于 Endpoint Prevent 监视](#)”。

关于打印/传真监视

Endpoint Prevent 允许您监视并禁止敏感信息被打印或传真给接受者。在 Microsoft Windows 中，用于打印和传真信息的机制是相同的，因此 Endpoint Prevent 机制也一样。

文件会一页一页地发送到打印机或传真机，然后再打印或传真每一页。Endpoint Prevent 会在将每个页面发送到打印机或传真机时对其进行分析。这意味着如果在文件中间发现违规，可能已经打印或传真了文件的前几页。例如，用户将一份 10 页的文档发送到打印机。文件会一页一页发送到打印机。Endpoint Prevent 在第三页发现违规，并从该处停止打印文件。而第一页和第二页都已经打印，但不会打印第三页到第十页。Endpoint Prevent 会将事件发送到包含文件信息和匹配文本的 Endpoint Server。

注意：不监视传真封面上的文本。

事件快照包括有关发送违规文件的端点计算机、违规文件本身、打印机名称及打印机类型等信息。打印机类型是本地连接的打印机、共享的打印机和网络打印机，或是已选择“打印至文件”打印机选项。

请参见第 777 页的“[设置报告首选项](#)”。

请参见第 1130 页的“[关于 Endpoint Prevent 监视](#)”。

关于剪贴板监视

Endpoint Prevent 可防止用户利用 Windows 剪贴板，将敏感数据从一个应用程序复制并粘贴到另一个应用程序。Endpoint Prevent 只适用于 Windows 剪贴板，但不能防止剪贴板在同一个应用程序之间传输敏感数据。

例如，假设用户从 Word 文档复制敏感信息并将其粘贴到 IM 消息中，则 Endpoint Prevent 会禁止传输。发生禁止的原因是复制和粘贴功能会使用 Windows 剪贴板。此用户会收到弹出式通知，说明禁止传输的原因。在端点报告中，事件快照包括事

件与粘贴到电子邮件中的信息文本。会在发生剪切或复制操作时创建事件，而不是在发生粘贴操作时创建。

请参见第 777 页的“[设置报告首选项](#)”。

请参见第 1130 页的“[关于 Endpoint Prevent 监视](#)”。

关于应用程序监控

通过应用程序监控，您可以监控 IM、电子邮件或 HTTP/S 客户端的第三方应用程序。默认情况下，Symantec Data Loss Prevention 只会监控主体应用程序，例如 AIM、Microsoft Outlook 或 Mozilla Firefox。第三方应用程序的示例包括 Skype、Mozilla Thunderbird 或 Google Chrome。必须先将 Symantec Data Loss Prevention 未专门监控的任何应用程序添加到“应用程序监控”页面，Symantec Data Loss Prevention 才能开始监控。例如，如果您的公司使用 Mozilla Thunderbird，则必须将 Thunderbird 添加到“应用程序监控”页面。因为默认情况下不监控 Mozilla Thunderbird，所以需要添加该应用程序。添加 Mozilla Thunderbird 后，Symantec Data Loss Prevention 可在应用程序通过网络发送电子邮件时对其进行监视。

此外，也可以配置对默认应用程序的全局更改。可以将黑名单或白名单数据与网络监控、CD/DVD 应用程序和使用打印/传真或剪贴板功能的应用程序关联起来。还可以指定是否希望 Symantec Data Loss Prevention 监控应用程序的网络、打印/传真、剪贴板或文件系统活动。例如，您可能希望排除 Microsoft Outlook 上的剪贴板活动。您可以在应用程序指纹加密页面上编辑 Microsoft Outlook 的设置以排除剪贴板活动。此页面上的应用程序仅是您希望修改其网络、打印/传真、剪贴板或文件系统监控的应用程序。

请参见第 1207 页的“[关于应用程序监控](#)”。

关于网络共享监视

通过网络共享监视，您可以防止敏感文件在网络共享和端点计算机之间传输。

例如，您有标记为 c: 驱动器的本地驱动器。您还有标记为 g: 驱动器的远程网络共享。您可以创建阻止敏感数据从 c: 驱动器复制到 g: 驱动器的策略。您也可以防止敏感数据从 g: 驱动器传输到 c: 驱动器。任何端点响应规则均适用于网络共享监视。对于网络共享监视，Endpoint Protect 仅阻止直接通过 Windows 资源管理器传输的敏感数据。不会监视网络共享访问的其他类型。网络共享访问的其他类型包括：FTP 传输、第三方应用程序或复制/粘贴应用程序。网络文件共享访问的这些其他类型可由 Symantec Data Loss Prevention 的其他检测功能监视。

请参见第 1130 页的“[关于 Endpoint Prevent 监视](#)”。

关于端点网络监视

Endpoint Prevent 允许您监视或禁止各种类型的网络事件。这些事件包括：

- HTTP/HTTPS
- 电子邮件/SMTP
- FTP
- IM

不论端点计算机是否连接到公司网络，Endpoint Prevent 都允许您禁止网络违规。例如，用户将便携式计算机带出办公室，并在咖啡店访问无线 Internet 连接。

Symantec DLP Agent 仍然能够检测、删除任何文件、文本或电子邮件，或禁止这些内容在不安全的网络上传输。当端点计算机未连接到 Endpoint Server 时，所生成的事件会存储在临时数据库中。事件会保留在数据库中，直到重新创建连接为止。在重新创建与 Endpoint Server 的连接后，会将事件发送给 Endpoint Server。

Symantec DLP Agent 可以监视 HTTP 或 HTTPS 网页与应用程序。例如，它能够监视并防止通过 Microsoft Internet Explorer、Mozilla Firefox 或任何其他 HTTP 应用程序传输敏感信息。HTTPS 监视功能允许您监视或防止通过可由 Internet Explorer 或 Firefox Web 浏览器访问的加密 HTTPS 站点传输任何文件。HTTP 与 HTTPS 保护也允许您阻止电子邮件与附件，不让它们通过 Web 电子邮件应用程序传输。事件包括目标 IP、URL 以及邮件信息。

Endpoint Prevent 会监视最常见的电子邮件应用程序，如 Microsoft Outlook 与 Lotus Notes。不论电子邮件协议为何，它都能够监视并防止任何信息从这些应用程序传输出去。附件以及邮件主题、正文和脚注的内容都会被分析。事件包括有关发送者、接受者以及电子邮件的信息。

FTP 监视可防止文件通过 FTP 协议传输到外部的文件存储库。例如，用户会使用 FTP 应用程序 Mozilla Filezilla 来尝试将违反策略的文件发送到远程文件存储库。Endpoint Prevent 会防止文件传输到 FTP 位置。随即会创建一个针对此次违规的事件，并显示在 Enforce Server 的“端点报告”部分中。事件快照会包含已尝试通过 FTP 发送文件的用户的相关信息。其中既会显示违规的文件，也会显示目标 FTP 服务器的 IP 地址。

它还可以监视 AIM、MSN 以及 Yahoo Messenger 等即时消息传送应用程序。IM 监视可根据个别消息或根据会话来分析传出的消息。例如，如果用户通过 IM 打开与另一人的聊天会话。Endpoint Prevent 会分析用户所发送的每则消息是否含有敏感信息。这些消息中的每一项都会被单独分析。与此同时，Endpoint Prevent 也会分析整场对话中是否含有不容易在个别消息中发现的敏感信息。IM 通信消息和文件也会受到禁止。IM 事件包含发送者、接受者以及会话内容的相关信息。

注意：某些网络类型与文件名监视条件不匹配。这些网络事件不包含文件名，因此不能与此条件匹配。不能与文件名条件匹配的网络监视类型包括 HTTP/HTTPS、IM 邮件正文和文本，以及 Outlook 邮件正文和文本。

所有事件都会报告在 Endpoint Prevent 下的“报告”部分中。

请参见第 1130 页的“[关于 Endpoint Prevent 监视](#)”。

关于 Endpoint Discover 监视

Endpoint Discover 扫描端点计算机的本地驱动器，以查找违反策略的所有当前现有文件。Endpoint Discover 扫描端点计算机上的所有本地驱动器。例如，如果您的计算机已安装两个本地物理驱动器，Endpoint Discover 扫描会针对违反您策略的任意文件，同时扫描两个本地驱动器。Endpoint Discover 不会扫描通过网络或可移动介质（如 eSATA 驱动器、闪存驱动器或 SD 卡）装入的驱动器。

Symantec DLP Agent 只能在本地针对 Endpoint Discover 执行 DCM 扫描。对于所有其他类型的扫描，Symantec DLP Agent 会将文件的文本发送到 Endpoint Server 进行分析。这样的设计方式意味着必须在 Endpoint Server 上执行 EDM 和 IDM 检测。

例如，您设置 Endpoint Discover 扫描来检查所有端点计算机上的所有本地驱动器。与扫描关联的策略包括 DCM 内容（关键字）以及 IDM 组件（信用卡号码）。

Endpoint Discover 检查本地驱动器时，它会针对关键字自动分析每个文件。如果它检测到可能匹配信用卡号码索引列表的文件，就会将该文件发送到 Endpoint Server 进行分析。

要开始或停止扫描，必须将 Symantec DLP Agent 连接至 Endpoint Server。如果 Symantec DLP Agent 未连接至 Endpoint Server，则会在它与 Endpoint Server 重新连接时开始扫描。只有在所有端点计算机都已完成扫描时，扫描才会完成。如果某端点计算机与 Endpoint Server 断开连接，则除非该端点计算机重新连接，否则扫描不能完成。如果端点计算机在扫描启动后断开连接，端点计算机会在重新连接到 Endpoint Server 后继续扫描。如果端点计算机仍然断开连接，且超出配置的超时周期，则扫描会报告超时状态。所有事件都会存储在代理存储区，直到计算机重新连接至 Endpoint Server 为止。如果代理存储区超过指定的大小限制，则扫描会一直等到代理存储区降低后方才进行。扫描会一直等到端点计算机重新连接至 Endpoint Server 并清除代理存储区之后方才进行。

请参见第 1129 页的“[关于 Symantec DLP Agent](#)”。

默认情况下，Symantec DLP Agent 会在计算机处于活动状态时扫描端点计算机上的大多数文件。在端点计算机闲置之前，不会扫描需要大量带宽来扫描的任何文件。这样做的好处是，当用户在计算机上处于活动状态时，Symantec DLP Agent 将使用较少的 CPU 带宽。您可以配置 Symantec DLP Agent 将端点计算机定义为空闲状态的方式。您可以将 Symantec DLP Agent 配置为，在端点计算机处于活动状态时不对其进行扫描。

请参见第 218 页的“[高级代理设置](#)”。

为 Endpoint Discover 违规所创建的事件会显示在“事件”部分的“发现”选项卡下。会以端点专用图标来标记事件。不能自动补救 Endpoint Discover 事件，必须手动补救事件。

请参见第 1140 页的“[关于端点报告](#)”。

关于目标 Endpoint Discover 扫描

您可以将已连接到特定 Endpoint Server 的所有端点计算机设为目标。或者，您也可以设置单个端点计算机作为 Endpoint Discover 扫描的目标。根据您指定的一组过滤器，连接到 Endpoint Server 的各个 Symantec DLP Agent 开始扫描。当 Endpoint Server 开始扫描时，扫描信息会分散到相关的所有 Symantec DLP Agent。Symantec DLP Agent 使用扫描过滤器分析扫描。

如果扫描排除了 Symantec DLP Agent，它就会将“未参与”状态发送到 Endpoint Server。

在 Endpoint Server 上，一次只能运行一个 Endpoint Discover 扫描。如果您根据扫描过滤器排除 Symantec DLP Agent，则除非完成第一次扫描，否则不会扫描这些 Symantec DLP Agent。

请参见第 1146 页的“[设置对 Endpoint Discover 目标的扫描](#)”。

关于端点计算机的策略

Symantec Data Loss Prevention 采用双层检测架构来分析端点计算机上的活动。它视需要直接对 Symantec DLP Agent 执行检测或在 Endpoint Server 上执行检测。Endpoint Server 可以执行所有类型的检测，例如 Exact Data Matching (EDM)、Indexed Document Matching (IDM) 以及 Directory Group Matching (DGM)。代理仅可以执行描述内容匹配 (DCM)。Symantec Data Loss Prevention 可以在本地根据关键字、正则表达式和数据标识符进行检测。它必须将输入内容发送至 Endpoint Server 才能根据确切数据指纹或索引文档指纹进行检测。

双层检测不仅意味着您可以将各种检测规则和响应规则组合在一个策略中并在端点计算机上使用，而且还意味着可以优化端点计算机上的系统利用率及 Symantec Data Loss Prevention 的性能。当创建应用于端点计算机的策略时，建议遵循以下准则：

不要创建将服务器端检测规则与 Endpoint Prevent 响应规则组合在一起的策略。例如，不要将 EDM、IDM 或者 DGM 规则与“端点阻止”或“端点通知”响应规则组合在一起。如果服务器端检测规则触发 Endpoint Prevent 响应规则，则 Symantec Data Loss Prevention 无法执行 Endpoint Prevent 响应规则。

当创建包括服务器端检测规则的端点策略时，请将该检测规则与代理端检测规则组合在一个复合规则中。此做法有助于 Symantec Data Loss Prevention 在端点上执行检测，而无需将内容发送到 Endpoint Server。Symantec Data Loss Prevention 可通过在端点上执行检测来节省网络带宽并提高性能。

例如，您可以将 EDM 检测规则与“发送者”检测规则组合在一个复合规则中。在复合规则中，必须满足所有条件 Symantec Data Loss Prevention 才记录匹配。相反，如果其中一个条件未满足，则 Symantec Data Loss Prevention 根本不检查第

二个条件即确定没有匹配。例如，要记录匹配，内容必须满足第一个条件 AND 所有其他条件。当通过这种方式设置复合规则时，Symantec DLP Agent 首先会根据代理端规则检查输入内容。如果没有匹配，Symantec Data Loss Prevention 则不需要将内容发送至 Endpoint Server。但是，如果创建了一个涉及 DCM 或 EDM 策略的复合规则，内容仍然会发送至 Endpoint Server。

在将服务器端检测规则（例如 EDM、IDM 或者 DGM 规则）与保留端点事件原始文件的“所有:限制事件数据保留”响应规则组合在一起之前，请考虑保留原始文件的带宽影响。在 Symantec DLP Agent 将内容发送至 Endpoint Server 进行分析时，它会根据检测要求发送文本数据或二进制数据。在可能的情况下，Symantec DLP Agent 会发送文本以减少带宽使用。默认情况下，Symantec Data Loss Prevention 会丢弃端点事件的原始文件。如果响应规则保留端点事件的原始文件，则 Symantec DLP Agent 必须将二进制数据发送至 Endpoint Server。在这种情况下，请确保网络能够在不降低性能的情况下处理 Symantec DLP Agent 与 Endpoint Server 之间增加的流量。

将代理端检测规则（例如 DCM）与 Endpoint Prevent 响应规则组合在同一个策略中。仅当 Symantec DLP Agent 检测规则触发响应时，Symantec Data Loss Prevention 才能执行 Endpoint Prevent 响应规则。

请参见第 1137 页的表 74-2。

表 74-2 不兼容的检测规则和响应规则

不要将这些基于服务器的检测规则...	...与这些 Endpoint Prevent 响应规则组合在一起。
<ul style="list-style-type: none">■ 内容匹配确切数据 (EDM)■ 内容匹配文档签名 (IDM)■ 发送者/用户匹配目录源 (DGM)■ 接受者匹配目录源 (DGM)	<ul style="list-style-type: none">■ Endpoint Prevent: 阻止■ Endpoint Prevent: 通知■ Endpoint Prevent: 用户取消

关于为 Endpoint Prevent 创建策略

Endpoint Prevent 的策略与 Network Prevent 的策略不同。

Endpoint Prevent 策略包括创建实时用户交互的响应规则。用户交互可阻止文件传输，或通知用户发生策略违规。然后会将这些通知附加至事件。

端点策略在检测发生的位置方面也不同。在 Endpoint Server 上执行 IDM、EDM 及 DGM 策略的检测。DCM 策略的检测则由 Symantec DLP Agent 直接执行。

“阻止”、“通知”及“用户取消”响应规则仅在 Symantec DLP Agent 上执行。

由于 IDM、EDM 及 DGM 策略的检测在 Endpoint Server 上执行，因此检测会花费更长时间，并使用更大的带宽。由于要将文件发送至 Endpoint Server 进行检测，

因此需要更多的时间和带宽。代理执行 DCM 策略的检测时，只会将事件发送至 Endpoint Server。

请参见第 1136 页的“[关于端点计算机的策略](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于 Endpoint Server 的监视策略与响应规则

特定于端点的响应规则包括“端点阻止”、“端点通知”、“端点隔离”和“用户取消”。“端点阻止”会停止移动违反策略的数据。“端点通知”会就发生的违规对用户进行培训，但不会阻止或停止移动数据。“端点隔离”将含有敏感信息的文件从本地驱动器移到安全位置。“端点隔离”仅适用于 Endpoint Discover。“用户取消”可以让端点用户决定是否允许数据进行传输。所有规则都会创建弹出式显示窗口，其中包括违反策略的相关信息。每个规则都会请求用户提供进行操作的理由。“端点阻止”、“端点通知”和“用户取消”适用于端点计算机上执行的所有 Endpoint Prevent 检测策略。例如，HTTP/HTTPS、电子邮件/STMP、FTP、CD/DVD、eSATA、打印/传真和 USB 监视均会使用“端点阻止”规则或“端点通知”规则。

“端点阻止”、“端点通知”和“用户取消”响应规则不适用于：

- 通过 Endpoint Discover 发现的违规
- 关于本地驱动器监视的违规

请参见第 314 页的“[实施策略](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于端点阻止

可以创建策略来限制任何数据从端点计算机进行传输。例如，您想要阻止包含关键字 Farallon 的任何文本、电子邮件或文件从该计算机进行传输。您可以创建关键字匹配策略，将 Farallon 这个单词作为违规关键字。

请参见第 314 页的“[实施策略](#)”。

您希望确保此策略用于所有端点计算机。在响应规则部分，选择“端点阻止”作为响应规则。此响应规则仅适用于此端点。如果将文件从硬盘传输至 CD/DVD 驱动器，则该特定端点计算机上会显示弹出式通知。此通知指出该操作违反了 Farallon 关键字策略。

“端点阻止”响应规则会防止移动文件。但是，您还希望记录违规发生的原因。在响应规则中，您可以创建一系列理由。这些理由允许违规的端点用户解释违规发生的原因。这些理由可包括用户培训、经管理员批准的文件移动或其他理由。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于端点通知

可以使用“端点通知”响应规则创建可对端点用户进行培训的策略和响应规则。

“端点通知”响应规则会显示说明违规的弹出式消息，并就相应的策略对端点用户进行培训。

例如，端点用户会发送电子邮件正文中包括Farallon这个单词的电子邮件。“端点通知”会生成发送至Endpoint Server的事件，并在端点计算机上显示弹出式通知。此通知会说明违反的策略以及现在监视的端点操作。端点用户输入违规的原因，接受通知，电子邮件将继续正常发送和接收。“端点通知”不会防止数据移动，它仅通知用户发生策略违规。端点用户的违规理由会成为事件报告的一部分，发送至Enforce Server。

并非所有策略组和策略都适用于端点响应规则。如果您尝试创建含不兼容的规则和响应的策略，则会接收到错误消息。此错误指出策略与端点响应规则不兼容。

响应规则可区分公司网络上创建的事件与公司网络之外创建的事件。此条件允许您指定是始终运行规则，还是仅在端点与公司网络连接或断开连接时运行规则。

请参见第 1136 页的“[关于端点计算机的策略](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于端点用户取消

您可以创建一个响应规则，让端点计算机用户决定是否允许从其计算机中传输敏感数据。您可以使用“用户取消”响应规则来指导端点用户遵守适当的业务策略。例如，如果端点用户通过电子邮件发送敏感信息并收到“用户取消”弹出式通知，则他们可以取消数据传输。现在，这些用户已接受了有关贵公司策略的培训。此外，如果端点用户传输敏感数据是一种合理需要，则他们可以允许此操作。如果他们允许此操作，这些数据会正常传输。

在这两种情况下，Symantec DLP Agent 均会生成一个事件并将其发送给 Enforce Server。

仅允许端点用户在特定时间内决定是否覆盖该策略。如果超出了指定时间，该策略会自动阻止数据传输并生成事件。默认情况下，该时间限制为 60 秒。该选项适用于在随后 10 秒内发生的所有违反该策略的情况。

如果阻止了同一策略的多个违规情况，端点用户必须仅输入一次理由。该理由将显示在事件的事件快照中。事件快照中还包含所采取的操作。事件快照包含以下操作之一：

- 已通知用户，操作：已允许
- 已通知用户，操作：已取消
- 已通知用户，操作：已取消超时
- 已通知用户，操作：已允许超时

注意：您可以指定是否允许超时后的默认操作阻止或允许数据传输。

请参见第 699 页的“[配置 Endpoint Prevent: 用户取消操作](#)”。

请参见第 1136 页的“[关于端点计算机的策略](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于规则结果缓存 (RRC)

规则结果缓存 (RRC) 是 DLP Agent 上的预检测形式。通过缓存与规则不匹配的任何内容的相关信息，DLP Agent 可以忽略这些内容。RRC 允许 DLP Agent 仅对新内容或最近更改的内容执行检测，因此可加速检测。

只有指定内容匹配 (DMC) 规则结果可以在 DLP Agent 中进行缓存。检测的其他类型（确切数据匹配 (EDM)、文件属性类型 (FPT) 和索引数据匹配 (IDM)）不适用于 RRC。此外，RRC 不适用于协议或组检测规则。

请参见第 283 页的“[策略检测简介](#)”。

只要与 DLP Agent 关联的策略发生更改，就会删除 RRC 缓存。以前的 RRC 结果将被清除，您必须再次扫描所有内容。但是，在完成首次扫描后，完成后续扫描要快得多。

默认情况下，RRC 处于活动状态。如果不需要 RRC，请转至高级代理设置，将其设置为“关闭”。

关于端点报告

使用事件报告可以跟踪和补救端点计算机上的事件。当检测到与策略规则的检测参数匹配的数据时，Symantec Data Loss Prevention 会报告事件。此类数据可能包括特定文件内容、电子邮件发送者或接受者、附件文件属性，或许多其他类型的信息。每块匹配检测参数的数据称为一个匹配条目，一个事件可能包括任意数量的匹配条目。

Endpoint Discover 的报告位于“发现报告”部分下。标记 Endpoint Discover 事件，以与其他类型的发现事件进行区分。

Endpoint Prevent 的报告位于 Enforce Server 的“报告”选项卡下。

您可以查看以下报告：

- 执行摘要 - Endpoint Prevent
- 事件 - 全部
- 事件 - 新建

- 策略摘要
- 状态摘要
- 最高的违规者

如果创建的事件包括用户理由，则会将这些理由纳入报告的事件快照部分。例如，如果发生要求用户输入响应User error的违规，则事件报告中将包括文本**特殊：用户键入响应：“User error”**。

如果用户选择预先生成的理由，则该理由会显示在报告中。理由显示在详细报告的“理由”标题下。

理由和通知与 Endpoint Discover 不兼容，因此 Endpoint Discover 报告中不会显示任何理由。

您也可以为 Endpoint Discover 与 Endpoint Prevent 创建自定义报告。然而，如果在输入理由时用户不在网络上，则事件快照的理由部分仍保持为空白。

请参见第 775 页的“[关于 Symantec Data Loss Prevention 报告](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

实施 Endpoint Discover

本章节包括下列主题：

- [如何实施 Endpoint Discover](#)

如何实施 Endpoint Discover

要实施 Endpoint Discover，必须执行一组特定的任务。这些任务类似于 Network Discover，但并不完全相同。完成下列配置任务：

表 75-1 实施 Endpoint Discover

阶段	操作	说明
步骤 1	安装 Symantec Management Console（可选）。	请参见第 1173 页的“ 关于 Symantec Management Console ”。
步骤 2	设置端点位置。	请参见第 1152 页的“ 设置端点位置 ”。
步骤 3	修改 Endpoint Server 配置。	请参见第 176 页的“ 服务器配置 - 基本 ”。
步骤 4	创建策略组。	请参见第 1144 页的“ 为 Endpoint Discover 创建策略组 ”。
步骤 5	创建策略。	请参见第 1144 页的“ 为 Endpoint Discover 创建策略 ”。
步骤 6	创建 Endpoint Discover 目标。	请参见第 1146 页的“ 设置对 Endpoint Discover 目标的扫描 ”。
步骤 7	安装 Symantec DLP Agent。	请参见第 1178 页的“ 关于 Symantec DLP Agent 安装 ”。
步骤 8	配置报告。	请参见第 775 页的“ 关于 Symantec Data Loss Prevention 报告 ”。

有关实施 Endpoint Discover 的任何主题的更多信息，请参见联机帮助。

为 Endpoint Discover 创建策略组

为 Endpoint Discover 创建策略组的方式与为 Network Discover 创建策略组的方式相同。这些策略组并非部署在系统中的不同节点上，而是通过 Symantec DLP Agent 来部署。创建策略组后，可以将特定策略分配给策略组。

创建策略组

- 1 转至“管理”>“设置”>“策略组”。
- 2 在显示的“策略组列表”屏幕上，单击“添加策略组”。
- 3 输入策略组名称（最多 256 个字符）及说明。选择一个有含义的名称，因为其他用户在选择要与角色、策略和 Endpoint Discover 目标关联的策略组时，必须访问此名称。
- 4 选择分配给此策略组的检测服务器。您可以将策略组分配给所有检测服务器或个别服务器。请注意，Symantec Data Loss Prevention 会自动将所有策略组分配给所有 Endpoint Discover Server。
- 5 单击“保存”。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

为 Endpoint Discover 创建策略

Symantec Data Loss Prevention 使用双层检测方法进行端点检测。Endpoint Discover 的检测在 Endpoint Server 上进行。Symantec DLP Agent 会将文件发送至 Endpoint Server 进行分析。IDM、EDM 及 DGM 策略均在 Endpoint Server 上执行。Symantec DLP Agent 会将打开的文件从端点计算机发送至 Endpoint Server 进行分析。

请参见第 1136 页的“[关于端点计算机的策略](#)”。

您可以将策略的状态设置为“活动”或“挂起”。默认情况下，策略设为“活动”状态。如果您选择“挂起”，则不会将策略应用至 Symantec DLP Agent。

以下说明适用于创建空白策略。您也可以根据先前存在的模板来创建策略。以下说明使用示例数据及特定说明来解释如何创建策略。

例如，假设您要创建 Endpoint Discover 策略，以查找标识号码以 1357 开头的文件。您具有以 1357 开头的所有号码的列表。以 EDM_m1 名称将此列表上传至 Symantec Data Loss Prevention 系统。Symantec Data Loss Prevention 会创建策略，该策略会在端点上发现包括其中任一敏感数据的所有文件。

为 Endpoint Discover 创建策略

- 1 转至 Enforce Server 上的“策略”>“策略列表”。
- 2 单击“添加策略”。
- 3 选择“添加空白策略”。
- 4 在“名称”字段中，输入**1357 identifier**。
- 5 在新策略的“说明”字段中，添加“发现所有以**1357**开头的标识符”。
- 6 从下拉菜单中，选择要与此策略关联的策略组。

针对此示例，请使用**EP eDAR**。

创建该策略之后，您必须向该策略中添加规则。

请参见第 1145 页的“[为 Endpoint Discover 添加规则](#)”。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

为 Endpoint Discover 添加规则

为 Endpoint Discover 创建策略后，必须向该策略中添加规则。您可以向策略中添加一个或多个规则。您必须向策略中至少添加一个规则。

请参见第 1144 页的“[为 Endpoint Discover 创建策略](#)”。

添加规则至策略

- 1 在“检测”选项卡下，单击“添加规则”，为策略添加规则。
 - 2 选择“内容匹配确切数据源”单选单击钮。
 - 3 从下拉菜单中，选择**EDM m1**。
- 此过程会将先前创建的列表链接至此规则。
- 4 单击“下一步”。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

关于端点隔离

您可创建自动响应规则，允许 Endpoint Discover 将文件从本地驱动器删除并放到安全的位置。如果 Endpoint Discover 扫描发现包含敏感数据的文件，会将该文件隔离并从不安全的位置删除。安全位置既可以在本地驱动器上，也可以是公司网络上的安全位置。您可创建替换机密数据的标记文件。标记文件会提醒端点计算机用户，文件包含机密信息，已被隔离。您可在标记文本中包含描述事件相关信息（例如文件名、违反的策略和安全文件夹的位置）的变量。

端点隔离响应规则仅适用于 Endpoint Discover。

隔离位置可以是本地驱动器上的安全文件夹，也可以是端点计算机可通过公司网络访问的远程文件共享中的文件夹。您可选择是要在安全位置启用凭据，还是允许任何匿名用户访问该位置。

注意：加密文件服务 (EFS) 文件夹不支持匿名访问。

并非所有策略组和策略都适用于端点响应规则。如果您尝试创建含不兼容的规则和响应的策略，则会接收到错误消息。此错误指出策略与端点响应规则不兼容。

请参见第 1136 页的“[关于端点计算机的策略](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

请参见第 693 页的“[配置“Endpoint Discover: 隔离文件”操作](#)”。

设置对 Endpoint Discover 目标的扫描

Endpoint Discover 目标用来配置 Symantec Data Loss Prevention Agent 扫描的位置。它们对应于 Endpoint Discover 进行检查以查找策略违规情况的目标本地驱动器、文件夹或端点计算机。例如，可以将固定驱动器或 Windows 中的“我的文档”文件夹配置为目标。Endpoint Discover 可以扫描与端点计算机关联的任何固定驱动器。Endpoint Discover 无法扫描可移动驱动器。您也可以指定过滤器，以确定所监视的端点计算机。此过滤称为目标 Endpoint Discover 扫描。若要创建 Endpoint Discover 目标，请使用下列步骤。

表 75-2 设置 Endpoint Discover 目标

步骤	说明	操作
步骤 1	单击“管理”>“发现扫描”>“发现目标”来配置新的 Endpoint Discover 目标。	请参见第 926 页的“ 添加新的 Network Discover 目标 ”。
步骤 2	对目标 Endpoint Discover 扫描执行所有其他的过滤器配置。	请参见第 1147 页的“ Endpoint Discover 目标的配置选项 ”。
步骤 3	单击“高级”选项卡以配置“扫描空闲超时”和“最大扫描持续时间”设置。	请参见第 1149 页的“ 配置 Endpoint Discover 扫描超时设置 ”。

注意：您无法调度 Endpoint Discover 目标扫描。您必须手动启动每一次扫描。还必须手动停止扫描、允许完成扫描或允许扫描超时。无法暂停 Endpoint Discover 扫描。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

关于 Endpoint Discover 目标过滤器

Endpoint Discover 目标过滤器影响 Endpoint Discover 与端点计算机的交互方式。Endpoint Discover 目标过滤器允许您指定以下属性：

- 扫描的文件类型。
- 要扫描的目标内的区域。
- 要扫描的端点计算机的子集。
- 要扫描的文件的大小。

Endpoint Discover 目标专门用于特定本地系统。与 Network Discover 不同，端点目标不需要定义的根系统或网络共享。

请参见第 1146 页的“[设置对 Endpoint Discover 目标的扫描](#)”。

请参见第 1147 页的“[Endpoint Discover 目标的配置选项](#)”。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

Endpoint Discover 目标的配置选项

Endpoint Discover 目标与 Symantec Data Loss Prevention 代理关联，并且专用于特定 Endpoint Server。Endpoint Discover 扫描配置为 Endpoint Server 的所有 Symantec Data Loss Prevention 代理。在 Endpoint Server 上，一次只能运行一个 Endpoint Discover 扫描。

您可以指定过滤器以包括或排除要监视的端点计算机。此过滤称为目标 Endpoint Discover 扫描。目标 Endpoint Discover 扫描排除的所有端点计算机均显示“未参与”。

下表提供可用于配置 Endpoint Discover 目标的设置摘要。

名称	请参见第 930 页的“ 为 Network Discover 目标配置必填字段 ”。
策略组	
服务器	
包括过滤器	请参见第 935 页的“ 设置发现过滤器以在扫描中包括或排除项目 ”。
排除过滤器	请参见第 935 页的“ 设置发现过滤器以在扫描中包括或排除项目 ”。
大小过滤器	请参见第 937 页的“ 按项目大小过滤发现目标 ”。

日期过滤器

请参见第 938 页的“[根据上次访问或修改日期过滤发现目标](#)”。

扫描超时设置

请参见第 1149 页的“[配置 Endpoint Discover 扫描超时设置](#)”。

设计包括过滤器和排除过滤器，以便您过滤以下内容：

- 文件
- 文件夹
- IP 地址
- 计算机名称
- WINS 名称

例如，您可以在包括过滤器部分下包含以下过滤器：

.doc, \$Documents\$, >.symantec.com, >192.168.32.0/8, >EDT*

目标 Endpoint Discover 扫描可以监视：

- 所有固定驱动器上与扫描相关的所有 .doc 文档
- \My Documents\ 文件路径中的所有文件
- .symantec.com 域中的所有端点计算机
- 192.168.32.0/8 网络上的所有计算机
- WINS 名称为 EDT 的所有端点计算机

请使用逗号分隔多个过滤器。

Endpoint Discover 使用通用语法来说明 IP 地址范围。此格式类似于标准无类别域间路由（CIDR）格式。Endpoint Discover IP 地址范围过滤器格式包括主要网络地址，后接 / 字符以及掩码位数。例如，IP 地址范围说明 192.64.110.0/24 的掩码位数为 24。这表示从 192.64.110.0 到 192.64.110.255 的所有 IP 地址都匹配此过滤器。同样，128.0.0.0/8 代表从 128.0.0.0 到 128.255.255.255 的 IP 地址范围。

在结构上，过滤器是布尔值，其中先使用 OR 表达式应用类似过滤器，然后使用 AND 表达式与其他过滤器组合。使用该示例，Symantec Data Loss Prevention 代理将扫描

.doc OR \$Documents\$ AND >*.symantec.com OR >192.168.32.0/8。

*.doc 及 \$Documents\$ 过滤器使用 OR 表达式，因为它们是文件或文件路径过滤器。
>.symantec.com 及 >192.168.32.0/8 过滤器使用 OR 表达式，因为它们是 IP 过滤器，且彼此类似。两组类似的过滤器使用 AND 表达式组合。

配置 Endpoint Discover 扫描超时设置

Endpoint Discover 扫描可能会由于一台或多台端点计算机与 Endpoint Server 的连接中断而无法完成。您可以配置“扫描空闲超时”设置，以便在端点计算机处于脱机状态的时间达到指定时间时停止 Endpoint Discover 扫描。

您也可以配置“最大扫描持续时间”，以便定义 Endpoint Discover 扫描要运行的最大持续时间。当 Endpoint Discover 扫描超过“最大扫描持续时间”时，Endpoint Discover 扫描便会停止。

Endpoint Discover 扫描历史记录将报告“超时”扫描状态。若要访问扫描历史记录，请从 Enforce Server 管理控制台选择“管理”>“扫描历史记录”。

配置“扫描空闲超时”设置

- 1 从“高级”设置选项卡找到“扫描空闲超时”。
- 2 输入时间量，然后选择“分钟”或“小时”。

注意：若要禁用“扫描空闲超时”，请选择“不确定”作为持续时间。

- 3 单击“保存”保存设置。

配置“最大扫描持续时间”设置

- 1 从“高级”设置选项卡找到“最大扫描持续时间”。
- 2 输入时间量，然后选择“分钟”、“小时”或“天”。

注意：若要禁用“扫描最大持续时间”，请选择“不确定”作为持续时间。

- 3 单击“保存”保存设置。

实施 Endpoint Prevent

本章节包括下列主题：

- [如何实施 Endpoint Prevent](#)

如何实施 Endpoint Prevent

Endpoint Prevent 会监视每台端点计算机上的传送数据。如果 Endpoint Prevent 检测到违规，就会禁止数据传输。或是通知违规用户，也可以要求用户作出解释。实施 Endpoint Prevent 时，要求您按顺序完成下列进程。

表 76-1 实施步骤

步骤	操作	操作
步骤 1	安装 Symantec Management Console (可选)	请参见第 1173 页的“ 关于 Symantec Management Console ”。
步骤 2	安装 Symantec DLP Agent	请参见第 1178 页的“ 关于 Symantec DLP Agent 安装 ”。
步骤 3	设置端点位置	请参见第 1152 页的“ 设置端点位置 ”。
步骤 4	创建端点代理配置	请参见第 1155 页的“ 关于代理配置 ”。
步骤 5	添加 Endpoint Server	请参见第 187 页的“ 添加检测服务器 ”。
步骤 6	创建端点策略	请参见第 314 页的“ 实施策略 ”。

步骤	操作	操作
步骤 7	创建端点响应规则	请参见第 1137 页的“ 关于为 Endpoint Prevent 创建策略 ”。
步骤 8	配置报告	请参见第 775 页的“ 关于 Symantec Data Loss Prevention 报告 ”。

这些步骤是正确实施 Endpoint Prevent 的必要条件。有关实施 Endpoint Prevent 的主题的详细信息，请参见联机帮助。

请参见第 485 页的“[关于实施同步的目录组匹配](#)”。

设置端点位置

“端点位置”用于定义 Symantec Data Loss Prevention 如何判断端点计算机是否已连接到公司网络。您可以指定是否要让 Endpoint Server 自动检测以查看端点计算机是否在公司网络上。或者，您也可以指定域名称或 IP 地址的列表，用以判断端点计算机是否已连接到网络。

使用自动端点位置判断功能时，如果 Symantec DLP Agent 可连接到 Endpoint Server，便会将该计算机视为已连接到网络。如果 Symantec DLP Agent 不能连接到 Endpoint Server，便会判定该端点计算机已与公司网络断开。使用手动端点位置判断功能时，您必须先输入某个范围的域名称或 IP 地址。然后 Symantec DLP Agent 会使用此信息来判断该端点计算机是否连接到公司网络。配置域名范围之后，Symantec DLP Agent 会在主机的 IP 地址上执行反向 DNS 查找。接着会将检索的 DNS 主机名称与列表中配置的域名称进行匹配。配置 IP 地址范围之后，Symantec DLP Agent 会将主机 IP 地址与配置的 IP 地址列表进行匹配。每个单独的主机 IP 地址都必须位于公司网络上，这样才会将端点计算机视为已连接到公司网络。

域名不得包含通配符，并且应该是简单的后缀，如 symantec.com。

IP 地址可能包含通配符来代替单个块。例如，192.168.*.*。

请参见第 1130 页的“[关于 Endpoint Prevent 监视](#)”。

设置端点位置设置

- 1 转至“系统”>“代理”>“端点位置”。随即将显示当前的端点位置设置。默认情况下，会将端点位置判断方法设为“自动”。
- 2 单击“配置”。
- 3 选择“自动”或“手动”，以指定判断方法。

4 如果选择“手动”，请在正确的字段中输入域名称或IP地址列表。每行只输入一个域名称或IP地址。

5 单击“保存”。

所做的更改会立即生效。

请参见第 1151 页的[“如何实施 Endpoint Prevent”](#)。

请参见第 185 页的[“Endpoint Server - 基本配置”](#)。

关于不同区域设置中的 Endpoint Prevent 响应规则

您可以创建特定于端点计算机的区域设置的不同端点响应规则通知。区域设置指的是端点计算机的操作系统中的系统区域设置。

例如，您可以用英语、法语或日语创建响应规则通知。如果将用户的区域设置指定为日语，则用户的屏幕上会显示通知的日语版本。如果使用法语区域设置的其他用户违反了同一策略，则会显示通知的法语版本。

Enforce Server 允许您指定多个用户通知。不过，指定的第一个语言是默认语言。不能删除默认语言响应通知。您可以添加或删除未指定为默认语言的任何通知或语言。在安装时，默认语言会设为设置成 Enforce Server 语言的任意语言。如果不支持您需要的语言，则 Enforce Server 会尝试显示英语通知。

例如，您有一台日语区域设置端点计算机和一台越南语区域设置端点计算机。越南语区域设置是不受支持。如果区域设置为日语的计算机上发生违规，则 Enforce Server 会显示日语通知。如果日语通知不可用，则 Enforce Server 会显示默认语言通知。如果区域设置为越南语的计算机违反了策略，则 Enforce Server 会显示英语通知，因为无法显示越南语通知。如果英语通知不可用，则 Enforce Server 会显示默认语言通知。

如果端点计算机上不支持您添加的第一个语言，则不能将该语言视为默认语言。端点计算机必须包含特定语言详细信息，以便将语言视为默认语言。即使通知文本以不受支持的语言显示，但通知窗口按钮和标题栏仍会以 Enforce Server 的默认区域设置显示。

如果要将不支持的语言定义为默认语言，则必须选择“其他”作为第一语言。该“其他”标签会删除列表中的所有其他语言。使用端点配置选项来修改弹出式窗口标签的文本。如果您选择“其他”选项，则不能指定其他语言响应。无论端点计算机的系统区域设置为何，在每台端点计算机上，“其他”设置都会显示该语言通知。

请参见第 218 页的[“高级代理设置”](#)。

注意：所有英语区域设置默认为英语（美国）设置。所有法语区域设置默认为法语设置。例如，法语（法国）设置支持所有类型的法语（如法语（加拿大）和法语（法国））。

请参见第 1154 页的“[设置不同区域设置的 Endpoint Prevent 响应规则](#)”。

设置不同区域设置的 Endpoint Prevent 响应规则

您可以为不同的区域设置，设置不同的响应规则。您指定的第一个区域设置将成为默认区域设置。尽管您可以删除附加区域设置，但无法删除该区域设置。

请参见第 1153 页的“[关于不同区域设置中的 Endpoint Prevent 响应规则](#)”。

设置本地化响应规则

1 正常创建响应规则。

请参见第 669 页的“[配置响应规则](#)”。

2 单击“添加语言”链接。

3 选择您要使用的语言。

如果您要将不支持的语言指定为默认语言，请选择“其他”。

4 使用指定的语言，在显示字段和理由字段中输入文本。

5 单击“保存”。

使用代理配置

本章节包括下列主题：

- [关于代理配置](#)
- [添加代理配置](#)
- [将代理配置应用于 Endpoint Server](#)

关于代理配置

Enforce Server 管理控制台上的“代理配置”页面允许您创建可应用于 Endpoint Server 的配置。

您可通过 Symantec Management Console (SMC) 将这些配置应用于各个 Symantec DLP Agent。

每个配置均包含 Endpoint Server 或代理的配置选项。这些配置选项确定在端点计算机上进行的检测的类型。您还可使用代理配置来指定过滤器和资源使用量限制。可以创建任意数量的不同代理配置。但是，不能删除默认代理配置。Symantec Data Loss Prevention 端点防护必须至少包含一个代理配置。您可修改默认配置，次数不限。

请参见第 1156 页的“[添加代理配置](#)”。

Endpoint Server 一次仅可使用一个配置。不能一次将多个配置与 Endpoint Server 相关联。

可通过 Symantec Management Console (SMC) 或 Enforce Server 管理控制台来分配代理配置。不能使用 SMC 创建新的代理配置。只能在 Enforce Server 管理控制台中创建配置。如果通过 SMC 分配代理配置，可直接将配置分配到代理。如果通过 Enforce Server 分配代理，则只能将代理配置分配到 Endpoint Server。

您也可以克隆代理配置。

请参见第 1156 页的“[关于克隆代理配置](#)”。

请参见第 1161 页的“[将代理配置应用于 Endpoint Server](#)”。

关于克隆代理配置

您可以克隆代理配置。克隆的配置与原始配置相同。当您想要保留大部分实体详细信息不变且只需要做一些小的改动时，可以克隆代理配置。单击编辑图标旁边的克隆图标以克隆配置。克隆配置时，您会看到该克隆的配置的一个可编辑版本。必须重命名克隆的配置才能将其与原始配置区分开。

代理配置页面包含所有可用代理配置的相关信息。

单击“添加配置”创建新代理配置。

添加代理配置

可以通过转到“系统”>“代理”>“代理配置”并单击“添加配置”按钮添加或编辑代理配置。

通过修改下列选项卡创建或编辑代理配置：

- 代理监控
- 代理配置
- 高级代理设置

“代理监控”选项卡。

使用此选项卡可选择要监控端点项的哪些方面。“代理监控”选项卡分为三个部分。

- “启用监控”部分。选择要监控的端点应用程序和目标。

字段	说明
目标	选择要监控的目标。目标是指端点计算机的物理方面，如 CD/DVD 驱动器、USB 连接的设备、打印机等。
电子邮件	选择要监控的电子邮件应用程序。
Web	选择要监控的 Web 应用程序。HTTPS 监控仅支持 Firefox 和 Internet Explorer 浏览器。
即时消息传送	选择要监控的即时消息传送应用程序。
应用程序	选择该字段可添加应用程序文件访问监控。 请参见第 1207 页的“ 关于应用程序监控 ”。

字段	说明
网络共享	选择该字段可监控网络共享。可以监控在本地驱动器和网络共享间传输的文件。

- “按文件属性过滤”部分。创建和编辑监控过滤器。基于所设置的过滤器，Symantec DLP Agent将根据协议、目标、文件大小、文件类型或文件路径监控或忽略数据。此部分列出了现有过滤器。过滤器按照其出现在列表中的顺序运行，该顺序是由“顺序”列决定的。

注意：按文件路径进行过滤时，将忽略驱动器盘符，因而代理上每个本地驱动器的指定路径都会被过滤出来。例如，如果输入 c:\temp，则会将具有两个本地驱动器的代理上的 c:\temp 和 d:\temp 都过滤出来。

- 要创建新过滤器，请单击“添加监控过滤器”。
- 要修改某个现有的过滤器，请在列表中单击该过滤器。
- 要删除现有的过滤器，请单击该过滤器的红色 X。
- 要更改过滤器的应用顺序，请在“顺序”列中单击该过滤器的编号。然后，在下拉列表中选择该过滤器的执行顺序。只有在单击屏幕顶部的“保存”后才会应用更改。

请参见第 744 页的[“配置 Endpoint Server 文件过滤器”](#)。

- “指定默认文件过滤器操作”部分。选择“监控”或“忽略”以指定如何处理不与任何过滤器匹配的文件。
- “按网络属性过滤”部分。创建与网络相关的过滤器，这些过滤器使代理基于 IP 地址或域监控或忽略网络流量。在相应的框中输入您要对其进行过滤的 IP 地址、HTTP 域和 HTTPS 域。

对于过滤 IP 地址，请使用下列规则：

输入要使用的任何基于 IP 的过滤器。如果您将此字段保留空白，Symantec Data Loss Prevention 会检查所有数据包。IP 协议过滤器的格式（可在协议定义和协议过滤器定义中找到）是：

```
ip_protocol_filter          := protocol_filter_multiple_entries [; *]
protocol_filter_multiple_entries  := protocol_filter_entry
                                    [; protocol_filter_multiple_entries]
protocol_filter_entry        := +|-, destination_subnet_description,
                                source_subnet_description
destination_subnet_description  := subnet_description
source_subnet_description      := subnet_description
subnet_description            := network_ip_address / bitmask
                                | *
```

将会针对过滤器条目按顺序对每个流进行评估，直至某个条目与流的 IP 参数相匹配。

条目开头的减号 (-) 表示丢弃该流。条目开头的加号 (+) 表示保留该流。

子网网络描述 * 表示任何数据包都与此条目匹配。

长度为 32 的子网位掩码表示条目必须与确切的网络地址匹配。例如，+10.67.0.0/16;*-,*
过滤器可匹配传入网络 10.67.x.x 的所有流，但不匹配任何其他流量。

注意：您将识别特征定义的越具体，您得到的结果也就越具体。例如，如果您只定义了一个特定 IP 地址，则只捕获涉及此 IP 地址的事件。如果您没有定义任何 IP 地址，或您定义的 IP 地址的范围很宽泛，则您得到的结果也会较宽泛。至少包括一个加号 (+) 子句和一个减号 (-) 子句以明确指出要包含的内容和要排除的内容。

注意：需要分别针对 HTTP 和 HTTPS 应用域过滤器。要为支持 HTTP 和 HTTPS 的任何网站添加过滤器，请在各自的文本框中为 HTTP 和 HTTPS 添加过滤器。IP 地址过滤器可与所有其他网络协议一起使用。

对于过滤 HTTP/HTTPS 域名，请使用下列规则：

您可以使用过滤器来包括（检查）或排除（忽略）来自特定发送者的邮件。您也可以使用过滤器来包括或排除特定的接受者。特定的过滤器语法取决于协议。

以下是域过滤器示例

```
Domain Filter      := <Domain Filter Entry> [,<Domain Filter Entry>]
Domain Filter Entry := { * | {-|+}<metadata value> }
```

您可以使用下列符号：

- 您可以在域条目中使用通配符 (*)。
例如，*symantec.com 可以匹配 www.symantec.com、www.dlp.symantec.com 以及所有以 symantec.com 结尾的域。
- 条目开头的减号 (-) 表明忽略该 URL。
- 条目开头的加号 (+) 表明检查该 URL。
- 如果您在过滤表达式的末尾添加星号 (*)，则忽略所有不与任何过滤器掩码显式匹配的 URL 域。

这些过滤器从左到右执行，直至发生第一个匹配或代理到达过滤器条目的末尾。

例如，如果过滤器是：

```
-sales.symantec.com,+*symantec.com,*
```

忽略发送到 sales.symantec.com 的 HTTP 请求，检查所有发送到任何其他 symantec.com 域的请求。过滤器中最后的星号会过滤掉所有与 www.xyz.com 类似的其他域。

注意：如果您将 HTTP/HTTPS 过滤器留空，则会检查所有 URL。

您使用此屏幕指定的过滤器只能应用到已配置了这些过滤器的个别 Endpoint Server。如果您有多个 Endpoint Server，则必须为每个服务器单独配置文件过滤器。

“代理配置”选项卡。

“代理配置”选项卡分为以下部分：

- “服务器通信”部分。设置 Symantec DLP Agent 可用来将数据发送到 Endpoint Server 的带宽最大值（Mb 或 Kb/秒）。使用量限制的默认设置为 5 Mbps。要更改带宽限制，请选择 Mbps 或 Kbps，然后在每秒最大值框中输入一个数字。
- “端点主机上的资源使用量”部分。使用此部分设置代理存储区在每个端点系统上用来存储事件的最大磁盘空间量。您可以指定硬盘的百分比，也可以使用具体的测量单位（字节、KB、MB 或 GB）指定特定大小。单击相应的单选按钮来选择是使用磁盘空间百分比还是使用绝对的存储限制。然后，在相应的框中输入数量。对于绝对大小，请从下拉列表中选择度量单位。
请参见第 1129 页的“[关于 Symantec DLP Agent](#)”。
- “Endpoint Discover 扫描的资源使用量”部分。使用此部分来限制端点系统上发现扫描的效果：

字段	说明
长期平均 CPU 使用率	<p>指定在一段时间内用于发现扫描的 CPU 资源的最大平均百分比。如果 Symantec DLP Agent 超出此最大 CPU 限制，Endpoint Discover 检测会终止，但 Endpoint Protect 检测会正常进行。</p> <p>注意：您对 CPU 资源阈值所做的任何更改都应立即生效。如果您在扫描期间进行了更改，该更改将在代理继续扫描后生效。</p>
电池剩余寿命下限	<p>指定运行代理所需的电池最小电量。如果电池电力低于此下限，则 Endpoint Discover 检测会停止，但 Endpoint Protect 检测可正常工作。</p>

- “文件恢复区域位置”部分。指定文件恢复参数。文件恢复位置是存储Symantec DLP Agent 阻止其传输的敏感数据副本的区域。这些副本会被保留，直至用户将其恢复；否则一段时间后被自动删除。

字段	说明
文件恢复区域位置	<p>指定文件恢复目录的路径。默认路径为 %TMP\RecoveredFiles。</p>
距到期的时间	<p>指定从文件恢复文件夹自动删除文件之前所经过的时间。</p>

请参见第 49 页的“[关于 Symantec Data Loss Prevention 管理](#)”。

请参见第 176 页的“[服务器配置 - 基本](#)”。

请参见第 175 页的“[服务器控件](#)”。

“高级代理设置”选项卡。

还可以为代理指定高级设置。这些设置会影响 Symantec DLP Agent 处理信息、检测违规和在端点计算机上执行的方式。

修改高级代理设置时要十分小心。请在对高级设置进行任何更改之前先联系 Symantec 支持部门。

请参见第 218 页的“[高级代理设置](#)”。

有关高级代理设置的信息，请参考 Symantec Data Loss Prevention 联机帮助。

注意：如果要修改现有的代理配置，请单击“保存并应用”按钮将更改应用到所有与配置相关联的 Endpoint Server。如果要创建新配置，请保存该配置，并且可以在“编辑代理配置”页面上应用它。

请参见第 1155 页的“[关于代理配置](#)”。

请参见第 1161 页的“[将代理配置应用于 Endpoint Server](#)”。

将代理配置应用于 Endpoint Server

您可将任何代理配置应用到与 Enforce Server 管理控制台连接的任何 Endpoint Server。一次只能将一个代理配置分配到一个 Endpoint Server。不过，一次可将不同的配置分配到多个 Endpoint Server。使用“应用配置”页面，可以一次将多个代理配置实体分配到您的所有 Endpoint Server。

如果使用 Symantec Management Console 来应用代理配置，则可将配置直接应用到您的代理。代理接收配置后，它们即与特定 Endpoint Server 关联。

有关更多信息，请参见“[Symantec Management Console 联机帮助](#)”。

请参见第 1155 页的“[关于代理配置](#)”。

将代理配置应用于 Endpoint Server

- 1 单击“代理配置”主页面上的“应用配置”按钮。
- 2 选择所需的 Endpoint Server。
- 3 从下拉菜单中选择所需的代理配置。
- 4 单击“应用并更新”。

如果要编辑代理配置实体，并将这些更改立即应用到关联的 Endpoint Server，可通过以下步骤完成。单击“编辑配置”页面的“保存并应用”按钮。

请参见第 1156 页的“[添加代理配置](#)”。

1162

| 使用代理配置
将代理配置应用于 Endpoint Server

使用 Endpoint FlexResponse

本章节包括下列主题：

- [关于 Endpoint FlexResponse](#)
- [部署 Endpoint FlexResponse](#)
- [关于在端点计算机上部署 Endpoint FlexResponse 插件](#)
- [使用静默安装过程部署 Endpoint FlexResponse 插件](#)
- [关于 Endpoint FlexResponse 实用程序](#)
- [使用 Endpoint FlexResponse 实用程序部署 Endpoint FlexResponse 插件](#)
- [在 Enforce Server 上启用 Endpoint FlexResponse](#)
- [使用 Endpoint FlexResponse 实用程序卸载 Endpoint FlexResponse 插件](#)
- [从特定端点计算机中检索 Endpoint FlexResponse 插件](#)
- [从端点计算机中检索 Endpoint FlexResponse 插件列表](#)

关于 Endpoint FlexResponse

Symantec Data Loss Prevention 提供了一组响应规则操作，您可以通过指定这些操作来对事件进行补救。所提供的这些操作包括记录、发送电子邮件、阻止最终用户操作、通知用户及其他响应。

您也可以使用 Endpoint FlexResponse 插件来提供其他响应操作。这些插件包含了自定义的指令，供在端点计算机上执行的补救操作使用。Endpoint FlexResponse 规则仅适用于自动响应规则。您无法为智能响应规则创建 Endpoint FlexResponse 规则操作。

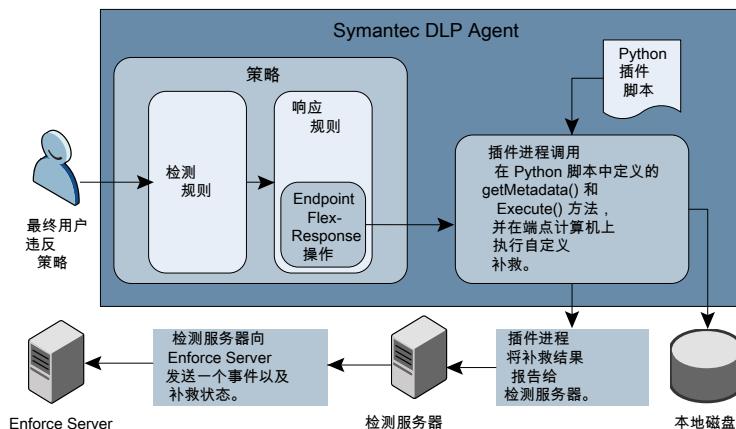
Symantec Data Loss Prevention 客户可通过联系 Symantec 或 Symantec 合作伙伴来获取 Endpoint FlexResponse 插件。此外，了解 Python 编程语言的开发人员还可以使用 Symantec 提供的 API 创建自定义的 Endpoint FlexResponse 插件脚本。这些自定义补救操作可以包括加密、应用数字版权管理 (DRM) 或修改机密信息。

您可以使用 Endpoint FlexResponse 实用程序将 Endpoint FlexResponse 插件部署到 Symantec Data Loss Prevention 部署中需要 Endpoint FlexResponse 操作的端点计算机。可以使用 Endpoint FlexResponse 实用程序手动部署这些插件，也可以使用系统管理软件 (SMS) 来分发该实用程序并部署这些插件。将 Endpoint FlexResponse 插件部署到端点计算机后，可以使用 Enforce Server 管理控制台将 **Endpoint:FlexResponse** 操作添加到响应规则，然后将该响应规则添加到活动策略中。

图 78-1 显示了引发 Endpoint FlexResponse 操作的活动的执行顺序。

图 78-1

Endpoint FlexResponse 插件流程



您可对以下类型的端点目标和协议使用 Endpoint FlexResponse 规则：

- Endpoint Discover
- 本地驱动器监控
- 可移动存储设备
- SMTP
- HTTP(S)

部署 Endpoint FlexResponse

请按照下面提供的步骤来部署 Endpoint FlexResponse 插件。

表 78-1 部署 Endpoint FlexResponse

步骤	操作	说明
步骤 1	获取（或创建）Endpoint FlexResponse 插件的 Zip 文件。	请与 Symantec 合作伙伴或 Symantec 销售代表联系。 Endpoint FlexResponse 插件不适用于默认 Symantec Data Loss Prevention 安装。
步骤 2	在 Enforce Server 上配置任何端点凭据。	请参见第 122 页的“ 配置端点凭据 ”。此步骤是可选的。
步骤 3	使用 Endpoint FlexResponse 实用程序和第三方系统管理软件 (SMS) 将该插件部署到端点计算机。	请参见第 1165 页的“ 关于在端点计算机上部署 Endpoint FlexResponse 插件 ”。
步骤 4	在 Enforce Server 上启用 Endpoint FlexResponse 操作。	请参见第 1169 页的“ 在 Enforce Server 上启用 Endpoint FlexResponse ”。
步骤 5	向响应规则添加 Endpoint FlexResponse 操作。	请参见第 668 页的“ 添加新的响应规则 ”。

关于在端点计算机上部署 Endpoint FlexResponse 插件

您必须先在端点计算机上安装 Symantec DLP Agent，然后再部署 Endpoint FlexResponse 插件。代理必须连接到活动的 Endpoint Server。

有关如何安装代理的信息，请参见《Symantec Data Loss Prevention 安装指南》。

您必须在需要 Endpoint FlexResponse 操作的每台端点计算机上都部署 Endpoint FlexResponse 插件。可以采用手动安装或静默安装方式来部署插件。静默安装方式涉及使用系统管理软件 (SMS) 将软件分发并安装到所有端点计算机。可能需要创建 SMS 脚本来访问安装文件夹。

本节假定您已创建或以其他方式获得了打包成 ZIP 文件的 Endpoint FlexResponse 插件。

要在端点计算机上部署 Endpoint FlexResponse 插件，需执行以下步骤：

- 步骤 1 将 Endpoint FlexResponse 实用程序复制到端点计算机。
请参见第 1167 页的“[关于 Endpoint FlexResponse 实用程序](#)”。
- 步骤 2 将插件需要的所有第三方 Python 模块复制到端点计算机。

- | | |
|------|---|
| 步骤 3 | 在 Enforce Server 上启用 Endpoint FlexResponse。请参见第 1169 页的“ 在 Enforce Server 上启用 Endpoint FlexResponse ”。 |
| 步骤 4 | 使用 Endpoint FlexResponse 实用程序部署 Endpoint FlexResponse 插件。 <code>(flrinst.exe)</code> 。使用以下可选方案之一： <ul style="list-style-type: none">■ 手动将插件部署到单台端点计算机上。当您要开发或测试 Endpoint FlexResponse 插件时，此可选方案最为有用。
请参见第 1169 页的“使用 Endpoint FlexResponse 实用程序部署 Endpoint FlexResponse 插件”。■ 使用静默安装过程和 SMS 软件部署插件。当您要部署已可投入生产环境中使用的 Endpoint FlexResponse 插件时，此可选方案最为有用。
请参见第 1166 页的“使用静默安装过程部署 Endpoint FlexResponse 插件”。 |
| 步骤 5 | 创建使用 Endpoint: FlexResponse 操作（引用此插件）的响应规则，然后将这些规则添加到活动策略中。

请参见《Symantec Data Loss Prevention 系统管理指南》中的“ 实施策略检测 ”。 |

使用静默安装过程部署 Endpoint FlexResponse 插件

可以使用系统管理软件 (SMS) 在多台端点计算机上部署 Endpoint FlexResponse 插件。虽然有关如何为 SMS 软件创建安装脚本的详细信息不在本文档的讨论范围内，但是请注意以下要求：

- 您必须先在端点计算机上安装 Symantec DLP Agent，然后再部署 Endpoint FlexResponse 插件。代理必须连接到活动的 Endpoint Server。
- 必须在要将 Endpoint FlexResponse 插件部署到的每台端点计算机上都安装 Endpoint FlexResponse 实用程序 (`flrinst.exe`)。
- 必须使 Endpoint FlexResponse 软件包（一个 `.zip` 文件）对每台端点计算机都可用。可以将该软件包复制到每台端点计算机，也可以在所有端点计算机都可访问的网络驱动器上提供该软件包。
- 要部署插件，请在创建安装脚本时使用 Endpoint FlexResponse 实用程序的命令行选项。请参见第 1168 页的表 78-3。
- 部署插件后请删除 Endpoint FlexResponse 实用程序。如果不将此实用程序从端点计算机上卸载，恶意用户可能会使用此实用程序卸载或修改 Endpoint FlexResponse 插件。

请参见第 1167 页的“[关于 Endpoint FlexResponse 实用程序](#)”。

有关如何使用 SMS 进行部署的更多信息，请参见各 SMS 应用程序的文档。

只能通过 Symantec 和 Symantec 合作伙伴获取 Endpoint FlexResponse 实用程序。Symantec Data Loss Prevention 分发包中并未附带它。

关于 Endpoint FlexResponse 实用程序

可以使用 Endpoint FlexResponse 实用程序来管理 Endpoint FlexResponse 插件。Endpoint FlexResponse 实用程序不是默认 Symantec Data Loss Prevention 下载文件的一部分，它只能通过 Symantec 或 Symantec 合作伙伴获取。

运行此实用程序前，请将 Python 脚本打包成单个 ZIP 文件。

表 78-2 Endpoint FlexResponse 实用程序操作

操作	说明
部署（安装）插件	使用 <code>install</code> 选项可将插件部署到端点计算机。
卸载插件	使用 <code>uninstall</code> 选项可从端点计算机中卸载插件。
检索已部署的插件	使用 <code>retrieve</code> 选项可检索端点计算机上已部署的特定插件。
查看已部署的插件的列表	使用 <code>list</code> 选项可以检索特定端点计算机上部署的所有插件的列表。此列表包含已部署的插件的名称。

Endpoint FlexResponse 实用程序必须从将 Symantec DLP Agent 部署到的文件夹中加以运行。此文件夹的位置是可配置的。默认情况下，此目录位于：

`c:\Program Files\Manufacturer\Endpoint Agent\`

该实用程序的名称为 `flrininst.exe`。该实用程序使用以下语法：

```
flrininst.exe -op=install|uninstall|retrieve|list  
-package=<package_name> -p=<Tools_password>
```

表 78-3 Endpoint FlexResponse 实用程序的选项

选项	说明
<code>-op=install uninstall retrieve list</code>	请使用以下参数之一： <ul style="list-style-type: none"> ■ <code>install</code> - 部署插件 ■ <code>uninstall</code> - 删除插件 ■ <code>list</code> - 显示已部署的插件的列表 ■ <code>retrieve</code> - 检索插件并将其另存为一个可编辑的文本文件。此文本文件包含在一个 ZIP 文件中，后者保存在从中运行该应用程序的目录中。
<code>-package=<package_name></code>	在您指定 <code>-op=install</code> 选项时，用于指定包含 Endpoint FlexResponse 插件的软件包（一个 ZIP 文件）的路径。软件包名称区分大小写。 在您指定 <code>-op=retrieve</code> 或 <code>-op=uninstall</code> 选项时，用于指定该软件包的名称。
<code>-p=<tools_password></code>	指定已为 Symantec Data Loss Prevention 部署配置的工具密码。 如果尚未配置工具密码，请使用默认密码 <code>VontuStop</code> 。 注意： 自 Symantec Data Loss Prevention 11.1.1 版开始，此密码不再是可选的。

如果您已经为 Symantec Data Loss Prevention 部署创建了工具密码，请使用 `-p` 选项将此密码传递给 Endpoint FlexResponse 实用程序。安装和卸载插件时需要用到此密码。可以在 Symantec Data Loss Prevention 安装期间配置工具密码，也可以使用 `endpointkeytool` 实用程序配置工具密码。请参见第 1212 页的“[关于 endpointkeytool 实用程序](#)”。有关更多信息，请参见《Symantec Data Loss Prevention 管理指南》。

如果您尚未配置工具密码，那么最终用户可以使用默认密码 `VontuStop` 来检索和修改以前安装的插件。Symantec 建议您配置一个工具密码以防发生此类篡改。另一种防止篡改的方式是，将 SMS 应用程序设置为在使用完 Endpoint FlexResponse 实用程序后将其删除。删除该实用程序可防止对插件进行任何未经授权的修改或卸载。

使用 Endpoint FlexResponse 实用程序部署 Endpoint FlexResponse 插件

可以使用 Endpoint FlexResponse 实用程序来部署 Endpoint FlexResponse 插件。插件必须采用 .zip 包格式。

部署 Endpoint FlexResponse 插件

- 1 在端点计算机上打开一个命令窗口，然后导航至 Symantec DLP Agent 安装工具目录。此目录的默认位置是 c:\Program Files\Manufacturer\Endpoint Agent\
- 2 输入下列命令：

```
flrinst.exe -op=install  
           -package=<path_to_plug-in>  
           -p=<myToolsPassword>
```

其中：

- <myToolsPassword> 是用于 Symantec Data Loss Prevention 部署的工具密码。如果您尚未指定工具密码，请使用默认密码：VontuStop。
- <path_to_plug-in name> 是插件 .zip 文件的完整路径。

例如：

```
flrinst -op=install -package=c:\installs\myFlexResponse_plugin.zip  
-p=myToolsPassword
```

请参见第 1164 页的“[部署 Endpoint FlexResponse](#)”。

请参见第 1167 页的“[关于 Endpoint FlexResponse 实用程序](#)”。

在 Enforce Server 上启用 Endpoint FlexResponse

在响应规则中使用 Endpoint FlexResponse 插件之前，必须通过 Enforce Server 启用 Endpoint FlexResponse 功能。默认情况下，Endpoint FlexResponse 功能未启用。可以通过“高级代理设置”启用 Endpoint FlexResponse 功能。

启用 Endpoint FlexResponse 功能

- 1 打开 Enforce Server 管理控制台并导航至“系统”>“代理”>“代理配置”，然后打开当前应用于以下 Endpoint Server 的代理配置：此 Endpoint Server 连接到要将 Endpoint FlexResponse 插件部署到的代理。
- 2 单击“高级代理设置”选项卡。
- 3 找到 PostProcessor.ENABLE_FLEXRESPONSE.int 设置。

4 将此设置更改为 1。

5 单击“保存并应用”。

请参见第 668 页的“[添加新的响应规则](#)”。

请参见第 1164 页的“[部署 Endpoint FlexResponse](#)”。

请参见第 1165 页的“[关于在端点计算机上部署 Endpoint FlexResponse 插件](#)”。

使用 Endpoint FlexResponse 实用程序卸载 Endpoint FlexResponse 插件

从端点计算机中卸载 Endpoint FlexResponse 插件

- 1 在端点计算机上打开一个命令窗口，然后导航至 Symantec DLP Agent 安装目录。此目录的默认位置是 c:\Program Files\Manufacturer\Endpoint Agent。
- 2 输入下列命令：

```
flrininst.exe -op=uninstall  
-package=<Plug-in name>  
-p=<myToolsPassword>
```

其中：

- <Plug-in name> 是插件软件包 .zip 文件的名称。
- <myToolsPassword> 是用于 Symantec Data Loss Prevention 部署的工具密码。如果您尚未指定工具密码，请使用默认密码：vontustop。

例如：

```
flrininst -op=uninstall -package=myFlexResponse_plugin.zip  
-p=myToolsPassword
```

从特定端点计算机中检索 Endpoint FlexResponse 插件

使用以下过程从端点计算机中检索特定插件。一次只能在一台端点计算机上使用检索功能。插件以 .zip 文件的形式显示在 Symantec DLP Agent 安装目录中。插件脚本是一个具有 .py 扩展名的纯文本文件，位于 .zip 文件内。

您可以通过编辑 .py 文件来编辑插件。如果进行了编辑，则必须先重新打包此 ZIP 文件并将插件重新部署到端点计算机，然后所做的编辑才会生效。修改的插件只影响进行修改时所在的单个端点计算机。

从特定端点计算机中检索 Endpoint FlexResponse 插件

- 1 在端点计算机上打开一个命令提示符窗口，然后导航至 Symantec DLP Agent 安装目录：

此目录的默认位置是 c:\Program Files\Manufacturer\Endpoint Agent\

- 2 输入下列命令：

```
firlinst -op=retrieve -package=<Plug-in name> -p=<myToolsPassword>
```

其中：

- <myToolsPassword> 是用于 Symantec Data Loss Prevention 部署的工具密码。如果您尚未指定工具密码，请使用默认密码：VontuStop。
- <plug-in name> 是插件 .zip 文件的名称。

例如：

```
firlinst -op=retrieve -package=myFlexResponse_plugin.zip  
-p=myToolsPassword
```

从端点计算机中检索 Endpoint FlexResponse 插件列表

请遵照以下过程检索特定端点计算机上已部署的插件的列表。您只能在单个端点计算机上使用列表功能。您无法在一组端点计算机上使用列表功能。

插件列表仅包含插件软件包的名称。列表不包含有关插件的任何类型描述。Symantec 建议您对插件采用描述性名称，以便您可以在列表中识别它们。

从端点计算机中检索 Endpoint FlexResponse 插件列表

- 1 在端点计算机上打开一个命令窗口，然后导航至 Symantec DLP Agent 安装工具目录。此目录的默认位置是 c:\Program Files\Manufacturer\Endpoint Agent\。
- 2 输入下列命令：

```
flrininst.exe -op=list -p=<myToolsPassword>
```

其中：<myToolsPassword> 是用于 Symantec Data Loss Prevention 部署的工具密码。如果您尚未指定工具密码，请使用默认密码：VontuStop。

例如：

```
flrininst -op=list -p=myToolsPassword
```

已部署的 Endpoint FlexResponse 插件的列表将显示在命令窗口中。

实施 Symantec DLP Agent

本章节包括下列主题：

- [关于 Symantec Management Console](#)
- [关于 Symantec DLP Agent 安装](#)

关于 Symantec Management Console

包括 Endpoint Discover 或 Endpoint Prevent 的 Symantec Data Loss Prevention 安装可以选择使用 Symantec Management Console 进行端点管理。Symantec Management Console (SMC) 是 Symantec Management Platform 的一部分，它提供一种集中的方式来管理 Symantec DLP Agent 的安装、升级和卸载。使用 SMC，您可查找组织中的所有端点计算机并将其添加到 SMC 进行管理。您还可以创建自己的组织结构，或是使用预定义的结构，例如 Active Directory (AD)。Symantec Management Console 包括故障排除工具，允许您在发生问题时调查 Symantec DLP Agent。

注意：与 Symantec Data Loss Prevention 一起安装和使用 Symantec Management Console 是可选的。您不需要使用 Symantec Management Console 保护您的数据。但是，Symantec Management Console 提供了 Symantec Data Loss Prevention 中未提供的若干工具和功能。

Symantec Management Console 使用单一登录 (SSO) 技术。您不需要为 Symantec Data Loss Prevention 与 Symantec Management Console 维护不同的凭据。

有关 Symantec Management Platform 的其他信息，请参考以下文档：

- SymWISE 上提供的“安装 Symantec Management Platform 产品”，网址为：<http://www.symantec.com/docs/HOWTO9795>。本文提供了安装 Symantec Installation Manager (SIM) 和 Symantec Management Platform (SMP) 的概述和步骤。

- 可从以下网址获取《Symantec Management Platform 安装指南》：
http://go.symantec.com/sim_doc。它包括安装基础架构（可安装 Data Loss Prevention 集成组件）的相关信息。
- 《Symantec Management Platform 安装使用指南》包含配置基础架构组件（例如，设置角色和权限）的相关信息。安装后，您可参见 Symantec Management Platform 中的帮助。
请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。
请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。
请参见第 1176 页的“[关于 Symantec Management Console 代理任务](#)”。

克隆广告与程序

如果您有多个 Endpoint Server，则可以克隆您的广告与程序。通过该过程，您可以在每个 Endpoint Server 上安装、升级或卸载 Symantec DLP Agent 和 Symantec Management Agent。通过克隆广告与程序，您可以为每个 Endpoint Server 复制特定的安装参数。为克隆的广告命名时，请采用与命名程序类似的方式。

例如，您创建了一个程序与广告，以将 Symantec DLP Agent 安装在名为 EndpointServer1 的 Endpoint Server 上。另外，您还有一个名为 EndpointServer2 的 Endpoint Server。您应克隆用于 EndpointServer1 的程序与广告，并将克隆重命名为 EndpointServer2。将在 EndpointServer2 中保留您为 EndpointServer1 指定的所有安装参数。必须为第二个 Endpoint Server 更改目标目录。

克隆广告与程序

- 1 在 Symantec Management Console 中，查找您想要克隆的广告或程序。
- 2 右键单击广告，然后选择“克隆”。
- 3 为克隆的广告或程序输入名称。
- 4 单击“确定”。
- 5 调整目标设置以及所需的任何其他参数。

有关 Symantec Management Console 及其提供的功能的更多信息，请参见 *Symantec Management Platform Administration Guide*（《Symantec Management Platform 管理指南》）。

请参见第 1173 页的“[关于 Symantec Management Console](#)”。

使用计算机发现

计算机发现允许您使用 Symantec Management Console 查找和注册所有端点计算机。此功能允许您查看网络上存在多少端点计算机，以及需要安装多少 Symantec DLP Agent。您可以将 Active Directory 用于添加端点计算机，也可以浏览不同的

域来指定所需的网络。您在网络中指定的任何端点计算机都可用于安装，也可以手动将计算机添加到网络。

使用计算机发现

- 1 在 DLP 门户页面的“发现计算机”部分下。
- 2 选择“AD 导入”选项或“域浏览”选项。
- 3 如果选择“域浏览”，则可输入域名称或在“域选择器”中浏览以添加域。选择需要让发现计算机工具更新端点计算机列表的计划，然后单击“保存更改”。
- 4 如果选择“AD 导入”，请选择需要用于发现端点计算机的资源导入规则，然后选择目录同步计划。单击“保存更改”。

请参见第 1173 页的“[关于 Symantec Management Console](#)”。

安装 Symantec Management Agent

在安装 Symantec DLP Agent 之前，必须安装 Symantec Management Agent。Symantec Management Agent 与 Symantec DLP Agent 可在端点计算机上同时运行。Symantec Management Agent 允许您部署 Symantec DLP Agent。还允许您使用许多代理排除故障任务。

注意：在 Symantec Data Loss Prevention v11.x 中，支持 SMP v7.0 和 SMP v7.1。

安装 Symantec Management Agent

- 1 在 DLP 门户页面中，单击“**安装 Symantec Management Agent**”链接。
- 2 单击“选择计算机”选项，然后选择要安装 Symantec Management Agent 的特定端点计算机。
- 3 单击“**安装 Symantec Management Agent**”选项。
- 4 单击“继续安装”。安装将立即启动。

注意：如果要按计划设置安装，请单击“安装设置”并修改弹出式窗口中的设置。

在安装 Symantec Management Agent 后，可以安装 Symantec DLP Agent。

关于 Symantec Management Console 报告

您可以查看关于两个代理的安装更新与部署更新的报告和 Get 状态。这些报告包含在 Symantec Management Console 应用程序的门户页面中。通过转到导航窗格中的“报表”>**DLP IC** 查看报告。

报告将显示：

- 网络中装有 Symantec DLP Agent 的端点计算机的数量。
- 关于仍未安装 Symantec DLP Agent 的端点计算机数量的状态更新。
- 已安装 Symantec DLP Agent 但未向 Symantec Management Console 注册的端点计算机的数量。
- 处于各个状态的端点计算机所占的百分比。
- DLP 打印屏幕的状态在端点计算机上表明。
此状态指示打印屏幕功能是否已禁用。
- Symantec DLP Agent 配置状态详细信息。
此报告指示代理的详细信息以及分配给这些代理的当前配置。

根据所需的报告类型，您可以向报告中添加过滤器，以查看特定信息。

系统管理员可以通过 Symantec Management Console 创建自己的报告。

有关 Symantec Management Console 中报告功能的更多信息，请参见 *Symantec Management Platform User's Guide*. (《Symantec Management Platform 用户指南》)。

您也可以看见不同的任务，以及 Symantec Management Agent 执行的任务的状态。任务与其状态分成下列部分：

- 说明
- 开始时间
- 状态

您可以依状态将这些 Symantec Management Agent 任务分组，还可以搜索特定任务。

有关更多信息，请参见《Symantec Management Platform 安装使用指南》。

请参见第 1173 页的“[关于 Symantec Management Console](#)”。

关于 Symantec Management Console 代理任务

Symantec Management Console 随附多种任务，可让您在发生问题时排除 Symantec DLP Agent 故障。代理任务包括以下内容：

- 启动代理

选择“启动代理”任务，会手动启动网络中特定的 Symantec DLP Agent。

■ 停止代理

选择“停止代理”任务，会停止网络中特定的 Symantec DLP Agent。

■ 重新启动代理

选择“重新启动代理”任务，会重新启动网络中已停止的特定 Symantec DLP Agent。

■ 终止代理

允许您终止 Symantec DLP Agent。

■ 更改 Endpoint Server

允许您指定当前 Endpoint Server 的主机名和 IP 地址。还允许您指定在主服务器失败时所启用的辅助 Endpoint Server。

■ 设置 DLP Agent 配置

将端点配置分配给 Symantec DLP Agent。

请参见第 1155 页的“[关于代理配置](#)”。

■ 获取代理配置

选择“获取配置”任务，会收集 Symantec Management Agent 的配置。此信息存储在 DLP IC 配置页面中指定的路径。

■ 切换打印屏幕

启用或禁用打印屏幕功能。

■ 提取代理日志

选择“提取代理日志”任务，会收集网络中特定 Symantec DLP Agent 的活动日志。

■ 将日志级别设为信息

选择“将日志级别设为信息”任务，允许您将特定日志的日志级别仅设为“信息”。您也可以设置个别的目标代理组件。

■ 将日志级别设为最精细

选择“将日志级别设为最精细”，允许您将特定日志的日志级别尽可能设置为最精细的详细信息。您也可以设置个别的目标代理组件。

有关更多信息，请参见《Symantec Management Platform 安装使用指南》。

创建用户任务

可以在 Symantec Management Console 的门户页面上创建除预定义任务之外的其他任务。例如，可以创建让您修改非默认记录程序上的日志级别的新任务。任务会自动显示在 Symantec Management Console 门户页面上的任务列表中。您可以从任务列表中删除任何您创建的任务。但不能删除任何预定义任务。

请参见第 1176 页的“[关于 Symantec Management Console 代理任务](#)”。

创建您自己的任务

- 1 在顶部的菜单中，转至“管理”>“任务和作业”。
- 2 单击“创建任务”链接。
- 3 从可用的树中选择任务类型。
- 4 输入任务的名称。
- 5 编辑信息以创建任务的具体信息。
- 6 设置要与此任务关联的服务器的任务服务器详细信息。
- 7 单击“确定”。

有关创建您自己的任务的更多信息，请参见《Symantec Management Platform 安装使用指南》。

请参见第 1173 页的“[关于 Symantec Management Console](#)”。

关于 Symantec DLP Agent 安装

您可以使用自动方法安装代理软件或者手动安装代理软件。

开始之前，确保已安装并配置 Endpoint Server。如果使用 Symantec Management Console (SMC) 来安装您的代理，还必须先安装 SMC。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

Symantec DLP Agent 的已安装内容

将 DLP Agent 安装到端点计算机上时，会同时安装几个组件。不要禁用或修改其中任何组件，否则 DLP Agent 可能无法正常工作。

表 79-1 安装的组件

组件	说明
驱动程序 (vfsmfd.sys)	检测端点文件系统中的任何活动，并将信息中继到 DLP Agent 服务。 此驱动程序安装在 Windows_dir\System32\drivers 下面。 例如，c:\windows\System32\drivers。 所有其他代理文件安装于代理安装目录中。

组件	说明
驱动程序 (tdifd116.sys)	<p>截取端点计算机上的网络流量（HTTP、FTP 及 IM 协议）。在 Symantec Data Loss Prevention Agent 分析内容后，tdifd105.sys 驱动程序会允许或阻止通过网络传输数据。</p> <p>此驱动程序安装在 <i>Windows_dir\System32\drivers</i> 下面。例如，<i>c:\windows\System32\drivers</i>。所有其他代理文件安装于代理安装目录中。</p>
驱动程序 (vrtam.sys)	<p>监视进程的创建及破坏，并将通知发送至 DLP Agent。此驱动程序会监视配置为“端点应用程序控制”一部分的应用程序；例如，CD/DVD 应用程序。</p> <p>此驱动程序安装在 <i>Windows_dir\System32\drivers</i> 下面。例如，<i>c:\windows\System32\drivers</i>。所有其他代理文件安装于代理安装目录中。</p>
驱动程序 (SFsCtrx116.sys)	<p>监视 Citrix XenApp 和 XenDesktop 上的活动。</p> <p>此驱动程序安装在 <i>Windows_dir\System32\drivers</i> 下面。例如，<i>c:\windows\System32\drivers</i>。所有其他代理文件安装于代理安装目录中。</p>
Symantec DLP Agent 服务	<p>接收来自驱动程序的所有信息，并将信息中继到 Endpoint Server。在安装期间，DLP Agent 在任务管理器下列为 edpa.exe。</p> <p>用户无法在他们的工作站上停止或删除此服务。</p>
监视程序服务	<p>进行自动检查，以查看 DLP Agent 是否正在运行。如果 DLP Agent 已停止，监视程序服务会重新启动 DLP Agent。这是一种交互关系。</p> <p>用户无法在他们的工作站上停止或删除此服务。</p>

DLP Agent 服务创建以下文件：

- 两个日志文件 (*edpa.log* 和 *edpa_ext.log*)，在安装目录中创建。

- 每个 DLP Agent 都会在端点上维护加密的数据库。数据库会存储事件信息及触发事件的原始文件（如果需要）。根据所使用的检测方法，DLP Agent 会在本地分析内容，或将其发送至 Endpoint Server 以供分析。
 - 将安装一个名为 rrc.ead 的数据库，以维护和包含规则结果缓存 (RRC) 的非匹配条目。请参见第 1140 页的“[关于规则结果缓存 \(RRC\)](#)”。
- 请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。
- 请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于 Symantec DLP Agent 的安装前步骤

安装 Symantec DLP Agent 之前，请确定端点计算机上运行的所有安全应用程序。然后配置这些应用程序以便允许 Symantec DLP Agent 运行所有功能。某些应用程序会在检测到 Symantec DLP Agent 的安装或初次启动时生成警报。这些警报揭示 Symantec DLP Agent 的存在，并且有时会允许用户完全阻止 Symantec DLP Agent。

请检查以下应用程序：

- 防病毒软件
- 防火墙软件

确保防病毒软件和防火墙软件均将 Symantec DLP Agent 认可为合法的程序。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

在 Windows Vista 和 Windows 7 中使用“提升的命令提示符”

如果您在运行 Windows Vista 或 Windows 7 的端点计算机上安装代理，则必须以“提升的命令提示符”模式运行命令提示符。鉴于 Windows Vista 操作系统的性质，此步骤为必须执行的步骤。如果没有先使用“提升权限的命令提示符”模式，则不能使用 install_agent.bat 脚本来安装代理。

在 Windows Vista 上启动“提升的命令提示符”模式

- 1 在 Windows “开始”菜单中的命令提示符图标上单击鼠标右键。
- 2 选择“以管理员身份运行”。

将以“提升的命令提示符”模式启动命令提示符。现在，您可以在端点计算机上安装 Symantec DLP Agent。

如果在 Windows 7 上安装，请按照以下过程使用“提升的命令提示符”模式。

在 Windows 7 上启动“提升的命令提示符”模式

- 1 单击“开始”菜单。
- 2 在“搜索程序和文件”字段，键入命令提示符。
“命令提示符”程序将显示在结果列表中。
- 3 按住 Shift 键并右键单击结果列表中的“命令提示符”条目。选择“以管理员身份运行”或“以其他用户身份运行”。
- 4 如果选择“以其他用户身份运行”，请输入具有管理员权限的用户的凭据。
- 5 将以“提升的命令提示符”模式启动命令提示符。使用该命令提示符在端点计算机上安装 Symantec DLP Agent。

请参见第 1143 页的[“如何实施 Endpoint Discover”](#)。

请参见第 1151 页的[“如何实施 Endpoint Prevent”](#)。

关于 Symantec DLP Agent 安全

Symantec Data Loss Prevention 使用高级加密标准 (AES) 技术来保护 Endpoint Server 和 Symantec DLP Agent 之间的通信。Symantec Data Loss Prevention 也使用 AES 来保护 Symantec DLP Agent 数据库文件的安全。

AES 是对称式密钥加密技术，支持大小为 128、192 及 256 位的密钥。

Symantec Data Loss Prevention 使用以下几组 AES 密钥：

- 一组用于保护代理数据库文件
- 一组用于验证 Endpoint Server 至 Symantec DLP Agent
- 一组用于加密 Endpoint Server 与 Symantec DLP Agent 之间的流量

数据库文件密钥仅用于 Symantec DLP Agent。不过，Endpoint Server 与 Symantec DLP Agent 必须共享身份验证密钥和流量加密密钥。默认情况下，Symantec Data Loss Prevention 会使用预定义的 128 位数据库密钥和身份验证密钥。流量加密密钥是随机生成的会话密钥，每次 Symantec DLP Agent 连接至 Endpoint Server 时都会协商该密钥。

虽然 Symantec Data Loss Prevention 中的信息是安全的，还是请您更改默认密钥。您可以更改数据库密钥、身份验证密钥及 AES 密钥的大小（128、192 及 256）。部署 Symantec DLP Agent 之前，您应当更改这些默认设置（将它们更改为使用唯一密钥或更改密钥大小）。Symantec Data Loss Prevention 包括 endpointkeytool 实用程序，以生成身份验证密钥。endpointkeytool 实用程序也允许您创建访问其他端点工具所需的工具密码。

请参见第 1211 页的[“关于端点工具”](#)。

请参见第 1212 页的“[关于 endpointkeytool 实用程序](#)”。

请参见第 1213 页的“[运行 endpointkeytool 实用程序](#)”。

每次 Symantec DLP Agent 连接至 Endpoint Server 时，都会随机生成新的流量加密密钥。一旦服务器与代理之间的连接会话结束，即会丢弃该密钥。每个 Symantec DLP Agent 连接会话的流量加密密钥都是唯一的。Endpoint Server 与所有 Symantec DLP Agent 通常会共享身份验证密钥。

默认情况下，Symantec Data Loss Prevention 配置为使用 128 位密钥来保护 Endpoint Server 和 Symantec DLP Agent 之间的通信。然而，可以增加身份验证密钥的大小以增强加密强度。如果增加了身份验证密钥的大小，则流量加密密钥的大小也会自动增加。通过此方式，这两个加密密钥始终具有匹配的大小。只有在安装 Symantec DLP Agent 前，才能更改身份验证密钥的大小。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于身份验证密钥

为所有的 Symantec Data Loss Prevention 客户提供了默认的 128 位身份验证密钥，该密钥已硬编码到产品中。此身份验证密钥适用于许多客户，但是您可以选择生成新的身份验证密钥。替换身份验证密钥前，您需要考虑数个要素。

生成新身份验证密钥的优点如下：

- 新的 AES 密钥可将您与其他使用默认密钥的 Symantec 客户隔离开来。默认配置将使用已硬编码为 Symantec Data Loss Prevention 的身份验证密钥。除非更改密钥，否则所有 Symantec Data Loss Prevention 客户都使用相同的身份验证密钥。
- 增加身份验证密钥的大小至 192 位或 256 位，可提高数据流量的加密安全性。密钥愈大，数据安全就愈不容易受到影响。

生成新身份验证密钥的缺点如下：

- 安装 Symantec DLP Agent 前，必须进行提前规划。安装代理后，您就不能再更改身份验证密钥。
- 美国政府规定使用 192 位及 256 位的 AES 密钥。出口法律高度限制在美国以外的地区使用这些密钥。使用较大的密钥还会影响系统性能。

您可以使用 endpointkeytool 实用程序更改身份验证密钥。

请参见第 1212 页的“[关于 endpointkeytool 实用程序](#)”。

请参见第 1213 页的“[运行 endpointkeytool 实用程序](#)”。

请参见第 1211 页的“[关于端点工具](#)”。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于监视程序服务

使用 DLP Agent 来部署监视程序服务。监视程序是一种确保 DLP Agent 已运行且处于活动状态的服务。这是一种交互关系。如果 DLP Agent 未收到来自监视程序服务的定期请求，它会自动重新启动监视程序服务。此交互关系可确保 DLP Agent 始终运行且处于活动状态。

用户无法停止其工作站上的监视程序服务。防止用户停止监视程序服务可使 DLP 代理在其工作站上保持使用中状态。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于 Endpoint Server 冗余

可以将 Symantec DLP Agent 配置为连接到多个 Endpoint Server。通过多个 Endpoint Server，可以在 Endpoint Server 不可用时及时将事件发送到 Enforce Server。例如，假设由于网络分隔区而使某个 Endpoint Server 不可用。在指定时间后，Symantec DLP Agent 会连接至其他 Endpoint Server，以传输已存储的事件。仅在当前 Endpoint Server 不可用时，Symantec DLP Agent 才会尽量故障转移至其他 Endpoint Server。如果原始 Endpoint Server 不可用，则 Agent 会尝试连接至配置列表中的其他 Endpoint Server。默认情况下，Symantec DLP Agent 会在 60 分钟内尝试重新连接至原始 Endpoint Server，之后才会接入至其他 Endpoint Server。

Symantec DLP Agent 连接至新 Endpoint Server 时，会从该 Endpoint Server 下载策略。然后立即开始应用新策略。要确保故障转移后事件检测的一致性，请在 Symantec DLP Agent 可能会连接的所有 Endpoint Server 上保留相同的策略。

对于 Endpoint Discover 监视，如果在扫描期间进行故障转移，则会中止旧的 Endpoint Discover 扫描。Symantec DLP Agent 会从新的 Endpoint Server 下载新的 Endpoint Discover 扫描配置与策略，并立即运行新扫描。只有当有效的 Endpoint Discover 扫描在新的 Endpoint Server 上配置时，才会运行新的扫描。

必须在安装 Symantec DLP Agent 时指定 Endpoint Server 的列表。添加 Endpoint Server 列表的过程显示在每种安装方法的下面。您可以指定含相关端口号的 IP 地址或主机名称。如果您指定主机名称，则 Symantec DLP Agent 会执行 DNS 查找以获取一组 IP 地址。然后会连接至每个 IP 地址。使用主机名称和 DNS 查找允许您进行动态配置更改，而不依赖所指定 IP 地址的静态安装时列表。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于 AgentInstall.msi 软件包

可以使用 AgentInstall.msi 软件包（或适用于 64 位 Windows 7 平台的 AgentInstall64.msi 软件包）在端点计算机上安装、配置或升级 Symantec DLP Agent。Symantec Management Console 或 Systems Management Server (SMS) 使用 Windows msixexec 安装程序以静默方式执行该软件包。您也可以通过在端点计算机上执行 AgentInstall.msi 软件包本身来以交互方式运行软件包安装程序。

AgentInstall.msi 软件包可接受各种配置属性，而不管您选择何种方法安装 Symantec DLP Agent。[表 79-2](#) 说明了 AgentInstall.msi 和 AgentInstall64.msi 的必需属性和可选属性。

表 79-2 AgentInstall.msi 和 AgentInstall64.msi 属性

属性名称	说明	必需或可选	默认值
ENDPOINTSERVER	<p>指定一个或多个 Endpoint Server 的主机名或 IP 地址（以分号分隔）。每个主机名称或 IP 地址都可后跟可选的端口号。如果未指定端口号，则会使用默认端口号。默认端口号为 8000。</p> <p>例如：</p> <pre>ENDPOINTSERVER="epserver.company.com;10.67.20.36:8002"</pre>	必需	None
ENABLEFIPS	启用 FIPS 兼容加密。如果需要，将此属性设为 Yes 以启用 FIPS 加密。	可选	Yes
KEY	<p>Symantec DLP Agent 和 Endpoint Server 用于建立安全连接的身份验证密钥。代理中包含一个默认的身份验证密钥，但是您可以使用 endpointkeytool 实用程序创建自己的密钥。要使用自己的密钥，请在部署及安装期间使用 KEY 参数指定。如果您在安装 Symantec DLP Agent 后决定指定密钥，则必须重新安装 Symantec DLP Agent 才能指定密钥。</p> <p>请参见第 1212 页的“关于 endpointkeytool 实用程序”。</p>	可选	None (使用常用默认密钥)。
SERVICENAME	指定在端点计算机的服务列表中显示的 Symantec DLP Agent 服务名称。Symantec DLP Agent 在计算机的任务列表中显示为 edpa.exe。	可选	EDPA
STARTSERVICE	确定是否在安装后在端点计算机上启动 Symantec DLP Agent 和监视程序服务。将此属性设为 No，可禁止在安装后启动这些服务。	可选	Yes
WATCHDOGNAME	指定在端点计算机的服务列表中显示的监视程序服务名称。监视程序在任务管理器中会显示为 wdp.exe。	可选	WDP

msiexec 安装程序还具有几个在安装 AgentInstall.msi 软件包时常用的公共属性。这些属性包括：

■ ARPSYSTEMCOMPONENT

此属性可防止在端点计算机的“添加或删除程序”(ARP)列表中显示 Symantec DLP Agent。如果您将该属性设置为 1，Symantec DLP Agent 将不会显示在列表中。默认情况下，该属性设置为 0，允许 Symantec DLP Agent 显示在 ARP 列表中。

■ INSTALLDIR

此属性可指定安装目录。默认安装目录为 *install_dir\Manufacturer\Endpoint Agent*。例如，*c:\Program Files\Manufacturer\Endpoint Agent*。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

关于卸载密码

卸载密码可防止未经授权的用户从端点计算机中删除 Symantec DLP Agent。如果未经授权的用户尝试不使用密码删除代理，将无法删除代理。

在代理安装期间创建或分配密码时，只有将代理删除然后重新安装后才能更改该密码。当您要从端点计算机中删除代理时，卸载密码参数弹出窗口将要求输入卸载密码。如果使用代理管理系统从大量端点计算机中删除代理，必须在卸载命令行中包括密码。

默认情况下，管理员可以输入错误密码的次数是有限制的。如果超过该限制，将退出卸载过程，且必须重新启动该过程。

可以使用 UninstallPwdKeyGenerator.exe 工具生成安全的卸载密码。

如果要将不同的密码分配给不同的端点计算机组，可以生成多个密码。

请参见第 1218 页的“[使用密码生成工具创建密码](#)”。

请参见第 1185 页的“[向代理添加卸载密码](#)”。

请参见第 1187 页的“[升级代理和卸载密码](#)”。

请参见第 1186 页的“[使用卸载密码](#)”。

向代理添加卸载密码

卸载密码可防止未经授权的用户从端点计算机中删除 Symantec DLP Agent。

只能在代理安装或升级期间将密码添加到 Symantec DLP Agent。如果存在要保护的现有代理，您必须删除代理，然后重新安装具有密码的代理。

使用 UninstallPwdKeyGenerator.exe 工具生成密码。

请参见第 1218 页的“[使用密码生成工具创建密码](#)”。

可以通过将密码参数包含到代理安装命令行中来添加卸载密码。您可以使用 Symantec Management Platform (SMP) 或软件管理系统 (SMS) 程序来安装具有卸载密码的代理。

请参见第 1178 页的“[关于 Symantec DLP Agent 安装](#)”。

不能通过安装向导将卸载密码添加到代理中。

将卸载密码添加到代理安装中

- ◆ 将卸载密码参数添加到代理安装命令行中

```
UNINSTALLPASSWORDKEY="<password key>"
```

其中 *<password key>* 是使用密码生成工具创建的密码。

示例代理安装命令行可能如以下示例所示：

```
msiexec /i AgentInstall.msi /q
INSTALLDIR="%ProgramFiles%\Manufacturer\Endpoint Agent\
ENDPOINTSERVER="hostname" PORT="8000" KEY="" UNINSTALLPASSWORDKEY=
"<password key>" SMC="hostname" SERVICENAME="EDPA" WATCHDOGNAME="WDP"
```

请参见第 1186 页的“[使用卸载密码](#)”。

使用卸载密码

当您需要卸载受密码保护的 Symantec DLP Agent 时，必须输入正确的密码才能继续卸载。如果手动卸载代理，将在端点计算机上显示弹出窗口，要求输入密码。您必须在该窗口中输入密码。如果使用软件管理系统，请在命令字符串中包括密码。

如果要卸载一组代理，请在代理卸载命令行中指定卸载密码。

使用命令行输入卸载密码

- ◆ 在卸载命令行中输入以下参数：

```
UNINSTALLPASSWORD="<password>"
```

其中 *<password>* 是在密码生成器中指定的密码。

代理命令行如以下示例所示：

```
msiexec /uninstall <product code> /q UNINSTALLPASSWORD="<password>"
```

请参见第 1218 页的“[使用密码生成工具创建密码](#)”。

请参见第 1185 页的“[关于卸载密码](#)”。

升级代理和卸载密码

可以在不影响密码的情况下升级受卸载密码保护的任何代理。如果您不希望更改密码，则不要将密码参数包括到升级命令行中。先前存在的卸载密码会自动包括在已升级的代理中。仅当要更改密码或将新密码添加到代理中时，才需要包括密码参数。

在升级代理时添加或更改密码

- ◆ 将以下密码参数添加到升级命令行中：

```
UNINSTALLPASSWORDKEY=<password key>
```

其中 <password key> 是使用密码生成工具创建的密码。

请参见第 1218 页的“[使用密码生成工具创建密码](#)”。

请参见第 1185 页的“[关于卸载密码](#)”。

使用 Symantec Management Console 安装 Symantec DLP Agent

可以使用 Symantec Management Console 安装 Symantec DLP Agent。Symantec Management Console 以半自动方式将 Symantec DLP Agent 组件安装到端点计算机上。

如果您之前购买并安装了 Symantec Management Console，则可以使用 Symantec Management Console 软件安装 Symantec DLP Agent。Symantec Management Console 以半自动方式将 Symantec DLP Agent 组件安装到端点计算机上。请注意，Symantec Data Loss Prevention 不包括 Symantec Management Console。

注意：要使用 Symantec Management Console 安装 Symantec DLP Agent，您必须首先使用 Symantec Management Console 的“计算机发现”功能。必须先安装 Symantec Management Agent。

请参见第 1176 页的“[关于 Symantec Management Console 报告](#)”。

Symantec Management Console 使用包含软件包、程序以及广告的系统来安装 Symantec DLP Agent。软件包包含安装目录的参考信息。程序本身是安装文件，且包含安装参数。您必须在安装程序的命令行中，指定与 Symantec DLP Agent 相关的 Endpoint Server。广告允许您指定想要安装 Symantec DLP Agent 的端点计算机，以及进行安装的时机。

您必须始终从本地目录安装 AgentInstall.msi 或 AgentINstall64.msi 软件包。如果您不是从本地目录安装，则会禁用 Symantec DLP Agent 的某些功能。

注意：Symantec Data Loss Prevention 支持 32 位和 64 位操作系统。标记有 **(x86)** 的 Symantec DLP Agent 链接安装或修改 32 位系统的 Symantec DLP Agent。标记有 **(x64)** 的 Symantec DLP Agent 链接安装或修改 64 位系统的 Symantec DLP Agent。

使用 Symantec Management Console 安装 Symantec DLP Agent

- 1 在 DLP 门户页面上，单击“**安装 Symantec DLP Agent (*bit information*)**”链接，其中 *(bit information)* 是所需的操作系统。
- 2 在右侧窗格中，单击红色的“关”图标旁边的下拉菜单，然后选择绿色的“开”图标。
- 3 确保将“程序名称”字段设置为“**安装 DLP Agent**”。
- 4 在“应用于”部分下，选择“应用于”>“计算机”菜单选项。根据需要添加过滤规则，选择端点计算机的子集。
将只在列出的计算机上安装 Symantec DLP Agent。
- 5 单击“**确定**”。
- 6 如果您想要调度日后再安装，请在“计划”部分中指定这些设置。
- 7 单击“**保存更改**”。

在保存有关安装的更改之后，请在 DLP 门户页面上查看安装状态。

使用无人参与安装方法安装 Symantec DLP Agent

您可以使用无人参与的安装过程（使用系统管理软件产品 (SMS)）将 Symantec DLP Agent 安装到端点计算机。您必须始终从本地目录安装 AgentInstall.msi 软件包。如果您不是从本地目录安装，则会禁用 Symantec DLP Agent 的某些功能。

执行无人参与的安装

- 1 在您的系统管理软件包中，请指定 AgentInstall.msi 或 AgentInstall64.msi 软件包。
- 2 指定 AgentInstall.msi 安装属性。
请参见第 1184 页的“[关于 AgentInstall.msi 软件包](#)”。
- 3 指定 msisexec 属性。
msisexec 实用程序的可选属性。
请参见第 1184 页的“[关于 AgentInstall.msi 软件包](#)”。
- 4 指定 msisexec 实用程序的任何可选属性。
请参见第 1184 页的“[关于 AgentInstall.msi 软件包](#)”。

有关如何将此信息输入到特定系统管理软件的详细信息，请参见软件产品文档。

安装 Symantec DLP Agent 时，您的系统管理软件会向指定的端点发出命令。命令的外观可能如以下示例所示：

```
msiexec /i AgentInstall.msi /q INSTALLDIR="C:\Program  
Files\Manufacturer\Symantec DLP Agent\" ARPSYSTEMCOMPONENT="1"  
ENDPOINTSERVER="epserver:8001"  
SERVICENAME="ENDPOINT" WATCHDOGNAME="WATCHDOG"
```

在此命令中：

`msiexec` 是用于执行 MSI 软件包的 Windows 命令。

`/i` 指定软件包的名称。

`/q` 指定静默安装。

`INSTALLDIR` 和 `ARPSYSTEMCOMPONENT` 是 `msiexec` 的可选属性。

`ENDPOINTSERVER`、`SMC`、`SERVICENAME` 和 `WATCHDOGNAME` 是 `AgentInstall.msi` 软件包的属性。

Symantec Data Loss Prevention 在 `install_dir\Endpoint\install_agent.bat` 中包括了示例安装命令。

安装代理后，每台端点计算机上的 Symantec DLP Agent 服务会自动启动。登录 Enforce Server，再转至“系统”>“代理”>“概述”。验证新安装或新升级的代理是否已注册（服务是否显示在列表中）。

注意：无论任何原因，请勿重命名 `Agentinstall.msi` 文件。如果您重命名此文件，系统管理软件将不能识别此文件，安装会失败。

注意：在安装 Symantec DLP Agent 过程中的某些阶段，可能会要求您重新启动端点计算机。

请参见第 1143 页的“[如何实施 Endpoint Discover](#)”。

请参见第 1151 页的“[如何实施 Endpoint Prevent](#)”。

手动安装 Symantec DLP Agent

您可以通过使用 `AgentInstall.msi` 或 `AgentInstall64.msi`（对于 64 位 Windows 7 平台）软件包在端点上手动安装 Symantec DLP Agent。

手动安装 Symantec DLP Agent

- 1 以管理员身份登录端点计算机。
- 2 将 AgentInstall.msi 或 AgentInstall64.msi 文件复制到端点计算机，然后双击该文件。
Symantec DLP Agent 安装向导将启动，显示 Symantec DLP Agent 设置面板。
- 3 单击 **Next** 以接受版权许可协议。
- 4 单击 **Next** 以接受授权许可协议。

注意：如果您的计算机尚未运行 Windows Installer 3.1，则 Symantec DLP Agent 安装程序会启动该程序的安装。在此情况下，系统会提示您在 Windows Installer 安装后重新启动计算机。重新启动之后，Symantec DLP Agent 安装程序会继续进行。

- 5 在以下字段中，键入适当的值：

■ **Endpoint Server**（必填）

输入至少一个 Endpoint Server 的主机名称或 IP 地址。例如，server.company.com。此值必须与您在 **Symantec Data Loss Prevention Enforce Server > Configure Server** 页面上为 Endpoint Server 设置的 **Agent Listener > Bind Address (Host/IP)** 值一致。如果您使用非默认端口号，请在服务器名称之后指定该端口号。例如，server.company.com:8001。

注意：您可以指定四个以上的 Endpoint Server。要执行此操作，请在提供的四个文本字段中的任一字段中输入一系列主机名称或 IP 地址（以分号分隔）。例如：epserver1.company.com; epserver2.company.com; epserver3.company.com; epserver4.company.com; 10.67.20.36:8002。

■ **Encryption Key**（可选）

您可以输入 Symantec DLP Agent 和 Endpoint Server 用于建立安全连接的自定义身份验证密钥。代理包括默认身份验证密钥，不过，您也可以使用 endpointkeytool 实用程序来创建自己的密钥。要使用自己的密钥，请在部署及安装期间使用 KEY 参数指定。如果您在安装 Symantec DLP Agent 后决定使用自定义密钥，则必须重新安装 Symantec DLP Agent 才能指定密钥。

■ **DLP Agent Service Name**（可选）

您可以编辑端点计算机的服务列表中显示的 Symantec DLP Agent 服务名称。

■ **DLP Watchdog Service Name**（可选）

您可以编辑端点计算机的服务列表中显示的监视程序服务名称。

- 6 单击 **Next**。
- 7 接受默认安装目录或输入新的安装目录，再单击 **Next**。
默认安装目录为 c:\Program Files\Manufacturer\Endpoint Agent。
- 8 在显示的 Confirm Installation 屏幕上，单击 **Install**。
安装过程需要一些时间。安装完成时，会显示“Installation Complete”屏幕。
- 9 单击 **Finish**。
- 10 转至“开始”>“控制面板”>“管理工具”，再双击“服务”。查找 Symantec DLP Agent 服务（列在于安装期间在“服务名称”字段中键入的名称下）。确保该服务正在运行。
现在 Symantec DLP Agent 将监视端点。
- 11 登录 Enforce Server，再转至 **System > Agents > Overview**。
- 12 验证 Symantec DLP Agent 是否已注册（显示在列表中）。
请参见第 1143 页的[“如何实施 Endpoint Discover”](#)。
请参见第 1151 页的[“如何实施 Endpoint Prevent”](#)。

管理 Symantec DLP Agent

本章节包括下列主题：

- [关于 Symantec DLP Agent 管理](#)
- [关于端点代理日志](#)

关于 Symantec DLP Agent 管理

您可以通过 Symantec Management Console 安装和管理 Symantec DLP Agent。安装完 Symantec DLP Agent 后，可以通过 Enforce Server 来管理它们。通过 Enforce Server，可以查看 Symantec DLP Agent 的事件和代理信息，并生成代理事件的报告。

Enforce Server 包含 Symantec DLP Agent 的概述、Symantec DLP Agent 事件的日志和升级实用程序。以下为您说明概览及事件日志页面。

要访问代理页面，请打开 **Enforce Server > “系统” > “代理”**。

请参见第 1193 页的“[使用代理概述屏幕](#)”。

请参见第 1198 页的“[代理管理事件屏幕](#)”。

使用代理概述屏幕

在代理概述屏幕上可以看到每个 Symantec DLP Agent 的状态。这些状态由每个代理旁边显示的各个图标来指明。您也可以对任意选定代理执行与代理相关的任务。使用复选框可选择想要修改的代理。

使用“操作”按钮可执行下列操作之一：

- [更改 Endpoint Server](#)
- [删除](#)
- [禁用](#)

- 启用
- 提取日志
- 删除“在调查中”
- 重置日志级别
- 重新启动
- 设置日志级别
- 设为“在调查中”
- 关闭

请参见第 1196 页的“[代理概述操作](#)”。

代理信息分为若干列。单击任何列标题，可在该列中按字母数字顺序对条目进行排序。要按倒序进行排序，请再次单击该列标题。默认情况下，Symantec Data Loss Prevention 会按照端点计算机名列出来代理。

表 80-1 代理概述屏幕

部分	说明
状态	<p>此代理的当前状态。</p> <p>可能的值有：</p> <ul style="list-style-type: none"> ■ 正常运行 表示代理服务和文件系统驱动程序正在运行，已创建缓存并且可用，已按预期建立连接。 ■ 警告 表示此代理可能需要引起关注。例如，当端点数据共享接近其存储限制时，Symantec Data Loss Prevention 会分配此状态。 ■ 中断 表示该代理已关闭，需要立即关注。例如，当数据共享为完全共享或不可用时，或者当连接断开时，Symantec Data Loss Prevention 会分配此状态。 ■ 日志状态更改 指出代理的日志级别已更改或重置。请参见第 1204 页的“关于端点代理日志”。 ■ 关闭 表示已通过“关闭”代理任务将该代理关闭，或者已在端点计算机关闭时将该代理关闭。 ■ 已禁用 表示已通过“禁用”代理任务禁用该代理。 ■ 在调查中 表示相关代理正在接受调查。代理可能由于多种原因而接受调查。这些原因包括：发送过多误报事件，或无法连接到 Endpoint Server。 可以对任何其他代理状态设置“在调查中”状态。 ■ 故障排除 表示代理上正在运行故障排除任务，或者代理上某故障排除任务刚过期。 可以将“故障排除”状态设置为任何其他代理状态。

部分	说明
计算机名称	端点计算机名。
最近的错误消息	Symantec Data Loss Prevention 会显示一条或多条与将代理状态更改为“关闭”的所有事件有关的消息。每条消息都会显示触发了状态更改的事件的时间和摘要。要查看特定代理的事件列表，请单击“代理管理概述”列表中的相关代理条目。
Endpoint Server	此代理所注册的 Endpoint Server。
IP	端点计算机 IP 地址。
版本	代理版本号。
连接	当前代理连接状态。
上次连接时间	某个具体 Symantec DLP Agent 上次连接到 Endpoint Server 的日期和时间。

可以按照多种条件（包括代理配置、服务器名称和代理 IP 地址）来总结代理概述页面。另外，还可以根据与 Symantec DLP Agent 相关的特定条件集合来对代理事件进行过滤。通过对代理进行总结和过滤，就可以按想要的顺序查看代理数据。例如，可以按照相关联的代理配置来总结代理，然后根据最近更新的代理来过滤这些配置。

请参见第 807 页的“[关于报告的过滤器和摘要选项](#)”。

请参见第 1198 页的“[代理管理事件屏幕](#)”。

代理概述操作

下表描述了可以在任何 Symantec DLP Agent 上执行的可用代理概述操作。

请参见第 1193 页的“[使用代理概述屏幕](#)”。

表 80-2 代理概述操作

操作	说明
更改 Endpoint Server	允许您更改代理连接到的 Endpoint Server。在主服务器出现故障且代理必须切换连接时，可以指定主 Endpoint Server 以及辅助 Endpoint Server。

操作	说明
删除	<p>删除代理</p> <p>当您删除代理时，会从 Endpoint Server 删除该代理以及所有关联事件。在 Enforce Server 管理控制台中将不再显示该代理。从 Endpoint Server 中删除代理并不意味着已将其从端点计算机中卸载。</p>
禁用	<p>禁用代理</p> <p>禁用代理并不从 Endpoint Server 中删除代理。禁用代理将禁用该端点计算机上的所有监控。关联的事件在 Endpoint Server 上仍然可见。与已删除的代理不同，已禁用的代理可以重新启用。</p>
启用	<p>启用已禁用的代理</p> <p>已启用的代理将自动与 Endpoint Server 重新连接并获取最新的策略。启用代理将启用该端点计算机上的监控。已启用的代理可以在 Endpoint Server 上记录事件。</p> <p>注意：在启用并重新启动代理之前，对关联策略的任何更新都不会发送到代理。</p>
提取日志	<p>用于提取代理的服务日志和操作日志。可以提取服务日志、操作日志或这两组日志。</p> <p>提取代理日志分为以下两步：</p> <ul style="list-style-type: none">■ 将代理日志从端点计算机提取到 Endpoint Server■ 收集从 Endpoint Server 到 Enforce Server 的代理日志 <p>从端点计算机提取日志时，日志以未加密的格式存储在 Endpoint Server 上。从 Endpoint Server 收集日志后，日志将从 Endpoint Server 中删除，且仅存储在 Enforce Server 上。您每次只能从一台端点计算机上收集日志。</p> <p>从 Enforce Server 日志页面访问日志。转至：“系统” > “服务器” > “日志” > “收集”。请参见第 244 页的“收集服务器日志和配置文件”。</p>
删除“在调查中”	从选定代理中删除“在调查中”标识。

操作	说明
重置日志级别	将指定代理的日志记录级别重置为默认“信息”级别。Symantec 技术支持使用代理日志进行疑难解答。 请参见第 1204 页的“ 关于端点代理日志 ”。
重新启动	重新启动指定的代理。
设置日志级别	设置指定代理的日志记录级别。Symantec 技术支持使用代理日志进行疑难解答。 注意： 建议您在更改代理的日志级别之前联络 Symantec 技术支持。 请参见第 1204 页的“ 关于端点代理日志 ”。
设为“在调查中”	在指定的代理上设置“在调查中”状态。 如果您认为代理存在某种问题，请将代理指定为“在调查中”。可以设置“在调查中”状态，而不管代理是正在运行、已禁用还是已关闭。在代理的主状态图标旁边将出现一个附加图标（标志）。
关闭	关闭指定的代理。 在关闭代理后，将无法通过 Enforce 管理控制台重新启动它。代理只能通过 Symantec Management Console (SMC) 或在单个端点计算机上重新启动。

可以在知识库文章中查看有关代理操作的最新信息。登录到 Altiris 知识库，网址为：<https://kb-vontu.altiris.com> 并搜索文章“关于 Symantec DLP Agent 故障排除任务”。或者，在登录后，可以搜索文章编号 54083。

代理管理事件屏幕

“代理管理事件”屏幕列出了在代理上所发生的事件。此类事件包括对数据库文件、连接、文件系统驱动程序和服务所做的更改。您可以过滤和总结事件列表，并单击各个事件条目以查看更多详细信息。

事件信息分为若干列。单击任何列标题，可在该列中按字母数字顺序对条目进行排序。要按倒序进行排序，请再次单击该列标题。默认情况下，Symantec Data Loss Prevention 按事件发生的时间顺序将其列出。

表 80-3 代理管理事件屏幕

条目	说明
类型	事件类型，包括下列可能值： 严重 代理信息 确定
时间	事件日期和时间。
Endpoint Server	与事件相关的 Endpoint Server 的名称。
计算机名称	端点计算机 IP 地址或主机名。
类别	事件类别，例如“代理服务状态”、“连接状态”、“文件系统驱动程序”或数据存储区。
子类别	事件子类别，例如“连接处于活动状态”或“连接已关闭”。

您可以单击任何事件以显示该事件的“代理事件详细信息”屏幕。

可以按照多种条件（包括代理配置、服务器名称和代理IP地址）来总结代理概述页面。另外，还可以根据与 Symantec DLP Agent 相关的特定条件集合来对代理事件进行过滤。通过总结和过滤事件可以按所需的顺序查看代理数据。例如，可以按照相关联的代理配置来总结代理，然后根据最近更新的代理来过滤这些配置。

请参见第 807 页的“[关于报告的过滤器和摘要选项](#)”。

关于代理事件过滤器选项

除默认的日期过滤器外，您还可以按事件类型（“严重”、“警告”、“信息”或“在调查中”）、与代理关联的 Endpoint Server、事件摘要信息和端点计算机名称进行过滤。

您还可以按 Symantec Data Loss Prevention 用于访问常规代理状态的信息的类别和子类别进行过滤。

表 80-4 代理事件过滤器选项

过滤器	说明
类别	事件所属的类别。事件的类型或类别有助于指定事件的严重性。例如，软件升级事件的严重性低于软件兼容性事件的严重性。搜索可包括或排除事件类别。
计算机名称	代理正运行于的端点计算机。搜索可基于完全匹配项进行包括、排除或搜索。如果仅使用一台计算机，则排除该计算机会导致没有匹配项。
服务器	代理事件所属的服务器。您可以包括或排除单个服务器中的所有事件。
子类别	事件类别的子类别。每个类别分成不同的子类别。例如，“配置更新”类别包含“配置错误”和“配置成功”子类别。
摘要	每个事件的基本信息。您可以按关键字或句子字符串进行过滤。过滤器可包括、排除摘要描述的完全匹配项或对其进行搜索。
类型	列出的事件类型。您可将事件列为严重，警告或信息。

选择过滤选项后，必须选择过滤器的子类别。例如，如果您按“类别”进行过滤，则必须选择特定类别，如“连接状态”。

请参见第 1198 页的“[代理管理事件屏幕](#)”。

关于 Symantec DLP Agent 删除

您可能需要从端点计算机中卸载 Symantec DLP Agent。您可以使用以下方式来卸载 Symantec DLP Agent：

表 80-5 [删除 Symantec DLP Agent](#)

[使用 Symantec Management Console 删除 Symantec DLP Agent](#)

[手动删除 Symantec DLP Agent](#)

[使用系统管理软件删除 Symantec DLP Agent](#)

使用 Symantec Management Console 删除 Symantec DLP Agent

可以使用 Symantec Management Console，从端点计算机删除 Symantec DLP Agent 和 Symantec Management Agent。

注意：Symantec Data Loss Prevention 支持 32 位和 64 位操作系统。标记有 **(x86)** 的 Symantec DLP Agent 链接安装或修改 32 位系统的 Symantec DLP Agent。标记有 **(x64)** 的 Symantec DLP Agent 链接安装或修改 64 位系统的 Symantec DLP Agent。

使用 Symantec Management Console 卸载 Symantec DLP Agent

- 1 在左侧的导航窗口中，转至：“**Data Loss Prevention** 门户” > “配
置” > “**V11.0 代理部署（位信息）**” > “卸载 DLP Agent（位信息）”，其中
(位信息) 为 32 位或 64 位系统文件夹。
- 2 在页面的右上角部分，单击红色的“关”图标，然后从下拉菜单中选择绿色的
“开”图标。
- 3 确保将“程序名称”字段设置为“卸载 Symantec DLP Agent”。
- 4 在“应用于”部分下，单击“应用于”选项，然后选择“计算机”。根据需要
添加过滤规则，选择端点计算机的子集。
将只从列出的计算机中卸载 Symantec DLP Agent。
- 5 单击“保存更改”。

注意：您也可调度卸载，使其在晚些时间运行。使用任务调度程序可调度要卸载代
理的时间。

有关使用 Symantec Management Console 的卸载选项的更多信息，请参见
《Symantec Management Platform 安装使用指南》。

请参见第 1200 页的“[关于 Symantec DLP Agent 删除](#)”。

请参见第 1173 页的“[关于 Symantec Management Console](#)”。

使用系统管理软件删除 Symantec DLP Agent

如果您在安装期间选择在“添加或删除程序”(ARP)列表中隐藏 Symantec Data
Loss Prevention 服务，请遵循此过程。由于 Symantec DLP Agent 未显示在 ARP
中，因此您不能将 ARP 列表用于卸载过程。您必须使用 MSI 命令才能删除 Symantec
DLP Agent。如果安装期间您已在 ARP 中隐藏 Symantec DLP Agent，则仅可使用
MSI 命令进行卸载。

使用 MSI 命令删除代理

1 打开命令提示符窗口。

2 输入以下字符串：

```
msiexec /x AgentInstall.msi
```

您可以将数个不同的选项添加至此命令提示符中。

3 单击“确定”。

将卸载 Symantec DLP Agent。

在代理未显示在 ARP 时手动删除代理

1 打开命令提示符窗口。

2 输入以下命令，其中 {*guid*} 是产品代码。您可以将数个其他选项添加至此命令提示符中：

```
msiexec /x {guid}
```

3 在该命令的末尾输入任何可选命令：

```
msiexec /x AgentInstall.msi
```

4 单击“确定”。

您可以将选项添加至卸载命令，例如：SilentMode 或 Logname。SilentMode 允许不必在桌面上显示用户界面即可卸载 Symantec DLP Agent。此安装在工作站的后台进行，用户看不到此安装。Logname 允许您设置所需的任何日志文件。但是仅当您具备原始安装程序时，才可使用此选项。如果您没有原始安装程序，则必须使用产品代码。

静默安装的代码为：

```
/QN:silentmode
```

Logname 的代码为：

```
/L*V _logname
```

msi.exe 具有数个其他选项。有关其他选项的信息，请参见 MSI 指南。

请参见第 1200 页的“[关于 Symantec DLP Agent 删除](#)”。

移除 Windows 7 或 Windows Vista 上的代理

如果从运行 Windows Vista 或 Windows 7 的端点计算机上卸载代理，则必须以“提升的命令提示符”模式运行命令提示符。鉴于 Windows Vista 操作系统的性质，此

步骤为必须执行的步骤。如果没有先使用“提升权限的命令提示符”模式，则不能使用 `install_agent.bat` 脚本来安装代理。

在 Windows Vista 上启动“提升的命令提示符”模式

- 1 在 Windows “开始”菜单中的命令提示符图标上单击鼠标右键。
- 2 选择“以管理员身份运行”。

将以“提升的命令提示符”模式启动命令提示符。现在，您可以在端点计算机上安装 Symantec DLP Agent。

如果在 Windows 7 上安装，则使用“提升的命令提示符”模式的过程如下。

在 Windows 7 上启动“提升的命令提示符”模式

- 1 单击“开始”菜单。
- 2 在“搜索程序和文件”字段，键入命令提示符。
“命令提示符”程序将显示在结果列表中。
- 3 按住 Shift 键并右键单击结果列表中的“命令提示符”条目。选择“以管理员身份运行”或“以其他用户身份运行”。
- 4 如果选择“以其他用户身份运行”，请输入具有管理员权限的用户的凭据。
- 5 将以“提升的命令提示符”模式启动命令提示符。使用该命令提示符在端点计算机上安装 Symantec DLP Agent。

请参见第 1200 页的[“关于 Symantec DLP Agent 删除”](#)。

手动删除 Symantec DLP Agent

您可以手动卸载 Symantec DLP Agent。只有在部署期间，将 Symantec DLP Agent 配置为显示在端点计算机的“添加或删除程序”列表中，才能进行手动卸载。

请参见第 1178 页的[“关于 Symantec DLP Agent 安装”](#)。

手动卸载代理

- 1 转至“开始”>“控制面板”，再双击“添加或删除程序”。
- 2 选择 **Agent Install**。
- 3 单击“删除”或“卸载”。

如果您使用 Windows Vista，系统会提示您使用“提升权限的命令提示符”模式。

请参见第 1200 页的[“关于 Symantec DLP Agent 删除”](#)。

关于端点代理日志

端点代理日志包含每个端点代理的服务和操作数据。每个端点代理都包含多个记录的组件。通过为每个端点代理组件设置日志级别，可以配置记录的信息量。配置端点代理组件的日志级别后，即可收集日志并将其发送给 Symantec 技术支持。

Symantec 技术支持可以使用这些日志进行疑难解答或提高 Symantec Data Loss Prevention Endpoint 安装的性能。

请参见第 1204 页的“[设置端点代理的日志级别](#)”。

请参见第 244 页的“[收集服务器日志和配置文件](#)”。

设置端点代理的日志级别

通过指定每个代理组件的日志级别，您可以配置为端点代理记录的数据量。Symantec 技术支持可以使用这些数据进行疑难解答或提高 Symantec Data Loss Prevention Endpoint 安装的性能。

请参见第 1204 页的“[关于端点代理日志](#)”。

注意：建议您在更改代理的日志级别之前，先联系 Symantec 技术支持。

设置端点代理的日志级别

- 1 在 Enforce 管理控制台中，导航至“系统”>“代理”>“概述”。
- 2 选择一个代理。
- 3 选择“操作”>“设置日志级别”。
- 4 从“日志级别”下拉列表中选择日志级别。
- 5 如果要更改此代理的所有组件的日志级别，请选择“所有组件”。
- 6 如果更改此代理的特定组件的日志级别，请在提供的字段中输入相应组件的名称。输入多个组件名称时，请使用逗号分隔各组件名称。针对输入组件名称所允许的最大长度为 255 个字符。
- 7 单击“确定”保存所做的更改。

“代理概述”屏幕会在代理旁边显示一个图标，表示已更改该代理的日志级别。

在对端点代理进行故障排除后，建议将代理的日志级别重置为默认设置。在重置代理的日志级别后，将仅记录代理的常规信息。

将端点代理的所有组件的日志级别重置为默认日志记录级别

- 1 在 Enforce 管理控制台中，导航至“系统”>“代理”>“概述”。
- 2 从列表中选择代理。
- 3 选择“操作”>“重置日志级别”。

“代理概述”屏幕会在代理旁边显示一个图标，表示已更改该代理的日志级别。

关于应用程序监控

本章节包括下列主题：

- [关于应用程序监控](#)
- [添加应用程序](#)

关于应用程序监控

通过应用程序监控，您可以监控 IM、电子邮件或 HTTP/S 客户端的第三方应用程序。默认情况下，Symantec Data Loss Prevention 只会监控主体应用程序，例如 AIM、Microsoft Outlook 或 Mozilla Firefox。第三方应用程序的示例包括 Skype、Mozilla Thunderbird 或 Google Chrome。必须先将 Symantec Data Loss Prevention 未专门监控的任何应用程序添加到“应用程序监控”页面，Symantec Data Loss Prevention 才能开始监控。例如，如果您的公司使用 Mozilla Thunderbird，则必须将 Mozilla Thunderbird 添加到“应用程序监控”页面。因为默认情况下不监控 Mozilla Thunderbird，所以需要添加该应用程序。添加 Mozilla Thunderbird 后，Symantec Data Loss Prevention 会监控该电子邮件客户端通过网络发送的文件附件。

此外，也可以配置对默认应用程序的全局更改。可以将黑名单或白名单数据与网络监控、CD/DVD 应用程序和使用打印/传真或剪贴板功能的应用程序关联起来。还可以指定是否希望 Symantec Data Loss Prevention 监控应用程序的网络、打印/传真、剪贴板或文件系统活动。例如，您可能希望排除 Microsoft Outlook 上的剪贴板活动。您可以在应用程序指纹加密页面上编辑 Microsoft Outlook 的设置以排除剪贴板活动。此页面上的应用程序仅是您希望修改其网络、打印/传真、剪贴板或文件系统监控的应用程序。

“应用程序监控”页面会显示当前监控的CD/DVD应用程序的列表。如果看不到所需的特定 CD/DVD 应用程序，必须将该应用程序添加至列表。

注意：可以删除所添加的任何应用程序，但是不能删除预先填入的应用程序。

另外，您还可以添加有关应用程序的发布者名称的详细信息。发布者名称详述了软件的制造商。通过添加发布者名称，Symantec Data Loss Prevention 可以验证应用程序，即使更改了应用程序的二进制名称，也可对其进行验证。发布者名称主要用于识别 Symantec 进程。但是，您可以为任意应用程序添加发布者名称。添加发布者名称是可选的。

请参见第 1208 页的“[添加应用程序](#)”。

注意：在第三方应用程序进行读取时，不会检测小于 64 字节的小文件。通常会检测大小超过 64 字节的文件。

添加应用程序

可以使用“添加应用程序监控”页面将第三方应用程序添加到监控策略。第三方应用程序可以包括下列应用程序类型：

- CD/DVD 应用程序（例如 Roxio）
- Internet 浏览器（例如 Google Chrome）
- IM 应用程序（例如 Skype）
- SMTP 应用程序（例如 Mozilla Thunderbird）

添加应用程序

1 在“应用程序信息”部分下，必须至少输入下列字段之一：

- 名称
- 二进制名称
- 内部名称
- 原始文件名
- 发布者名称

如果您输入了“发布者名称”，则可以选择“验证发布者名称”选项。使用此选项，可确保应用程序的发布者名称是正确的。使用“验证发布者名称”选项可能会影响性能，因为它增加了系统资源占用。

2 在“应用程序监控配置”部分下，选择下列一个或多个监控选项：

- 网络访问
- 打印机/传真
- 发送到剪贴板

■ 文件系统活动

3 如果已选择“文件系统活动”，则可以选择下列选项之一：

- 监控应用程序文件访问
- 监控 CD/DVD 写入

通过选择“应用程序文件访问”或 CD/DVD 选项，可以选择监控应用程序打开的文件或应用程序读取的文件。

请参见第 1207 页的[“关于应用程序监控”](#)。

使用 Endpoint Server 工具

本章节包括下列主题：

- [关于端点工具](#)

关于端点工具

Symantec Data Loss Prevention 提供了大量工具来帮助您使用 Symantec DLP Agent。这些工具包含在 VontuAgentInstaller.zip 文件中。请将这些工具安装到安全的目录下。这些端点工具会与密钥存储区文件（位于 Agent Install 目录下）搭配工作。这些工具必须与密钥存储区文件同在一个文件夹下才能正常工作。每个工具都需要密码才能操作。一般的工具密码会在安装期间生成。

您可以使用 endpointkeytool 更改密码，或是创建工具特定的密码。Symantec 建议您将工具安装到包括 Keystore 文件的 Symantec DLP Agent 安装目录下。但是，endpointkeytool 实用程序会安装在 Enforce 上，您可以在 Vontu\Enforce\Protect\bin 处找到它。

请参见第 1212 页的“[关于 endpointkeytool 实用程序](#)”。

以下列表包含一些可以使用端点工具完成的任务：

表 82-1 端点工具任务列表

任务	工具名称	链接
为代理创建唯一的 128 位密钥	endpointkeytool.exe	关于 endpointkeytool 实用程序
关闭代理和监视程序服务	Service_Shutdown.exe	关闭代理和监视程序服务
检测代理访问的数据库文件	vontu_sqlite3.exe	检测代理访问的数据库文件
查看扩展日志文件	logdump.exe	查看扩展日志文件

任务	工具名称	链接
生成代理的卸载密码	UninstallPwdKeyGenerator.exe	请参见第1218页的“ 使用密码生成工具创建密码 ”。

您还可以使用 Symantec Management Console 执行其中一些任务。

请参见第 1176 页的“[关于 Symantec Management Console 代理任务](#)”。

在 Windows 7 或 Vista 上使用端点工具

如果要在运行 Windows 7 或 Vista 的计算机上使用端点工具，您必须以“提升权限的命令提示符”模式运行命令提示符。鉴于 Windows 7 和 Vista 操作系统的性质，此过程为必需。您不能在未使用“提升权限的命令提示符”模式的情况下运行端点工具。

在 Windows 7 中启动提升权限的命令提示符模式

- 1 在 Windows 的“开始”菜单中，单击“搜索程序和文件”字段。输入 command。
- 2 按住 **Shift** 键的同时右键单击命令提示符窗口。
- 3 选择“以管理员身份运行”选项。

在 Windows Vista 中启动提升权限的命令提示符模式

- 1 在 Windows 的“开始”菜单中，右键单击“命令提示符”图标。
- 2 选择“以管理员身份运行”。

将以“提升权限的命令提示符”模式启动命令提示符。您现在即可使用端点工具。

请参见第 1211 页的“[关于端点工具](#)”。

关于 endpointkeytool 实用程序

使用 endpointkeytool 命令行实用程序可生成身份验证密钥，还可以定义工具密码。Symantec Data Loss Prevention 使用默认密钥。您必须生成自己唯一的密钥，以确保不会与另一位客户使用相同的密钥。请备份并安全保存 endpointkeytool 所生成的文件。在开始之前，请确保已安装 Endpoint Server，但未安装任何 Symantec DLP Agent。

注意：在美国以外地区，部分密钥大小不能识别时，请检查您的操作系统授权许可限制。

请参见第 1211 页的“[关于端点工具](#)”。

请参见第 1213 页的“[运行 endpointkeytool 实用程序](#)”。

请参见第 1181 页的“[关于 Symantec DLP Agent 安全](#)”。

运行 endpointkeytool 实用程序

必须以 Symantec Data Loss Prevention 操作系统用户帐户运行 endpointkeytool 实用程序。默认情况下，此帐户为 protect。endpointkeytool 实用程序的命令选项为：

选项	说明
<code>-keysize=<128/192/256></code>	指定已生成的密钥文件的位大小。
<code>-pwd=tools_password</code>	指定用于访问端点工具的密码。该密码默认为 <i>VontuStop</i> 。您必须指定一个密码。
<code>[-dir=directory]</code>	可选的 <code>-dir</code> 参数指定放置 <code>keystore</code> 文件的目录。

除非您使用 `-dir` 参数指定不同的目录，否则，`keystore` 文件 `*.endpointRecoveryStore` 会在 `endpointkeytool` 实用程序所在的 `\bin` 目录中创建。默认情况下，该 `\bin` 目录为 `...Enforce\Protect\bin`。此密钥存储区文件只有在移至 `keystore` 目录后才能发挥作用。

注意：如果 `keystore` 目录中有多个 `keystore` 文件，则不会启动 Endpoint Server。

生成 endpointkeytool 文件

- 1 以 Symantec Data Loss Prevention 用户帐户，使用所需参数运行 `endpointkeytool` 实用程序，例如：

```
endpointkeytool generate -keysize=128 -pwd=VontuStop
```

- 2 使用 `-pwd=tools_password` 和 `-keysize=128/192/256` 参数，输入工具密码。在命令中，`tools_password` 是您要使用的密码，`128/192/256` 是您要使用的密钥大小。
- 3 除非您已使用 `-dir` 选项来指定生成密钥存储区文件的位置，否则请将密钥存储区文件置于安全且易于记忆的目录中。验证密钥存储区目录是否仅包括一个密钥存储区文件。

- 4 将密钥存储区文件的副本保存在安全的位置。如果 Symantec DLP Agent 上的 keystore 文件发生任何意外，可使用 keystore 文件的副本来替换损坏的文件。

Endpoint Server 必须使用在相同 endpointkeytool 会话中生成的密钥。使用其他密钥的任何 Symantec DLP Agent 均不能进行身份验证，且不能与服务器进行通信。如果密钥存储区文件发生问题，则会生成身份验证失败端点系统事件。Symantec DLP Agent 状态显示在管理控制台的“代理概述”屏幕中。

- 5 将身份验证密钥复制到用于安装 Symantec DLP Agent 的 MSI 安装脚本的 KEY 参数。该过程可确保安装脚本使用相同的身份验证密钥安装所有 Symantec DLP Agent。如果 KEY 参数保留为空白，则 Symantec DLP Agent 会使用默认密钥。

Endpoint Server 的 keystore 目录位于 Vontu/Protect/keystore。空的密钥存储区目录表示 Symantec Data Loss Prevention 使用默认的嵌入式密钥存储区文件。将生成的密钥存储区文件复制到密钥存储区目录后，会覆盖默认的密钥存储区文件。

如果您忘记工具密码，则可以使用 endpointkeytool 恢复选项进行恢复：

```
endpointkeytool recover [-dir=output_dir]
```

- 6 通过 Enforce 控制台重新启动 Endpoint Server。

请参见第 1211 页的“[关于端点工具](#)”。

请参见第 1181 页的“[关于 Symantec DLP Agent 安全](#)”。

请参见第 1212 页的“[关于 endpointkeytool 实用程序](#)”。

请参见第 1182 页的“[关于身份验证密钥](#)”。

关闭代理和监视程序服务

Service_Shutdown.exe 工具会关闭 Symantec DLP Agent 和监视程序服务。为了防止篡改，用户不能个别停止 Symantec DLP Agent 或监视程序服务。此工具可让管理员同时停止两种 Symantec Data Loss Prevention 服务。

运行 Service_Shutdown.exe 工具

- ◆ 从安装目录运行以下命令：

```
service_shutdown [-p=password]
```

其中，安装目录是安装 Symantec Data Loss Prevention 的目录，而 [-p=password] 是您先前指定的密码。如果您未输入密码，系统会提示您输入密码。默认密码为 VontuStop。

您必须从与 Symantec DLP Agent Keystore 文件所在的同一目录运行 Service_Shutdown.exe 工具。

请参见第 1211 页的“[关于端点工具](#)”。

检测代理访问的数据库文件

利用 vontu_sqlite3.exe 工具，可以检查 Symantec DLP Agent 使用的数据库文件。它提供 SQL 接口来查询和更新数据库文件。如果无此工具，您将不能查看数据库文件的内容（因为它已加密）。要调查或更改 Symantec Data Loss Prevention 文件时，请使用此工具。

运行 vontu_sqlite3.exe 工具

- 1 从 Symantec DLP Agent 安装目录，运行以下命令：

```
vontu_sqlite3 -db=database_file [-p=password]
```

其中，*database_file* 是数据库文件，而 *password* 是指定的工具密码。

所有 Symantec Data Loss Prevention 数据库文件均位于 Symantec DLP Agent 安装目录中，且结尾为扩展名 *.ead。运行该命令后，系统会提示您输入密码。

- 2 除非您已创建唯一密码，否则请输入默认密码 Vontustop。

会提供 Shell，您可以输入 SQL 语句来查看或更新数据库。

有关此 Shell 中所提供命令的完整文档，请参考
<http://www.sqlite.org/sqlite.html>。

请参见第 1211 页的“[关于端点工具](#)”。

查看扩展日志文件

利用 logdump.exe 工具，可以查看 Symantec DLP Agent 的扩展日志文件。基于安全原因，会隐藏扩展日志文件。一般情况下，您只需与 Symantec Data Loss Prevention 支持人员一同查看日志文件。如果不使用此工具，将无法查看任意 Symantec DLP Agent 日志文件。

运行日志转储工具

- ◆ 从 Symantec DLP Agent 安装目录，运行以下命令：

```
logdump -log=log_file [-p=password]
```

其中，*log_file* 是您要查看的日志文件，而 *password* 是指定的工具密码。所有 Symantec Data Loss Prevention 扩展日志文件均位于 Symantec DLP Agent 安装目录。文件名称格式为 edpa_ext 文件编号.log。运行该命令后，您可以看到 de-obfuscated 日志。

注意：使用 Windows Powershell 运行 logdump.exe 时，需要在日志文件两侧加引号。例如，应运行：

```
logdump "-log=log_file" [-p=password]
```

通过此视图，您可以打印其他日志的内容。

打印其他日志的内容

- 1 请从命令窗口运行：

```
logdump -log=log_file -p=password > deobfuscated_log_file_name
```

- 2 再次输入密码，以打印日志。

请参见第 1211 页的“[关于端点工具](#)”。

关于设备 ID 实用程序

Symantec Data Loss Prevention 提供 DeviceID.exe 实用程序来协助您配置检测用的端点设备。

请参见第 470 页的“[关于端点设备检测](#)”。

DeviceID 实用程序可扫描计算机以查找所有连接的设备，并为各个可检测设备报告设备实例 ID 字符串。

请参见第 1217 页的“[使用设备 ID 实用程序](#)”。

表 82-2 设备 ID 实用程序示例输出

结果	说明
卷	DeviceID.exe 工具发现的卷或装入点。 例如： 卷： E:\

结果	说明
设备 ID	各设备的设备实例 ID。 例如： USBSTOR\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\5F73HF00Y9DBOG0DXJ
正则表达式	用于检测该设备实例的正则表达式。 例如： USBSTOR\\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\\5F73HF00Y9DBOG0DXJ

使用设备 ID 实用程序

使用设备 ID 实用程序提取设备实例 ID 字符串并确定系统可识别哪些要检测的设备。

请参见第 1216 页的“[关于设备 ID 实用程序](#)”。

请参见第 470 页的“[关于端点设备检测](#)”。

使用设备 ID 实用程序

1 获取 DeviceID.exe 实用程序。

此实用程序与 Endpoint Sever 实用程序软件包一起提供。

请参见第 1211 页的“[关于端点工具](#)”。

2 将 DeviceID.exe 实用程序复制到要在其中确定设备 ID 的计算机。

3 将要检查的设备安装到已复制了 DeviceID.exe 实用程序的计算机。

例如，插入一个或多个 USB 设备、连接硬盘驱动器等等。

4 从命令行运行 DeviceID.exe 实用程序。

例如，如果已将 DeviceID.exe 实用程序复制到 C:\temp 目录，则请输入以下命令：

C:\temp>DeviceID

要将结果输出到文件，请输入以下命令：

C:\TEMP>DeviceID > deviceids.txt

此文件显示在 C:\temp 目录中且包含 DeviceID 进程的输出。

5 查看 DeviceID 进程的结果。

命令提示符显示各个卷或装入点的结果。

请参见第 1216 页的[表 82-2](#)。

6 使用 DeviceID 实用程序针对当前连接的设备评估建议的正则表达式字符串。

请参见第 1218 页的[表 82-3](#)。

7 使用正则表达式模式配置检测用的端点设备。

请参见第 474 页的[“创建及修改端点设备配置”](#)。

表 82-3 设备 ID 正则表达式评估

命令参数	示例
DeviceID.exe [-m] [Volume] [Regex]	DeviceID.exe -m E:\ "USBSTOR\\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\\.*" 注意： 正则表达式字符串需要括在引号内。
返回	“匹配!” 或 “不匹配!”

使用密码生成工具创建密码

使用卸载密码生成器工具可创建唯一的密码密钥。

卸载密码生成器工具的名称是 UninstallPwdKeyGenerator.exe。

卸载密码可防止未经授权的用户删除 Symantec DLP Agent。

UninstallPwdKeyGenerator.exe 工具使用 PGPSdk.dll 文件创建唯一的密码。该工具和该文件必须位于同一管理员的工具目录下才能起作用。默认情况下，UninstallPwdKeyGenerator.exe 工具和 PGPSdk.dll 文件应位于管理员工具目录下。

注意：UninstallPwdKeyGenerator.exe 仅可在 Microsoft Windows 环境下运行。
不能在其他任何操作系统中使用该工具。

创建卸载密码

1 在命令窗口中，导航至 Symantec Data Loss Prevention keystore 目录。

2 输入下列命令：

`-xp=<uninstall password>`

其中 `<uninstall password>` 是要使用的密码。选择唯一的密码密钥。

将生成密码密钥。安装代理时，在命令行中输入该密钥。

请参见第 1185 页的[“向代理添加卸载密码”](#)。

10

部分

监视和防止移动设备上的数 据丢失

- 83. Symantec Data Loss Prevention for Mobile 简介
- 84. 实施 Mobile Prevent (Web)

1220 |

Symantec Data Loss Prevention for Mobile 简介

本章节包括下列主题：

- [Symantec Data Loss Prevention for Mobile 的工作方式](#)
- [Mobile Prevent 的部署选项](#)
- [关于将 Mobile Prevent 部署为单机解决方案](#)
- [关于 Mobile Prevent 的数字证书](#)
- [关于 VPN 服务器和按需 VPN](#)
- [关于 Microsoft Exchange ActiveSync](#)
- [关于移动设备管理](#)

Symantec Data Loss Prevention for Mobile 的工作方式

Symantec Data Loss Prevention for Mobile 通过 Wi-Fi 接入或通过 3G 蜂窝连接与企业网络相连接。Webmail、第三方应用程序（如 Yahoo 和 Facebook）以及包括 Microsoft Exchange ActiveSync 在内的企业电子邮件应用程序的网络流量都通过 HTTP/S 协议进行发送。通过 Microsoft ActiveSync 以 HTTP 或 HTTPS 协议信息的形式可以发送企业电子邮件。Microsoft ActiveSync 在企业代理服务器经过检测后从该服务器接收信息，然后将邮件发送到企业 Exchange Server。根据您的策略，可以阻止通过应用程序（如 Facebook 或 Dropbox）发送的邮件。

请参见第 1223 页的“[关于将 Mobile Prevent 部署为单机解决方案](#)”。

若要发送企业邮件或访问企业网络，移动设备必须通过虚拟专用网络 (VPN) 连接到企业网络。Mobile Prevent 解决方案要求移动设备使用“按需 VPN”功能创建持续

且受保护的 VPN 连接。如果不连接到企业网络，Mobile Prevent 就无法检测任何违规策略。

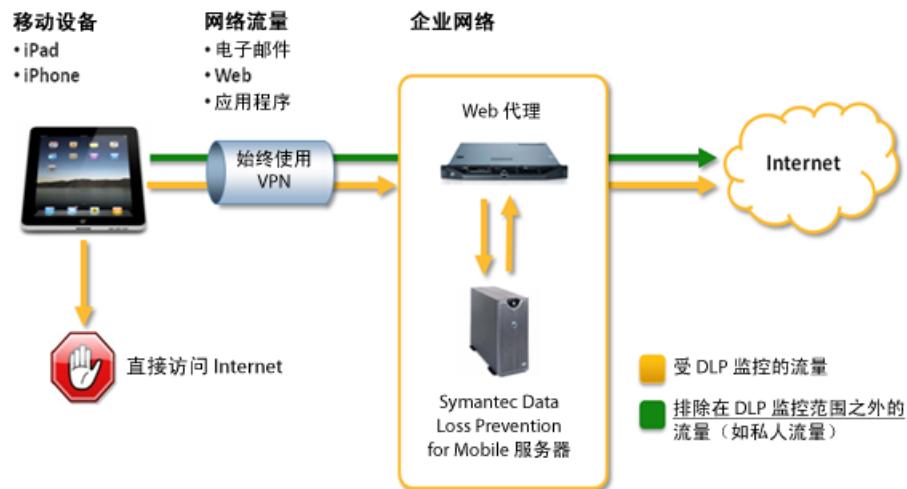
请参见第 1228 页的“[关于 VPN 服务器和按需 VPN](#)”。

VPN 配置可通过移动设备管理 (MDM) 解决方案在配置文件中指定。MDM 解决方案会对要连接到企业网络的每个移动设备应用一个配置文件。

请参见第 1230 页的“[关于移动设备管理](#)”。

请参阅《Symantec Data Loss Prevention 系统要求和兼容性指南》，以取得 Mobile Prevent 的要求详细信息。

下图显示了启用 Symantec Data Loss Prevention for Mobile 所必需的连接：



请参见第 1231 页的“[实施 Mobile Prevent](#)”。

Mobile Prevent 的部署选项

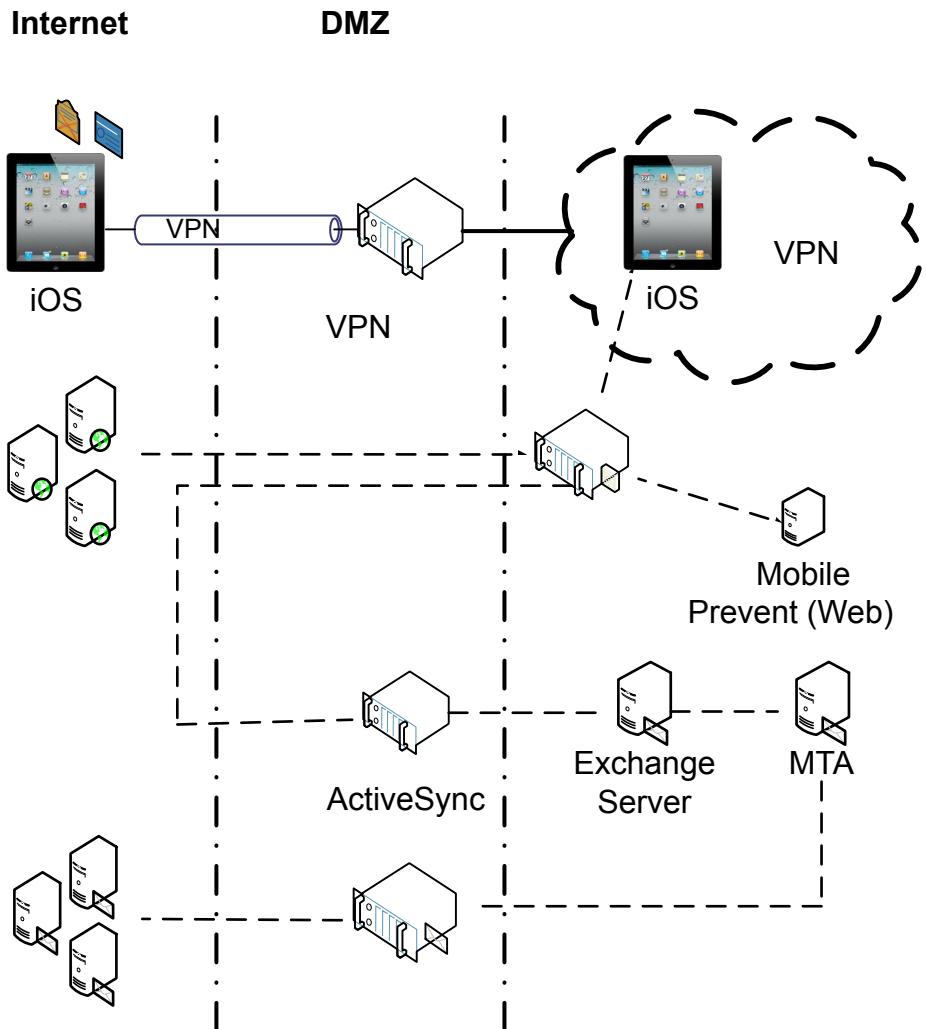
可以将 Mobile Prevent 作为一个独立产品进行部署，也可以将其与 Network Prevent for Web 一起部署。您必须为要部署的每个产品购买单独的许可证。

Symantec Data Loss Prevention 的用户界面因您购买的许可证而异。屏幕上显示的内容可能与本产品文档中的描述略有差异。

请参见第 1223 页的“[关于将 Mobile Prevent 部署为单机解决方案](#)”。

关于将 Mobile Prevent 部署为单机解决方案

当您将 Mobile Prevent 部署为单机解决方案时，没有其他检测服务器会与 Mobile Prevent for Web Server 一起部署。此 Mobile Prevent for Web Server 通过与 Enforce Server 和企业代理服务器进行交互来监控移动设备上的事件并防止出现这些事件。下图描绘了 Mobile Prevent 解决方案在企业基础架构中所处的位置：



在这种部署中，移动设备通过 VPN 服务器连接到企业网络。VPN 服务器则为每台移动设备分配一个 IP 地址。设备可通过此地址来访问内部企业网络。为设备分配了唯一 IP 地址后，所有 HTTP、HTTPS 和 FTP 通信均受 Mobile Prevent for Web Server 监控。每个设备都必须通过 VPN 连接到企业网络。如果与企业网络的 VPN 连接断开，Mobile Prevent 便无法检测任何违规情况。

iPad 和 iPhone 使用称为按需 VPN 这一功能来自动建立安全的 VPN 连接，而无需用户干预。按需 VPN 要求采用基于证书的身份验证来与 VPN 服务器建立连接。

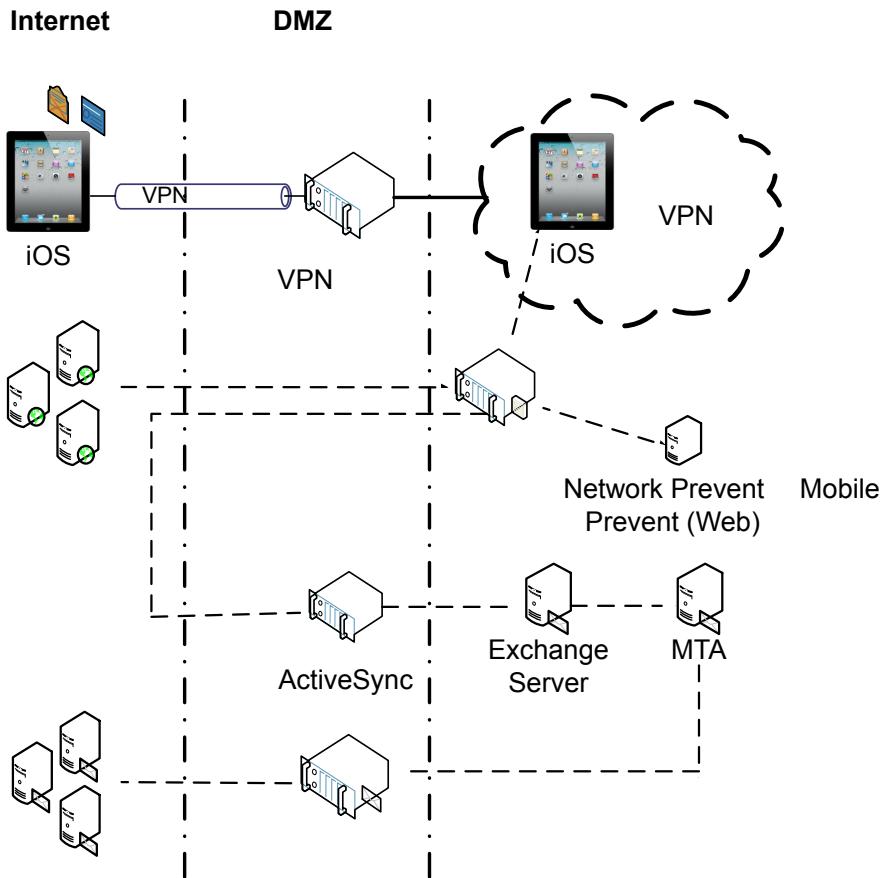
VPN 连接建立后，通信通过代理服务器进行发送并由 Mobile Prevent for Web Server 加以分析。代理服务器与 Mobile Prevent for Web Server 之间的通信通过 ICAP 协议进行传送。如果未发现违规，则会在内部或外部将通信发送至其目标。如果发现违规，则会创建一个事件并采取响应操作。事件将记录在 Enforce Server 上。

当移动设备通过 Microsoft Exchange ActiveSync 发送电子邮件时，会将 HTTP/HTTPS 数据包发送到 ActiveSync 服务器。然后，会将数据包发送至 Exchange Server。所有企业电子邮件都应经由 Microsoft Exchange ActiveSync。Mobile Prevent 不支持 SMTP 协议。

注意：Mobile Prevent 不支持响应模式 (RESPMOD)。

关于将 Mobile Prevent 与 Network Prevent 一起部署

您也可以将 Mobile Prevent 与 Network Prevent for Web 一起部署。下图描绘了这两个产品在企业基础架构中所处的位置。



请参见第 1223 页的“[Mobile Prevent 的部署选项](#)”。

在此场景中，Mobile Prevent for Web Server 和 Network Prevent Server 部署为单个检测服务器。合并后的检测服务器称为 Network and Mobile Prevent for Web Server。

在此组合部署中，移动设备仍通过 VPN 服务器连接到企业网络。VPN 服务器则为每台移动设备分配一个IP地址。在此组合部署中，必须指定VPN服务器用于Mobile Prevent子网的IP地址范围。通过使用某个特定范围的IP地址，Symantec Data Loss Prevention可以识别Mobile Prevent;事件。为设备分配了唯一的IP地址后，所有HTTP、HTTPS、Microsoft Exchange ActiveSync电子邮件和FTP流量均受到Network and Mobile Prevent for Web Server监控。每个设备都必须通过VPN连接到企业网络。如果与企业网络的VPN连接断开，Mobile Prevent便无法检测任何违规情况。

VPN 连接建立后，流量通过代理服务器进行发送并由 Network and Mobile Prevent for Web Server 加以分析。如果未发现违规，则会将流量发送至其目标。如果在通过移动设备时生成了事件，则事件会标记为“移动”事件，并显示在“移动”事件页中。如果在数据流经企业网络时生成了事件，则事件会标记为 Network Prevent for Web 事件。

注意：同时部署 Mobile Prevent 和 Network Prevent for Web 可能会对 Network Prevent for Web Server 的性能产生不利影响。如果移动设备流量来自低速 3G 网络，并且延迟高于 Network Prevent for Web 流量，则可能会影响性能。

关于 Mobile Prevent 的数字证书

Mobile Prevent 需要数字证书才能确保用户的有效性、对 VPN 服务器启用基于证书的身份验证以及允许代理服务器进行 SSL 截取。

请参见第 78 页的“[关于对用户进行身份验证](#)”。

您可以使用 MDM 解决方案将这些证书部署到多个移动设备，使其成为移动设备配置文件的组成部分。

请参见第 1230 页的“[关于移动设备管理](#)”。

请参见第 1235 页的“[配置 VPN 配置文件](#)”。

下表对您必须为 Mobile Prevent 创建的四个证书进行了说明：

表 83-1 Mobile Prevent 的数字证书

证书	安装位置	说明
证书颁发机构 (CA) 的根证书	移动设备、VPN 服务器、代理服务器	基本 CA。所有其他证书均由此根 CA 或其从属 CA 签名。如果设备信任此根 CA，则该设备还信任由此根 CA 或其从属 CA 签名的所有有效证书。
用户证书	移动设备	标识单个用户。用户必须具有此证书才能访问企业子网。此证书将发送至 VPN 服务器进行身份验证。此证书是建立到企业网络的 VPN 隧道所必需的。
从属证书颁发机构	代理服务器	从属 CA 证书向代理服务器授予为 HTTPS 服务器颁发服务器身份证件的权限。此证书是进行 SSL 截取所必需的。在移动设备连接到企业子网后，代理服务器会截取流量，随后担当 HTTPS 服务器与移动设备之间的中间人。 代理服务器充当从属 CA，它验证来自 HTTPS 服务器的证书，并为 HTTPS 服务器颁发新证书。

证书	安装位置	说明
设备证书	VPN 服务器	先确定 VPN 服务器主机名的身份有效，然后移动设备才能连接到它。此证书可确保移动设备不会连接到未经授权的 VPN 服务器。

关于 VPN 服务器和按需 VPN

您的移动设备通过连接到 VPN 服务器来获得对企业网络的访问。

VPN 服务器为连接到它的每个移动设备分配一个 IP 地址。这些 IP 地址构成了一个 VPN 子网。通过此 VPN 子网，您的移动设备得以访问企业网络和企业代理服务器。您可以指定 VPN 服务器可分配给其他设备的 IP 地址范围。VPN 服务器分配给移动设备的所有 IP 地址都在这个范围内。如果未指定地址范围给 VPN 服务器，网络可以任意分配 IP 地址给移动设备。通过特定的 IP 地址范围，Symantec Data Loss Prevention 可以识别为移动设备分配了哪些 IP 地址以及哪些地址未连接。使用 IP 地址范围有助于识别事件是由哪个移动设备生成的。

如果同时部署 Mobile Prevent 和 Network Prevent for Web，IP 地址可标识网络和移动事件类型。

在 Mobile Prevent 端，按需 VPN 可确保 VPN 连接不会中断。Apple 移动设备使用“按需 VPN”动态创建 VPN 会话。当连接至已配置域（例如.com、.net 或 .org）的特定列表时，“按需 VPN”便会启动 VPN 会话。要配置按需 VPN 功能，需采用基于证书的身份验证。通过配置按需 VPN 在 iOS 移动设备上自动启用 VPN 的方式，可以确保所有通信均经由您的企业网络。您需要以透明模式部署 Web 代理，用于在企业网络中，将来自移动设备的流量路由到 Symantec Data Loss Prevention。路由的网络流量会使用 ICAP 服务。

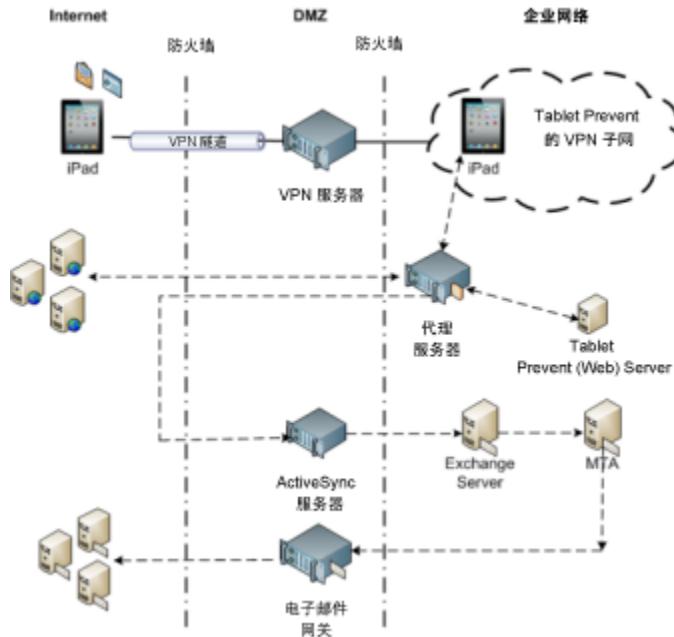
可使用移动设备管理 (MDM) 解决方案应用网络和 VPN 配置。

关于 Microsoft Exchange ActiveSync

借助 Microsoft Exchange ActiveSync，您可以从移动设备发送企业电子邮件。ActiveSync 可以向企业网络内部或外部的收件人发送电子邮件。ActiveSync 通过 HTTP 或 HTTPS 协议发送企业电子邮件。所有在内部或外部传输且违反策略的敏感信息都会被阻止。

下例说明了企业邮件是如何通过 ActiveSync 发送的：

注意：下图也适用于 iPhone。



在本示例中，邮件从配置有 ActiveSync 的 iPad 电子邮件客户端发出，经由与 VPN 相连的企业网络。该邮件以 HTTP/S 请求的形式发送。ActiveSync 服务器收到该邮件后，接着将其发送到 Microsoft Exchange Server。Exchange Server 以 SMTP 邮件的形式将该邮件发送至 MTA 服务器。MTA 服务器将这封企业邮件发送至收件人。

您可以通过过滤的方式禁用 ActiveSync 监控。

请参见第 1229 页的“[忽略 Microsoft Exchange ActiveSync 监控](#)”。

忽略 Microsoft Exchange ActiveSync 监控

如果您不希望监控经由 ActiveSync 的企业电子邮件，请按以下过程操作：

忽略 Microsoft Exchange ActiveSync 监控

- 1 在 Enforce Server 管理控制台上，转至 Mobile Prevent for Web Server 的“服务器设置”。
- 2 在“请求过滤”部分下，将 ActiveSync 服务器的主机名添加到“忽略向主机或域的请求”字段中。
- 3 单击“保存”。

请参见第 1228 页的“[关于 Microsoft Exchange ActiveSync](#)”。

关于移动设备管理

使用移动设备管理 (MDM) 解决方案可管理多个移动设备，并可向其应用各种配置设置。您可以将预配置了企业邮件设置、VPN 设置、安全证书和代理服务器设置的用户配置文件加载到移动设备上。若要访问 Mobile Prevent for Web Server，必须使用 MDM 解决方案应用 VPN 服务器配置文件。VPN 服务器配置文件用于为按需 VPN 设置条件，使所有网络流量都通过 VPN 路由并路由到您的企业网络中。只能监控流入企业网络中的网络流量是否存在违规行为。

请参见第 1235 页的“[配置 VPN 配置文件](#)”。

实施 Mobile Prevent (Web)

本章节包括下列主题：

- [实施 Mobile Prevent](#)

实施 Mobile Prevent

Mobile Prevent for Web Server 可使用 ICAP 与 VPN 服务器、MDM 解决方案和 Web 代理服务器集成。如果它在 Web 内容中检测到机密数据，代理便会根据 Mobile Prevent 策略中的规定拒绝请求或删除 HTML 内容。

首先，您需要了解实施 Mobile Prevent 所需的高级步骤。有关更多详细信息，请查看交叉引用章节。Mobile Prevent 有两种部署方案：它即可作为独立产品部署，也可与 Network Prevent 一起安装。下面的过程假定您将 Mobile Prevent 作为独立产品实施。如果您要将 Mobile Prevent 与 Network Prevent 一起实施，还必须遵循 Network Prevent 的实施说明。

请参见第 1223 页的“[关于将 Mobile Prevent 部署为单机解决方案](#)”。

请参见第 905 页的“[实施 Network Prevent for Web](#)”。

注意：下列过程假定您的环境中已有 VPN 和代理服务器在运行。

表 84-1 实施 Mobile Prevent

步骤	过程	有关更多信息
步骤 1	添加新 Mobile Prevent Server。	请参见第 187 页的“ 添加检测服务器 ”。
步骤 2	配置 Mobile Prevent Server。	请参见第 1232 页的“ 配置 Mobile Prevent for Web Server ”。

步骤	过程	有关更多信息
步骤 3	使用 Mobile Prevent 子网中您要分配给企业移动设备的 IP 地址范围配置 VPN 服务器。	参见 VPN 服务器的文档。
步骤 4	配置 MDM 应用程序的 VPN 配置文件。	请参见第 1235 页的“ 配置 VPN 配置文件 ”。
步骤 5	定义代理上用于将流量路由到 Mobile Prevent Web Server 的 ICAP 服务。	请参见第 910 页的“ 关于代理服务器配置 ”。
步骤 6	创建和部署 Mobile Prevent 的策略。	请参见第 1239 页的“ 创建 Mobile Prevent 的策略 ”。
步骤 7	针对测试策略生成事件，以测试系统。	请参见第 1241 页的“ 测试 Mobile Prevent ”。
步骤 8	如有需要，请对实施问题进行故障排除。	请参见第 916 页的“ Network Prevent for Web Server 的故障排除信息 ”。

有关如何在您的组织中配置 Mobile Prevent 以使其正常工作的详细信息，请参见《Symantec Data Loss Prevention 系统要求和兼容性指南》。

配置 Mobile Prevent for Web Server

您可以使用 Mobile Prevent for Web Server 的多个配置选项。例如，您可以将服务器配置为：

- 忽略小型 HTTP/S 请求或响应。
- 忽略特定主机或域（例如企业子公司的域）的请求或响应。
- 忽略用户搜索引擎查询。

请参见第 187 页的“[添加检测服务器](#)”。

修改 Mobile Prevent for Web Server 配置

- 1 转至“系统”>“服务器”>“概述”，然后单击 Mobile Prevent for Web Server。
- 2 在显示的“服务器详细信息”屏幕上，单击“配置”。

如后续步骤中所述，您可以验证或修改 **ICAP** 选项卡上的设置。该选项卡分为如下几个部分：“请求过滤”、“响应过滤”和“连接”。

- 3 验证或修改“试用模式”设置。

- 4 针对来自 HTTP 客户端（用户代理）的请求验证或修改过滤器选项。“请求过滤”部分的选项如下：

忽略小于以下大小的请求

指定要检查的HTTP请求的最小正文大小。
(默认为 4096 个字节。) 例如，在搜索引擎（如 Yahoo 或 Google）中键入的搜索字符串通常很短。通过调整该值，您可以将这些搜索排除在检查范围之外。

忽略没有附件的请求

让服务器只检查包含附件的请求。如果您主要涉及一些计划发布敏感文件的请求，该选项非常有用。

忽略主机或域的请求

让服务器忽略您指定的主机或域的请求。如果预期公司总部和分公司之间有大量 HTTP 流量，则该选项非常有用。您可以键入一个或多个主机或域名（例如 www.company.com），每个域名各占一行。

忽略来自用户代理的请求

让服务器忽略来自您指定的用户代理 (HTTP 客户端) 的请求。如果组织使用频繁发送 HTTP 请求的程序或语言（如 Java），则该选项非常有用。您可以键入一个或多个用户代理值（例如java/6.0.29），每个值各占一行。

5

注意: Mobile Prevent 不支持“响应过滤”选项。

针对来自 Web 服务器的响应验证或修改过滤器选项。“**响应过滤**”部分的选项如下:

忽略小于以下大小的响应 指定该服务器所检查的 HTTP 响应的最小正文大小。(默认为 4096 字节。)

检查内容类型 指定响应中 Symantec Data Loss Prevention 应监视的 MIME 内容类型。默认情况下，该字段包含 Microsoft Office、PDF 以及纯文本格式的内容类型值。要添加其他值，请每行键入一个 MIME 内容类型。例如，键入
application/wordperfect5.1 让 Symantec Data Loss Prevention 分析 WordPerfect 5.1 文件。

注意，在 Web 代理层指定 MIME 内容类型通常更加高效。

忽略来自主机或域的响应 让服务器忽略来自您指定的主机或域的响应。您可以键入一个或多个主机或域名(例如 www.company.com)，每个域名各占一行。

忽略对用户代理的响应 让服务器忽略对您指定的用户代理(HTTP 客户端)的响应。您可以键入一个或多个用户代理值(例如 java/1.4.2_xx)，每个值各占一行。

- 6 验证或修改 HTTP 代理服务器和 Mobile Prevent for Web Server 之间 ICAP 连接的设置。“连接”选项如下：

TCP 端口	指定该服务器用来侦听 ICAP 请求的 TCP 端口号。该端口号必须与在将 ICAP 请求发送至该服务器的 HTTP 代理上配置的值一样。建议值为 1344。
最大请求数	指定来自 HTTP 代理的最大并行 ICAP 请求连接数。默认值为 25。
最大响应数	指定来自 HTTP 代理的最大并行 ICAP 请求响应数。默认值为 25。
连接积压	指定允许的等待连接数。等待连接即等待来自浏览器的 HTTP 响应的用户。最小值为 1。如果 HTTP 代理收到太多请求（或响应），则代理会根据代理配置来处理这些请求或响应。您可以将 HTTP 代理配置为阻止大于该值的任何请求（或响应）。

- 7 在“移动 IP 范围”字段中，输入为 VPN 服务器配置的、用于分配给移动设备的 IP 地址范围。IP 地址可用来标识移动设备上触发为移动事件的事件。
您在此范围中输入的 IP 地址不会动态影响 VPN 服务器。此范围仅用于在管理控制台标识您的移动设备。在您配置 VPN 服务器以分配地址时，您必须输入完全相同的 IP 地址范围。
- 8 单击“保存”退出“配置服务器”屏幕，然后单击“完成”退出“服务器详细信息”屏幕。

配置 VPN 配置文件

您必须先配置 VPN 配置文件，然后移动设备才能连接到企业网络。VPN 配置文件集安全证书、VPN 服务器配置设置、按需 VPN 设置以及所有网络配置设置于一身。通常，VPN 配置文件通过 MDM 解决方案加以设置和应用。除 VPN 配置文件之外，还可配置移动设备的其他方面，如 Microsoft Exchange ActiveSync、防火墙属性或 LDAP 设置。

请参见第 1230 页的“[关于移动设备管理](#)”。

下表说明了为启用 Mobile Prevent 而必须采用的最基本的 VPN 配置文件设置。具体设置的名称可能会因您所用的 MDM 解决方案而异。

表 84-2 基本的 VPN 配置文件设置

设置的类型	设置	说明
VPN配置设置		
	连接名称	连接类型的名称。通常，这是一个具有唯一性的名字，以便您以后能够识别它。
	连接类型	为您的 VPN 服务器选择连接类型。 例如，IPSec (Cisco)。
	服务器名称	输入您的 VPN 服务器的主机名或 IP 地址。
	用户名	连接到 VPN 服务器的移动设备的用户名。 例如，指定了该用户的名字和姓氏的 <名字_姓氏>。
	计算机身份验证	选择证书选项。若要启用 Mobile Prevent，您必须使用您所属公司以及证书颁发机构的证书。
	身份证书	选择您要添加的用户的证书。
	启用按需 VPN	您必须启用按需 VPN。 启用按需 VPN 后，您便可以添加您所需的特定域后缀。所有域后缀都应使用按需操作“始终建立”加以启用。 例如，将域后缀 .com、.net、.org 和 .gov 添加为“始终建立”的后缀。只要调用包含上述某一后缀的域名，就必须先建立 VPN 隧道，然后连接才能完成。
凭据设置		
	我的公司	您所属公司的证书。这是证书颁发机构 (CA) 的根证书。
	我们的公司	这是代理服务器的证书。
	用户凭据	这是用于访问代理服务器的个人用户凭证。
WI-FI 设置		如果您要强制指定特定的 Wi-Fi 网络以便您的移动设备在其中仅使用特定的网络，请使用 Wi-Fi 设置。如果您指定具有唯一性的 Wi-Fi 设置，那么您的移动设备将无法连接到任何其他 Wi-Fi 网络。

关于代理服务器配置

要将 Web 请求转发给 Mobile Prevent，您必须至少配置一个 HTTP/S 代理服务器。HTTP 代理充当 Mobile Prevent Server 的 ICAP 客户端。Mobile Prevent 仅支持

ICAP 的请求修改 (REQMOD) 模式。请勿将 HTTP 代理配置为响应修改 (RESPMOD) 模式。

注意：代理服务器必须以透明模式部署。有关详细信息，请参考代理服务器的文档。

请参见第 913 页的“[指定一个或多个代理服务器](#)”。

请参见第 1237 页的“[代理服务器与 Mobile Prevent 间的兼容性](#)”。

请参见第 1237 页的“[配置请求模式服务](#)”。

代理服务器与 Mobile Prevent 间的兼容性

Mobile Prevent for Web Server 可以与以下 Web 代理一起操作：

表 84-3 Mobile Prevent 所支持的代理服务器

代理	支持的协议	配置信息
Blue Coat ProxySG	HTTP、HTTPS、FTP over HTTP 或 FTP 代理	Blue Coat 产品文档

请参见第 913 页的“[指定一个或多个代理服务器](#)”。

请参见第 910 页的“[关于代理服务器配置](#)”。

配置请求模式服务

有关配置代理服务器的详细信息，请参考代理服务器产品文档，或联系代理服务器管理员。

配置代理服务器：

- ◆ REQMOD。在代理服务器上，创建 ICAP REQMOD 服务，该服务将请求转发到 Mobile Prevent。如果代理服务器支持的协议不同，请将其配置为处理所需的协议。

对于 REQMOD 模式，代理服务器上的 ICAP 服务应类似如下所示：

```
icap://ip_address|FQDN[:port]/reqmod
```

其中：

- *ip_address|FQDN* 使用 IP 地址或完全限定的域名标识 Mobile Prevent for Web Server。
- *Port* 是 Mobile Prevent for Web Server 倾听的端口号。使用默认的 ICAP 端口 (1344) 时，指定端口号为可选步骤。

- 要在 REQMOD 模式中正确工作，必须使用 /reqmod。

示例：

```
icap://10.66.194.45/reqmod  
icap://10.66.194.45:1344/reqmod  
icap://netmonitor1.company.com/reqmod
```

注意：代理上的 ICAP 服务定义中指定的端口，必须与 Mobile Prevent for Web Server 倾听的端口相匹配。

请参见第 910 页的“[代理服务器与 Network Prevent for Web 的兼容性](#)”。

请参见第 910 页的“[关于代理服务器配置](#)”。

指定一个或多个代理服务器

默认情况下，Mobile Prevent for Web Server 可接受从网络上任何系统到 ICAP 服务端口的连接。为安全起见，您可以将 ICAP 连接限制为仅应用于指定的系统（或“白名单”）。将一个或多个系统添加白名单后，不在白名单上的系统则不能连接至 Mobile Prevent for Web Server ICAP 服务端口。

注意：Icap.BindAddress 设置会影响代理服务器白名单。默认情况下，Icap.BindAddress 设置为 0.0.0.0，而侦听程序会绑定到所有可用地址。如果 Icap.BindAddress 指示侦听程序绑定到特定 IP，则在白名单上的代理也必须能够访问该侦听程序地址。

创建允许连接到 Mobile Prevent for Web Server ICAP 服务端口的系统白名单：

- 在 Enforce Server 管理控制台中，转至“系统”>“服务器”>“概述”，然后单击所需的 Mobile Prevent for Web Server。
- 在显示的“服务器详细信息”屏幕上，单击“服务器设置”。
- 向下滚动至 Icap.AllowHosts 设置。

默认情况下，Icap.AllowHosts 设置为 any，表示网络上的所有其他系统均可与此 Mobile Prevent for Web Server 进行通信。

- 您可以限制允许与此 Mobile Prevent for Web Server 连接的系统。删除 any，输入您要授权的系统 IP 地址或完全限定域名称 (FQDN)。

请以逗号分隔多个地址。例如：

123.14.251.31,webcache.corp.mycompany.com,123.14.223.111。 仅使用逗号分隔多个条目；不要包含空格。

- 单击“保存”。

对此设置所做的更改在您重新启动 Mobile Prevent for Web Server 之后才会生效。

请参见第 1237 页的“[代理服务器与 Mobile Prevent 间的兼容性](#)”。

请参见第 1236 页的“[关于代理服务器配置](#)”。

为 Mobile Prevent 启用 GET 处理

默认情况下，Mobile Prevent 不处理 HTTP GET 命令，因为这类命令的流量很高。若要使服务器处理 GET 命令，请按照以下过程操作：

为 Mobile Prevent 启用 GET 处理

- 1 按代理服务器文档所述，将 Web 代理服务器配置为将 GET 请求转发至 Mobile Prevent for Web Server。
- 2 确保 Mobile Prevent for Web Server 上的 **L7.processGets** 高级服务器设置必须为 true（默认值）。
- 3 减小 Mobile Prevent for Web Server 上的 **L7.minSizeofGetURL** 高级设置的大小。从默认值 100 减小为小于最短网站 URL（您要从其处理 GET 命令）长度的字节数。如果将最小 URL 大小设为 10，将处理所有情况。但是请注意，减小 GET 的最小大小会增大必须处理的请求数，这会增加服务器流量负载。
- 4 调整 Mobile Prevent 的“服务器详细信息”页 ICAP 部分中的“忽略小于以下大小的请求”设置。从默认的 4096 字节减少为将使请求接受 DLP 检查的较小值。但是请注意，减少此值会增加服务器流量负载。

创建 Mobile Prevent 的策略

您可以创建包含大多数标准响应规则的策略。响应规则包括：添加注释、限制事件数据保留、记录到 Syslog 服务器、设置属性和设置状态。

请参见第 775 页的“[关于 Symantec Data Loss Prevention 报告](#)”。

也可以加入以下 Mobile Prevent Server 所特有的响应规则：

■ Network Prevent 和 Mobile Prevent: 阻止 HTTP/HTTPS

阻止包含机密数据的发布（按策略中所定义）。这包括 Web 发布、基于 Web 的电子邮件、上传到网站或附加到基于 Web 的电子邮件的文件。

注意：某些应用程序可能不会对**“Network Prevent 和 Mobile Prevent: 阻止 HTTP/HTTPS”**响应操作做出适当响应。在 Yahoo! Mail 应用程序中，检测服务器在阻止文件上传时出现过这种情况。如果用户尝试上传电子邮件附件并且附件触发了**“Network Prevent: 阻止 HTTP/HTTPS”**响应操作，Yahoo! Mail 不会做出响应，也不会显示说明文件已被阻止的错误消息。相反，Yahoo! Mail 看上去仍在继续上传选择的文件，但是上传永远无法完成。用户必须在某个时间通过手动单击“取消”来取消上传。

其他应用程序可能也存在这种情况，这取决于它们如何处理阻止请求。在这些情况下，即使应用程序没有发出这种指示，也会创建检测服务器事件，并阻止文件上传。

■ Network Prevent 和 Mobile Prevent: 删除 HTTP/HTTPS

从包含机密数据的发布中删除机密数据（按策略中所定义）。这包括基于 Web 的电子邮件和上传到网站的文件。请注意，“删除 HTTP/HTTPS 内容”操作仅对请求有效。

■ Network Prevent 和 Mobile Prevent: 阻止 FTP 请求

阻止包含机密数据的 FTP 传输（按策略中所定义）。

有关设置任意响应规则操作的详细信息，请打开联机帮助。

转至“管理”>“策略”>“响应规则”，然后单击“添加响应规则”。

即使不在策略中加入响应规则，只要策略包含检测规则 Mobile Prevent 也会捕获事件。可以设置此类策略，在实施阻止或删除内容的策略之前监视移动设备上的 Web 和 FTP 活动。

如果已将代理配置为同时转发 HTTP/HTTPS 请求和响应，则策略对二者均有效。例如，策略同时适用于网站的上传和下载内容。

创建 Mobile Prevent 的测试策略

1 在 Enforce Server 管理控制台中创建包含 Mobile Prevent 特有操作之一的响应规则。例如，创建包含**“Network Prevent 和 Mobile Prevent: 阻止 HTTP/HTTPS”**操作的响应规则。

请参见第 669 页的**“配置响应规则”**。

2 创建包含在上一步中配置的响应规则的策略。

例如，按如下所示创建称为“测试策略”的策略：

- 包括按照关键字“secret”进行匹配的“内容匹配关键字”检测规则。
- 包括**“Network Prevent 和 Mobile Prevent: 阻止 HTTP/HTTPS”**响应规则。

■ 将它与“默认”策略组相关联。

请参见第 330 页的[“配置策略”](#)。

针对安全银行业务配置 Mobile Prevent

若要使移动设备用户可发送其银行信息，可将代理服务器配置为允许此类流量绕过检测服务器。绕过检测服务器使移动设备用户可访问他们自己的个人信用卡和在线银行信息以及将这些信息用于合法用途。如果未将代理服务器配置为允许个人银行信息绕过检测，则用户提交个人银行信息可能会创建事件。具有相关基于角色的权限的 Symantec Data Loss Prevention 用户可能会查看包含组织内用户机密银行信息的事件快照。

配置代理服务器，使其将网络流量直接重定向到银行网站。还可以使用此解决方法来允许发往其他安全网站的网络流量。通过将流量重定向到这些特定网站，移动设备用户在访问这些站点时就不会发生策略违规误报。组织中的其他人看不到这些用户发送到这些站点的信息。

注意：以下过程是一个说明如何将 Blue Coat 代理服务器配置为重定向网络流量的示例。有关如何配置代理服务器的更多信息，请参见代理服务器随附的文档。

将代理服务器配置为重定向网络流量

- 1 使用管理员帐户登录到代理服务器。
- 2 打开 **Visual Policy Manager (VPM)**（可视策略管理器 (VPM)）。
- 3 选择 **SSL Intercept Layer policy**（SSL 截取层策略）。
- 4 为目标主机添加一个规则。对于本示例，请输入允许用户访问的银行业务网站的主机名。
- 5 在 **Action**（操作）下，选择 **Disable SSL interception**（禁用 SSL 截取）。
- 6 单击 **Apply**（应用）保存更改。

测试 Mobile Prevent

可以通过发送违反测试策略的电子邮件来对 Mobile Prevent 进行测试。

测试系统

- 1 将您的移动设备连接到 Internet 并连接到您公司的 VPN。
- 2 打开您公司的电子邮件客户端，然后发送一封附件中包含机密数据的电子邮件。例如，访问 Microsoft Outlook 客户端，并发送一封附件含有 *Secret* 一词及更多文本段落的电子邮件。

- 3 在 Enforce Server 管理控制台中，转至“事件”>“移动设备”，然后单击“事件 - 全部”。查找生成的事件。例如，搜索包括适当的时间戳和策略名称的事件条目。
- 4 单击相关事件条目来查看完整的事件快照。
请参见第 776 页的[“关于使用报告的策略”](#)。

索引

符号

- 824
- “颁发机构信息访问”字段 108
- “服务器详细信息”屏幕 194
 - 服务器配置 176
- “系统概述”屏幕
 - 检测服务器, 添加 187

A

- AddDefaultHeader 字段 897
- AddDefaultPassHeader 字段 897
- Administrator 帐户
 - 电子邮件帐户 53
 - 关于 51
 - 密码, 更改 52
- AdminPasswordReset 实用程序 95
- AES 密钥 261
- AgentInstall.msi 软件包 1184
- AllowHosts 字段 900, 913, 1238
- 安装
 - 插件 1167
- 安装日志文件 233

B

- BindAddress 字段 899, 913, 1238
- Blue Coat ProxySG 911, 1237
- BoxMonitor 进程 234
- 报告 731, 747, 755, 775
 - 控制板 779
 - 事件 777
 - 系统事件 126
 - 选项列表 801
 - 摘要 783
- 报告 API 796
- 报告 API 权限 88
- 本地化. 请参见 语言和字符集
- 补救 713
 - 电子邮件响应变量 718
 - 命令 717

部署

- SMS 1166
 - 使用 Endpoint FlexResponse 实用程序 1169
 - 使用静默安装 1166

C

- CA 证书
 - 导入 190
- CD/DVD
 - 关于 1131
- create_error_file 属性 271
- CRLDP 吊销检查
 - 配置代理 111
 - 支持 108
- 操作日志文件 233
- 策略
 - 部署 310
 - 创建 347
 - 关于 305
 - 管理 347
 - 解决方案软件包 308
 - 配置 330
 - 权限, 创建 310
 - 权限, 管理 310
 - 权限, 响应规则 310
 - 删除 353
 - 数据配置文件 312
 - 添加 329
 - 添加响应规则 352
 - 组件 306
- 策略, 关于
 - 实施 314
 - 用户组 314
- 策略规则
 - 复合 344
- 策略规则, 检测
 - 添加 332
- 策略规则, 配置
 - 规则严重性 337
 - 匹配计数 337

- 策略规则, 条件
 - 配置 334
- 策略规则, 组
 - 添加 332
- 策略检测
 - 端点匹配条件 293
 - 端点事件 284
 - 服务器执行逻辑 297
 - 复合规则 297
 - 规则 290
 - 规则严重性 295
 - 国际语言 495
 - 技术 285
 - 简单规则 297
 - 简介 283
 - 可识别的文件类型 506
 - 跨组件匹配 294
 - 例外 290, 296
 - 目录组匹配 (DGM) 288
 - 内容 283
 - 内容条件 290
 - 确切数据匹配 (EDM) 286
 - 身份 285
 - 身份匹配条件 293
 - 索引文档匹配 (IDM) 287
 - 网络 284
 - 文件属性 284
 - 文件属性匹配条件 291
 - 向量机学习 (VML) 287
 - 移动 284
 - 用于网络的协议监控 292
 - 邮件组件 294
 - 语言 285
 - 指定内容匹配 (DCM) 288
 - 自定义 289
 - 组匹配条件 293
- 策略检测, 端点
 - 端点设备类或 ID 476
 - 端点位置 476
 - 目标, 关于 470
 - 设备, 关于 470
 - 设备, 管理 474
 - 设备, 配置 474
 - 设备, 添加 474
 - 实施, 关于 469
 - 位置, 关于 471
 - 协议, 关于 470
 - 协议或端点监控 471
- 策略检测, 关键字匹配
 - 实施 445
 - 示例 446
 - 通配符, 关于支持, 对 445
- 策略检测, 关键字匹配, 配置
 - 内容匹配关键字 448
- 策略检测, 关于
 - Enterprise Vault 数据分类服务 47
 - 关键字匹配 445
- 策略检测, 国际
 - 查找关键字 497
 - 数据标识符 497
- 策略检测, 配置
 - 选择匹配的邮件组件 339
- 策略检测, 配置的 DGM
 - “发送者/用户匹配来自确切数据配置文件的目录”条件 493
 - “接受者匹配来自确切数据配置文件的目录”条件 493
 - 创建确切数据源文件 492
- 策略检测, 配置的目录组匹配
 - 实施, 关于 491
- 策略检测, 条件
 - “发送者/用户匹配来自确切数据配置文件的目录”条件 493
 - “接受者匹配来自确切数据配置文件的目录”条件 493
 - 端点设备类或 ID 476
 - 端点位置 476
 - 发送者/用户基于目录服务器组匹配用户组 488
 - 发送者/用户匹配模式 480
 - 接受者基于目录服务器组匹配用户组 489
 - 内容匹配关键字 448
 - 内容匹配确切数据 (EDM) 372
 - 内容匹配文档签名 380
 - 内容匹配正则表达式 453
 - 协议或端点监控 471
 - 协议监控 467
 - 邮件附件大小或文件大小匹配 461
 - 邮件附件或文件类型匹配 460
 - 邮件附件名或文件名匹配 462
 - 自定义文件类型签名 463
- 策略检测, 网络
 - 实施 465
 - 协议监控 466
- 策略检测, 文件大小
 - 邮件附件大小或文件大小匹配 461
- 策略检测, 文件类型
 - 邮件附件或文件类型匹配 460

- 自定义 458
- 自定义文件类型签名 463
- 策略检测, 文件名
 - 邮件附件名或文件名匹配 462
- 策略检测, 文件属性
 - 实施 457
 - 文件类型检测 458
- 策略检测, 移动
 - 实施 467
 - 协议监控 467
- 策略检测, 正则表达式
 - 编写 454
 - 内容匹配正则表达式 453
 - 实施 453
- 策略检测, 指定身份
 - 发送者/用户匹配模式 480
 - 关于 479
- 策略检测, 自定义文件类型
 - 启用方法 463
- 策略检测, 关键字邻近
 - 关于 446
- 策略检测模板, 配置
 - 1998 年人权法 612
 - 1998 年英国数据保护法案 594
 - Caldicott 报告 587
 - CAN-SPAM 法案 589
 - FACTA 2003 (红色标记规则) 602
 - HIPAA 和 HITECH (包括 PHI) 608
 - NASD 规则 2711 以及 NYSE 规则 351 和 472 616
 - NASD 规则 3010 和 NYSE 规则 342 618
 - NERC 电气设备安全指导 619
 - OMB 备忘录 06-16 和 FIPS 199 条例 623
 - PIPEDA 626
 - SEC 公平披露规则 634
 - SWIFT 代码 641
 - Symantec DLP 感知与避免 641
 - Webmail 646
 - Yahoo 留言板 647
 - 暴力与武器 646
 - 并购协议 615
 - 常见间谍软件上传站点 591
 - 出版文档 630
 - 出口管理条例 (EAR) 600
 - 赌博 606
 - 非法药品 612
 - 个人纳税识别号 (ITIN) 613
 - 攻击性语言 621
 - 国防信息系统 (DMS) 的常规服务分类 597
 - 国际武器贸易条例 (ITAR) 613
 - 加密数据 600
 - 加拿大社会保险号 589
 - 价格信息 628
 - 简历 631
 - 金融服务法案 606
 - 金融信息 605
 - 禁止访问的网站 605
 - 竞争对手通信 591
 - 客户数据保护 593
 - 媒体文件 614
 - 美国情报控制标记 (CAPCO) 和 DCID 1/7 644
 - 美国社会安全号 645
 - 密码文件 625
 - 欧盟数据保护规定 596
 - 萨班斯-奥克斯利法案 632
 - 设计文档 598
 - 受限接受者 631
 - 受限文件 631
 - 外国资产管制办公室 (OFAC) 622
 - 网络安全 621
 - 网络图 620
 - 下流语言 636
 - 项目数据 629
 - 信用卡号 592
 - 英国国家保险号码 643
 - 英国国民保健服务 (NHS) 号 642
 - 英国护照号 643
 - 英国驾照号 642
 - 英国税号策略 644
 - 英国选民登记号 642
 - 员工数据保护 599
 - 源代码 637
 - 支付卡行业 (PCI) 数据安全标准 625
 - 种族歧视语言 630
 - 州数据隐私 637
 - 专有媒体文件 629
 - 策略例外
 - 复合 344
 - 配置 342
 - 添加 340
 - 策略例外, 配置
 - 匹配计数 337
 - 策略模板
 - 创建策略 317
 - 从 10 版导出 352
 - 导出 311, 351
 - 导入 311, 351
 - 导入 11 版 352
 - 机密文档 591

- 客户和员工数据保护 322
 - 美国监管执法 319
 - 添加 329
 - 系统定义的 308
 - 英国与国际监管执法 321
 - 策略模板, 国际
 - 关于 495
 - 策略模板, 类型
 - 端口 80 上的 Yahoo 和 MSN Messenger 648
 - 机密的或分类的数据保护 323
 - 可接受使用执法 325
 - 网络安全执法 324
 - 策略模板, 配置
 - 确切数据配置文件, 选择 326
 - 索引文档配置文件, 选择 327
 - 策略条件
 - 内容匹配数据标识符 428
 - 策略违规标头 901
 - 启用 902
 - 策略组
 - 部署 310
 - 创建 349
 - 关于 309
 - 管理 350
 - 默认策略组 309
 - 删除 353
 - 修改 349
 - 插件
 - 在端点上部署 1165
 - 查询 270
 - 查找参数
 - 参数组 840
 - 查找插件. 请参见 关于
 - CSV 关键字映射 857
 - CSV 属性映射 857
 - CSV 数据文件要求 855
 - CSV 文件分隔符 856
 - CSV 文件位置 856
 - CSV, 工作原理 838
 - CSV, 字符集 857
 - LDAP 测试 865
 - LDAP 服务器连接 863
 - LDAP 配置 862
 - LDAP 属性映射 863
 - LDAP, 工作原理 839
 - 部署 841
 - 查找参数 846
 - 超时 853
 - 加载 851
 - 脚本, 运作方式 839
 - 脚本编写 868
 - 脚本链接 872
 - 脚本配置 867
 - 脚本协议过滤 870
 - 脚本语言 839
 - 类型 838
 - 链接 850
 - 链接多个插件 841
 - 启用 850
 - 实施, 工作流程 842
 - 数据所有者电子邮件输出 853
 - 数据所有者输出 853
 - 自定义 876
 - 自定义 (旧版) 840
 - 自动查找 853
 - 自动加载 853
 - 查找插件, 脚本
 - 加密凭据 871
 - 启用凭据 871
 - 产品套件. 请参见 Symantec Data Loss Prevention
 - 常见名称(CN)值 108
 - 存档
 - 事件 823–824
 - 存档的事件
 - 还原 824
 - 删除 825
- D**
- DBPasswordChanger 实用程序
 - 简介 260, 263
 - 使用的先决条件 263
 - 使用示例 264
 - 位于 263
 - 运行 264
 - Documentum 目标 1103
 - 打印机/传真 1132
 - 代理 1166
 - 代理服务器 905, 1231
 - 兼容性, 与 910, 1237
 - 配置 910, 912–913, 1236–1238
 - 代理概述
 - 操作 1196
 - 代理概述屏幕 1193
 - 代理配置
 - 关于 1155
 - 添加 1156
 - 应用 1161

- 代理事件
 - 关于 1198
 - 过滤器选项 1199
- 代码编号
 - 系统事件 138
- 登录和注销 51
- 电子邮件
 - 隔离 901
 - 阻止 900
- 吊销检查
 - 配置 110
 - 支持 108
- 调试日志文件 233, 245
- 逗号分隔值 272
- 端点
 - 不兼容的检测规则和响应规则 1137
 - 不同区域设置中的响应规则 1153
 - 策略 1136
 - 代理高级设置 218
 - 代理日志 1204
 - 代理日志级别 1204
 - 隔离响应规则 1145
 - 设置端点位置 1152
 - 事件摘要屏幕 743
 - 用户取消响应规则 1139
 - 在不同的区域设置中设置响应规则 1154
 - 摘要报告 743
 - 端点服务器
 - 冗余 1183
 - 端点工具 1211
 - endpointkeytool 实用程序 1212–1213
 - logdump.exe 工具 1215
 - Service_Shutdown.exe 工具 1214
 - vontu_sqlite3.exe 工具 1215
 - 在 Windows Vista 上使用 1212
 - 端点目标
 - 配置 1147
 - 端点实用程序 260
 - 端点事件
 - 快照 736
 - 列表 733
 - 目标或协议特定的信息 741
 - 端点位置
 - 设置 1152
- E**
- ECU. 请参见 环境检查实用程序
- eculogs.zip 文件
 - 内容 263
- ECUoutput.txt 文件 263
- EDM 索引
 - 使用 278
- EDMIndexDirectory 文件夹 270
- Endace 卡 883
 - 安装驱动程序 885
 - 配置要使用的 Network Monitor 887
 - 驱动程序 884
- Endpoint Discover
 - 报告 1140
 - 创建策略 1144
 - 创建策略组 1144
 - 工作原理 1128
 - 关于 1127
 - 监视 1135
 - 介绍 46
 - 目标过滤器 1147
 - 目标扫描 1136
 - 配置目标 1147
 - 扫描超时设置 1149
 - 扫描空闲超时 1149
 - 扫描目标 1146
 - 实施 1143
 - 添加规则 1145
 - 最大扫描持续时间 1149
- Endpoint FlexResponse
 - 部署 1164
 - 部署插件 1165
 - 关于 1163
 - 使用 Endpoint FlexResponse 实用程序部署插件 1169
 - 使用 FlexResponse 实用程序卸载 1170
 - 在 Enforce Server 上启用 1169
- Endpoint FlexResponse 实用程序 1167
 - 密码 1168
 - 选项 1167
- Endpoint Prevent
 - CD/DVD 监视器 1131
 - 报告 1140
 - 报告响应规则 740
 - 创建策略 1137
 - 打印/传真监视 1132
 - 工作原理 1128
 - 关于 1127
 - 监视 1130
 - 剪贴板监视器 1132
 - 简介 46
 - 可移动介质 1130
 - 实施 1151

- 通知响应规则 1138–1139
 网络共享监视 1133
 网络监视 1133
 应用程序监控 1133
 阻止响应规则 1138
- Endpoint Server**
 关于 1129
 配置, 基本 185
 配置文件过滤器 744
endpointkeytool 实用程序 261, 1212
- Enforce**
 简介 43
 日志记录 239
Enforce Server 262
 不同区域设置中的响应规则 1153
 关于 50
 简介 43
 警报, 配置以发送 135
 启用 Endpoint FlexResponse 1169
 选择非英语语言, 为 62
 在不同的区域设置中设置响应规则 1154
- Enforce Server** 管理控制台
 配置文件屏幕 54
Enforce 控制台. 请参见 管理控制台
- Enterprise Vault** 数据分类服务
 关于 47
- EnvironmentCheckUtility** 命令 262–263
ErrorLog.txt 文件 263
ethtool 883
Exchange 目标 1023
ExportEDMProfile.edm 文件 270
- F**
- Firefox** 浏览器 762
flinst.exe 实用程序
 部署插件 1169
 关于 1167
 检索插件 1170
 检索插件列表 1171
 卸载插件 1170
 反射模式 893
 访问控制列表 (ACL)
 事件快照 806
 分隔符字符 271
 分类
 事件快照 770
 事件列表 769
 分类测试模式 769–770
- 分类服务器
 配置 186
服务 261
服务器 (DLP). 请参见 检测服务器和 Enforce Server
服务器 FlexResponse
 补救 967, 973–974
 部署插件 968, 970
 概述 965
 故障排除 975
 配置 689, 968, 970
 配置响应规则操作 689
 配置自定义属性 970
 使用智能响应操作 973
- G**
- GET 命令 888, 914, 1239
高级服务器设置 886
高级进程控制 174
隔离文件 992
工具密码 1168
关联 730, 754, 771
 关于
 VPN 服务器 1228
 报告 747
 事件详细信息 748
管理
 简介 49
管理控制台
 登录和注销 51
 关于 50
管理器进程 235
管理员帐户
 密码, 重置 95
规则结果缓存 1140
国际化. 请参见 语言和字符集
过滤请求 908, 1233
- H**
- HostLogFile.txt** 文件 263
HTTP 代理. 请参见 代理服务器
HTTP 请求 182
 忽略 907–908, 1232–1233
 阻止 914, 1239
还原
 存档的事件 824
环境检查实用程序
 查找 262–263
 简介 260

- 介绍 261
输出 263
运行 262
基于表单的登录
禁用 114
- I**
- ICAP 45, 907, 912–913, 1232, 1237–1238
配置 910, 1235
Indexed Document Matching
实施, 关于 377
Indexer.properties 文件 271
编辑 279
indexesusing
使用 278
Internet 内容修改协议. 请参见 ICAP
iptables 命令 898–899
iso-8859-1 编码 270, 277
- J**
- JDBC 驱动程序 270
监视程序服务 1183
剪贴板 1132
检测
可破解的 CAD 格式 505
可破解的电子表格格式 502
可破解的电子邮件格式 505
可破解的封装格式 503
可破解的其他格式 506
可破解的数据库文件格式 506
可破解的图形格式 505
可破解的文本和标记格式 504
可破解的文字处理文件格式 500
可破解的演示文稿格式 501
文字处理格式 499
检测, 文件属性
文件和附件大小 459
文件名 459
检测服务器 262
“服务器详细信息”屏幕 194
错误和警告列表 193
的类型 42
服务器设置 195
关于 173
控件 175
配置 176
日志记录 237
删除 189
- 设置, 高级 187
添加 187
系统概述屏幕 191
状态 191
交换端口分析器. 请参见 SPAN
角色
管理 96
配置 85
添加 85, 96
角色, 关于
基于角色的访问控制 77
建议的 82
解决方案软件包, 包括 83
配置 81
警报. 请参见 系统警报
- K**
- 控制板 779
编辑 795
查看 780
删除 800
控制板报告
创建 780
调度 793
配置 782
控制台. 请参见 管理控制台
快照 731, 754
- L**
- Language Pack Utility 63
Linux 系统 898
Livelink 目标 1111
Lock Manager 服务 262
logdump.exe 工具 1215
logdump.exe 实用程序 261
Lotus Notes 目标 995
联机证书状态协议. 请参见 OCSP 吊销检查
列出插件 1167
- M**
- manager-certauth.security 112
manager-certauth.security 文件 110
Microsoft Exchange 目标 1061
Microsoft ISA 911
Microsoft TMG 911
MIME 类型 183, 909, 1234
minSizeofGetURL 字段 914, 1239

- Mobile Prevent**
 - 测试 1241
 - 创建策略 1239
 - 实施 1231
 - 银行业务 1241
- Mobile Prevent (Web)**
 - 配置 1238
- Mobile Prevent for Web**
 - 故障排除 916
 - 配置 913
- Mobile Prevent for Web Server**
 - 配置 1232
- monitorSettings 目录** 261–262
- monitorSettings 文件夹** 263
- MTA** 44, 181, 891, 893, 896
 - 配置 899
- MTAResubmitPort 字段** 897
- MX 记录** 180, 895
- 密码** 264
 - 另请参见 DBPasswordChanger 实用程序
 - Administrator** 52
 - 更改 54, 56, 264
 - 管理员 95
 - 为 Network Discover 扫描加密 934
 - 重置 95
 - 密码更新窗口 56
 - 密码身份验证
 - 禁用 114
 - 启用或禁用 104
- 目录服务器 (LDAP)**
 - 关于连接至 486
 - 连接至 116
- 目录组匹配 (DGM)**
 - 关于 288
- 目录组匹配 (DGM), 同步**
 - 发送者/用户基于目录服务器组匹配用户组 488
 - 计划索引编制 118
 - 接受者基于目录服务器组匹配用户组 489
 - 实施, 关于 485
 - 用户组, 创建 487
 - 用户组, 修改 487
- 目录组匹配 (DGM), 已配置**
 - 实施, 关于 491
- N**
- Napatech** 883
- Network Discover**
 - 报告 757, 961
 - 编辑目标 927
- 发现的运作方式** 921
- 隔离文件** 992
- 简介** 919
- 介绍** 45
- 配置** 923
- 配置目标** 929–930
- 日志记录** 237
- 扫描程序的工作原理** 1041
- 设置** 923
- 事件报告** 757–759, 961–962
- 事件快照** 760
- 事件列表** 763
- 事件摘要** 767
- 添加新目标** 926
- Network Discover Server**
 - Linux** 926
 - 配置 924
 - 配置, 基本 184
 - 配置并行扫描 958
- Network Discover 目标** 1049
 - DB2 数据库** 1003
 - Domino 服务器** 995
 - Exchange** 1023, 1061
 - Livelink** 1111
 - Lotus Notes** 995
 - Oracle 数据库** 1003
 - SharePoint** 1011
 - SharePoint 2003** 1085
 - SharePoint 2007** 1075
 - SQL Server 2005** 1003
 - SQL 数据库** 1003
 - UNIX 文件系统** 1049
 - Web 服务** 1119
 - Web 服务器** 1093
 - Windows 远程服务器文件系统** 1049
 - 删除 946
 - 网站 1093
 - 文档 1103
 - 文件共享 985
 - 自定义 1119
- Network Discover 扫描**
 - 按项大小过滤 937
 - 包含项或储存库 935
 - 报告 943
 - 报告扫描历史记录 947
 - 报告扫描详细信息 950
 - 并行 958
 - 差异扫描 958
 - 调度 931

- 根据上次访问的日期过滤 938
- 根据上次修改的日期过滤 938
- 管理 943
 - 加密密码 934
 - 监控 943
 - 库存扫描 941
 - 目标列表 944
 - 排除项或储存库 935
 - 删除 949
 - 删除目标 946
 - 身份验证 933
 - 审核目标 941
 - 限制 940
 - 优化 940, 953
 - 状态 953
- Network Monitor**
 - 测试 888–889
 - 创建策略 888
 - 简介 44
 - 配置 886
 - 日志记录 239
 - 实施 881, 883
 - 使用 Endace 卡 886
 - 要求 881
- Network Monitor Server**
 - 配置 177
- Network Prevent (Email)**
 - 退回邮件 703
- Network Prevent for Email**
 - 测试 902
 - 创建策略 900
 - 简介 44
 - 路由受限端口至 898
 - 配置 893
 - 启用策略违规标头 902
 - 日志记录 239
 - 实施 891, 893
 - 与 MTA 集成 893
 - 阻止电子邮件 900
- Network Prevent for Email Server**
 - 配置 179
- Network Prevent for Web**
 - 测试 916
 - 创建策略, 为 914
 - 简介 44
 - 配置 907
 - 实施 905–906
- Network Prevent for Web Server**
 - 配置 182
- Network Protect**
 - 隔离文件 992
 - 介绍 45
- Network Protect 服务器**
 - 配置, 基本 184
- new_oracle_password 参数** 264
- NIC** 881, 883
- Notification 服务** 262
- O**
 - OCSP 吊销检查**
 - 禁用 112
 - 配置 112
 - 配置代理 111
 - 支持 108
 - Oracle 数据库** 262
 - NLS_LANGUAGE 设置** 62
 - NLS_TERRITORY 设置** 62
- P**
 - PACKET_MMAP 软件** 884
 - password_file 参数** 264
 - pcapstart.reg 文件** 885
 - pdx 扩展名** 277
 - Plugins.properties 文件** 968
 - processGets 字段** 914, 1239
 - ProtectInstaller_10.5.exe 文件** 273
 - 配置文件** 270, 277
 - 匹配项** 730, 754
 - 凭据** 121
 - 凭据存储**
 - 编辑凭据 123
 - 端点凭据 122
 - 管理 123
 - 删除凭据 123
- Q**
 - 确切数据匹配 (EDM)**
 - 创建数据源文件 361
 - 关于 286
 - 迁移旧有 DOE 配置 362
 - 准备编制索引 363
 - 确切数据匹配 (EDM), 关于**
 - 匹配计数 359
 - 确切数据配置文件 359
 - 数据所有者例外 (DOE), 关于 357
 - 索引编制日程表 358
 - 字段映射 358

- 确切数据匹配 (EDM), 配置
 将确切数据源上传到 Enforce 364
 内容匹配确切数据条件, 配置 372
 确切数据配置文件 365
 实施过程 356
 远程 EDM 索引器 364
- 确切数据匹配 (EDM), 配置文件
 调度配置文件索引编制 371
 管理 359
 添加 359
 映射字段 369
- 确切数据匹配 (EDM), 文件编码
 东亚语言, UTF-16 275
 东亚语言, UTF-8 编码 275
 拉丁字符, iso-8859-1 275
- 确切数据匹配, 关于
 实施 356
- R**
- rdx 扩展名 277
 REQMOD 910, 912, 1237
 RequestProcessor 设置 902
 RequestProcessor 字段 897, 899, 902
 RESPROMD 910, 912, 1237
 RRC. 请参见 规则结果缓存
 日志
 查看 138
 日志文件 233
- S**
- Secure Computing Secure Web 911
 ServerSocketPort 字段 897
 Service_Shutdown.exe 工具 1214
 Service_Shutdown.exe 实用程序 261
 SharePoint 2003 目标 1085
 SharePoint 2007 目标 1075
 SharePoint 目标 1011
 SMTP 900
 SOAP 消息 236
 SPAN 881, 883
 SQL 261, 270
 SQL 预索引器实用程序
 查找 269
 故障排除 271
 简介 260
 介绍 269
 命令行选项 270-271
 运行远程 EDM 索引器 269
- Squid Web Proxy 911
 SSL 证书
 导入 190
 sslkeytool 264
 生成服务器证书 266
 选项 265
- sslkeytool 实用程序
 简介 260
- Symantec Data Loss Prevention
 产品套件 41
 初始系统设置 52
 管理 49
- Symantec Data Loss Prevention for Mobile
 简介 47
- Symantec Data Loss Prevention 服务器. 请参见 检测
 服务器和 Enforce Server
- Symantec DLP Agent
 AgentInstall.msi 软件包 1184
 安全 1181
 安装 1178
 安装前步骤 1180
 高级设置 218
 关于 1129
 管理 1193
 监视程序服务 1183
 删除 1200
 身份验证密钥 1182
 使用 Symantec Management Console 进行安装 1187
 使用 Symantec Management Console 进行删除 1201
 使用系统管理软件 (SMS) 删除 1201
 使用系统管理软件安装 1188
 手动安装 1189
 手动删除 1203
 已安装的内容 1178
 在 Windows Vista 上安装 1180
 在 Windows Vista 上移除 1202
- Symantec DLP 服务
 启动 73-75
 停止 73-75
- Symantec Management Agent
 安装 1175
- Symantec Management Console 1173
 Symantec Management Agent 1175
 报告 1176
 创建用户任务 1177
 代理任务 1176
 克隆广告与程序 1174

- 使用计算机发现 1174
- Symantec Web Gateway 911
- syslog 服务器 134
- System Center Configuration Manager 1188
- Systems Management Server (SMS) 1188
- 扫描
 - 差异扫描 955
 - 增量扫描 955–957
- 删除
 - 存档的事件 825
- 身份验证密钥 1182
- 身份验证凭据 121
- 升级, 系统 152
- 升级代理
 - 卸载密码 1187
- 实用程序
 - 简介 259–260
- 事件 723, 726–728, 730–731, 748, 750, 752, 754
 - 补救 725, 750
 - 存档 823–824
 - 还原存档的 824
 - 禁止存档 825
 - 删除 799
 - 属性, 状态 827
 - 自定义属性 833
 - 自定义属性, 以及 835
- 事件报告 775
 - Network Discover 759
 - 保存 789
 - 编辑自定义报告 795
 - 补救事件 715
 - 查看事件 785
 - 查看摘要报告 784
 - 创建摘要报告 784
 - 打印 804
 - 导出为 CSV 795
 - 导出为 XML 795
 - 导航页面 801
 - 调度 789, 791
 - 过滤 788, 807
 - 过滤器选项 802
 - 简介 777
 - 控制板 779, 786
 - 控制板, 创建 780
 - 控制板, 配置 782
 - 删除自定义报告 800
 - 设置常规过滤器 808
 - 设置高级过滤器 815
 - 设置首选项 777
- 实施战略 776
- 通过电子邮件发送 803
- 摘要 779, 783, 807
- 摘要选项 802, 811
- 自定义 786
- 事件报告和更新 API
 - 权限 88
- 事件报告权限 88
- 事件报告与更新 Web 服务 236
- 事件补救 713
 - 电子邮件响应变量 718
 - 命令 717
- 事件更新权限 88
- 事件快照
 - ACL 信息 806
 - Network Discover 760
 - 策略部分 805
 - 分类 770
 - 关联选项卡 805
 - 历史记录选项卡 804
 - 匹配项部分 806
 - 自定义属性部分 804
- 事件列表
 - Mobile Prevent 748
 - Network Discover 763
 - Network Monitor 和 Network Prevent 723
 - 分类 769
- 事件详细信息 748
- 事件摘要
 - Network Discover 767
- 试用模式 180, 893, 907, 1232
- 受限端口 897–898
- 属性 727, 731, 748, 754, 834
- 数据包捕获软件 882–883
 - 安装 884
- 数据标识符
 - “内容匹配数据标识符”条件 428
 - 编辑验证器输入 438
 - 创建 437
 - 关于 414
 - 管理 428
 - 规范化程序, 列表 430
 - 可选验证器, 关于 418
 - 可选验证器, 可接受字符 434
 - 可选验证器, 配置 433
 - 克隆, 手动 438
 - 跨组件匹配 419
 - 宽度, 关于 417
 - 宽度, 列表 430

模式 420
 模式语言限制, 关于 420
 配置, 关于 424
 实施, 模式 440
 实施, 自定义 439
 实施自定义脚本验证器 442
 数据规范化程序, 关于 424
 添加 428
 系统定义的 415
 修改 437
 修改, 关于 419
 选择验证器 441
 验证器, 关于 421
 验证器, 可用 421
 自定义, 关于 423
 自定义脚本验证器, 关于 421
 最佳做法 442
 数据丢失防护. 请参见 Symantec Data Loss Prevention
 数据分类服务
 事件快照 770
 事件列表 769
 数据库
 编制索引 270-271
 索引 270
 索引文档匹配
 “内容匹配文档签名”条件 380
 过滤文档 386
 计划索引编制 388
 加入白名单 383
 排除内容 383
 准备文档源以便编制索引 382
 索引文档匹配 (IDM)
 关于 287
 配置文档配置文件 384
 实施 382
 添加文档配置文件 384
 文档配置文件, 管理 378
 文档配置文件, 添加 378

T

Tab 符分隔的文件 272
 TagHighestSeverity 字段 902
 TagPolicyCount 字段 902
 TagScore 字段 902
 telnet 命令 899
 TLS 代理 180, 898
 Tomcat
 更改信任存储区密码 106
 将证书添加到 105

U

UTF-16 编码 270, 277
 UTF-8 编码 270, 277

V

Vontu 服务
 启动 70-75
 停止 70-75
 vontu_sqlite3.exe 工具 1215
 vontu_sqlite3.exe 实用程序 261
 VPN
 关于 1228

W

Web 存档 830
 Web 服务 88
 Websense V 系列 912
 Webwasher 911
 WinPcap 软件 883-884
 安装 884
 网络 TAP 881, 883
 网络共享监视 1133
 网络接口卡. 请参见 NIC
 网络连接
 检查 262
 违犯的策略 901
 文件
 编制索引 272

X

X-CFilter-Loop: Reflected 标头 897
 X-DLP-Max-Severity 标头 902
 X-DLP-Policy-Count 标头 902
 X-DLP-Score 标头 902
 XML 架构 796
 系统报告
 调度 791
 系统概述屏幕 191
 错误和警告列表 193
 服务器状态 191
 系统警报
 关于 135
 配置服务器 135
 添加 136
 修改 136
 系统设置, 初始 52
 系统升级 152

- 系统事件 125
 - Syslog 服务器 134
 - 报告 126
 - 报告, 过滤 127
 - 报告, 已保存 128
 - 代码编号 138
 - 类型 (严重性) 130
 - 事件详细信息 129
 - 通知方法 126
 - 响应 132
 - 阈值, 配置 130
- 系统帐户 262
- 下一 MTA 字段 896
- 响应规则 726
 - 编写电子邮件响应 716
 - 关于 653
 - 管理 667
 - 配置 669
 - 添加 667
 - 修改排序 673
 - 最佳做法 665
- 响应规则, 操作
 - Endpoint Discover: 隔离文件 693
 - Endpoint Prevent 通知, 配置 697
 - Endpoint Prevent 用户取消, 配置 699
 - Endpoint Prevent 阻止 694
 - Endpoint: FlexResponse 692
 - Mobile Prevent 阻止 FTP 请求 701
 - Mobile Prevent 阻止 HTTP/S 702
 - Network Prevent 阻止 FTP 请求 701
 - Network Prevent 阻止 HTTP/S 702
 - Network Prevent: 删除 HTTP/HTTPS 内容 706
 - Network Prevent: 修改 SMTP 邮件 704
 - Network Prevent: 阻止 SMTP 邮件 703
 - Network Protect 复制文件 707
 - Network Protect 隔离文件, 配置 708
 - 保留端点事件数据 685
 - 丢弃网络事件数据 686
 - 发送电子邮件通知 687
 - 记录到 Syslog 服务器 686
 - 配置 671
 - 设置属性 690
 - 设置状态 691
 - 添加注释 684
 - 限制事件数据保留 684
- 响应规则, 关于
 - 操作 654
 - 操作的执行优先级 662
 - 创建权限 664
- 删除 674
- 实施 664
- 条件 661
- 执行 659
- 智能 660
- 智能, 配置 670
- 自动 659
- 响应规则, 类型
 - Endpoint Prevent 通知 1139
 - Endpoint Prevent 用户取消 1139
 - Endpoint Prevent 阻止 1138
 - network protect 658
 - 端点 656
 - 端点隔离 1145
 - 分类 658
 - 所有检测服务器 655
 - 网络 657
- 响应规则, 添加
 - 智能 668
 - 自动 668
- 响应规则, 条件
 - 端点设备 676
 - 端点位置 675
 - 配置 670
 - 事件类型 677
 - 事件匹配数 678
 - 协议或端点监控 679
 - 严重性 681
- 响应过滤 909, 1234
- 向量机学习 (VML)
 - “当前配置文件”选项卡 399
 - “临时工作区”选项卡 399
 - 编辑配置文件名称, 说明 408
 - 创建新的 VML 配置文件 398
 - 调整内存分配 403
 - 调整相似度阈值 412
 - 关于 287
 - 管理 VML 配置文件 406
 - 管理培训集 405
 - 接受培训 404
 - 拒绝培训 404
 - 培训内容 397
 - 培训配置文件 401
 - 配置 VML 规则 408
 - 配置 VML 例外 410
 - 上传培训的内容 399
 - 实施过程 396
 - 相似度评分 411
 - 相似度阈值 411

校验和卸载 883

卸载 1170

卸载密码

使用 1186

许可证 151

Y

移动设备

部署情景 1223

银行业务

Mobile Prevent 1241

应用程序监控 1133

关于 1207

添加应用程序 1208

用户

管理 97

添加 97

用户, 关于

配置 81

用户, 密码

配置强密码或循环密码 95

用户, 身份验证

Active Directory 97

将 Enforce 与 Active Directory 集成 98

为 Active Directory 身份验证配置 Enforce 101

验证 Active Directory 连接 100

用户, 帐户

配置 91

添加 91

用户代理 908, 1233

邮件传输代理. 请参见 MTA

语言包

Language Pack Utility 63

关于 61

语言和字符集

选择非英语语言 62

语言包, 关于 61

语言包, 使用 63

字符集, 使用 60

远程 EDM 索引器实用程序

安装 273-274

创建 EDM 配置文件 275

故障排除 278

简介 260, 272

命令行选项 277

使用示例 277

使用要求 272

卸载 279

运行 272-275, 277-278

运行 SQL 预索引器 269

Z

增量扫描 955-957

摘要报告 731, 755

证书

sslkeytool 264, 266

服务器, 生成 266

证书存储

添加身份验证 121

证书吊销列表分发点. 请参见 CRLDP 吊销检查

证书身份验证

故障排除 113

配置 102

配置吊销检查 108, 110

启用或禁用 104

添加 CA 证书 105

映射 CN 值 108

指定内容匹配 (DCM)

关于 288

转发模式 893

状态属性 827

状态值

配置 829

删除 829

添加 829

状态组

配置 829

删除 829

添加 829

字符编码 270

自定义属性 731, 754, 833-834

编辑 835

查询选项 (事件快照) 835

创建 835

使用 833

事件快照 804

手动设置值 836

填充 835

用途 834

阻止请求 914, 1239

组规则, 类型

接受者匹配模式 482

组例外, 类型

接受者匹配模式 482