

安装指南

Novell[®] Sentinel 6.1 Rapid Deployment

SP2

2011 年 4 月

www.novell.com



法律声明

Novell, Inc. 对本文档的内容或使用不作任何声明或保证，特别是对适销性或用于任何特定目的的适用性不作任何明示或暗示保证。另外，Novell, Inc. 保留随时修改本出版物及其内容的权利，并且没有义务将这些修改通知任何个人或实体。

Novell, Inc. 对任何软件不作任何声明或保证，特别是对适销性或用于任何特定目的的适用性不作任何明示或暗示保证。另外，Novell, Inc. 保留随时修改 Novell 软件全部或部分内容的权利，并且没有义务将这些修改通知任何个人或实体。

依据本协议提供的任何产品或技术信息都将受到美国出口控制和其他国家 / 地区的贸易法律的约束。您同意遵守所有出口控制法规，并同意在出口、再出口或进口可交付产品之前取得所有必要的许可证或分类证书。您同意不出口或再出口至当前美国出口排除列表上所列的实体，或者美国出口法律中规定的任何被禁运的国家 / 地区或支持恐怖主义的国家 / 地区。您同意不将可交付产品用于禁止的核武器、导弹或生物化学武器的最终用途。有关出口 Novell 软件的详细讯息，请访问 [Novell International Trade Services 网页 \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/)。如果您未能获得任何必要的出口许可，Novell 对此不承担任何责任。

版权所有 © 1999-2011 Novell, Inc. 保留所有权利。未经出版商的明确书面许可，不得复制、影印、传送此出版物的任何部分或将其储存在检索系统上。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

联机文档: 要访问该 Novell 产品及其他 Novell 产品的最新联机文档，请参见 [Novell 文档网页 \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/)。

Novell 商标

有关 Novell 商标，请参见 [Novell 商标和服务标记列表 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html)。

第三方资料

所有第三方商标均属其各自所有者的财产。

目录

关于本指南	7
1 产品概述	9
1.1 Sentinel 6.1 Rapid Deployment 概述	9
1.2 Sentinel 6.1 Rapid Deployment 配置	10
1.3 Sentinel Rapid Deployment 用户界面	11
1.3.1 Sentinel 6.1 Rapid Deployment Web 界面	11
1.3.2 Sentinel 控制中心	12
1.3.3 Sentinel 数据管理器	12
1.3.4 Sentinel 解决方案设计器	12
1.3.5 Sentinel Plug-In SDK	13
1.4 Sentinel 服务器组件	13
1.4.1 数据访问服务	13
1.4.2 讯息总线	13
1.4.3 Sentinel 数据库	13
1.4.4 Sentinel 收集器管理器	14
1.4.5 关联引擎	14
1.4.6 iTRAC	14
1.4.7 Sentinel Advisor 和攻击检测	14
1.4.8 Web 服务器	14
1.5 Sentinel 插件	14
1.5.1 收集器	15
1.5.2 连接器和集成器	15
1.5.3 关联规则和操作	15
1.5.4 报告	15
1.5.5 iTRAC 工作流程	16
1.5.6 解决方案包	16
1.6 语言支持	16
2 系统要求	17
2.1 支持的平台	17
2.1.1 支持的操作系统	17
2.2 硬件要求	18
2.3 支持的 Web 浏览器	20
2.4 虚拟环境	20
2.5 建议的限制	20
2.5.1 收集器管理器限制	20
2.5.2 报告限制	21
2.6 测试结果	21
3 安装	23
3.1 概述	23
3.1.1 服务器组件	23
3.1.2 客户端应用程序	24
3.2 在 SUSE Linux Enterprise 服务器上安装	24
3.2.1 先决条件	24
3.2.2 安装 Sentinel Rapid Deployment	25

3.3	安装收集器管理器和客户端应用程序	30
3.3.1	下载安装程序	30
3.3.2	Sentinel Rapid Deployment 客户端组件的端口号	30
3.3.3	安装 Sentinel 客户端应用程序	31
3.3.4	在 SLES 或 Windows 上安装 Sentinel 收集器管理器	33
3.4	手动启动和停止 Sentinel 服务	35
3.5	手动升级 Java	35
3.6	安装后配置	36
3.6.1	更改日期和时间设置	36
3.6.2	将 SMTP 集成器配置为发送 Sentinel 通知	36
3.6.3	收集器管理器服务	37
3.6.4	管理时间	37
3.7	LDAP 鉴定	38
3.7.1	概述	38
3.7.2	先决条件	38
3.7.3	配置 Sentinel 服务器以进行 LDAP 鉴定	39
3.7.4	配置多个 LDAP 服务器以实现故障转移	41
3.7.5	为多个 Active Directory 域配置 LDAP 鉴定	43
3.7.6	使用 LDAP 用户身份凭证进行登录	44
3.8	将许可证密钥从评估密钥升级到产品密钥	44
4	升级 Sentinel Rapid Deployment	45
4.1	先决条件	45
4.2	在服务器上安装增补程序	45
4.3	升级收集器管理器和客户端应用程序	46
4.3.1	升级收集器管理器	46
4.3.2	升级客户端应用程序	47
5	Sentinel Rapid Deployment 安全注意事项	49
5.1	强化	49
5.1.1	开箱即用强化	49
5.1.2	确保 Sentinel Rapid Deployment 数据安全	49
5.2	在网络中保证通讯安全	50
5.2.1	Sentinel 服务器进程之间的通讯	50
5.2.2	Sentinel 服务器与 Sentinel 客户端应用程序之间的通讯	50
5.2.3	服务器与数据库之间的通讯	51
5.2.4	收集器管理器与事件源之间的通讯	51
5.2.5	与 Web 浏览器之间的通讯	51
5.2.6	数据库与其他客户端之间的通讯	51
5.3	保护用户和口令	52
5.3.1	操作系统用户	52
5.3.2	Sentinel 应用程序和数据库用户	52
5.3.3	实施用户的口令策略	53
5.4	保护 Sentinel 数据	53
5.5	备份信息	56
5.6	保护操作系统的安全	57
5.7	查看 Sentinel 审计事件	57
5.8	使用 CA 证书	58
6	测试 Sentinel Rapid Deployment 功能	59
6.1	测试 Rapid Deployment 安装	59
6.2	测试后的清理	70

6.3	使用真实数据	71
7	卸载 Sentinel Rapid Deployment	73
7.1	卸载 Sentinel Rapid Deployment 服务器	73
7.2	卸载远程收集器管理器和 Sentinel 客户端应用程序	73
7.2.1	Linux	73
7.2.2	Windows	74
7.2.3	卸载后过程	74
A	更新 Sentinel Rapid Deployment 主机名	77
A.1	服务器	77
A.2	客户端应用程序	77
B	疑难解答提示	79
B.1	由于输入无效身份凭证而导致数据库鉴定失败	79
B.2	Sentinel Web 界面启动失败	79
B.3	在启用 UAC 后，远程收集器管理器在 Windows 2008 上发生例外	80
B.4	未针对映像的收集器管理器创建 UUID	80
C	PostgreSQL 数据库维护的最佳实践	83
C.1	修改内存配置参数	83
C.2	降低 Vacuum/Analyze 造成的 I/O 影响	83

关于本指南

本指南的目的是提供对 Novell Sentinel 6.1 Rapid Deployment Service Pack 2 的简介，并对安装过程进行说明。

- ◆ 第 1 章“产品概述”（第 9 页）
- ◆ 第 2 章“系统要求”（第 17 页）
- ◆ 第 3 章“安装”（第 23 页）
- ◆ 第 4 章“升级 Sentinel Rapid Deployment”（第 45 页）
- ◆ 第 5 章“Sentinel Rapid Deployment 安全注意事项”（第 49 页）
- ◆ 第 6 章“测试 Sentinel Rapid Deployment 功能”（第 59 页）
- ◆ 第 7 章“卸装 Sentinel Rapid Deployment”（第 73 页）
- ◆ 附录 A “更新 Sentinel Rapid Deployment 主机名”（第 77 页）
- ◆ 附录 B “疑难解答提示”（第 79 页）
- ◆ 附录 C “PostgreSQL 数据库维护的最佳实践”（第 83 页）

适用对象

本文档供信息安全专业人员使用。

反馈

我们希望收到您对本手册和本产品中包含的其他文档的意见和建议。请使用每页联机文档底部的用户意见功能并发表您的意见。

其他文档

Sentinel 技术文档可分成几本不同的卷册。它们是：

- ◆ *Novell Sentinel Rapid Deployment 安装指南* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)
- ◆ *Novell Sentinel Rapid Deployment 用户指南* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html)
- ◆ *Novell Sentinel Rapid Deployment 参考指南* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html)
- ◆ *Novell Sentinel 安装指南* (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)
- ◆ *Novell Sentinel 用户指南* (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/)
- ◆ *Novell Sentinel 参考指南* (http://www.novell.com/documentation/sentinel61/s61_reference/?page=/documentation/sentinel61/s61_reference/data/)
- ◆ *Sentinel SDK* (http://www.novell.com/developer/develop_to_sentinel.html)

Sentinel SDK 站点提供了有关开发收集器（专有或 JavaScript）以及 JavaScript 关联操作的细节。

联系 Novell

- ◆ *Novell 网站* (<http://www.novell.com>)
- ◆ *Novell 技术支持* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- ◆ *Novell 自我支持* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- ◆ *增补程序下载站点* (<http://download.novell.com/index.jsp>)
- ◆ *Novell 24x7 支持* (<http://www.novell.com/company/contact.html>)
- ◆ *Sentinel TIDS* (<http://support.novell.com/products/sentinel>)
- ◆ *Sentinel 社区支持论坛* (<http://forums.novell.com/novell-product-support-forums/sentinel/>)
- ◆ *Sentinel 插件网站* (<http://support.novell.com/products/sentinel/secure/sentinelplugins.html>)
- ◆ 通知电子邮件列表：通过 Sentinel 插件网站进行注册

产品概述

Sentinel 6.1 Rapid Deployment 是 Novell Sentinel 的一个简化版本，它使用了开放源代码的 PostgreSQL、activeMQ 和 JasperReports 组件。

以下章节将帮助您了解 Sentinel 6.1 Rapid Deployment 系统的主要组件。本《Sentinel Rapid Deployment 安装指南》包含有关安装和配置过程的详细信息。《Sentinel Rapid Deployment 用户指南》(http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) 则对体系结构、操作及管理过程进行了详细说明。

- ◆ 第 1.1 节“Sentinel 6.1 Rapid Deployment 概述”（第 9 页）
- ◆ 第 1.2 节“Sentinel 6.1 Rapid Deployment 配置”（第 10 页）
- ◆ 第 1.3 节“Sentinel Rapid Deployment 用户界面”（第 11 页）
- ◆ 第 1.4 节“Sentinel 服务器组件”（第 13 页）
- ◆ 第 1.5 节“Sentinel 插件”（第 14 页）
- ◆ 第 1.6 节“语言支持”（第 16 页）

1.1 Sentinel 6.1 Rapid Deployment 概述

Sentinel 是一种安全信息和事件管理解决方案。它可接收来自整个企业中许多来源的信息，并将这些信息标准化、设置这些信息的优先顺序，然后将这些信息提供给您，以便您制定与威胁、风险和策略相关的决策。

Sentinel 可实现日志收集、分析和报告过程的自动化，以确保 IT 控件有效支持威胁检测要求和审计要求。Sentinel 使用对安全性与合规性事件以及 IT 控件的连续自动监控替代了劳动密集型的手动执行过程。

Sentinel 还会收集并关联来自整个组织的网络基础设施以及第三方系统、设备和应用程序的安全和非安全信息。Sentinel 以 GUI 形式显示收集的数据、识别安全性或合规性问题并跟踪修正活动，以简化易于出错的过程并构建一个严谨、安全的管理程序。

通过自动事件响应管理可以记录并正式确定对事件及违反策略的情况进行跟踪、提交和响应的过程，并可以提供与问题工单系统的双向集成。使用 Sentinel 可以及时响应事件并有效解决事件。

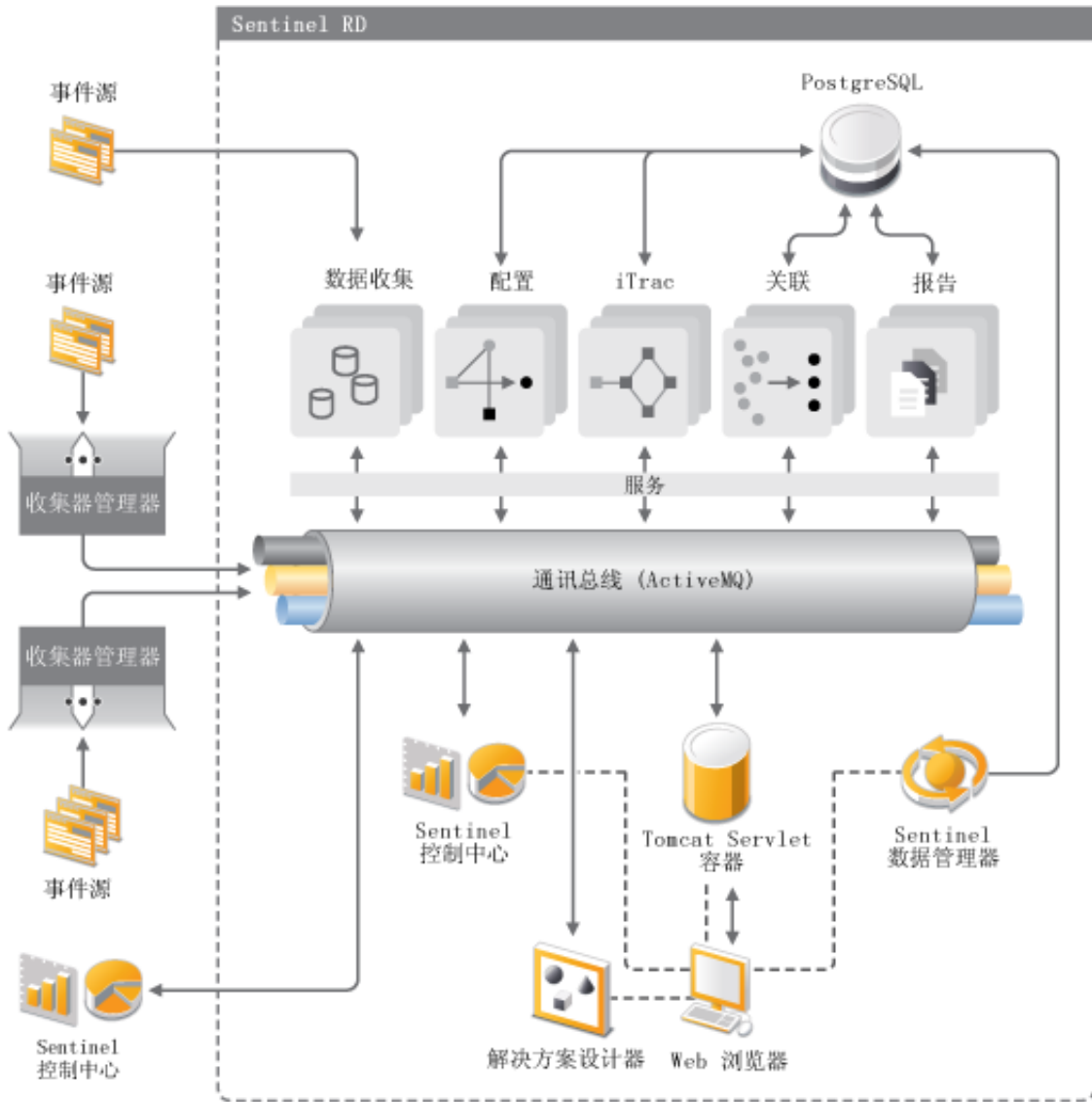
使用解决方案包可以简便地将 Sentinel 关联规则、动态列表、映射、报告和 iTRAC 工作流程分发并导入到控件中。这些控件可设计为符合特定规范要求（如“支付卡行业数据安全标准”），或者，它们可以与特定数据源（如数据库的用户身份验证事件）关联。

借助于 Sentinel Rapid Deployment，您可以获得：

- ◆ 集成的自动化实时安全管理和合规性监控（覆盖所有系统和网络）功能。
- ◆ 一个由业务策略决定 IT 策略和行动的架构。
- ◆ 对整个企业的安全、系统和访问事件的自动记录和报告。
- ◆ 内置的事件管理和修正功能。
- ◆ 展示和监控对内部策略和政府法规（例如 Sarbanes-Oxley 法案、HIPAA 法案、GLBA 和 FISMA 法案等）的遵守情况的能力。实施这些控件所需的内容正是通过解决方案包分发并实施的。

以下是 Sentinel Rapid Deployment 的概念性体系结构的图示，其中说明了涉及执行安全性和合规性管理的组件。

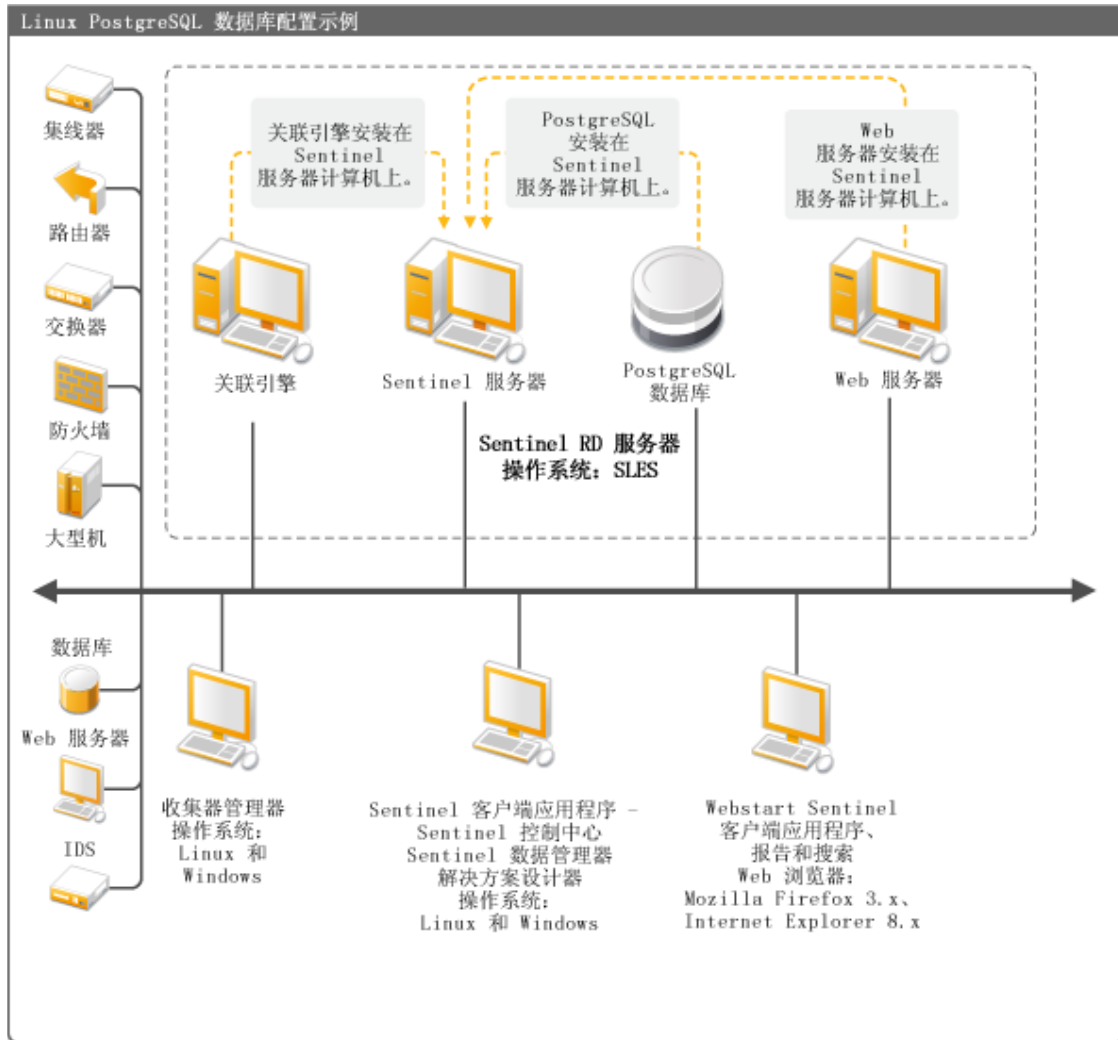
图 1-1 Sentinel 的概念性体系结构



1.2 Sentinel 6.1 Rapid Deployment 配置

下图说明了 Sentinel 6.1 Rapid Deployment 的配置设置。

图 1-2 Sentinel 6.1 Rapid Deployment 配置



1.3 Sentinel Rapid Deployment 用户界面

Sentinel 包含以下易于使用的用户界面：

- ◆ [Sentinel 6.1 Rapid Deployment Web 界面](#)
- ◆ [Sentinel 控制中心](#)
- ◆ [Sentinel 数据管理器](#)
- ◆ [Sentinel 解决方案设计器](#)
- ◆ [Sentinel Plug-In SDK](#)

1.3.1 Sentinel 6.1 Rapid Deployment Web 界面

通过 Novell Sentinel 6.1 Rapid Deployment Web 界面，您可以管理报告，启动 Sentinel 控制中心 (SCC)、Sentinel 数据管理器和解决方案设计器。您还可以从 Sentinel 6.1 Rapid Deployment Web 界面的 *应用程序* 页面下载收集器管理器的安装程序和客户端安装程序。

有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[通过 Web 界面管理 Sentinel Rapid Deployment](#)”。

1.3.2 Sentinel 控制中心

SCC 提供了一个集成的安全管理仪表盘，分析人员可以利用此仪表盘快速确定新的趋势或攻击、处理实时图形信息并与之交互，并且对事件做出响应。

您可以将 SCC 作为客户端应用程序启动或通过使用 Java Webstart 启动。

SCC 的主要功能包括：

- ◆ **活动视图：**提供实时分析和可视化
- ◆ **分析：**运行并保存脱机查询
- ◆ **事件：**提供事件创建和管理
- ◆ **关联：**提供关联规则定义和管理
- ◆ **iTRAC：**提供记录、实施和跟踪事件解决过程的流程管理
- ◆ **报告：**提供历史报告和度量标准
- ◆ **事件源管理：**提供收集器部署和监视
- ◆ **解决方案管理器：**安装、实施和测试解决方案包内容

有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[Sentinel 控制中心](#)”。

1.3.3 Sentinel 数据管理器

使用 Sentinel 数据管理器可以管理 Sentinel 数据库。您可以在 Sentinel 数据管理器中执行以下操作：

- ◆ 监视数据库空间使用情况。
- ◆ 查看和管理数据库分区。
- ◆ 管理数据库存档。
- ◆ 将存档的数据重新导入到数据库。

有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[Sentinel 数据管理器](#)”。

1.3.4 Sentinel 解决方案设计器

Sentinel 解决方案设计器用于创建和修改解决方案包。解决方案包是已打包的 Sentinel 内容集，如关联规则、操作、iTRAC 工作流程和报告。

Sentinel 内容是 Sentinel 系统的扩展功能。该内容包括 Sentinel 操作、集成器，以及收集器、连接器等 Sentinel 插件和可能包含其他类型插件的解决方案包。这些模块化的组件用于与第三方系统进行集成、安装完整的基于控制的安全解决方案，以及为检测到的事件提供自动修正。

有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[解决方案包](#)”。

1.3.5 Sentinel Plug-In SDK

Sentinel Plug-In SDK 中包含 Novell Engineering 开发的库和代码，以及模板和样本代码，您可以用来开发自己的项目。有关详细信息，请参见 [Sentinel SDK \(http://www.novell.com/developer/develop_to_sentinel.html\)](http://www.novell.com/developer/develop_to_sentinel.html)。

1.4 Sentinel 服务器组件

Sentinel 由以下组件组成：

- ◆ 第 1.4.1 节 “数据访问服务”（第 13 页）
- ◆ 第 1.4.2 节 “讯息总线”（第 13 页）
- ◆ 第 1.4.3 节 “Sentinel 数据库”（第 13 页）
- ◆ 第 1.4.4 节 “Sentinel 收集器管理器”（第 14 页）
- ◆ 第 1.4.5 节 “关联引擎”（第 14 页）
- ◆ 第 1.4.6 节 “iTRAC”（第 14 页）
- ◆ 第 1.4.7 节 “Sentinel Advisor 和攻击检测”（第 14 页）
- ◆ 第 1.4.8 节 “Web 服务器”（第 14 页）

1.4.1 数据访问服务

Sentinel 数据访问服务是用于与 Sentinel 数据库通讯的主要组件。数据访问服务器需与其他服务器组件一同工作，以便将从收集器管理器收到的事件存储到数据库中、过滤数据、处理活动视图显示、执行数据库查询并处理结果，以及处理管理任务（如用户鉴定和授权）。有关详细信息，请参见《*Sentinel Rapid Deployment 参考指南*》中的“[数据访问服务](#)”。

1.4.2 讯息总线

Sentinel 6.1 Rapid Deployment 使用名为 Apache Active MQ 的开放源代码讯息中介程序。该讯息总线可在一秒内将数千个讯息包在 Sentinel 的组件之间进行移动。Apache Active MQ 体系结构是基于 Java 面向消息的中间件 (Java Message Oriented Middleware, JMOM) 构建的，JMOM 支持客户端和服务端应用程序之间的异步调用。当目标程序繁忙或未连接时，讯息队列将提供临时存储。有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[通讯服务器](#)”。

1.4.3 Sentinel 数据库

Sentinel 产品基于存储安全性事件以及所有 Sentinel 元数据的后端数据库构建。Sentinel 6.1 Rapid Deployment 支持 PostgreSQL。事件以规范化的形式与资产和漏洞数据、身份信息、事件和工作流程状态以及许多其他类型的数据存储在一起。有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[Sentinel 数据管理器](#)”。

1.4.4 Sentinel 收集器管理器

Sentinel 收集器管理器管理数据收集、监视系统状态讯息并根据需要执行事件过滤。收集器管理器的主要功能包括转换事件、通过分类为事件添加业务相关性、对事件执行全局过滤、对事件进行路由以及将运行状况讯息发送到 Sentinel 服务器。Sentinel 收集器管理器将直接连接到讯息总线。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[收集器管理器](#)”。

1.4.5 关联引擎

关联引擎可通过自动分析收到的事件流来发现感兴趣的模式，从而提高安全事件管理的智能水平。关联功能允许您定义用于确定严重威胁以及复杂攻击模式的规则，以便确定事件的优先级并进行有效的事件管理和响应。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[关联选项卡](#)”。

1.4.6 iTRAC

Sentinel 提供用于定义事件响应过程并使其自动执行的 iTRAC 工作流程管理系统。可以将 Sentinel 中通过关联规则标识的事件或手动标识的事件与 iTRAC 工作流程关联。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[iTRAC 工作流程](#)”。

1.4.7 Sentinel Advisor 和攻击检测

Sentinel Advisor 是一种可选的数据订阅服务，其中包括已知攻击、漏洞和补救措施方面的信息。此数据结合您所在环境的已知漏洞和实时入侵检测或预防信息，可提供主动的攻击检测，并可让您在存在漏洞的系统遭受攻击时立即采取措施。

Sentinel 6.1 Rapid Deployment 安装在默认情况下会安装一份 Advisor 数据快照。您需要 Advisor 许可证来订购持续的 Advisor 数据更新。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[Advisor 的使用和维护](#)”。

1.4.8 Web 服务器

Sentinel Rapid Deployment 使用 Apache Tomcat 作为其 Web 服务器，以实现与 Sentinel Rapid Deployment Web 界面的安全连接。

1.5 Sentinel 插件

Sentinel 提供各种用于扩展和增强系统功能的插件。其中某些会预安装到系统中。更多插件（及更新）可从 [Sentinel 6.1 插件网站 \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html) 下载。

一些插件（如 Remedy 集成器、IBM Mainframe 连接器和 SAP XAL 连接器）需要额外的许可证才能下载。

- ◆ [第 1.5.1 节“收集器”](#)（第 15 页）
- ◆ [第 1.5.2 节“连接器和集成器”](#)（第 15 页）
- ◆ [第 1.5.3 节“关联规则和操作”](#)（第 15 页）
- ◆ [第 1.5.4 节“报告”](#)（第 15 页）

- ◆ 第 1.5.5 节 “iTRAC 工作流程”（第 16 页）
- ◆ 第 1.5.6 节 “解决方案包”（第 16 页）

1.5.1 收集器

Sentinel 会从源设备收集数据，并会在对事件进行关联和分析并将其发送到数据库之前，通过将分类、利用检测和业务相关性注入数据流，来提供更丰富的事件流。更丰富的事件流意味着数据已与所需业务环境相关联，从而可确定并清除内部或外部的威胁以及违反策略的情况。

Sentinel 收集器可分析来自以下各种类型的设备和更多类型设备的数据：

◆ 入侵检测系统（主机）	◆ 防病毒检测系统
◆ 入侵检测系统（网络）	◆ Web 服务器
◆ 防火墙	◆ 数据库
◆ 操作系统	◆ 大型主机
◆ 策略监视	◆ 漏洞评估系统
◆ 鉴定	◆ 目录服务
◆ 路由器和交换机	◆ 网络管理系统
◆ VPN	◆ 专有系统

可以使用标准 JavaScript 开发工具和收集器 SDK 编写 JavaScript 收集器。

1.5.2 连接器和集成器

连接器通过标准协议（如 JDBC 和 Syslog）提供从收集器管理器到事件源的连接。事件将从连接器传递到收集器以进行分析。

通过集成器可以对 Sentinel 外部的系统执行修正操作。例如，关联操作可使用 SOAP 集成器来启动 Novell Identity Manager 工作流程。

可选的 Remedy AR Integrator 提供了根据 Sentinel 事件创建 Remedy 工单的能力。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[操作管理器和集成器](#)”。

1.5.3 关联规则和操作

关联规则识别事件流中的重要模式。关联规则触发时会启动关联操作，例如发送电子邮件通知、启动 iTRAC 工作流程或使用集成器执行操作。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[关联选项卡](#)”。

1.5.4 报告

可以使用 JasperReports 从 Sentinel Rapid Deployment Web 界面运行多种仪表板和操作报告。此报告通常通过解决方案包分发。

1.5.5 iTRAC 工作流程

iTRAC 工作流程提供了一致的可重复过程以用于管理事件。工作流程模板通常通过解决方案包分发。iTRAC 提供了一组默认模板，您可以加以修改以使其符合自己的需求。有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[iTRAC 工作流程](#)”。

1.5.6 解决方案包

解决方案包是已打包的 Sentinel 相关内容集，如关联规则、操作、iTRAC 工作流程和报告。Novell 提供了侧重于特定业务要求的解决方案包，如 PCI-DSS 解决方案包，该解决方案包处理对支付卡行业数据安全标准的合规性方面的问题。Novell 还创建了收集器包，该包中的内容侧重于特定事件源，例如 Windows Active Directory。有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[解决方案包](#)”。

1.6 语言支持

提供以下语言的 Sentinel 组件：

- ◆ 捷克语
- ◆ 英语
- ◆ 法语
- ◆ 德语
- ◆ 意大利语
- ◆ 日语
- ◆ 荷兰语
- ◆ 波兰语
- ◆ 葡萄牙语
- ◆ 简体中文
- ◆ 西班牙语
- ◆ 繁体中文

系统要求

为获得最佳性能和可靠性，您必须在已获批准的软件和硬件（如本章节中所列）上安装 Sentinel Rapid Deployment 组件。本章节所述的要求已经过质量保证流程的全面检验和认可。

- ◆ 第 2.1 节“支持的平台”（第 17 页）
- ◆ 第 2.2 节“硬件要求”（第 18 页）
- ◆ 第 2.3 节“支持的 Web 浏览器”（第 20 页）
- ◆ 第 2.4 节“虚拟环境”（第 20 页）
- ◆ 第 2.5 节“建议的限制”（第 20 页）
- ◆ 第 2.6 节“测试结果”（第 21 页）

2.1 支持的平台

表 2-1 列出了 Novell 认可或支持的软件与操作系统组合。经过认可的组合已使用 Novell Engineering 的整套测试套件进行了测试。支持的组合预计可以发挥全部功能。

2.1.1 支持的操作系统

Novell 支持在本章节中所述的操作系统版本上运行 Sentinel Rapid Deployment。Novell 还支持在经过次要更新（如安全增补程序或热修复）的这些操作系统上运行。不过，在经过重大更新的这些平台的系统上运行 Sentinel Rapid Deployment 则不受支持，除非这些更新已经过 Novell 的测试和认可。

Sentinel Rapid Deployment 服务器组件包括通讯服务器、关联引擎、数据访问服务 (DAS)、Web 服务器以及 Advisor 数据订阅服务。

Sentinel 客户端应用程序包括 Sentinel 控制中心 (SCC)、Sentinel 数据管理器 (SDM) 以及 Sentinel 解决方案设计器 (SSD)。

收集器管理器有特殊的平台要求。

表 2-1 支持和认可的操作系统

平台	服务器组件	Sentinel 客户端应用程序	收集器管理器
SUSE Linux Enterprise Server (SLES) 11 SP1 (64 位)	已认可	已认可	已认可
SUSE Linux Enterprise Server (SLES) 11 SP1 (32 位)	不支持	支持	支持
SUSE Linux Enterprise Server (SLES) 10 SP3 (64 位)	已认可	支持	支持
SUSE Linux Enterprise Server (SLES) 10 SP3 (32 位)	支持	支持	支持

平台	服务器组件	Sentinel 客户端应用程序	收集器管理器
Windows Server 2008 R2 (64 位)	不支持	已认可	已认可
Windows Server 2003 R2 (64 位)	不支持	支持	支持
Windows Server 2003 R2 (32 位)	不支持	支持	支持
Windows XP SP3 (32 位)	不支持	支持	不支持
Windows Vista SP2 (32 位)	不支持	支持	不支持
Windows 7	不支持	已认可	不支持

请遵循下列指南以获得最佳性能、稳定性和可靠性：

- ◆ 对于 SLES，Sentinel Rapid Deployment 服务器计算机的操作系统必须至少包含 SLES 的基础服务器和 X Window 组件。
- ◆ 对于 Sentinel Rapid Deployment 服务器，请使用 ext3 文件系统。有关文件系统的详细信息，请参见《存储管理指南》中的 [Linux 中的文件系统概述 \(http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html\)](http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html)。

注释：

- ◆ 在安装了 Open Enterprise Server 的 SLES 上不支持 Sentinel Rapid Deployment。
- ◆ Sentinel 6.1 Rapid Deployment 服务器的 32 位演示版本设计为使用 32 位硬件和操作系统，供规模有限的演示和测试环境使用。签订了 Sentinel 6.1 Rapid Deployment 支持合同的客户或合作伙伴可以获得关于此平台的有限支持，Novell 技术支持会针对那些可在 64 位生产平台上重现的问题提供支持服务。由于 32 位硬件的固有限制，Novell 技术支持不会受理 32 位演示版本的性能和可伸缩性问题。32 位演示版本不支持用于生产环境。

2.2 硬件要求

Sentinel Rapid Deployment 服务器组件运行于 x86-64 (64 位) 硬件之上，根据具体操作系统的不同也有例外情况，如第 2.1.1 节“支持的操作系统” (第 17 页) 中所述。Sentinel 已在 AMD Opteron 和英特尔“至强”硬件上经过了认可。“天腾”服务器不受支持。

本章节中包括一些用于 Sentinel 系统设计的一般硬件建议。设计建议是根据事件发生率范围而得出的。但是，这些建议基于以下假设：

- ◆ 事件发生率处于每秒事件数 (EPS) 范围的上限。
- ◆ 平均事件大小为 1 KB。
- ◆ 所有事件都存储在数据库中 (即，没有用于丢弃事件的过滤器)。
- ◆ 相当于 90 天的数据被联机存储到数据库中。
- ◆ 表 2-2 在第 19 页 和表 2-3 在第 19 页 中的规格不包括用于 Advisor 数据的存储空间。
- ◆ 该 Sentinel 服务器有 5 GB (默认值) 的磁盘空间用于临时缓存无法立即插入到数据库中的事件数据。

- ◆ Sentinel 服务器还提供默认值为 5 GB 的磁盘空间，用于存储无法立即插入到集合事件文件的事件。
- ◆ 可选的 Advisor 订购要求服务器上有 1 GB 的额外磁盘空间。

Sentinel 实施的硬件建议因不同的实施而异，因此，建议在最后确定 Sentinel 体系结构之前，先咨询 Novell 咨询服务部门或任意 Novell Sentinel 合作伙伴。下列建议可以作为指南使用。

在 SLES 版本中，数据库嵌入在 Sentinel Rapid Deployment 服务器中，并与该服务器安装在同一台计算机上。

注释：由于事件负载较高以及需要本地超速缓存，Sentinel 服务器需要拥有本地或共享的条带磁盘阵列 (RAID)，并且该阵列至少包含 4 个磁盘主轴。

表 2-2 单台计算机配置 (最多 2000 eps)

组件	RAM	空间	CPU
计算机 1: Sentinel Rapid Deployment 服务器	16 GB	1 TB, SAS (15K rpm) 硬盘	Dell PowerEdge 2900, 2 x Quad-Core Intel Xeon E5310 (1.6 GHz), 带千兆以太网 NIC
◆ 嵌入式 PostgreSQL 数据库 (3 GB)		硬件 RAID 10	
◆ 收集器管理器 (1228 MB)			
◆ DAS_Core (1579 MB)			
◆ DAS_Binary (1404 MB)			
◆ 关联引擎 (1073 MB)			
◆ 4 个收集器 (Generic、Cisco、Snort 和 IBM, 各生成 500 eps)			
◆ 部署了 10 个关联规则			
◆ 10 个唯一活动视图			
◆ 3 个同步用户			
◆ 部署了 2 张地图			

表 2-3 三台计算机配置 (最多 5000 eps)

组件	RAM	空间	CPU
计算机 1: Sentinel Rapid Deployment 服务器	16 GB	1 TB, SAS (15K rpm) 硬盘	Dell PowerEdge 2900, 2 x Quad-Core Intel Xeon E5310 (1.6 GHz), 带千兆以太网 NIC
◆ 嵌入式 PostgreSQL 数据库 (3 GB)		硬件 RAID 10	
◆ 收集器管理器 (1228 MB)			
◆ DAS_Core (1579 MB)			
◆ DAS_Binary (1404 MB)			
◆ 关联引擎 (1073 MB)			
◆ 4 个收集器 (各生成 500 eps, 1500 EPS 来自远程收集器管理器 1, 1500 EPS 来自远程收集器管理器 2。)			

组件	RAM	空间	CPU
计算机 2: 收集器管理器 <ul style="list-style-type: none"> ◆ 收集器管理器 / 收集器 ◆ 3 个收集器 (每个生成 500 eps) 	4 GB	300 GB, SATA (3 Gbit/s) 硬盘	Intel Core 2 Duo E6750 (2.66 GHz), 带千兆以太网 NIC
计算机 3: 收集器管理器 <ul style="list-style-type: none"> ◆ 收集器管理器 / 收集器 ◆ 3 个收集器 (每个生成 500 eps) 	4 GB	300 GB, SATA (3 Gbit/s) 硬盘	Intel Core 2 Duo E6750 (2.66 GHz), 带千兆以太网 NIC

2.3 支持的 Web 浏览器

- ◆ Mozilla Firefox 3.x
- ◆ Internet Explorer 8.x

2.4 虚拟环境

Sentinel Rapid Deployment 在 VMWare ESX 服务器上接受了广泛测试，Novell 完全支持在此环境中使用 Sentinel Rapid Deployment。要在 ESX 或其他任何虚拟环境中获得与物理计算机相近的性能，虚拟环境应提供与物理计算机建议配置相同的内存、CPU、磁盘空间及 I/O 条件。

有关适用于 SLES 系统的物理计算机建议的信息，请参见第 2.2 节“硬件要求”（第 18 页）

2.5 建议的限制

本章节中所述的限制为以 Novell 或客户所做性能测试为基础而提出的建议，并非硬性限制。这些建议只是近似值。在具备高度动态特性的系统中，最好在构建系统时预留一定缓冲空间，为系统扩展留下余地。

- ◆ 第 2.5.1 节“收集器管理器限制”（第 20 页）
- ◆ 第 2.5.2 节“报告限制”（第 21 页）

2.5.1 收集器管理器限制

除非另行指明，否则收集器管理器限制假设系统配置如下：4 个 CPU 核心，每个核心的频率为 2.2 GHz，4 GB RAM，操作系统为 SLES 11。

表 2-4 收集器管理器性能参数

属性	限制	注释
收集器管理器的最大数量	20	此限制假设每个收集器管理器都以低 EPS 运行（例如，低于 100 EPS）。当每秒事件数增长时，此限制会随之降低。
单个收集器管理器上连接器（完全利用）的最大数量	每个 CPU 核心一个，至少保留一个 CPU 核心供操作系统及其他处理程序使用	完全利用的连接器是指以该类型的连接器所能实现的最高 EPS 运行的连接器。

属性	限制	注释
单个收集器管理器上收集器（完全利用）的最大数量	每个 CPU 核心一个，至少保留一个 CPU 核心供操作系统及其他处理程序使用	完全利用的收集器是指以该类型的收集器所能实现的最高 EPS 运行的收集器。
单个收集器管理器上设备的最大数量	2000	Sentinel Rapid Deployment 服务器的限制也是 2000，因此如果单个收集器管理器上有 2000 个设备，则仅这一个收集器管理器就会让整体 Sentinel 系统达到其设备数量限制。
Sentinel Rapid Deployment 服务器上设备的最大数量	2000	Sentinel Rapid Deployment 服务器上的设备数限制是 2000。

2.5.2 报告限制

表 2-5 报告性能参数

属性	限制	注释
已保存报告的最大数量	200	可以根据报告大小以及服务器上未被系统其余进程占用的可用磁盘空间来增大或减小此限制。
同时运行的最大报告数量	3	此限制假设服务器未由于执行数据收集或其他任务而处于高利用率状态。

2.6 测试结果

Sentinel Rapid Deployment 可让您根据环境的需要采用不同的配置。以下性能测试信息为 Novell 针对下列表格中所列特定配置进行的测试结果。

针对 Sentinel 实施提供的硬件建议根据每种实施的不同而异；因此，我们建议您在最终确定 Sentinel 体系结构之前，先向 Novell 咨询服务或任何 Novell Sentinel 合作伙伴进行咨询。下列测试信息可以作为指南使用。

Linux 测试目的是通过使用不同数量的设备调整最高 EPS 值，并调整特定 EPS 的最大设备数。使用了以下硬件配置：

- ◆ CPU 核心数量：4
- ◆ CPU 型号：Intel Xeon CPU X5770， 2.93 GHz
- ◆ RAM：16 GB
- ◆ 硬盘大小（+RAID 类型和 RAID 中的磁盘数）：1.7 TB（RAID 5， 6 个磁盘）

注释：所有测试都是使用基于 syslog 的事件源完成。其他连接器的性能可能有所不同。

下表显示了您在 SLES 系统上使用不同数量的设备可以调整的最高 EPS：

表 2-6 SLES 系统上的最高 EPS

系统设置	设备数	最高 EPS
4 个收集器管理器（一个本地，三个远程），每个管理器包含 10 个收集器，每个收集器生成 500 EPS	25	5,000
4 个收集器管理器（一个本地，三个远程），每个管理器包含 10 个收集器，每个收集器生成 500 EPS	100	5,000
4 个收集器管理器（一个本地，三个远程），每个管理器包含 10 个收集器，每个收集器生成 500 EPS	1,000	5,000

下表显示了您在 SLES 系统上使用不同 EPS 率可以调整的最大设备数：

表 2-7 SLES 系统上的最大设备数

系统设置	EPS	最大设备数
1 个收集器管理器，包含 1 个收集器，该收集器生成 500 EPS	500	2,000
1 个收集器管理器，包含 2 个收集器，每个收集器生成 500 EPS	1,000	2,000
1 个收集器管理器，包含 3 个收集器，每个收集器生成 500 EPS	1,500	2,000

注释：

- ◆ 如果要调整更多的 EPS 或设备，请安装更多的收集器管理器。
- ◆ 最大设备数限制并非硬性限制，而是基于 Novell 完成的性能测试提供的建议值。这些建议值假定每个设备每秒的平均事件率较小（小于 3 EPS）。更高的 EPS 率会导致可持续最大设备数降低。可使用等式“（最大设备数）x（每个设备的平均 EPS）= 最大事件率”算出特定的平均 EPS 率或设备数的大致限制，前提是最大设备数不超过上面指定的限制。

本章节提供安装 Sentinel Rapid Deployment 和客户端组件的相关信息。

- ◆ 第 3.1 节“概述”（第 23 页）
- ◆ 第 3.2 节“在 SUSE Linux Enterprise 服务器上安装”（第 24 页）
- ◆ 第 3.3 节“安装收集器管理器和客户端应用程序”（第 30 页）
- ◆ 第 3.4 节“手动启动和停止 Sentinel 服务”（第 35 页）
- ◆ 第 3.5 节“手动升级 Java”（第 35 页）
- ◆ 第 3.6 节“安装后配置”（第 36 页）
- ◆ 第 3.7 节“LDAP 鉴定”（第 38 页）
- ◆ 第 3.8 节“将许可证密钥从评估密钥升级到产品密钥”（第 44 页）

3.1 概述

Sentinel 安装包为您提供了一个简单易用的单计算机服务器安装程序，供您安装运行 Sentinel Rapid Deployment 所需的一切。Sentinel Rapid Deployment 服务器安装程序将安装以下组件：

- ◆ 第 3.1.1 节“服务器组件”（第 23 页）
- ◆ 第 3.1.2 节“客户端应用程序”（第 24 页）

3.1.1 服务器组件

表 3-1 Sentinel 服务器组件和应用程序

组件	说明
	Sentinel 数据库存储着配置和事件数据。
讯息总线	基于 JMS 的讯息总线处理 Sentinel 系统中各组件之间的通讯。
关联引擎	关联引擎执行实时事件分析。
Advisor	Advisor 提供检测到的 IDS 攻击和漏洞扫描输出之间的实时关联，以立即指出组织中新增的危险。
数据访问服务	包括数据存储、查询、显示和处理组件。
Web 服务器	支持 Sentinel Rapid Deployment 的 Web 界面。
收集器管理器	用于处理事件源的连接、数据分析和映射等的服务。
	通过 Sentinel Rapid Deployment Web 界面上提供的收集器管理器安装程序，可以将收集器管理器分发到其他位置、其他计算机和其他操作系统。例如，您可以在一台 Windows 计算机上安装一个附加的收集器管理器以收集 Windows 事件。

组件	说明
iTRAC	Sentinel 提供用于定义事件响应过程并使其自动执行的 iTRAC 工作流程管理系统。可以将 Sentinel 中通过关联规则标识的事件或手动标识的事件与 iTRAC 工作流程关联。

3.1.2 客户端应用程序

Sentinel 控制中心、Sentinel 数据管理器以及解决方案设计器等客户端应用程序默认会安装于 Sentinel Rapid Deployment 服务器上。您可以使用以下任意方法启动客户端应用程序：

- ◆ 使用 Sentinel Rapid Deployment Web 界面。要通过 Webstart 启动 Sentinel 应用程序，客户端系统中应当安装 Java 1.6.0_20 或更高版本，并应设置 JRE 路径。

请将 JAVA_HOME 环境变量设置为指向 JRE 6 文件夹的位置。将导出路径设置为指向 JRE 6 位置下的 bin 文件夹。

- ◆ 以 Sentinel Rapid Deployment 安装文件所有者的身份使用 `<安装目录>/bin`。例如：
`./bin/<client_application>.sh`

表 3-2 Sentinel 客户端应用程序

组件	说明
Sentinel 控制中心	供安全性或合规性分析人员使用的主控制台。
Sentinel 数据管理器	数据库管理实用程序。
解决方案设计器	用于创建解决方案包的应用程序。
Sentinel 收集器管理器	一项处理到事件源的连接、数据分析和映射等的服务。收集器管理器安装在 Sentinel 服务器上，但是可通过可下载的安装程序在远程 Windows 或 Linux 计算机上安装更多的收集器管理器。

3.2 在 SUSE Linux Enterprise 服务器上安装

- ◆ [第 3.2.1 节“先决条件”](#)（第 24 页）
- ◆ [第 3.2.2 节“安装 Sentinel Rapid Deployment”](#)（第 25 页）

3.2.1 先决条件

在安装 Sentinel Rapid Deployment 之前，请确保您已满足以下先决条件。有关这些先决条件的详细信息（包括经过认可的平台的列表），请参见 [第 2 章“系统要求”](#)（第 17 页）。

- ◆ [服务器](#)（第 25 页）
- ◆ [客户端](#)（第 25 页）
- ◆ [Advisor](#)（第 25 页）

重要：使用完整安装程序的 Sentinel Rapid Deployment 安装应始终在干净的系统上进行。如果任何计算机上以前安装了其他版本的 Sentinel，例如 Sentinel Classic 或 Sentinel Log Manager，您必须先将其卸载。有关卸载先前版本的 Sentinel 的信息，请参见相应的安装指南：

- ◆ 有关卸载 Sentinel Classic 的详细信息，请参见《Sentinel 安装指南》(http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html) 中的“卸载 Sentinel”一章。
 - ◆ 有关卸载 Sentinel Log Manager 的详细信息，请参见《Sentinel Log Manager 1.1 安装指南》(http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html) 中的“卸载 Sentinel Log Manager”一章。
-

服务器

- ◆ 确保每台服务器计算机达到了最低的系统要求。有关系统要求的详细信息，请参见第 2 章“系统要求”（第 17 页）。
- ◆ 以 `hostname -f` 命令返回一个有效主机名这种方式配置操作系统。
- ◆ 如果希望能够从 Sentinel 系统发送邮件通知，请安装并配置 SMTP 服务器。

客户端

- ◆ 确保每台客户端计算机达到了最低的系统要求。有关这些先决条件的详细信息，请参见第 2 章“系统要求”（第 17 页）。
- ◆ 确保您从其中运行安装程序的目录的名称中只含 ASCII 字符（且不含特殊字符）。
- ◆ 当在 Linux 计算机上安装远程收集器管理器或客户端应用程序时，请确保未针对 /tmp 文件夹为管理员用户设置文件夹级别限制。
- ◆ 确保在 Windows 上为收集器管理器的域用户提供了高级用户特权，普通用户权限不能满足收集器管理器安装的需要。
- ◆ 如果要在 64 位计算机上安装收集器管理器，请确保 32 位库可用。在运行以专有语言（其中包括了几乎所有在 2008 年 6 月之前编写的收集器）编写的收集器时以及在运行特定连接器（如 LEA 连接器）时，需要使用 32 位库。基于 JavaScript 的收集器和 Sentinel 的其余部分都支持 64 位。在 Linux 平台上，验证这些库是否可用是特别重要的。默认情况下，Linux 平台可能不包括这些库。

Advisor

如果要安装 Advisor，您必须购买 Sentinel 攻击检测和 Advisor 数据订阅。购买了订阅后，请使用您的 Novell eLogin 来下载和更新 Advisor 数据。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“Advisor 的使用和维护”一章。

3.2.2 安装 Sentinel Rapid Deployment

Sentinel Rapid Deployment 服务器可按以下方式安装：

- ◆ 使用根权限进行单脚本安装（第 26 页）
- ◆ 非根安装（第 28 页）

Sentinel Rapid Deployment 安装程序脚本会在安装期间提供以下选项：

- ◆ **-all**：您必须具有根用户权限才能使用此选项。此选项会创建一个用户（默认值：novell）、一个用户组（默认值：novell），然后安装 Sentinel Rapid Deployment 服务器。还可以在系统启动时自动运行 Sentinel Rapid Deployment 服务。
- ◆ **-install**：此选项只提供安装 Sentinel Rapid Deployment 服务器的功能。
- ◆ **-createuser**：您必须具有根用户权限才能使用此选项。此选项只会创建用户（默认值：novell）和用户组（默认值：novell）。
- ◆ **-createservice**：您必须具有根用户权限才能使用此选项。此选项只提供让 Sentinel Rapid Deployment 服务在系统启动时自动运行的功能。
- ◆ **-help**：此选项会显示有关如何使用安装脚本选项的帮助内容。

使用根权限进行单脚本安装

1 以根用户身份登录。

执行安装的用户必须拥有对将用于存放所下载安装程序文件的临时目录的写权限。

2 从 Novell 下载站点将 [sentinel6_rd_linux_x86-64.tar.gz](http://download.novell.com/) (<http://download.novell.com/>) 安装程序下载至临时目录。

3 提取安装程序：

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

4 切换到提取安装程序的目录：

```
cd sentinel6_rd_linux_x86-64
```

5 使用 -all 选项运行 install.sh 脚本：

```
./install.sh -all
```

安装脚本会先检查可用内存和磁盘空间。如果可用内存少于 1 GB，脚本会自动终止安装。如果可用内存大于 1 GB 但少于 4 GB，脚本会显示一条讯息，提醒您可用内存少于建议值。它还会询问您是否要继续进行安装。如果要继续安装，请输入 y，如果不希望继续，请输入 n。

6 指定用户名，或按 Enter 选择默认用户名。默认用户名为 novell。

如果指定的用户名已存在，安装程序会显示一条讯息，说明该用户已存在并列出于所属的组。继续 [步骤 8](#)。

如果指定的用户名不存在，安装程序将创建该用户名。继续 [步骤 7](#)。

7 指定组名称，或按 Enter 选择默认组名称。默认组名称为 novell。

如果指定的组名称已存在，安装程序将继续进行安装。如果指定的组名称不存在，安装程序将创建该组，并显示一条讯息，说明指定的用户名已在指定的组内创建。

指定的用户和组将拥有 Sentinel 的安装和运行进程。

8 指定安装路径，或按 Enter 选择默认路径。默认路径为 /opt/novell/。

指定的安装路径不应包含空格。如果路径包含空格，安装脚本会提示您提供一个不含空格的安装路径。

9 通过输入相应的编号，从以下语言中选择一种语言：

序列号	语言
1	捷克语

序列号	语言
2	英语
3	法语
4	德语
5	意大利语
6	日语
7	荷兰语
8	波兰语
9	葡萄牙语
10	简体中文
11	西班牙语
12	繁体中文

最终用户许可协议即会以选定的语言显示。

- 10** 阅读最终用户许可协议，如果同意其中的条款并想要继续安装，请输入 1。如果要退出安装，请输入 2。

随后，安装程序开始提取文件，并显示有关许可证的提示。

- 11** 输入 1 以使用为期 90 天的评估许可证密钥，或输入 2 以使用有效许可证密钥。

如果您输入 2，安装程序会提示您输入有效的 Sentinel RD 许可证密钥。如果指定的许可证密钥无效，安装程序会提示您重新指定有效的许可证密钥。如果第二次指定的许可证密钥仍然无效，安装程序将自动安装为期 90 天的评估许可证密钥。您可以稍后再输入有效许可证。

脚本随后会加载试用许可证或有效许可证。

- 12** 指定 dbauser 用户的口令，然后再次指定该口令进行确认。

dbauser 身份凭证用于在 PostgreSQL 数据库中创建表和分区。

- 13** 指定 admin 用户的口令，然后再次指定该口令进行确认。

当程序提示您为 admin 和 dbauser 用户指定口令时，请勿在口令中使用反斜线 (\) 和撇号 (') 字符，因为 PostgreSQL 数据库不允许使用这些字符。

安装脚本会安装 PostgreSQL 数据库，创建表和分区，然后安装 Sentinel Rapid Deployment 服务器。

安装后，您可以：

- ◆ 使用以下网址启动 Sentinel Rapid Deployment Web 界面：<https://<服务器IP>:8443/sentinel>。<服务器IP> 即安装了 Sentinel Rapid Deployment 的计算机的 IP 地址。
- ◆ 以步骤 6 中创建的用户身份运行 <安装目录>/bin/control_center.sh 来启动 Sentinel 控制中心。

非根安装

如果贵组织的策略禁止以根用户身份运行完整安装过程，则可以分两步完成安装。安装过程的第一部分必须以根特权来执行，第二部分必须以 Sentinel 管理用户身份（管理用户在第一部分创建）执行。

- 1 登录要安装 Sentinel Rapid Deployment 的服务器。

执行安装的用户必须拥有对将用于存放所下载安装程序文件的临时目录的写权限。

- 2 从 Novell 下载站点将 `sentinel6_rd_linux_x86-64.tar.gz` (<http://download.novell.com/>) 安装程序下载至临时目录。

- 3 提取安装程序：

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

- 4 以根用户身份登录。

- 5 切换到提取安装程序的目录：

```
cd sentinel6_rd_linux_x86-64
```

- 6 使用 `-createuser` 选项运行 `install.sh` 脚本：

```
./install.sh -createuser
```

- 7 指定用户名，或按 `Enter` 选择默认用户名。默认用户名为 `novell`。

如果指定的用户名已存在，安装程序会显示一条讯息，说明该用户已存在并列出于用户所属的组。继续步骤 9。

如果指定的用户名不存在，安装程序将创建该用户名。继续步骤 8。

- 8 指定组名称，或按 `Enter` 选择默认组名称。默认组名称为 `novell`。

如果指定的组名称已存在，安装程序将继续进行安装。如果指定的组名称不存在，安装程序将创建该组，并显示一条讯息，说明指定的用户名已在指定的组内创建。

指定的用户和组将拥有 Sentinel 的安装和运行进程。

- 9 指定安装路径，或按 `Enter` 选择默认路径。默认路径为 `/opt/novell/`。

指定的安装路径不应包含空格。如果路径包含空格，安装脚本会提示您提供一个不含空格的安装路径。

- 10 以非根用户身份登录。例如：

```
su - novell
```

- 11 使用 `-install` 选项运行安装脚本：

```
./install.sh -install
```

安装脚本会先检查可用内存和磁盘空间。如果可用内存少于 1 GB，脚本会自动终止安装。如果可用内存大于 1 GB 但少于 4 GB，脚本会显示一条讯息，提醒您可用内存少于建议值。它还会询问您是否要继续进行安装。如果要继续安装，请输入 `y`，如果不希望继续，请输入 `n`。

- 12 指定安装路径，或按 `Enter` 选择默认路径。默认路径为 `/opt/novell/`。

指定的安装路径不应包含空格。如果路径包含空格，安装脚本会提示您提供一个不含空格的安装路径。

- 13 通过输入相应的编号，从以下语言中选择一种语言：

序列号	语言
1	捷克语
2	英语
3	法语
4	德语
5	意大利语
6	日语
7	荷兰语
8	波兰语
9	葡萄牙语
10	简体中文
11	西班牙语
12	繁体中文

最终用户许可协议即会以选定的语言显示。

- 14** 阅读最终用户许可协议，如果同意其中的条款并想要继续安装，请输入 1。如果要退出安装，请输入 2。

随后，安装程序开始提取文件，并显示有关许可证的提示。

- 15** 输入 1 以使用为期 90 天的评估许可证密钥，或输入 2 以使用有效许可证密钥。

如果您输入 2，安装程序会提示您输入有效的 Sentinel RD 许可证密钥。如果指定的许可证密钥无效，安装程序会提示您重新指定有效的许可证密钥。如果第二次指定的许可证密钥仍然无效，安装程序将自动安装为期 90 天的评估许可证密钥。您可以稍后再输入有效许可证。

脚本随后会加载试用许可证或有效许可证。

- 16** 指定 dbauser 用户的口令，然后再次指定该口令进行确认。

dbauser 身份凭证用于在 PostgreSQL 数据库中创建表和分区。

- 17** 指定 admin 用户的口令，然后再次指定该口令进行确认。

当程序提示您为 admin 和 dbauser 用户指定口令时，请勿在口令中使用反斜线 (\) 和撇号 (') 字符，因为 PostgreSQL 数据库不允许使用这些字符。

- 18** (视情况而定) 安装完成后，如果您希望系统启动时 Sentinel Rapid Deployment 服务自动运行，请以根用户身份使用 -createservice 选项运行 install.sh 脚本：

```
./install.sh -createservice
```

安装后，您可以：

- ◆ 使用以下网址启动 Sentinel Rapid Deployment Web 界面：<https://<服务器IP>:8443/sentinel>。<服务器IP> 即安装了 Sentinel Rapid Deployment 的计算机的 IP 地址。
- ◆ 以上面步骤 7 中创建的用户身份运行 <安装目录>/bin/control_center.sh 来启动 Sentinel 控制中心。

3.3 安装收集器管理器和客户端应用程序

使用 Novell Sentinel Rapid Deployment Web 界面来下载收集器管理器安装程序和客户端安装程序。

- ◆ 第 3.3.1 节“下载安装程序”（第 30 页）
- ◆ 第 3.3.2 节“Sentinel Rapid Deployment 客户端组件的端口号”（第 30 页）
- ◆ 第 3.3.3 节“安装 Sentinel 客户端应用程序”（第 31 页）
- ◆ 第 3.3.4 节“在 SLES 或 Windows 上安装 Sentinel 收集器管理器”（第 33 页）

3.3.1 下载安装程序

1 打开 Web 浏览器访问以下 URL:

```
https://<svrname.example.com>:8443/sentinel
```

使用实际 DNS 名称或运行着 Sentinel 的服务器 IP 地址来替换 <svrname.example.com>。
URL 区分大小写。

2 如果系统提示您校证书，请查看证书信息，如果证书有效，请单击是。

3 指定用户名和口令以访问 Sentinel 帐户。

4 使用 *语言* 下拉列表选择语言。

该语言应与 Sentinel Rapid Deployment 服务器和本地计算机的语言代码相同。请确保浏览器的语言设置配置为支持希望使用的语言。

5 单击 *登录*。

6 选择 *应用程序*。

您可以下载以下安装程序:

选项	说明	操作
收集器管理器安装程序	通过收集器管理器安装程序，您可以在支持的 Windows 和 Linux 平台上安装 Sentinel 收集器管理器。	单击 <i>下载收集器管理器安装程序</i> ，然后按照屏幕指导进行操作。
客户端安装程序	通过客户端安装程序，您可以在支持的平台上安装 Sentinel 控制中心、Sentinel 解决方案设计器和 Sentinel 数据管理器。	单击 <i>下载客户端安装程序</i> ，然后按照屏幕指导进行操作。

有关安装收集器管理器的详细信息，请参见第 3.3.4 节“在 SLES 或 Windows 上安装 Sentinel 收集器管理器”（第 33 页），有关安装客户端安装程序的详细信息，请参见第 3.3.3 节“安装 Sentinel 客户端应用程序”（第 31 页）。

3.3.2 Sentinel Rapid Deployment 客户端组件的端口号

使用下列端口配置您的防火墙设置，以允许 Sentinel Rapid Deployment 服务器和客户端组件之间的访问。

表 3-3 Sentinel Rapid Deployment 组件可兼容的端口号

端口号	说明
61616	远程收集器管理器使用此端口号来通过 ActiveMQ 连接到 Sentinel Rapid Deployment 服务器。
10013	Sentinel 控制中心使用此端口号来通过代理连接到 Sentinel Rapid Deployment 服务器。
5432	Sentinel 数据管理器使用此端口号来连接到 PostgreSQL 数据库。
8443	Web 客户端使用此端口号来连接到 Sentinel Rapid Deployment 服务器。

3.3.3 安装 Sentinel 客户端应用程序

您可以在 Linux 或 Windows 系统上安装 Sentinel 客户端应用程序。要安装客户端应用程序：

- 1 浏览至存放下载的客户端安装程序的文件夹。
- 2 从文件中解压缩安装脚本：

平台	操作
Windows	解压缩 client_installer.zip 文件。 文件将被解压缩到一个名称为 disk1 的目录中。
Linux	使用根权限运行以下命令： <code>unzip client_installer.zip</code> 文件将被解压缩到一个名称为 disk1 的目录中。

- 3 转到安装目录，然后开始安装：

平台	操作
Windows	运行 <code>disk1\setup.bat</code> 注释： 在 Windows Vista 计算机中，通过使用右键单击菜单选项中的 <i>以管理员身份运行</i> 选项来启动命令提示符。
Linux	<ul style="list-style-type: none"> ◆ GUI 模式： <code>< 安装目录 >/disk1/setup.sh</code> ◆ 控制台模式： <code>< 安装目录 >/disk1/setup.sh -console</code>

以下列出的步骤只适用于 GUI 模式。

- 4 单击下拉箭头，然后选择其中一种语言。
- 5 在欢迎屏幕中，单击 *下一步*。
- 6 阅读并接受“最终用户许可协议”。单击 *下一步*。
- 7 接受默认安装目录或单击 *浏览* 指定安装位置。单击 *下一步*。

重要：不能安装到名称中使用了特殊字符或非 ASCII 字符的目录。例如，在 Windows x86-64 上安装 Sentinel Rapid Deployment 时，默认路径是 C:\Program Files(x86)。如果要继续安装，您必须更改这一默认路径以免使用特殊字符，例如 (x86) 中的括号。

8 选择要安装的 Sentinel 应用程序。

下列选项可用：

组件	说明
Sentinel 控制中心	供安全性或合规性分析人员使用的主控制台。
Sentinel 数据管理器 (SDM)	用于手动数据库管理活动。
解决方案设计器	帮助您创建解决方案包。

9 如果选择安装 Sentinel 控制中心，安装程序会提示您需要分配给 Sentinel 控制中心的最大内存空间。指定仅由 Sentinel 控制中心使用的最大 JVM 堆大小 (MB)。

允许的范围是 64-1024 MB。

如果已经安装了任何 Sentinel 应用程序，此选项将不可用。

10 指定用户名，或按 Enter 选择默认用户名。默认用户名为 esecadm。

这是拥有所安装的 Sentinel 产品的用户的用户名。如果此用户尚不存在，将创建此用户，并在指定的目录中创建主目录。

11 指定用户主目录，或按 Enter 选择默认目录。默认目录为 /export/home。

如果用户名为 esecadm，则相应的主目录为 /export/home/esecadm。

12 如果您在步骤 10 中选择了默认用户名，则请为用户指定以 esecadm 用户身份登录的口令。否则，请在步骤 10 中创建的用户设置口令。

13 请指定下列信息：

- ◆ **讯息总线端口：**通讯服务器正在侦听的端口。直接连接到通讯服务器的组件将使用此端口。默认的端口号是 61616。
- ◆ **Sentinel 控制中心代理端口：**SSL 代理服务器（数据访问服务器代理）侦听以接受用户名和口令的端口。SSL 代理服务器将基于经过鉴定的连接来接受身份凭证。Sentinel 控制中心使用此端口以连接到 Sentinel 服务器。默认端口号是 10013。
- ◆ **通讯服务器主机名：**安装了 Sentinel Rapid Deployment 服务器的计算机 IP 地址或主机名。

确保端口号与 Sentinel Rapid Deployment 服务器上的端口号（位于 <安装目录>/config/configuration.xml）一样，以便能进行通讯。请记住这些端口，以便将来在其他计算机上进行安装。有关端口号的详细信息，请参见第 3.3.2 节“Sentinel Rapid Deployment 客户端组件的端口号”（第 30 页）。

14 单击 **下一步**。

此时将显示安装摘要。

15 单击 **安装**。

16 单击 **完成** 以完成安装。

注释：再次登录时，请使用您在步骤 10 中指定的用户名。

如果忘记了设置的用户名，请打开终端控制台，并以根用户身份输入以下命令：

env | grep ESEC_USER

如果已经创建了用户并设置了环境变量，此命令将会返回用户名。

3.3.4 在 SLES 或 Windows 上安装 Sentinel 收集器管理器

Sentinel Rapid Deployment Web 界面的“应用程序”页中提供了可供您下载的 Sentinel 收集器管理器安装程序。要安装收集器管理器：

- 1 浏览至存放下载的收集器管理器安装程序的文件夹。
- 2 从文件中解压缩安装脚本：

平台	操作
Windows	解压缩 scm_installer.zip 文件。 文件将被解压缩到一个名称为 disk1 的目录中。
Linux	使用根权限运行以下命令： <pre>unzip scm_installer.zip</pre> 文件将被解压缩到一个名称为 disk1 的目录中。

- 3 转到 disk1 目录，然后开始安装：

平台	操作
Windows	运行以下命令： <pre>disk1\setup.bat</pre>
Linux	<ul style="list-style-type: none">◆ GUI 模式： <安装目录>/disk1/setup.sh◆ 控制台模式： <install_directory>/disk1/setup.sh -console

- 4 选择一种语言以继续进行安装。
- 5 阅读“欢迎”屏幕，然后单击 **下一步**。
- 6 阅读并接受“最终用户许可协议”。单击 **下一步**。
- 7 接受默认的安装目录或单击 **浏览**指定安装位置，然后单击 **下一步**。

重要：不能安装到名称中使用了特殊字符或非 ASCII 字符的目录。例如，在 Windows x86-64 上安装 Sentinel 时，默认路径是 C:\Program Files (x86)。如果要继续安装，您必须更改该默认路径以免使用特殊字符，例如 (x86) 中的括号。

- 8 指定 Sentinel 管理员用户名和相应的主目录路径。

如果已经安装了任何 Sentinel 应用程序，该选项将不可用。

- ◆ **OS Sentinel 管理员用户名：**默认为 esecadm。
这是拥有所安装的 Sentinel 产品的用户的用户名。如果此用户尚不存在，将创建此用户，并在指定的目录中创建相应的主目录。
- ◆ **OS Sentinel 管理员用户主目录：**默认值是 /export/home。如果 esecadm 是用户名，那么相应的主目录是 /export/home/esecadm。

要以 `esecadm` 用户身份登录，您需要先设置其口令。

9 请指定下列信息：

- ◆ **讯息总线端口：** 通讯服务器正在侦听的端口。直接连接到通讯服务器的组件将使用此端口。默认的端口号是 `61616`。
- ◆ **通讯服务器主机名：** 安装了 Sentinel Rapid Deployment 服务器的计算机 IP 或主机名。

确保 Sentinel 系统中每个计算机上的端口号为同一个才可以通讯。请记住这些端口，以便将来在其他计算机上进行安装。

10 单击 *下一步*。

11 请指定下列信息：

- ◆ **自动内存配置：** 选择要分配给收集器管理器的总内存大小。安装程序将根据估计的操作系统和数据库开销来自动确定组件之间的最优内存分配。

重要： 您可以修改 `configuration.xml` 文件中的 `-Xmx` 值，以更改变分配给收集器管理器进程的 RAM。`configuration.xml` 文件位于 Linux 上的 `<安装目录>/config`，或 Windows 上的 `<安装目录>\config`。

- ◆ **自定义内存配置：** 单击 *配置* 调整内存分配。只有在计算机上有足够内存，此选项才可用。

12 单击 *下一步*。

此时将会显示摘要屏幕，其中显示了选定要安装的功能。

13 单击 *安装*。

14 安装完成后，系统将提示您输入 ActiveMQ JMS 策略使用的用户名和口令来连接到中介程序。

请使用用户名 `collectormanager` 及相应口令，该口令可在 Sentinel 服务器上的 `<安装目录>/config/activemqusers.properties` 文件中找到。

`activemqusers.properties` 文件中提供的身份凭证示例如下：

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

`collectormanager` 为用户名，`cefc76062c58e2835aa3d777778f9295` 为相应口令。

在安装收集器管理器服务时，必须使用 `collectormanager` 用户及其相应的口令。在这种情况下，`collectormanager` 用户仅对进行收集器管理器操作所需要的通讯通道具有访问权限。

安装完成后，系统将提示您进行重引导或重新登录并手动启动 Sentinel 服务。

15 单击 *完成* 重引导系统。

16 使用您在 **步骤 8** 中指定的用户名重新登录。

如果忘记了该用户名，请打开终端控制台并使用根身份凭证输入以下命令。

```
env | grep ESEC_USER
```

如果已经创建了用户并设置了环境变量，此命令将会返回用户名。

注释： 在 Windows 2008 平台上安装的收集器管理器以及映像的收集器管理器都存在一些问题。有关如何对这些问题进行查错的信息，请参见 [附录 B “疑难解答提示”](#)（第 79 页）。

3.4 手动启动和停止 Sentinel 服务

要手动启动 Sentinel 服务，请使用以下任意命令：

平台	命令
Linux	<code><install_directory>/bin/sentinel.sh start</code>
Windows	<code><install_directory>/bin/sentinel.bat start</code>

要手动停止 Sentinel 服务，请使用以下任意命令：

平台	命令
Linux	<code><install_directory>/bin/sentinel.sh stop</code>
Windows	<code><install_directory>/bin/sentinel.bat stop</code>

您还可以使用以下命令来启动或停止 Sentinel 服务。

```
/etc/init.d/sentinel.sh stop|start
```

3.5 手动升级 Java

Java 版本 1.6.0_24 与 Sentinel Rapid Deployment 服务器安装程序捆绑在一起，安装 Sentinel Rapid Deployment 服务器会同时安装该 Java 版本。但是，如果在服务器上将 Java 升级到最新版本，则需要执行下列步骤才能让 Sentinel Rapid Deployment 使用该最新版本：

- 1 根据安装 Sentinel Rapid Deployment 服务器的操作系统下载相应的 jre 分发版。
执行升级的用户必须对 Sentinel Rapid Deployment 安装目录以及将用于存放下载的升级文件的目录具有写访问权限。
 - 如果 Sentinel Rapid Deployment 安装在 SUSE Linux Enterprise Server 上，请从 [Java 下载站点 \(http://www.java.com/en/download/manual.jsp\)](http://www.java.com/en/download/manual.jsp) 下载 32 位和 64 位两种 jre 分发版。

- 2 将 Sentinel Rapid Deployment 安装目录中的 jre 和 jre64 文件夹分别重命名为 jre_old 和 jre64_old。

```
cd <install_path>/sentinel_rd  
mv jre jre_old  
mv jre64 jre64_old
```

注释：之所以进行重命名，是因为在 Java 升级无法正常进行时，可以还原到原先的版本。如果 Java 在升级后能够正常工作，您便可删除重命名的文件夹。

- 3 提取下载的 jre 分发版。
- 4 将 32 位文件夹重命名为 jre，将 64 位目录重命名为 jre64。
- 5 将重命名的 jre 和 jre64 文件夹复制到 Sentinel Rapid Deployment 的安装目录。

```
copy jre <install_path>/sentinel_rd/  
copy jre64 <install_path>/sentinel_rd/
```

- 6（视情况而定）确保已为运行 Sentinel Rapid Deployment 服务器的用户设置了对 jre 和 jre64 文件夹的必要所有权和许可权限。
- 7 依次重新启动 Sentinel Rapid Deployment 服务器和浏览器，然后检查 Java 是否已正确安装。

3.6 安装后配置

本章节帮助您了解 Sentinel Rapid Deployment 服务的安装后配置。

- ◆ 第 3.6.1 节“更改日期和时间设置”（第 36 页）
- ◆ 第 3.6.2 节“将 SMTP 集成器配置为发送 Sentinel 通知”（第 36 页）
- ◆ 第 3.6.3 节“收集器管理器服务”（第 37 页）
- ◆ 第 3.6.4 节“管理时间”（第 37 页）

3.6.1 更改日期和时间设置

Sentinel 控制中心内的默认日期和时间格式都可被覆盖。有关自定义日期和时间格式以使其符合您当地时区的详细信息，请参见 [Java 网站 \(http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html\)](http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html)。

- 1 编辑 SentinelPreferences.properties 文件。

```
<install_directory>/config/SentinelPreferences.properties
```

- 2 去除以下行中的注释，并为 Sentinel 控制中心的事件日期 / 时间字段自定义日期和时间格式：

```
com.eSecurity.Sentinel.event.datetimetypeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
```

3.6.2 将 SMTP 集成器配置为发送 Sentinel 通知

在 Sentinel Rapid Deployment 中，将 JavaScript SendEmail 操作与 SMTP 集成器结合使用可在 Sentinel 界面的各种环境中将邮件讯息发送给收件人。SMTP 集成器必须配置为采用有效的连接信息才能正常工作。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[发送电子邮件](#)”。

每个 Sentinel 安装中都会自动创建 SendEmail 操作插件的单个操作实例。除了需在操作参数中配置邮件讯息收件人和邮件内容之外，SendEmail 操作无需进行配置。

在下列情况下，Sentinel 会在内部触发该 SendEmail 操作以发送邮件：

- ◆ 当生成关联规则时，SendEmail 操作会被触发。此 SendEmail 操作是齿轮图标表示的操作，只对关联（与 JS JavaScript 图标表示的 JavaScript SendEmail 操作相对）有效。
- ◆ 当工作流程包含配置为发送电子邮件的邮件步骤或活动时。
- ◆ 用户打开某个事件并选择执行配置为发送电子邮件的活动时。
- ◆ 用户右键单击某个事件并选择 *电子邮件* 时。
- ◆ 用户打开某个事件并选择 *电子邮件事件* 时。

3.6.3 收集器管理器服务

- ◆ [安装更多收集器管理器](#)（第 37 页）
- ◆ [使用一般收集器](#)（第 37 页）

安装更多收集器管理器

收集器管理器可管理所有数据收集进程和数据分析。有时，可能必须将其他 Sentinel 收集器管理器节点添加到 Sentinel 环境中，才能在各台计算机之间实现负载平衡。远程收集器管理器具有以下几项优点：

- ◆ 提供分布式的事件分析和处理，可提高系统性能。
- ◆ 通过与事件源的搭配在源系统上进行过滤、加密和数据压缩。如此可降低网络带宽要求，提供附加的数据安全性。
- ◆ 可在更多操作系统上进行安装。例如，可在 Microsoft Windows 上安装收集器管理器节点，以使用 WMI 协议进行数据收集。
- ◆ 提供文件超速缓存，使远程收集器管理器可以在服务器暂时忙于存档或处理大量事件时超速缓存大量的数据。对于本身并不支持事件超速缓存的协议（如 syslog）而言，这是一种优势。

可以通过在其他计算机上安装“收集器管理器”组件的实例来对这些组件进行负载平衡。您可以在新计算机上运行安装程序，安装更多的收集器管理器。有关安装收集器管理器的详细信息，请参见第 3.3.4 节“[在 SLES 或 Windows 上安装 Sentinel 收集器管理器](#)”（第 33 页）。

使用一般收集器

在安装 Sentinel Rapid Deployment 的过程中，将会配置一个名为“一般收集器”的收集器。默认情况下，它会以每秒 5 个事件 (eps) 的速率创建事件。

如果您希望为系统配备更多收集器，可以从 [Novell 网站 \(http://support.novell.com/products/sentinel/collectors.html\)](http://support.novell.com/products/sentinel/collectors.html) 下载。

3.6.4 管理时间

必须将 Sentinel 服务器连接到 NTP（网络时间协议）服务器或其他类型的时间服务器。如果计算机之间的系统时间未同步，则 Sentinel 关联引擎和活动视图将无法正常工作。系统不会将来自收集器管理器的事件视作实时事件，因此不会避开 Sentinel 控制中心和关联引擎而将其直接发送到 Sentinel 数据库。

默认情况下，实时数据的阈值是 120 秒。该阈值可通过更改 event-router.properties 文件中 esecurity.router.event.realtime.expiration 的值来修改。Sentinel 事件时间根据“信任设备时间”或“收集器管理器时间”来填充。当配置收集器时，可以选择“信任设备时间”。“信任设备时间”是设备生成日志的时间，而“收集器管理器时间”是“收集器管理器”系统的本地系统时间。

3.7 LDAP 鉴定

除了数据库鉴定外，Sentinel Rapid Deployment 还支持 LDAP 鉴定。通过将 Sentinel Rapid Deployment 服务器配置为使用 LDAP 鉴定，可让用户使用其 Novell eDirectory 或 Microsoft Active Directory 身份凭证登录到 Sentinel Rapid Deployment。

- ◆ 第 3.7.1 节“概述”（第 38 页）
- ◆ 第 3.7.2 节“先决条件”（第 38 页）
- ◆ 第 3.7.3 节“配置 Sentinel 服务器以进行 LDAP 鉴定”（第 39 页）
- ◆ 第 3.7.4 节“配置多个 LDAP 服务器以实现故障转移”（第 41 页）
- ◆ 第 3.7.5 节“为多个 Active Directory 域配置 LDAP 鉴定”（第 43 页）
- ◆ 第 3.7.6 节“使用 LDAP 用户身份凭证进行登录”（第 44 页）

3.7.1 概述

您可以将 Sentinel Rapid Deployment 服务器配置为通过安全 SSL 连接进行 LDAP 鉴定，既可使用 LDAP 目录匿名搜索，也可以不使用。

注释：如果 LDAP 目录禁用匿名搜索，则请勿将 Sentinel Rapid Deployment 服务器配置为使用匿名搜索。

- ◆ **匿名搜索：**在创建 Sentinel Rapid Deployment LDAP 用户帐户时，您必须指定目录用户名，但无需指定用户判别名 (DN)。

当 LDAP 用户登录 Sentinel Rapid Deployment 时，Sentinel Rapid Deployment 服务器会根据指定的用户名在 LDAP 目录中执行匿名搜索，以寻找相应的 DN，然后使用该 DN 来针对 LDAP 目录鉴定用户登录。

- ◆ **非匿名搜索：**在创建 Sentinel Rapid Deployment LDAP 用户帐户时，您必须同时指定目录用户名和用户 DN。

当 LDAP 用户登录 Sentinel Rapid Deployment 时，Sentinel Rapid Deployment 服务器会使用指定的用户 DN 针对 LDAP 目录鉴定用户登录，并不会在 LDAP 目录中执行任何匿名搜索。

另外，还有一种只适用于 Active Directory 的方法。有关详细信息，请参见使用 Active Directory 中的 UserPrincipalName 属性进行非匿名 LDAP 鉴定。

3.7.2 先决条件

- ◆ 导出 LDAP 服务器 CA 证书（第 38 页）
- ◆ 启用 LDAP 目录匿名搜索（第 39 页）

导出 LDAP 服务器 CA 证书

与 LDAP 服务器之间的安全 SSL 连接需要 LDAP 服务器 CA 证书，您必须将该证书导出为采用 Base64 编码的文件。

- ◆ **eDirectory：**请参见导出企业 CA 自我签名证书 (<http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html>)。

要导出 iManager 中的 eDirectory CA 证书，必须安装适用于 iManager 的 Novell Certificate Server 插件。

- ◆ **Active Directory:** 请参见[如何启用 SSL 上的 LDAP 与第三方证书颁发机构 \(http://support.microsoft.com/kb/321051\)](http://support.microsoft.com/kb/321051)。

启用 LDAP 目录匿名搜索

要使用匿名搜索来执行 LDAP 鉴定，您必须启用 LDAP 目录匿名搜索。默认情况下，eDirectory 中会启用匿名搜索，Active Directory 中则会禁用。

要启用 LDAP 目录匿名搜索，请参考以下信息进行操作：

- ◆ **eDirectory:** 请参见“[LDAP 服务器 象属性 \(http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html\)](http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html)”一节中的 ldapBindRestrictions。
- ◆ **Active Directory:** ANONYMOUS LOGON 用户对象必须拥有适当的列出内容许可权限以及对 sAMAccountName 和 objectclass 属性的读取权限。有关详细信息，请参见[如何配置为允许匿名查询 Active Directory \(http://support.microsoft.com/kb/320528\)](http://support.microsoft.com/kb/320528)。

对于 Windows Server 2003，您必须执行额外配置。有关详细信息，请参见在[Windows Server 2003 上配置 Active Directory \(http://support.microsoft.com/kb/326690/en-us\)](http://support.microsoft.com/kb/326690/en-us)。

3.7.3 配置 Sentinel 服务器以进行 LDAP 鉴定

1 请确保您已满足第 3.7.2 节“先决条件”（第 38 页）中所述的先决条件。

2 以根用户身份登录 Sentinel Rapid Deployment 服务器。

3 将导出的 LDAP 服务器 CA 证书文件复制到 <安装目录>/config 目录。

4 以如下所示的方式设置证书文件的所有权和许可权限：

```
chown novell:novell <安装目录>/config/<证书文件>
```

```
chmod 700 <安装目录>/config/<证书文件>
```

5 切换为 novell 用户：

```
su - novell
```

6 切换到 <安装目录>/bin 目录。

7 运行 LDAP 鉴定配置脚本：

```
./ldap_auth_config.sh
```

该脚本会先对 config 目录中的 auth.login 和 configuration.xml 这两个配置文件进行备份，将它们分别保存为 auth.login.sav 和 configuration.xml.sav，然后才会对原文件进行修改以进行 LDAP 鉴定。

8 请指定下列信息：

按 Enter 接受默认值，或指定一个新值以覆盖默认值。

- ◆ **Sentinel 安装位置:** Sentinel 服务器上的安装目录。
- ◆ **LDAP 服务器主机名或 IP 地址:** 安装了 LDAP 服务器的计算机的主机名或 IP 地址。默认值为 localhost。但是，您不可将 LDAP 服务器安装在与 Sentinel 服务器相同的计算机上。
- ◆ **LDAP 服务器端口:** 安全 LDAP 连接的端口号。默认端口号是 636。
- ◆ **LDAP 目录匿名搜索:** 要执行匿名搜索，请指定 y。否则请指定 n。默认值为 y。

如果指定 n，请完成 LDAP 配置，并执行[不执行匿名搜索的 LDAP 鉴定（第 40 页）](#)一节中所述的步骤。

- ◆ **使用的 LDAP 目录：** 只有当您为匿名搜索指定了“y”时，此参数才会显示。请指定 1 以使用 Novell eDirectory，或指定 2 以使用 Active Directory。默认值是 1。
- ◆ **要在其中搜索用户的 LDAP 子树：** 只有当您为匿名搜索指定了“y”时，此参数才会显示。该子树即用户对象所在目录中的子树。以下是一些指定 eDirectory 和 Active Directory 子树的示例：

- ◆ eDirectory:
ou=users,o=novell

注释： 对于 eDirectory，如果未指定子树，则将在整个目录中进行搜索。

- ◆ Active Directory:
CN=users,DC=TESTAD,DC=provo, DC=novell,DC=com

注释： 对于 Active Directory，子树不能为空。

- ◆ **LDAP 服务器证书的文件名：** 您在[步骤 3](#)中复制的 eDirectory/Active Directory CA 证书的文件名。

9 输入以下内容之一：

- ◆ y: 接受所输入的值
- ◆ n: 输入新值
- ◆ q: 退出配置

成功完成配置后：

- ◆ LDAP 服务器证书会被添加到位于 <安装目录>/config/ldap_server.keystore 的密钥存储区。
- ◆ <安装目录>/config 目录中的 auth.login 和 configuration.xml 配置文件会得到更新，以启用 LDAP 鉴定。

10 输入 y 以重新启动 Sentinel 服务。

重要： 如果出现任何错误，请还原对 config 目录中的 auth.login 和 configuration.xml 配置文件所做的更改：

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

11（视情况而定）如果为[LDAP 目录匿名搜索](#)：指定了 n，请继续[不执行匿名搜索的 LDAP 鉴定（第 40 页）](#)。

不执行匿名搜索的 LDAP 鉴定

在配置 Sentinel Rapid Deployment 以进行 LDAP 鉴定时，如果您针对 LDAP 目录匿名搜索选择了“n”，则 LDAP 鉴定将不会执行匿名搜索。

如果使用 Sentinel 控制中心创建 LDAP 用户帐户，请务必为非匿名 LDAP 鉴定指定 *LDAP 用户 DN*。对 eDirectory 和 Active Directory 都可使用此方法。

有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[为 Sentinel 创建 LDAP 用户帐户](#)”。

此外，对于 Active Directory，有一种备选的方法可以执行无需匿名搜索的 LDAP 鉴定。有关详细信息，请参见[使用 Active Directory 中的 UserPrincipalName 属性进行非匿名 LDAP 鉴定](#)。

使用 Active Directory 中的 UserPrincipalName 属性进行非匿名 LDAP 鉴定

对于 Active Directory，您还可以使用 userPrincipalName 属性执行无需匿名搜索的 LDAP 鉴定：

- 1 请确保针对 Active Directory 用户将 userPrincipalName 属性设置为 `<sAMAccountName@domain>`。

有关详细信息，请参见 [User-Principal-Name 属性 \(http://msdn.microsoft.com/en-us/library/ms680857\(VS.85\).aspx\)](http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx)。

- 2 请确保您执行了步骤 1（第 39 页）到步骤 10（第 40 页），并为 LDAP 目录匿名搜索（第 39 页）指定了 n。
- 3 在 Sentinel 服务器上，编辑 `<安装目录>/config/auth.login` 文件中的 LdapLogin 部分：

```
LdapLogin {
  com.sun.security.auth.module.LdapLoginModule required
  userProvider="ldap://LDAP server IP:636/DN of the Container that contains
the user objects"
  authIdentity="{USERNAME}@Domain Name"
  userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
  useSSL=true;
};
```

例如：

```
LdapLogin {
  com.sun.security.auth.module.LdapLoginModule required
  userProvider="ldap://137.65.151.12:636/DC=Test-
AD,DC=provo,DC=novell,DC=com"
  authIdentity="{USERNAME}@Test-AD.provo.novell.com"
  userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
  useSSL=true;
};
```

- 4 重新启动 Sentinel 服务：

```
/etc/init.d/sentinel stop
/etc/init.d/sentinel start
```

3.7.4 配置多个 LDAP 服务器以实现故障转移

要将一个或多个 LDAP 服务器配置为 LDAP 鉴定的故障转移服务器：

- 1 确保您执行了步骤 2（第 39 页）到步骤 10（第 40 页），将 Sentinel 服务器配置为针对 LDAP 主服务器进行 LDAP 鉴定。
- 2 以 novell 用户身份登录 Sentinel 服务器。
- 3 停止 Sentinel 服务。

```
/etc/init.d/sentinel stop
```

- 4 切换到 `<安装目录>/config` 目录：

```
cd <install_directory>/config
```

- 5 打开 auth.login 文件进行编辑。

```
vi auth.login
```

- 更新 LdapLogin 部分中的 userProvider，指定多个 LDAP URL。请以空格分隔各个 URL。
例如：

```
userProvider="ldap://ldap-url1 ldap://ldap-url2"
```

对于 Active Directory，请确保 LDAP URL 中的子树不为空。

有关指定多个 LDAP URL 的详细信息，请参见类 LdapLogin 模块 (<http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html>) 中对 userProvider 选项的说明。

- 保存更改。
- 导出各 LDAP 故障转移服务器的证书，并将证书文件复制到 Sentinel 服务器上的 <安装目录>/config 目录。

有关详细信息，请参见导出 LDAP 服务器 CA 证书（第 38 页）。

- 确保您针对各 LDAP 故障转移服务器的证书文件设置了所需的所有权和许可权限。

```
chown novell:novell <install_directory>/config/<cert-file>
```

```
chmod 700 <install_directory>/config/<cert-file>
```

- 将各 LDAP 故障转移服务器证书添加到配置 Sentinel 服务器以进行 LDAP 鉴定（第 39 页）一节中步骤 8 创建的 ldap_server.keystore 密钥存储区。

```
<install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts  
-file <certificate-file> -alias <alias_name> -keystore  
ldap_server.keystore -storepass sentinel
```

将 <certificate-file> 替换为 Base64 编码格式的 LDAP 证书文件名，并将 <alias_name> 替换为要导入的证书的别名。

重要：请确保您指定了别名。如果未指定别名，密钥工具将默认采用 mykey 作为别名。在将多个证书导入密钥存储区而未指定别名时，密钥工具将报错，告知您该别名已经存在。

- 启动 Sentinel 服务。

```
/etc/init.d/sentinel start
```

如果 Sentinel 服务器在发现 LDAP 主服务器停机之前就已超时，则服务可能不会连接到 LDAP 故障转移服务器。为确保 Sentinel 服务器可连接到 LDAP 故障转移服务器而不会发生超时：

- 以根用户身份登录 Sentinel 服务器。
- 打开 sysctl.conf 文件进行编辑：

```
vi /etc/sysctl.conf
```
- 确保 net.ipv4.tcp_syn_retries 的值设置为 3。如果该条目不存在，请添加条目。保存文件：

```
net.ipv4.tcp_syn_retries = 3
```
- 执行命令以使所做更改生效：

```
/sbin/sysctl -p  
/sbin/sysctl -w net.ipv4.route.flush=1
```
- 在 <安装目录>/bin 目录的 control_center.sh 和 solution_designer.sh 中添加 -Desecurity.remote.timeout=60 参数，以设置 Sentinel 服务器超时值：

control_center.sh:

```
"<install_directory>/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="<install_directory>/data/
control_center.cache" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
control_center_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
Desecurity.remote.timeout=60 -jar ../lib/console.jar
```

solution_designer.sh:

```
"<install_directory>/jre/bin/java" -classpath $LOCAL_CLASSPATH $MEMORY -
Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="<install_directory>/lib/
contentinstaller.jar" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -Desecurity.cache.directory=../
data/solution_designer.cache -Desecurity.remote.timeout=60
com.esecurity.content.exportUI.ContentPackBuilder
```

3.7.5 为多个 Active Directory 域配置 LDAP 鉴定

如果要鉴定的 LDAP 用户位于多个 Active Directory 域中，您可以按如下所述针对 LDAP 鉴定配置 Sentinel Rapid Deployment 服务器：

- 1 确保遵照步骤 2（第 39 页）至步骤 10（第 40 页），将 Sentinel 服务器配置为针对第一个域的 Active Directory 域控制器进行 LDAP 鉴定。另请确保为 [LDAP 目录匿名搜索](#)（第 39 页）指定了 n。
- 2 以 novell 用户身份登录 Sentinel 服务器。
- 3 停止 Sentinel 服务。
/etc/init.d/sentinel stop
- 4 切换到 <安装目录>/config 目录：
cd <install_directory>/config
- 5 打开 auth.login 文件进行编辑。
vi auth.login
- 6 编辑 LdapLogin 部分以指定多个 LDAP URL，并使用空格分隔每个 URL。

例如：

```
LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    userProvider="ldap://<IP of the domain 1 domain controller>:636
ldap://<IP of the domain 2 domain controller>:636"
    authIdentity="{USERNAME}"
    useSSL=true;
};
```

有关指定多个 LDAP URL 的详细信息，请参见类 `LdapLogin` 模块 (<http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html>) 中对 `userProvider` 选项的说明。

7 保存更改。

8 导出每个域的域控制器证书，并将证书文件复制到 Sentinel 服务器上的 `<安装目录>/config` 目录。

有关详细信息，请参见[导出 LDAP 服务器 CA 证书](#)（第 38 页）。

9 确保您设置了证书文件的必要所有权和许可权限。

```
chown novell:novell <install_directory>/config/<cert-file>
chmod 700 <install_directory>/config/<cert-file>
```

10 将各证书添加到[配置 Sentinel 服务器以进行 LDAP 鉴定](#)（第 39 页）一节中[步骤 8](#)创建的 `ldap_server.keystore` 密钥存储区。

```
<install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
-file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

将 `<certificate-file>` 替换为 Base64 编码格式的 LDAP 证书文件名，并将 `<alias_name>` 替换为要导入的证书的别名。

重要：请确保您指定了别名。如果未指定别名，密钥工具将默认采用 `mykey` 作为别名。在将多个证书导入密钥存储区而未指定别名时，密钥工具将报错，告知您该别名已经存在。

11 启动 Sentinel 服务。

```
/etc/init.d/sentinel start
```

3.7.6 使用 LDAP 用户身份凭证进行登录

成功将 Sentinel 服务器配置为使用 LDAP 鉴定后，您可以在 Sentinel 控制中心内创建 Sentinel LDAP 用户帐户。有关创建 LDAP 用户帐户的详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[为 Sentinel 创建 LDAP 用户帐户](#)”。

创建 LDAP 用户帐户后，您便可以使用自己的 LDAP 用户名和口令登录到 Sentinel Rapid Deployment Web 用户界面、Sentinel 控制中心和 Sentinel 解决方案设计器。

注释：要修改现有 LDAP 配置，请重新运行 `ldap_auth_config` 脚本，为各个参数指定新的值。

3.8 将许可证密钥从评估密钥升级到产品密钥

如果在评估之后购买了产品，请按照下述过程来更新许可证密钥，以避免重新安装：

- 1 以 Sentinel 管理员操作系统用户（默认用户为 `novell`）身份登录安装了 Sentinel Rapid Deployment 的计算机。
- 2 在命令提示符处，将目录切换到 `<安装目录>/bin`。
- 3 输入下面的命令：

```
./softwarekey.sh
```
- 4 指定 1 以设置主密钥。按 `Enter`。
- 5 输入新的有效许可证密钥，并在更新许可证密钥后按照屏幕指导退出。

升级 Sentinel Rapid Deployment

4

本章节提供将 Sentinel Rapid Deployment 现有版本升级到最新增补程序的相关信息。

注释：此增补程序只适用于 Sentinel Rapid Deployment 的 64 位安装版本。将此增补程序应用于 32 位演示系统将导致安装失效。

- ◆ 第 4.1 节“先决条件”（第 45 页）
- ◆ 第 4.2 节“在服务器上安装增补程序”（第 45 页）
- ◆ 第 4.3 节“升级收集器管理器和客户端应用程序”（第 46 页）

4.1 先决条件

- ◆ 确保您要升级的系统已经安装了 Sentinel 6.1 Rapid Deployment SP1。
- ◆ 确认启用了 Sentinel 数据管理器作业，以确保当前的联机分区不会达到 P_MAX。如果达到 P_MAX，并且您是手动添加的分区，则 Sentinel 控制中心将无法成功启动。

4.2 在服务器上安装增补程序

- 1 以 novell 用户身份登录要安装增补程序的服务器。

安装增补程序之前，务必使用以下命令对 Sentinel 数据库、配置文件夹和数据文件夹进行备份：

Sentinel 数据库：

```
tar -cf backup.tar <install_directory>/3rdparty/postgresql/database_files
tar -cf backupdata.tar <install_directory>/3rdparty/postgresql/data
```

配置文件夹：

```
tar -cf backupconfig.tar <install_directory>/config
```

数据文件夹：

```
tar -cf backupdata.tar <install_directory>/data
```

有关这些命令的详细信息，请参见 PostgreSQL 网站上的[文件系统级备份 \(http://www.postgresql.org/docs/8.1/static/backup-file.html\)](http://www.postgresql.org/docs/8.1/static/backup-file.html)。

- 2 备份事件源管理 (ESM) 配置并创建 ESM 导出文件。

有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[导出配置](#)”。

- 3 从 [Novell 增补程序查找器 \(http://download.novell.com/patch/finder/\)](http://download.novell.com/patch/finder/) 下载 Sentinel Rapid Deployment 的增补程序安装程序。

- 4 将下载的安装程序包复制到临时目录。

- 5 停止 Sentinel 服务：

```
sentinel.sh stop
```

- 6 指定以下命令以提取安装程序包中的文件：

```
unzip <install_filename>
```

将 <install_filename> 替换为安装程序文件的实际名称。

7 切换到提取后的安装程序文件所在的目录：

```
cd <directory_name>
```

将 *<directory_name>* 替换为提取后的文件所在目录的实际名称。

8 指定以下命令以在服务器上安装增补程序，然后遵照屏幕指导进行操作：

```
./service_pack.sh
```

安装完成后，Sentinel 服务将自动启动。

9 在运行收集器管理器和 / 或客户端应用程序的所有计算机上应用增补程序。

4.3 升级收集器管理器和客户端应用程序

- ◆ 第 4.3.1 节“升级收集器管理器”（第 46 页）
- ◆ 第 4.3.2 节“升级客户端应用程序”（第 47 页）

4.3.1 升级收集器管理器

- ◆ Linux（第 46 页）
- ◆ Windows（第 46 页）

Linux

1 以根用户身份登录 Sentinel Rapid Deployment 收集器管理器所在的计算机。

2 从 Novell 增补程序查找器 (<http://download.novell.com/patch/finder/>) 下载 Sentinel Rapid Deployment 的增补程序安装程序。

3 将下载的安装程序文件复制到临时目录。

4 指定以下命令以提取安装程序 ZIP 包中的文件：

```
unzip <install_filename>
```

使用安装文件实际名称替换 *<install_filename>*。

5 切换到提取后的安装程序文件所在的目录：

```
cd <directory_name>
```

将 *<directory_name>* 替换为提取后的安装程序文件所在目录的实际名称。

6 停止收集器管理器服务。

```
<install_directory>/bin/sentinel.sh stop
```

7 运行服务包安装程序，然后遵照屏幕指导进行操作：

```
./service_pack.sh
```

安装完成后，收集器管理器服务将自动启动。

Windows

1 以管理员用户身份登录 Sentinel Rapid Deployment 收集器管理器所在的计算机。

2 从 Novell 增补程序查找器 (<http://download.novell.com/patch/finder/>) 下载 Sentinel Rapid Deployment 的增补程序安装程序。

3 将安装程序文件复制到临时目录。

4 提取安装程序包中的文件。

5 停止收集器管理器服务。

```
<install_directory>\bin\sentinel.bat stop
```

6 浏览至提取后的安装程序文件所在的目录。

7 按以下方式之一运行安装程序：

- ◆ 双击 service_pack.bat 文件，然后遵照屏幕指导进行操作。
- ◆ 在命令提示符处，运行 service_pack.bat 文件，然后遵照屏幕指导进行操作。

安装完成后，收集器管理器服务将自动启动。

4.3.2 升级客户端应用程序

- ◆ [Linux](#)（第 47 页）
- ◆ [Windows](#)（第 47 页）

Linux

1 以根用户身份登录运行 Novell Sentinel Rapid Deployment 客户端应用程序的计算机。

2 从 [Novell 增补程序查找器](http://download.novell.com/patch/finder/) (<http://download.novell.com/patch/finder/>) 下载 Sentinel Rapid Deployment 的增补程序安装程序。

3 将下载的安装程序包复制到临时目录。

4 指定以下命令以提取安装程序包中的文件：

```
unzip <install_filename>
```

使用安装文件实际名称替换 *<install_filename>*。

5 切换到提取后的安装程序文件所在的目录：

```
cd <directory_name>
```

将 *<directory_name>* 替换为提取后的文件所在目录的实际名称。

6 运行安装程序，然后遵照屏幕指导进行操作：

```
./service_pack.sh
```

Windows

1 以管理员身份登录运行 Novell Sentinel Rapid Deployment 客户端应用程序的计算机。

2 从 [Novell 增补程序查找器](http://download.novell.com/patch/finder/) (<http://download.novell.com/patch/finder/>) 下载 Sentinel Rapid Deployment 的增补程序安装程序。

3 将下载的安装程序文件复制到临时目录。

4 提取安装程序包中的文件。

5 浏览至提取后的安装程序文件所在的目录。

6 按以下方式之一运行安装程序：

- ◆ 双击 service_pack.bat 文件，然后遵照屏幕指导进行操作。
- ◆ 在命令提示符处，运行 service_pack.bat 文件，然后遵照屏幕指导进行操作。

Sentinel Rapid Deployment 安全注 意事项

5

本章节提供有关如何安全地安装、配置和维护 Novell Sentinel Rapid Deployment 的详细说明。

- ◆ 第 5.1 节“强化”（第 49 页）
- ◆ 第 5.2 节“在网络中保证通讯安全”（第 50 页）
- ◆ 第 5.3 节“保护用户和口令”（第 52 页）
- ◆ 第 5.4 节“保护 Sentinel 数据”（第 53 页）
- ◆ 第 5.5 节“备份信息”（第 56 页）
- ◆ 第 5.6 节“保护操作系统的安全”（第 57 页）
- ◆ 第 5.7 节“查看 Sentinel 审计事件”（第 57 页）
- ◆ 第 5.8 节“使用 CA 证书”（第 58 页）

5.1 强化

- ◆ 第 5.1.1 节“开箱即用强化”（第 49 页）
- ◆ 第 5.1.2 节“确保 Sentinel Rapid Deployment 数据安全”（第 49 页）

5.1.1 开箱即用强化

- ◆ 所有不必要的端口都已关闭。
- ◆ 在可能的情况下，服务端口只会侦听本地连接，不允许进行远程连接。
- ◆ 安装文件时只设置了最基本的特权，因此只有少数用户可以读取文件。
- ◆ 不允许使用默认口令。
- ◆ 运行数据库报告时使用只对数据库拥有选定许可权限的用户身份。
- ◆ 所有 Web 接口都需要使用 HTTPS。
- ◆ 已针对应用程序运行漏洞扫描，并且所有潜在安全问题都已解决。
- ◆ 所有网络通讯默认都使用 SSL，并针对鉴定进行了相应配置。
- ◆ 用户帐户口令在存储到文件系统或数据库中时默认都会加密。

5.1.2 确保 Sentinel Rapid Deployment 数据安全

由于 Sentinel Rapid Deployment 中数据的高度敏感性质，您必须保证计算机的物理安全，并将其放置在一个安全的网络区域中。要从安全网络之外的事件源收集数据，请使用远程连接器管理器。有关远程收集器管理器的详细信息，请参见“第 3.3 节“安装收集器管理器和客户端应用程序”（第 30 页）”。

5.2 在网络中保证通讯安全

Sentinel Rapid Deployment 中的各种组件之间通过网络进行通讯，并且系统中使用了各种通讯协议。

- ◆ 第 5.2.1 节“Sentinel 服务器进程之间的通讯”（第 50 页）
- ◆ 第 5.2.2 节“Sentinel 服务器与 Sentinel 客户端应用程序之间的通讯”（第 50 页）
- ◆ 第 5.2.3 节“服务器与数据库之间的通讯”（第 51 页）
- ◆ 第 5.2.4 节“收集器管理器与事件源之间的通讯”（第 51 页）
- ◆ 第 5.2.5 节“与 Web 浏览器之间的通讯”（第 51 页）
- ◆ 第 5.2.6 节“数据库与其他客户端之间的通讯”（第 51 页）

5.2.1 Sentinel 服务器进程之间的通讯

Sentinel 服务器进程包括 DAS Core、DAS Binary、关联引擎、收集器管理器和 Web 服务器。它们使用 ActiveMQ 互相进行通讯。

默认情况下，这些服务器进程之间的通讯使用 SSL 通过 ActiveMQ 消息总线进行。要配置 SSL，请在 <安装目录>/configuration.xml 中指定以下信息：

```
<jms brokerURL="failover://(ssl://localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
```

有关设置自定义服务器和客户端证书的详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[进程](#)”。

5.2.2 Sentinel 服务器与 Sentinel 客户端应用程序之间的通讯

Sentinel 控制中心 (SCC)、Sentinel 数据管理器 (SDM) 和解决方案设计器等 Sentinel 客户端应用程序默认通过 SSL 代理服务器使用 SSL 通讯。

要在 SCC、SDM 和解决方案设计器全部作为客户端应用程序在服务器上运行时启用 Sentinel 服务器与这些应用程序之间的通讯，请在 <安装目录>/configuration.xml 中指定以下信息：

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystategy.ProxiedClientStrategyFactory">
  <transport type="ssl">
    <ssl host="localhost" keystore="<install_directory>/config/.proxyClientKeystore" port="10013" usecacerts="false"/>
  </transport>
</strategy>
```

要启用 Sentinel 服务器与通过 WebStart 运行的 SCC、SDM 和解决方案设计器之间的通讯，需按如下方式在服务器上的 <安装目录>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml 文件中定义通讯策略：

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystategy.ProxiedCl
ientStrategyFactory" >
  <transport type="ssl">
    <ssl host="127.0.0.1" port="10013" keystore="./.novell/sentinel/
.proxyClientKeystore" />
  </transport>
</strategy>
```

有关设置自定义服务器和客户端证书的详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[进程](#)”。

5.2.3 服务器与数据库之间的通讯

服务器与数据库之间的通讯所用的协议是 JDBC 驱动程序定义的。一些驱动程序可以对数据库的通讯进行加密。

Sentinel Rapid Deployment 使用 PostgreSQL 驱动程序（在 [PostgreSQL 下载页 \(http://jdbc.postgresql.org/download.html\)](http://jdbc.postgresql.org/download.html) 提供的 postgresql-<版本>.jdbc3.jar）连接 PostgreSQL 数据库，这是一种 Java（IV 类型）实施。此驱动程序支持数据通讯加密。要配置数据通讯加密，请参见 [PostgreSQL 加密选项 \(http://www.postgresql.org/docs/8.1/static/encryption-options.html\)](http://www.postgresql.org/docs/8.1/static/encryption-options.html)。

注释：启用加密会影响系统的性能。因此，数据库通讯默认不会加密。但是，由于数据库与服务器之间的通讯是通过回写网络接口发生的，且不会曝露给开放网络，因此，不会造成安全问题。

5.2.4 收集器管理器与事件源之间的通讯

您可以对 Sentinel Rapid Deployment 进行适当配置，让其以安全方式从不同的事件源收集数据。不过，安全数据收集取决于事件源所支持的特定协议。例如，Check Point LEA、Syslog 和 Audit Connectors 适当配置后都可以对其与事件源之间的通讯进行加密。

有关可启用的安全功能的详细信息，请参见 [Novell Sentinel 插件网站 \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html) 上提供的连接器和事件源供应商文档。

5.2.5 与 Web 浏览器之间的通讯

Web 服务器默认配置为通过 HTTPS 进行通讯。有关详细信息，请参见 [Tomcat 文档 \(http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html\)](http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html)。

5.2.6 数据库与其他客户端之间的通讯

可以使用 Sentinel 数据管理器或任何第三方应用程序（如 Pgadmin）将 PostgreSQL SIEM 数据库配置为允许来自任何客户端计算机的连接。

要允许 Sentinel 数据管理器从任何客户端计算机进行连接，请在 `<安装目录>/3rdparty/postgresql/data/pg_hba.conf` 文件中添加下行：

```
host    all             all             0.0.0.0/0          md5
```

如果要限制允许运行并通过 SDM 连接到数据库的客户端连接，请使用主机 IP 地址替换上面的行。pg_hba.conf 中的下行指示 PostgreSQL 接受来自本地计算机的连接，这样 Sentinel 数据管理器仅允许在服务器上运行。

```
host all all 127.0.0.1/32 md5
```

如果要限制其他客户端计算机的连接，您可以添加其他 host 条目。

5.3 保护用户和口令

- ◆ [第 5.3.1 节“操作系统用户”](#)（第 52 页）
- ◆ [第 5.3.2 节“Sentinel 应用程序和数据库用户”](#)（第 52 页）
- ◆ [第 5.3.3 节“实施用户的口令策略”](#)（第 53 页）

5.3.1 操作系统用户

- ◆ [服务器安装](#)（第 52 页）
- ◆ [收集器管理器安装](#)（第 52 页）

服务器安装

Sentinel Rapid Deployment 服务器安装过程中会创建一个系统用户和一个拥有 <安装目录> 中所安装的文件的用户。如果该用户不存在，则将创建此用户，并将其用户主目录设置为 <安装目录>。如果创建了新用户，则默认不会为该用户设置口令，以最大限度地确保安全性。如果希望以安装过程中创建的用户身份登录系统，您必须在安装完成后为其设置一个口令。

收集器管理器安装

根据安装了收集器管理器的操作系统的不同，系统用户的安全性级别也有所不同。

Linux: 安装程序会提示您指定拥有安装的文件的用户名，以及要创建其用户主目录的位置。默认情况下，系统用户为 esecadm；但是，您可以更改此系统用户名。如果该用户不存在，则将创建用户及其主目录。如果创建了新用户，安装过程中将不为该用户设置口令，以最大限度地确保安全性。如果希望以该用户身份登录系统，您必须在安装完成后为其设置一个口令。默认组为 esec。

在客户端安装期间，如果用户已经存在，则安装程序将不会再次提示指定用户。此行为与卸载或重新安装软件时的行为类似。不过，您可以让安装程序再次提示用户：

- 1 删除第一次安装时创建的用户和组
- 2 从 /etc/profile 中清除 ESEC_USER 环境变量

Windows: 没有创建用户。

系统用户的口令策略由所使用的操作系统定义。

5.3.2 Sentinel 应用程序和数据库用户

所有的 Sentinel Rapid Deployment 应用程序用户都为本地数据库用户，并且其口令通过使用本地数据库平台遵循的过程进行保护。这些用户拥有对数据库中特定表的只读权限，这样他们可以在数据库中执行查询操作。

安装程序会使用以下用户身份创建并配置 PostgreSQL 数据库：

- ♦ **admin:** admin 用户是所有 Sentinel 应用程序的管理员用户，用于登录系统。
- ♦ **dbauser:** dbauser 是可管理数据库的超级用户。dbauser 的口令在 Sentinel Rapid Deployment 服务器的安装过程中设置。此口令存储在 <用户主目录>/pgpass 中。系统会遵循 PostgreSQL 数据库口令策略。有关详细信息，请参见第 5.3.3 节“实施用户的口令策略”（第 53 页）。
- ♦ **appuser:** appuser 是 Sentinel 应用程序用于连接数据库的非超级用户。默认情况下，appuser 使用在安装过程中随机生成的口令，该口令以加密方式存储在 <安装目录>/config 目录下的 XML 文件（das_core.xml、das_binary.xml 和 advisor_client.xml）中。要更改 appuser 的口令，请使用 <install_directory>/bin/dbconfig 实用工具。有关详细信息，请参见《Sentinel Rapid Deployment 参考指南》中的“DAS 容器文件”。

注释：系统还有一个拥有整个数据库（包括系统数据库表）的 PostgreSQL 数据库用户。默认情况下，该 PostgreSQL 数据库用户设置为 NOLOGIN，这样就无人能以该 PostgreSQL 用户身份登录。

5.3.3 实施用户的口令策略

Sentinel Rapid Deployment 采用了基于标准的机制，让口令策略的实施更加容易。

安装程序会使用以下用户身份创建并配置 PostgreSQL 数据库：

dbauser: 数据库所有者（数据库管理员用户）。口令在安装过程中设置。

appuser: 这是用于从 Sentinel Rapid Deployment 登录数据库的应用程序用户。口令在安装过程中随机生成，仅供内部使用。

admin: 管理员身份凭证可用于登录 Sentinel Rapid Deployment Web 界面。口令在安装过程中设置。

默认情况下，用户口令存储在 Sentinel Rapid Deployment 内嵌入的 PostgreSQL 数据库中。PostgreSQL 允许您使用多种基于标准的鉴定机制，详情请参见 PostgreSQL 文档的“客户端鉴定 (<http://www.postgresql.org/docs/8.3/static/client-authentication.html>)”部分的说明。

使用这些机制将会影响 Sentinel Rapid Deployment 中的所有用户帐户，包括 Web 应用程序的用户以及仅用于后端服务的帐户，例如 dbauser 和 appuser。

一个更简单的选项是使用 LDAP 目录来鉴定 Web 应用程序用户。要在 Sentinel Rapid Deployment 服务器上启用此选项，请参见第 3.7 节“LDAP 鉴定”（第 38 页）。此选项不会影响用于后端服务的帐户，这些帐户将仍会通过 PostgreSQL 进行鉴定，除非您更改了 PostgreSQL 配置设置。

通过使用这些基于标准的机制以及您环境中现有的机制（如 LDAP 目录），您可以实现理想的 Sentinel Rapid Deployment 口令策略实施。

5.4 保护 Sentinel 数据

重要：由于 Sentinel 服务器中数据的高度敏感性，应该保证计算机的物理安全，并将其放置在一个安全的网络区域中。要从安全网络之外的事件源收集数据，请使用远程连接器管理器。

对于一些特定组件，必须存储口令，这样当系统需要连接到某资源（如数据库或事件源）时，就可以使用这些口令。既然这样，当存储口令时，将首先对其进行加密以避免未经授权就访问明文口令。

虽然口令会经过加密，但您还是必须注意，为了避免口令泄露，需要保护对存储的口令数据的访问权限。例如，您可以确保未授权用户无法读取包含敏感数据的文件。

文件

advisor_client.xml

数据库身份凭证

数据库身份凭证存储在 <安装目录>/config/server.xml 文件中

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
  <property name="username">appuser</property>
  <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Advisor 身份凭证

```
<obj-component id="DownloadComponent">
  <class>esecurity.ccs.comp.advisor.feed.NewAdvClientDownload</class>
  <property name="advisor.downloadfrom.url">https://secure-www.novell.com/
sentinel/advisor/advisordata</property>
  <property name="username">admin</property>
  <!-- Set the password (encrypted) using the adv_change_password script -
-->
  <property name="password">jqhlWIX8HD6GDHVX9FApWg==</property>
<property name="compression.enabled">true</property>
  <!--
    Set the following properties to connect through an HTTP proxy.
    Set the proxy password (encrypted) using the adv_change_password script
    (make a
    copy of the script and add "-x" to the java cmd line to set the proxy
    password
    instead of the advisor password.
  -->
  <!--
  <property name="proxy_host"></property>
  <property name="proxy_port"></property>
  <property name="proxy_username"></property>
  <property name="proxy_password"></property>
  -->
</obj-component>
```

Configuration.xml

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
</strategy>
```

das_binary.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
<property name="username">appuser</property>
<property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

das_core.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
<property name="username">appuser</property>
<property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

有些数据库表用于存储口令和证书。这类敏感数据会加密并存储在以下所列的表中。必须限制对这些表的访问权限。

- ◆ **evt_src:** evt_src_config 列的数据
- ◆ **evt_src_collector:** 列: evt_src_collector_props
- ◆ **evt_src_grp (不确定):** 列: evt_src_default_config
- ◆ **md_config:** 列: data
- ◆ **integrator_config:** 列: integrator_properties
- ◆ **md_view_config:** 列: view_data
- ◆ **esec_content:** 列: content_context、content_hash
- ◆ **esec_content_grp_content:** 列: content_hash
- ◆ **sentinel_plugin:** 列: content_pkg、file_hash

Sentinel Rapid Deployment 存储了配置数据和事件数据。这些数据存储在以下位置:

组件	配置数据的位置	事件数据的位置
Sentinel Rapid Deployment 服务器	数据库表和文件系统 (< 安装目录>/config) 这些配置信息包括加密的数据库、事件源、集成器和口令。	数据库 (EVENTS、CORRELATED_EVENTS、EVT_SMRY_、AUDIT_RECORD 表) 以及文件系统的以下位置: < 安装目录>/data/eventdata 和 < 安装目录>/data/raw data 事件数据可以作为分区管理工作的一部分存档在文件系统中。

组件	配置数据的位置	事件数据的位置
关联引擎	文件系统（< 安装目录 >/config）。唯一敏感的配置信息是用于连接到消息总线的客户端密钥对。	correlation_engine.cache
DAS Core	< 安装目录 >/config	das_core.cache
DAS Binary	< 安装目录 >/config	如果数据库出现故障，事件数据可能会被缓存。 das_binary.cache
收集器管理器	文件系统（< 安装目录 >/config）。唯一敏感的配置信息是用于连接到消息总线的收集器管理器用户口令。	在发生错误（如消息总线发生故障或事件溢出）时，事件数据可能会缓存到文件系统中。此事件数据存储在 < 安装目录 >/data/collector_mgr.cache 目录中。
客户端应用程序	文件系统（安装目录/config）。客户端应用程序不会在其配置文件中存储任何敏感信息。 例如，客户端应用程序可以将 ESM 数据导出到一个本地文件系统中。如果加密口令出现在导出的事件源的配置中，则导出的文件中会包含加密口令。尽管口令进行了加密，ESM 导出权限还是仅提供给拥有此特权的可信任用户。	无

5.5 备份信息

- ◆ 必须定期备份事件。备份媒体应该存储在一个安全的外设装置中。
- ◆ 备份系统数据。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[备份和恢复实用程序](#)”。
- ◆ 对于敏感数据，请使用以下方法之一对数据备份进行加密：
 - ◆ 如果创建数据的应用程序支持加密，则对其数据进行加密。例如，数据库产品和第三方工具支持数据加密。使用在备份时可以加密数据的备份软件。此方法可能会影响性能和管理，尤其影响管理加密密钥。
 - ◆ 在备份数据时使用可加密敏感备份媒体的加密设备。
- ◆ 如果在装置外传输或存储媒体，请使用一家在媒体传输和存储方面较为专业的公司。确保您的磁带可以通过条形码进行跟踪，存储在良好的环境中，并由在处理媒体方面声誉良好的公司处理。
- ◆ 装载恢复证书。Novell Sentinel 服务默认并未配置为用于恢复代理。在通过 YaST 进行服务器配置时，请确保配置了恢复代理路径。此路径应该包含服务可以装载的证书列表，以供用户从中选择。

有关详细信息，请参见《*Sentinel Rapid Deployment 参考指南*》中的“[Sentinel 6.1 Rapid Deployment 服务器的证书管理](#)”。

YaST 包含一些模块，用于对 X.509 证书进行基本管理，这些管理主要包括创建 CA、子 CA 及其证书。有关如何管理和更新证书的详细信息，请参见《*SUSE Linux Enterprise Server 10 安装和管理指南*》(http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html) 中的管理 X.509 证书 (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html)。

5.6 保护操作系统的安全

- ◆ SUSE Linux Enterprise Server (SLES) 10 SP3 或更高版本支持 Sentinel Rapid Deployment。有关保护 SLES 计算机安全的详细信息，请参见 [SUSE Linux Enterprise Server 10 文档](http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html) (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html)。
- ◆ 使用防火墙保护对 Sentinel Rapid Deployment 的访问安全。如果可以从公司网络外部访问 Sentinel 服务器，则应该使用防火墙阻止入侵者直接访问。

在防火墙中启用以下端口：

组件	端口
ActiveMQ	61616
PostgreSQL	5432
Tomcat	8443
Sentinel 控制中心代理客户端端口	10013
代理的受信任客户端	10014
在引擎和管理器之间使用的 internal_gateway_server 和 internal_gateway	5556
internal_router_server 和 internal_router_client	5558
在事件路由器的客户端和服务器之间使用	
事件侦听程序端口	35000
在 config/collector_mgr.properties 中通过 “esecurity.agentmanager.event.port” 进行配置	

注释：如果安装时标有星号的端口已被使用，则这些端口可能有所不同。如果这些端口在安装时已被使用，请替换在安装时系统针对其发出提示的端口号。

有关在 SLES 10 上启用防火墙的详细信息，请参见《*SLES 10 管理指南*》中的[使用 YaST 配置防火墙](http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html) (http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html)。

5.7 查看 Sentinel 审计事件

Sentinel Rapid Deployment 会针对用户执行的许多操作和系统活动内部执行的操作生成审计事件。可以在活动视图中查看这些事件，或通过搜索或报告访问这些事件。不过，您必须拥有必要的许可权限才能查看系统事件。

有关详细信息，请参见《*Sentinel Rapid Deployment 用户指南*》中的“[Sentinel 系统事件](#)”。

5.8 使用 CA 证书

可以使用由某个主要证书颁发机构 (CA) (如 VeriSign、Thawte 或 Entrust) 签名的证书替换自我签名证书。还可以使用由不常见 CA (如公司或组织内部的 CA) 签名的证书替换自我签名证书。

有关详细信息, 请参见 《*Sentinel Rapid Deployment 参考指南*》中的“[Sentinel 6.1 Rapid Deployment 服务器的证书管理](#)”。

测试 Sentinel Rapid Deployment 功能

6

Sentinel Rapid Deployment 安装时附有一个一般收集器，可用来测试系统的许多基本功能。您可以使用此收集器来测试活动视图、事件创建、关联规则和报告。

- ◆ 第 6.1 节“测试 Rapid Deployment 安装”（第 59 页）
- ◆ 第 6.2 节“测试后的清理”（第 70 页）
- ◆ 第 6.3 节“使用真实数据”（第 71 页）

6.1 测试 Rapid Deployment 安装

以下过程介绍了测试 Sentinel Rapid Deployment 系统的步骤以及预期结果。您可能无法看到完全相同的事件，但您的结果应类似于下面的结果。

通过这些测试，基本上可以确认下列事项：

- ◆ Sentinel 服务已启动并且正在运行。
- ◆ 可以通过讯息总线进行通讯。
- ◆ 正在发送内部审计事件。
- ◆ 可以通过收集器管理器发送事件。
- ◆ 事件正在被插入到数据库中，并且可以使用报告进行检索。
- ◆ 可以创建和查看事件。
- ◆ 关联引擎会评估规则并触发关联事件。
- ◆ Sentinel 数据管理器连接到数据库，并可读取分区信息。

如果上述任何测试失败，请查看安装日志和其它日志文件，并与 [Novell 技术支持 \(http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup\)](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) 联系（如有必要）。

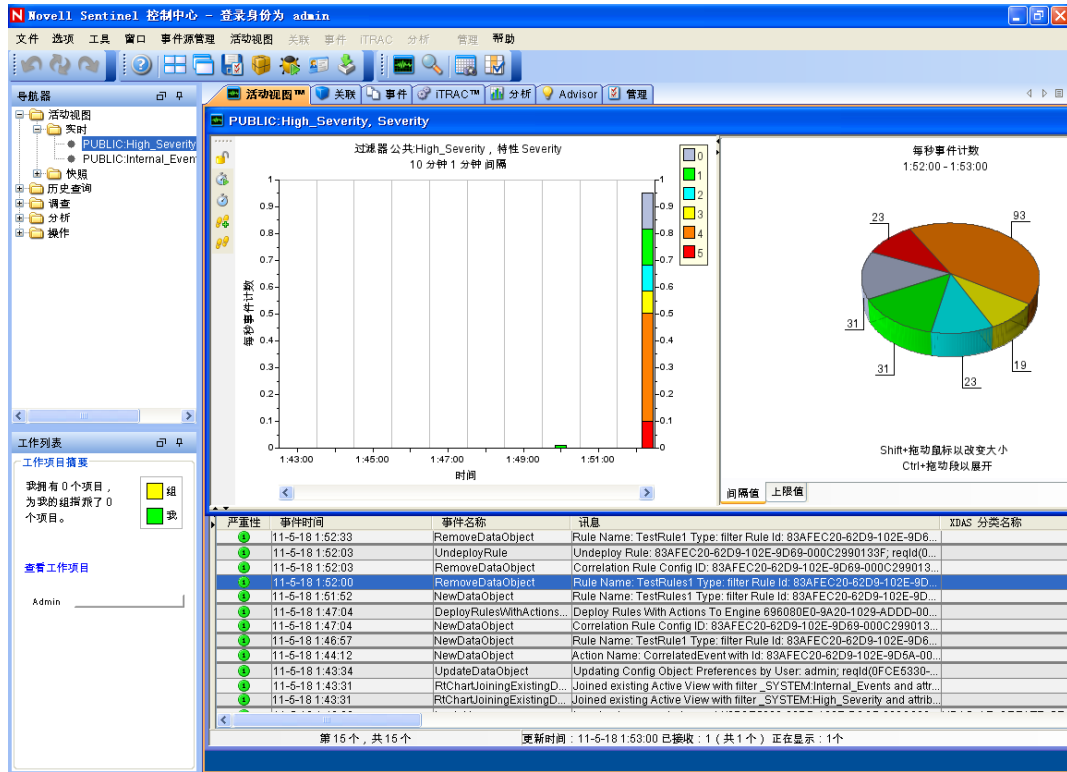
要测试安装，请执行下列操作：

- 1 登录到 Sentinel Rapid Deployment Web 界面。
有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[访问 Novell Sentinel Web 界面](#)”。
- 2 选择“搜索”页，然后搜索任何内部事件。应该返回一个或多个事件。
例如，要搜索严重性级别为 3-5 的内部事件，请选择 *包括系统事件*，然后在 *搜索* 字段中输入 *sev:[3 TO 5]*。
有关搜索功能的详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“[运行事件搜索](#)”。
SP2 中默认不启用搜索功能。不过，如果您想启用此功能，请参见《Sentinel Rapid Deployment 用户指南》中的“[在 Web 用户界面中启用搜索选项](#)”。
- 3 选择“报告”页，指定参数，然后运行报告。
例如，单击“Sentinel 核心事件配置”旁的 *运行* 按钮，指定所需参数，然后单击 *运行*。

有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“运行报告”。

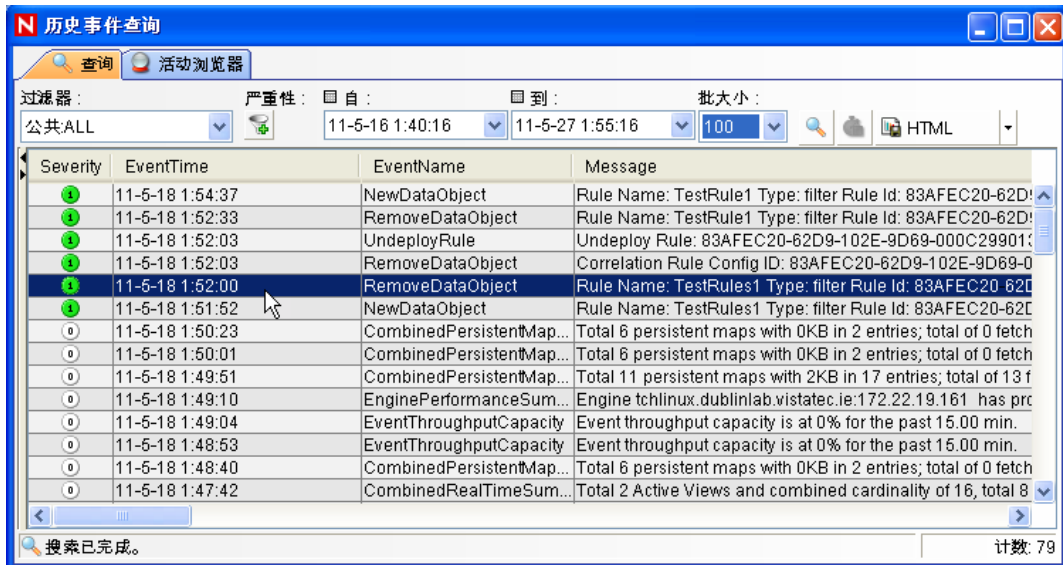
- 4 在“应用程序”页上，单击启动 Sentinel 控制中心。
- 5 以安装期间指定的 Sentinel 管理用户（默认为 admin）身份登录到系统。

Sentinel 控制中心随即会打开，您可以看到活动视图选项卡，其中显示了通过内部事件和高严重性公用过滤器过滤出的事件。

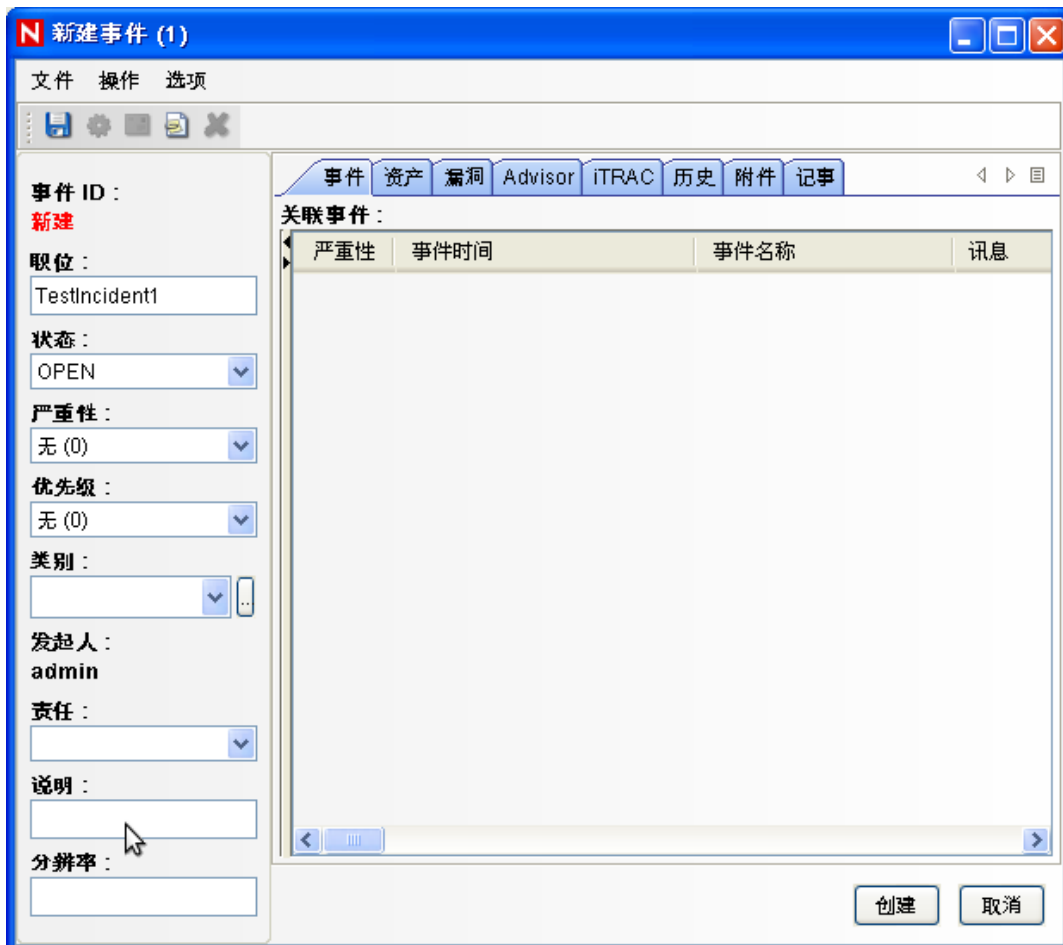


- 6 转至事件源管理菜单，然后选择实时视图。
- 7 在图形视图中，右键单击 5 eps 事件源，然后选择启动。
- 8 关闭“事件源管理实时视图”窗口。
- 9 单击活动视图选项卡。

您可以查看标题为“公共：高严重性、严重性”的活动窗口。启动收集器以及将数据显示在此窗口中可能需要一段时间。
- 10 单击工具栏上的事件查询按钮。“历史事件查询”窗口便会显示。
- 11 在“历史事件查询”窗口中，单击过滤器向下箭头以选择过滤器。请选择公用：全部过滤器。
- 12 选择收集器在期间处于活动状态的某个时段。请使用自和至下拉列表选择日期范围。
- 13 选择批文件大小。
- 14 单击放大图标运行查询。



- 15 按住 Ctrl 或 Shift 键，然后从“历史事件查询”窗口中选择多个事件。
- 16 右键单击窗口，然后选择 *创建事件* 以显示“新建事件”窗口。

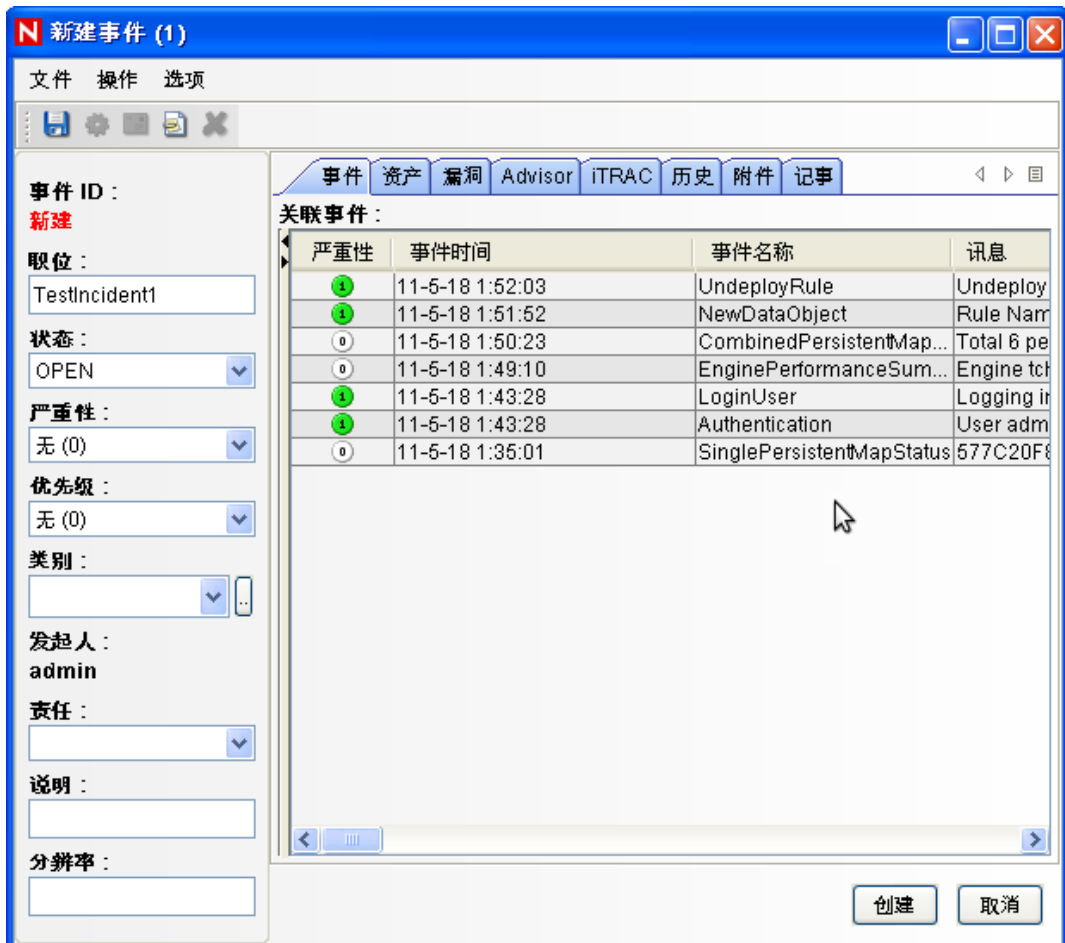


17 将事件命名为 TestIncident1，然后单击 *创建*。看到成功通知后，单击 *保存*。

18 单击 *事件* 选项卡，查看您刚才在“事件视图管理器”中创建的事件。



19 双击事件以显示相应事件。



20 关闭“事件”窗口。

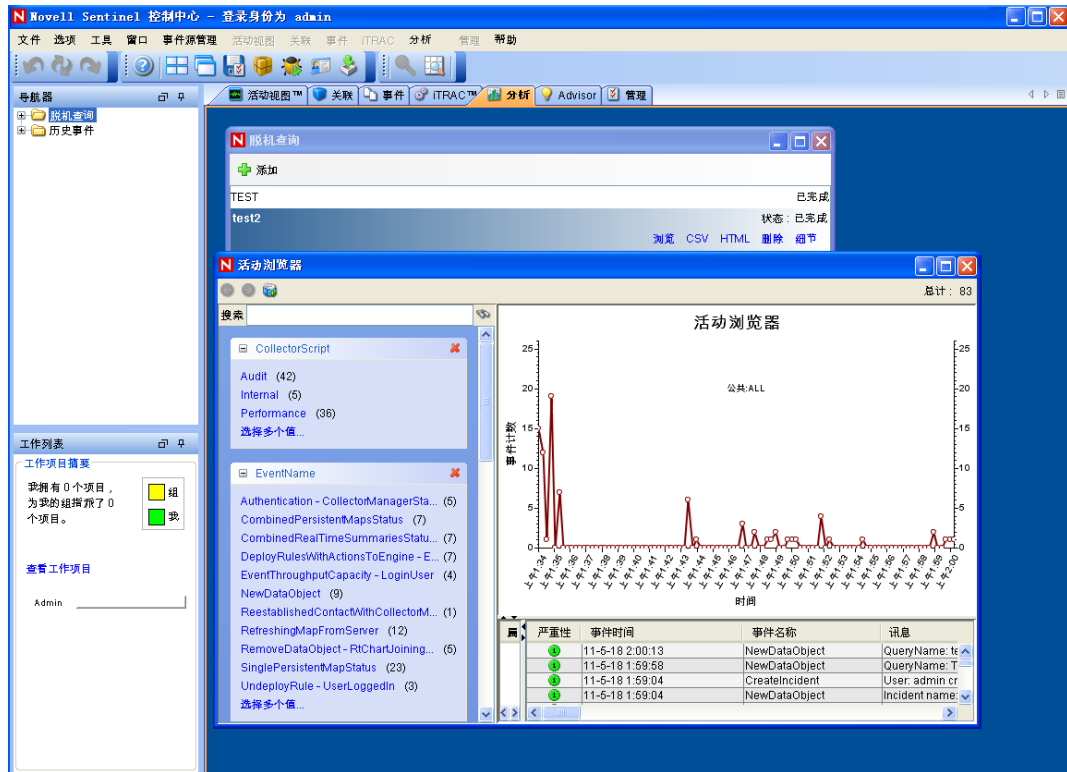
21 单击 *分析* 选项卡。

22 从 *分析* 菜单中或“导航器”中单击 *脱机查询*。

23 在“脱机查询”窗口中，单击 *添加*。

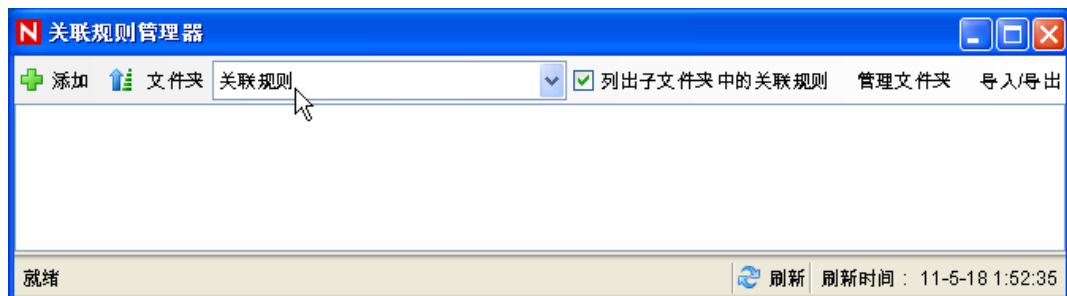
24 指定名称，选择过滤器，选择时段，然后单击 *确定*。

25 单击 *浏览* 以在“活动浏览器”窗口中查看事件列表及相关细节。



您可以查看收集器、目标 IP、严重性、目标服务端口以及资源等细节。

26 选择 **关联** 选项卡。关联规则管理器便会显示。



27 单击“**添加**”。“关联规则”向导便会显示。



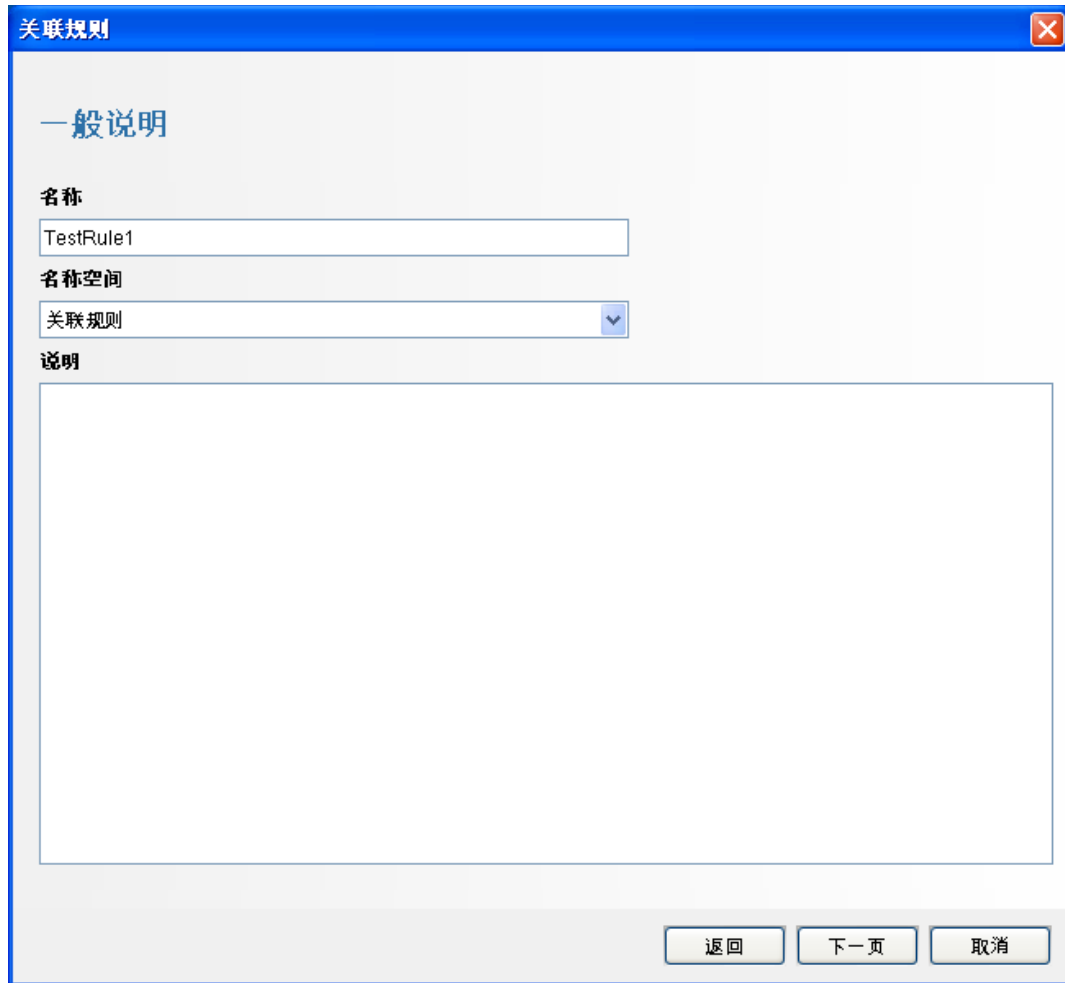
28 单击 *简单*。“简单规则”窗口便会显示。



- 29 使用下拉菜单将准则设置为：“严重性 = 4”，然后单击下一步。“更新准则”窗口便会显示。



- 30 选择在每次激活此规则时不再继续执行下一个操作，使用下拉菜单将时段设置为 1 分钟，然后单击下一步。“一般说明”窗口便会显示。



关联规则

一般说明

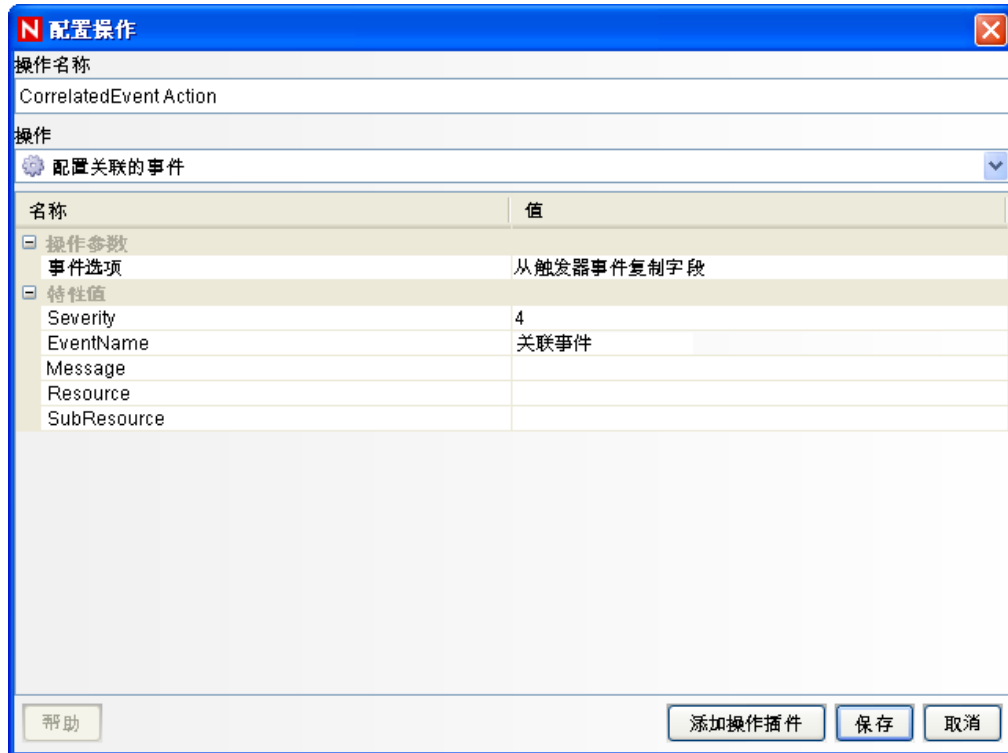
名称
TestRule1

名称空间
关联规则

说明

返回 下一页 取消

- 31 将规则命名为 *TestRule1* 并提供说明，然后单击 *下一步*。
 - 32 选择 *否*，*不另外创建规则*，然后单击 *下一步*。
 - 33 创建一个操作以将其关联到您创建的规则：
 - 33a 执行下列任一操作：
 - ◆ 选择 *工具 > 操作管理器 > 添加*。
 - ◆ 在“部署规则”窗口中，单击 *添加操作*。有关详细信息，请参见 [步骤 34](#) 到 [步骤 35](#)（第 68 页）。
- “配置操作”窗口便会显示。



33b 在“配置操作”窗口中，指定下列内容：

- ◆ 指定操作名称，例如“关联事件操作”。
- ◆ 从操作下拉列表中选择配置关联事件。
- ◆ 设置事件选项。
- ◆ 将严重性设置为 5。
- ◆ 指定事件名称，例如“关联事件”。
- ◆ 指定讯息（如果需要）。

有关创建操作的详细信息，请参见《Sentinel Rapid Deployment 用户指南》中的“创建操作”。

33c 单击保存。

34 打开“关联规则管理器”窗口。

35 选择一个规则，然后单击部署规则链接。“部署规则”窗口便会显示。

36 在“部署规则”窗口中，选择要部署规则的引擎。

37 选择您在步骤 33（第 67 页）中创建的要与规则关联的操作，然后单击确定。



38 选择关联引擎管理器。

在关联引擎下，可以看到该规则已部署并启用。

名称	主机名	主机 ID	运行状况	启用/禁用	ID	平均处理...	状态持续...	已处理的...	已激活的...
Sentinel									
shrabani-st.blr.no	shrabani-st.	172.22.19...	正常	已启用	696080E0...	1 毫秒	13.02 分钟	53	
TestRule1			正常	已启用	83AFEC20...		6.48 秒	0	0
CorrelatedEvent									

39 触发一个严重性为 4 的事件，例如鉴定失败，以激活之前部署的关联规则。

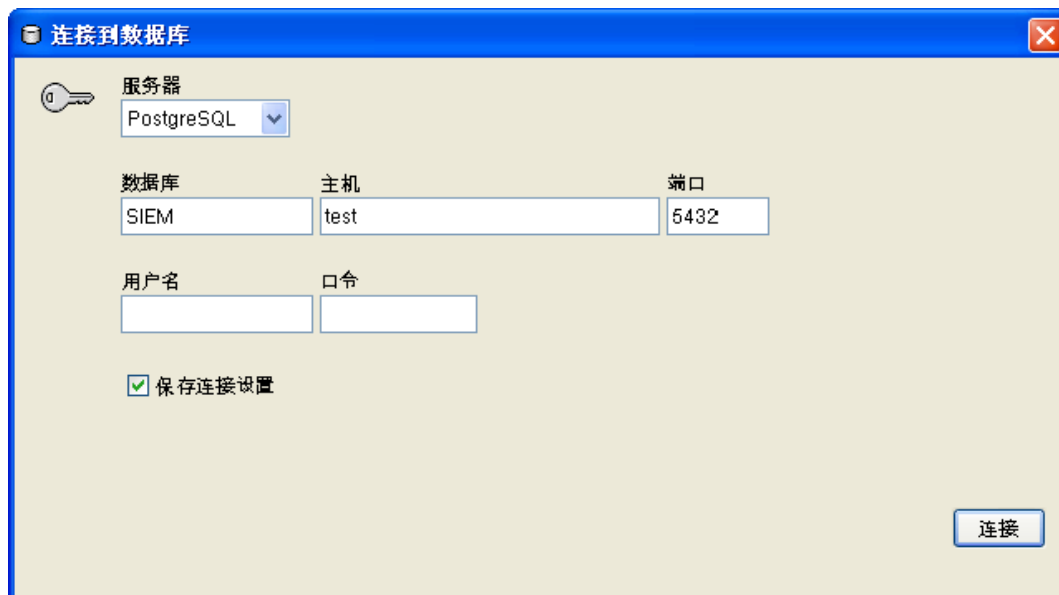
例如，打开 Sentinel 控制中心登录窗口，然后指定错误的用户身份凭证以生成此类事件。

40 单击活动视图选项卡，然后校验是否生成了关联事件。

严重性	事件时间	事件名称	消息	XDAS 分类名称
4	11-5-18 1:47:04	DeployRulesWithActions...	Deploy Rules With Actions To Engine 696080E0-9A20-1029-ADD-00...	
4	11-5-18 1:47:04	NewDataObject	Correlation Rule Config ID: 83AFEC20-62D9-102E-9D69-000C299013...	
4	11-5-18 1:46:57	NewDataObject	Rule Name: TestRule1 Type: filter Rule Id: 83AFEC20-62D9-102E-9D6...	
4	11-5-18 1:44:12	NewDataObject	Action Name: CorrelatedEvent with Id: 83AFEC20-62D9-102E-9D5A-00...	

41 关闭“Sentinel 控制中心”。

- 42 在“应用程序”页上，单击启动 Sentinel 数据管理器。
- 43 以安装过程中指定的数据库管理用户（默认为 dbauser）身份登录到 Sentinel 数据管理器。



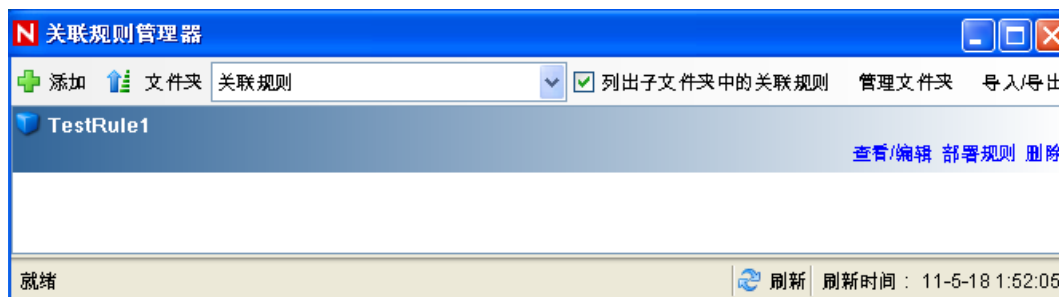
- 44 单击各个选项卡以验证您是否可以访问它们。
- 45 关闭 Sentinel 数据管理器。

如果执行了上述所有步骤而未出现任何错误，那么您便已完成 Sentinel 系统安装的基本验证。

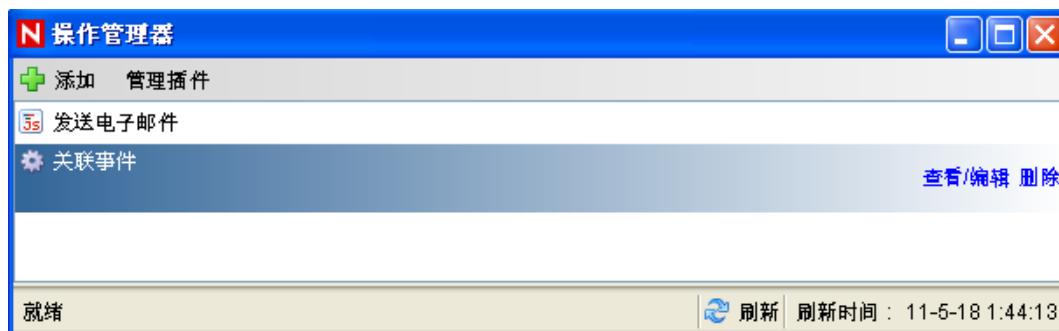
6.2 测试后的清理

完成了系统验证之后，应去除为测试创建的对象。

- 1 以安装期间指定的 Sentinel 管理用户（默认为 admin）身份登录到系统。
- 2 选择关联选项卡。
- 3 打开“关联引擎管理器”。
- 4 在关联引擎管理器中右键单击 *TestRule1*，然后选择取消部署。
- 5 打开“关联规则管理器”。
- 6 选择 *TestRule1*，然后单击删除。



- 7 选择 *工具 > 操作管理器* 显示“操作管理器”窗口。
- 8 选择 *关联事件* 操作，单击 *删除*，然后单击 *是* 以确认删除。



- 9 选择 *事件源管理* 菜单，然后选择 *实时视图*。
- 10 在图形事件源层次结构中，右键单击 *一般收集器*，然后选择 *停止*。
- 11 关闭“事件源管理”窗口。
- 12 单击 *事件* 选项卡。
- 13 打开“事件视图管理器”。
- 14 选择 *TestIncident1* 并右键单击，然后选择 *删除*。

6.3 使用真实数据

要开始使用真实数据，您需要导入并配置适用于您环境的收集器，配置您自己的规则，构建 iTRAC 工作流程，等等。有关详细信息，请参见《Sentinel Rapid Deployment 用户指南》。Sentinel 解决方案包可帮助您快速入门。有关详细信息，请参见 [Sentinel 内容页 \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html)。

卸载 Sentinel Rapid Deployment

7

- ◆ 第 7.1 节“卸载 Sentinel Rapid Deployment 服务器”（第 73 页）
- ◆ 第 7.2 节“卸载远程收集器管理器和 Sentinel 客户端应用程序”（第 73 页）

7.1 卸载 Sentinel Rapid Deployment 服务器

- 1 以根用户身份登录。
- 2 切换到 setup 目录。
`cd <install_directory>/setup`
- 3 运行 `uninstall.sh` 脚本以卸载 Sentinel Rapid Deployment 服务器：
`./uninstall.sh`
该脚本会向您显示一条讯息，提示您 Sentinel Rapid Deployment 将会被完全去除。
- 4 指定在卸载 Sentinel Rapid Deployment 服务器时是要保留还是要去除用户。按 `y` 会去除用户，按 `n` 会保留用户。
- 5 指定在卸载 Sentinel Rapid Deployment 服务器时是要保留还是要去除组。按 `y` 会去除组，按 `n` 会保留组。
- 6 输入 `y` 开始卸载，或输入 `n` 退出卸载。

7.2 卸载远程收集器管理器和 Sentinel 客户端应用程序

- ◆ 第 7.2.1 节“Linux”（第 73 页）
- ◆ 第 7.2.2 节“Windows”（第 74 页）
- ◆ 第 7.2.3 节“卸载后过程”（第 74 页）

7.2.1 Linux

- 1 以根用户身份登录。
- 2（视情况而定）如果您要卸载收集器管理器，请停止 Sentinel Rapid Deployment 服务：
`<install_directory>/bin/sentinel.sh stop`
- 3 转到以下位置：
`<install_directory>/_uninst`
- 4 执行以下任一操作：

方式	命令
GUI	<code>./uninstall.bin</code>
	继续步骤 5（第 74 页）。

方式	命令
控制台	<code>./uninstall.bin -console</code>

继续按照屏幕说明操作。

- 5 选择一种语言，然后单击 *确定*。
- 6 在 Sentinel UninstallShield 向导中，单击 *下一步*。
- 7 选择要卸装的组件，然后单击 *下一步*。
- 8 确保所有正在运行的 Sentinel 应用程序已停止，然后单击 *下一步*。
此时将显示为卸装选择的功能摘要。
- 9 单击 *卸装*。
- 10 单击 *完成*。

7.2.2 Windows

- 1 以管理员用户身份登录。
- 2 (视情况而定) 如果您要卸装收集器管理器，请停止 Sentinel Rapid Deployment 服务：
`<install_directory>\bin\sentinel.bat stop`
- 3 执行以下操作之一：
 - ◆ 选择 *开始* > *所有程序* > *Sentinel* > *卸装 Sentinel*。
 - ◆ 选择 *开始* > *运行*，输入 `<安装目录>_uninst`，然后双击 `uninstall.exe`。
- 4 选择一种语言，然后单击 *确定*。
此时将显示 Sentinel Rapid Deployment UninstallShield 向导。
- 5 单击 *下一步*。
- 6 选择要卸装的组件，然后单击 *下一步*。
- 7 确保所有正在运行的 Sentinel 应用程序已停止，然后单击 *下一步*。
此时将显示选择要卸装的功能的摘要。
- 8 单击 *卸装*。
- 9 选择重引导系统，然后单击 *完成*。

7.2.3 卸装后过程

卸装应用程序后，某些系统设置将保留，可手动将其去除。在执行 Sentinel 的干净安装之前应该去除这些设置，特别是当 Sentinel 卸装遇到错误时更应如此。

注释：在 Linux 中，卸装收集器管理器或客户端应用程序并不会从操作系统中去除 Sentinel 管理员用户。必要时可手动去除该用户。

- ◆ [Linux \(第 75 页\)](#)
- ◆ [Windows \(第 75 页\)](#)

Linux

- 1 以根用户身份登录。
- 2 去除安装了 Sentinel 软件的 < 安装目录 > 中的内容。
- 3 去除 /etc/init.d 目录中的以下文件（如果存在）：
sentinel
只有在安装了收集器管理器时才适用。
- 4 确保没有人以 Sentinel 管理员用户（默认为 esecadm）身份登录，然后去除用户、主目录和 esec 组：
 - ◆ 运行 userdel -r esecadm
 - ◆ 运行 groupdel esec
- 5 去除 /root/InstallShield 目录。
- 6 去除 /etc/profile 的 InstallShield 部分。
- 7 重新启动计算机。

Windows

- 1 删除 %CommonProgramFiles%\InstallShield\Universa 文件夹及其所有内容。
- 2 删除 < 安装目录 > 文件夹（默认为 C:\Program Files\Novell\Sentinel6）。
- 3 右键单击 *我的电脑* > *属性* > *高级选项卡*。
- 4 单击 *环境变量* 按钮。
- 5 删除下列变量（如果存在）：
 - ◆ ESEC_HOME
 - ◆ ESEC_VERSION
 - ◆ ESEC_JAVA_HOME
 - ◆ ESEC_CONF_FILE
 - ◆ WORKBENCH_HOME
- 6 去除 PATH 环境变量中所有指向 Sentinel 安装的项。
- 7 删除桌面上的所有 Sentinel 快捷方式。
- 8 从 *开始* 菜单中删除快捷方式 *开始* > *程序* > *Sentinel* 文件夹。
- 9 重新启动计算机。

更新 Sentinel Rapid Deployment 主机名

A

- ◆ 第 A.1 节“服务器”（第 77 页）
- ◆ 第 A.2 节“客户端应用程序”（第 77 页）

A.1 服务器

在运行期间或安装期间，Sentinel 服务器上会自动更新主机名的变动。如果在主机名更新后服务器未正常工作，您必须手动验证以下内容：

- ◆ 在 Sentinel 重新启动后，所有的 jnlp 文件和 configuration.xml 文件都会更新。
- ◆ sentinel_host 数据库表中的主机名条目已更新。
- ◆ 对 <安装目录>/config/configuration.xml 文件中本地循环（localhost 或 127.0.0.1）的所有引用都未受影响。

A.2 客户端应用程序

对于客户端应用程序，必须在以下位置手动更改服务器主机名或 IP 地址，以指向正确的服务器：

- ◆ <安装目录>/config/configuration.xml。

Sentinel 控制中心和解决方案设计器使用此信息。

- ◆ <安装目录>/config/SentinelPreferences.properties 文件中提供的帮助 URL。
- ◆ 运行以下命令以更新 sdm.connect 文件中的主机名：

```
sdm -action saveConnection -server <postgresql> -host <hostIpaddress/  
hostName> -port <portnum> -database <databaseName/SID> [-driverProps  
<propertiesFile> {-user <dbUser> -password <dbPass> | -winAuth} -  
connectFile <filenameToSaveConnection>
```


疑难解答提示

本章节为您提供了一组查错建议，可以帮助您解决一些 Sentinel Rapid Deployment 的安装问题。

- ◆ 第 B.1 节 “由于输入无效身份凭证而导致数据库鉴定失败”（第 79 页）
- ◆ 第 B.2 节 “Sentinel Web 界面启动失败”（第 79 页）
- ◆ 第 B.3 节 “在启用 UAC 后，远程收集器管理器在 Windows 2008 上发生例外”（第 80 页）
- ◆ 第 B.4 节 “未针对映像的收集器管理器创建 UUID”（第 80 页）

B.1 由于输入无效身份凭证而导致数据库鉴定失败

常见原因：如果在将 Sentinel Rapid Deployment 服务器配置为使用 LDAP 鉴定的过程中输入了无效的 LDAP 服务器主机名或 IP 地址，则数据库鉴定将会失败。

操作：确保输入有效的 LDAP 服务器主机名或 IP 地址。

B.2 Sentinel Web 界面启动失败

常见原因：您在运行着 Identity Audit 进程的计算机上已经安装了 Sentinel Rapid Deployment，或者其卸装不完全。

操作：Sentinel Rapid Deployment 与 Novell Identity Audit 不能安装于同一台计算机上。在安装 Identity Audit 的计算机上安装 Sentinel Rapid Deployment 之前，请务必完全卸装 Identity Audit。

如果 Identity Audit 进程未完全停止，那么就无法成功地完全卸装 Identity Audit。这种情况下，就有可能在安装 Sentinel Rapid Deployment 或启动其应用程序时发生冲突。

- 1 运行以下命令以关闭 Identity Audit 服务：

```
/etc/init.d/identity_audit stop
```

- 2 运行以下命令确保所有 Identity Audit 已经停止工作：

```
ps -ef | grep novell
```

- 3 必要时手动停止所有剩余进程。

```
kill -9 pid
```

- 4 使用必要的根许可权限卸装 Identity Audit。

有关详细信息，请参见《Identity Audit 指南》(<http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/>)。

B.3 在启用 UAC 后，远程收集器管理器在 Windows 2008 上发生例外

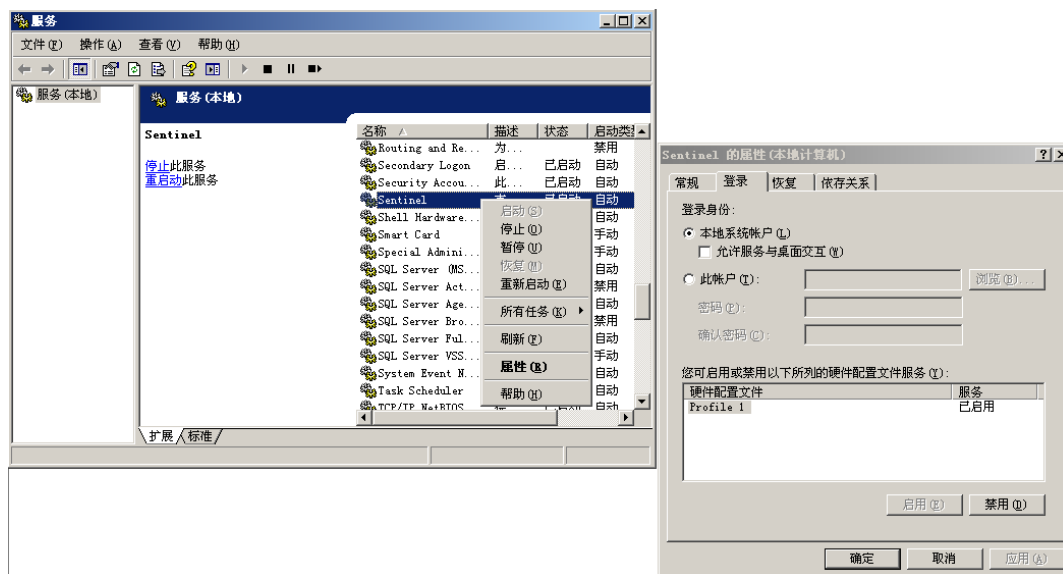
问题：以属于“管理员”组的任何用户身份登录，然后在终端提示符中执行 setup.bat 命令以安装收集器管理器。重新启动系统或手动启动收集器管理器服务，然后使用相同的用户身份凭证登录。异常记录在 collector_manager0.0.log 文件中，会影响以下收集器管理器功能：

- ◆ 映射无法初始化。
- ◆ 在收集器管理器 (Win2008) 计算机的文件系统上使用文件连接器无法选择任何一个事件源文件。

常见原因：在 64 位的 Windows 2008 SP1 标准版上安装了收集器管理器。默认情况下，计算机的“用户访问控制”(UAC) 功能会设置为启用。

操作：将 Sentinel Rapid Deployment 服务的登录拥有者更改为当前用户。默认情况下，登录拥有者设置为本地系统帐户。要更改默认选项：

- 1 运行 services.msc 以打开服务窗口。
- 2 右键单击 Sentinel，然后选择属性。



- 3 在“Sentinel 属性”窗口中，选择登录选项卡。
- 4 选择此帐户，然后提供用于安装收集器管理器的当前用户身份凭证。

B.4 未针对映像的收集器管理器创建 UUID

如果您为收集器管理器服务器创建了映像（例如通过使用 ZenWorks 映像），并在不同的计算机上恢复了相应映像，则 Sentinel Rapid Deployment 将不能唯一识别收集器管理器的各个新实例。造成这一问题的原因是 UUID 出现重复。

您必须在新安装的收集器管理器系统上执行以下步骤来生成 UUID：

- 1 删除位于 <安装目录>/data 文件夹中的 host.id 或 sentinel.id 文件。

2 重新启动收集器管理器。

收集器管理器便会自动生成 UUID。

PostgreSQL 数据库维护的最佳实践



您可以对数据库进行优化调整，以提升数据库服务器的性能。本章节中所述限制皆为近似建议值，而非硬性限制。不过，在具备高度动态特性的系统中，最好在构建系统时预留一定缓冲空间，为系统扩展留下余地。

- ◆ 第 C.1 节“修改内存配置参数”（第 83 页）
- ◆ 第 C.2 节“降低 Vacuum/Analyze 造成的 I/O 影响”（第 83 页）

C.1 修改内存配置参数

为优化调整 PostgreSQL 数据库服务器，请修改 <安装目录>/3rd party/postgresql/data/postgresql.conf 文件中的以下内存配置参数：

- ◆ **shared_buffers**：决定专门供 PostgreSQL 用于超速缓存数据的内存容量。为实现更佳性能，您可以将此参数值设置为可用 RAM 容量的四分之一。
- ◆ **effective_cache_size**：决定为操作系统和数据库内部的磁盘超速缓存分配多少内存容量。您可以考虑操作系统和其他应用程序的内存使用量，估算出这一参数的合适大小。可以将系统可用内存总容量的一半分配给此参数。
- ◆ **work_mem**：决定内部排序操作和哈希表在切换到临时磁盘文件之前所用的内存容量。其单位为千字节 (KB)。默认值为 1024 KB (1 MB)。

对于复杂查询，可能会出现并行运行多项排序和哈希操作的情况。每项操作都可使用 **work_mem** 值指定的内存容量，超过这一容量才会开始将数据放入临时磁盘文件中。如果您要在 Sentinel Rapid Deployment 系统上安排较多报告任务，请将此值设置为 500MB 到 1GB 之间。

- ◆ **maintenance_work_mem**：决定数据库维护操作（例如 VACUUM、CREATE INDEX 和 ALTER TABLE ADD FOREIGN KEY）使用的最大内存容量。其单位为千字节 (KB)。默认值为 16384 KB (16 MB)。

将该设置设为较大的值有可能可以改善执行数据删除和恢复数据库转储时的性能。不必改动此参数的值，默认值已足以应对 Sentinel Rapid Deployment 操作所需。

C.2 降低 Vacuum/Analyze 造成的 I/O 影响

您可以通过多种方式改善 PostgreSQL 数据库的性能。

- ◆ 以下两个参数可以控制自动 vacuum 操作，默认情况下，这些参数在 Sentinel Rapid Deployment 服务器安装期间会被注释，而您必须去除注释并设置相应值。
 - ◆ **vacuum_cost_delay**：定义当超出成本限制时，进程休眠的时间。例如，可以将此值设置为 100。
 - ◆ **vacuum_cost_limit**：定义导致 vacuum 进程休眠的累积成本。例如，可以将此值设置为 10000。

如果将这些参数的值设置为非零值，则可以降低 vacuum 和 analyze 命令对一般数据库活动造成的 I/O 影响。运行报告时，如此设置所能改善的性能可以忽略不计，因为此时 vacuum 所需的时间比较长。

- ◆ 默认情况下，`autovacuum` 进程设置为 `true`，会定期运行以恢复磁盘空间并更新规划工具的统计数字。随着数据库大小的增长，`autovacuum` 将不能维护所有数据库对象。此时如果性能不佳，请以 `cron` 作业的形式运行 `AnalyzePartitions.sh` 脚本。此 `cron` 作业应由拥有 `Sentinel Rapid Deployment` 进程的用户进行设置。

例如：

```
30 11 * * * $ESEC_HOME/bin/AnalyzePartitions.sh
```

其中：

- ◆ 30 为分钟。
- ◆ 11 为小时。
- ◆ `ESEC_HOME` 为数据库的绝对路径。

在此示例中，脚本将在每天的 11:30 运行。

- ◆ 避免将存档安排在报告作业期间运行。如果您将这两个进程安排为同时运行，由于 PostgreSQL 的相关 `bug`，报告将会进入等待状态，在存档作业完成后才开始处理数据。此更改会影响数据库的性能。