安装指南

Novell®
Sentinel Log Manager

1.1

July 08, 2010

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/)。如果您未能获得任何必要的出口许可， Novell 对此不负任何责任。

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)。

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)。

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

本指南提供 Novell Sentinel Log Manager 及其安装的概述。

适用对象

本指南适用于 Novell Sentinel Log Manager 管理员和最终用户。

反馈

我们希望听到您对本手册和本产品中包含的其他文档的意见和建议。请使用联机文档各页底部的 “用户注释”功能，或转到 Novell 文档反馈网站 (http://www.novell.com/documentation/feedback.html)，并在该处输入您的注释。

其他文档

有关构建个人插件 （例如， JasperReports）的详细信息，请访问 Sentinel SDK 网页 (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel)。 Sentinel Log Manager 报告插件的构建环境与 Novell Sentinel 存档的内容相同。

有关 Sentinel 文档的详细信息，请参考 Sentinel 文档网站 (http://www.novell.com/documentation/sentinel61/index.html)。

有关配置 Sentinel Log Manager 的补充文档，请参阅 *《Sentinel Log Manager 1.1 管理指南》*。

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/)

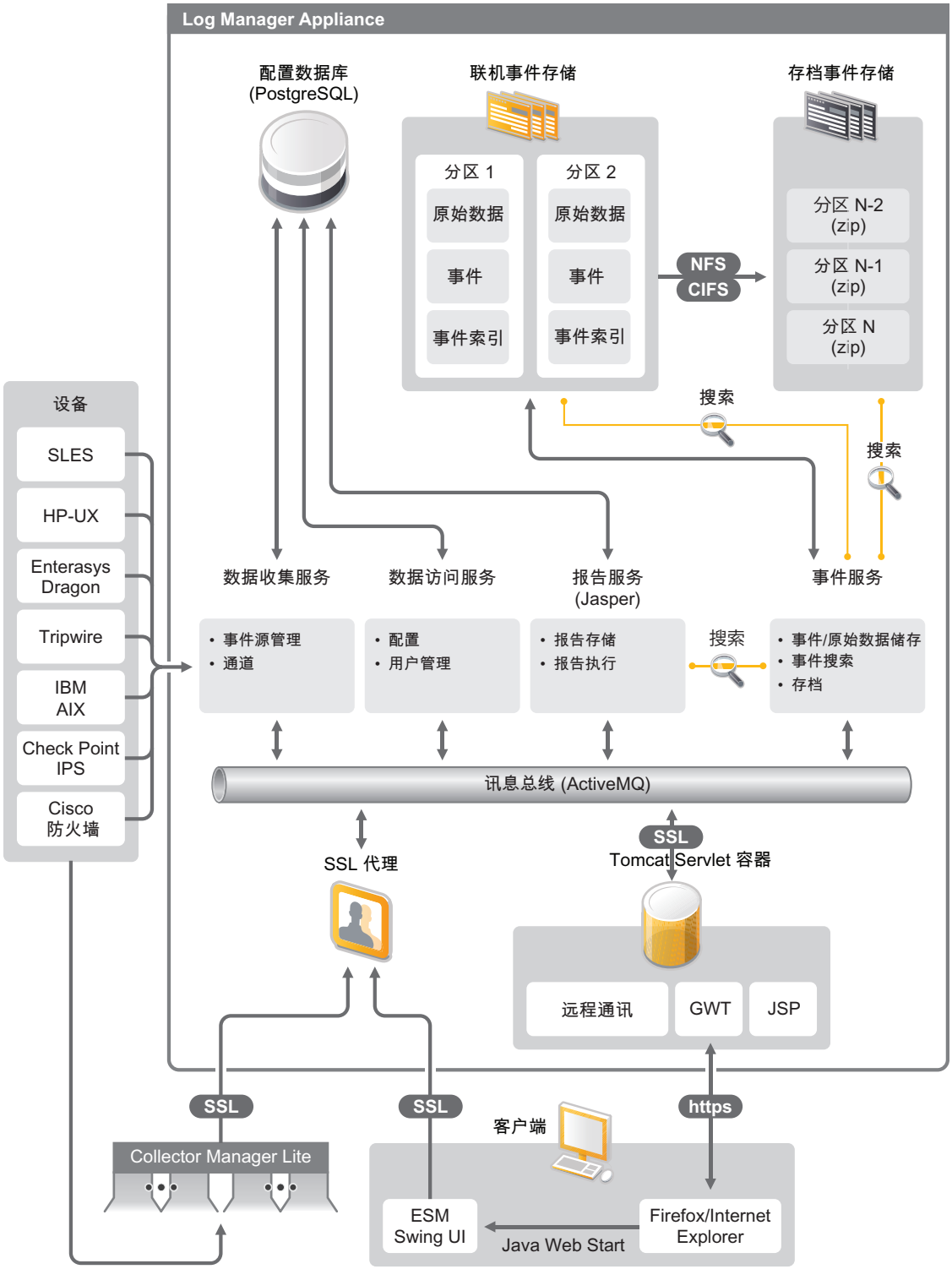
1 简介

Novell Sentinel Log Manager 从各种设备和应用程序收集并管理数据，包括入侵检测系统、防火墙、操作系统、路由器、 Web 服务器、数据库、交换机、大型机和防病毒事件源。Novell Sentinel Log Manager 为各种应用程序和设备提供高事件率处理、长期数据保留、基于策略的数据保留、区域数据集合以及简单的搜索和报告功能。

1.1 产品概述

Novell Sentinel Log Manager 1.1 向组织提供了一个灵活和可缩放的日志管理解决方案。Novell Sentinel Log Manager 是一个解决基本日志收集和管理难题的日志管理解决方案，它还提供了一个完整的解决方案，专门用于降低风险控制成本及复杂性，同时简化合规要求。

图 1-1 Novell Sentinel Log Manager 体系结构



Novell Sentinel Log Manager 具有以下功能：

- 使用分布式搜索功能，客户不仅可以在本地 Sentinel Log Manager 服务器上搜索收集的事件，还可以从一台集中式控制台中的一台或多台 Sentinel Log Manager 服务器上进行搜索。
- 预置合规报告，可为审核或取证分析简化生成合规报告任务。
- 通过非专有储存技术，客户可充分利用其现有的基础设施，从而进一步控制成本。
- 增强的基于浏览器的用户界面，支持收集、储存、报告和搜索日志数据，极大地简化了监视和管理任务。
- 通过新建组和用户权限功能实现 IT 管理员的粒度和高效控制及自定义，提高 IT 基础设施活动的透明度。

本节包括以下信息：

1.1.1 事件源

Novell Sentinel Log Manager 从事件源中收集数据，这些事件源可将日志生成到 syslog、Windows 事件日志、文件、数据库、 SNMP、 Novell Audit、安全性设备事件交换 (SDEE)、安全性检查点开放平台 (OPSEC) 和其他储存机制和协议。

若有合适的连接器解析来自这些事件源的数据，那么 Sentinel Log Manager 可支持所有事件源。 Novell Sentinel Log Manager 提供许多事件源的收集器。普通事件收集器从拥有合适连接器的未识别的事件源收集和处理数据。

您可以使用事件源管理界面为数据收集配置事件源。

有关受支持事件源的完整列表，请参阅第 2.6 节 “支持的事件源”（第 19 页）。

1.1.2 事件源管理

事件源管理界面可使您导入和配置 Sentinel 6.0 和 6.1 连接器和收集器。

您可以通过事件源管理窗口的实时视图执行以下任务：

- 通过使用配置向导，添加或编辑到事件源的连接。
- 查看到事件源的连接的实时状态。
- 将事件源配置导入至实时视图，或从实时视图导出事件源配置。
- 查看并配置随 Sentinel 安装的连接器和收集器。
- 从集中式储存库中导入连接器和收集器，或将连接器和收集器导出至集中式储存库。

- 通过配置的收集器和连接器监视数据流。
- 查看原始数据信息。
- 设计、配置和创建事件源层次的组件，并使用这些组件执行所需操作。

有关详细信息，请参阅 *《Sentinel 用户指南》*(http://www.novell.com/documentation/sentinel61/#admin) 的 “事件源管理”部分。

1.1.3 数据收集

Novell Sentinel Log Manager 通过连接器和收集器的帮助从已配置的事件源收集数据。

收集器是将各种事件源的数据解析为标准 Sentinel 事件结构的脚本，或在一些情况从外部数据源收集其他形式的数据。每个收集器应与一个兼容的连接器一起部署。连接器实现了 Sentinel Log Manager 收集器和事件或数据源之间的连接。

Novell Sentinel Log Manager 为 syslog 和 Novell Audit 提供了增强的基于 Web 的用户界面支持，可轻松地从不同的事件源收集日志。

Novell Sentinel Log Manager 会使用各种连接方式来收集数据：

- Syslog 连接器自动接受和配置通过用户数据报协议 (UDP)、传送控制协议 (TCP) 或安全传输层系统 (TLS) 发送数据的 syslog 数据源。
- 审计连接器自动接受和配置启用审计的 Novell 数据源。
- 文件连接器读取日志文件。
- SNMP 连接器接收 SNMP 陷阱。
- JDBC 连接器从数据库表进行读取。
- WMS 连接器访问台式机和服务器上的 Windows 事件日志。
- SDEE 连接器连接支持 SDEE 协议的设备 （如 Cisco 设备）。
- 检查点日志导出 API (LEA) 连接器在 Sentinel 收集器和检查点防火墙服务器之间实现集成。
- Sentinel 链接连接器接受来自其他 Novell Sentinel Log Manager 服务器的数据。
- 进程连接器接受来自输出事件日志的自编进程的数据。

您也可以购买一个附加许可证，以下载 SAP 和大型机操作系统的连接器。

要获取许可证，可拨打电话 1-800-529-3400，或联系 Novell 技术支持 (http://support.novell.com)。

有关配置连接器的详细信息，请参阅位于 Sentinel 内容网站 (http://support.novell.com/products/sentinel/sentinel61.html) 的连接器文档。

有关配置数据收集的详细信息，请参阅 *《Sentinel Log Manager 1.1 管理指南》*中的 “配置数据收集”。

注释：您必须始终下载和导入最新版本的收集器和连接器。更新的收集器和连接器将定期发布到 Sentinel 6.1 内容网站 (http://support.novell.com/products/sentinel/sentinel61.html)。连接器和收集器的更新包括修复、附加事件支持和性能改进。

1.1.4 收集器管理器

收集器管理器为 Sentinel Log Manager 提供一个灵活的数据收集点。 Novell Sentinel Log Manager 在安装时将在默认情况下安装一个收集器管理器。但是，您可以在您的网络中的合适位置远程安装收集器管理器，这些远程收集器管理器将运行连接器和收集器，并将收集的数据转发到 Novell Sentinel Log Manager，以便储存和处理。

有关安装附加收集器管理器的信息，请参阅安装附加收集器管理器。（第 47 页）。

1.1.5 数据储存

数据从数据收集组件流向数据储存组件。这些组件使用一个基于文件的数据储存和索引系统保存收集的设备日志数据，使用一个 PostgreSQL 数据库保存 Novell Sentinel Log Manager 配置数据。

数据以压缩格式储存在服务器文件系统上，然后储存到配置的位置以长期储存。数据可以储存到本地，也可以储存在远程安装的 SMB (CIFS) 或 NFS 共享上。数据文件基于数据保留策略中配置的时间表从本地和网络储存位置中删除。

若特定数据的数据保留时间已超过限制或可用空间降到指定磁盘空间值以下，您可以配置数据保留策略以从储存位置删除数据。

有关配置数据储存的详细信息，请参阅 “《Sentinel Log Manager 1.1 管理指南》”中的*配置数据储存*。

1.1.6 搜索和报告

搜索和报告组件帮助您在本地和网络数据储存和索引系统中搜索和报告事件日志数据。储存的事件数据可以进行一般搜索或针对特定事件字段 （如源用户名）进行搜索。这些搜索结果可以进一步精确或筛选，并作为报告模板保存供以后使用。

Sentinel Log Manager 带有预装报告。您也可以上载附加报告。您可以按时间表或必要时运行报告。

关于默认报告列表的信息，请参阅 *《Sentinel Log Manager 1.1 管理指南》*中的 “报告”。

有关搜索事件和生成报告的信息，请参阅 *《Sentinel Log Manager 1.1 管理指南》*中的 “搜索”和 “报告”。

1.1.7 Sentinel 链接

Sentinel 链接可用于在两个 Sentinel Log Manager 之间转发事件数据。使用一组分级的 Sentinel Log Manager，可以在多个区域位置保留完整的日志，同时将比较重要的事件转发至某个单独的 Sentinel Log Manager 以进行集中搜索和报告。

此外， Sentinel 链接可以将重要事件转发至 Novell Sentinel （一套完整的安全信息事件管理 (SIEM) 系统），从而实现高级关联、事件更新、高价值背景信息 （例如，服务器危急程度或来自身份管理系统的身份信息）注入。

1.1.8 基于 Web 的用户界面

Novell Sentinel Log Manager 带有一个基于 Web 的用户界面，以配置和使用 Log Manager。用户界面功能由 Web 服务器和一个基于 Java Web Start 的图形用户界面提供。所有用户界面通过使用一个加密连接与服务器进行通信。

您可以使用 Novell Sentinel Log Manager Web 界面执行以下任务：

- 搜索事件
- 将搜索准则另存为报告模板
- 查看和管理报告
- 起动事件源管理界面以为数据源而非 syslog 和 Novell 应用程序配置数据收集。（仅管理员）
- 配置数据转发 （仅管理员）
- 为远程安装下载 Sentinel 收集器管理器安装程序 （仅管理员）
- 查看事件源的健康状态 （仅管理员）
- 为 syslog 和 Novell 数据源配置数据收集 （仅管理员）
- 配置数据储存并查看数据库的状态 （仅管理员）
- 配置数据存档 （仅管理员）
- 配置关联操作以将匹配事件数据发送到输出通道 （仅管理员）
- 管理用户帐户和许可权限 （仅管理员）

1.2 安装概述

Novell Sentinel Log Manager 可以作为设备安装，也可安装在现有的 SUSE Linux Enterprise Server (SLES) 11 操作系统上。若 Sentinel Log Manager 作为设备安装， Log Manager 服务器则安装在 SLES 11 操作系统上。

默认情况下， Novell Sentinel Log Manager 安装以下组件：

- Sentinel Log Manager 服务器
- 通信服务器
- Web 服务器和基于 Web 的用户界面
- 报告服务器
- 收集器管理器

部分这些组件需要附加配置。

默认情况下， Novell Sentinel Log Manager 将安装一个收集器管理器。若您想要附加的收集器管理器，您可以在远程计算机上单独进行安装。有关详细信息，请参阅第 7 章 “安装附加收集器管理器。”（第 47 页）。

系统要求

2

以下部分描述 Novell Sentinel Log Manager 的硬件、操作系统、浏览器、受支持连接器和事件源兼容性要求。

2.1 硬件要求

2.1.1 Sentinel Log Manager 服务器

Novell Sentinel Log Manager 支持 64 位 Intel Xeon 和 AMD Opteron 处理器，但不支持 Itanium 处理器。

注释：这些要求针对平均事件大小为 300 字节。

保留 90 天在线数据的生产系统建议满足以下硬件要求：

表 2-1 *Sentinel Log Manager 硬件要求*

要求	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
压缩	高达 10:1	高达 10:1	高达 10:1
最大事件源数量	最多 1000	最多 1000	最多 2000
最大事件率	500	2500	7500
CPU	一个 Intel Xeon E5450 3-GHz （4 核） CPU 或 两个 Intel Xeon L5240 3-（2 核） CPU （共 4 核）	一个 Intel Xeon E5450 3-GHz （4 核） CPU 或 两个 Intel Xeon L5240 3-（2 核） CPU （共 4 核）	两个 Intel Xeon X5470 3.33-GHz （4 核） CPU （共 8 核）

要求	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
随机存取存储器 (RAM)	4 GB	4 GB	8 GB
储存	2 个 500 GB， 7200 RPM 驱动器 （硬件 RAID 带 256 MB 缓存， RAID 1）	2 个 1 TB， 7200 RPM 驱动器 （硬件 RAID 带 256 MB 缓存， RAID 1）	6 个 450 GB，15000 RPM 驱动器（硬件 RAID 带 512 MB 缓存， RAID 10）

注释：

- 一台计算机可以包括多个事件源。例如，一台 Windows 服务器可以包括两个 Sentinel 事件源，因为您想从 Windows 操作系统以及托管在该服务器的 SQL Server 数据库收集数据。
- 您必须将网络储存位置设置到一个外部多驱动器储存网络区域 (SAN) 或网络附属储存 (NAS) 上。
- 推荐的稳态量是最大许可的 EPS 的 80%。若达到此限制， Novell 建议您添加附加 Sentinel Log Manager 实例。

注释：最大事件源限制不是硬限制，而是基于 Novell 进行的性能测试和假定每个事件源每秒处于低平均事件率 （小于 3 EPS）。高 EPS 率将导致低可持续最大事件源。可使用等式（最大事件源）x （每个事件源平均 EPS） = 最大事件率算出特定的平均 EPS 率或事件源数的大致限制，只要最大事件源数不超过上面指定的限制。

2.1.2 收集器管理器服务器

- ❑ 一个 Intel Xeon L5240 3-GHz （2 核 CPU）
- ❑ 256 MB RAM
- ❑ 10 GB 可用磁盘空间。

2.1.3 数据储存要求评估

Sentinel Log Manager 用于长期保留原始数据，以遵守法律和其他要求。 Sentinel Log Manager 采用压缩形式以帮助您高效使用本地和网络储存空间。但是随着时间增长，储存要求将变得严重起来。

要克服大型储存系统的成本限制问题，您可以使用经济有效的数据储存系统来长期储存数据。基于磁带的储存系统是最常见并且经济有效的解决方案。但是，磁带不允许随机访问已储存的数据，而要执行快速搜索则必须支持随机访问。因此，希望有一种长期储存数据的混合方式，其中需要搜索的数据位于随机访问储存系统上，而需要保留且不搜索的数据保存到经济有效的备用系统上，如磁带。有关部署这种混合方式的说明，请参阅 *《Sentinel Log Manager 1.1 管理指南》*中的 “对长期数据储存使用顺序存取储存”。

要确定 Sentinel Log Manager 所需的随机存取储存空间的大小，首先估计您需要对多少天的数据执行定期搜索或运行报告。您应当在本地 Sentinel Log Manager 计算机上拥有足够的硬盘空间，或者在远程 Server Message Block (SMB) 协议、CIFS 协议、网络文件系统 (NFS) 或 SAN 上拥有足够空间，以用于 Sentinel Log Manager 储存数据。

您也应当拥有以下超出您的最低要求的附加硬盘空间。

- 考虑到高于预期的数据率。
- 要将数据从磁带复制回 Sentinel Log Manager，以在历史数据上执行搜索和报告。

使用以下公式估计储存数据所需的空间大小：

- **事件数据储存大小：**{ 天数 } x { 每秒事件数 } x { 平均事件字节大小 } x 0.000012 = 所需的储存大小 （以 GB 为单位）

  事件大小通常为 300-1000 字节。
- **原始数据储存大小：**{ 天数 } x { 每秒事件数 } x { 平均原始数据字节大小 } x 0.000012 = 所需的储存大小 （以 GB 为单位）

  syslog 讯息的平均原始数据大小通常是 200 字节。
- **总储存字节：**({ 事件平均字节大小 } + { 原始数据平均字节大小 }) x { 天数 } x { 每秒事件数 } x 0.000012 = 所需的总储存大小 （以 GB 为单位）

注释：这些数字仅仅是基于您的事件数据大小和压缩数据的大小而所做的估计。

以上公式计算出在外部储存系统上储存完全压缩的数据所需的最低储存空间。当本地储存装满时， Sentinel Log Manager 将数据从本地 （部分压缩）压缩并移动到外部 （完全压缩）储存系统中。因此，估计外部储存空间需求对于数据保留变得至关重要。要为最近的数据改善搜索和报告性能，您可以将本地储存空间提高到 Sentinel Log Manager 的硬件要求以上；但是并不要求这样做。

您还可以使用以上公式确定长期数据储存系统 （如磁带）所需的储存空间。

2.1.4 虚拟环境

Sentinel Log Manager 经过广泛测试，完全支持 VMware ESX 服务器。虚拟环境中的性能结果类似于在物理计算机上获取的测试结果，但是虚拟环境应提供与物理计算机上建议的相同的内存、 CPU、磁盘空间和 I/O。

2.2 支持的操作系统

本部分包含 Sentinel Log Manager 服务器和远程收集器管理器的受支持操作系统的信息。

- 第 2.2.1 节 “Sentinel Log Manager”（第 17 页）
- 第 2.2.2 节 “收集器管理器”（第 18 页）

2.2.1 Sentinel Log Manager

本部分仅当将在现有的操作系统上安装 Sentinel Log Manager 时适用。

- ❑ 64 位 SUSE Linux Enterprise Server 11。
- ❑ 高性能文件系统。

  注释：所有 Novell 测试都使用 ext3 文件系统进行。

2.2.2 收集器管理器

您可以在以下操作系统上安装附加收集器管理器：

- Linux （第 18 页）
- Windows （第 18 页）

Linux

- ❑ SUSE Linux Enterprise Server 10 SP2 （32 位和 64 位）
- ❑ SUSE Linux Enterprise Server 11 （32 位和 64 位）

Windows

- ❑ Windows Server 2003 （32 位和 64 位）
- ❑ Windows Server 2003 SP2 （32 位和 64 位）
- ❑ Windows Server 2008 （64 位）

2.3 支持的浏览器

Sentinel Log Manager 界面在以下受支持的浏览器上对 1280 x 1024 或更高分辨率显示进行了优化：

- 第 2.3.1 节 “Linux”（第 18 页）
- 第 2.3.2 节 “Windows”（第 18 页）

2.3.1 Linux

- ❑ Mozilla Firefox 3.6

2.3.2 Windows

- ❑ Mozilla Firefox 3 （3.6 最佳）
- ❑ Microsoft Internet Explorer 8 （8.0 最佳）

Internet Explorer 8 的先决条件

- 若 Internet 安全级别设置为高，在登录到 Novell Sentinel Log Manager 以后将仅显示空白页。要解决此问题，请导航到*工具* > *Internet 选项* > *安全选项卡* > *可信站点*。单击*站点*按钮，将 Sentinel Log Manager 网站添加到受信任站点列表。
- 确保*工具* > *兼容性视图*选项未选中。
- 若*文件下载的自动提示*选项未启用，浏览器可能阻止文件下载弹出窗口。要解决此问题，导航到*工具* > *Internet 选项* > *安全选项卡* > *自定义级别*，然后向下拖动到下载部分，选择*启用*以启用*文件下载的自动提示*选项。

2.4 受支持的虚拟环境

- ❑ VMware ESX/ESXi 3.5/4.0 或更高

- ❑ VMPlayer 3 （仅演示版）
- ❑ Xen 3.1.1

2.5 受支持的连接器

Sentinel Log Manager 支持所有 Sentinel 和 Sentinel RD 支持的连接器。

- ❑ 审计连接器
- ❑ 检查点 LEA 进程连接器
- ❑ 数据库连接器
- ❑ 数据生成器连接器
- ❑ 文件连接器
- ❑ 进程连接器
- ❑ Syslog 连接器
- ❑ SNMP 连接器
- ❑ SDEE 连接器
- ❑ Sentinel 链接连接器
- ❑ WMS 连接器
- ❑ 大型机连接器
- ❑ SAP 连接器

注释：大型机和 SAP 连接器要求一个单独许可证。

2.6 支持的事件源

Sentinel Log Manager 支持各种设备和应用程序，包括入侵检测系统、防火墙、操作系统、路由器、 Web 服务器、数据库、交换机、大型机和防病毒事件源。来自事件源的数据会进行不同程度的解析和标准化，具体取决于数据处理时是使用普通事件收集器将整个事件有效负载放入公共字段，还是使用设备特定的收集器将数据解析到单个字段中。

Sentinel Log Manager 支持以下事件源：

- ❑ Cisco 防火墙 （6 和 7）
- ❑ Cisco Switch Catalyst 6500 系列 (CatOS 8.7)
- ❑ Cisco Switch Catalyst 6500 系列 (IOS 12.2SX)
- ❑ Cisco Switch Catalyst 5000 系列 (CatOS 4.x)
- ❑ Cisco Switch Catalyst 4900 系列 (IOS 12.2SG)
- ❑ Cisco Switch Catalyst 4500 系列 (IOS 12.2SG)
- ❑ Cisco Switch Catalyst 4000 系列 (CatOS 4.x)
- ❑ Cisco Switch Catalyst 3750 系列 (IOS 12.2SE)
- ❑ Cisco Switch Catalyst 3650 系列 (IOS 12.2SE)
- ❑ Cisco Switch Catalyst 3550 系列 (IOS 12.2SE)
- ❑ Cisco Switch Catalyst 2970 系列 (IOS 12.2SE)

- Cisco Switch Catalyst 2960 系列 (IOS 12.2SE)
- Cisco VPN 3000 （4.1.5、 4.1.7 和 4.7.2）
- Extreme Networks Summit X650 （含 ExtremeXOS 12.2.2 和早期版本）
- Extreme Networks Summit X450a （含 ExtremeXOS 12.2.2 和早期版本）
- Extreme Networks Summit X450e （含 ExtremeXOS 12.2.2 和早期版本）
- Extreme Networks Summit X350 （含 ExtremeXOS 12.2.2 和早期版本）
- Extreme Networks Summit X250e （含 ExtremeXOS 12.2.2 和早期版本）
- Extreme Networks Summit X150 （含 ExtremeXOS 12.2.2 和早期版本）
- Enterasys Dragon （7.1 和 7.2）
- 普通事件收集器
- HP HP-UX （11iv1 和 11iv2）
- IBM AIX （5.2、 5.3 和 6.1)
- Juniper Netscreen Series 5
- McAfee Firewall Enterprise
- McAfee 网络安全平台 （2.1、 3.x 和 4.1）
- McAfee VirusScan Enterprise （8.0i、 8.5i 和 8.7i）
- McAfee ePolicy Orchestrator （3.6 和 4.0）
- McAfee AV Via ePolicy Orchestrator 8.5
- Microsoft Active Directory （2000、 2003 和 2008）
- Microsoft SQL Server （2005 和 2008）
- Nortel VPN （1750、 2700、 2750 和 5000）
- Novell Access Manager 3.1
- Novell Identity Manager 3.6.1
- Novell Netware 6.5
- Novell Modular Authentication Services 3.3
- Novell Open Enterprise Server 2.0.2
- Novell Privileged User Manager 2.2.1
- Novell Sentinel Link 1
- Novell SUSE Linux Enterprise Server
- 在 Novell 支持网站 (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~) 可以获取包含 eDirectory 工具增补程序的 Novell eDirectory 8.8.3
- Novell iManager 2.7
- Red Hat Enterprise Linux
- Sourcefire Snort （2.4.5、 2.6.1、 2.8.3.2 和 2.8.4）
- Snare for Windows Intersect Alliance （3.1.4 和 1.1.1）
- Sun Microsystems Solaris 10
- Symantec AntiVirus Corporate Edition （9 和 10）
- TippingPoint 安全管理系统 （2.1 和 3.0）

- ❑ Websense Web Security 7.0
- ❑ Websense Web Filter 7.0

注释：要从 Novell iManager 和 Novell Netware 6.5 事件源启用数据收集，请在事件源管理界面中为每个事件源添加一个收集器和一个子连接器 （审计连接器）实例。当完成此操作后，这些事件源将显示在 Sentinel Log Manager Web 控制台中的 *Audit 服务器*选项卡下。

支持附加事件源的收集器可从 Sentinel 6.1 内容网站 (http://support.novell.com/products/sentinel/sentinel61.html) 获取，也可使用 Sentinel 插件 SDK 网站 (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) 上提供的 SDK 插件进行构建。

在现有的 SLES 11 系统上进行安装

3

这部分描述使用应用程序安装程序在现有的 SUSE Linux Enterprise Server (SLES) 11 系统上安装 Sentinel Log Manager 的过程。您可以使用多种方式安装 Sentinel Log Manager 服务器：标准安装过程、自定义安装过程或无提示安装过程，其中无提示安装过程将无需用户输入，使用默认值进行。您还可以作为非根用户安装 Sentinel Log Manager。

若您选择自定义安装方法，则可以选择使用许可证密钥安装产品，并选择一个鉴定选项。除数据库鉴定之外，您还可以为 Sentinel Log Manager 设置 LDAP 鉴定。当您为 LDAP 鉴定配置 Sentinel Log Manager 时，用户可以使用其 Novell eDirectory 或 Microsoft Active Directory 证书登录到服务器。

若您希望在部署中安装多个 Sentinel Log Manager 服务器，则可以在一个配置文件中记录这些安装选项，然后使用该文件运行一个无人照管的安装。有关详细信息，请参阅第 3.4 节 “无提示安装”（第 26 页）。

在继续安装之前，请确保已满足第 2 章 “系统要求”（第 15 页）中指定的最低要求。

3.1 开始之前的准备工作

- ❑ 确保您的硬件和软件满足第 2 章 “系统要求”（第 15 页）中提到的最低要求。
- ❑ 以 hostname -f 命令返回一个有效主机名这种方式配置操作系统。
- ❑ 从 Novell 客户关怀中心 (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) 获取许可证密钥以安装授权的版本。
- ❑ 使用网络时间协议 (NTP) 同步时间。
- ❑ 安装以下操作系统命令：
  - mount
  - umount
  - ID
  - df
  - du
  - sudo
- ❑ 确保以下端口在防火墙中打开：

  TCP 8080、 TCP 8443、 TCP 61616、 TCP 10013、 TCP 1289、 TCP 1468、 TCP 1443 和 UDP 1514

3.2 标准安装

标准安装过程将安装含所有默认选项和一个 90 天评估许可证的 Sentinel Log Manager。

1. 从 Novell 下载站点下载和复制安装文件。
2. 作为根登录到要安装 Sentinel Log Manager 的服务器。
3. 指定以下命令从 tar 文件抽取安装文件：

   ```
   tar xfz <install_filename>
   ```

   使用安装文件实际名称替换 <*install_filename*>。
4. 指定以下命令运行 install-slm 脚本，以安装 Sentinel Log Manager：

   ```
   ./install-slm
   ```

   若您希望在多个系统上安装 Sentinel Log Manager，则可以在一个文件中记录您的安装选项。您可以使用此文件在其他无人照管的系统上安装 Sentinel Log Manager。要记录您的安装选项，请指定以下命令：

   ```
   ./install-slm -r responseFile
   ```
5. 要使用选择的语言继续，请选择该语言旁边的编号。

   最终用户许可证协议将以选定的语言显示。
6. 阅读最终用户许可证协议并输入 yes 或 y 接受此许可证，然后继续安装。

   安装将开始安装所有的 RPM 包。该安装完成可能需要几秒钟的时间。

   若不存在，安装将创建一个 novell 组和一个 novell 用户。
7. 当收到提示时，请指定标准安装选项以继续。

   安装将采用安装程序附带的 90 天评估许可证密钥继续进行。使用此许可证密钥可以激活所有产品功能，并获得 90 天的试用期。在试用期内或试用期结束后，您随时可以使用购买的许可证密钥替换评估许可证。
8. 指定管理员用户的口令。
9. 确认管理员用户的口令。

   安装程序将选择*仅鉴定数据库*方法并继续安装。

   Sentinel Log Manager 安装完成并且服务器将启动。在安装完成之后系统执行一次性初始化时，所有服务启动可能需要大约 5-10 分钟。在登录到服务器之前请等候这段时间。
10. 要登录到 Sentinel Log Manager 服务器，请使用安装输出中指定的 URL。此 URL 类似于 https://10.0.0.1:8443/novelllogmanager。

    有关登录到该服务器的详细信息，请参阅 第 5 章 “登录到 Web 界面”（第 39 页）。
11. 要配置事件资源以向 Sentinel Log Manager 发送数据，请参阅 *《Sentinel Log Manager 1.1 管理指南》*中的 “配置数据收集”。

3.3 自定义安装

若您选择自定义安装方法，则可以选择使用许可证密钥安装产品，并选择一个鉴定选项。除数据库鉴定之外，您还可以为 Sentinel Log Manager 设置 LDAP 鉴定。当您为 LDAP 鉴定配置 Sentinel Log Manager 时，用户可以使用 LDAP 目录证书登录到服务器。

若您在安装过程中未为 LDAP 鉴定配置 Sentinel Log Manager，可根据需要在安装之后配置鉴定。要在安装之后设置 LDAP 鉴定，请参阅 *《Sentinel Log Manager 1.1 管理指南》*中的“LDAP 鉴定”。

1. 从 Novell 下载站点下载和复制安装文件。
2. 作为根登录到要安装 Sentinel Log Manager 的服务器。
3. 指定以下命令从 tar 文件抽取安装文件：

   ```
   tar xfz <install_filename>
   ```

   使用安装文件实际名称替换 <*install_filename*>。
4. 指定以下命令运行 install-slm 脚本，以安装 Sentinel Log Manager：

   ```
   ./install-slm
   ```
5. 要使用选择的语言继续，请选择该语言旁边的编号。

   最终用户许可证协议将以选定的语言显示。
6. 阅读最终用户许可证协议并输入 yes 或 y 接受此许可证，然后继续安装。

   安装将开始安装所有的 RPM 包。该安装完成可能需要几秒钟的时间。

   若不存在，安装将创建一个 novell 组和一个 novell 用户。
7. 当收到提示时，请指定自定义安装选项以继续。
8. 当提示指定许可证密钥选项时，请输入 2 以为已购买的产品指定许可证密钥。
9. 指定许可证密钥，然后按 Enter。

   有关许可证密钥的详细信息，请参阅 *《Sentinel Log Manager 1.1 管理指南》*中的“管理许可证密钥”。
10. 指定管理员用户的口令。
11. 确认管理员用户的口令。
12. 指定数据库管理员口令 (dbauser)。
13. 确定数据库管理员口令 (dbauser)。
14. 您可以为以下服务配置指定范围内的任何有效端口号：
    - Web 服务器
    - Java 消息服务
    - 客户端代理服务
    - 数据库服务
    - 代理内部网关

    若您想以默认端口继续，请输入选项 6 以继续自定义安装。
15. 指定通过一个外部 LDAP 目录鉴定用户的选项。
16. 指定 LDAP 服务器的 IP 地址或主机名。

    默认值为 localhost。但是，您不可将 LDAP 服务器安装在与 Sentinel Log Manager 服务器相同的计算机上。
17. 选择以下 LDAP 连接类型之一：
    - **SSL/TSL LDAP 连接：**为鉴定在浏览器和服务器之间建立一个安全连接。输入 1 以指定此选项。
    - **未加密 LDAP 连接：**建立一个未加密连接。输入 2 以指定此选项。

18 指定 LDAP 服务器端口号。默认 SSL 端口是 636，默认非 SSL 端口是 389。

19 （有条件）若您已选择 SSL/TSL LDAP 连接，则指定 LDAP 服务器证书是否经著名的 CA 签名。

20 （有条件）若您指定了 n，则指定 LDAP 服务器证书的文件名。

21 选择您是否想在 LDAP 目录上执行匿名搜索：

- **在 LDAP 目录上执行匿名搜索：**Sentinel Log Manager 服务器基于指定的用户名在 LDAP 目录上执行一次*匿名搜索*，以获取相应 LDAP 用户的判别名 (DN)。输入 1 以指定此方法。
- **不要在 LDAP 目录上执行匿名搜索：**输入 2 以指定此选项。

22 （有条件）若您已选择匿名搜索，则指定搜索属性并将其移动到步骤 25。

23 （有条件）若您在步骤 21 中未选择匿名搜索，请指定您是否在使用 Microsoft Active Directory。

对于 Active Directory， userPrincipalName 属性的值形式是 userName@domainName，可以在搜索 LDAP 用户对象之前选择性用于鉴定用户，无需输入用户 DN。

24 （有条件）若希望对 Active Directory 使用以上方法，请指定域名。

25 指定基础 DN。

26 按 y 指定提供的选项正确，否则按 n 并更改配置。

27 要登录到 Sentinel Log Manager 服务器，请使用安装输出中指定的 URL。此 URL 类似于 https://10.0.0.1:8443/novelllogmanager。

有关登录到该服务器的详细信息，请参阅 第 5 章 “登录到 Web 界面”（第 39 页）。

3.4 无提示安装

若需要在部署中安装多个 Sentinel Log Manager 服务器， Sentinel Log Manager 无提示或无人照管安装非常有用。在此情况下，您可以在第一次安装期间记录安装参数，然后在所有其他服务器上运行记录的文件。

1 从 Novell 下载站点下载和复制安装文件。

2 作为根登录到要安装 Sentinel Log Manager 的服务器。

3 指定以下命令从 tar 文件抽取安装文件：

```
tar xfz <install_filename>
```

使用安装文件实际名称替换 <*install_filename*>。

4 指定以下命令运行 install-slm 脚本以在无提示模式下安装 Sentinel Log Manager：

```
./install-slm -u responseFile
```

有关创建响应文件的信息，请参阅第 3.2 节 “标准安装”（第 24 页）。安装将使用响应文件中储存的值继续。

5 要登录到 Sentinel Log Manager 服务器，请使用安装输出中指定的 URL。此 URL 类似于 https://10.0.0.1:8443/novelllogmanager。

有关登录到该服务器的详细信息，请参阅 第 5 章 “登录到 Web 界面”（第 39 页）。

6 要配置事件资源以向 Sentinel Log Manager 发送数据，请参阅 “《Sentinel Log Manager 1.1 管理指南》”中的 “配置数据收集”。

3.5 非根安装

如果组织政策不允许以根身份运行 Sentinel Log Manager 完整安装，大多数安装步骤可使用其他用户身份安装。

1. 从 Novell 下载站点下载和复制安装文件。
2. 指定以下命令从 tar 文件抽取安装文件：

   ```
   tar xfz <install_filename>
   ```

   使用安装文件实际名称替换 <*install_filename*>。
3. 以根身份登录到要使用根身份安装 Sentinel Log Manager 的服务器。
4. 指定以下命令：

   ```
   ./bin/root_install_prepare
   ```

   此时将显示要使用根权限执行的一列命令。

   若不存在，还将创建一个 novell 组和一个 novell 用户。
5. 接受命令列表。

   显示的命令将被执行。
6. 指定以下命令以更改为新创建的非根 novell 用户：novell：

   su novell
7. 指定以下命令：

   ```
   ./install-slm
   ```
8. 要使用选择的语言继续，请选择该语言旁边的编号。

   最终用户许可证协议将以选定的语言显示。
9. 阅读最终用户许可证协议并输入 yes 或 y 接受此许可证，然后继续安装。

   安装将开始安装所有的 RPM 包。该安装完成可能需要几秒钟的时间。
10. 将提示您指定安装模式。
    - 若选择标准安装，请遵循第 3.2 节 “标准安装”（第 24 页）中的步骤 8 至步骤 11。
    - 若选择自定义安装，请遵循第 3.3 节 “自定义安装”（第 24 页）中的步骤 8 至步骤 23。

    Sentinel Log Manager 安装结束，服务器将启动。
11. 指定以下命令以更改为根用户：

    ```
    su root
    ```
12. 指定以下命令以结束安装：

    ./bin/root_install_finish
13. 要登录到 Sentinel Log Manager 服务器，请使用安装输出中指定的 URL。此 URL 类似于 https://10.0.0.1:8443/novelllogmanager。

    有关登录到该服务器的详细信息，请参阅 第 5 章 “登录到 Web 界面”（第 39 页）。

安装设备

4

Novell Sentinel Log Manager 设备是在 SUSE Studio 的基础上构建的一个准备运行式软件设备，整合了强化的 SUSE Linux Enterprise Server (SLES) 11 操作系统和 Novell Sentinel Log Manager 软件集成更新服务，以提供简洁无缝的用户体验，并使客户可利用现有的投资。该软件设备可在硬件上或虚拟环境中安装。

4.1 开始之前的准备工作

- 确保符合硬件要求。有关详细信息，请参阅第 2.1 节 “硬件要求”（第 15 页）。
- 从 Novell 客户关怀中心 (http://www.novell.com/center) 获取许可证密钥以安装授权的版本。
- 从 Novell 客户关怀中心 (http://www.novell.com/center) 获取注册码以注册软件更新。
- 使用网络时间协议 (NTP) 同步时间。
- （有条件）如果计划使用 VMware，请确保拥有 VMware 转换器，以同时将图像上传到 VMware ESX 服务器并转换成可在 ESX 服务器上运行的格式。

4.2 使用的端口

注意 Novell Sentinel Log Manager 设备使用以下端口进行通信，一些已在防火墙中打开。

4.2.1 在防火墙中打开的端口

表 4-1 *Sentinel Log Manager 使用的网络端口*

端口	说明
TCP 1289	用于 Novell Audit 连接。
TCP 289	转发到 1289 以进行 Novell Audit 连接。
TCP 22	用于确保壳层访问 Sentinel Log Manager 设备的安全。

端口	说明
UDP 1514	用于 syslog 讯息。
UDP 514	转发到 1514 以用于 syslog 讯息。
TCP 8080	用于 HTTP 通信。还被 Sentinel Log Manager 设备用于更新服务。
TCP 80	转发到 8080 用于 Sentinel Log Manager 的 Web 服务器的 HTTP 通信。还被 Sentinel Log Manager 设备用于更新服务。
TCP 8443	用于 HTTPS 通信。还被 Sentinel Log Manager 设备用于更新服务。
TCP 1443	用于 SSL 加密 syslog 讯息。
TCP 443	转发到 8443 用于 Sentinel Log Manager 的 Web 服务器的 HTTPS 通信。还被 Sentinel Log Manager 设备用于更新服务。
TCP 61616	用于收集器管理器和服务器之间的通信。
TCP 10013	由事件源管理用户界面 SSL 代理使用。
TCP 54984	由 Sentinel Log Manager 设备管理控制台 (WebYaST) 使用。
TCP 1468	用于 syslog 讯息。

4.2.2 本地使用的端口

表 4-2 用于本地通信的端口

端口	说明
TCP 61617	用于 Web 服务器和服务器之间的内部通信。
TCP 5556	用于环路接口的内部通信，internal_gateway_server 和 internal_gateway 之间。用于代理引擎和收集器管理器之间的通信。
TCP 5432	用于 PostgreSQL database 数据库。无需默认打开此端口。但若使用 Sentinel SDK 开发报告，则必须打开此报告。有关详细信息，请参阅 Sentinel 插件 SDK 网站 (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)。
两个附加的随机选择的 TCP 端口	用于代理引擎和收集器管理器之间的通信。
TCP 8005	用于与 Tomcat 进程的内部通信。
TCP 32000	用于代理引擎和收集器管理器之间的通信。

4.3 安装 VMware 设备

要从 VMware ESX 服务器运行设备映像，请在服务器上导入并安装该设备映像。

1 下载 VMware 设备安装文件。

正确的 VMware 设备文件的文件名中有 vmx。例如，
Sentinel_Log_Manager_1.1.0.0_64_VMX.x86_64-0.777.0.vmx.tar.gz

2 建立一个设备映像可以安装至的 ESX 数据储存。

3 以管理员身份登录到要安装该设备的服务器。

4 指定以下命令从安装了 VM 转换器的机器抽取压缩的设备映像。

tar zxvf <*install_file*>

使用实际文件名替换 <*install_file*>。

5 要将 VMware 映像导入到 ESX 服务器，请使用 VMware 转换器并按照安装向导中的屏幕指导操作。

6 登录到 ESX 服务器机器。

7 选择导入的设备 VMware 映像，然后单击*开机*图标。

8 选择您的语言，然后单击 *下一步*。

9 选择键盘布局，然后单击 *下一步*。

10 阅读并接受 Novell SUSE Enterprise Server 软件许可证协议。

11 阅读并接受 Novell Sentinel Log Manager 最终用户许可证协议。

12 在主机名和域名屏幕中，指定主机名和域名。确保选择了 *将主机名写入到 /etc/hosts* 选项。

13 选择 *下一步*。主机名配置即保存。

14 执行以下步骤之一：

- 要使用当前的网络连接设置，请选择 *网络配置 II* 中的 *使用以下配置*。
- 要更改网络连接设置，请选择 *更改*。

15 设置时间和日期，单击 *下一步*，然后单击 *完成*。

注释：要在安装后更改 NTP 配置，请从设备命令行使用 YaST。可使用 WebYast 更改时间和日期，但不是 NTP 配置。

如果在安装后时间立即显示未同步，请运行以下命令重新启动 NTP：

```
rcntp restart
```

---

16 设置 Novell SUSE Enterprise Server 根口令，然后单击 *下一步*。

17 设置根口令，然后单击 *下一步*。

18 设置 Sentinel Log Manager Admin 口令和 dbauser 口令，然后单击 *下一步*。

19 选择 *下一步*。网络连接设置即保存。

安装将继续并完成。记录控制台中显示的设备 IP 地址。

20 进行第 4.6 节 “设备的安装后设置”（第 34 页）。

4.4 安装 Xen 设备

1 下载 Xen 虚拟设备安装文件并复制到 /var/lib/xen/images。

正确的 Xen 虚拟设备文件名包含 xen。例如， Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.xen.tar.gz

2 使用以下命令解压该文件：

```
tar -xvzf <install_file>
```

使用安装文件实际名称替换 <*install_file*>。

3 更改到新的安装目录。此目录有以下文件：

- <*file_name*>.raw 映像文件。
- <*file_name*>.xenconfig 文件

4 使用一个文本编辑器打开 <*file_name*>.xenconfig 文件。

5 按如下操作修改该文件：

在磁盘设置中指定 .raw 文件的完整路径。

指定您的网络配置的网桥设置。例如， "bridge=br0" 或 "bridge=xenbr0"。

指定名称和内存设置的值。

例如：

```
# -*- mode: python; -*-
name="Sentinel_Log_Manager_1.1.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.1.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

6 在修改了 <*filename*>.xenconfig 文件后，指定以下命令以创建 VM：

xm create <*file_name*>.xenconfig

7 （可选）要验证 VM 是否创建，请指定以下命令：

xm list

VM 将显示在列表中。

例如，若在 .xenconfig 文件中配置了 name=” Sentinel_Log_Manager_1.1.0.0_64”，则 VM 将显示该名称。

8 要开始此安装，请指定以下命令：

xm console <*vm name*>

使用 .xenconfig 文件的名称设置中指定的名称替换 <*vm_name*>，该名称也是步骤 7 中返回的值。例如：

xm console Sentinel_Log_Manager_1.1.0.0_64

9 选择您的语言，然后单击 *下一步*。

10 选择键盘布局，然后单击 *下一步*。

11 阅读并接受 Novell SUSE Enterprise Server 软件许可证协议。

12 阅读并接受 Novell Sentinel Log Manager 最终用户许可证协议。

13 在主机名和域名屏幕中，指定主机名和域名。确保选择了 *将主机名写入 /etc/hosts* 选项。

14 选择 *下一步*。主机名配置即保存。

15 执行以下步骤之一：

- 要使用当前的网络连接设置，请选择 *网络配置 II* 中的 *使用以下配置*。
- 要更改网络连接设置，请选择 *更改*。

16 设置时间和日期，请单击 *下一步*，然后单击 *完成*。

注释：要在安装后更改 NTP 配置，请从设备命令行使用 YaST。可使用 WebYast 更改时间和日期，但不是 NTP 配置。

如果在安装后时间立即显示未同步，请运行以下命令重新启动 NTP：

```
rcntp restart
```

17 设置 Novell SUSE Enterprise Server 根口令，然后单击 *下一步*。

18 设置 Sentinel Log Manager Admin 口令和 dbauser 口令，然后单击 *下一步*。

安装将继续并完成。记录控制台中显示的设备 IP 地址。

19 进行第 4.6 节 “设备的安装后设置”（第 34 页）。

4.5 在硬件上安装设备

在硬件上安装设备前，确保从支持的站点下载了设备 ISO 磁盘映像并进行了解压，通过 DVD 方式提供。

1 从已插入此 DVD 的 DVD 驱动器启动物理计算机。

2 使用安装向导的屏幕指导。

3 通过在启动菜单选择顶部安装来运行 DVD。

4 阅读并接受 Novell SUSE Enterprise Server 软件许可证协议。

5 阅读并接受 Novell Sentinel Log Manager 最终用户许可证协议。

6 选择 *下一步*。

7 在主机名和域名屏幕中，指定主机名和域名。

确保选择了 *将主机名写入到 /etc/hosts* 选项。

8 选择 *下一步*。主机名配置即保存。

9 执行以下步骤之一：

- 要使用当前的网络连接设置，请选择网络配置 II 屏幕中的 *使用以下配置*。
- 要更改网络连接设置，请选择 *更改*。

10 选择 *下一步*。网络连接设置即保存。

11 设置时间和日期，然后单击 *下一步*。

注释：要在安装后更改 NTP 配置，请从设备命令行使用 YaSTfrom。可使用 WebYast 更改时间和日期，但不是 NTP 配置。

如果在安装后时间立即显示未同步，请运行以下命令重新启动 NTP：

```
rcntp restart
```

12 设置根口令，然后单击 *下一步*。

13 设置 Sentinel Log Manager Admin 口令和 dbauser 口令，然后单击 *下一步*。

14 在控制台输入用户名和口令以登录设备。

用户名的默认值是 root，口令是 password。

15 要在物理服务器上安装设备，请运行以下命令：

```
/sbin/yast2 live-installer
```

安装将继续并完成。记录控制台中显示的设备 IP 地址。

16 进行第 4.6 节 “设备的安装后设置”（第 34 页）。

4.6 设备的安装后设置

登录到设备 Web 控制台并初始化软件：

1 打开 Web 浏览器并登录到 https://*<IP 地址>*:*8443*。此时将显示 Sentinel Log Manager Web 页面。

安装完成和服务器重新启动后，设备控制台将显示设备的 IP 地址。

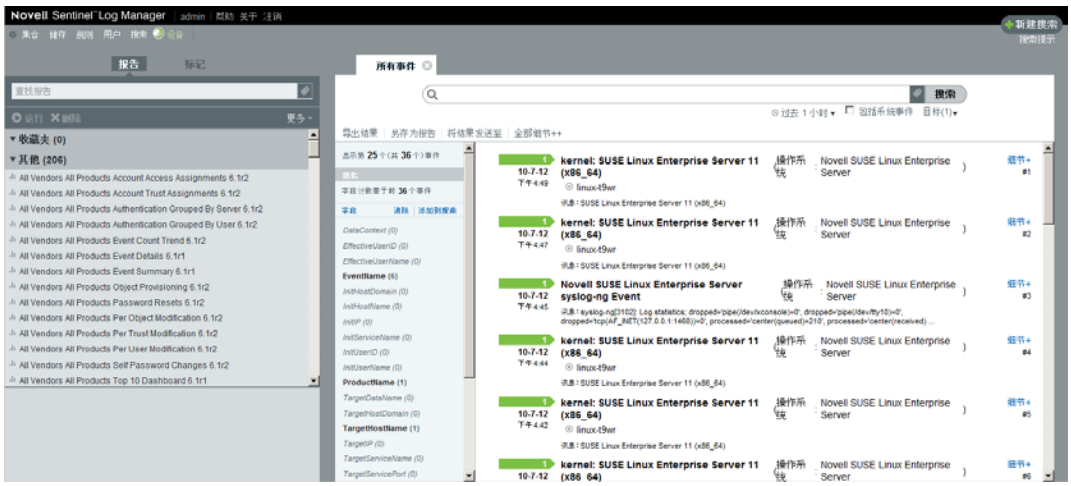
2 您可以配置 Sentinel Log Manager 设备用于数据储存和数据收集。有关配置设备的更多信息，请参阅 *《Sentinel Log Manager 1.1 管理指南》*。

3 要注册更新，请参阅第 4.8 节 “注册更新”（第 36 页）。

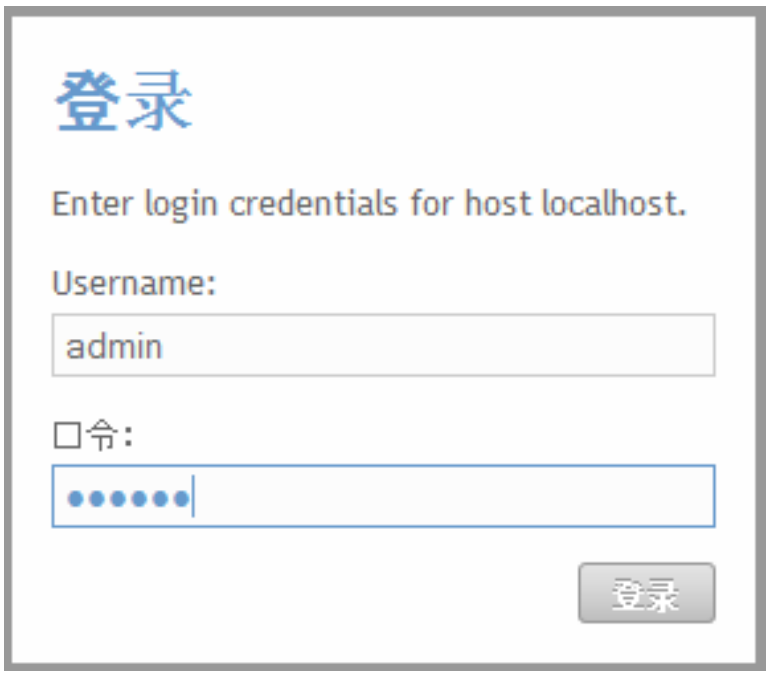
4.7 配置 WebYaST

Novell Sentinel Log Manager 设备用户界面配有 WebYaST。WebYaST 是一个基于 Web 的远程控制台，用于控制基于 SUSE Linux Enterprise 的设备。您可以使用 WebYaST 访问、配置和监视 Sentinel Log Manager 设备。以下过程简短描述了配置 WebYaST 的步骤。有关详细配置信息，请参阅 WebYaST 用户指南 (http://www.novell.com/documentation/webyast/)。

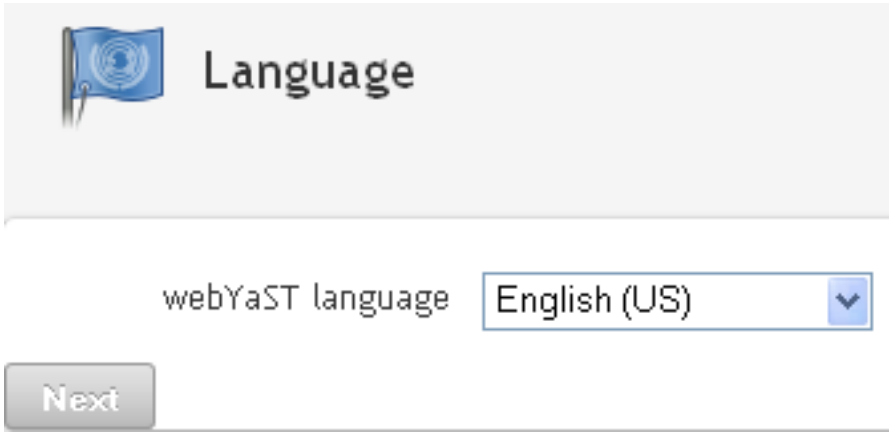
1 登录到 Sentinel Log Manager 设备。



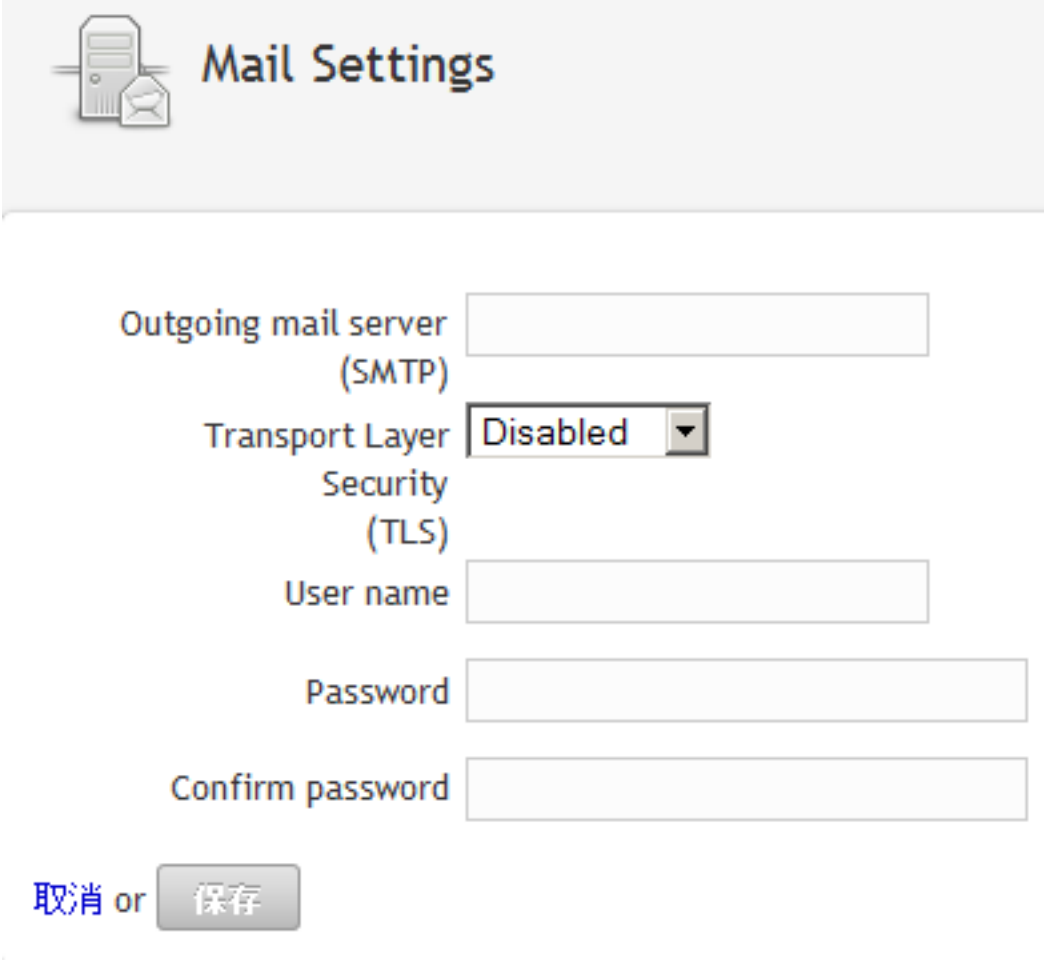
2 单击 *设备*。



3 指定系统的登录凭证，然后单击*登录*。



4 选择您的语言，然后单击*下一步*。



5 指定配置邮件服务器的详细信息，然后单击*保存*。

此时即会显示注册页。

6 配置 Sentinel Log Manager 服务器以按照第 4.8 节 “注册更新”（第 36 页）中的描述接收更新。

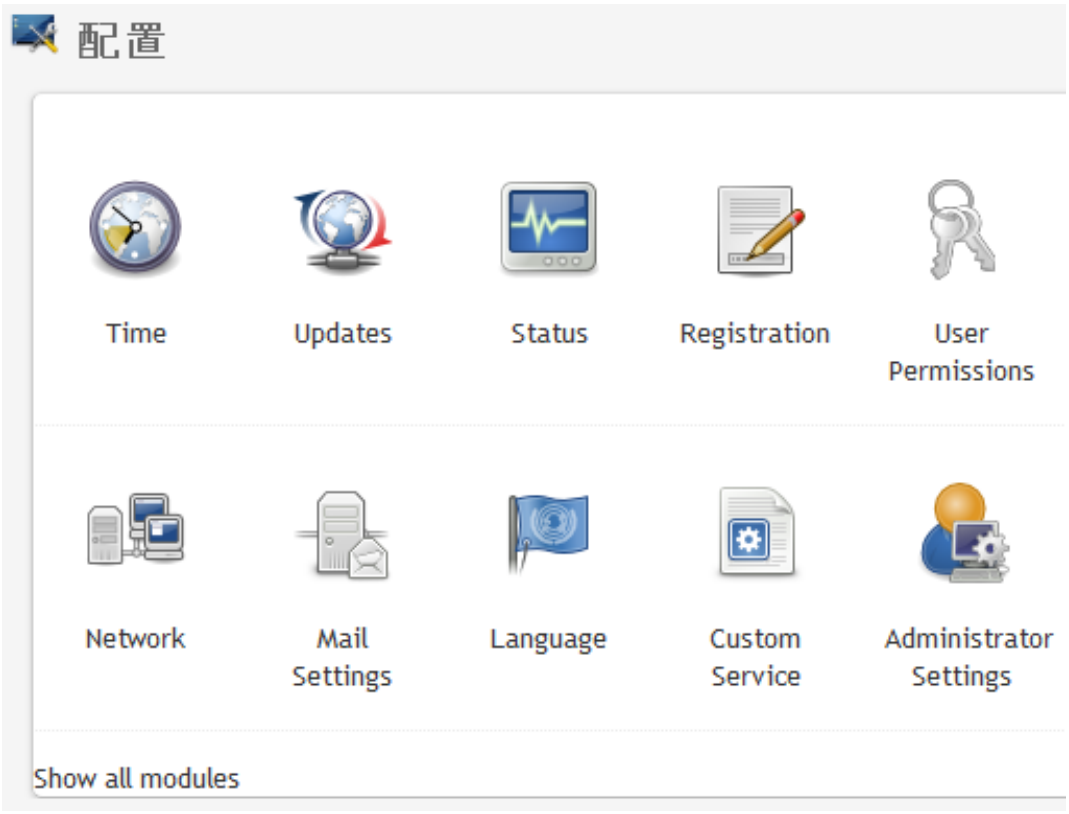
7 单击*下一步*完成初始设置。

4.8 注册更新

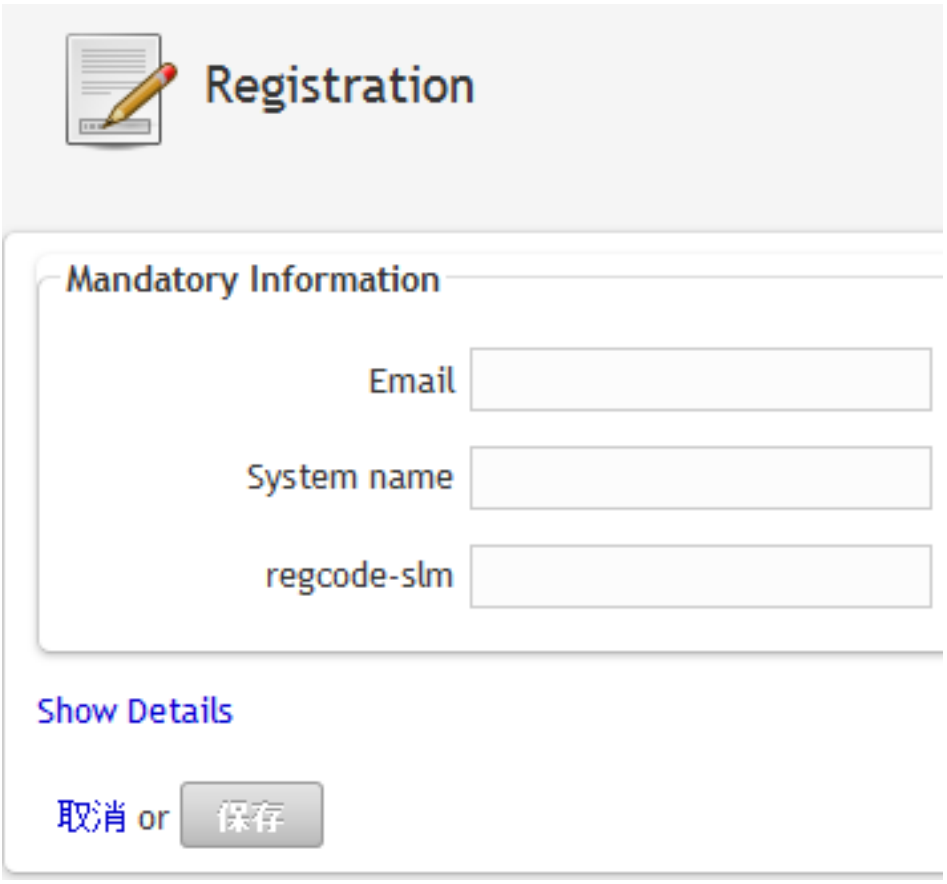
1 登录到 Sentinel Log Manager 设备。

登录到 Sentinel Log Manager 设备。

2 单击*设备*起动 WebYaST。


配置
Time
Updates
Status
Registration
User Permissions
Network
Mail Settings
Language
Custom Service
Administrator Settings
Show all modules

3 单击*注册*。

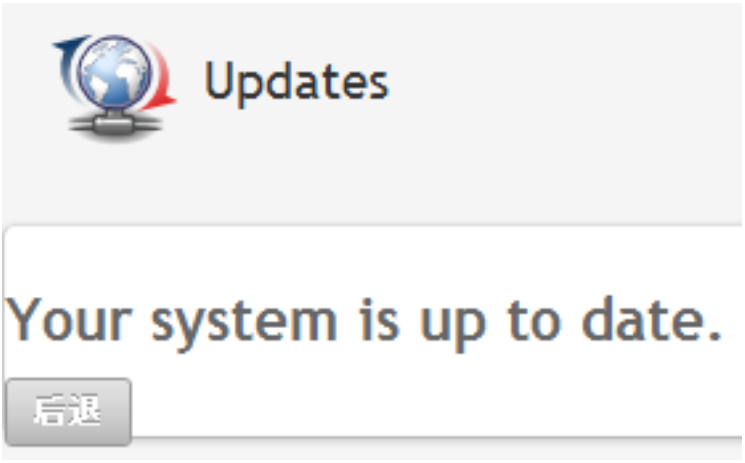


4 指定设备注册码。

5 单击*保存*。

6 要检查是否有任何更新，请单击*更新*。

结果页指示是否有任何更新。



登录到 Web 界面

5

安装期间创建的管理员用户可登录到 Web 界面配置和使用 Sentinel Log Manager：

1. 打开支持的 Web 浏览器。有关更多信息，请参见第 2.3 节 “支持的浏览器”（第 18 页）。
2. 指定 Novell Sentinel Log Manager 页面的 URL （例如， https://10.0.0.1:8443/novelllogmanager），然后按 Enter。
3. （有条件）首次登录 Sentinel Log Manager 时，将提示您接受一个证书。在接受证书后将显示 Sentinel Log Manager 登录页面。

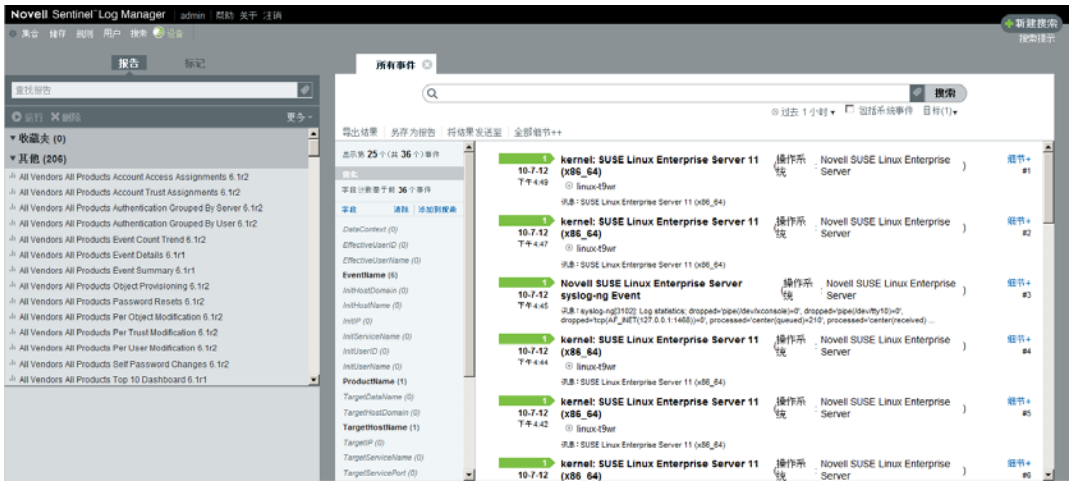
4 指定 Sentinel Log Manager 管理员的用户名和口令。

5 选择 Sentinel Log Manager 界面的语言。

Sentinel Log Manager 用户界面语言有英语、葡萄牙语、法语、意大利语、德语、西班牙语、日语、繁体中文和简体中文。

6 单击*登录*。

此时将显示 Novell Sentinel Log Manager Web 用户界面。



升级 Sentinel Log Manager 6

可使用升级脚本将 Novell Sentinel Log Manager 从 1.0.0.4 或更高版本升级到 Sentinel Log Manager 1.1。

6.1 从 1.0 升级到 1.1

1. 若您的 Sentinel Log Manager 服务器版本早于 1.0.0.4，则必须将其升级到 1.0.0.4 版或更高版本。
2. 从 Novell 下载站点下载和复制安装文件。
3. 作为根登录到要安装 Sentinel Log Manager 的服务器。
4. 指定以下命令以停止 Sentinel Log Manager 服务器：

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

   例如， /opt/novell/sentinel_log_mgr_1.0_x86-64/bin/server.sh stop
5. 指定以下命令从 tar 文件抽取安装文件：

   ```
   tar xfz <install_filename>
   ```

   使用安装文件实际名称替换 <*install_filename*>。
6. 指定以下命令运行 install-slm 脚本以升级 Sentinel Log Manager：

   ```
   ./install-slm
   ```
7. 要使用选择的语言继续，请选择该语言旁边的编号。

   最终用户许可证协议将以选定的语言显示。
8. 阅读最终用户许可证协议并输入 yes 或 y 接受此许可证，然后继续安装。
9. 安装脚本将提示您存在早期产品版本，并提示您指定是否升级该产品。若按 n，安装将终止。要继续升级，请按 y。

   安装将开始安装所有的 RPM 包。该安装完成可能需要几秒钟的时间。

   现有 Sentinel Log Manager 1.0 安装将保留不动，以下内容除外：

   - 若 1.0 数据目录 （例如， /opt/novell/sentinel_log_manager_1.0_x86-64/data）和 1.1 数据目录 （例如， /var/opt/novell/sentinel_log_mgr/data）位于同一文件系统，那么 <1.0>/data/eventuate 和 <1.0>/data/rawdata 子目录将被移动到 1.1 位置，因为 eventdata 和 rawdata 目录通常非常大。若 1.0 数据和 1.1 数据目录位于不同的文件系统，则 eventdata 和 rawdata 子目录将复制到 1.1 位置， 1.0 文件保留不动。
   - 若现有 1.0 数据目录 （例如， /opt/novell/sentinel_log_mgr_1.0_x86-64）位于一个单独安装的文件系统上并且含有 1.1 数据目录 (/var/opt/novell/sentinel_log_mgr/data) 的文件系统空间不足，可允许安装程序从 1.0 位置到 1.1 位置重新安装该文件系统。/etc/fstab 中的任何条目也将更新。若决定不让安装程序重新安装现有文件系统，升级将停止。然后可在文件系统上为 1.1 数据目录创建足够的空间。

10 当 Sentinel Log Manager 安装成功并且服务器功能正常时，必须指定以下命令手动去除 Sentinel Log Manager 1.0 目录。

```
rm -rf /opt/novell/slm_1.0_install_directory
```

例如：

```
rm -rf /opt/novell/sentinel_log_mgr_1.0_x86-64
```

永久移除该安装目录将删除 Sentinel Log Manager 1.0 安装

6.2 升级收集器管理器

1 以管理员身份登录到 Sentinel Log Manager。

2 选择*收集* > *高级*。

3 单击*下载安装程序*链接。在收集器管理器升级安装程序部分。

将显示一个窗口，有在本地计算机打开或保存 scm_upgrade_installer.zip 文件的选项。保存文件。

4 将文件复制到临时位置。

5 抽取 .zip 文件的内容。

6 作为收集器管理器安装的拥有者，根据您的操作软件运行以下升级文件之一：

- 要升级 Windows 收集器管理器，请运行 service_pack.bat。
- 要升级 Linux 收集器管理器，请运行 service_pack.sh。

7 按照屏幕指导完成安装。

8 重启动计算机。

6.3 从 1.0 到 1.1 设备迁移

若已安装 Sentinel Log Manager 1.0 并希望迁移到 Sentinel Log Manager 设备 1.1，请按照下面的步骤迁移数据和配置。

1 （有条件）若安装的 Sentinel Log Manager 版本低于 1.0 hotfix 4，请将其升级到 Sentinel Log Manager 1.0 hotfix 5，此为提供的最新的热修复。从 Novell 补丁下载站点 (http://download.novell.com/protected/Summary.jsp?buildid=VgZ3aerzjYc~) 下载该热修复。

注释：必须是注册用户才能下载补丁。若尚未注册，请在补丁下载站点单击 “注册” 创建一个用户帐户。

---

2 升级到 Sentinel Log Manager 1.1。有关详细信息，请参阅第 6.1 节 “从 1.0 升级到 1.1” （第 43 页）。

3 指定以下命令以更改为 novell 用户：

```
su -novell
```

4 指定以下命令以更改为 /bin 用户：

```
cd /opt/novell/sentinel_log_mgr/bin
```

5 指定以下命令完整备份 Sentinel Log Manager 1.1 数据和配置。

```
./backup_util.sh -m backup -c -e -l -r -s -w -f $APP_HOME/data/
<backupfilename>
```

使用一个文件名替换 <*backupfilename*> 以储存备份数据。

有关备份数据的详细信息，请参阅 “备份和恢复数据”。

6 在一台独立的计算机上安装 Sentinel Log Manager 设备 1.1。有关详细信息，请参阅第 4 章 “安装设备”（第 29 页）。

7 将含有备份数据的文件复制到新安装的 Sentinel Log Manager 1.1 设备上。

8 指定以下命令：

```
chown novell:novell <backfupfilename>
```

9 指定以下命令以更改为 /bin 用户：

```
cd /opt/novell/sentinel_log_mgr/bin
```

10 指定以下命令从 Sentinel Log Manager 1.1 应用程序完整恢复备份的数据：

```
./backup_util.sh -m restore -f $APP_HOME/data/<backupfilename>
```

有关详细信息，请参阅 “备份和恢复数据”。

安装附加收集器管理器。 7

收集器管理器为 Novell Sentinel Log Manager 管理所有的数据收集和数据分析。 Sentinel Log Manager 安装进程默认将在 Sentinel Log Manager 服务器上安装一个收集器管理器。但是可在分布式安装中安装多个收集器管理器。

7.1 开始之前的准备工作

- 确保您的硬件和软件满足第 2 章 “系统要求”（第 15 页）中提到的最低要求。
- 使用网络时间协议 (NTP) 同步时间。
- 在 Sentinel Log Manager 服务器上，收集器管理器需要到讯息总线端口 (61616) 的网络连接。在开始安装收集器管理器前，确保所有防火墙和其他网络设置允许通过此端口进行通信。

7.2 附加收集器管理器的优势

在一个分布式网络中安装多个收集器管理器可提供一些优势：

- **改进系统性能：**附加收集器管理器可在一个分布式环境中分析和处理事件数据，从而提升系统性能。
- **提供了附加数据安全并降低了网络带宽要求：**若收集器管理器与事件源位于同一位置，筛选、加密和数据压缩都可在源处执行。
- **可从附加操作系统收集数据：**例如，可在 Microsoft Windows 上安装一个收集器管理器以通过 WMI 协议启用数据收集。
- **文件超速缓存：**如果启用文件超速缓存，远程收集器管理器可在服务器暂时存档事件或处理事件暴增时超速缓存大量数据。对于本身并不支持事件超速缓存的协议 （如 syslog）而言，此功能是一种优势。

7.3 安装附加收集器管理器。

1. 以管理员身份登录到 Sentinel Log Manager。
2. 选择*收集* > *高级*。
3. 单击*下载安装程序*链接。在收集器管理器安装程序部分。

   将显示一个窗口，其中具有在本地计算机打开或保存 scm_installer.zip 文件的选项。保存文件。
4. 复制并抽取该文件到要安装收集器管理器的位置。
5. 根据您的操作软件运行以下安装文件之一：
   - 要在 Windows 系统上安装收集器管理器，请运行 setup.bat。
   - 要在 Linux 系统上安装收集器管理器，请运行 setup.sh。

6 选择一种语言，然后单击*确定*。

此时将显示安装程序。

7 单击“确定”。

8 阅读并接受许可证协议，然后单击*下一步*。

9 可以选择默认安装目录或浏览并选择目录，然后单击*下一步*。

10 不更改默认讯息总线端口 (61616)，指定通信服务器的主机名，然后单击*下一步*。

11 单击*下一步*使用默认自动内存配置 （256 MB）。

此时将显示安装摘要。

12 单击*安装*。

13 指定收集器管理器的用户名和口令。

注释：用户名和口令储存在 Sentinel Log Manager 服务器上的 /etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties 文件中。

---

14 当提示时永久接受证书。

15 单击*完成*以完成安装。

16 重启动计算机。

卸装 Sentinel Log Manager 8

本节介绍卸装 Novell Sentinel Log Manager 服务器和收集器管理器的过程。

8.1 卸装设备

若希望保留任何 Log Manager 数据，在卸装设备前必须备份该数据，以在稍后恢复。有关详细信息，请参阅 *《Sentinel Log Manager 1.1 管理指南》*中的 “备份和恢复数据”。

若不需要保留任何数据，请使用以下步骤卸装设备：

- **VMware ESX 设备：**如果虚拟计算机专用于 Novell Sentinel Log Manager，而您不需要保留任何数据，请删除虚拟机以卸装 Log Manager 虚拟设备。
- **Xen 设备：**如果 Xen 虚拟计算机专用于 Novell Sentinel Log Manager，而您不需要保留任何数据，请删除虚拟机以卸装 Log Manager 虚拟设备。
- **硬件设备：**如果系统专用于 Novell Sentinel Log Manager，而您不需要保留任何数据，请重新格式化硬盘，以卸装物理计算机上的 Log Manager。

8.2 从现有 SLES 11 系统卸装

1. 作为根登录到 Sentinel Log Manager 服务器。
2. 要运行卸装脚本，请执行以下命令：

   ```
   /opt/novell/sentinel_log_mgr/setup/uninstall-slm
   ```

3. 当提示重新确认希望卸装时，请按 y。

   将首先停止 Sentinel Log Manager 服务器，然后卸装。

8.3 卸装收集器管理器

本节介绍卸装在 Windows 或 Linux 计算机上安装的 Sentinel 收集器管理器的过程。

8.3.1 卸装 Linux 收集器管理器

1. 以根用户身份登录。
2. 在安装收集器管理器的计算机上，导航到以下位置：

   $ESEC_HOME/_unist

3. 运行以下命令：

```
./uninstall.bin
```

4 选择一种语言，然后单击*确定*。

5 在安装向导中单击*下一步*。

6 选择要卸装的功能，然后单击*下一步*。

7 停止所有正在运行的 Sentinel Log Manager 应用程序，然后单击*下一步*。

8 单击*卸装*。

9 单击*完成*。

10 选择*重引导系统*，然后单击*完成*。

8.3.2 卸装 Windows 收集器管理器

1 以管理员身份登录。

2 停止 Sentinel Log Manager 服务器。

3 选择 “开始” > “运行”。

4 指定以下内容：

%Esec_home%_uninst

5 双击 uninstall.exe 运行它。

6 选择一种语言，然后单击*确定*。

此时将显示安装向导。

7 单击 “下一步”。

8 选择要卸装的功能，然后单击*下一步*。

9 停止所有正在运行的 Sentinel Log Manager 应用程序，然后单击*下一步*。

10 单击*卸装*。

11 单击*完成*。

12 选择*重引导系统*，然后单击*完成*。

8.3.3 手动清理目录

- Linux （第 50 页）
- Windows （第 50 页）

Linux

1 以根身份登录到要卸装收集器管理器的计算机。

2 停止所有 Sentinel Log Manager 进程。

3 去除 /opt/novell/sentinel6 的内容。

Windows

1 以管理员身份登录到要卸装收集器管理器的计算机。

2 删除 %CommonProgramFiles%\InstallShield\Universa 文件夹及其所有内容。

3 删除 %ESEC_HOME% 文件夹。此文件夹默认位置为 C:\Program Fil s\Novell\Sentinel6。

排查安装错误

A

本节包含安装过程中可能出现的一些问题及解决这些问题的步骤。

A.1 因为错误网络配置导致安装失败

首次启动时，如果安装程序发现网络设置不正确，将会显示一条错误讯息。若网络不可用，在设备上安装 Sentinel Log Manager 将失败。

要解决此问题，请正确配置网络设置。当验证配置时， ifconfig 命令应返回有效的 IP 地址，hostname -f 命令应返回有效的主机名。

A.2 在 SLES 11 上使用 VMware Player 3 配置网络问题

在 SLES 11 上尝试使用 VMware Player 3 配置网络时可能看见以下错误：

```
Jan 12 14:57:34.761: vmx| VNET: MACVNetPortOpenDevice: Ethernet0: can't open
vmnet device (No such device or address)
Jan 12 14:57:34.761: vmx| VNET: MACVNetPort_Connect: Ethernet0: can't open
data fd
Jan 12 14:57:34.761: vmx| Msg_Post: Error
Jan 12 14:57:34.761: vmx| [msg.vnet.connectvnet] Could not connect Ethernet0
to virtual network "/dev/vmnet0". More information can be found in the
vmware.log file.
Jan 12 14:57:34.761: vmx|[msg.device.badconnect] Failed to connect virtual
device Ethernet0.
Jan 12 14:57:34.761: vmx| --
```

此错误指示 VMX 文件可能已被其他 VM 打开了。要解决此问题，必须按照以下所示更新 VMX 文件中的 MAC 地址：

1. 在文本编辑器中打开 VMX 文件。
2. 从 ethernet0.generatedAddress 字段复制 MAC 地址。
3. 从来宾操作系统打开 /etc/udev/rules.d/70-persistent-net.rules 文件。
4. 将原行注释掉，然后按如下所示键入一个 SUBSYSTEM 行：

   ```
   SUBSYSTEM=="net", DRIVERS=="?*", ATTRS{address}==<MAC address>,
   NAME="eth0"
   ```

5. 使用步骤 2 步骤 2 中复制的 MAC 地址替换 <*MAC address*>。
6. 保存并关闭文件。
7. 在 VMware Player 中打开 VM。

A.3 升级以非根用户而非 Novell 用户身份安装的 Log Manager

若尝试升级以非根用户而非 novell 用户身份安装的 Novell Sentinel Log Manager 1.0 服务器，升级过程失败。发生此问题是由 Sentinel Log Manager 1.0 安装时设置的文件权限性质造成的。

要升级以非根用户而非 novell 用户身份安装的 Sentinel Log Manager 1 0 服务器 请执行以下操作：

1. 创建 novell 用户。
2. 将 Sentinel Log Manager 1.0 安装的所有权更改为 novell:novell。

   ```
   chown -R novell:novell /opt/novell/<install_directory>
   ```

   将 <*install_directory*> 更改为安装目录的名称。例如，

   ```
   chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
   ```
3. 在 config/esecuser.properties 中将 ESEC_USER 项更改为 novell。
4. 以根身份登录，然后升级到 Sentinel Log Manager 1.1、有关升级的详细信息，请参阅第 6.1 节 “从 1.0 升级到 1.1”（第 43 页）。

Sentinel 技术

本章节介绍了此文档中所使用的术语。

收集器
一个实用工具，在对事件进行关联和分析并将其发送到数据库之前，会通过将分类、利用检测和业务相关性注入数据流，来分析数据并递送更丰富的事件流。

连接器：
一个使用行业标准方法连接到数据源以获取原始数据的实用工具。

数据保留
定义事件在从 Sentinel Log Manager 服务器删除之前保留的时间的策略。

事件源
记录事件的施放器或系统。

事件源管理
ESM - 事件源管理 (ESM) 界面，您可以使用 Sentinel 连接器和 Sentinel 收集器管理和监视 Sentinel 与其事件源之间的连接。

每秒的事件数
EPS - 一个用于测量网络从其安全设备和应用程序生成数据的速度的值。此值也为 Sentinel Log Manager 可从安全设备收集和储存数据的速度。

集成器
使 Sentinel 系统可连接到其他外部系统的插件。 JavaScript 操作可使用集成器与其他系统互动。

原始数据
未处理的事件，由连接器接收并直接发送到 Sentinel Log Manager 讯息总线，然后写入到 Sentinel Log Manager 服务器的磁盘上。由于储存在设备中的原始数据的格式问题，原始数据会因连接器的不同而有所不同。