NetIQ Sentinel 7.1

安装和配置指南

June 2013

法律声明

NetIQ Sentinel 受美国专利 （专利号为 05829001）的保护。

本文档及其中所述软件按许可协议或保密协议的条款提供，并受这些条款的约束。除非在此类许可协议或保密协议中有明确规定，否则 NETIQ CORPORATION 将按 “ 原样 ” 提供本文档及其中所述软件，不做任何明示或暗示的保证 （包括但不限于对用于具体目的的适销性或适用于的暗示保证）。美国的某些州不允许免除对某些交易的明示或暗示保证，因此本声明可能不适用于您。

为明确起见，特此声明：任何模块、适配器或其他类似的材料 （统称 “ 模块 ”），均根据与之相关或与之进行互操作的 NetIQ 产品或软件的相应版本按 《最终用户许可协议》的条款和条件进行许可，访问、复制或使用某个 “ 模块 ”，即表示您同意受此类条款的约束。如果您不同意 《最终用户许可协议》的条款，则将无权使用、访问或复制 “ 模块 ”，因此，您必须销毁 “ 模块 ” 的所有副本，并联系 NetIQ 以寻求进一步的指导。

未经 NetIQ Corporation 的事先书面许可，不得转借、销售或赠予本文档及其中所述软件，除非法律另外许可。除非在此类许可协议或保密协议中有明确规定，否则，未经 NetIQ Corporation 的事先书面同意，不得对本文档或其中所述软件中的任何部分进行复制，也不得将其储存在检索系统中，或以任何形式或任何方式 （包括电子方式、机械方式等）进行传输。本文档中的某些公司、名称和数据仅用于说明，不得代表真实的公司、个人或数据。

本文档可能包含不准确的技术信息或印刷错误。此处的信息将定期进行更改。这些更改可能会纳入本文档的新版中。 NetIQ Corporation 可能会随时对本文档所述软件进行改进或更改。

美国政府的有限权利：如果本软件和文档是由美国政府、代表美国政府或由美国政府的主要承包商或分包商 （任何层级）根据 48 C.F.R. 227.7202-4 （针对国防部 (DOD) 采购）以及 48 C.F.R. 2.101 和 12.212 （针对非 DOD 采购）的规定获取的，则美国政府对本软件和文档的各方面权利 （包括使用、修改、复制、发布、执行、显示或披露本软件或文档的权利），将受许可协议中规定的商业许可权利和限制的约束。

目录

关于本书和库

*《安装和配置指南》*介绍了 NetIQ Sentinel，并说明了如何安装和配置 Sentinel。

目标受众

本指南适用于 Sentinel 管理员和顾问。

库中的其他信息

此库提供了以下信息资源：

管理指南

提供管理 Sentinel 部署所需的管理信息和任务。

用户指南

提供有关 Sentinel 的概念信息。本书还概述了许多任务的用户界面和分步指导。

关于 NetIQ Corporation

我们是一家全球性的企业软件公司，专注于您的环境中三大永恒挑战：变化、复杂性和风险，设法帮助您应对这些挑战。

我们的观点

适应变化及管理复杂性和风险实乃老生常谈

实际上在您面临的所有挑战中，这些也许是容易让您失控的最突出变数，从而无法安全地衡量、监视和管理您的物理环境、虚拟环境和云计算环境所需。

提供更好、更快的关键业务服务

我们相信，尽可能多地为 IT 组织提供控制，是更及时、经济有效地交付服务的唯一方法。只有在组织不断做出改变，并且管理这些变化所需的技术本身日益复杂时，持续存在的压力 （如变化和复杂性）才会继续增大。

我们的理念

销售智能解决方案，而不只是软件

为了提供可靠的控制，我们首先务必了解 IT 组织 （如贵组织）的实际日常运作情况。这才是我们可以开发出实用的智能型 IT 解决方案以成功取得公认的重大成果的唯一途径。并且，这比单纯销售软件要有价值得多。

推动您走向成功是我们的追求

我们将您的成功视为我们业务活动的核心。从产品启动到部署，我们深知：您需要与您当前购买的解决方案配合使用和完美集成的解决方案；您需要在部署后获得持续的支持并接受后续的培训；您还需要真正易于合作的伙伴一起应对变化。总之，只有您成功，才是我们都成功。

我们的解决方案

- 身份和访问管理
- 访问管理
- 安全管理
- 系统和应用程序管理
- 工作负载管理
- 服务管理

与销售支持联系

若对产品、定价和功能有疑问，请与本地合作伙伴联系。如果无法与合作伙伴联系，请与我们的销售支持团队联系。

全球：	www.netiq.com/about_netiq/officelocations.asp
美国和加拿大：	1-888-323-6768
电子邮件：	info@netiq.com
网站：	www.netiq.com

联系技术支持

有关具体的产品问题，请与我们的技术支持团队联系。

全球：	www.netiq.com/support/contactinfo.asp
北美和南美：	1-713-418-5555
欧洲、中东和非洲：	+353 (0) 91-782 677
电子邮件：	support@netiq.com
网站：	www.netiq.com/support

联系文档支持

我们的目标是提供满足您的需要的文档。如果您有改进建议，请单击 www.netiq.com/documentation 上发布的 HTML 版文档任何页面底部的**添加注释**。您还可以发送电子邮件至 Documentation-Feedback@netiq.com。我们会重视您的意见，欢迎您提供建议。

联系在线用户社区

Qmunity 是 NetIQ 在线社区的简称，它是让您可与同行和 NetIQ 专家沟通的协作网络。通过提供更多即时信息、指向实用资源的有用链接，以及 NetIQ 专家的支持， Qmunity 有助于确保您可以掌握必要的知识，以充分发挥所依赖的 IT 投资的潜力。有关详细信息，请访问 http://community.netiq.com。

了解 Sentinel

本节将详细介绍何谓 Sentinel，以及 Sentinel 如何为您的组织提供事件管理解决方案。

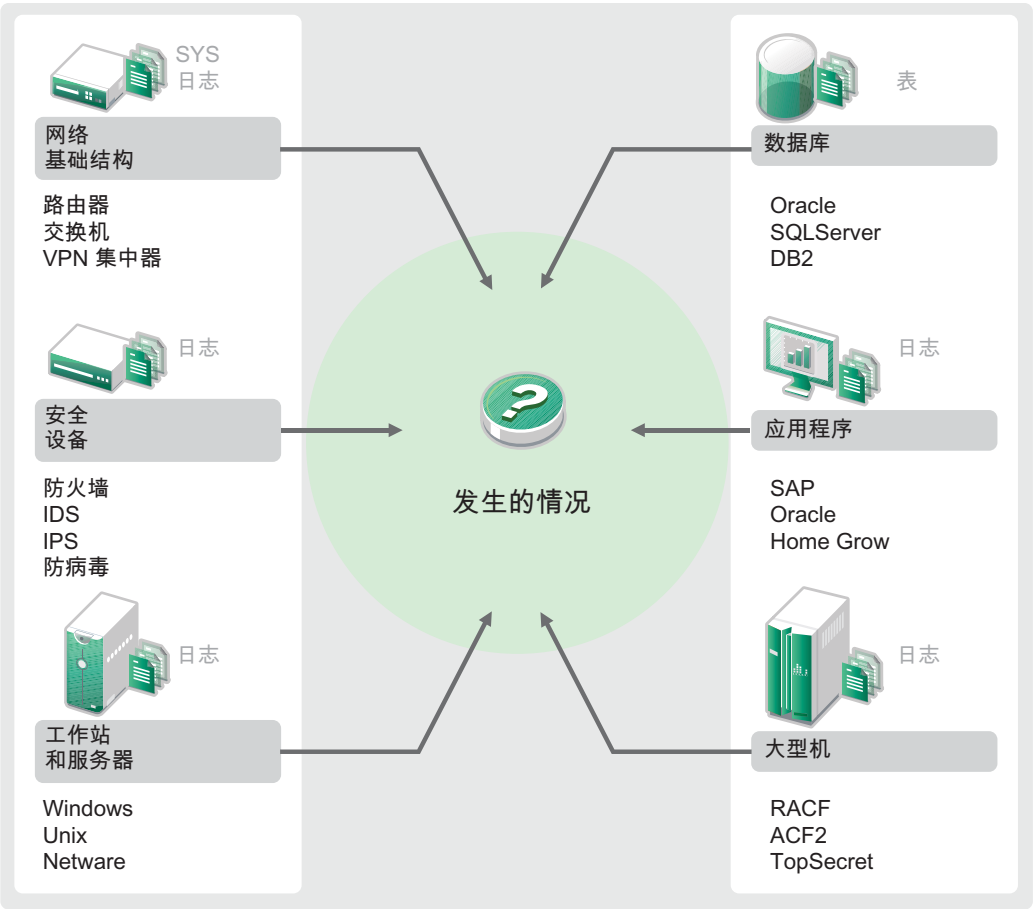
1 Sentinel 是什么？

Sentinel 是一个安全信息和事件管理 (SIEM) 解决方案，同时也是一个合规性监视解决方案。 Sentinel 可自动监视最复杂的 IT 环境，并提供所需的安全性以保护您的 IT 环境。

1.1 保护 IT 环境的挑战

由于环境的复杂性，在确保 IT 环境安全时遇到了挑战。许多不同的应用程序、数据库、大型机、工作站和服务器都有事件日志。此外，您还有安全设备和网络基础设施设备，它们都有您的 IT 环境中所发生事件的日志。

图 1-1 *您的环境中发生了什么事件*



挑战源自以下事实：

- 您的 IT 环境中存在许多设备 .
- 日志的格式各不相同 .
- 日志储存在单独的区域中 .
- 日志中生成的信息数量巨大 .
- 如果不手动分析所有日志，便无法确定谁执行了什么操作 .

要利用信息，必须能够执行以下操作：

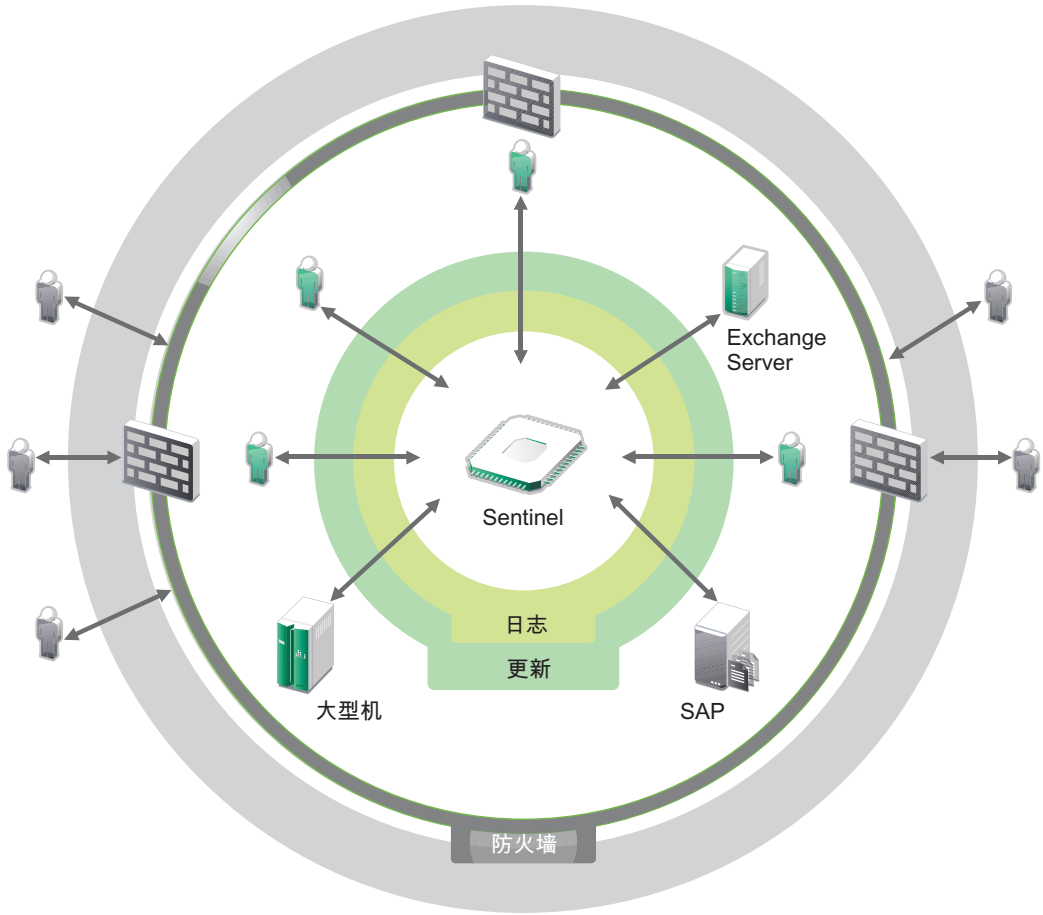
- 收集数据 .
- 合并数据 .
- 将不同的数据规范化为可轻松比较的事件。
- 将事件映射到标准法规 .
- 分析数据 .
- 比较多个系统中的事件以确定是否存在安全性问题 .
- 当数据不符合规范时发送通知 .
- 对通知采取措施以遵循企业策略 .
- 生成报告以证实合规性 .

了解保护 ·IT· 环境所面临的挑战之后，您需要确定如何保护企业免受内外部用户的影响，而不会将其视作恶意用户，或者给其招致负担，以致无法提高工作效率。 Sentinel 可为此提供解决方案。

1.2 Sentinel 提供的解决方案

Sentinel 充当了企业安全性的中枢神经系统。它可从包括应用程序、数据库、服务器、储存和安全设备在内的整个基础设施中提取数据。它可以自动或手动分析和关联数据，并使数据可以操作。

图 1-2 *Sentinel 提供的解决方案*



结果是，您了解在任意给定时间点您的 IT 环境中所发生的事件，并且还能够将对资源执行的操作及其执行人员关联起来。这使您可以确定用户行为并有效地监视控件。无论此人是否为内部人员，您都可以将他们执行的所有操作关联起来，这样，在他们造成任何损害之前，未经授权的活动就能清楚得知了。

Sentinel 通过下列功能以具有成本效益的方式来实现这一切：

- 提供单个解决方案跨多个法规应对 IT 控制。
- 消除您的网络环境中应该发生什么和实际正在发生什么之间的认识鸿沟 .
- 向审计人员和监管人员证明您的企业在安全控制方面实施了适当的记录、监视和报告工作 .
- 提供即用型合规性监视和报告程序 .
- 获得持续监视企业在合规性与安全计划方面取得的成效所需的洞察力与控制力 .

Sentinel 可使日志收集、分析和报告过程自动执行，以确保 IT 控制有效支持威胁检测要求和审计要求。 Sentinel 提供了自动监视安全性事件、合规性事件和 IT 控件的功能，允许您在发生安全性违规或不合规事件时立即采取措施。使用 Sentinel，您还可以轻松收集有关环境的摘要信息，以便您能够与主要利益相关者沟通整体安全态势。

2 Sentinel 工作原理

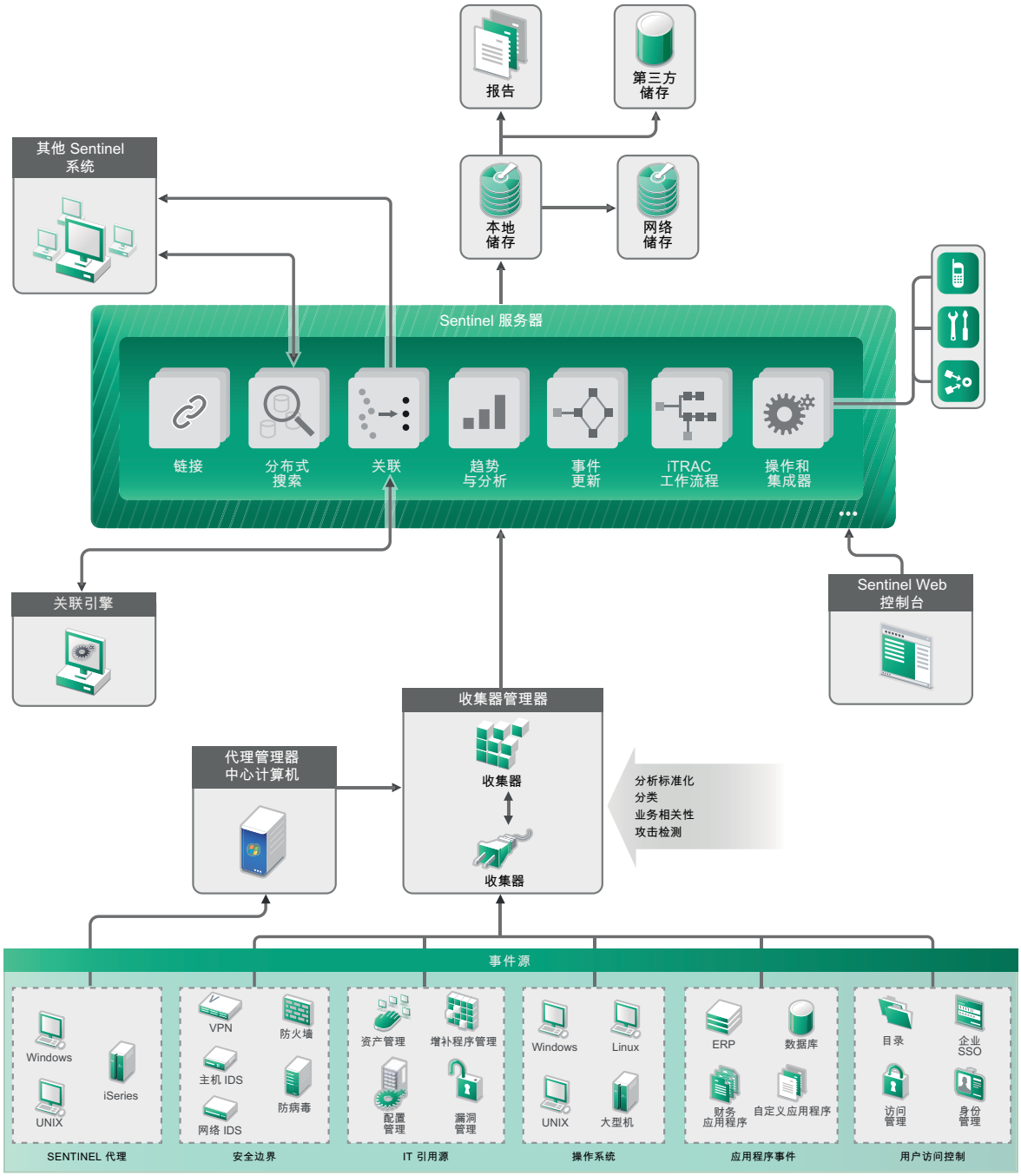
Sentinel 会持续管理整个 IT 环境中的安全信息和事件，以便提供完整的监视解决方案。

Sentinel 执行以下操作：

- 从 IT 环境的所有不同事件源中收集日志、事件和安全信息。
- 将收集的日志、事件和安全信息规范化为通用格式。
- 使用灵活的可自定义数据保留策略将事件储存在基于文件的数据储存中。
- 提供以分级方式链接多个 Sentinel 系统 （包括 Sentinel Log Manager）的功能。
- 使您不仅可以在本地 Sentinel 服务器上搜索事件，还可以在分布于全球的其他 Sentinel 服务器上进行搜索。
- 执行静态分析，该分析允许您定义一个基线，然后将其与正在发生的事件进行对比，从而确定是否存在未发现的问题。
- 关联给定期限内相似或类似的一组事件以确定模式。
- 对事件进行分组，以便进行有效的响应管理和跟踪。
- 提供基于实时和历史事件的报告。

下图说明了 Sentinel 的工作原理：

图 2-1 Sentinel 体系结构



以下章节将详细介绍 Sentinel 的部件：

- 第 2.1 节 “ 事件源 ”（第 21 页）
- 第 2.2 节 “Sentinel 事件 ”（第 21 页）
- 第 2.3 节 “ 收集器管理器 ”（第 22 页）
- 第 2.4 节 “ 代理管理器 ”（第 23 页）
- 第 2.5 节 “ 关联 ”（第 23 页）

2.1 事件源

Sentinel 从 IT 环境的许多不同源中收集安全信息和事件。这些源称为事件源。事件源可以是网络上的许多不同项目。

安全外围：安全设备，包括用于为环境创建安全周边的软硬件，例如防火墙、 IDS 和 VPN。

操作系统：在网络中运行的不同操作系统中的事件。

IT 引用源：用于维护和跟踪资产、增补程序、配置和漏洞的软件。

应用程序事件：从网络中安装的应用程序生成的事件。

用户访问控件：从允许用户访问公司资源的应用程序或设备生成的事件。

2.2 Sentinel 事件

Sentinel 会从设备接收信息，将此信息规范化为称作 “ 事件 ” 的结构，对事件进行分类，然后发送事件进行处理。通过向事件中添加类别信息 （分类），可以更轻松地在以不同方式报告事件的系统之间比较事件。例如，鉴定故障。事件由实时显示器、关联引擎、仪表板和后端服务器进行处理。

一个事件包含 200 多个字段。事件字段的类型和用途各不相同。例如，一些预定义的字段包括严重性、危急程度、目标 IP 和目标端口。此外，还有两组可配置的字段：供 Sentinel 内部使用以允许将来扩展的保留字段，以及用于客户扩展的客户字段。

通过重命名，可以将字段用作他途。字段的源可以是外部的 （这意味着设备或对应的收集器对其进行了明确设置），也可以是引用的。引用字段的值使用映射服务计算为一个或多个其他字段的函数。例如，可以将字段定义为构建代码，以用于包含指定为事件目标 IP 的资产的构建。再比如，可以通过采用了客户定义映射 （使用事件中的目标 IP）的映射服务来计算字段。

2.2.1 映射服务

映射服务允许复杂机制在整个系统中传播业务相关性数据。此数据可以通过提供环境的引用信息来丰富事件，从而使分析人员能够做出更好的决定、撰写更有用的报告，以及制定出经过深思熟虑的关联规则。

您可以通过使用映射将额外的信息 （如，主机和身份详细信息）添加到从源设备传入的事件中来丰富事件。这些额外的信息可用于高级关联和报告。系统支持多种内置映射以及由用户定义的自定义映射

Sentinel 中定义的映射采用两种方式进行储存：

- 内置映射储存在数据库中，使用收集器代码中的 API 进行更新，并且会自动导出为映射服务。
- 自定义映射储存为 CSV 文件，可在文件系统上或通过映射数据配置 UI 进行更新，然后由映射服务进行装载。

对于这两种方式， CSV 文件都保存在中心的 Sentinel 服务器中，但是对映射所做的更改会分发给每个收集器管理器并在本地进行应用。此分布式处理方式可以确保映射活动不会使主服务器过载。

2.2.2 流式传输映射

映射服务会利用一个动态更新模型，并将映射从一个点流式传输到另一个点，从而避免在动态内存中生成大型静态映射。在 Sentinel 等关键任务实时系统（需要稳定、可预测且灵活的数据移动，而不依赖系统上的任何临时负载）中，这种流式传输功能尤其可体现出其重要价值。

2.2.3 攻击检测（映射服务）

Sentinel 提供了交叉引用事件数据签名与漏洞扫描程序数据的功能。当攻击试图利用有漏洞的系统时，将会立即自动通知用户。这是通过下列几项完成的：

- Advisor 传递
- 入侵检测
- 漏洞扫描
- 防火墙

Advisor 可在事件数据签名和漏洞扫描程序数据之间提供交叉引用。 Advisor 源包含有关漏洞、威胁以及事件签名和漏洞插件规范化的信息。有关 Advisor 的详细信息，请参阅 *《NetIQ Sentinel 7.1 管理指南》* 中的 “ 配置 Advisor”。

2.3 收集器管理器

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以下内容：

- 转换事件 .
- 通过映射服务向事件中添加业务相关性。
- 对事件执行全局过滤。
- 路由事件。
- 确定实时数据、漏洞数据、资产数据或非实时数据。
- 向 Sentinel 服务器发送运行状况讯息。

2.3.1 收集器

收集器可规范化连接器中的信息并收集这些信息。收集器采用 JavaScript 编写，它们为以下操作定义了逻辑：

- 从连接器中接收原始数据。

- 分析并规范化数据。
- 向数据应用可重复的逻辑。
- 将特定于设备的数据转换为特定于 Sentinel 的数据。
- 设置事件的格式。
- 将已规范化、已分析和已设置格式的数据传递到收集器管理器。
- 对事件进行特定于设备的过滤。

2.3.2 连接器

连接器提供了从事件源到 Sentinel 系统的连接。连接器使用行业标准协议获取事件 （例如 syslog），使用 JDBC 读取数据库表，使用 WMI 读取 Windows 事件日志等。连接器提供以下功能：

- 将原始事件数据从事件源到收集器的传输。
- 特定于连接的过滤。
- 连接错误处理。

2.4 代理管理器

代理管理器提供了基于主机的数据收集，以补充无代理数据收集，因为它让您可以执行以下操作：

- 访问无法通过网络提供的日志。
- 在严格控制的网络环境中操作。
- 限制对关键服务器的攻击面，以改善安全状况。
- 在网络中断期间，提高数据收集的可靠性

代理管理器允许您部署代理和管理代理配置，可作为流入 Sentinel 的事件的收集点。有关代理管理器的详细信息，请参见代理管理器文档。

2.5 关联

单个事件可能看似微不足道，但与其他事件相结合，它可能就会提醒您注意某个潜在问题。 Sentinel 可以使用您在关联引擎中创建和部署的规则来帮助您关联此类事件，并采取适当措施以缓解任何问题。

关联通过自动分析传入事件流来查找所需的模式，从而提高安全性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，请参阅 *《NetIQ Sentinel 7.1 用户指南》*中的 “ 关联事件数据 ”。

要根据关联规则监视事件，您必须在关联引擎中部署规则。当符合规则准则的事件发生时，关联引擎将生成描述该模式的关联事件。有关详细信息，请参见 *《NetIQ Sentinel 7.1 用户指南》*中的 “ 关联引擎 ”。

2.6 安全智能

使用 Sentinel 中的关联功能可以查找已知模式的活动，无论是出于安全性、合规性，还是其他原因考虑。安全智能功能则查找异常 （可能是恶意的）且不符合任何已知模式的活动。

Sentinel 中的安全智能功能主要是对时间系列数据进行统计分析，以使分析人员能够通过自动统计引擎或用于手动解释的统计数据可视化表示，来识别并分析偏离项 （异常）。有关详细信息，请参阅 *《NetIQ Sentinel 7.1 用户指南》* 中的 “ 分析数据中的趋势 ”。

2.7 事件补救

Sentinel 提供自动事件响应管理系统，让您可以记录并正式确定跟踪、提交和响应事件及策略违反情况的过程，并可提供与故障派单系统的双向集成。使用 Sentinel 可以及时响应事件并有效解决事件。有关详细信息，请参见 *《NetIQ Sentinel 7.1 用户指南》* 中的 “ 配置事件 ”。

2.8 iTrac 工作流程

iTRAC 工作流程旨在提供一个简单、灵活的解决方案，以便自动执行企业的事件响应进程并对其跟踪。 iTRAC 利用 Sentinel 的内部事件系统通过解析来跟踪标识中的安全性或系统问题 （通过关联规则或手动标识）。

工作流程可以使用手动和自动步骤进行构建。支持分支、基于时间的提升和本地变量等高级功能。通过与外部脚本和插件的集成，可以灵活地与第三方系统进行交互。综合的报告使管理员可以了解和微调事件响应进程。有关详细信息，请参阅 *《NetIQ Sentinel 7.1 用户指南》* 中的 “ 配置 iTRAC 工作流 ”。

2.9 操作和集成器

在 Sentinel 中，“ 操作 ” 手动或自动执行某些类型的操作，如发送电子邮件。“ 操作 ” 可以通过路由规则、手动执行事件或事件操作以及关联规则触发。 Sentinel 提供了一组预配置 “ 操作 ”。可以使用默认 “ 操作 ”，然后根据需要重新配置它们，您也可以添加新 “ 操作 ”。有关详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》* 中的 “ 配置操作 ”。

“ 操作 ” 可以自行执行，也可以利用通过集成器插件配置的 Integrator 实例。集成器插件扩展了 Sentinel 更新操作的特性和功能。集成器提供了连接到外部系统 （如 LDAP、 SMTP 或 SOAP 服务器）以执行操作的功能。有关详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》* 中的 “ 配置集成器 ”。

2.10 报告

Sentinel 提供了对收集的数据运行报告的功能。 Sentinel 中预打包了各种可自定义的报告。一些报告十分灵活，让您可以指定要在结果中显示的列。

您可以运行和安排 PDF 报告，并通过电子邮件发送它们。您还可以将任意报告作为搜索来运行，然后与搜索的结果进行交互，就像与搜索进行交互一样，例如优化搜索或对结果执行操作。此外，您可以在分布于不同地理位置的 Sentinel 服务器上运行报告。有关详细信息，请参阅 *《NetIQ Sentinel 7.1 用户指南》* 中的 “ 报告 ”。

2.11 事件分析

Sentinel 提供了一组强大的工具，可以帮助您轻松查找并分析重要事件数据。在任何特定类型的分析中，系统都会进行调整并优化以实现最大效率，而且提供的方法便于从一种类型的分析转换到另一种类型，从而实现无缝转换。

在 Sentinel 中调查事件通常首先从近乎实时的活动视图开始。尽管有更高级的工具可用，但活动视图显示的过滤事件流以及摘要图表足够用于对事件趋势和事件数据进行简单、粗略的分析，而且还可用于识别特定事件。在一段时间过后，您便可以为特定数据类（如，来自关联的输出）构建经过调整的过滤器。您可以将活动视图用作仪表板，以便显示整体运作和安全态势。

然后，您可以使用交互式搜索对事件执行更为详细的分析。这使您能够快速、方便地搜索和查找与特定查询相关的数据，如，由特定用户执行的活动或在特定系统上执行的活动。通过单击事件数据或使用左侧的细化窗格，您可以快速地分析感兴趣的特定事件。

在分析数百个事件时， Sentinel 的报告功能可以对事件布局进行自定义控制，并且还可显示较大的数据量。 Sentinel 允许您将搜索界面中构建的交互式搜索传输到报告模板中，从而使此转换更加方便；该报告模板可以立即创建报告，以更加适合大量事件的格式显示相同的数据。

Sentinel 包含许多用于此用途的模板。一些模板已调整为显示特定类型的信息（如，鉴定数据或用户创建），还有一些模板则为通用模板，这些模板允许您以交互方式自定义报告中的组和列。

在一段时间过后，您便会开发出可使工作流更简便的常用过滤器和报告。 Sentinel 完全支持储存此信息并将其分配给组织中的用户。有关详细信息，请参阅 *《NetIQ Sentinel 7.1 用户指南》*。

2.12 Sentinel 数据路由和储存

Sentinel 提供了多个用于路由、储存和提取所收集数据的选项。默认情况下， Sentinel 会从收集器管理器接收两个独立但相关的数据流：已分析的事件数据和原始数据。原始数据将立即储存在受保护分区以提供安全的证据链。已分析的事件数据将根据您定义的规则进行路由，并可以过滤出来，发送到储存，发送到实时分析，以及路由到外部系统。发送到储存的所有事件数据将进一步与用户定义的保留策略进行匹配，后者可确定数据将放入哪个分区，并且还可定义清理策略，根据该策略，将保留然后最终删除事件数据。

Sentinel 的数据储存基于三层结构：

- **联机储存**
  - **主储存或本地储存：**经过优化，可实现快速写入和检索。最近收集的事件数据（以及最常搜索的内容）储存在此处。
  - **辅助储存或网络储存：**经过优化，可在仍支持快速检索的同时，减少空间使用量。 Sentinel 会自动将数据分区迁移到辅助储存。

  注释：使用辅助储存是可选的。数据保留策略、搜索和报告对事件数据分区执行操作，而不管它们实际是位于主储存、辅助储存还是两者。

- **脱机储存或存档储存：**

  关闭分区后，您可以将已关闭的分区备份到脱机储存，如便宜的海量储存、 Amazon Glacier 等。如有必要，您可以临时重新导入脱机分区，以进行长期司法分析。

您还可以将 Sentinel 配置为使用数据同步策略，将事件数据和事件数据摘要提取到外部数据库。有关详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》*中的“ 配置数据储存 ”。

计划 Sentinel 安装

本节将指导您完成安装 Sentinel 之前的注意事项规划。如果您要安装后续章节中未涉及到的配置，或者您有任何问题，请与 NetIQ 技术支持联系。

3 实现核对清单

使用以下核对清单完成 Sentinel 的计划、安装和配置：

❒	任务	参见
❒	复查产品体系结构信息，以了解 Sentinel 部件。	第 I 部分 “ 了解 Sentinel” （第 13 页）。
❒	复查 Sentinel 许可，以确定是需要安装试用版的 Sentinel 还是企业版的 Sentinel。	第 4 章 “ 了解许可证信息 ” （第 31 页）。
❒	评估您的环境以确定硬件配置。确保安装 Sentinel 及其部件的计算机满足指定的要求。	第 5 章 “ 满足系统要求 ” （第 33 页）。
❒	默认情况下， Sentinel 附带了收集器管理器和关联引擎。复查收集器管理器和关联引擎每秒事件数 (EPS)，并确定您是否需要安装附加收集器管理器和关联引擎以提高性能和改善负载平衡。	第 9.1 节 “ 附加收集器管理器的优势 ”（第 61 页）和 第 9.2 节 “ 附加关联引擎的优势 ” （第 62 页） .
❒	安装 Sentinel。	第 III 部分 “ 安装 Sentinel” （第 59 页）。
❒	确保在 Sentinel 服务器上配置时间。	第 16 章 “ 配置时间 ” （第 95 页）。
❒	当您安装 Sentinel 时，将默认安装在发布 Sentinel 时提供的 Sentinel 插件。出于数据收集和报告目的，配置即用型插件。	第 17 章 “ 配置即用型插件 ” （第 99 页）。
❒	根据需要在您的环境中安装附加收集器和连接器。	第 13 章 “ 安装附加的收集器和连接器 ” （第 87 页）。
❒	根据需要在您的环境中安装附加收集器管理器和关联引擎。	第 11.6 节 “ 安装附加的收集器管理器和关联引擎 ” （第 71 页）。

4 了解许可证信息

Sentinel 提供了多个许可证供您使用。默认情况下， Sentinel 附带了试用许可证。

4.1 试用许可证

Sentinel 默认许可证允许您在 90 天的评估期内，使用 Sentinel 的所有企业功能。使用试用许可证运行的系统会在 Web 界面上显示一个指示器，指示使用了临时许可证密钥。它还显示了离功能过期所剩的天数，指示如何升级到完整许可证。

注释： 系统的失效日期基于系统中的最早数据。如果您在系统中恢复了较早的事件，则将会相应地调整失效日期。

在 90 天的试用期过后，大部分功能将会禁用，但是您仍然可以登录并更新系统以使用企业许可证密钥。

在升级到企业许可证之后，所有功能都将恢复。为了避免任何功能上的中断，必须在过期之前使用企业许可证升级系统。

4.2 企业许可证

在购买 Sentinel 时，您会通过客户门户收到一个许可证密钥。取决于您购买的产品，您的许可证密钥会启用某些功能、数据收集速率和事件源。可能存在许可证密钥未强制遵循的其他许可证条款，因此请仔细阅读许可证协议。

要更改许可证，请联系您的帐户管理员。要将许可证密钥添加到系统，请参见 *《NetIQ Sentinel 7.1 管理指南》*。

5 满足系统要求

本章将介绍 Sentinel 的硬件、操作系统和浏览器要求。

5.1 支持的操作系统和平台

NetIQ 支持在本节介绍的操作系统上运行 Sentinel。 NetIQ 还支持在安装了这些操作系统的次要更新（如安全补丁或热修复）的系统上运行 Sentinel。但是，在 NetIQ 对这些操作系统的主要更新进行测试并认证之前， NetIQ 不支持在安装了这些主要更新的系统上运行 Sentinel。

NetIQ 支持以下操作系统和平台上的 Sentinel 服务器、收集器管理器和关联引擎：

类别	要求
操作系统	Sentinel 支持以下操作系统： ◆ SUSE Linux Enterprise Server (SLES) 11 SP2 64 位 * ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 （64 位） * SLES 的 Open Enterprise Server 安装不支持 Sentinel **重要：**对于传统安装，请确保在您的操作系统中启用了 Internet 协议版本 6 (IPv6)。如果未启用 IPv6，则主要部件将无法运行。 对于设备安装，默认情况下启用 IPv6。
虚拟平台	NetIQ 提供了在以下虚拟平台上安装 SLES 11 SP2 64 位服务器和 Sentinel 的设备： ◆ VMWare ESX 4.0 和 5.0 ◆ Xen 4.0

类别	要求
DVD ISO	NetIQ 提供了一个在以下平台上安装 SLES 11 SP2 （64 位）和 Sentinel 的 DVD ISO 文件： ◆ Hyper-V Server 2008 R2 ◆ 未安装操作系统的硬件
文件系统	**传统安装：** ◆ **在 SLES 系统上：**Sentinel 支持 ext3 和 XFS 文件系统。 ◆ **在 RHEL 系统上：**Sentinel 支持 ext4 和 XFS 文件系统。 **设备安装：** Sentinel 使用 ext3 文件系统。 有关文件系统的详细信息，请参见 *《SLES 11 SP2 储存管理指南》*中的 Linux 中的文件系统概述 (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html)。

5.2 支持的数据库平台

Sentinel 包含一个基于文件的嵌入式储存系统和 PostgreSQL 数据库，二者都是运行 Sentinel 所必需的。但是，如果您使用可选的数据同步功能将数据复制到数据仓库，则 Sentinel 支持将 PostgreSQL、Oracle 11g R2 版本或 Microsoft SQL Server 2008 R2 用作数据仓库。

5.3 支持的浏览器

Sentinel Web 界面进行了优化，以供在以下受支持的浏览器中以 1280 x 1024 或更高分辨率查看：

注释：要正确装载 Sentinel 客户端应用程序，您必须在系统上安装 Java Webstart。

平台	浏览器
Windows 7	◆ Firefox 版本 5 至版本 18 ◆ Internet Explorer 8、 9 和 10.* 有关 Internet Explorer 8 的信息，请参阅 Internet Explorer 的先决条件 （第 34 页）。
SLES 11 SP2 和 RHEL 6	◆ Firefox 版本 5 至版本 18

5.3.1 Internet Explorer 的先决条件

如果因特网安全级别设置为 “ 高 ”，则在登录 Sentinel 后会显示空白页，并且浏览器可能会阻止文件下载弹出窗口。要解决此问题，您需要首先将安全级别设置为 “ 中 - 高 ”，然后更改到自定义级别，如下所示：

1. 导航到*工具* > *Internet 选项* > *安全*选项卡，然后将安全级别设置为*中 - 高*。

2. 确保*工具 > 兼容性视图*选项未选中。
3. 导航到*工具 > Internet 选项 > 安全选项卡 > 自定义级别*，然后向下滚动到*下载*部分，并在*文件下载的自动提示*选项下选择*启用*。

5.4 系统大小信息

Sentinel 实现可能因环境需要而异，因此，在最终确定 Sentinel 体系结构之前，您应该先咨询 NetIQ 咨询服务部门或任何 NetIQ Sentinel 合作伙伴。

本节提供的大小信息基于在 NetIQ 使用测试时提供给我们的硬件执行的测试。可能存在着功能更强大且可以处理更大负载的大型硬件配置。

一体机配置将所有处理负载都置于 Sentinel 服务器上，而不是将负载分配到远程收集器管理器和关联引擎。虽然一体机配置对于只以有限方式使用少部分功能的简单方案很管用，但在使用大量功能或以广泛方式使用时，它们不能很好地扩展。例如，如果您使用多个即用型关联规则，这会使系统上的负载增大，并可能导致同一服务器上的其他功能由于关联引擎的资源使用率增加而受到影响。

- 当使用的收集器不在少数时，需要将负载分配到远程收集器管理器。
- 当您使用多个即用型关联规则时，需要将负载分配到远程关联引擎。
- 当您计划增加要使用的功能数或以广泛方式使用时，分配负载不失为好主意。

事实证明， CPU 执行超线程的能力对系统可以处理的负载有着重大的积极影响。因此，在决定要购买哪种 CPU 时，一定要注意在下面的参照测试中是否启用了超线程，并确保您选择的 CPU 具有良好或较好的超线程功能。

类别	描述	演示一体机 不能用于生产	中型一体机	基于代理的中型数据收集	大型一体机	大型分布式无代理数据收集	特大型
保留 EPS 功能	每秒事件数率由实时部件处理并由系统保留在储存中。	100 EPS	2500 EPS	2500 EPS	9000 EPS	11000 EPS	11000+ EPS
操作 EPS 功能	系统每秒从事件源收到的总事件数率。这包括在储存数据前由系统的智能过滤功能丢弃的数据，并且此数字用于基于 EPS 的许可证合规性目的。	100 EPS	2500+ EPS	2500+ EPS	9000 EPS	16000 EPS	16000+ EPS
Sentinel 服务器硬件							

类别	描述	演示一体机 不能用于生产	中型一体机	基于代理的中型数据收集	大型一体机	大型分布式无代理数据收集	特大型
CPU		Intel Xeon CPU E5420 @ 2.50GHz（4 个 CPU 核），不带超线程功能	双 Intel Xeon CPU E5450 @ 3.00GHz（每个 CPU 4 个内核；共 8 个内核），不带超线程功能	双 AMD Opteron 2431 @ 2.40 GHz（每个 CPU 6 个内核；共 12 个内核）	双 Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz （8 核） CPU（共 16 核），带超线程功能		联系 NetIQ 服务
本地存储	本地超速缓存数据，可提高搜索性能。	500 GB 7.2k RPM 驱动器	5 个 300 GB SAS 15k RPM（硬件 RAID 0）	3 个 146 GB SAS 10K RPM（RAID 0，条带大小 128k）	5 TB， 8 个 600 GB SAS 15k RPM （硬件 RAID 0，条带大小 128k）		
网络储存	包括本地储存中的数据副本。	未用	未用	未用	未用		
内存		4 GB	24 GB	16 GB	64 GB		
远程收集器管理器 # 1 硬件							
CPU		不适用 （仅限本地嵌入式 CM）				双 Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz （8 核） CPU （共 16 核），带超线程功能	联系 NetIQ 服务
储存						20 GB 可用空间	联系 NetIQ 服务
内存						24 GB	
远程收集器管理器 # 2 硬件							

类别	描述	演示一体机 不能用于生产	中型一体机	基于代理的中型数据收集	大型一体机	大型分布式无代理数据收集	特大型
CPU		不适用 （仅限本地嵌入式 CM）				8 核 Intel(R) Xeon(R) CPU X5570 @ 2.93GHz （虚拟机）	联系 NetIQ 服务
储存						50 GB	
内存						8 GB	
代理管理器硬件							
CPU		不适用 （仅限无代理收集）		双 Intel Xeon 5140 @ 2.33 GHz （每个 CPU 2 个内核；共 4 个内核）	不适用 （仅限无代理收集）		联系 NetIQ 服务
储存				2 个 300 GB SAS 10K RPM （RAID 0，条带大小 128k）			
内存				16 GB			
远程关联引擎硬件							
CPU		不适用 （仅限本地嵌入式 CE）					联系 NetIQ 服务
储存							
内存							

类别	描述	演示一体机 不能用于生产	中型一体机	基于代理的中型数据收集	大型一体机	大型分布式无代理数据收集	特大型
数据收集							
收集器管理器 (CM) 分配	放置在每个收集器管理器上的事件源数和每秒事件数负载。 过滤百分比表示收集后立即过滤出多少规范化事件，而不进行储存或传递到分析引擎。请注意，这些规范化事件所基于的非规范化原始日志数据不受过滤影响，并始终储存。 本地嵌入式 CM 位于 Sentinel 服务器计算机上。	**本地嵌入式 CM** 事件源：101 EPS：100 已过滤：0%	**本地嵌入式 CM** 事件源：2500 EPS：2500 已过滤：0%	**本地嵌入式 CM** 事件源：5000 EPS：2500 已过滤：0%	**本地嵌入式 CM** 事件源：500 EPS：9000 已过滤：0%	**本地嵌入式 CM** 未用 **远程 CM #1** 事件源：110 EPS：9500 已过滤：21% 原始数据已禁用 **远程 CM #2** 事件源：20 EPS：6500 已过滤：54% 原始数据已禁用	联系 NetIQ 服务

类别	描述	演示一体机 不能用于生产	中型一体机	基于代理的中型数据收集	大型一体机	大型分布式无代理数据收集	特大型
已使用的收集器		**IBM AIX 6.1r3** 源：100 EPS：99 **NetIQ Universal Event 2011.1r1** 源：1 EPS：1	每个收集器都有自己的 syslog 服务器。 **Oracle Solaris 6.1r3** 源：1000 EPS：1000 **IBM AIX 6.1r3** 源：1000 EPS：1000 **Sourcefire Snort 2011.1r1** 源：500 EPS：500	自定义测试收集器（无分析） **代理管理器连接器服务器 1** 源：5000 EPS：2500	以下每个收集器均有自己的 syslog 服务器，以如下 EPS 速率进行分析： **Oracle Solaris 6.1r3** EPS：2000 **Sourcefire Snort 2011.1r1** EPS：1500 **NetIQ Universal Event 2011.1r1** EPS：2000 **Juniper Netscreen Series 2011.1r1** EPS：1500 **IBM AIX 6.1r3：2000** EPS：2000	以下每个收集器均有自己的 syslog 服务器，以如下 EPS 速率进行分析： **Oracle Solaris 6.1r3** RCM #1：2000 RCM #2：2000 **Sourcefire Snort 2011.1r1** RCM #1：2000 RCM #2：1000 **NetIQ Universal Event 2011.1r1** RCM #1：2000 RCM #2：0 **Juniper Netscreen Series 2011.1r1** RCM #1：2000 RCM #2：1500	联系 NetIQ 服务

类别	描述	演示一体机 不能用于生产	中型一体机	基于代理的中型数据收集	大型一体机	大型分布式无代理数据收集	特大型
						IBM AIX 6.1r3 RCM #1：1500 RCM #2：0 **IBM iSeries 2011.1r3** RCM #1：0 RCM #2：2000	联系 NetIQ 服务
Total		事件源：101 EPS：100 已过滤：0%	事件源：2500 EPS：2500 已过滤：0%	事件源：5000 EPS：2500 已过滤：0%	事件源：500 EPS：9000 已过滤：0%	事件源：130 操作 EPS：16000 保留 EPS：11000 已过滤：25%	
数据存储							
用户将定期搜索过去多久的数据？	为提高搜索性能而本地超速缓存的数据量。	7 天					联系 NetIQ 服务
什么搜索百分比将覆盖上述天数以前的数据？	影响本地或网络储存每秒输入 / 输出操作数量 (IOPS)	10%					
必须保留过去多久的数据？	影响保留所有数据所需的磁盘空间量。如果启用了网络储存，这会影响所需的网络储存大小。否则，它会影响所需的本地储存大小。	14 天					

类别	描述	演示一体机 不能用于生产	中型一体机	基于代理的中型数据收集	大型一体机	大型分布式无代理数据收集	特大型
网络储存设备是否将可用并连接？	影响所有数据是将本地储存还是网络储存可用于成本较低的长期联机储存。网络储存中的数据保持联机状态。	否					联系 NetIQ 服务
将使用摘要和其他数据同步策略优化多少报告？	影响数据同步策略的数量，该数量影响本地储存的大小和 IOPS。	5 （即用型）			4 （即用型，源摘要 RDD 除外，该项落在后面）		
用户活动							
平均有多少用户将同时处于活动状态？	影响本地和网络储存及其他项目的 IOPS 数量。	1					联系 NetIQ 服务
平均而言，活动用户将同时执行多少个搜索？	影响本地和网络储存的 IOPS 数量。	1 个搜索或报告 （但两者不能同时存在），每个报告 20k 事件，每个搜索 100M 事件		未使用搜索或报告负载进行测试	1 每个搜索 80M 事件	1 每个搜索 20M 事件	
平均而言，活动用户将同时运行多少个报告？	影响本地和网络储存的 IOPS 数量。	1 个搜索或报告 （但两者不能同时存在），每个报告 20k 事件，每个搜索 100M 事件		未使用搜索或报告负载进行测试	1 每个报告 1k 事件	1 每个报告 60k 事件、5k 页面	
分析							
与关联规则相关的事件数据百分比是多少？	关联引擎将处理的数据量。	100% （即用型） （每秒 3 个关联）		100% （即用型） （每秒 0 个关联）	0%	0% （有些数据到达太晚无法进行实时关联）	联系 NetIQ 服务

类别	描述	演示一体机 不能用于生产	中型一体机	基于代理的中型数据收集	大型一体机	大型分布式无代理数据收集	特大型
将使用多少个简单关联规则 （仅过滤 / 触发）？	影响关联引擎的 CPU 占用率。	84 个 （即用型）			0		联系 NetIQ 服务
将使用多少个复杂关联规则？	影响关联引擎的 CPU 占用率和内存使用率。	0 个 （即用型）					
关联引擎 (CE) 分配		本地嵌入式 CE （所有规则）					
将对多少数据集执行异常检测？	安全智能仪表板数，该数字影响 CPU 占用率、本地储存大小和内存使用率。	1 （每个事件流的 1%）		0			
高可用性							
注释	当超出上述系统负载时，显式功能遭禁用或发出事件警告。				原始数据已禁用 未使用的关联和安全智能 报告的事件超出 30k 会导致不稳定	原始数据已禁用 未使用的关联和安全智能 报告的事件数大于上述数量会导致不稳定 增加保留的 EPS 将最终在此系统配置中导致不稳定	联系 NetIQ 服务

5.5 计划数据储存的分区

安装 Sentinel 时，您必须将本地储存的磁盘分区装入安装 Sentinel 的同一位置，默认情况下为 /var/opt/novell 目录。

/var/opt/novell/sentinel 目录下的整个目录结构必须位于单个磁盘分区，以确保磁盘用量计算正确。否则，自动数据管理功能可能会提前删除事件数据。有关 Sentinel 目录结构的详细信息，请参见 第 15 章 “Sentinel 目录结构 ”（第 91 页）。

最佳做法是，确保此数据目录位于与可执行文件、配置和操作系统文件所在磁盘分区不同的磁盘分区。单独储存变量数据的好处包括更易于备份文件集、在损坏时恢复更简单，以及在磁盘分区已满时提高稳健性。它还提高了系统的总体性能，文件越小，系统效率越高。有关详细信息，请参见 “ 磁盘分区 ”。

5.5.1 在传统安装中使用分区

在传统安装中，您可以在安装 Sentinel 之前修改操作系统的磁盘分区布局。管理员应该基于第 15 节 “Sentinel 目录结构 ”（第 91 页）中详细介绍的目录结构来创建想要的分区，并将它挂载到适当的设备上。在运行安装程序时， Sentinel 会安装到预先创建的目录中，从而使安装跨越多个分区。

注释：

- 您可以在运行安装程序时使用 --location 选项指定与默认目录不同的顶层位置来储存文件。将您传给 --location 选项的值附加到目录路径前面。例如，如果指定 --location=/foo，数据目录将为 /foo/var/opt/novell/sentinel/data，配置目录将为 /foo/etc/opt/novell/sentinel/config。
- 不得对 --location 选项使用文件系统链接 （如软链接）。

5.5.2 在设备安装中使用分区

使用 DVD ISO 设备格式，您可以在安装过程中配置设备文件系统分区。例如，您可以为 /var/opt/novell/sentinel 安装点创建一个单独的分区，以将所有数据都放在一个单独的分区。但是，对于其他设备格式，您只能在安装后配置分区。您可以使用 SuSE YaST 系统配置工具添加分区并将目录移到新的分区。有关在安装后创建分区的信息，请参见第 12.4.2 节 “ 创建分区 ”（第 83 页）。

5.6 连接器和收集器系统要求

每个连接器和收集器都有自己的一些系统要求和支持的平台。请参阅 Sentinel 插件网页 (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) 上的连接器和收集器文档。

5.7 虚拟环境

Sentinel 经过广泛测试，完全支持 VMware ESX 服务器。当设置虚拟环境时，虚拟机必须拥有两个或更多 CPU。要在 ESX 或其他任何虚拟环境中获得与物理计算机类似的性能测试结果，虚拟环境应提供与物理计算机建议配置相同的内存、 CPU、磁盘空间以及 I/O 条件。

有关物理计算机建议配置的详细信息，请参阅第 5 章 “ 满足系统要求 ”（第 33 页）。

6 在 FIPS140-2 模式下操作 Sentinel 的部署注意事项

可以有选择地将 Sentinel 配置为使用 Mozilla 网络安全服务 (NSS) 实现其内部加密和其他功能，因为该服务是经过 FIPS 140-2 验证的加密提供程序。这样做的目的是确保 Sentinel 获得 “FIPS 140-2 Inside”，并符合美国联邦采购政策和标准。

如果启用 Sentinel FIPS 140-2 模式，则将导致 Sentinel 服务器、Sentinel 远程收集器管理器、Sentinel 远程关联引擎、 Sentinel Web UI、 Sentinel 控制中心和 Sentinel Advisor 服务之间的通讯使用经过 FIPS 140-2 验证的加密法。

6.1 Sentinel 中的 FIPS 实现

Sentinel 使用操作系统提供的 Mozilla NSS 库。 Red Hat Enterprise Linux (RHEL) 和 SUSE Linux Enterprise Server (SLES) 具有不同的 NSS 包。

RHEL 6.2 提供的 NSS 加密模块已经过 FIPS 140-2 验证。 SLES 11 SP2 提供的 NSS 加密模块尚未经过 FIPS 140-2 正式验证，但是 SUSE 模块正在接受 FIPS 140-2 验证。在经过验证后，无需事先对 Sentinel 进行更改，即可在 SUSE 平台上提供 “FIPS 140-2 Inside”。

有关 RHEL 6.2 FIPS 140-2 认证的详细信息，请参见*经过 FIPS 140-1 和 FIPS 140-2 验证的加密模块*。

6.1.1 RHEL NSS 包

Sentinel 需要使用以下 64 位 NSS 包支持 FIPS 140-2 模式：

- nspr-4.9-1.el6.x86_64
- nss-sysinit-3.13.3-6.el6.x86_64
- nss-util-3.13.3-2.el6.x86_64
- nss-softokn-freebl-3.12.9-11.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64
- nss-3.13.3-6.el6.x86_64
- nss-tools-3.13.3-6.el6.x86_64

如果未安装其中任意一个包，则只有在安装该包之后，才能在 Sentinel 中启用 FIPS 140-2 模式。

6.1.2 SLES NSS 包

Sentinel 需要使用以下 64 位 NSS 包支持 FIPS 140-2 模式：

- libfreebl3-3.13.1-0.2.1
- mozilla-nspr-4.8.9-1.2.2.1
- mozilla-nss-3.13.1-0.2.1
- mozilla-nss-tools-3.13.1-0.2.1

如果未安装其中任意一个包，则只有在安装该包之后，才能在 Sentinel 中启用 FIPS 140-2 模式。

6.2 Sentinel 中启用 FIPS 的部件

以下 Sentinel 部件提供 FIPS 140-2 支持：

- 所有 Sentinel 平台部件都已经过更新，可以支持 FIPS 140-2 模式。
- 以下支持加密法的 Sentinel 插件已经过更新，可以支持 FIPS 140-2 模式：
  - 代理管理器连接器 2011.1r1 和更高版本
  - 数据库 (JDBC) 连接器 2011.1r2 和更高版本
  - 文件连接器 2011.1r1 和更高版本 （仅当文件事件源类型为本地或 NFS 时）。
  - LDAP Integrator 2011.1r1 和更高版本
  - Sentinel Link 连接器 ·2011.1r3 和更高版本
  - Sentinel Link Integrator 2011.1r2 和更高版本
  - SMTP 集成器 2011.1r1 和更高版本
  - Syslog 连接器 2011.1r2 和更高版本
  - Windows 事件 (WMI) 连接器 2011.1r2 和更高版本

  有关将这些 Sentinel 插件配置为在 FIPS 140-2 模式下运行的详细信息，请参见将 Sentinel 插件配置为在 FIPS 140-2 模式下运行 （第 105 页）。

在发布本文档时，以下支持可选加密法的 Sentinel 连接器尚未经过更新，无法支持 FIPS 140-2 模式。但是，您可以继续使用这些连接器收集事件。有关将这些连接器与处于 FIPS 140-2 模式的 Sentinel 一起使用的说明，请参见将不启用 FIPS 的连接器与处于 FIPS 140-2 模式的 Sentinel 一起使用 （第 110 页）。

- 检查点 (LEA) 连接器 2011.1r2
- Cisco SDEE 连接器 2011.1r1
- 文件连接器 2011.1r1 （CIFS 和 SCP 功能涉及加密，不能在 FIPS 140-2 模式下正常工作）。
- NetIQ Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

在发布本文档时，以下支持 SSL 的 Sentinel 集成器尚未经过更新，无法支持 FIPS 140-2 模式。但是，将这些集成器与处于 FIPS 140-2 模式的 Sentinel 一起使用时，可以继续使用未加密的连接。

- Remedy 集成器 2011.1r1 或更高版本
- SOAP 集成器 2011.1r1 或更高版本

上面未列出的任何其他 Sentinel 插件都不使用加密法，因此，在 Sentinel 中启用 FIPS 140-2 模式不会对其产生影响。您无需执行任何附加步骤，即可将它们与处于 FIPS 140-2 模式的 Sentinel 一起使用。

有关 Sentinel 插件的详细信息，请参见 Sentinel 插件网站。如果您要请求其中某个尚未更新的插件提供 FIPS 支持，请使用 Bugzilla 提交请求。

6.3 实现核对清单

下表概述了将 Sentinel 配置为在 FIPS 140-2 模式下操作所需执行的任务。

任务	有关详细信息，请参见 ...
计划部署。	第 6.4 节 “ 部署方案 ”（第 47 页）。
确定您是需要在安装 Sentinel 期间启用 FIPS 140-2 模式，还是需要在以后启用该模式。 要在安装期间启用 Sentinel 的 FIPS 140-2 模式，您需要在安装过程中选择自定义或无提示安装方法。	第 11.2.2 节 “ 自定义安装 ”（第 67 页）。 第 11.3 节 “ 执行无提示安装 ”（第 68 页） 第 18 章 “ 在现有的 Sentinel 安装中启用 FIPS 140-2 模式 ”（第 101 页）
将 Sentinel 插件配置为在 FIPS 140-2 模式下运行。	第 19.5 节 “ 将 Sentinel 插件配置为在 FIPS 140-2 模式下运行 ”（第 105 页）。
将证书导入 Sentinel FIPS 密钥存储区。	第 19.6 节 “ 将证书导入 FIPS 密钥存储区数据库 ”（第 110 页）

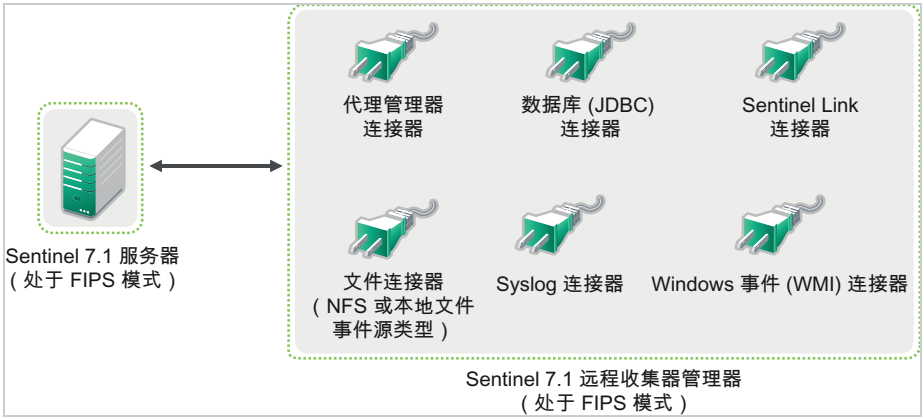
注释： NetIQ 强烈建议在开始转换到 FIPS 模式之前，创建 Sentinel 系统的备份。如果出于某种原因而必须将服务器还原为非 FIPS 模式，则唯一支持这样做的方法就是从备份中恢复。有关还原为非 FIPS 模式的详细信息，请参见将 Sentinel 还原为非 FIPS 模式 （第 110 页）。

6.4 部署方案

本节将介绍处于 FIPS 140-2 模式的 Sentinel 的部署方案。

6.4.1 方案 1：完全 FIPS 140-2 模式下的数据收集

在此方案中，只能通过支持 FIPS 140-2 模式的连接器执行数据收集。我们假定此环境包含一个 Sentinel 服务器，并通过远程收集器管理器收集数据。您可能拥有一个或多个远程收集器管理器。



仅当您的环境涉及到使用支持 FIPS 140-2 模式的连接器从事件源收集数据时，才能执行以下过程。

1 必须拥有一个处于 FIPS 140-2 模式的 Sentinel 7.1 服务器。

注释：如果 （全新安装或升级的） Sentinel 服务器处于非 FIPS 模式，则必须在 Sentinel 服务器上启用 FIPS。有关详细信息，请参见启用 Sentinel 服务器以在 FIPS 140-2 模式下运行 （第 101 页）。

2 必须拥有一个在 FIPS 140-2 模式下运行的 Sentinel 7.1 远程收集器管理器。

注释：如果 （全新安装或升级的）远程收集器管理器是在非 FIPS 模式下运行的，则必须在该远程收集器管理器上启用 FIPS。有关详细信息，请参见在远程收集器管理器和关联引擎上启用 FIPS 140-2 模式 （第 101 页）。

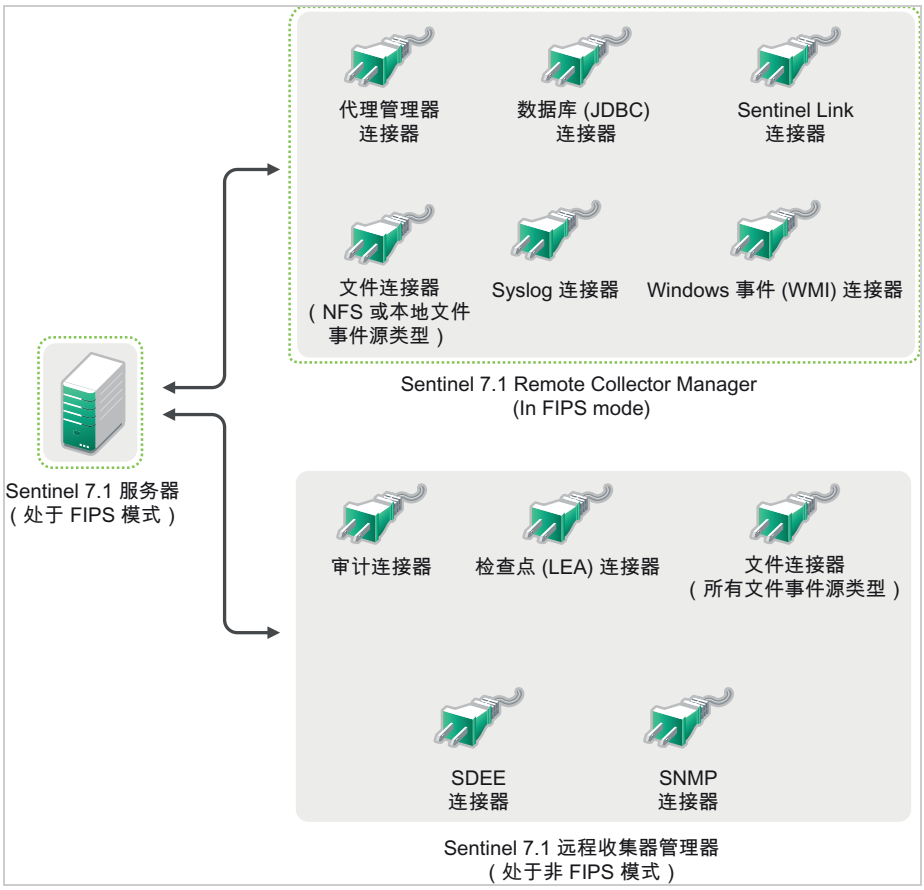
3 确保 FIPS 服务器和远程收集器管理器能够互相通讯。

4 将远程关联引擎 （如果有）转换为在 FIPS 模式下运行。有关详细信息，请参见在远程收集器管理器和关联引擎上启用 FIPS 140-2 模式 （第 101 页）。

5 将 Sentinel 插件配置为在 FIPS 140-2 模式下运行。有关详细信息，请参见将 Sentinel 插件配置为在 FIPS 140-2 模式下运行 （第 105 页）。

6.4.2 方案 2：部分 FIPS 140-2 模式下的数据收集

在此方案中，将使用支持 FIPS 140-2 模式的连接器以及不支持 FIPS 140-2 模式的连接器执行数据收集。我们假定此环境包含一个 Sentinel 服务器，并通过远程收集器管理器收集数据。您可能拥有一个或多个远程收集器管理器。



要使用支持和不支持 FIPS 140-2 模式的连接器处理数据收集，建议您拥有两个远程收集器管理器：一个在 FIPS 140-2 模式下运行，用于支持 FIPS 的连接器；另一个在非 FIPS （正常）模式下运行，用于不支持 FIPS 140-2 模式的连接器。

如果您的环境涉及到使用支持 FIPS 140-2 模式的连接器以及尚未支持 FIPS 140-2 模式的连接器从事件源收集数据，则必须执行以下过程。

1 必须拥有一个处于 FIPS 140-2 模式的 Sentinel 7.1 服务器。

注释：如果 （全新安装或升级的） Sentinel 服务器处于非 FIPS 模式，则必须在 Sentinel 服务器上启用 FIPS。有关详细信息，请参见启用 Sentinel 服务器以在 FIPS 140-2 模式下运行 （第 101 页）。

---

2 确保一个远程收集器管理器在 FIPS 140-2 模式下运行，而另一个远程收集器管理器继续在非 FIPS 模式下运行。

2a 如果您没有启用 FIPS 140-2 模式的远程收集器管理器，则必须在远程收集器管理器上启用 FIPS 模式。有关详细信息，请参见在远程收集器管理器和关联引擎上启用 FIPS 140-2 模式（第 101 页）。

2b 在非 FIPS 远程收集器管理器上更新服务器证书。有关详细信息，请参见在远程收集器管理器和关联引擎中更新服务器证书 （第 105 页）。

3 确保两个远程收集器管理器能够与启用 FIPS 140-2 的 Sentinel 服务器进行通讯。

4 将远程关联引擎 （如果有）转换为在 FIPS 模式下运行。有关详细信息，请参见在远程收集器管理器和关联引擎上启用 FIPS 140-2 模式 （第 101 页）。

5 将 Sentinel 插件配置为在 FIPS 140-2 模式下运行。有关详细信息，请参见将 Sentinel 插件配置为在 FIPS 140-2 模式下运行 （第 105 页）。

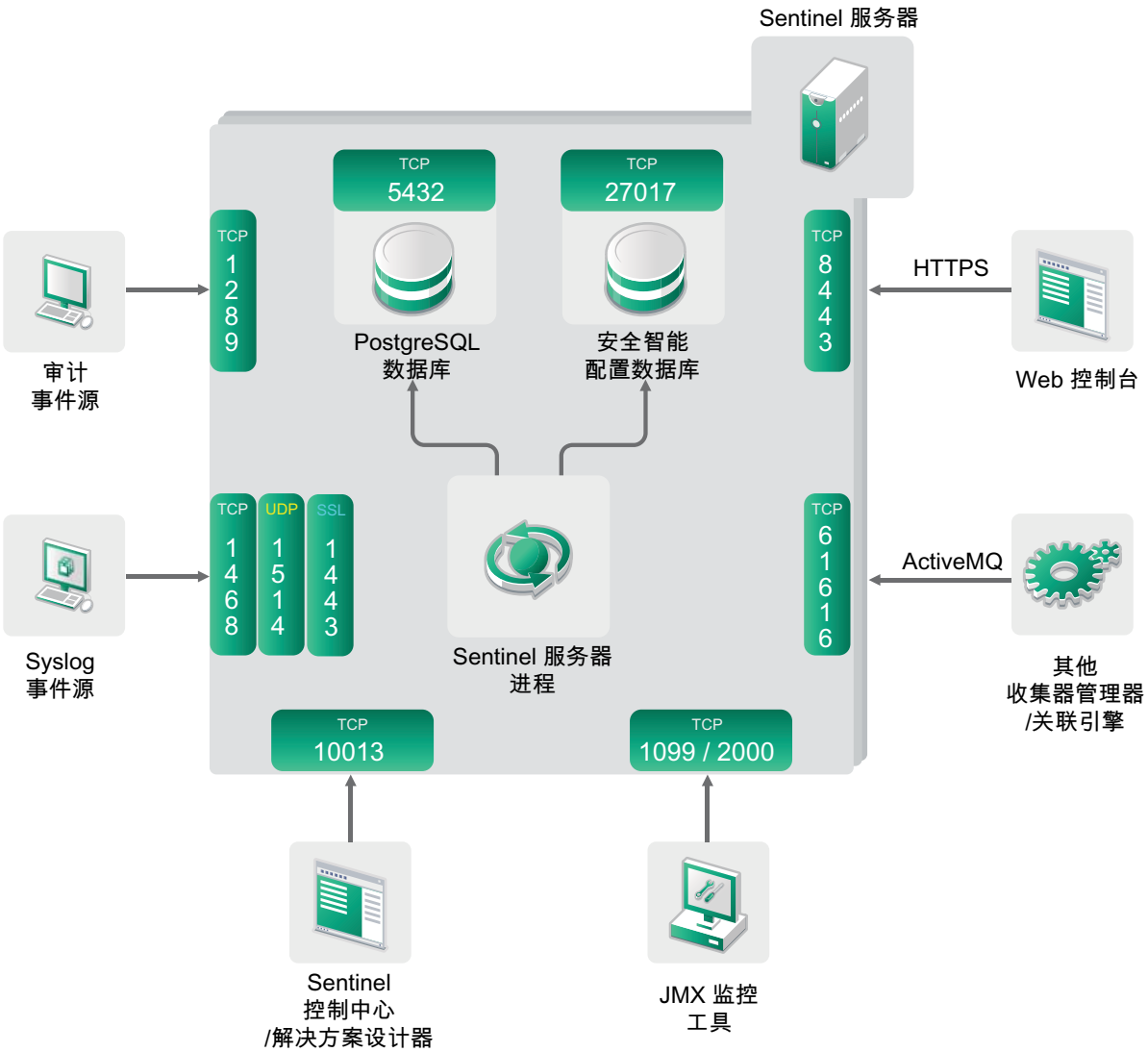
5a 在以 FIPS 模式运行的远程收集器管理器中部署支持 FIPS 140-2 模式的连接器。

5b 在非 FIPS 远程收集器管理器中部署不支持 FIPS 140-2 模式的连接器。

7 使用的端口

Sentinel 使用不同的端口与其他组件进行外部通信。对于设备安装，默认情况下会在防火墙上打开这些端口。但是，对于传统安装，您必须配置要安装 Sentinel 的操作系统，以便在防火墙上打开这些端口。下图说明了 Sentinel 中使用的端口：

图 7-1 *Sentinel 中使用的端口*



- 第 7.1 节 “Sentinel 服务器端口 ”（第 52 页）
- 第 7.2 节 “ 收集器管理器端口 ”（第 53 页）
- 第 7.3 节 “ 关联引擎端口 ”（第 54 页）

7.1 Sentinel 服务器端口

Sentinel 服务器使用以下端口进行内外部通讯。

7.1.1 本地端口

Sentinel 使用以下端口与数据库和其他内部进程进行内部通信。

端口	说明
TCP 27017	用于安全智能配置数据库。
TCP 28017	用于安全智能数据库 Web 界面。
TCP 32000	用于封装程序进程和服务器进程之间的内部通讯。

7.1.2 网络端口

为了使 Sentinel 正确运行，请确保在防火墙上打开了以下端口：

端口	方向	必需 / 可选	描述
TCP 5432	入站	可选。默认情况下，此端口只在回写接口上进行侦听。	用于 PostgreSQL database 数据库。无需默认打开此端口。但是，使用 Sentinel SDK 制作报告时，必须打开此端口。有关详细信息，请参见 Sentinel 插件 SDK。
TCP 1099 和 2000	入站	可选	监视工具会结合使用它们，以便通过 Java 管理扩展 (JMX) 连接到 Sentinel 服务器进程。
TCP 1289	入站	可选	用于 Audit 连接。
UDP 1514	入站	可选	用于 syslog 讯息。
TCP 8443	入站	必需	用于 HTTPS 通信。
TCP 1443	入站	可选	用于 SSL 加密 syslog 讯息。
TCP 61616	入站	可选	用于来自收集器管理器和关联引擎的传入连接。
TCP 10013	入站	必需	由 Sentinel 控制中心和解决方案设计器使用。
TCP 1468	入站	可选	用于 syslog 讯息。
TCP 10014	入站	可选	远程收集器管理器使用该端口来通过 SSL 代理连接到服务器。但是，这种情况很少见。默认情况下，远程收集器管理器使用 SSL 端口 61616 连接到服务器。
TCP 443	出站	可选	如果使用 Advisor，该端口将启动与 Advisor 服务的连接，以通过因特网访问 Advisor 更新 URL (https://secure-www.novell.com/sentinel/download/advisor/)。
TCP 8443	出站	可选	如果使用分布式搜索，该端口将启动与其他 Sentinel 系统的连接，以执行分布式搜索。

端口	方向	必需 / 可选	描述
TCP 389 或 636	出站	可选	如果使用 LDAP 鉴定，该端口将启动与 LDAP 服务器的连接。
TCP/UDP 111 和 TCP/UDP 2049	出站	可选	如果网络储存已配置为使用 NFS。
TCP 137、 138、 139、 445	出站	可选	如果网络储存已配置为使用 CIFS。
TCP JDBC （与数据库相关）	出站	可选	如果使用数据同步，该端口将启动与使用 JDBC 的目标数据库的连接。使用的端口依赖于目标数据库。
TCP 25	出站	可选	启动与电子邮件服务器的连接。
TCP 1290	出站	可选	如果 Sentinel 向其他 Sentinel 系统转发事件，此端口将启动与该系统的 Sentinel Link 连接。
UDP 162	出站	可选	如果 Sentinel 向接收 SNMP 陷阱的系统转发事件，该端口将向接收方发送一个包。
UDP 514 或 TCP 1468	出站	可选	当 Sentinel 向接收 Syslog 讯息的系统转发事件时，将使用此端口。如果该端口为 UDP，则它会向接收方发送一个包。如果该端口为 TCP，则它会启动与接收方的连接。

7.1.3 Sentinel 服务器设备特定的端口

除了上述端口之外，还为设备打开了以下端口。

端口	方向	必需 / 可选	描述
TCP 22	入站	必需	用于对 Sentinel 设备进行安全外壳访问。
TCP 54984	入站	必需	由 Sentinel 设备管理控制台 (WebYaST) 使用。还被 Sentinel 设备用于更新服务。
TCP 289	入站	可选	转发到 1289 以进行 Audit 连接。
UDP 443	入站	可选	转发到 8443 以进行 HTTPS 通信。
UDP 514	入站	可选	转发到 1514 以用于 syslog 讯息。
TCP 1290	入站	可选	允许通过 SuSE 防火墙连接的 Sentinel Link 端口。
UDP 和 TCP 40000 - 41000	入站	可选	在配置数据收集服务器 （如， syslog）时可使用的端口。默认情况下， Sentinel 不侦听这些端口。
TCP 443 或 80	出站	必需	启动与因特网上的 NetIQ 设备软件更新储存库的连接，或者与您网络中的订阅管理工具服务的连接。
TCP 80	出站	可选	启动与订阅管理工具的连接。

7.2 收集器管理器端口

收集器管理器使用以下端口与其他部件进行通讯。

7.2.1 网络端口

要使 Sentinel 收集器管理器正确运行，请确保在防火墙上打开了以下端口：

端口	方向	必需 / 可选	描述
TCP 1289	入站	可选	用于 Audit 连接。
UDP 1514	入站	可选	用于 syslog 讯息。
TCP 1443	入站	可选	用于 SSL 加密 syslog 讯息。
TCP 1468	入站	可选	用于 syslog 讯息。
TCP 1099 和 2000	入站	可选	监视工具会结合使用它们，以便通过 Java 管理扩展 (JMX) 连接到 Sentinel 服务器进程。
TCP 61616	出站	必需	启动与 Sentinel 服务器的连接。

7.2.2 收集器管理器设备特定的端口

除了上述端口之外，还为 Sentinel 收集器管理器设备打开了以下端口。

端口	方向	必需 / 可选	描述
TCP 22	入站	必需	用于对 Sentinel 设备进行安全外壳访问。
TCP 54984	入站	必需	由 Sentinel 设备管理控制台 (WebYaST) 使用。还被 Sentinel 设备用于更新服务。
TCP 289	入站	可选	转发到 1289 以进行 Audit 连接。
UDP 514	入站	可选	转发到 1514 以用于 syslog 讯息。
TCP 1290	入站	可选	这是允许通过 SuSE 防火墙进行连接的 Sentinel 链接端口。
UDP 和 TCP 40000 - 41000	入站	可选	在配置数据收集服务器（如， syslog）时可使用的端口。默认情况下， Sentinel 不侦听这些端口。
TCP 443	出站	必需	启动与因特网上的 NetIQ 设备软件更新储存库的连接，或者与您网络中的订阅管理工具服务的连接。
TCP 80	出站	可选	启动与订阅管理工具的连接。

7.3 关联引擎端口

关联引擎使用以下端口与其他部件进行通讯。

7.3.1 网络端口

要使 Sentinel 关联引擎正确运行，请确保在防火墙上打开了以下端口：

端口	方向	必需 / 可选	描述
TCP 1099 和 2000	入站	可选	监视工具会结合使用它们，以便通过 Java 管理扩展 (JMX) 连接到 Sentinel 服务器进程。
TCP 61616	出站	必需	启动与 Sentinel 服务器的连接。

7.3.2 关联引擎设备特定的端口

除了上述端口之外， Sentinel 关联引擎设备上还打开了以下端口。

端口	方向	必需 / 可选	描述
TCP 22	入站	必需	用于对 Sentinel 设备进行安全外壳访问。
TCP 54984	入站	必需	由 Sentinel 设备管理控制台 (WebYaST) 使用。还被 Sentinel 设备用于更新服务。
TCP 443	出站	必需	启动与因特网上的 NetIQ 设备软件更新储存库的连接，或者与您网络中的订阅管理工具服务的连接。
TCP 80	出站	可选	启动与订阅管理工具的连接。

8 安装选项

您可以执行 Sentinel 的传统安装，也可以安装设备。本章将介绍这两个安装选项。

8.1 传统安装

传统安装就是使用应用程序安装程序，在现有的 SUSE Linux Enterprise Server (SLES) 11 或 Red Hat Enterprise Linux (RHEL) 6 操作系统上安装 Sentinel。 Sentinel 可以采用以下方式进行安装：

- **交互式 :** 安装过程中需要用户输入一些内容。在安装期间，您可以将安装选项 （用户输入或默认值）记录到某个文件中，供以后在执行无提示安装时使用。您可以执行标准安装，也可以执行自定义安装。

标准安装	自定义安装
使用配置的默认值。所需的唯一用户输入是口令。	提示您指定配置设置的值。您可以选择默认值或指定必要的值。
使用默认的 90 天评估密钥进行安装。	允许使用 90 天许可证密钥或有效的许可证密钥进行安装。
允许您指定 Admin 口令，并使用 Admin 口令作为 dbauser 和 appuser 的默认口令。	允许您指定 Admin 口令。对于 dbauser 和 appuser，可以指定新口令或使用 Admin 口令。
对所有组件都安装默认端口。	允许为不同的组件指定端口。
在非 FIPS 模式下安装 Sentinel。	允许您在 FIPS 140-2 模式下安装 Sentinel。
使用内部数据库鉴定用户。	除了提供用于设置数据库鉴定的选项外，还提供用于设置 Sentinel 的 LDAP 鉴定的选项。当您为 LDAP 鉴定配置 Sentinel 时，用户可以使用其 Novell eDirectory 或 Microsoft Active Directory 证书登录到服务器。

有关交互式安装的详细信息，请参见第 11.2 节 “ 执行交互式安装 ”（第 66 页）。

- **无提示：**如果您希望在部署中安装多个 Sentinel 服务器，则可以在执行标准安装或自定义安装期间，将这些安装选项记录在一个配置文件中，然后使用该文件运行无人照管的安装。有关无提示安装的详细信息，请参见第 11.3 节 “ 执行无提示安装 ”（第 68 页）。

8.2 设备安装

设备安装就是同时安装 SLES 11 SP2 64 位操作系统和 Sentinel。

Sentinel 设备采用以下格式：

- VMWare 设备映像

- Xen 设备映像
- 可直接部署到硬件服务器的硬件设备 Live DVD 映像

有关设备安装的详细信息，请参见第 12 章 “ 设备安装 ”（第 75 页）。

安装 Sentinel

本节将介绍如何安装 Sentinel 和附加的部件。

9 安装概述

安装 Sentinel 时将在 Sentinel 服务器中安装以下部件：

- **Sentinel 服务器进程：**这是 Sentinel 的主要部件。 Sentinel 服务器进程将处理来自 Sentinel 的其他部件的请求，并启用无缝的系统功能。 Sentinel 服务器进程可处理各种请求，例如过滤数据，处理搜索查询，以及处理管理任务 （包括用户鉴定和授权）。
- **万维网服务器 :** Sentinel 使用 Jetty 作为其 Web 服务器，以实现与 Sentinel Web 界面的安全连接。
- **PostgreSQL 数据库：**Sentinel 具有一个内置数据库，用于储存 Sentinel 配置信息、资产和漏洞数据、身份信息、事件和工作流程状态，等等。
- **MongoDB 数据库：**储存安全智能数据。
- **收集器管理器 :** 收集器管理器为 Sentinel 提供了一个灵活的数据收集点。 Sentinel 安装程序将在安装期间默认安装一个收集器管理器。
- **关联引擎 :** 关联引擎处理来自实时事件流的事件，以确定是否应触发任何关联规则。
- **Advisor:** Advisor 由 Security Nexus 提供支持，是一种可选的数据订阅服务，用于提供来自入侵检测和预防系统以及企业漏洞扫描结果的实时事件之间的设备级关联。有关 Advisor 的详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》* 中的 “ 配置 Advisor”。
- **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。您可以从 Sentinel 插件网站下载附加的插件和更新。 Sentinel 插件包括以下内容：
  - 收集器
  - 连接器
  - 关联规则和操作
  - 报告
  - iTRAC 工作流程
  - 解决方案包

Sentinel 具有高度可伸缩的体系结构，如果期望事件率较高，则可将部件分布在多台计算机上，以实现系统的最佳性能。对部件进行独立的伸缩可提供经济高效的可伸缩性和性能。

9.1 附加收集器管理器的优势

可以在网络中的适当位置安装附加的收集器管理器。这些远程收集器管理器可以运行连接器和收集器，并将收集的数据转发到 Sentinel 服务器以进行储存和处理。有关安装附加收集器管理器的信息，请参阅第 11.6 节 “ 安装附加的收集器管理器和关联引擎 ”（第 71 页）。

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：**附加的收集器管理器可在分布式环境中分析并处理事件数据，从而提高系统性能。

- **提供了附加数据安全并降低了网络带宽要求：**如果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。
- **文件超速缓存：**当服务器暂时忙于存档事件或处理激增的事件时，附加的收集器管理器可以超速缓存大量数据。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。

注释：一个系统上不能安装多个收集器管理器。您可以在远程系统上安装附加的收集器管理器，然后将它们连接到 Sentinel 服务器。

9.2 附加关联引擎的优势

您可以部署多个关联引擎（每个关联引擎位于其各自的服务器上），而无需复制配置或添加数据库。对于具有大量关联规则或极高事件率的环境，安装多个关联引擎并将某些规则重新部署到新的关联引擎可能很有利。当 Sentinel 系统整合了其他数据源，或者当事件率提高时，多个关联引擎可以提供伸缩功能。有关安装附加关联引擎的信息，请参见第 11.6 节 “ 安装附加的收集器管理器和关联引擎 ”（第 71 页）。

注释：一个系统上不能安装多个关联引擎。您可以在远程系统上安装附加的关联引擎，然后将它们连接到 Sentinel 服务器。

---

10 安装核对清单

在开始安装前，请确保已完成以下任务：

- ❒ 确认您的硬件和软件满足第 5 章 “ 满足系统要求 ”（第 33 页）中列出的系统要求。
- ❒ 如果以前安装过 Sentinel，请确保没有以前的安装所残留的文件或系统设置。有关详细信息，请参见附录 C “ 卸装 ”（第 143 页）。
- ❒ 如果您计划安装许可版本，请从 Novell 客户关怀中心获取许可证密钥。
- ❒ 确保第 7 章 “ 使用的端口 ”（第 51 页）中列出的端口已在防火墙中打开。
- ❒ 要使 Sentinel 安装程序正常工作，系统必须能够返回主机名或有效的 IP 地址。为此，请将主机名添加到 /etc/hosts 文件中包含 IP 地址的行，然后输入 hostname -f 以确保主机名正确显示。
- ❒ 使用网络时间协议 (NTP) 同步时间。
- ❒ **在 RHEL 系统上：**若要获得最佳性能，必须为 PostgreSQL 数据库正确设置内存设置。SHMMAX 参数必须大于等于 1073741824。

  要设置适当的值，请将以下信息追加到 /etc/sysctl.conf 文件中：

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- ❒ **对于传统安装：**
  - ❒ 确保已在您的操作系统中启用了 IPv6。如果未启用 IPv6，则主要部件将无法运行。
  - ❒ Sentinel 服务器的操作系统必须至少包括 SLES 服务器或 RHEL 6 服务器的 Base Server 部件。Sentinel 需要以下 RPM 的 64 位版本：
    - bash
    - bc
    - coreutils
    - gettext
    - glibc
    - grep
    - libgcc
    - libstdc
    - lsof
    - net-tools
    - openssl
    - python-libs
    - sed
    - zlib

11 传统安装

本章将介绍各种 Sentinel 安装方法。

11.1 了解安装选项

./install-sentinel --help 显示以下选项：

选项	值	说明
--location	目录	指定根目录 (/) 以外的目录来安装 Sentinel。
-m, --manifest	文件名	指定除默认清单文件以外要使用的产品清单文件。
--no-configure		指定不在安装后配置产品。
-n, --no-start		指定在安装或配置后不启动或不重新启动 Sentinel。
-r, --recordunattended	文件名	指定一个记录可用于无人照管安装的参数的文件。
-u, --unattended	文件名	使用来自指定文件的参数，以便在无人照管的系统上安装 Sentinel。
-h, --help		显示可在安装 Sentinel 时使用的选项。
-l, --log-file	文件名	将日志讯息记录到某个文件中。
--no-banner		禁止显示标题页讯息。
-q, --quiet		显示更少讯息。
-v, --verbose		显示安装期间的所有讯息。

11.2 执行交互式安装

本节将介绍标准安装和自定义安装。

11.2.1 标准安装

使用以下步骤执行标准安装：

1. 从 Novell 下载网页 (http://download.novell.com/index.jsp) 中下载 Sentinel 安装文件：
   - **1a** 在*产品或技术*字段中，浏览并选择 *SIEM-Sentinel*。
   - **1b** 单击*搜索*。
   - **1c** 单击与 *Sentinel 7.1 评估版*对应的 *下载*列中的按钮。
   - **1d** 单击*继续下载*，然后指定客户名称和口令。
   - **1e** 单击 *下载*获取适合您平台的安装版本。
2. 在命令行指定以下命令来提取安装文件。

   ```
   tar zxvf <install_filename>
   ```

   使用安装文件实际名称替换 <*install_filename*>。
3. 切换到提取安装程序的目录：

   ```
   cd <directory_name>
   ```
4. 指定以下命令来安装 Sentinel：

   ```
   ./install-sentinel
   ```

   或

   如果您希望在多个系统上安装 Sentinel，则可以在一个文件中记录您的安装选项。可将此文件用于其他系统上的无人照管 Sentinel 安装。要记录您的安装选项，请指定以下命令：

   ```
   ./install-sentinel -r <response_filename>
   ```
5. 指定您希望用于安装的语言数量，然后按下 Enter。

   最终用户许可证协议将以选定的语言显示。
6. 按空格键以通读许可证协议。
7. 输入 yes 或 y 以接受许可证并继续安装。

   安装过程中可能会花几分钟加载安装程序包和提示选择配置类型。
8. 在提示时，请指定 1 以使用标准配置继续安装。

   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。
9. 指定管理员用户 admin 的口令。
10. 再次确认此口令。

此口令由 admin、 dbauser 和 appuser 使用。

Sentinel 安装结束，服务器将启动。安装之后，因为系统要执行一次性初始化，所以可能需要花费几分钟来启动所有服务。等待安装完成之后，才能登录到服务器。

要访问 Sentinel Web 界面，请在 Web 浏览器中指定下列 URL：

`https://<IP_Address_Sentinel_server>:8443.`

<IP_Address_Sentinel_server> 是 Sentinel 服务器的 IP 地址或 DNS 名称，8443 是 Sentinel 服务器的默认端口。

11.2.2 自定义安装

如果使用自定义配置安装 Sentinel，则可以指定许可证密钥，为不同用户更改口令，并为用于与内部组件交互的其他端口指定值。

1. 从 Novell 下载网页中下载 Sentinel 安装文件：
   - **1a** 在*产品或技术*字段中，浏览并选择 *SIEM-Sentinel*。
   - **1b** 单击*搜索*。
   - **1c** 单击与 *Sentinel 7.1 评估版*对应的 *下载*列中的按钮。
   - **1d** 单击*继续下载*，然后指定客户名称和口令。
   - **1e** 单击 *下载*获取适合您平台的安装版本。
2. 在命令行指定以下命令来提取安装文件。

   `tar zxvf <install_filename>`

   使用安装文件实际名称替换 <*install_filename*>。
3. 在所提取目录的根中指定以下命令来安装 Sentinel：

   `./install-sentinel`

   或

   如果您希望使用此自定义配置在多个系统上安装 Sentinel，则可以在一个文件中记录您的安装选项。您可将此文件用于其他系统上的无人照管 Sentinel 安装。要记录您的安装选项，请指定以下命令：

   `./install-sentinel -r <response_filename>`
4. 指定您希望用于安装的语言数量，然后按下 Enter。

   最终用户许可证协议将以选定的语言显示。
5. 按空格键以通读许可证协议。
6. 输入 yes 或 y 以接受许可协议并继续安装。

   安装过程中可能会花几分钟加载安装程序包和提示选择配置类型。
7. 指定 2 以执行 Sentinel 的自定义配置。
8. 输入 1 以使用默认的 90 天评估许可证密钥。

   或

   输入 2 以输入购买的 Sentinel 许可证密钥。
9. 指定管理员用户 admin 的口令并再次确认口令。
10. 指定数据库用户 dbauser 的口令并再次确认口令。

dbauser 帐户是 Sentinel 用来与数据库交互的身份。在此处输入的口令可用于执行数据库维护任务，包括在忘记或丢失 admin 口令时重设置 admin 口令。

11 指定应用程序用户 appuser 的口令并再次确认口令。

12 通过输入想要的编号，然后指定新端口号，更改分配给 Sentinel 服务的端口。

13 更改端口之后，指定 7 以完成更改。

14 输入 1 以便仅使用内部数据库来鉴定用户。

或

如果已在域中配置了 LDAP 目录，请输入 2 以使用 LDAP 目录鉴定来鉴定用户。

默认值为 1。

15 ***如果要在 FIPS 140-2 模式下启用 Sentinel***，请按 y。

15a 指定密钥存储区的强口令，然后再次确认口令。

注释：口令必须至少包含七个字符。口令必须至少包含下列其中三种字符：数字、 ASCII 小写字母、 ASCII 大写字母、 ASCII 非字母数字字符和非 ASCII 字符。

如果 ASCII 大写字母是第一个字符，或者数字是最后一个字符，则这些字符将不计算在内。

15b 如果要将外部证书插入密钥存储区数据库以建立信任，请按 y 并指定证书文件的路径。否则，请按 n

15c 执行第 19 章 “ 在 FIPS 140-2 模式下操作 Sentinel”（第 103 页）中所述的任务，以完成 FIPS 140-2 模式配置。

Sentinel 安装结束，服务器将启动。安装之后，因为系统要执行一次性初始化，所以可能需要花费几分钟来启动所有服务。等待安装完成之后，才能登录到服务器。

要访问 Sentinel Web 界面，请在 Web 浏览器中指定下列 URL：

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_Sentinel_server> 是 Sentinel 服务器的 IP 地址或 DNS 名称，8443 是 Sentinel 服务器的默认端口。

11.3 执行无提示安装

如果需要在部署中安装多个 Sentinel 服务器，则无提示或无人照管安装非常有用。在这种方案中，您可以在交互式安装期间记录安装参数，然后在其他服务器上运行记录的文件。可以记录使用标准配置或自定义配置安装 Sentinel 时的安装参数。

要执行无提示安装，请确保您已将安装参数记录到某个文件中。有关创建响应文件的信息，请参阅第 11.2.1 节 “ 标准安装 ”（第 66 页）或第 11.2.2 节 “ 自定义安装 ”（第 67 页）。

要在 FIPS 140-2 模式下启用 Sentinel，请确保响应文件包含以下参数：

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

要执行无提示安装，请使用以下步骤：

1 从 Novell 下载网页中下载安装文件。

2 以 root 登录要安装 Sentinel 的服务器。

3 指定以下命令从 tar 文件提取安装文件：

```
tar -zxvf <install_filename>
```

使用安装文件实际名称替换 <*install_filename*>。

4 指定以下命令，在无提示模式下安装 Sentinel：

```
./install-sentinel -u <response_file>
```

将使用储存在响应文件中的值继续安装。

5 **如果选择启用 FIPS 140-2 模式，**执行第 19 章 “ 在 FIPS 140-2 模式下操作 Sentinel”（第 103 页）中所述的任务，以完成 FIPS 140-2 模式配置。

Sentinel 安装结束，服务器将启动。安装之后，因为系统要执行一次性初始化，所以可能需要花费几分钟来启动所有服务。等待安装完成之后，才能登录到服务器。

11.4 以非根用户身份安装 Sentinel

如果组织策略不允许以 root 用户身份运行完整的 Sentinel 安装，则可以以另一个用户的身份安装 Sentinel。在此安装过程中，以 root 用户身份执行前几步，然后以 root 用户创建的另一个用户身份继续安装 Sentinel。最后，根用户完成安装。

1 从 Novell 下载网页中下载安装文件

2 在命令行指定以下命令从 tar 文件提取安装文件：

```
tar -zxvf <install_filename>
```

使用安装文件实际名称替换 <*install_filename*>。

3 以 root 身份登录到要使用 root 身份安装 Sentinel 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。如果您希望非根用户在非默认位置安装 Sentinel，可以在命令中指定 --location 选项。例如：

```
./bin/root_install_prepare --location=/foo
```

将您传给 --location 选项的值 foo 附加到目录路径前面。

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 （有条件）要执行交互式安装：

7a 指定以下命令：

```
./install-sentinel
```

要在非默认位置安装 Sentinel，请在命令中指定 --location 选项。例如：

```
./install-sentinel --location=/foo
```

7b 继续执行步骤 9。

8 （有条件）要执行无提示安装：

8a 指定以下命令：

```
./install-sentinel -u <response_file>
```

将使用储存在响应文件中的值继续安装。

8b 继续执行步骤 12。

9 指定您希望用于安装的语言数量。

最终用户许可证协议将以选定的语言显示。

10 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 程序包。该安装完成可能需要几秒钟的时间。

11 将提示您指定安装模式。

- 如果您选择执行标准配置，请继续执行第 11.2.1 节 “ 标准安装 ”（第 66 页）中的步骤 8 到步骤 10。
- 如果您选择执行自定义配置，请继续执行第 11.2.2 节 “ 自定义安装 ”（第 67 页）中的步骤 7 到步骤 14。

12 以 root 用户身份登录，指定以下命令来完成安装：

```
./bin/root_install_finish
```

Sentinel 安装结束，服务器将启动。安装之后，因为系统要执行一次性初始化，所以可能需要花费几分钟来启动所有服务。等待安装完成之后，才能登录到服务器。

要访问 Sentinel Web 界面，请在 Web 浏览器中指定下列 URL：

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_Sentinel_server> 是 Sentinel 服务器的 IP 地址或 DNS 名称，8443 是 Sentinel 服务器的默认端口。

11.5 安装之后修改配置

安装 Sentinel 之后，如果希望输入有效的许可证密钥，请更改口令或修改任何已分配的端口，可以运行 configure.sh 脚本修改它们。该脚本可在 /opt/novell/sentinel/setup 文件夹中找到。

1 在命令行指定以下命令来运行 configure.sh 脚本：

```
./configure.sh
```

2 指定 1 以执行标准配置，或指定 2 以执行自定义 Sentinel 配置。

3 按空格键以通读许可证协议。

4 输入 yes 或 y 以接受许可协议并继续安装。

安装过程可能会花几分钟时间来加载安装程序包。

5 输入 1 以使用默认的 90 天评估许可证密钥。

或

输入 2 以输入购买的 Sentinel 许可证密钥。

6 决定您是否希望为 admin 管理员用户保留现有口令。

- 如果希望保留现有口令，请输入 1，然后继续执行步骤 7。
- 如果希望更改现有口令，请输入 2，指定新口令，然后继续执行步骤 7。

7 决定您是否希望为 dbauser 数据库用户保留现有口令。

- 如果希望保留现有口令，请输入 1，然后继续执行步骤 8。
- 如果希望更改现有口令，请输入 2，指定新口令，然后继续执行步骤 8。

dbauser 帐户是 Sentinel 用来与数据库交互的身份。在此处输入的口令可用于执行数据库维护任务，包括在忘记或丢失 admin 口令时重设置 admin 口令。

8 决定您是否希望为 appuser 应用程序用户保留现有口令。

- 如果希望保留现有口令，请输入 1，然后继续执行步骤 9。
- 如果希望更改现有口令，请输入 2，指定新口令，然后继续执行步骤 9。

9 通过输入想要的编号，然后指定新端口号，更改分配给 Sentinel 服务的端口。

10 更改端口之后，指定 7 以完成更改。

11 输入 1 以便仅使用内部数据库来鉴定用户。

或

如果已在域中配置了 LDAP 目录，请输入 2 以使用 LDAP 目录鉴定来鉴定用户。

默认值为 1。

11.6 安装附加的收集器管理器和关联引擎

默认情况下， Sentinel 将会安装收集器管理器和关联引擎。根据您的环境，您可能需要安装附加的收集器管理器和关联引擎。有关附加收集器管理器和关联引擎的优势的信息，请参见第 9.1 节 “ 附加收集器管理器的优势 ”（第 61 页）和第 9.2 节 “ 附加关联引擎的优势 ”（第 62 页）。

重要：必须在单独的系统上安装附加的收集器管理器或关联引擎。远程收集器管理器或远程关联引擎不能位于安装了 Sentinel 服务器的同一个系统上。

11.6.1 安装核对清单

在开始安装前，请确保已完成以下任务。

- ❒ 确保您的硬件和软件满足最低要求。有关详细信息，请参阅第 5 章 “ 满足系统要求 ”（第 33 页）。
- ❒ 使用网络时间协议 (NTP) 同步时间。
- ❒ 在 Sentinel 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，确保所有防火墙和网络设置都允许通过此端口进行通信。

11.6.2 安装附加的收集器管理器和关联引擎

1. 在 Web 浏览器中指定以下 URL 以起动 Sentinel Web 界面：

   `https://<IP_Address_Sentinel_server>:8443.`

   <*IP_Address_Sentinel_server*> 是 Sentinel 服务器的 IP 地址或 DNS 名称，8443 是 Sentinel 服务器的默认端口。

   使用在安装 Sentinel 服务器期间指定的用户名和口令登录。
2. 在工具栏中，单击 *下载*。
3. 在收集器管理器标题下，单击 *下载安装程序*。
4. 单击 *保存文件* 将安装程序保存到想要的位置。
5. 指定以下命令提取安装文件。

   `tar zxvf <install_filename>`

   使用安装文件实际名称替换 <*install_filename*>。
6. 切换到提取安装程序的目录。
7. 指定以下命令以安装收集器管理器或关联引擎：

   对于收集器管理器：

   `./install-cm`

   对于关联引擎：

   `./install-ce`

   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 1.5 GB，脚本会自动终止安装。
8. 指定您希望用于安装的语言数量。

   最终用户许可证协议将以选定的语言显示。
9. 按空格键以通读许可证协议。
10. 输入 yes 或 y 以接受许可协议并继续安装。

    安装过程可能会等几秒后才提示选择配置类型。
11. 当提示时，指定 1 以使用标准配置继续安装。
12. 输入已安装 Sentinel 的机器的默认通讯服务器主机名或 IP 地址。
13. 为收集器管理器或关联引擎指定用户名和口令。

    用户名和口令储存在 Sentinel 服务器上的 /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties 文件中。
14. 当提示时永久接受证书。
15. 输入 yes 或 y 在 Sentinel 中启用 FIPS 140-2 模式，并继续执行 FIPS 配置。
16. 根据提示继续安装，直到安装完成。

11.6.3 为收集器管理器或关联引擎添加自定义用户

Sentinel 建议您对远程收集器管理器和关联引擎使用默认用户名。但是，如果您安装了多个远程收集器管理器并希望独立标识它们，则可以创建新用户：

1. 以能够访问 Sentinel 安装文件的用户身份登录服务器。
2. 打开 activemqgroups.properties 文件。

   此文件位于 /<*install_dir*>/etc/opt/novell/sentinel/config/ 目录中。
3. 添加以逗号分隔的新用户名，如下所示：

   对于收集器管理器，请在 cm 部分中添加新用户。例如：

   ```
   cm=collectormanager,cmuser1,cmuser2,...
   ```

   对于关联引擎，请在 admins 部分中添加新用户。例如：

   ```
   admins=system,correlationengine,ceuser1,ceuser2,...
   ```
4. 保存并关闭文件。
5. 打开 activemqusers.properties 文件。

   此文件位于 /<*install_dir*>/etc/opt/novell/sentinel/config/ 目录中。
6. 为您在步骤 3 中创建的用户添加口令。

   口令可为任何随机字符串。例如：

   对于收集器管理器用户：

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   collectormanager=1c51ae56
   cmuser1=1b51de55
   cmuser2=1a51ce57
   ```

   对于关联引擎用户：

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   correlationengine=68790d7a
   ceuser1=69700c6d
   ceuser2=70701b5c
   ```
7. 保存并关闭文件。
8. 重新启动 Sentinel 服务器。

12 设备安装

Sentinel 设备是一个构建于 SUSE Studio 之上、随时可以运行的软件设备。该设备将一个强化的 SUSE Linux Enterprise Server (SLES) 11 SP 2 操作系统与 Sentinel 软件集成更新服务相结合，提供一种轻松且无缝的用户体验，从而允许客户充分利用现有投资。该软件设备可在硬件上或虚拟环境中安装。

12.1 安装 VMware 设备

本节将介绍如何在 VMware ESX 服务器上安装 Sentinel、收集器管理器和关联引擎。

12.1.1 安装 Sentinel

使用以下步骤在 VMware ESX 服务器上安装 Sentinel：

1. 从 Novell 下载网站下载 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_server_7.1.0.0.x86_64.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 转换器的机器提取压缩的设备映像。

   ```
   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 SUSE Linux Enterprise Server (SLES) 11 SP2 软件许可证协议。

11 阅读并接受 NetIQ Sentinel 最终用户许可证协议。

12 在主机名和域名页面上，指定主机名和域名，然后确保选中*为回环 IP 指派主机名*选项。

13 单击*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 页面上的*使用以下配置*，然后单击*下一步*。
- 要更改网络连接设置，请选择*更改*，进行所需更改，然后单击*下一步*。

网络连接设置即保存。

15 设置时间和日期，然后单击*下一步*。

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 root 口令，然后单击*下一步*。

安装过程会检查可用内存和磁盘空间。如果可用的内存小于 2.5 GB，则安装过程会不允许您继续进行操作，*下一步*按钮会变为灰色。

如果可用内存大于 2.5 GB 但少于 6.7 GB，安装过程中会显示一条讯息，提醒您可用内存少于建议值。当显示该讯息时，请单击*下一步*继续执行安装。

17 设置 Sentinel admin 口令，然后单击*下一步*。

安装之后，因为系统要执行一次性初始化，所以可能需要花费几分钟来启动所有服务。等待安装完成之后，才能登录到服务器。

18 记录控制台中显示的设备 IP 地址。

19 继续执行第 12.4 节 “ 设备的安装后配置 ”（第 82 页）。

12.1.2 安装附加的收集器管理器和关联引擎

除了需要从 Novell 下载网站下载相应的文件，安装收集器管理器的过程与安装关联引擎的过程相同。

1 从 Novell 下载网站 (http://download.novell.com/index.jsp) 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_collector_manager_7.1.0.0.x86_64.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 转换器的机器提取压缩的设备映像。

```
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 指定收集器管理器应该连接到的 Sentinel 服务器的主机名 /IP 地址。

9 指定通讯服务器端口号。默认讯息总线端口为 61616。

10 指定 JMS 用户名，即收集器管理器或关联引擎的用户名。收集器管理器的默认用户名为 collectormanager，而关联引擎的默认用户名为 correlationengine。

11 指定 JMS 用户的口令。

用户名和口令储存在 Sentinel 服务器上的 /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties 文件中。

12 （可选）要验证口令，请查看 activemqusers.properties 中的以下一行

对于收集器管理器：

```
collectormanager=<password>
```

在本示例中， collectormanager 是用户名，相对应的值是口令。

对于关联引擎：

```
correlationengine=<password>
```

在本示例中， correlationengine 是用户名，相对应的值是口令。

13 单击 *下一步*。

14 接受证书。

15 单击 *下一步*完成安装。

安装完成之后，安装程序将显示一条讯息，指出此设备是 Sentinel 收集器管理器或 Sentinel 关联引擎 （具体取决于您选择安装的部件）；同时还会显示 IP 地址。系统还会显示 Sentinel 服务器用户界面 IP 地址。

12.1.3 安装 VMware 工具

要使 Sentinel 在 VMware 服务器上有效运行，则需要安装 VMware 工具。 VMware 工具是一个实用程序套件，可增强虚拟机操作系统的性能。它还改进了虚拟机的管理。有关安装 VMware 工具的详细信息，请参阅 VMware Tools for Linux Guests (https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177)。

有关 VMware 文档的详细信息，请参阅 《工作站用户手册》(http://www.vmware.com/pdf/ws71_manual.pdf)。

12.2 安装 Xen 设备

本节将介绍如何在 Xen 设备映像上安装 Sentinel、收集器管理器和关联引擎。

- 第 12.2.1 节 “ 安装 Sentinel”（第 78 页）
- 第 12.2.2 节 “ 安装附加的收集器管理器和关联引擎 ”（第 79 页）

12.2.1 安装 Sentinel

使用以下步骤在 Xen 设备映像上安装 Sentinel：

1. 从 Novell 下载网站 (http://download.novell.com/index.jsp) 将 Xen 虚拟设备安装文件下载到 /var/lib/xen/images。

   正确的 Xen 虚拟设备文件名包含 xen。例如， Sentinel_7.1.0.0.x86_64.xen.tar.gz.

2. 使用以下命令解压该文件：

   ```
   tar -zxvf <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
   - <*file_name*>.xenconfig

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 disk 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 name 和 memory 设置的值。

     例如：

     ```
     # -*- mode: python; -*-
     name="Sentinel_7.1.0.0.x86_64"
     memory=4096
     ```

   - 注释以下行：

     ```
     vfb=["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
     ```

   - 添加以下行：

     ```
     extra = "console=hvc0 xencons=tty"
     ```

   更新的 xenconfig 文件必须如下所示：

   ```
   # -*- mode: python; -*-
   name=install_file_name
   memory=4096
   disk=["tap:aio:/var/lib/xen/images/install_directory/install_filename]
   vif=[ "bridge=br0" ]
   #vfb=["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
   extra = "console=hvc0 xencons=tty"
   ```

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 会显示在生成的列表中。

   例如，如果在 .xenconfig 文件中配置了 name="Sentinel_7.1.0.0.x86_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_7.1.0.0.x86_64

安装过程会先检查可用内存和磁盘空间。如果可用内存小于 2.5 GB，安装会自动终止。如果可用内存大于 2.5 GB 但少于 6.7 GB，安装过程中会显示一条讯息，提醒您可用内存少于建议值。如果要继续安装，请输入 y，如果不希望继续，请输入 n。

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 SUSE Linux Enterprise Server (SLES) 11 SP2 软件许可证协议。

12 阅读并接受 NetIQ Sentinel 最终用户许可证协议。

13 在主机名和域名页面上，指定主机名和域名，然后确保选中 *为回环 IP 指派主机名*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* 页面上的 *使用以下配置*。
- 要更改网络连接设置，请选择 *更改*，然后做出所需更改。

16 选择 *下一步*。网络连接设置即保存。

17 要设置日期和时间，请单击 *下一步*，然后单击 *完成*

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
```

18 设置 SUSE Enterprise Server root 口令，然后单击 *下一步*。

19 设置 Sentinel admin 口令，然后单击 *下一步*。

Sentinel 安装将继续并完成。安装之后可能需要几分钟来启动所有服务，因为系统会执行一次性初始化。等待安装完成之后，才能登录到服务器。

记录控制台中显示的设备 IP 地址。

20 继续执行第 12.4 节 “ 设备的安装后配置 ”（第 82 页）。

12.2.2 安装附加的收集器管理器和关联引擎

除了需要从 Novell 下载网站下载相应的文件，安装收集器管理器的过程与安装关联引擎的过程相同。

1 完成第 12.2.1 节 “ 安装 Sentinel”（第 78 页）中的步骤 1 到步骤 14。

2 在网络配置 II 屏幕上，选择 *更改*并指定您要在其上安装附加收集器管理器或关联引擎的虚拟机的 IP 地址。

3 指定特定 IP 的子网掩码。

4 选择 *下一步*。网络连接设置即保存。

5 设置时间和日期，然后选择 *下一步*。

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
```

6 设置 SUSE Enterprise Server root 口令，然后选择 *下一步*。

7 指定收集器管理器或关联引擎应连接到的 Sentinel 服务器的主机名 /IP 地址。

8 指定通讯服务器端口号。默认讯息总线端口为 61616。

9 指定 JMS 用户名，即收集器管理器或关联引擎的用户名。

10 指定 JMS 用户的口令。

用户名和口令储存在 Sentinel 服务器上的 /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties 文件中。

11 （可选）要验证口令，请查看 activemqusers.properties 文件中的以下一行：

对于收集器管理器：

```
collectormanager=<password>
```

在本示例中， collectormanager 是用户名，相对应的值是口令。

对于关联引擎：

```
correlationengine=<password>
```

在本示例中， correlationengine 是用户名，相对应的值是口令。

12 选择 *下一步*完成安装。

安装完成之后，安装程序将显示一条讯息，指出此设备是 Sentinel 收集器管理器或关联引擎 （具体取决于您选择安装的部件）；同时还会显示 IP 地址。

12.3 安装 ISO 设备

在硬件上安装设备前，确保已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。

重要：使用 ISO 磁盘映像 （裸机和 Hyper-V）在硬件上执行安装时，至少需要 4.5 GB 的内存才能完成安装。

- 第 12.3.1 节 “ 安装 Sentinel”（第 80 页）
- 第 12.3.2 节 “ 安装附加的收集器管理器和关联引擎 ”（第 81 页）

12.3.1 安装 Sentinel

使用以下步骤在硬件上安装 Sentinel 设备：

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。

安装过程会先检查可用内存和磁盘空间。如果可用内存小于 2.5 GB，安装会自动终止。如果可用内存大于 2.5 GB 但少于 6.7 GB，安装过程中会显示一条讯息，提醒您可用内存少于建议值。如果要继续安装，请输入 y，如果不希望继续，请输入 n。

4 选择您的语言，然后单击 *下一步*。

5 选择键盘布局，然后单击 *下一步*。

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

7 阅读并接受 NetIQ Sentinel 最终用户许可证协议。

8 选择 *下一步*。

9 在主机名和域名页面上，指定主机名和域名，然后确保选中 *为回环 IP 指派主机名*选项。

10 选择 *下一步*。主机名配置即保存。

11 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 页面上的 *使用以下配置*。
- 要更改网络连接设置，请选择 *更改*，然后做出所需更改。

12 选择 *下一步*。网络连接设置即保存。

13 设置时间和日期，然后单击 *下一步*。

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
```

14 设置 root 口令，然后单击 *下一步*。

15 设置 Sentinel admin 口令，然后单击 *下一步*。

16 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，口令是在步骤 14 中设置的口令。

17 停止 Sentinel 服务器：

```
service sentinel stop
```

18 输入以下命令以重新设置 UI，从而在 YaST 中得到清晰的显示：

```
reset
```

19 要在物理服务器上安装设备，请确保已选中 *将 Sentinel 设备安装到硬盘驱动器（仅针对 Live DVD 映像）*复选框。

默认情况下选中此复选框。如果取消选中此复选框，则设备将不会安装在物理服务器上，并且只以 LIVE DVD 模式运行。

在安装之后，因为系统要执行一次性初始化，可能需要花费几分钟时间来启动所有服务。等待安装完成之后，才能登录到服务器。

20 记录控制台中显示的设备 IP 地址。

21 继续执行第 12.4 节 “ 设备的安装后配置 ”（第 82 页）。

12.3.2 安装附加的收集器管理器和关联引擎

安装收集器管理器的过程与安装关联引擎的过程相同，但是您需要从 Novell 下载网站下载相应的文件。

1 完成第 12.3.1 节 “ 安装 Sentinel”（第 80 页）中的步骤 1 到步骤 14。

2 指定收集器管理器应该连接到的 Sentinel 服务器的主机名 /IP 地址。

3 指定通讯服务器端口号。默认讯息总线端口为 61616。

4 指定 JMS 用户名，即收集器管理器或关联引擎的用户名。

5 指定 JMS 用户的口令。

6 单击 *下一步*。

用户名和口令储存在 Sentinel 服务器上的 /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties 文件中。

7 要验证口令，请查看 activemqusers.properties 文件中的以下一行：

对于收集器管理器：

```
collectormanager=<password>
```

在本示例中， collectormanager 是用户名，相对应的值是口令。

对于关联引擎：

```
correlationengine=<password>
```

在本示例中， correlationengine 是用户名，相对应的值是口令。

8 要在物理服务器上安装设备，请确保已选中*将 Sentinel 设备安装到硬盘驱动器（仅针对 Live DVD 映像）*复选框。

默认情况下选中此复选框。如果取消选中此复选框，设备将不会安装在物理服务器上，并且只在 LIVE DVD 模式下运行。

9 在提示时接受证书。

10 输入 yes 或 y 在 Sentinel 中启用 FIPS 140-2 模式，并继续执行 FIPS 配置。

11 根据提示继续安装，直到安装完成。

安装完成之后，安装程序将显示一条讯息，指出此设备是 Sentinel 收集器管理器或关联引擎（具体取决于您选择安装的部件）；同时还会显示 IP 地址。系统还会显示 Sentinel 服务器用户界面 IP 地址。

12.4 设备的安装后配置

安装 Sentinel 之后，需要执行其他配置才能使设备正常工作。

- 第 12.4.1 节 “ 配置 WebYaST”（第 82 页）
- 第 12.4.2 节 “ 创建分区 ”（第 83 页）
- 第 12.4.3 节 “ 注册更新 ”（第 83 页）
- 第 12.4.4 节 “ 使用 SMT 配置设备 ”（第 84 页）

12.4.1 配置 WebYaST

Sentinel 设备用户界面配备了 WebYaST，它是一个基于 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 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 设备。

2 单击 *设备*。

3 配置 Sentinel 服务器以按照第 12.4.3 节 “ 注册更新 ”（第 83 页）中的描述接收更新。

4 单击 *下一步*完成初始设置。

12.4.2 创建分区

可以在设备中添加分区，并使用 YaST 工具将某个目录移动到新分区。

使用以下过程创建一个新分区，并将数据文件从其所在目录移动到新创建的分区：

1 以 root 用户身份登录到 Sentinel。

2 运行以下命令在设备上停止 Sentinel：

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

3 指定以下命令以更改为 novell 用户：

```
su -novell
```

4 将目录 /var/opt/novell/sentinel 的内容移到一个临时位置。

5 切换为 root 用户。

6 输入以下命令访问 YaST 控制中心：

```
yast
```

7 选择 *系统* > *分区程序*。

8 阅读警告并选择 *是*以添加新的未使用分区。

9 将新分区装入到 /var/opt/novell/sentinel。

10 指定以下命令以更改为 novell 用户：

```
su -novell
```

11 将数据目录的内容从临时位置 （数据目录的内容已在步骤 4 中保存到该位置）移回新分区中的 /var/opt/novell/sentinel。

12 运行以下命令重新启动 Sentinel 设备：

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

12.4.3 注册更新

必须在设备更新通道中注册 Sentinel 设备，才能接收增补程序更新。要注册设备，必须先从 Novell 客户关怀中心获取设备注册代码或设备激活密钥。

使用以下步骤注册设备以接收更新：

1 登录到 Sentinel 设备。

2 单击 *设备*起动 WebYaST。

3 单击 *注册*。

4 指定您希望用来接收更新的电子邮件 ID，然后指定系统名称和设备注册代码。

5 单击 *保存*。

12.4.4 使用 SMT 配置设备

在运行的设备不能直接访问因特网的安全环境中，您可以使用 Subscription Management Tool (SMT) 配置设备，以便在发布 Sentinel 的最新版本时，能够将设备升级到这些版本。 SMT 是与 Novell 客户中心相集成的程序包代理系统，可提供主要的 Novell 客户中心功能。

先决条件

- 获取 Sentinel 的 Novell 客户中心身份凭证，以从 Novell 获得更新。有关获取身份凭证的信息，请与 Novell 支持部门联系。
- 确保在您希望安装 SMT 的计算机上安装 SLES 11 SP2 的同时也安装了下列软件包：
  - htmldoc
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - perl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - yum-metadata-parser
  - createrepo
  - perl-DBI
  - apache2-prefork
  - libapr1
  - perl-Data-ShowTable
  - perl-Net-Daemon
  - perl-Tie-IxHash
  - fltk
  - libapr-util1
  - perl-PIRPC
  - apache2-mod_perl
  - apache2-utils
  - apache2
  - perl-DBD-mysql
- 安装 SMT 并配置 SMT 服务器。有关详细信息，请参阅 《SMT 文档》中的下列各节：
  - SMT 安装
  - SMT 服务器配置
  - 使用 SMT 镜像安装程序和更新储存库
- 在设备计算机上安装 wget 实用程序。

配置设备

有关使用 SMT 配置设备的信息，请参见适用于 SUSE Linux Enterprise 11 的订阅管理工具 (SMT) 文档。

要启用设备储存库，请执行以下命令：

smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64

smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64

smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64

升级设备

有关升级设备的信息，请参见第 21.3 节 “ 使用 SMT 升级设备 ”（第 118 页）。

12.5 使用 WebYaST 停止和启动服务器

您可以按照以下步骤使用 Web 界面启动和停止 Sentinel 服务器：

1. 登录到 Sentinel 设备。
2. 单击*设备*起动 WebYaST。
3. 单击*系统服务*。
4. 要停止 Sentinel 服务器，请单击*停止*。
5. 要启动 Sentinel 服务器，请单击*启动*。

13 安装附加的收集器和连接器

默认情况下，所有发布的收集器和连接器都会在安装 Sentinel 时安装。如果您要安装在发布 Sentinel 之后发布的新收集器或连接器，请参考以下章节中的信息。

13.1 安装收集器

使用以下步骤安装收集器：

1. 从 Sentinel 插件网站下载所需的收集器。
2. 登录到 https://<*IP 地址*>:8443 上的 Sentinel Web 界面，其中 8443 是 Sentinel 服务器的默认端口。
3. 单击工具栏中的*应用程序*，然后单击*应用程序*。
4. 单击*起动控制中心*以起动 Sentinel 控制中心。
5. 在工具栏中，单击*事件源管理* > *实时视图*，然后单击*工具* > *导入插件*。
6. 找到并选择您在步骤 1 中下载的收集器文件，然后单击 *下一步*。
7. 按照剩余的提示操作，然后单击*完成*。

要配置收集器，请参见 Sentinel 插件网站上提供的特定收集器的文档。

13.2 安装连接器

使用以下步骤安装连接器：

1. 从 Sentinel 插件网站下载所需的连接器。
2. 登录到 https://<*IP 地址*>:8443 上的 Sentinel Web 界面，其中 8443 是 Sentinel 服务器的默认端口。
3. 单击工具栏中的*应用程序*，然后单击*应用程序*。
4. 单击*起动控制中心*以起动 Sentinel 控制中心。
5. 在工具栏中，选择*事件源管理* > *实时视图*，然后单击*工具* > *导入插件*。
6. 找到并选择您在步骤 1 中下载的连接器文件，然后单击 *下一步*。
7. 按照剩余的提示操作，然后单击*完成*。

要配置连接器，请参见 Sentinel 插件网站上提供的特定连接器的文档。

14 校验安装

通过执行以下任一操作，可以确定安装是否成功：

- 校验 Sentinel 的版本：

  ```
  /etc/init.d/sentinel version
  ```

- 校验 Sentinel 服务是否已启动并在运行：

  ```
  /etc/init.d/sentinel status
  ```

- 校验 Web 服务是否已启动并在运行：

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  默认端口号是 8443。

- 访问 Sentinel Web 界面：

  1. 起动支持的 Web 浏览器。
  2. 指定 Sentinel Web 界面的 URL：

     ```
     https://<IP_Address/DNS_Sentinel_server:8443>
     ```

     IP_Address/DNS_Sentinel_server 是 Sentinel 服务器的 IP 地址或 DNS 名称，而 8443 是 Sentinel 服务器的默认端口。
  3. 使用在安装期间指定的管理员名称和口令登录。默认用户名为 admin。

15 Sentinel 目录结构

默认情况下， Sentinel 目录位于以下位置：

- 数据文件位于 /var/opt/novell/sentinel/data 和 /var/opt/novell/sentinel/3rdparty 目录中。
- 可执行文件和库储存在以下目录中：
  - /opt/novell/sentinel/bin
  - /opt/novell/sentinel/setup
  - /opt/novell/sentinel/3rdparty
- 日志文件位于目录 /var/opt/novell/sentinel/log 中
- 配置文件位于以下目录 /etc/opt/novell/sentinel 中
- 进程 ID (PID) 文件位于目录 /var/run/sentinel/server.pid 中

  利用 PID，管理员可确定 Sentinel 服务器的父进程，监视或终止进程。

IV 配置 Sentinel

本节将介绍如何配置 Sentinel 和即用型插件。

16 配置时间

事件的时间对 Sentinel 中的事件处理非常重要。它对报告、审计用途和实时处理都很重要。本节将介绍如何了解 Sentinel 中的时间、以及如何配置时间和处理时区。

16.1 理解 Sentinel 中的时间

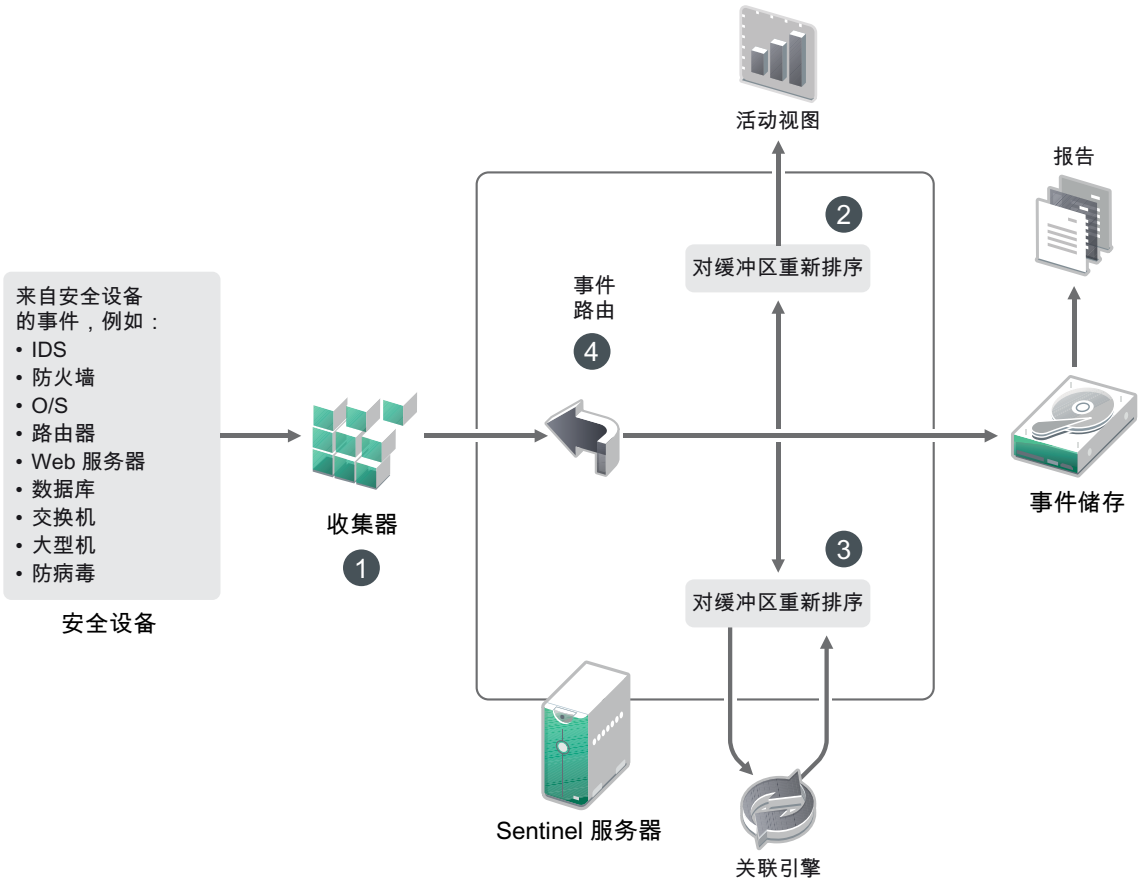
Sentinel 是由分布到您的整个网络中的多个进程组成的分布式系统。此外，事件源可能会引入一定的延迟。为了适应此需求， Sentinel 进程会在处理事件之前将事件重新排序到一个时序流中。

每个事件都有三个时间字段：

- **事件时间：**这是由所有分析引擎、搜索、报告等使用的事件时间。
- **Sentinel 进程时间：**Sentinel 从设备收集数据的时间，该时间是从收集器管理器系统时间得到的。
- **观察器事件时间：**设备放在数据中的时间戳。数据可能并非始终包含可靠的时间戳，并且可能与 Sentinel 进程时间大不相同。例如，当设备批量递送数据时。

下图演示了 Sentinel 实现此目的的方式：

图 16-1 *Sentinel 时间*



1. 默认情况下，“ 事件时间 ” 设置为 “Sentinel 进程时间 ”。但是，理想情况是使 “ 事件时间 ” 与 “ 观察器事件时间 ” 相匹配 （如果它可用且可信赖）。最好将数据收集配置为**信任事件源时间** （如果设备时间可用、准确且已由收集器正确分析）。收集器会将 “ 事件时间 ” 设置为与 “ 观察器事件时间 ” 相匹配。
2. “ 事件时间 ” 与服务器时间相差 5 分钟内 （在过去或未来）的事件通常由活动视图来处理。“ 事件时间 ” 与服务器时间在未来相差 5 分钟以上的事件不会显示在活动视图中，但会插入事件储存中。“ 事件时间 ” 与服务器时间在未来相差 5 分钟以上并在过去相差不到 24 小时的事件仍然会显示在图表中，但不会显示在该图表的事件数据中。必须执行向下钻取操作才能从事件储存中检索这些事件。
3. 事件将排序到 30 秒的时间间隔中，以便关联引擎可以按时间顺序处理它们。如果 “ 事件时间 ” 早于服务器时间 30 秒以上，则关联引擎不会处理这些事件。
4. 如果 “ 事件时间 ” 早于收集器管理器系统时间 5 分钟以上，Sentinel 会直接将这些事件路由到事件储存，从而绕过 “ 关联 ”、“ 活动视图 ” 和 “ 安全智能 ” 等实时系统。

16.2 配置 Sentinel 中的时间

关联引擎处理事件的时序流，并检测事件中的模式以及流中的时态模式。但是，生成事件的设备有时可能不会在其日志讯息中包含时间。要使用 Sentinel 正确配置时间，您有两个选择：

- 在收集器管理器上配置 NTP，并在事件源管理器中的事件源上取消选择*信任事件源时间*。Sentinel 使用收集器管理器作为事件的时间源。
- 选择事件源管理器中的事件源上*信任事件源时间*。Sentinel 使用日志讯息中的时间作为正确时间。

要在事件源上更改此设置，请执行以下操作：

1. 登录到 “ 事件源管理 ”。

   有关详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》* 中的 “ 访问事件源管理 ”。
2. 右键单击您希望更改其时间设置的事件源，然后选择*编辑*。
3. 在*常规*选项卡底部选择或取消选择*信任事件源*。
4. 单击*确定*保存更改。

16.3 处理时区

在分布式环境中，时区的处理可能非常复杂。例如，您的事件源可能位于一个时区，收集器管理器位于另一个时区，后端 Sentinel 服务器位于第三个时区，而查看数据的客户端位于第四个时区。当您添加夏令时间和许多没有报告为它们所设置的时区的时间源 （如所有 syslog 源）等问题时，需要处理许多可能出现的问题。 Sentinel 非常灵活，您可以正确表示事件实际发生的时间，将这些事件与来自相同或不同时区内的其他源的其他事件进行比较。

一般而言，在处理事件源报告时间戳的方式上，有 3 种方案：

- 事件源以 UTC 的形式报告时间。例如，所有标准的 Windows 事件日志总是以 UTC 形式进行报告。
- 事件源报告本地时间，但始终在时间戳中包含该时区。例如，构造时间戳过程中遵循 RFC3339 日期格式的任何事件源都包含时区，用它作为偏移，其他事件源会报告长时区 ID （如美国 / 纽约）或短时区 ID （如 EST），由于存在冲突的和不充分的解决方法，所以可能导致一些问题。
- 事件源报告本地时间，但不指明时区。不幸的是，极其常见的 syslog 格式也采用此模式。

对于第一种方案，您可以始终计算发生事件的绝对 UTC 时间 （假设使用了一种时间同步协议），所以您可以轻松地对比该事件发生的时间和世界其他事件源的时间。但是，您无法自动确定发生时间的本地时间是何时。出于此原因， Sentinel 允许客户手动设置事件源的时区，方法是编辑事件源管理器中的事件源节点并指定合适的时区。此信息不会影响 DeviceEventTime 或 EventTime 的计算，但它位于 ObserverTZ 字段中，可用于计算各种 ObserverTZ 字段，如 ObserverTZHour。这些字段始终使用本地时间表示。

在第二种方案中，如果使用长格式时区 ID 或偏移量，则可通过转换为 UTC 来获得绝对权威的 UTC 时间 （储存在 DeviceEventTime 中），但您也可以计算本地时间 ObserverTZ 字段。如果使用短时区 ID，可能会发生冲突。

第三种方案需要管理员来手动设置所有受影响源的事件源时区，以便 Sentinel 可以正确计算 UTC 时间。如果通过在事件源管理器中编辑事件源节点来正确指定了时区，那么 DeviceEventTime （以及可能 EventTime）可能不正确， ObserverTZ 和相关联的字段可能也不正确。

一般而言，给定类型的事件源 （如 Microsoft Windows）的收集器知道事件源如何提供时间戳，并相应地进行调整。在事件源管理器中为所有事件源节点手动设置时区始终是一种不错的策略，除非知道事件源报告本地时间并始终在时间戳中包含时区

对事件源的时间戳表示形式的处理是在收集器中和收集器管理器上进行的。 DeviceEventTime 和 EventTime 储存为 UTC， ObserverTZ 字段储存为设置为事件源本地时间的字符串。此信息从收集器管理器发送到 Sentinel 服务器并储存在事件储存中。收集器管理器和 Sentinel 服务器所在的时区不应影响此进程或储存的数据。但是，当客户端在 Web 浏览器中查看事件时， UTC EventTime 会根据 Web 浏览器而转换为本地时间，所以所有事件都会提供给本地时区内的客户端。如果用户希望查看源的本地时间，他们可以检查 ObserverTZ 字段以了解详细信息。

17 配置即用型插件

默认情况下， Sentinel 附带了多个插件。本章将介绍如何配置即用型插件。

17.1 配置解决方案包

Sentinel 附带了多种有用的即用型内容，您可以立即使用这些内容来满足许多分析需求。其中的许多内容都来自预安装的 Sentinel 核心解决方案包和 ISO 27000 系列的解决方案包。有关详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》* 中的 “ 使用解决方案包 ”

使用解决方案包，可以对内容进行分类，并将其分组到视为一个单元的控件或策略集中。解决方案包中的控件是预安装的，可向您提供这些即用型内容，但是您必须使用 Sentinel Web 控制台正式实现或测试这些控件。

如果您希望借助特定的严密规程来验证 Sentinel 实现可以按照设计进行使用，则可以采用解决方案包中内置的正式证明过程。此证明过程可实现和测试解决方案包控件，就像您实现和测试任何其他解决方案包中的控件一样。在此过程中，实现人员和测试人员将证明他们已完成各自的工作；这些证明随后将成为审计追踪的一部分，通过检查它们便可验证是否正确部署了任何特定控件。

您可以通过使用解决方案管理器来完成证明过程。有关实现和测试控件的详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》* 中的 “ 安装和管理解决方案包 ”。

17.2 配置收集器、连接器、集成器和操作

有关配置即用型插件的信息，请参见 Sentinel 插件网站上提供的特定插件文档。

18 在现有的 Sentinel 安装中启用 FIPS 140-2 模式

本章将介绍如何在现有的 Sentinel 安装中启用 FIPS 140-2 模式。

注释：这些说明假定 Sentinel 已安装在 /opt/novell/sentinel 目录中。必须以 novell 用户的身份执行命令。

18.1 启用 Sentinel 服务器以在 FIPS 140-2 模式下运行

要启用 Sentinel 服务器以在 FIPS 140-2 模式下运行，请执行以下操作：

1. 登录到 Sentinel 服务器。
2. 切换到 novell 用户 (su novell)。
3. 浏览至 Sentinel bin 目录。
4. 运行 convert_to_fips.sh 脚本并按照屏幕指导操作。
5. 执行第 19 章 “ 在 FIPS 140-2 模式下操作 Sentinel”（第 103 页）中所述的任务，以完成 FIPS 140-2 模式配置。

18.2 在远程收集器管理器和关联引擎上启用 FIPS 140-2 模式

如果要将批准 FIPS 的通讯用于在 FIPS 140-2 模式下运行的 Sentinel 服务器，必须在远程收集器管理器和关联引擎上启用 FIPS 140-2 模式。

要启用远程收集器管理器或关联引擎以在 FIPS 140-2 模式下运行，请执行以下操作：

1. 登录到远程收集器管理器或关联引擎系统。
2. 切换到 novell 用户 (su novell)。
3. 浏览至 bin 目录。默认位置为 /opt/novell/sentinel/bin。
4. 运行 convert_to_fips.sh 脚本并按照屏幕指导操作。
5. 执行第 19 章 “ 在 FIPS 140-2 模式下操作 Sentinel”（第 103 页）中所述的任务，以完成 FIPS 140-2 模式配置。

19 在 FIPS 140-2 模式下操作 Sentinel

本章将介绍如何在 FIPS 140-2 模式下配置和操作 Sentinel。

19.1 在 FIPS 140-2 模式下配置 Advisor 服务

Advisor 服务使用安全的 HTTPS 连接从 Advisor 服务器下载其源。需要将服务器用来进行安全通讯的证书添加到 Sentinel FIPS 密钥存储区数据库中。

要校验是否已成功注册到资源管理数据库，请执行以下操作：

1. 从 Advisor 服务器下载证书，并将文件保存为 advisor.cer。
2. 将 Advisor 服务器证书导入 Sentinel FIPS 密钥存储区。

   有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

19.2 在 FIPS 140-2 模式下配置分布式搜索

本节介绍如何在 FIPS 140-2 模式下配置分布式搜索。

方案 1：源和目标 Sentinel 服务器均处于 FIPS 140-2 模式

要允许在以 FIPS 140-2 模式运行的多个 Sentinel 服务器上执行分布式搜索，您需要添加用于与 FIPS 密钥存储区进行安全通讯的证书。

1. 登录到分布式搜索源计算机。
2. 浏览至证书目录：

   ```
   cd <sentinel_install_directory>/config
   ```

3. 将源证书 (sentinel.cer) 复制到目标计算机上的临时位置。
4. 将源证书导入目标 Sentinel FIPS 密钥存储区。

   有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

5 登录到分布式搜索目标计算机。

6 浏览至证书目录：

```
cd /etc/opt/novell/sentinel/config
```

7 将目标证书 (sentinel.cer) 复制到源计算机上的临时位置。

8 将目标系统证书导入源 Sentinel FIPS 密钥存储区。

9 在源计算机和目标计算机上重启动 Sentinel 服务。

方案 2：源 Sentinel 服务器处于非 FIPS 模式，而目标 Sentinel 服务器处于 FIPS 140-2 模式

必须将源计算机上的 Web 服务器密钥存储区转换为证书格式，然后将证书导出到目标计算机。

1 登录到分布式搜索源计算机。

2 创建证书 (.cer) 格式的 Web 服务器密钥存储区：

```
<sentinel_install_directory>/jre/bin/keytool -export -alias webserver -
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
password -file <certificate_name.cer>
```

3 将分布式搜索源证书 (Sentinel.cer) 复制到分布式搜索目标计算机上的临时位置。

4 登录到分布式搜索目标计算机。

5 将源证书导入目标 Sentinel FIPS 密钥存储区。

有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

6 在目标计算机上重启动 Sentinel 服务。

方案 3：源 Sentinel 服务器处于 FIPS 模式，而目标 Sentinel 服务器处于非 FIPS 模式

1 登录到分布式搜索目标计算机。

2 创建证书 (.cer) 格式的 Web 服务器密钥存储区：

```
<sentinel_install_directory>/jre/bin/keytool -export -alias webserver -
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
password -file <certificate_name.cer>
```

3 将证书复制到分布式搜索源计算机上的临时位置。

4 将目标证书导入源 Sentinel FIPS 密钥存储区。

有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

5 在源计算机上重启动 Sentinel 服务。

19.3 在 FIPS 140-2 模式下配置 LDAP 鉴定

要针对在 FIPS 140-2 模式下运行的 Sentinel 服务器配置 LDAP 鉴定，请执行以下操作：

1 从 LDAP 管理员处获取 LDAP 服务器证书，您也可以使用命令。例如，

```
openssl s_client -connect <LDAP server IP>:636
```

然后将返回的文本 （BEGIN 和 END 行之间的文本，但不包括 BEGIN 和 END 行）复制到某个文件中。

2 将 LDAP 服务器证书导入 Sentinel FIPS 密钥存储区。

有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

3 以管理员角色的用户身份登录到 Sentinel Web 控制台，并继续配置 LDAP 鉴定。

有关详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》*中的*配置 LDAP 鉴定*。

注释：此外，也可以通过运行 /opt/novell/sentinel/setup 目录中的 ldap_auth_config.sh 脚本，针对在 FIPS 140-2 模式下运行的 Sentinel 服务器配置 LDAP 鉴定。

19.4 在远程收集器管理器和关联引擎中更新服务器证书

要将现有远程收集器管理器和关联引擎配置为与以 FIPS 140-2 模式运行的 Sentinel 服务器进行通讯，您可以将远程系统转换为 FIPS 140-2 模式，也可以将 Sentinel 服务器证书更新到远程系统，并将收集器管理器或关联引擎保留为非 FIPS 模式。处于 FIPS 模式的远程收集器管理器可能无法处理不支持 FIPS 的事件源，或者需要某个尚未启用 FIPS 的 Sentinel 连接器的事件源。

如果您不打算在远程收集器管理器或关联引擎上启用 FIPS 140-2 模式，则必须将最新的 Sentinel 服务器证书复制到远程系统，以使收集器管理器或关联引擎能够与 Sentinel 服务器进行通讯。

要在远程收集器管理器或关联引擎中更新 Sentinel 服务器证书，请执行以下操作：

1 登录到远程收集器管理器或关联引擎所在的计算机。
2 切换到 novell 用户 (su novell)。
3 浏览至 bin 目录。默认位置为 /opt/novell/sentinel/bin。
4 运行 updateServerCert.sh 脚本并按照屏幕指导操作。

19.5 将 Sentinel 插件配置为在 FIPS 140-2 模式下运行

本节将介绍如何将各个 Sentinel 插件配置为在 FIPS 140-2 模式下运行。

注释：这些说明假定 Sentinel 已安装在 /opt/novell/sentinel 目录中。必须以 novell 用户的身份执行命令。

19.5.1 代理管理器连接器

仅当您在配置代理管理器事件源服务器的联网设置期间选择了*已加密 (HTTPS)* 选项时，才能执行以下过程。

要将代理管理器连接器配置为在 FIPS 140-2 模式下运行，请执行以下操作：

1. 添加或编辑代理管理器事件源服务器。通过配置屏幕继续操作，直到显示“安全性”窗口。有关详细信息，请参见 *《代理管理器连接器指南》*。
2. 从 *客户端鉴定类型* 字段中选择一个选项。客户端鉴定类型可确定 SSL 代理管理器事件源服务器校验要尝试发送数据的代理管理器事件源身份的严格程度。
   - **打开：** 允许来自代理管理器代理的所有 SSL 连接。不执行任何客户端证书验证或鉴定。
   - **严格：** 验证证书是否为有效的 X.509 证书，同时检查客户端证书是否受事件源服务器的信任。需要将新源明确添加到 Sentinel （这可以防止欺骗源发送未授权的数据）。

     对于 *严格* 选项，必须将每个新代理管理器客户端的证书导入 Sentinel FIPS 密钥存储区。当 Sentinel 在 FIPS 140-2 模式下运行时，您无法使用事件源管理 (ESM) 界面导入客户端证书。

     有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

注释： 在 FIPS 140-2 模式下，代理管理器事件源服务器使用 Sentinel 服务器密钥对；无需导入该服务器密钥对。

3. 如果在代理中启用了服务器鉴定，则还必须将代理配置为信任 Sentinel 服务器证书或远程收集器管理器证书，具体取决于部署连接器的位置。

   Sentinel 服务器证书的位置： /etc/opt/novell/sentinel/config/sentinel.cer

   远程收集器管理器证书的位置： /etc/opt/novell/sentinel/config/rcm.cer

注释： 在使用由证书颁发机构 (CA) 进行数字签名的自定义证书时，代理管理器代理必须信任相应的证书文件。

19.5.2 数据库 (JDBC) 连接器

仅当您在配置数据库连接期间选择了 *SSL* 选项时，才能执行以下过程。

要将数据库连接器配置为在 FIPS 140-2 模式下运行，请执行以下操作：

1. 在配置连接器之前，请从数据库服务器下载证书，然后将该证书以 database.cert 文件的形式保存到 Sentinel 服务器的 /etc/opt/novell/sentinel/config 目录中。

   有关详细信息，请参考相关的数据库文档。
2. 将证书导入 Sentinel FIPS 密钥存储区。

   有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。
3. 继续配置连接器。

19.5.3 Sentinel 链接连接器

仅当您在配置 Sentinel Link 事件源服务器的联网设置期间选择了 *已加密 (HTTPS)* 选项时，才能执行以下过程。

要将 Sentinel Link 连接器配置为在 FIPS 140-2 模式下运行，请执行以下操作：

1. 添加或编辑 Sentinel Link 事件源服务器。通过配置屏幕继续操作，直到显示“安全性”窗口。有关详细信息，请参见 *《Sentinel Link 连接器指南》*。

2 从*客户端鉴定类型*字段中选择一个选项。客户端鉴定类型可确定 SSL Sentinel Link 事件源服务器校验要尝试发送数据的 Sentinel Link 事件源 (Sentinel Link Integrator) 身份的严格程度。

- **打开：**允许来自客户端 (Sentinel Link Integrator) 的所有 SSL 连接。不执行任何集成器证书验证或鉴定。
- **严格：**验证集成器证书是否为有效的 X.509 证书，同时检查集成器证书是否受事件源服务器的信任。有关详细信息，请参考相关的数据库文档。

  对于*严格*选项：

  - 如果 Sentinel Link Integrator 处于 FIPS 140-2 模式，则您必须将 /etc/opt/novell/sentinel/config/sentinel.cer 文件从发送方 Sentinel 计算机复制到接收方 Sentinel 计算机。将此证书导入接收方 Sentinel FIPS 密钥存储区。

    注释：在使用由证书颁发机构 (CA) 进行数字签名的自定义证书时，必须导入相应的自定义证书文件。

  - 如果 Sentinel Link Integrator 处于非 FIPS 模式，您必须将自定义集成器证书导入接收方 Sentinel FIPS 密钥存储区。

    注释：如果发送方为 Sentinel 日志管理器 （处于非 FIPS 模式），而接收方为处于 FIPS 140-2 模式的 Sentinel，则要在发送方导入的服务器证书将是接收方 Sentinel 计算机中的 /etc/opt/novell/sentinel/config/sentinel.cer 文件。

  当 Sentinel 在 FIPS 140-2 模式下运行时，您无法使用事件源管理 (ESM) 界面导入客户端证书。有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

注释：在 FIPS 140-2 模式下，Sentinel Link 事件源服务器使用 Sentinel 服务器密钥对。不需要导入该服务器密钥对。

19.5.4 Syslog 连接器

仅当您在配置 Syslog 事件源服务器的网络设置期间选择了 *SSL* 协议时，才能执行以下过程。

要将 Syslog 连接器配置为在 FIPS 140-2 模式下运行，请执行以下操作：

1 添加或编辑 Syslog 事件源服务器。通过配置屏幕继续操作，直到显示 “ 联网 ” 窗口。有关详细信息，请参见 *《Syslog 连接器指南》*。

2 单击 *设置*。

3 从*客户端鉴定类型*字段中选择一个选项。客户端鉴定类型可确定 SSL Syslog 事件源服务器校验要尝试发送数据的 Syslog 事件源身份的严格程度。

- **打开：**允许来自客户端 （事件源）的所有 SSL 连接。不执行任何客户端证书验证或鉴定。
- **严格：**验证证书是否为有效的 X.509 证书，同时检查客户端证书是否受事件源服务器的信任。必须将新源明确添加到 Sentinel （这可以防止欺骗源向 Sentinel 发送数据）。

  对于*严格*选项，必须将 syslog 客户端的证书导入 Sentinel FIPS 密钥存储区。

  当 Sentinel 在 FIPS 140-2 模式下运行时，您无法使用事件源管理 (ESM) 界面导入客户端证书。

  有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

注释：在 FIPS 140-2 模式下， Syslog 事件源服务器使用 Sentinel 服务器密钥对。不需要导入该服务器密钥对。

4 如果在 syslog 客户端中启用了服务器鉴定，则必须将该客户端配置为信任 Sentinel 服务器证书或远程收集器管理器证书，具体取决于部署连接器的位置。

Sentinel 服务器证书文件位于 /etc/opt/novell/sentinel/config/sentinel.cer 位置中。

远程收集器管理器证书文件位于 /etc/opt/novell/sentinel/config/rcm.cer 位置中。

注释：在使用由证书颁发机构 (CA) 进行数字签名的自定义证书时，客户端必须信任相应的证书文件。

19.5.5 Windows 事件 (WMI) 连接器

要将 Windows 事件 (WMI) 连接器配置为在 FIPS 140-2 模式下运行，请执行以下操作：

1 添加或编辑 Windows 事件连接器。通过配置屏幕继续操作，直到显示 “ 安全性 ” 窗口。有关详细信息，请参见 *《Windows 事件 (WMI) 连接器指南》*。

2 单击 *设置*。

3 从 *客户端鉴定类型*字段中选择一个选项。客户端鉴定类型可确定 Windows 事件连接器校验要尝试发送数据的客户端 Windows 事件收集服务 (WECS) 身份的严格程度。

- **打开：**允许来自客户端 WECS 的所有 SSL 连接。不执行任何客户端证书验证或鉴定。
- **严格：**验证证书是否为有效的 X.509 证书，同时检查客户端 WECS 证书是否已由 CA 进行签名。需要明确添加新源 （这可以防止欺骗源向 Sentinel 发送数据）。

  对于*严格*选项，必须将客户端 WECS 的证书导入 Sentinel FIPS 密钥存储区。当 Sentinel 在 FIPS 140-2 模式下运行时，您无法使用事件源管理 (ESM) 界面导入客户端证书。

  有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

注释：在 FIPS 140-2 模式下， Windows 事件源服务器使用 Sentinel 服务器密钥对。不需要导入该服务器密钥对。

4 如果在 Windows 客户端中启用了服务器鉴定，则必须将该客户端配置为信任 Sentinel 服务器证书或远程收集器管理器证书，具体取决于部署连接器的位置。

Sentinel 服务器证书文件位于 /etc/opt/novell/sentinel/config/sentinel.cer 位置中。

远程收集器管理器证书文件位于 /etc/opt/novell/sentinel/config/rcm.cer 位置中。

注释：在使用由证书颁发机构 (CA) 进行数字签名的自定义证书时，客户端必须信任相应的证书文件。

5 如果您要自动同步事件源或使用 Active Directory 连接填充事件源的列表，则必须将 Active Directory 服务器证书导入 Sentinel FIPS 密钥存储区。

有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

19.5.6 Sentinel Link Integrator

仅当您在配置 Sentinel Link Integrator 的网络设置期间选择了 *已加密 (HTTPS)* 选项时，才能执行以下过程。

要将 Sentinel Link Integrator 配置为在 FIPS 140-2 模式下运行，请执行以下操作：

1 当 Sentinel Link Integrator 处于 FIPS 140-2 模式时，服务器鉴定是必需的。在配置集成器实例之前，请将 Sentinel Link 服务器证书导入 Sentinel FIPS 密钥存储区：

- **如果 Sentinel Link 连接器处于 FIPS 140-2 模式：**

  如果连接器部署在 Sentinel 服务器上，则您必须将 /etc/opt/novell/sentinel/config/sentinel.cer 文件从接收方 Sentinel 计算机复制到发送方 Sentinel 计算机。

  如果连接器部署在远程收集器管理器上，则您必须将 /etc/opt/novell/sentinel/config/rcm.cer 文件从接收方远程收集器管理器计算机复制到接收方 Sentinel 计算机。

  将此证书导入发送方 Sentinel FIPS 密钥存储区。

  注释：在使用由证书颁发机构 (CA) 进行数字签名的自定义证书时，必须导入相应的自定义证书文件。

- 如果 Sentinel Link 连接器处于非 FIPS 模式：

  将自定义 Sentinel Link 服务器证书导入发送方 Sentinel FIPS 密钥存储区。

  注释：当 Sentinel Link Integrator 处于 FIPS 140-2 模式，而 Sentinel Link 连接器处于非 FIPS 模式时，请使用连接器上的自定义服务器密钥对。不要使用内部服务器密钥对。

有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

2 继续配置集成器实例。

注释：在 FIPS 140-2 模式下， Sentinel Link Integrator 使用 Sentinel 服务器密钥对。不需要导入集成器密钥对。

19.5.7 LDAP Integrator

要将 LDAP Integrator 配置为在 FIPS 140-2 模式下运行，请执行以下操作：

1 在配置集成器实例之前，请从 LDAP 服务器下载证书，然后将该证书以 ldap.cert 文件的形式保存到 Sentinel 服务器的 /etc/opt/novell/sentinel/config 目录中。

例如，使用

```
openssl s_client -connect <LDAP server IP>:636
```

然后将返回的文本 （BEGIN 和 END 行之间的文本，但不包括 BEGIN 和 END 行）复制到某个文件中。

2 将证书导入 Sentinel FIPS 密钥存储区。

有关导入证书的详细信息，请参见将证书导入 FIPS 密钥存储区数据库 （第 110 页）。

3 继续配置集成器实例。

19.5.8 SMTP 集成器

SMTP 集成器支持 2011.1r2 及更高版本的 FIPS 140-2。无需进行配置更改。

19.5.9 将不启用 FIPS 的连接器与处于 FIPS 140-2 模式的 Sentinel 一起使用

本节将介绍如何将不启用 FIPS 的连接器与处于 FIPS 140-2 模式的 Sentinel 一起使用。如果您的源不支持 FIPS，或者您想要从环境中的非 FIPS 连接器收集事件，我们建议采用这种方法。

要将非 FIPS 连接器与处于 FIPS 140-2 模式的 Sentinel 一起使用，请执行以下操作：

1. 安装处于非 FIPS 模式的远程收集器管理器，以连接到处于 FIPS 140-2 模式的 Sentinel 服务器。

   有关详细信息，请参见第 11.6 节 “ 安装附加的收集器管理器和关联引擎 ”（第 71 页）。
2. 将非 FIPS 连接器专门部署到非 FIPS 远程收集器管理器。

注释：当非 FIPS 连接器 （例如审计连接器和文件连接器）部署在已连接到处于 FIPS 140-2 模式的 Sentinel 7.1 服务器的非 FIPS 远程收集器管理器上时，会出现某些已知的问题。有关这些已知问题的详细信息，请参见 “ 《NetIQ Sentinel 7.0.1 自述》 ”。

19.6 将证书导入 FIPS 密钥存储区数据库

只有将证书插入 Sentinel FIPS 密钥存储区数据库，才能建立从拥有这些证书的部件到 Sentinel 的安全 (SSL) 通讯。在 Sentinel 中启用了 FIPS 140-2 模式时，您无法照常使用 Sentinel 用户界面上载证书。必须手动将证书导入 FIPS 密钥存储区数据库。

对于要使用部署到远程收集器管理器的连接器的事件源，您必须将证书导入远程收集器管理器 （而非中心 Sentinel 服务器）的 FIPS 密钥存储区数据库。

要将证书导入 FIPS 密钥存储区数据库，请执行以下操作：

1. 将证书文件复制到 Sentinel 服务器或远程收集器管理器上的任意临时位置。
2. 浏览至 Sentinel bin 目录。默认位置为 /opt/novell/sentinel/bin。
3. 运行以下命令将证书导入 FIPS 密钥存储区数据库，然后按照屏幕指导操作：

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```
4. 当提示重启动 Sentinel 服务器或远程收集器管理器时，请输入 yes 或 y。

19.7 将 Sentinel 还原为非 FIPS 模式

本节将介绍如何将 Sentinel 及其部件还原为非 FIPS 模式。

- 第 19.7.1 节 “ 将 Sentinel 服务器还原为非 FIPS 模式 ”（第 110 页）
- 第 19.7.2 节 “ 将远程收集器管理器或远程关联引擎还原为非 FIPS 模式 ”（第 111 页）

19.7.1 将 Sentinel 服务器还原为非 FIPS 模式

仅当您在将 Sentinel 服务器转换为在 FIPS 140-2 模式下运行之前创建了该服务器的备份时，才能将以 FIPS 140-2 模式运行的 Sentinel 服务器还原为非 FIPS 模式。

注释：当您将 Sentinel 服务器还原为非 FIPS 模式时，在转换为运行 FIPS 140-2 模式之后的事件、事件数据以及对 Sentinel 服务器所做的配置更改将会丢失。 Sentinel 系统将重新恢复到非 FIPS 模式的上一个恢复点。在还原为非 FIPS 模式之前，应该创建当前系统的备份以供将来使用。

要将 Sentinel 服务器还原为非 FIPS 模式，请执行以下操作：

1. 以根用户身份登录 Sentinel 服务器。
2. 切换到 novell 用户。
3. 浏览至 Sentinel bin 目录。默认位置为 /opt/novell/sentinel/bin。
4. 运行以下命令将 Sentinel 服务器还原为非 FIPS 模式，然后按照屏幕指导操作：

   ```
   ./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
   ```

   例如，如果 non-fips201301241911135903 4887.tar.gz 是备份文件，请运行以下命令：

   ```
   ./backup_util.sh -f non-fips201301241911135903 4887.tar.gz -m 'restore'
   ```

5. 重启动 Sentinel 服务器。

19.7.2 将远程收集器管理器或远程关联引擎还原为非 FIPS 模式

您可以将远程收集器管理器或远程关联引擎还原为非 FIPS 模式。

要将远程收集器管理器或远程关联引擎还原为非 FIPS 模式，请执行以下操作：

1. 登录到远程收集器管理器或远程关联引擎系统。
2. 切换到 novell 用户 (su novell)。
3. 浏览至 bin 目录。默认位置为 /opt/novell/sentinel/bin。
4. 运行 revert_to_nonfips.sh 脚本并按照屏幕指导操作。
5. 重启动远程收集器管理器或远程关联引擎。

V 升级 Sentinel

本节将介绍如何升级 Sentinel 和其他部件。

20 升级 Sentinel 服务器

重要：Sentinel 7.1 及更高版本要求操作系统必须已启用 IPv6。请确保在将系统升级到 Sentinel 7.1 或更高版本之前，已在操作系统中启用 IPv6。如果未启用 IPv6，则主要部件将无法运行。

使用以下步骤升级 Sentinel 服务器：

1. 备份您的配置，然后创建 ESM 导出。

   有关备份数据的详细信息，请参见 “ 备份和恢复数据 ”（在 *《NetIQ Sentinel 7.1 管理指南》*中）。
2. 从 Novell 下载站点下载最新的安装程序。
3. 以 root 身份登录要升级 Sentinel 的服务器。
4. 指定以下命令从 tar 文件提取安装文件：

   ```
   tar xfz <install_filename>
   ```

   使用安装文件实际名称替换 <*install_filename*>。
5. 将目录更改为抽取安装文件的位置。
6. 指定以下命令来升级 Sentinel：

   ```
   ./install-sentinel
   ```
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，输入 yes 或 y 接受许可证，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。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。
10. 清除 Web 浏览器超速缓存，以查看最新的 Sentinel 版本。
11. （条件）要升级收集器管理器系统和关联引擎系统，请参见第 22 章 “ 升级收集器管理器或关联引擎 ”（第 119 页）。

21 升级 Sentinel 设备

本章中的过程将指导您完成 Sentinel 设备以及收集器管理器和关联引擎设备的升级。

21.1 升级 Sentinel 7.0.2 及更高版本的设备

1. 以管理员角色中的用户身份登录 Sentinel 设备。
2. **如果要升级 Sentinel 设备**，请单击 *设备*以起动 WebYaST。
3. **如果要升级收集器管理器或关联引擎设备**，请使用端口 54984 指定收集器管理器或关联引擎计算机的 URL，以起动 WebYaST。
4. 备份您的配置，然后创建 ESM 导出。

   有关备份数据的详细信息，请参见 “ 备份和恢复数据 ”（在 *《NetIQ Sentinel 7.1 管理指南》*中）。
5. （有条件）如果尚未注册该设备以进行自动更新，请先注册以进行更新。

   有关详细信息，请参见第 12.4.3 节 “ 注册更新 ”（第 83 页）。

   如果设备未注册，则 Sentinel 将显示一则黄色警告，指示该设备未注册。
6. 要检查是否有任何更新，请单击 *更新*。

   将显示可用的更新。
7. 选择并应用更新。

   完成更新可能需要几分钟时间。更新成功后将显示 WebYaST 登录页面。

   升级设备之前， WebYaST 将自动停止 Sentinel 服务。升级完成之后，必须手动重新启动此服务。
8. 使用 Web 界面重新启动 Sentinel 服务。

   有关详细信息，请参见第 12.5 节 “ 使用 WebYaST 停止和启动服务器 ”（第 85 页）。
9. 清除 Web 浏览器超速缓存，以查看最新的 Sentinel 版本。

21.2 升级 Sentinel 7.0 和 7.0.1 设备

由于增补程序的供应商名称已从 Novell 更改为 NetIQ，在 WebYaST 中升级 Sentinel 7.0 和 7.0.1 设备失败。您需要使用 zypper 增补程序升级设备。

要使用 zypper 增补程序升级设备，请执行以下操作：

1. 备份您的配置，然后创建 ESM 导出。有关详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》*中的“ 备份和恢复数据 ”。
2. 以根用户身份登录到设备控制台。
3. 运行以下命令：

   ```
   /usr/bin/zypper patch
   ```

4. 输入 1 以接受将供应商从 Novell 更改为 NetIQ。
5. 输入 Y 以继续操作。
6. 输入 yes 以接受许可证协议。
7. 重启动 Sentinel 设备。
8. 清除 Web 浏览器超速缓存，以查看最新的 Sentinel 版本。

21.3 使用 SMT 升级设备

在设备无需直接访问因特网即可运行的安全环境中，您可以使用订阅管理工具 (SMT) 配置设备，以便您能够将设备升级到可用的最新版本。

1. 确保使用 SMT 配置设备。

   有关详细信息，请参阅第 12.4.4 节“ 使用 SMT 配置设备 ”（第 84 页）。
2. 以根用户身份登录到设备控制台。
3. 刷新储存库以进行升级：

   ```
   zypper ref -s
   ```

4. 检查是否已启用设备以进行升级：

   ```
   zypper lr
   ```

5. （可选）检查设备的可用更新：

   ```
   zypper lu
   ```

6. （可选）检查包含设备可用更新的程序包：

   ```
   zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
   ```

7. 更新设备：

   ```
   zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
   ```

8. 重新启动设备。

   ```
   rcsentinel restart
   ```

22 升级收集器管理器或关联引擎

运用以下步骤升级收集器管理器或关联引擎：

1. 备份配置设置并创建 ESM 导出。

   有关详细信息，请参见 *《NetIQ Sentinel 7.1 管理指南》*中的“ 备份和恢复数据 ”。
2. 以管理员角色的用户身份登录 Sentinel Web 界面。
3. 选择 *下载*。
4. 在“ 收集器管理器安装程序 ”部分中，单击 *下载安装程序*。

   此时将显示一个窗口，其中提供了在本地计算机上打开或保存安装程序文件的选项。
5. 保存文件。
6. 将文件复制到临时位置。
7. 提取文件的内容。
8. 运行以下脚本：

   对于收集器管理器：

   ```
   ./install-cm
   ```

   对于关联引擎：

   ```
   ./install-ce
   ```
9. 按照屏幕上的指导完成安装。
10. 清除 Web 浏览器超速缓存，以查看最新的 Sentinel 版本。

23 升级 Sentinel 插件

除非特定插件与最新版本的 Sentinel 不兼容，否则， Sentinel 的升级安装不会升级插件。

通常，新的和更新的 Sentinel 插件上载到 Sentinel 插件网站。要获取插件的最新 bug 修复、文档更新和增强功能，请下载并安装最新版本的插件。有关安装插件的信息，请参见特定的插件文档。

VI 附录

A 配置 Sentinel 的高可用性

许多客户都在设法将 Sentinel 安装到高可用性环境中，旨在确保尽量一致地收集关键的企业事件数据。许多安全与合规性要求都依赖于全面的数据收集来证实符合这些要求 - 某些遗漏的事件可能会阻止威胁或违规的检测，并给组织招致不可接受的风险。经 NetIQ 的测试和认证， Sentinel 可以在高可用性环境中工作，并支持灾难恢复体系结构。

本附录介绍了如何以主动 - 被动高可用性模式安装产品。在此模式下，如果发生硬件或软件故障，Sentinel 可将故障转移到冗余群集节点。本附录未介绍主动 - 主动配置，并且不保证实现任何特定的运行时间目标。 NetIQ 顾问和 NetIQ 合作伙伴可帮助您实现 Sentinel 高可用性和灾难恢复。

注释：NetIQ 仅支持 Sentinel 一步式安装中的高可用性配置。它不直接支持收集器管理器或关联引擎的分布式安装。

A.1 概念

高可用性是指一种设计方法，旨在使系统尽可能地保持可用。其目的是最大程度地减少诸如系统故障和维护等的停机因素，并最大限度地缩短检测发生的停机事件并从其中恢复所需的时间。事实上，自动检测停机事件并从其中恢复很快成为必要的手段，因为必须实现最高级别的可用性。

A.1.1 外部系统

Sentinel 是一种复杂的多层应用程序，它依赖于各种服务并提供各种服务。此外，它与多个外部第三方系统集成，以进行数据收集、数据共享和事件更新。大多数高可用性解决方案都允许实现者声明应该高度可用的服务与依赖服务之间的相关性，但是，这只适用于在群集本身上运行的服务。 Sentinel 外部的系统 （例如事件源）必须单独进行配置，以便在组织需要时可供使用；另外，这些系统还必须配置为能够正确处理 Sentinel 有段时间不可用 （例如发生故障转移事件）的情况。如果严格限制访问权限 （例如，使用鉴定的会话在第三方系统与 Sentinel 之间发送 / 接收数据），则必须将第三方系统

配置为接受来自任何群集节点的会话，或者发起到任何群集节点的会话 （针对此目的，应该使用虚拟 IP 配置 Sentinel）。 NetIQ 无法保证在我们的产品与不受我们控制的第三方系统之间实现任何特定级别的高可用性。

A.1.2 共享储存

所有高可用性群集都需要某种形式的共享储存，以便在源节点发生故障时，能够在群集节点之间快速移动应用程序数据。储存本身应该高度可用；通常，可以借助于使用光纤通道网络连接到群集节点的储存区域网络 (SAN) 技术实现这种高可用性。其他系统使用网络挂接储存 (NAS)、iSCSI 或其他技术，这些技术可用于远程装入共享储存。共享储存的基本要求是，群集能够完全将储存从发生故障的群集节点移动到新的群集节点。

注释：对于 iSCSI，您应使用您的硬件支持的最大讯息传送单位 (MTU)。较大的 MTU 有利于提高储存性能。如果储存的延迟和 / 或带宽慢于建议值，则 Sentinel 可能会遇到问题。

Sentinel 可对共享储存使用两种基本方法。第一种方法是将所有部件 （应用程序二进制文件、配置和事件数据）定位在共享储存上。在发生故障转移时，储存将从主节点上卸载，并移到备份节点；这样就可以从共享储存装载整个应用程序和配置了。第二种方法是将事件数据储存在共享储存上，但应用程序二进制文件和配置驻留在每个群集节点上。在发生故障转移时，只会将事件数据移到备份节点。

每种方法都有各自的优缺点，但第二种方法允许 Sentinel 安装使用符合 FHS 的标准安装路径，可用于验证 RPM 打包，还可用于进行热增补和重新配置，以最大程度地减少停机时间。

此解决方案将向您介绍一个有关在群集上进行安装的过程示例，该群集使用 iSCSI 共享储存，并将应用程序二进制文件 / 配置定位在每个群集节点上。

A.1.3 服务监视

任何高可用性环境的一个关键要素是，能够以可靠且一致的方式监视应该保持高度可用的资源，以及这些资源所依赖的任何资源。 SLE HAE 使用名为资源代理的部件执行此监视操作，资源代理的任务是提供每个资源的状态，以及 （根据要求）启动或停止该资源。

资源代理只有提供了受监视资源的可靠状态，才能防止出现不必要的停机。误报 （认为某个资源已发生故障，但事实上它能够自行恢复）可能会导致其实不必要的服务迁移 （及相关的停机），而漏报（资源代理报告某个资源在正常运行，但事实上该资源未正常运行）可能会阻止服务的正常使用。另一方面，对服务进行外部监视可能相当困难。例如， Web 服务端口可能会响应简单的 ping 命令，但是当发出实际查询时无法提供正确的数据。在许多情况下，必须在服务本身中内置自检功能，才能提供真正准确的度量。

此解决方案为 Sentinel 提供了基本的 OCF 资源代理，该代理可以监视重大的硬件、操作系统或 Sentinel 系统故障。目前， Sentinel 的外部监视功能基于 IP 端口探测，因此，在某种程度上存在误报和漏报读取内容的可能性。我们计划不断改进 Sentinel 和资源代理，以提高此部件的准确性。

A.1.4 隔离

在 HA 群集中，关键服务不断受到监视，并在发生故障时将在其他节点上自动重启动。但是，如果主节点出现通讯问题，则这种自动化操作可能会引入问题；尽管在该节点上运行的服务看似已停止，但实则还在运行并向共享储存写入数据。在此情况下，在备份节点上启动一组新的服务可能很容易导致数据损坏。

群集使用各种技术 （统称为 “ 隔离 ”）防止发生这种情况，这些技术包括节点分裂检测 (SBD) 和逐出其他节点 (STONITH)）。其主要目标是防止共享储存上发生数据损坏。

A.2 可支持性

根据定义的群集特征以及本文档中定义的并经过我们实验室测试的预期行为，NetIQ 支持此解决方案。其他群集配置只有在您的环境中出现的问题能够在我们的内部测试环境中再现时才受支持，这就避免了实现中存在的局部差异成为问题的原因。

A.3 系统要求

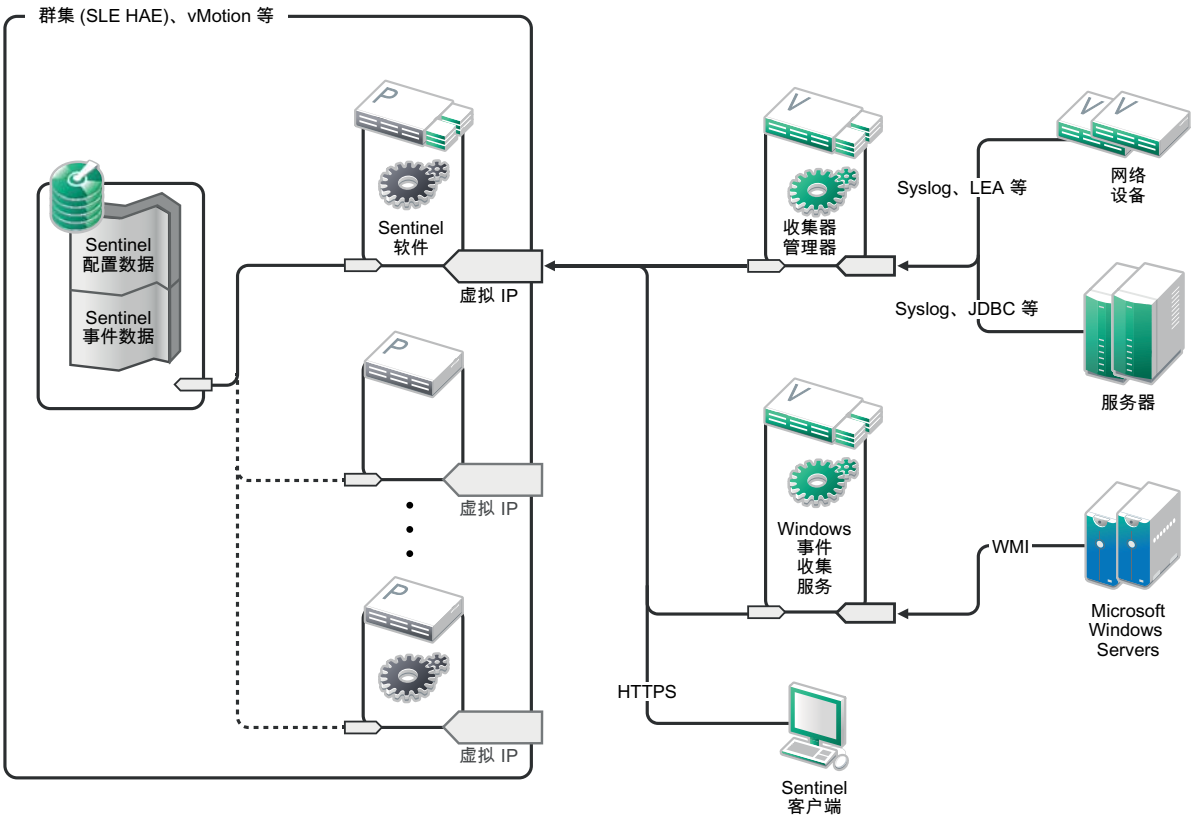
在分配群集资源以支持高可用性安装时，请考虑以下要求：

- 托管 Sentinel 服务的每个群集节点都必须符合第 5 章 “ 满足系统要求 ”（第 33 页）中指定的要求。
- 确保为 Sentinel 数据和应用程序提供足够的共享储存。
- 在发生故障转移时可在节点之间迁移的服务的虚拟 IP 地址。
- 具有有效许可证的 Sentinel 安装程序 （TAR 文件）。
- 具有有效许可证的 SUSE Linux High Availability Extension （ISO 映像）。
- 符合第 5 章 “ 满足系统要求 ”（第 33 页）中记录的性能与大小特征的共享储存设备。本示范解决方案将使用一个将 iSCSI 目标配置为共享储存的标准 SUSE Linux VM。
- 至少有两个群集节点满足在客户环境中运行 Sentinel 的资源要求。本示范解决方案将使用两个 SUSE Linux VM。
- 群集节点与共享储存通讯的方法，例如用于 SAN 的 FibreChannel。本示范解决方案将使用专用的 IP 地址连接到 iSCSI 目标。
- 可在群集节点之间迁移以用作 Sentinel 的外部 IP 地址的虚拟 IP。
- 每个群集节点至少有一个 IP 地址用于内部群集通讯。本示范解决方案将使用简单的单播 IP 地址，但在生产环境中最好使用多播 IP 地址。

A.4 安装和配置

本节将提供有关在高可用性环境中安装和配置 Sentinel 的步骤。每个步骤都描述了常规方法，然后引用了演示设置，其中记录了示范群集解决方案的细节。您可以使用本文档中未列出的其他选项或技术，但要受第 A.2 节 “ 可支持性 ”（第 127 页）中所述限制的约束。

下图显示了主动 - 被动高可用性体系结构：



- 第 A.4.1 节 “ 初始设置 ”（第 128 页）
- 第 A.4.2 节 “ 共享储存设置 ”（第 129 页）
- 第 A.4.3 节 “Sentinel 安装 ”（第 132 页）
- 第 A.4.4 节 “ 群集安装 ”（第 133 页）
- 第 A.4.5 节 “ 群集配置 ”（第 134 页）
- 第 A.4.6 节 “ 资源配置 ”（第 136 页）
- 第 A.4.7 节 “ 网络储存配置 ”（第 137 页）

A.4.1 初始设置

按照针对 Sentinel 记录的要求以及本地客户要求，配置计算机硬件、网络硬件、储存硬件、操作系统、用户帐户和其他基本系统资源。测试系统以确保其运行正常且稳定。

- 作为最佳实践，应该将所有群集节点的时间同步，您可以使用 NTP 或类似的技术实现此目的。
- 群集将要求提供可靠的主机名解析。作为最佳实践，您可能需要将所有内部群集主机名输入到 /etc/hosts 文件中，以确保在发生 DNS 故障时群集能够持续工作。如果任一群集节点无法***按名称***解析所有其他节点，则本节中所述的群集配置将会失败。
- 每个群集节点的 CPU、RAM 和磁盘空间特征必须满足第 5 章 “ 满足系统要求 ”（第 33 页）中根据预期事件率定义的系统要求。

- 储存节点的磁盘空间和 I/O 特征必须满足第 5 章 “ 满足系统要求 ”（第 33 页）中根据本地和 / 或网络储存的预期事件率和数据保留策略定义的系统要求。
- 如果您要配置操作系统防火墙以限制对 Sentinel 和群集的访问，请参考第 7 章 “ 使用的端口 ”（第 51 页），以了解必须根据本地配置以及要发送事件数据的源提供的端口的细节。

本示范解决方案将使用以下配置：

- 两个 SUSE Linux 11 SP2 群集节点 VM
  - 操作系统安装不需要安装 X Windows，但如果需要 GUI 配置，则可以安装 X Windows。引导脚本可设置为在不使用 X 的情况下启动 （运行级别为 3），这样便可做到只在需要时才启动该脚本。
  - 节点将包含两个 NIC：一个用于外部访问，而另一个用于 iSCSI 通讯。
  - 使用可用于通过 SSH 或类似协议远程访问的 IP 地址配置外部 NIC。在本示例中，我们将使用 172.16.0.1 (node01) 和 172.16.0.2 (node02)。
  - 每个节点都应该为操作系统、 Sentinel 二进制文件和配置数据、群集软件、临时空间等提供足够的磁盘空间。请参见 SUSE Linux 和 SLE HAE 系统要求，以及 Sentinel 应用程序要求。
- 一个将 iSCSI 目标配置为共享储存的 SUSE Linux 11 SP2 VM
  - 操作系统安装不需要安装 X Windows，但如果需要 GUI 配置，则可以安装 X Windows。引导脚本可设置为在不使用 X 的情况下启动 （运行级别为 3），这样便可做到只在需要时才启动该脚本。
  - 系统将包含两个 NIC：一个用于外部访问，而另一个用于 iSCSI 通讯。
  - 使用可用于通过 SSH 或类似协议远程访问的 IP 地址配置外部 NIC。在本示例中，我们将使用 172.16.0.3 (storage03)。
  - 系统应该为操作系统和临时空间提供足够的空间，为共享储存提供大量的空间来保存 Sentinel 数据，并为 SBD 分区提供少量的空间。请参见 SUSE Linux 系统要求，以及 Sentinel 事件数据储存要求。在本示范解决方案中，我们会将所有数据 （本地、网络、 SBD）放置在单个磁盘上；但在生产部署中，可以将它们分配到不同的节点。

注释：在生产群集中，您可以在单独的 NIC （也可能是用于实现冗余的一对 NIC）上使用不可路由的内部 IP 进行内部群集通讯。

A.4.2 共享储存设置

设置您的共享储存，并确保能够将它装入每个群集节点。如果您在使用 FibreChannel 和 SAN，这可能会涉及到物理连接和其他配置。共享储存将用于保存 Sentinel 的数据库和事件数据，因此，必须根据预期事件率和数据保留策略，针对客户环境相应调整共享储存的大小。

典型的实现可能会使用通过 FibreChannel 连接到所有群集节点的高速 SAN，并使用一个大型 RAID 阵列储存本地事件数据。可以将单独的 NAS 或 iSCSI 节点用于速度较慢的网络储存。只要群集节点可以像普通的块设备那样装入本地储存，就能供解决方案使用。网络储存也可以作为块设备装入，或者可能是 NFS 或 CIFS 卷。

注释：您应该配置共享储存，并在每个群集节点上进行测试性装入，但是，储存的实际装入将由群集配置来处理。

在本示范解决方案中，我们将使用由 SUSE Linux VM 托管的 iSCSI 目标：

本示范解决方案将使用 SUSE Linux VM 上配置的 iSCSI 目标。该 VM 是初始设置中列出的 storage03。iSCSI 设备可使用任何文件或块设备进行创建，但为简单起见，我们这里将使用专为此目的创建的文件。

连接到 storage03 并启动控制台会话。使用 dd 命令为 Sentinel 本地储存创建一个任意所需大小的空文件：

```
dd if=/dev/zero of=/localdata count=10240000 bs=1024
```

在本例中，我们创建了一个用零 （从 /dev/zero pseudo-device 复制）填充的 10GB 文件。请参见 dd 的信息或手册页，以了解有关命令行选项的细节。例如，您可以创建不同大小的 “ 磁盘 ”。 iSCSI 目标将此文件视为磁盘；当然，如果您愿意的话，可以使用实际的磁盘。

重复此过程为网络储存创建文件：

```
dd if=/dev/zero of=/networkdata count=10240000 bs=1024
```

在本示例中，我们使用了两个大小与性能特征相同的文件 （“ 磁盘 ”）。在生产部署中，您可以将本地储存放置在高速 SAN 上，而将网络储存放置在速度较慢的 iSCSI、 NFS 或 CIFS 卷上。

将这些文件配置为 iSCSI 目标：

1. 从命令行 （如果您愿意，可以使用 GUI）运行 YaST：/sbin/yast
2. 选择 **Network Devices （网络设备）** > **Network Settings （网络设置）**。
3. 确保已选择**概述**选项卡。
4. 从显示的列表中选择辅助 NIC，然后按 Tab 切换到 “ 编辑 ” 并按 Enter。
5. 在**地址**选项卡上，指派静态 IP 地址 10.0.0.3。这将是内部 iSCSI 通讯 IP。
6. 单击**下一步**，然后单击**确定**。
7. 在主屏幕上，选择**网络服务** > **iSCSI 目标**。
8. 出现提示时，请从 SUSE Linux 11 SP2 媒体安装所需的软件 (iscsitarget RPM)。
9. 单击**服务**，选择**引导时**选项，以确保在引导操作系统时启动该服务。
10. 单击**全局**，然后选择**无鉴定**，因为 iSCSI 的当前 OCF 资源代理不支持鉴定。
11. 单击**目标**，然后单击**添加**以添加新目标。

    iSCSI 目标将自动生成 ID，然后显示可用 LUN （驱动器）的空列表。
12. 单击**添加**以添加新的 LUN。
13. 将 LUN 编号保留为 0，然后在**路径**对话框中浏览 （在 Type=fileio 下面），并选择已创建的 /localdata 文件。如果您将专用磁盘用于储存，请指定块设备，例如 /dev/sdc。
14. 重复步骤 12 至步骤 13，并在这次添加 LUN 1 和 /networkdata。
15. 将其他选项保留为默认值。单击**确定**，然后单击**下一步**。
16. 再次单击**下一步**，以选择默认鉴定选项，然后单击**完成**以退出配置。当系统请求重启动 iSCSI 时接受请求。
17. 退出 YaST。

以上过程在 IP 地址为 10.0.0.3 的服务器上公开了两个 iSCSI 目标。在每个群集节点上，请确保该节点能够装入本地数据共享储存设备。另外，还必须格式化该设备 （一次）：

1. 连接到其中一个群集节点 (node01) 并启动 YaST。
2. 选择 **Network Devices （网络设备）** > **Network Settings （网络设置）**。

3 确保已选择**概述**选项卡。

4 从显示的列表中选择辅助 NIC，然后按 Tab 切换到 “ 编辑 ” 并按 Enter。

5 单击**地址**，指派静态 IP 地址 10.0.0.1。这将是内部 iSCSI 通讯 IP。

6 选择**下一步**，然后单击**确定**。

7 单击**网络服务** > **iSCSI 发起程序**。

8 出现提示时，请从 SUSE Linux 11 SP2 媒体安装所需的软件 (open-iscsi RPM)。

9 单击**服务**，选择**引导时**，以确保在引导时启动 iSCSI 服务。

10 单击**已发现的目标**，然后选择**发现**。

11 指定 iSCSI IP 地址 (10.0.0.3)，选择**无鉴定**，然后单击**下一步**。

12 选择 IP 地址为 10.0.0.3 的已发现 iSCSI 目标，然后选择**登录**。

13 切换到**启动**下拉列表中的 “ 自动 ”，并选择**无鉴定**，然后单击**下一步**。

14 切换到**已连接的目标**选项卡，以确保连接到目标。

15 退出配置。此时， iSCSI 目标应该已作为块设备装入群集节点上。

16 在 YaST 主菜单中，选择**系统** > **分区程序**。

17 在系统视图中，列表中应该会显示新的硬盘 （例如 /dev/sdb 和 /dev/sdc），它们将属于 IET-VIRTUAL-DISK 类型。按 Tab 切换到列表中的第一项 （应该是本地储存），并选择该磁盘，然后按 Enter。

18 选择**添加**以将新分区添加到空磁盘。将该磁盘格式化为 ext3 主分区，但不要装入它。确保已选择 “ 不要装入分区 ” 选项。

19 选择**下一步**，然后在查看要做的更改后选择**完成**。假定您要在此共享 iSCSI LUN 上创建单个大型分区，则最终应生成 /dev/sdb1 或类似的已格式化磁盘 （下面称为 /dev/<SHARED1>）。

20 返回到分区程序，并针对 /dev/sdc 或与网络储存对应的任意块设备重复分区 / 格式化过程 （步骤 16 至步骤 19）。这应该会生成 /dev/sdc1 分区或类似的已格式化磁盘 （下面称为 /dev/<NETWORK1>）。

21 退出 YaST。

22 最后，根据如下所述创建一个安装点，并对本地分区进行测试性装入 （确切的设备名称取决于特定的实现）：

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

23 应该能够在新分区上创建文件，并在装入该分区的任何位置看到这些文件。

要卸载，请执行以下操作：

```
# umount /var/opt/novell
```

重复上述过程中的步骤 1 至步骤 15，以确保每个群集节点都能够装入本地共享储存。但是，请将步骤 5 中的节点 IP 替换为其他 IP （例如， node02 > 10.0.0.2）。

A.4.3 Sentinel 安装

可以使用两个选项安装 Sentinel：将 Sentinel 的任何部分都安装到共享储存中 （使用 --location 选项将 Sentinel 安装重定向到已装入共享储存的任何位置），或者只将可变应用程序数据放置在共享储存中。

在此示范解决方案中，我们将采用后一种方法，将 Sentinel 安装到可以托管 Sentinel 的每个群集节点上。在首次安装 Sentinel 时，我们将会执行完整安装，包括应用程序二进制文件、配置和所有数据储存区。在其他群集节点上执行后续安装时，只会安装应用程序，并假定在以后的某个时间 （例如，在装入共享储存后）提供实际的 Sentinel 数据。

示范解决方案：

在此示范解决方案中，我们将 Sentinel 安装到每个群集节点，同时只在共享储存上储存可变应用程序数据。这会将应用程序二进制文件和配置保留在标准位置，使我们能够校验 RPM，并在特定的情况下支持热增补。

在第一个节点上安装

1. 连接到其中一个群集节点 (node01) 并打开控制台窗口。
2. 下载 Sentinel 安装程序 （tar.gz 文件），并将其储存在群集节点上的 /tmp 中。
3. 执行以下命令：

```
mount /dev/<SHARED1> /var/opt/novell

cd /tmp

tar -xvzf sentinel_server*.tar.gz

cd sentinel_server*

./install-sentinel --record-unattended=/tmp/install.props
```

1. 完成整个标准安装，并根据需要配置产品。安装程序将会安装二进制文件、配置和数据库，并设置用户名 / 口令和网络端口。
2. 启动 Sentinel 并测试基本功能。您可以使用标准的外部群集节点 IP 访问本产品。
3. 关闭 Sentinel 并卸下共享储存：

```
rcsentinel stop

umount /var/opt/novell
```

此步骤将去除自动启动脚本，使群集可以管理产品。

```
cd /

insserv -r sentinel
```

在后续节点上安装

在其他节点上重复安装：

初始 Sentinel 安装程序将创建一个用户帐户供本产品使用，该用户帐户在安装时使用下一个可用的用户 ID。在无人照管模式下执行后续安装时，将尝试使用相同的用户 ID 创建帐户，但确实存在冲突的可能性 （如果群集节点在安装时不相同）。强烈建议执行以下操作之一：

- 跨群集节点同步用户帐户数据库 （通过 LDAP 或类似的程序手动同步），确保在执行后续安装之前进行同步。在此情况下，安装程序将检测用户帐户是否存在，并使用现有的用户帐户。
- 观察后续无人照管安装的输出 - 如果无法使用相同的用户 ID 创建用户帐户，将会发出警告。

1 连接到每个附加的群集节点 (node02) 并打开控制台窗口。

2 执行以下命令：

```
cd /tmp
scp root@node01:/tmp/sentinel_server*.tar.gz
scp root@node01:/tmp/install.props
tar -xvzf sentinel_server*.tar.gz
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
cd /
insserv -r sentinel
```

在此过程结束时， Sentinel 应已安装在所有节点上，但在同步各个密钥之前 （在配置群集资源时会执行这种同步），它有可能无法正常工作。

A.4.4 群集安装

在每个节点上安装群集软件，并使用群集管理器注册每个群集节点。此操作的执行过程因群集实现而异，但在过程结束时，每个群集节点应出现在群集管理控制台中。

在我们的示范解决方案中，我们将设置 SUSE Linux High Availability Extension，并使用 Sentinel 特定的资源代理将它覆盖：

如果您不使用 OCF 资源代理监视 Sentinel，则可能需要为本地群集环境开发一个类似的监视解决方案。 Sentinel 的 OCF 资源代理是一个简单的外壳脚本，它可以运行各种检查，以校验 Sentinel 是否正常工作。如果您想要开发自己的解决方案，则应该研究现有的资源代理并以此为例 （资源代理储存在 Sentinel 下载包中的 sentinel-ha.rpm 内。）

有许多方法可用于配置 SLE HAE 群集，但我们将选择可以十分简单地完成配置的选项。第一步是安装核心 SLE HAE 软件； SLE HAE 文档中详尽地介绍了相关过程。有关安装 SLES 外接式附件的信息，请参见 《部署指南》。

必须在所有群集节点 （在我们的示例中为 node01 和 node02）上安装 SLE HAE。外接式附件将安装核心群集管理和通讯软件，以及用于监视群集资源的许多资源代理。

在安装群集软件后，应安装一个附加的 RPM，以提供 Sentinel 特定的附加群集资源代理。该 RPM 可以在安装产品时解压的正常 Sentinel 下载包中储存的 novell-Sentinel-ha-7.1*.rpm 内找到。

在每个群集节点上，将 novell-Sentinel-ha-7.1*.rpm 复制到 /tmp 目录中，然后执行以下命令：

```
cd /tmp
rpm -i novell-Sentinel-ha-7.1*.rpm
```

A.4.5 群集配置

您必须配置群集软件，以便将每个群集节点注册为群集的成员。作为此配置的一部分，您还可以设置隔离和 STONITH 资源，以确保群集的一致性。

我们的示范解决方案基本上使用了不包含附加冗余或其他高级功能的最简单配置。我们还使用了单播地址 （而不是首选的多播地址），因为它要求的与网络管理员之间的交互更少，并且足以用于实现测试目的。我们还设置了一个基于 SBD 的简单隔离资源。

示范解决方案：

本示范解决方案将使用私用 IP 地址进行内部群集通讯，并使用单播地址最大程度地减少从网络管理员请求多播地址的需要。本解决方案还将使用托管共享储存的同一个 SUSE Linux VM 上配置的 iSCSI 目标，以用作实现隔离目的的 SBD 设备。如前所述， iSCSI 设备可使用任何文件或块设备进行创建，但为简单起见，我们这里将使用专为此目的创建的文件。

以下配置步骤与 “ 共享储存设置 ” 中的步骤非常相似：

SBD 设置

连接到 storage03 并启动控制台会话。使用 **dd** 命令创建一个任意所需大小的空文件：

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```

在本例中，我们创建了一个用零 （从 /dev/zero pseudo-device 复制）填充的 1MB 文件。

将该文件配置为 iSCSI 目标：

1. 从命令行 （如果您愿意，可以使用 GUI）运行 YaST：/sbin/yast
2. 选择**网络服务** > **iSCSI 目标**。
3. 单击**目标**并选择现有目标。
4. 选择**编辑**。 UI 将显示可用 LUN （驱动器）的列表。
5. 选择**添加**以添加新的 LUN。
6. 将 LUN 编号保留为 2。在**路径**对话框中浏览，并选择已创建的 /sbd 文件。
7. 将其他选项保留为默认值，依次选择**确定**和**下一步**，然后再次单击**下一步**，以选择默认的鉴定选项。
8. 单击**完成**以退出配置。根据需要重启动服务。退出 YaST。

注释：以下步骤要求每个群集节点都能够解析所有其他群集节点的主机名 （否则，文件同步服务 csync2 将会失败）。如果 DNS 未设置或不可用，请在列出每个 IP 及其主机名 （由 hostname 命令报告）的 /etc/hosts 文件中添加每个主机的项。

此过程应会在 IP 地址为 10.0.0.3 的服务器上公开 SBD 设备的 iSCSI 目标 (storage03)。

节点配置

连接到群集节点 (node01) 并打开控制台：

1. 运行 YaST.
2. 打开**网络服务** > **iSCSI 发起程序**。
3. 选择**已连接的目标**，然后选择您在前面配置的 iSCSI 目标。
4. 选择**注销**选项，并从目标中注销。

5 切换到**已发现的目标**选项卡，选择**目标**，然后重新登录以刷新设备列表 （保留自动启动选项和 “无鉴定 ”）。

6 选择**确定**以退出 iSCSI 发起程序工具。

7 打开**系统** > **分区程序**，然后将 SBD 设备标识为 1MB IET-VIRTUAL-DISK。该设备将以 **/dev/sdd** 或类似的形式列出 - 请记下具体的标识。

8 退出 YaST。

9 执行命令 ls -l /dev/disk/by-id/，并记下已链接到您前面找到的设备名称的设备 ID。

10 执行命令 sleha-init。

11 当系统提示您提供要绑定到的网络地址时，请指定外部 NIC IP (172.16.0.1)。

12 接受默认的多播地址和端口。稍后我们将覆盖这些信息。

13 输入 “y” 以启用 SBD，然后指定 /dev/disk/by-id/< 设备 ID>，其中， < 设备 ID> 是您前面找到的 ID （可以使用 Tab 键自动填写路径）。

14 完成向导并确保未报告任何错误。

15 启动 YaST。

16 选择**高可用性** > **群集** （在某些系统上只需直接选择 “ 群集 ”）。

17 在左侧的框中，确保已选择**通讯通道**。

18 按 Tab 切换到配置的首行，并将所选的 udp 更改为 udpu （这会禁用多播并选择单播）。

19 选择**添加成员地址**并指定此节点 (172.16.0.1)，然后重复此步骤并添加其他群集节点：172.16.0.2。

20 选择**完成**以完成配置。

21 退出 YaST。

22 运行命令 /etc/rc.d/openais restart，以使用新的同步协议重启动群集服务。

连接到每个附加的群集节点 (node02) 并打开控制台：

1 运行以下命令：sleha-join

2 输入第一个群集节点的 IP 地址。

在某些情况下，群集通讯无法正常初始化。如果群集无法启动 （openais 服务无法启动），请执行以下操作：

- 手动将 corosync.conf 从 node1 复制到 node02，或者在 node 1 上运行 csync2 -x -v，或者通过 YaST 在 node02 上手动设置群集。
- 在 node02 上运行 /etc/rc.d/openais start

在某些情况下， xinetd 服务无法正常添加新的 csync2 服务可能会导致脚本失败。为了使其他节点能够将群集配置文件一直同步到此节点，需要此服务。如果显示诸如 csync2 运行失败之类的错误，则表明您可能遇到此问题。要修复此问题，请执行 kill -HUP `cat /var/run/xinetd.init.pid，然后重新运行 sleha-join 脚本。

此时，您应该能够在每个群集节点上运行 crm_mon，并发现群集在正常运行。或者，您可以使用 Web 控制台 “hawk”- 默认的登录身份凭证为 “hacluster/linux”。

对于此示例，我们需要稍微调整两个附加参数；这些调整是否适用于客户的生产群集将取决于其群集的配置：

1. 将全局群集选项 no-quorum-policy 设置为 ignore。我们之所以执行此操作，原因在于我们只有一个双节点群集，因此，任何一个节点发生故障都会破坏仲裁，并关闭整个群集：crm configure property no-quorum-policy=ignore

   注释：如果您的群集具有两个以上的节点，请不要设置此选项。

2. 将全局群集选项 default-resource-stickiness 设置为 1。这会促使资源管理器将资源保持为就地运行，而不是将它们移动到其他位置：crm configure property default-resource-stickiness=1。

A.4.6 资源配置

如 “ 群集安装 ” 中所述，此解决方案提供了一个 OCF 资源代理，用于监视 SLE HAE 下的核心服务，您可以根据需要创建替代的资源代理。该软件还依赖于其他多个资源，这些资源的资源代理默认为随 SLE HAE 一起提供。如果您不想要使用 SLE HAE，则需要使用其他某种技术监视这些附加资源：

- 与该软件所用的共享储存对应的文件系统资源。
- 与用来访问服务的虚拟 IP 对应的 IP 地址资源。
- 该软件用来储存配置和事件元数据的 Postgres 数据库软件。

还有其他一些资源，例如用于安全智能的 MongoDB，以及 ActiveMQ 讯息总线；至少目前可将这些资源作为核心服务的一部分进行监视。

示范解决方案

本示范解决方案使用所需资源的简单版本，例如简单的文件系统资源代理。您可以根据需要选择使用更复杂的群集资源，例如 cLVM （文件系统的逻辑卷版本）。

本示范解决方案提供了 crm 脚本，用于帮助完成群集配置。该脚本将从安装 Sentinel 的过程中生成的无人照管安装文件提取相关的配置变量。如果您未生成安装文件，或者想要更改资源的配置，则可以相应地编辑该脚本。

连接到安装了 Sentinel 的原始节点 （这必须是您在其上运行完全 Sentinel 安装的节点），然后执行以下操作 （<SHARED1> 是您前面创建的共享卷）：

```
mount /dev/<SHARED1> /var/opt/novell
```

```
cd /usr/lib/ocf/resource.d/novell
```

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

群集中出现的新资源可能有问题；如果遇到此问题，请在 node02 上运行 /etc/rc.d/openais restart。

install-resources.sh 脚本将提示您提供两个值 （即您希望用户在访问 Sentinel 时使用的虚拟 IP，以及共享储存的设备名称），然后将自动创建所需的群集资源。请注意，脚本要求已装入共享卷，并要求在安装 Sentinel 的过程中创建的无人照管安装文件 (/tmp/install.props) 存在。您只需要在第一个已安装的节点上运行此脚本；所有相关的配置文件将自动同步到其他节点。

如果客户环境与此示例解决方案不同，您可以编辑 resources.cli 文件 （位于同一个目录中），并在该文件中修改基元定义。例如，本示范解决方案使用了简单的文件系统资源；您可能需要使用一个群集感知程度更高的 cLVM 资源。

在运行外壳脚本后，您可以发出 crm satus 命令，其输出应如下所示：

```
crm status
```

```
Last updated: Thu Jul 26 16:34:34 2012
Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
Stack: openais
Current DC: node01 - partition with quorum
Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
2 Nodes configured, 2 expected votes
5 Resources configured.
```

```
Online: [ node01, node02 ]
stonith-sbd    (stonith:external/sbd):    Started node01
 Resource Group: sentinelgrp
     sentinelip    (ocf::heartbeat:IPaddr2):    Started node01
     sentinelfs    (ocf::heartbeat:Filesystem):    Started node01
     sentineldb    (ocf::novell:pgsql):    Started node01
     sentinelserver    (ocf::novell:sentinel):    Started node01
```

此时，应该已在群集中配置了相关的 Sentinel 资源。您可以在群集管理工具中检查这些资源的配置和分组方式 （例如，通过运行 crm status）。

A.4.7 网络储存配置

此过程的最后一步是配置网络储存，使 Sentinel 能够将事件分区迁移到更经济的储存中。这是一个可选操作，事实上，不需要像配置系统的其他部件一样，将网络储存配置为高度可用 - 您可以使用任何目录 （无论是否从 SAN 装入），或者 NFS 或 CIFS 卷。

在顶部菜单栏中单击**储存**，选择**配置**，然后选择 “ 未配置的网络储存 ” 下的其中一个单选按钮，以完成此设置。

示范解决方案

本示范解决方案将使用简单的 iSCSI 目标作为网络共享储存位置，这在很大程度上与本地储存的配置相同。在生产实现中，有可能会使用不同的储存技术。

使用以下过程配置网络储存以供 Sentinel 使用：

注释：由于我们要为此示范解决方案使用 iSCSI 目标，因此将以用作网络储存的目录的形式装入目标。这样，我们需要以类似于配置本地储存文件系统的方式，将装入配置为文件系统资源。由于存在其他可能的差异，因此，在执行资源安装脚本的过程中未自动完成这些设置；我们需要在这里手动进行配置。

1. 复查前面的步骤，以确定创建了哪个分区以用作网络储存 （/dev/<NETWORK1>，或者类似于 /dev/sdc1 的标识）。如果需要，请创建一个可用于装入分区的空目录 （例如 /var/opt/netdata）。
2. 将网络文件系统设置为群集资源：使用 Web GUI 或运行命令：

   ```
   crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/
   dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
   ```

   其中， /dev/<NETWORK1> 是在前面 “ 共享储存设置 ” 一节中创建的分区，而 <PATH> 是该分区可以装入到的任何本地目录。
3. 将新资源添加到受管资源组：

   ```
    crm resource stop sentinelgrp
    crm configure delete sentinelgrp
    crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb
   sentinelserver
    crm resource start sentinelgrp
   ```
4. 您可以连接到当前托管资源的节点 （使用 crm status 命令或 Hawk），并确保已正确装入网络储存 （使用 mount 命令）。

5 登录到 Sentinel Web 界面。

6 依次选择**储存**和**配置**，然后在 “ 未配置的网络储存 ” 下选择 **SAN （本地装入）**。

7 键入网络储存装入到的路径，例如 /var/opt/netdata。

本示范解决方案使用了所需资源的简单版本，例如简单的文件系统资源代理 - 客户可以根据需要选择使用更复杂的群集资源，例如 cLVM （文件系统的逻辑卷版本）。

A.5 备份和恢复

本文档中介绍的高可用性故障转移群集提供了某种冗余级别，这样，如果群集中某个节点上的服务发生故障，该服务将会自动进行故障转移，并在群集中的另一个节点上恢复。当发生此类事件时，必须将发生故障的节点恢复到正常运行状态，使系统中的冗余能够恢复，并在再次发生故障时提供保护。本节将探讨如何在各种故障情况下恢复发生故障的节点。

A.5.1 备份

尽管高可用性故障转移群集 （例如本文档中介绍的群集）提供了冗余层，但是，以传统方式定期备份配置和数据仍很重要，不过，在发生丢失或损坏的情况下，可能无法轻松地从中恢复。*《NetIQ Sentinel 7.1 管理指南》*中的 “ 备份和恢复数据 ” 一节介绍了如何使用 Sentinel 的内置工具创建备份。这些工具应该在群集中的主动节点上使用，因为群集中的被动节点对共享储存设备没有必需的访问权限。其他商用的备份工具也可以使用，这些工具可能对使用它们的节点有着不同的要求。

A.5.2 恢复

临时故障

如果故障是临时性的，并且对应用程序和操作系统软件以及配置没有造成明显的损坏，则只需清除临时故障 （例如，重引导节点），即可将节点恢复到正常运行状态。如果需要，可以使用群集管理用户界面将运行中的服务故障回复到原始群集节点。

节点损坏

如果故障导致了节点储存系统中的应用程序、操作系统软件或配置损坏，则需要重新安装损坏的软件。重复本文档前面介绍的向群集添加节点的步骤，即可将节点恢复到正常运行状态。如果需要，可以使用群集管理用户界面将运行中的服务故障回复到原始群集节点。

群集数据配置

如果共享储存设备上发生数据损坏，并且共享储存设备无法从这种损坏中恢复，则会导致影响整个群集的损坏，并且使用本文档中所述的高可用性故障转移群集也无法从这种损坏中自动恢复。*《NetIQ Sentinel 7.1 管理指南》*中的“备份和恢复数据”一节介绍了如何使用 Sentinel 的内置工具从备份中恢复。这些工具应该在群集中的主动节点上使用，因为群集中的被动节点对共享储存设备没有必需的访问权限。其他商用的备份和恢复工具也可以使用，这些工具可能对使用它们的节点有着不同的要求。

B 排查安装问题

本节包含安装过程中可能出现的一些问题以及解决这些问题的措施。

B.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。如果网络不可用，在设备上安装 Sentinel 将失败。

要解决此问题，请正确配置网络设置。要验证配置，请使用 ifconfig 命令返回有效的 IP 地址，并使用 hostname -f 命令返回有效的主机名。

B.2 UUID 不是为收集器管理器或关联引擎映像而创建

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 将不能唯一识别收集器管理器的各个新实例。这是因为重复的 UUID 造成的。

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新的 UUID：

1. 删除位于 /var/opt/novell/sentinel/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。

C 卸装

本附录将介绍如何卸装 Sentinel 以及卸装后的任务。

C.1 卸装核对清单

使用以下核对清单卸装 Sentinel：

- ❒ 卸装 Sentinel 服务器。
- ❒ 卸装收集器管理器和关联引擎 （如果有）。
- ❒ 执行卸装后的任务以完成 Sentinel 卸装。

C.2 卸装 Sentinel

有一个卸装脚本可帮助您去除 Sentinel 安装。在执行全新安装之前，应该执行以下所有步骤，以确保以前的安装没有剩下任何文件或系统设置。

警告：以下说明包括修改操作系统设置和文件。如果您对修改这些系统设置和文件不熟悉，请联系您的系统管理员。

C.2.1 卸装 Sentinel 服务器

使用以下步骤卸装 Sentinel 服务器：

1. 以 root 用户身份登录到 Sentinel 服务器。

   注释：如果安装是以 root 用户身份执行的，则非 root 用户无法卸装 Sentinel 服务器。但是，如果安装是以非 root 用户身份执行的，则非 root 用户可以卸装 Sentinel 服务器。

2. 访问以下目录：

   ```
   /opt/novell/sentinel/setup/
   ```

3. 运行以下命令：

   ```
   ./uninstall-sentinel
   ```

4 当提示重新确认希望卸装时，请按 y。

该脚本首先停止服务，然后完全去除它。

C.2.2 卸装收集器管理器或关联引擎

使用以下步骤卸装收集器管理器和关联引擎：

1 以 root 身份登录。

注释：如果您是以根用户身份安装的远程收集器管理器或远程关联引擎，则无法以非根用户身份执行卸装。但是，如果是由非根用户执行的安装，则非根用户可以执行卸装。

2 转到以下位置：

```
/opt/novell/sentinel/setup
```

3 运行以下命令：

```
./uninstall-sentinel
```

脚本会显示一条警告，指示将会彻底删除收集器管理器或关联引擎及所有相关数据。

4 输入 y 去除收集器管理器或关联引擎。

该脚本首先停止服务，然后完全去除它。但是，“ 收集器管理器和关联引擎 ” 图标仍会在 Web 界面中显示为非活动状态。

5 执行以下附加步骤可在 Web 界面中手动删除收集器管理器和关联引擎：

收集器管理器 :

1. 访问 *事件源管理 > 实时视图*。
2. 右键单击要删除的收集器管理器，然后单击 *删除*。

关联引擎 :

1. 以管理员身份登录到 Sentinel Web 界面。
2. 展开 *关联*，然后选择您希望删除的关联引擎。
3. 单击 *删除* 按钮 （回收站图标）。

C.3 卸装后的任务

在卸装 Sentinel 服务器时，不会从操作系统中去除 Sentinel 管理员用户。您必须手动去除该用户。

卸装 Sentinel 之后，某些系统设置会保留。在执行 Sentinel 的 “ 干净 ” 安装之前应该去除这些设置，尤其是如果 Sentinel 卸装遇到错误时。

要手动 Sentinel 系统设置：

1 以 root 身份登录。

2 确保所有 Sentinel 流程均已停止。

3 去除 /opt/novell/sentinel （或 Sentinel 软件安装的任何位置）下的内容。

4 确保没有人以 Sentinel 管理员操作系统用户 （默认为 novell）身份登录，然后去除用户、主目录以及组。

```
userdel -r novell
```

groupdel novell

5 重启动操作系统。