Sentinel™

安装和配置指南

2018 年 7 月

NetIQ

法律声明

关于本书和库

*《安装和配置指南》*介绍了 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。

了解 Sentinel

本节将详细介绍 Sentinel 及其如何为您的组织提供事件管理解决方案。

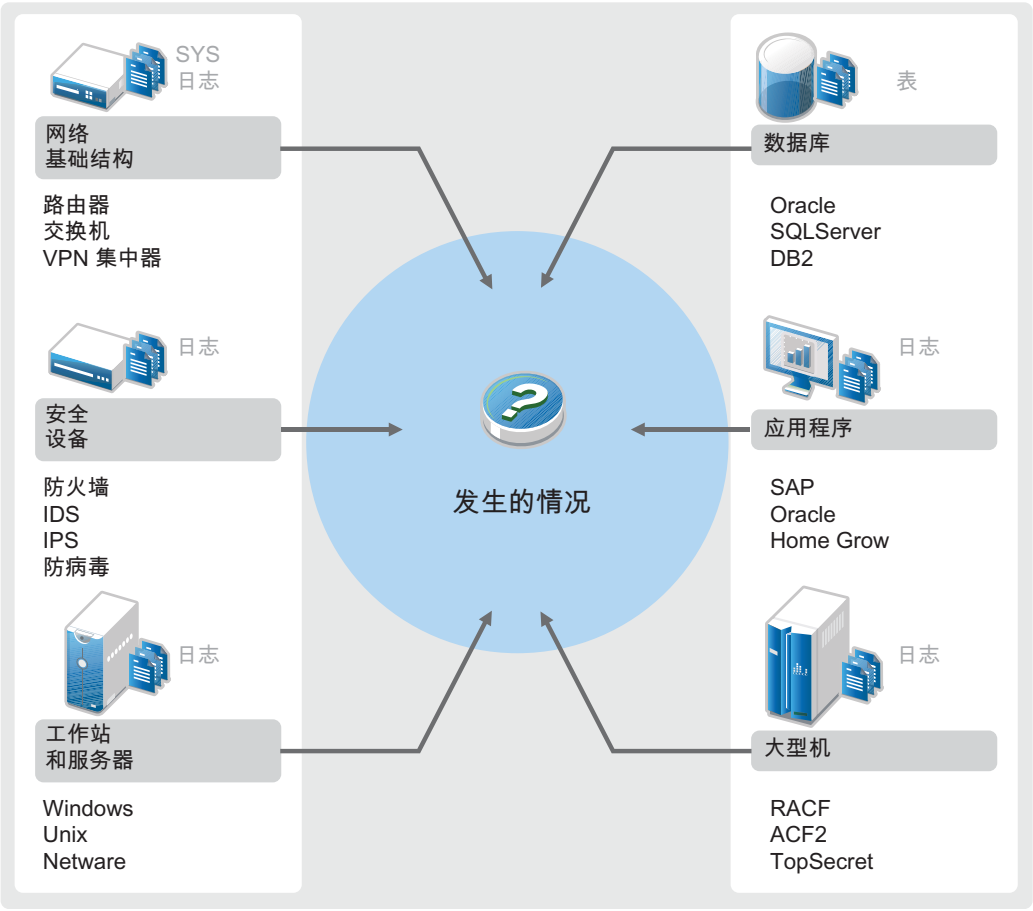
1 Sentinel 是什么？

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。

保护 IT 环境的挑战

由于环境的复杂性，确保 IT 环境安全已成为一项挑战。通常，IT 环境中存在许多应用程序、数据库、大型主机、工作站和服务器，且所有这些条目均会生成事件日志。您的 IT 环境中可能还存在会生成事件日志的安全设备和网络基础设施设备。

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.
- 日志存储在不同的位置。
- 日志文件中捕获的信息量非常大。
- 无需手动分析日志文件，即可确定事件触发器。

要利用日志中的信息，必须能够执行以下操作：

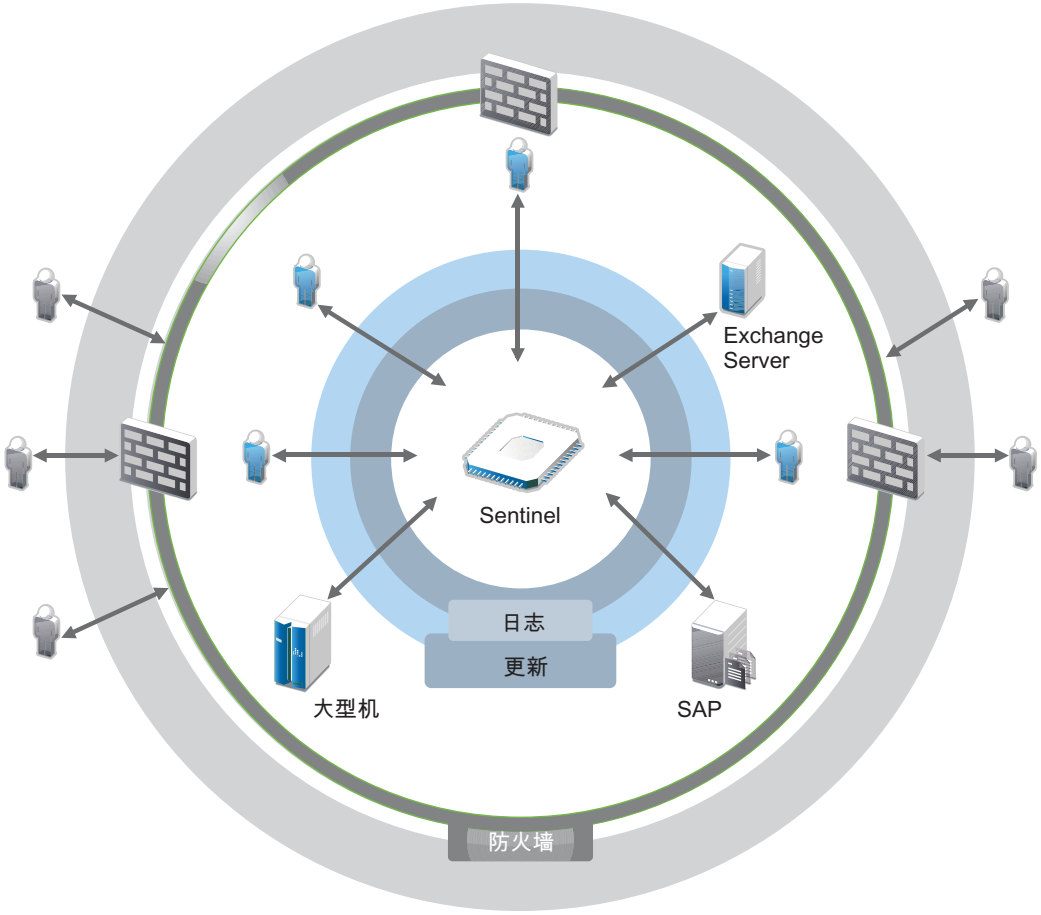
- 收集数据.
- 合并数据.
- 将不同的数据规范化为可轻松比较的事件。
- 将事件映射到标准法规.
- 分析数据.
- 比较多个系统中的事件以确定是否存在安全性问题.
- 数据不符合规范时发送通知。
- 对通知采取措施以遵循企业策略.
- 生成报告以证实合规性.

了解保护 IT 环境的挑战后，您需要确定如何保护用户的企业而又不影响用户体验。Sentinel 可为此提供解决方案。

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收集数据。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



通过 Sentinel，您可以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。这样您就可以确定用户行为并有效地监视活动以防止恶意活动。

Sentinel 通过以下途径实现此目标：

- 提供单个解决方案应对跨多个安全标准的 IT 控制。
- 填补了对 IT 环境的预期行为及其实际结果之间的鸿沟。
- 帮助您遵从安全标准。
- 提供即用型合规性监视和报告程序.

Sentinel 可使日志收集、分析和报告过程自动执行，以确保 IT 控件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事件、合规性事件和 IT 控制的功能。如果存在安全漏洞或发生非合规性事件，您可以立即采取措施。 通过 Sentinel，您还可以收集有关环境的摘要信息，并与您的主要利益相关人共享这些信息。

2 Sentinel 工作原理

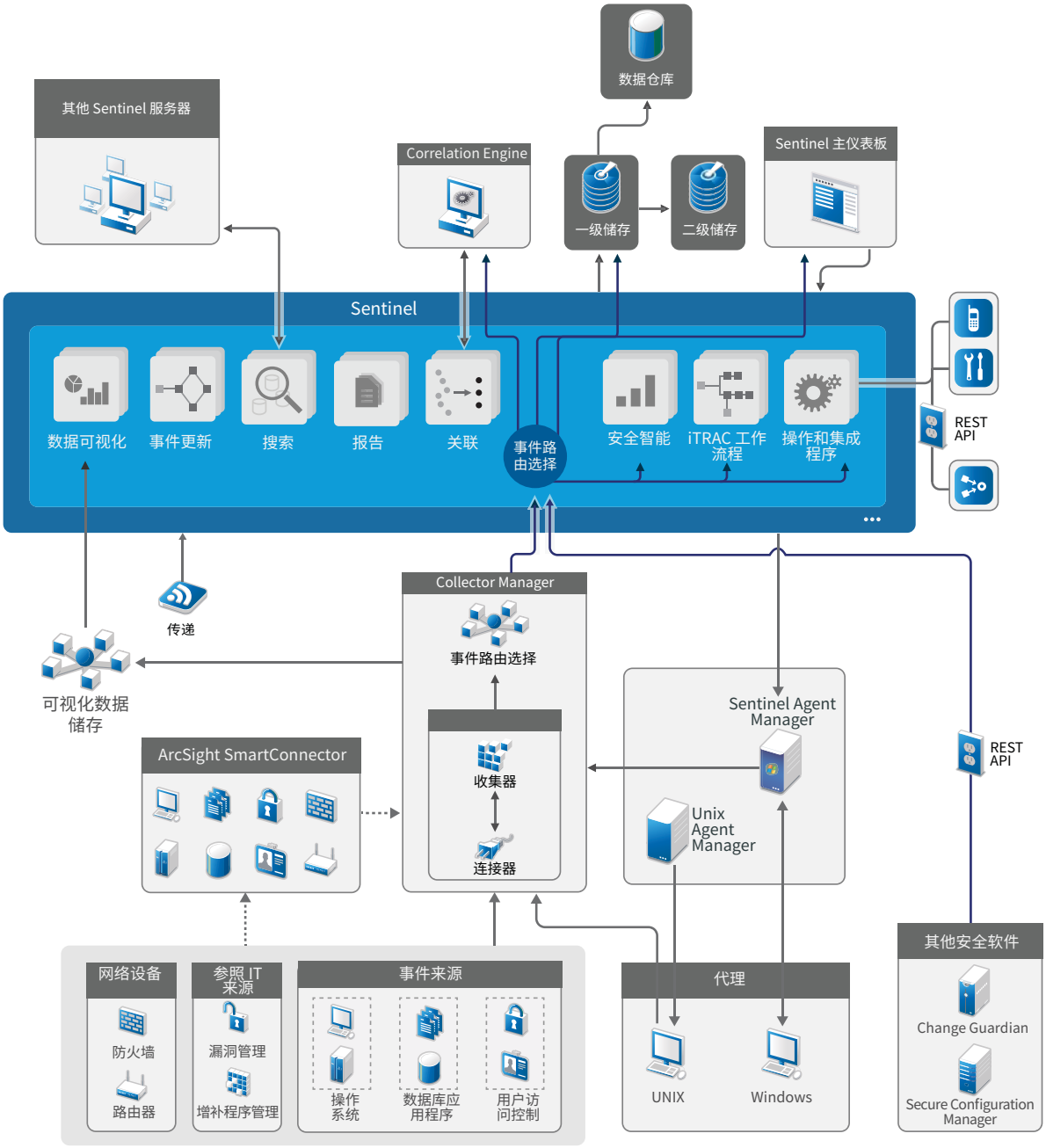
Sentinel 会持续管理整个 IT 环境中的安全信息和事件，以便提供完整的监视解决方案。

Sentinel 执行以下操作：

- 从 IT 环境的各种源中收集日志、事件和安全信息。
- 将收集的日志、事件和安全信息规范化为标准 Sentinel 格式。
- 根据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或基于 Hadoop 的可缩放储存中。
- 收集 IP 流数据并帮助您监视网络活动的详细情况。
- 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。
- 关联给定时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。

下图说明了在使用传统储存作为数据储存选项时 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：

- 事件源（第 21 页）
- Sentinel 事件（第 21 页）
- Collector Manager（第 23 页）
- ArcSight SmartConnector（第 24 页）
- 代理管理器（第 24 页）

事件源

Sentinel 从 IT 环境的各种源中收集安全信息和事件。这些源称为事件源。通常，您的网络中存在以下事件源：

安全外围： 安全设备，包括用于为环境创建安全外围的硬件和软件，如防火墙、入侵检测系统 (IDS) 和虚拟专用网 (VPN)。

操作系统： 网络中运行的各种操作系统。

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： 网络中安装的各种应用程序。

用户访问控件： 允许用户访问公司资源的应用程序或设备。

有关从事件源收集事件的详细信息，请参见“《 Sentinel 管理指南》”中的*收集和路由事件数据*。

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。

事件表示从第三方安全设备、网络、应用设备或内部 Sentinel 源报告给 Sentinel 的规范化日志记录。有以下几种类型的事件：

- 外部事件（从安全设备接收到的事件），如下所述：
  - 入侵检测系统 (IDS) 检测到的攻击
  - 操作系统报告的成功登录
  - 客户定义的情况，如用户访问某个文件
- 内部事件（由 Sentinel 生成的事件），包括：
  - 禁用关联规则
  - 数据库填充

Sentinel 将类别信息（分类）添加到事件，以便更轻松地对比报告不同事件的系统中的事件。事件由实时显示器、Correlation Engine、仪表板和后端服务器进行处理。

一个事件包含 200 多个字段；事件字段类型和目的各不相同。例如，一些预定义的字段包括严重性、危急程度、目标 IP 地址和目标端口。

有两组可配置的字段：

- 保留字段：供 Sentinel 内部使用，以便将来扩展功能。
- 客户字段：供客户使用以允许自定义。

字段的源可以是外部的，也可以是引用的：

- 外部字段的值由设备或相应收集器显式设置。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 地址的资产的构建。
- 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，可以通过采用了客户定义映射（使用事件中的目标 IP 地址）的映射服务来计算字段。

- 映射服务（第 22 页）
- 流式传输映射（第 22 页）
- 攻击检测（第 22 页）

映射服务

映射服务在整个系统中传输业务相关数据。此数据可以使用引用信息来丰富事件。

您可以通过使用映射将额外的信息（如主机和身份信息）添加到从源设备传入的事件，以此来丰富事件数据。Sentinel 可以使用此额外的信息进行高级关联和报告。Sentinel 支持多个内置映射以及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，在内部进行更新且会自动导出到映射服务。
- 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用户界面进行更新，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 Collector Manager 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。

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。对于像 Sentinel 这样任务关键型的实时系统，它们需要稳定、可预测且敏捷地移动数据，并且又不依赖于系统中的任何临时负载，上述特点便能发挥其作用。

攻击检测

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。存在尝试利用易受攻击系统时，Sentinel 会自动及时通知用户。Sentinel 通过以下功能完成此操作：

- Advisor 传递
- 入侵检测

- 漏洞扫描
- 防火墙

Advisor 传递包含有关漏洞、威胁以及事件签名和漏洞插件规范化的信息。它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。有关 Advisor 传递的详细信息，请参见“《 Sentinel 管理指南》”中的*检测漏洞和攻击*。

Collector Manager

Collector Manager 管理数据收集、监视系统状态讯息并执行事件过滤。Collector Manager 的主要功能包括以下内容：

- 通过使用连接器来收集数据。
- 通过使用收集器来分析和规范化数据。

收集器

收集器从连接器收集信息并进行规范化。它们执行以下功能：

- 从连接器中接收原始数据。
- 分析并规范化数据：
  - 将特定于事件源的数据转换为特定于 Sentinel 的数据。
  - 通过以 Sentinel 可读取的格式更改信息来丰富事件。
  - 事件的特定于事件源的过滤。
- 通过映射服务向事件添加业务相关性：
  - 将事件映射到身份。
  - 将事件映射到资产。
- 路由事件。
- 将已规范化、已分析和已设置格式的数据传递到 Collector Manager。
- 向 Sentinel 服务器发送运行状况讯息。

有关收集器的更多信息，请参见 Sentinel 插件网站。

连接器

连接器提供了从事件源到 Sentinel 系统的连接。

连接器提供以下功能：

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

ArcSight SmartConnector

Sentinel 使用 ArcSight SmartConnector 从 Sentinel 不直接支持的各种类型事件来源中收集事件。SmartConnector 从支持的设备收集事件，将事件规范化为通用事件格式 (CEF)，并通过 Syslog Connector 将事件转发到 Sentinel。然后，Connector 将事件转发到 Universal Common Event Format Collector 进行分析。

有关通过 SmartConnector 配置 Sentinel 的详细信息，请参见 Sentinel 插件网站中的 Universal Common Event Format Collector 文档。

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：

- 访问网络中不可用的日志。
- 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，并可作为流入 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。

Sentinel 数据路由和数据储存

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 Collector Manager 接收分析的事件数据和原始数据。Sentinel 会储存原始数据以提供安全证据链，并根据您定义的规则对分析的事件数据进行路由。您可以过滤分析的事件数据、将其发送到存储或实时分析，并路由到外部系统。Sentinel 进一步对照用户定义的保留政策匹配所有发往储存的事件数据。保留策略控制应从系统删除事件数据的时间。

根据每秒事件数(EPS)大小和您的部署要求，您可以选择使用基于文件的传统数据储存或基于Hadoop的可缩放储存作为数据储存选项。有关详细信息，请参见数据储存考虑事项（第 39 页）。

事件可视化

Sentinel 提供以图表、表格和地图形式显示数据的事件可视化。这些可视化将使得可视化和分析大量事件（包括 IP 流事件）变得更加轻松。您也可以创建自己的可视化和仪表板。

Sentinel 中默认存在事件可视化，并具有可缩放储存。在传统储存设置中，事件可视化仅在启用了可视化数据储存 (Elasticsearch) 以储存数据和建立数据索引后可用。有关启用 Elasticsearch 的更多信息，请参见配置“可视化数据储存”（第 42 页）。

关联

单个事件看起来可能很普通，但结合其他事件时可能会提醒您存在潜在问题。Sentinel 可以通过使用在 Correlation Engine 中创建和部署的规则来帮助您关联此类事件，并采取适当的措施来缓解任何问题。

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。有关关联的详细信息，请参见“《 Sentinel 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 Correlation Engine 中部署规则。当符合规则准则的事件发生时，Correlation Engine 将生成描述该模式的关联事件。有关详细信息，请参见 “《 Sentinel 用户指南》”中的 *Correlation Engine*。

安全智能

借助 Sentinel 提供的关联功能，您能够查找已知的活动模式，从而可以分析安全性、合规性或任何其他原因。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，从而识别并分析异常。有关详细信息，请参见 “《 Sentinel 用户指南》”中的*分析数据中的趋势*。

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。还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 “《 Sentinel 用户指南》”中的*配置事件*。

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）。

您可以使用手动和自动步骤构建工作流程。iTRAC 工作流程支持高级功能，如分支、基于时间的升级和本地变量。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，请参见 “《 Sentinel 用户指南》”中的*配置 iTRAC 工作流*。

操作和集成器

“操作”手动或自动执行某些类型的操作，如发送电子邮件。您可以通过路由规则、手动执行事件或事件操作以及关联规则来触发“操作”。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 “《Sentinel 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 “《Sentinel 管理指南》”中的*配置集成器*。

搜索

Sentinel 提供一个选项用以执行事件搜索操作。通过必要的配置，您还可以搜索由 Sentinel 生成的系统事件，并查看每个事件的原始数据。有关详细信息，请参见“《Sentinel 用户指南》”中的*搜索事件*。

您还可以搜索分布在不同地理位置上的 Sentinel 服务器。有关详细信息，请参见“《Sentinel 管理指南》”中的*配置数据联合*。

报告

Sentinel 提供了对收集的数据运行报告的功能。Sentinel 中打包了各种可自定义的报告。一些报告是可配置的，让您可以指定要在结果中显示的列。

您可以运行、进行日程安排和以电子邮件形式发送 PDF 格式的报告。您还可以将任意报告作为搜索来运行，然后使用搜索的结果，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，请参见 “《Sentinel 用户指南》”中的*报告*。

身份跟踪

Sentinel 为身份管理系统提供了集成框架，以便跟踪每个用户帐户的身份，以及这些身份已执行的事件。Sentinel 可提供用户信息，如联系人信息、用户帐户、最近的鉴定事件、最近的访问事件、权限更改等。通过显示启动特定操作的用户或受操作影响的用户相关信息，Sentinel 改进了事件响应时间并支持基于行为的分析。有关详细信息，请参见 “《Sentinel 用户指南》”中的*利用身份信息*。

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。Sentinel 优化了系统，对任何类型的分析均可实现最高效率，并提供了从一种分析转换到另一种分析的方法以实现无缝转换。

在 Sentinel 中调查事件通常先从近乎实时的事件视图开始。尽管有更高级的工具可用，但事件视图可显示过滤事件流以及摘要图表，用于对事件趋势和事件数据进行简单、快速的分析，以及识别特定事件。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。您可以将事件视图用作仪表板，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。通过将在搜索界面中构建的交互式搜索传送到报告模板，Sentinel 使此转换变得更加容易。这可以立即创建显示相同数据的报告，但格式更适合于较大的事件量。

Sentinel 包含许多用于此用途的报告模板。报告模板有两种类型：

- 精确调整以显示特定类型的信息的模板，如鉴定数据或用户创建。
- 可通过交互式方式对报告中的组和列进行自定义的通用模板。

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 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，请参见 *《Sentinel 用户指南》*。

计划 Sentinel 安装

以下章节将指导您计划 Sentinel 安装。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 技术支持联系。

3 实现核对清单

使用以下核对清单计划、安装和配置 Sentinel。

如果从 Sentinel 先前版本升级，则不使用此核对清单。有关升级的信息，请参见第 V 部分 “升级 Sentinel” （第 135 页）。

❒	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 许可信息，以确定是需要使用 Sentinel 的评估许可证还是需要使用 Sentinel 的企业许可证。	第 4 章“了解许可证信息”（第 33 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 37 页）。
❒	根据每秒事件数 (EPS) 确定适合环境的部署类型。 确定为改善性能和负载平衡所需要安装的 Collector Manager 和 Correlation Engine 数量。	第 6 章“部署考虑事项”（第 39 页）.
❒	复查最新的 Sentinel 发行说明以了解新功能和已知问题。	Sentinel 发行说明
❒	安装 Sentinel。	第 III 部分 “安装 Sentinel” （第 67 页）。
❒	配置 Sentinel。	第 IV 部分 “配置 Sentinel” （第 107 页）.
❒	Sentinel 包括即用型关联规则。默认情况下，一些关联规则配置为在触发规则时执行发送电子邮件的操作，如“通知安全管理员”操作。因此，您必须通过配置 SMTP 集成器和“发送电子邮件”操作来配置 Sentinel 服务器的邮件服务器设置。	Sentinel 插件网站中的 SMTP 集成器和发送电子邮件操作文档。
❒	根据需要在您的环境中安装附加收集器和连接器。	第 16 章“安装附加的收集器和连接器”（第 103 页）。
❒	根据需要在您的环境中安装附加的 Collector Manager 和 Correlation Engine。	第 III 部分 “安装 Sentinel” （第 67 页）。

4 了解许可证信息

Sentinel 包括各式功能，可满足许多客户的各种需求。您可以根据需要选择相应的许可模型。

Sentinel 平台提供以下两种许可模型：

- **Sentinel Enterprise：** 该解决方案功能齐全，能够启用所有核心的实时可视化分析功能和许多附加功能。Sentinel Enterprise 专注于 SIEM 用例，如实时威胁检测、警报和修正。
- **Sentinel for Log Management：** 该解决方案适用于日志管理用例，能够收集、存储、搜索和报告数据等。

  Sentinel for Log Management 展现了 Sentinel Log Manager 1.2.2 中所提供功能的重大升级，并且在某些情况下，更改了该结构的重要部分。要计划升级到 Sentinel for Log Management，请参见 Sentinel 常见问题页面。

根据您购买的解决方案和外接式附件，您可以购买相应的许可证密钥和权利，以启用 Sentinel 中的权限功能。尽管许可证密钥和权限可管理产品功能和下载的基本访问权限，但您应查看购买协议和最终用户许可证协议了解附加的条款与条件。

下表概括了各解决方案中提供的特定服务和功能：

表 4-1 *Sentinel 服务和功能*

服务和功能	**Sentinel Enterprise**	**Sentinel for Log Management**
核心功能 ◆ 事件收集、分析、规范化和分类 ◆ 非事件数据收集（资产数据、漏洞数据和用户身份数据） ◆ 行内前后关系映射 ◆ 使用保留策略的事件储存，确保无否决 ◆ 目标为传统储存（内外部）的事件路由 ◆ 事件搜索和可视化 ◆ IP 流集合、储存和可视化 ◆ 报告 ◆ 联邦信息处理标准刊物 140-2 (FIPS 140-2) 支持 ◆ 手动触发的操作 ◆ 手动事件创建和管理	是	是
Sentinel 链接	是	是
数据同步	是	是
恢复存档的事件数据	是	是
数据联合（分布式搜索）	是	是

服务和功能	Sentinel Enterprise	Sentinel for Log Management
攻击检测 (Advisor)*	是	是
可缩放储存	是	是
关联	是	否
◆ 实时事件模式关联 ◆ 由关联规则触发的操作 ◆ 警报分类 ◆ 警报可视化		
安全智能	是	否
◆ 异常规则 ◆ 实时统计分析		

*Advisor 由 Security Nexus 提供支持，是一项附加服务。必须购买额外的许可证才能使用此服务。

Sentinel 许可证

本节提供有关 Sentinel 许可证类型的信息。

- 评估许可证（第 34 页）
- 免费许可证（第 35 页）
- 企业许可证（第 35 页）

评估许可证

默认评估许可证允许您在特定的评估期内，通过受硬件容量制约的不限 EPS 使用 Sentinel Enterprise 的所有功能。有关 Sentinel Enterprise 中所提供的功能的信息，请参见 表 4-1“Sentinel 服务和功能”（第 33 页）。

系统的失效日期基于系统中的最早数据。如果您将旧的事件恢复到系统，Sentinel 会相应地更新失效日期。

在评估许可证失效后，Sentinel 可以使用基本的免费许可证运行，但该许可证功能有限，事件率仅限 25 EPS。仅当 Sentinel 配置有传统储存时，这种方式才适用。

在可缩放储存部署中，当评估许可证失效后，Sentinel 就不再储存事件和原始数据。

在升级到企业许可证后，Sentinel 恢复所有功能。为了避免任何功能中断，必须在评估许可证失效之前使用企业许可证升级系统。

免费许可证

免费许可证允许您使用一组带有25EPS有限事件率的有限功能。免费许可证仅适用于带有传统储存的Sentinel。

免费许可证允许您收集和储存事件。当 EPS 率超过 25 时，Sentinel 储存接收到的事件，但并不在搜索结果或报告中显示这些事件的细节。Sentinel 使用 OverEPSLimit 标记来标记这些事件。

免费许可证不提供实时功能。可以通过将许可证升级到企业许可证来恢复所有功能。

注释： Sentinel 免费版本不提供技术支持和产品更新。

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。根据您购买的许可证，许可证密钥会启用某些功能、数据收集率和事件源。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。

若要更改许可证，请联系您的帐户管理员。

您可以在安装过程中或其后的任何时间添加企业许可证密钥。若要添加许可证密钥，请参见“《Sentinel 管理指南》”中的*添加许可证密钥*。

5 满足系统要求

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

有关推荐的硬件、支持的操作系统、设备平台和浏览器的信息，请参见 Sentinel 技术信息网站。

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。请参见 Sentinel 插件网站上的连接器和收集器文档。

虚拟环境

VMwareESX服务器支持Sentinel。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测试结果相同的性能结果，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。

有关建议的物理计算机相关信息，请参见 Sentinel 技术信息网站。

6 部署考虑事项

Sentinel 具有可缩放的体系结构，该体系结构可以扩展，以便处理您需要放在 Sentinel 上的负载。本章概述了在缩放 Sentinel 部署时要考虑的最重要的事项。 技术支持或 合作伙伴服务专家可以与您一起设计适用于您 IT 环境的 Sentinel 系统。

数据储存考虑事项

根据 EPS 大小，您可以选择使用传统储存或可缩放储存来储存 Sentinel 数据并为其编制索引。您的 Sentinel 部署取决于您选择使用的数据储存选项。

表 6-1 传统储存与可缩放储存之间的比较

传统储存	可缩放储存
默认情况下，数据储存在基于文件的传统储存中，索引在 Sentinel 服务器上本地完成。 除基于文件的数据储存外，您还可以选择在“可视化数据储存”中储存和索引事件，以利用数据可视化功能。有关详细信息，请参见配置“可视化数据储存”（第 42 页）。	数据储存在基于 Hadoop 的可缩放储存中，并使用可缩放分布式索引机制为数据编制索引。
最高可无缝垂直扩展到约 20000 EPS。如有更高需求，您必须添加额外的 Sentinel 服务器才能让 EPS 实现更大幅度的提升。	无缝水平扩展到非常大的 EPS，例如每秒 100 万个事件。
数据收集在多个 Sentinel 服务器之间进行负载平衡。因此，数据分布在不同的 Sentinel 服务器上，应进行单独的管理。	数据收集由单个 Sentinel 服务器管理。因此，在单个 Sentinel 服务器上集中进行数据管理和资源管理。
数据在磁盘上按租户标记，而非按租户隔离。	数据在磁盘上按租户标记并隔离。
必须通过手动方式或使用SAN磁盘等成本高昂的储存机制复制和提供数据。	由于 Hadoop 在商用硬件上运行，因此，可以经济有效地复制和提供数据。

- 针对传统储存进行规划（第 40 页）
- 针对可缩放储存进行规划（第 43 页）
- Sentinel 目录结构（第 45 页）

针对传统储存进行规划

基于文件的数据储存具有三层结构：

联机储存	主储存，以前称为本地储存。	经过优化，可实现快速写入和检索。存储最新收集的事件数据和最常搜索的事件数据。
	辅助储存，以前称为网络储存。（可选）	已进行了优化，以便减少价格更低的可选储存上的空间用量，同时仍然支持快速检索。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，不管它们是位于主储存、辅助储存还是两者。	
脱机储存	存档储存	关闭分区时，可以将分区备份到任何文件存储服务（如AmazonGlacier）。您可以临时重新导入分区，以在需要时随时用于长期法证分析。

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，请参阅“《 Sentinel 管理指南》”中的*配置数据同步*。

安装 Sentinel 时，您必须将主储存的磁盘分区装入将安装 Sentinel 的位置，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 Sentinel 目录结构（第 45 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。单独储存可变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。

注释： 在 ext3 文件系统中文件存储有限制，即目录的文件或子目录不得超过 32000 个。如果将有大量保留策略或您要更长久地保留数据（例如一年），可以使用 XFS 文件系统。

- 在传统安装中使用分区（第 41 页）
- 在设备安装中使用分区（第 41 页）
- 分区布局的最佳实践（第 42 页）
- 配置“可视化数据储存”（第 42 页）

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 Sentinel 目录结构（第 45 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目录上。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）。

在设备安装中使用分区

如果您正在使用 DVD ISO 设备格式，您可以按照 YaST 屏幕上的说明在安装时配置设备文件系统的分区。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，请参见为传统储存创建分区（第 100 页）。

分区布局的最佳实践

对于任何已安装的系统，许多组织都有自己记录的最佳实践分区布局方案。以下分区建议旨在为未定义任何策略的组织提供指导，并考虑到特定于 Sentinel 的文件系统用法。通常，Sentinel 遵循文件系统层次结构标准（如果可行）。

分区	安装点	大小	注释
Root	/	100 GB	包含操作系统文件和 Sentinel 二进制文件/配置。
引导	/boot	150 MB	引导分区
主储存	/var/opt/novell/sentinel	使用系统大小信息进行计算。	此区域将包含 Sentinel 收集的主要数据，再加上其他变量数据，例如日志文件。可以与其他系统共享此分区。
辅助储存	基于储存类型（NFS、CIFS 或 SAN）的位置。	使用系统大小信息进行计算。	这是辅助储存区域，可按此处所示在本地装入，也可以远程装入。
存档储存	远程系统	使用系统大小信息进行计算。	此储存用于存档的数据。

配置“可视化数据储存”

Sentinel 提供以图表、表格和地图形式显示数据的事件可视化。这些可视化将使得可视化和分析大量事件变得更加轻松。您也可以创建自己的可视化和仪表板。

Sentinel 利用了基于浏览器的分析和搜索仪表板 Kibana，可以帮助您搜索和可视化事件。Kibana 访问可视化数据储存 (Elasticsearch) 中的数据，以在仪表板中显示事件。默认情况下，Sentinel 包含一个仅储存和索引警报的节点。必须启用事件可视化，才能在 Elasticsearch 中存储和索引事件。

启用 Elasticsearch 储存数据和建立数据索引时，Sentinel 仅索引可视化所需的一些特定事件字段，并将索引字段储存在 Elasticsearch 中。Sentinel 会为每一天创建专用索引，并使用 UTC 时区（午夜-午夜）计算索引日期。索引名称采用 security.events.normalized_yyyyMMdd 格式。例如，索引 security.events.normalized_20160101 中包含事件时间是 2016 年 1 月 1 日的所有事件。

配置可视化数据储存包含下列内容：

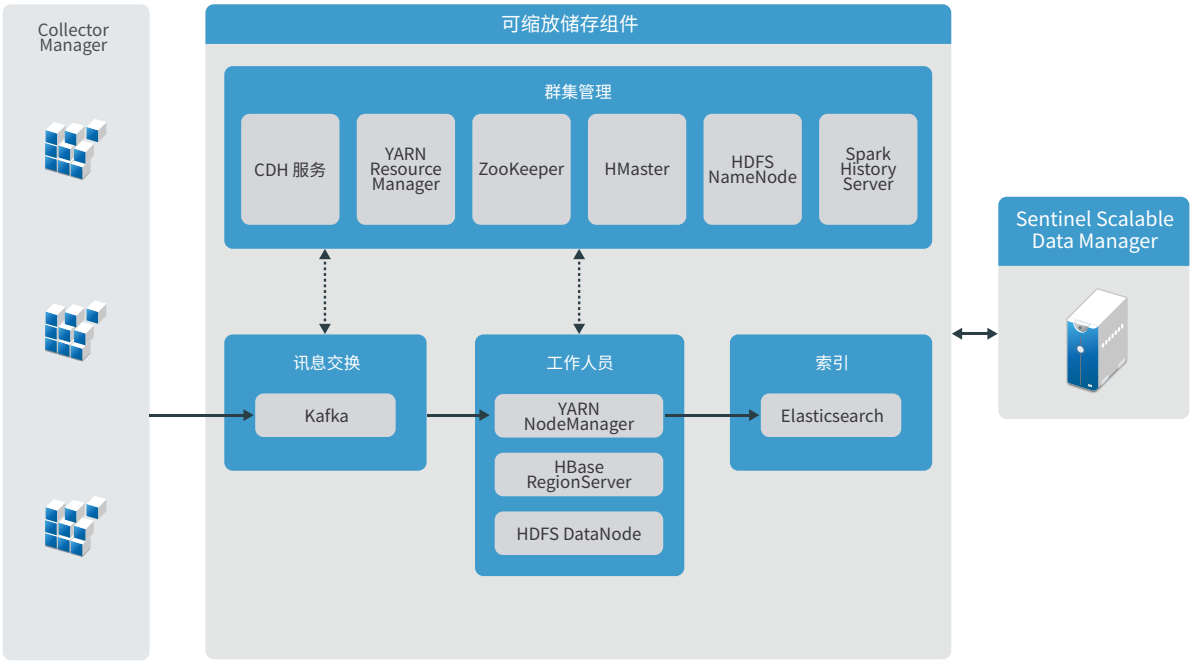
- **在群集模式中安装 Elasticsearch 节点：** 默认情况下，Sentinel 包含一个 Elasticsearch 节点。为了使 Sentinel 服务器保持最佳性能和稳定性，您必须在群集模式下安装其他 Elasticsearch 节点。有关详细信息，请参见第 12 章“安装和配置 Elasticsearch”（第 73 页）。
- **启用事件可视化：** 默认情况下，事件可视化为禁用状态。要启用事件可视化，请参见第 20 章“启用事件可视化”（第 115 页）。
- **性能优化：** Sentinel 自动配置特定 Elasticsearch 设置以实现最优性能。您可以根据需要自定义这些设置。例如，您可以修改希望 Elasticsearch 索引的事件字段。有关详细信息，请参见Elasticsearch 性能优化（第 78 页）。

针对可缩放储存进行规划

Sentinel 使用 Cloudera's Distribution Including Apache Hadoop (CDH) 框架储存和管理大型数据。对于索引事件，Sentinel 使用 Elastic 的可缩放分布式索引引擎，即 Elasticsearch。

下图说明了可缩放储存中使用的各种组件：

图 6-1 可缩放储存体系结构



- **讯息交换：** Sentinel 将使用 Apache Kafka 作为可缩放的讯息交换系统，用于从 Collector Manager 接收规范化事件和原始数据。Collector Manager 会将原始数据和事件数据发送到 Kafka 群集。

  默认情况下，Sentinel 会创建以下 Kafka 主题：

  - **security.events.normalized：** 储存所有已处理的事件数据和规范化的事件数据，包括系统生成的事件和内部事件。
  - **security.events.raw：** 储存来自事件源的所有原始数据。

  事件和原始数据采用 Apache Avro 架构。有关详细信息，请参见 Apache Avro 文档。架构文件位于 /etc/opt/novell/sentinel/scalablestore 目录中。

- **工作人员：** 此节点托管实时处理和储存作业。ApacheSpark可实时处理大规模数据，例如根据租户 ID 隔离事件、请求大量数据、将数据储存到记录系统 (SOR)，以及实现可缩放索引。

  Apache HBase 是基于 Hadoop 的可缩放分布式数据储存。它可以用作规范化事件和原始数据的 SOR，并按照租户 ID 进行隔离。

  根据租户 ID，Sentinel 会为每个租户创建单独的名称空间。例如，默认租户的名称空间是 1。在每个名称空间下，Sentinel 都会创建下述表，并根据事件时间储存数据。

  - ***<tenant_ID>*:security.events.normalized:** 储存所有已处理的事件数据和规范化的事件数据，包括系统生成的事件和内部事件。
  - ***<tenant_ID>*:security.events.raw:** 储存来自事件源的所有原始数据。

- **群集管理：** 此节点托管所有主服务和群集管理服务。ApacheZooKeeper可充当集中式服务，用于维护配置信息、为服务命名、提供分布式同步，以及提供组服务。
- **索引：** Sentinel 会使用 Elasticsearch 作为可缩放的分布式索引引擎，以便索引事件。您可以从用于事件搜索和可视化的 Elasticsearch 访问数据。

  Sentinel 会为每一天创建专用索引，并使用 UTC 时区（午夜-午夜）计算索引日期。索引名称采用 security.events.normalized_yyyyMMdd 格式。例如，索引 security.events.normalized_20160101 中包含事件时间是 2016 年 1 月 1 日的所有事件。为了实现最佳性能，Sentinel 仅为某些特定事件字段编制索引。您可以修改希望 Elasticsearch 为其编制索引的事件字段。有关详细信息，请参见Elasticsearch 性能优化（第 78 页）。

可缩放储存配置

启用可缩放储存之后，Sentinel 服务器用户界面会精简，以便只管理某些 Sentinel 功能，如数据集合、关联、事件路由选择、搜索和可视化事件，以及执行特定管理活动。此精简版的 Sentinel 称为 Sentinel Scalable Data Manager (SSDM)。对于其他 Sentinel 功能，例如安全智能，以及传统的搜索和报告，您必须安装带有传统储存的 Sentinel 独立实例，并使用 Sentinel Link 将特定事件数据从 SSDM 路由到 Sentinel。

以下列表提供 SSDM 中不可用的服务和功能的信息：

- 报告
- 安全智能
- 搜索期间执行事件操作
- 测试关联规则
- 事件创建和管理
- 手动对事件执行操作
- 数据同步
- iTRAC 工作流程
- 对触发关联事件的事件进行辩证分析
- 查看安全配置管理器和 Change Guardian 事件的事件附件。

启用可缩放储存是一次性配置，无法还原。如果您想要禁用可缩放储存并切换到传统储存，您必须重新安装 Sentinel。

以下核对清单概述了配置可缩放储存时需要执行的任务：

表 6-2 可缩放储存配置核对清单

	任务	参见
❒	查看部署信息，了解需要如何部署带有可缩放储存的 Sentinel。	使用可缩放储存进行三层部署（第 50 页）
❒	查看先决条件，并完成所有必需的任务。	第 13 章“安装和设置可缩放储存”（第 81 页）。
❒	启用可缩放储存。 您可以在安装期间或安装后启用可缩放储存。 在升级安装版中，只有升级 Sentinel 之后，方能启用可缩放储存。	要在安装期间启用可缩放储存，请对 Sentinel 执行自定义安装。请参见Sentinel 服务器自定义安装（第 86 页）。 要在安装或升级后启用可缩放储存，请参阅《*Sentinel 管理指南*》中的安装后启用可缩放储存。
❒	使用 Sentinel 配置 CDH 组件和 Elasticsearch。	《Sentinel 管理指南》中的*配置可缩放储存*。

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。
- 可执行文件和库存储在 /opt/novell/sentinel 目录中。
- 日志文件位于目录 /var/opt/novell/sentinel/log 中。
- 临时文件位于 /var/opt/novell/sentinel/tmp 目录中。
- 配置文件位于目录 /etc/opt/novell/sentinel 中。
- 进程 ID (PID) 文件位于 /home/novell/sentinel/server.pid 目录中。

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

分布式部署的优势

默认情况下，Sentinel 服务器包括以下组件：

- **Collector Manager：** Collector Manager 为 Sentinel 提供了一个灵活的数据收集点。
- **Correlation Engine：** Correlation Engine 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。
- **Elasticsearch：** 一个储存数据和建立数据索引的可选数据储存组件。默认情况下，Sentinel 包含一个 Elasticsearch 节点。如果预计 EPS 较大，超过 2500，则必须在群集中部署其他 Elasticsearch 节点。

重要： 在生产环境中，您应设置一个分布式部署，因为它可以将数据收集组件隔离到独立的计算机上，这对以最佳系统稳定性处理峰值和其他异常情况很重要。

本节描述了分布式部署的优势。

- 附加 Collector Manager 的优势（第 46 页）
- 附加 Correlation Engine 的优势（第 46 页）

附加 Collector Manager 的优势

默认情况下，Sentinel 服务器包含有一个 Collector Manager。然而，对于生产环境，当收到大量数据时，分布式 Collector Manager 可以提供更好的隔离。在这种情况下，分布式 Collector Manager 可能变得过载，但是 Sentinel 服务器仍将保持对用户请求的响应。

在一个分布式网络中安装多个 Collector Manager 可提供下列优势：

- **改进系统性能：** 附加的 Collector Manager 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 Collector Manager 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 Collector Manager 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。

可以在网络中的适当位置安装附加的 Collector Manager。这些远程 Collector Manager 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 Collector Manager 的信息，请参见第 III 部分 “安装 Sentinel” （第 67 页）。

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

附加 Correlation Engine 的优势

您可以部署多个 Correlation Engine（每个 Correlation Engine 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 Correlation Engine 并将某些规则重新部署到新的 Correlation Engine 可能很有利。多个 Correlation Engine 可以提供随着 Sentinel 系统整合其他数据源或事件率提高而伸缩的功能。有关安装附加 Correlation Engine 的信息，请参见第 III 部分 “安装 Sentinel” （第 67 页）。

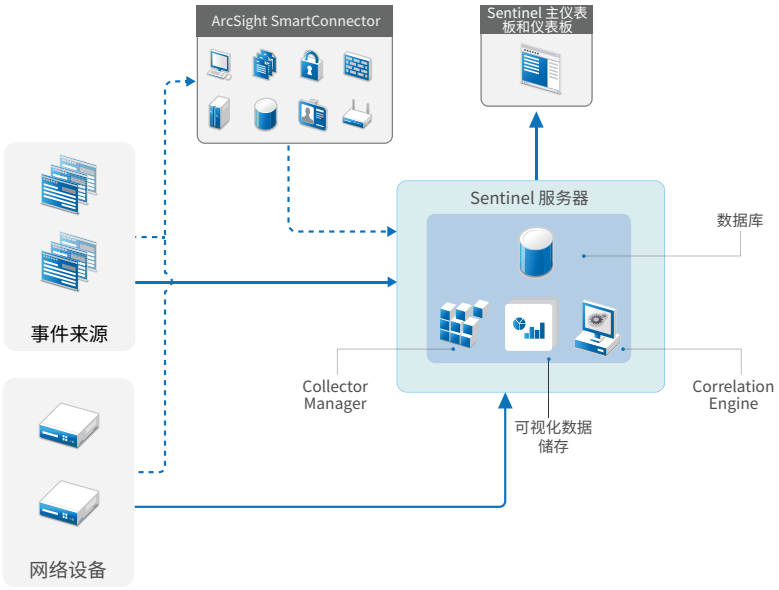
注释： 一个系统上不能安装多个 Correlation Engine。您可以在远程系统上安装附加的 Correlation Engine，然后将它们连接到 Sentinel 服务器。

一体机部署

最基本的部署选项是在单台计算机上包含 Sentinel 的所有组件的一体机系统。仅当您将相对较小的负载放置在系统上并且不需要监视 Windows 计算机时，一体机部署才适用。在许多环境中，不可预测且波动的负载以及不同组件之间的资源冲突可能会导致性能问题。

重要： 对于生产环境，您应设置一个分布式部署，因为它可以将数据收集组件隔离到独立的计算机上，这对以最佳系统稳定性处理峰值和其他异常情况很重要。

图 6-2 一体机部署

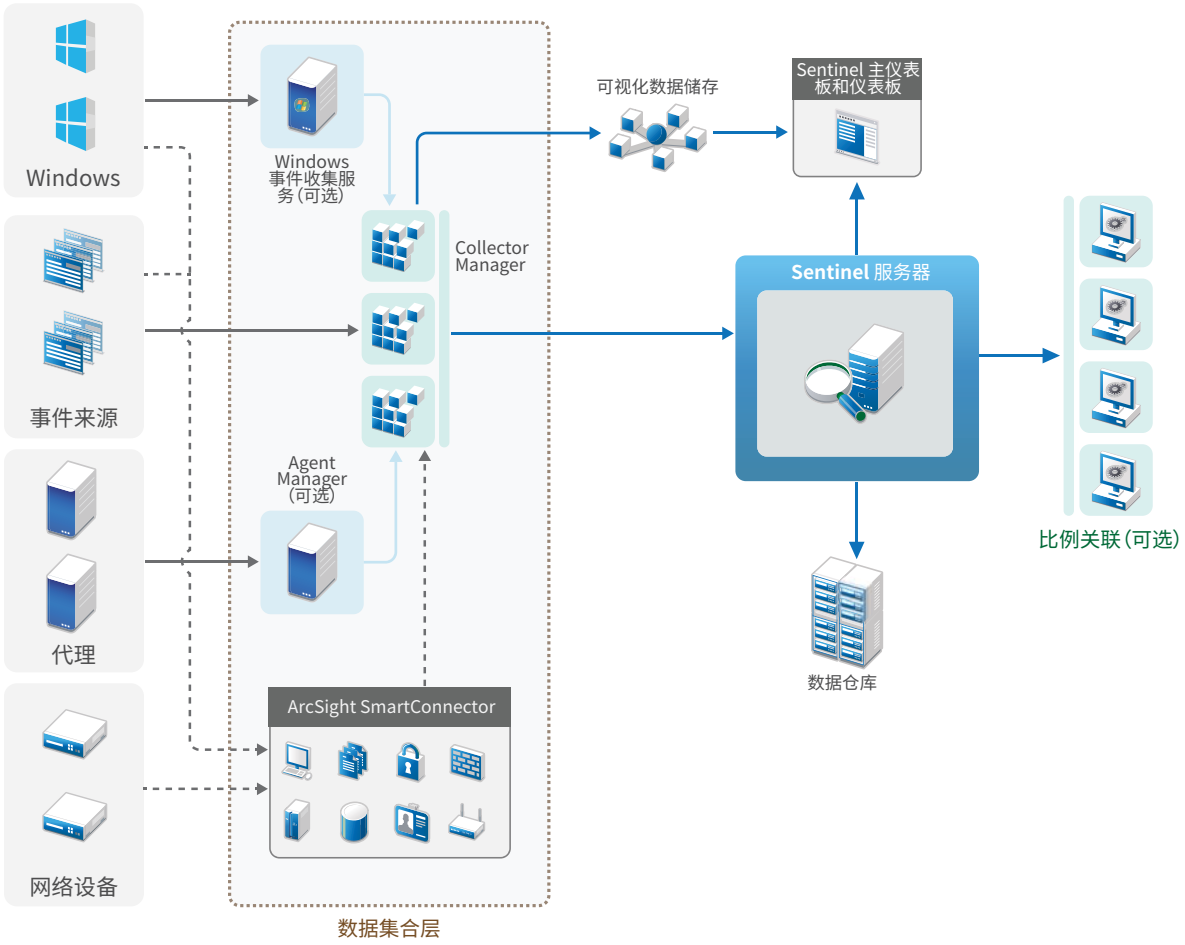


一层分布式部署

一层部署增加了监视 Windows 计算机以及处理比一体机部署更大的负载的功能。您可以通过添加 Collector Manager 和 Correlation Engine 计算机来从中央 Sentinel 服务器卸载处理，从而横向扩展数据收集和关联。除了处理事件和相关规则的负载外，远程收集器管理器和关联引擎还会释放中心 Sentinel 服务器上的资源，以便为其他请求（如事件储存和搜索）提供服务。随着系统上的负载越来越大，中心 Sentinel 服务器将最终出现瓶颈，您将需要一个包含更多层的部署，以便进一步向外扩展。

（可选）您可以将 Sentinel 配置为将事件数据复制到数据仓库中，这对于将自定义报告、分析和其他处理转移到其他系统会很有用。

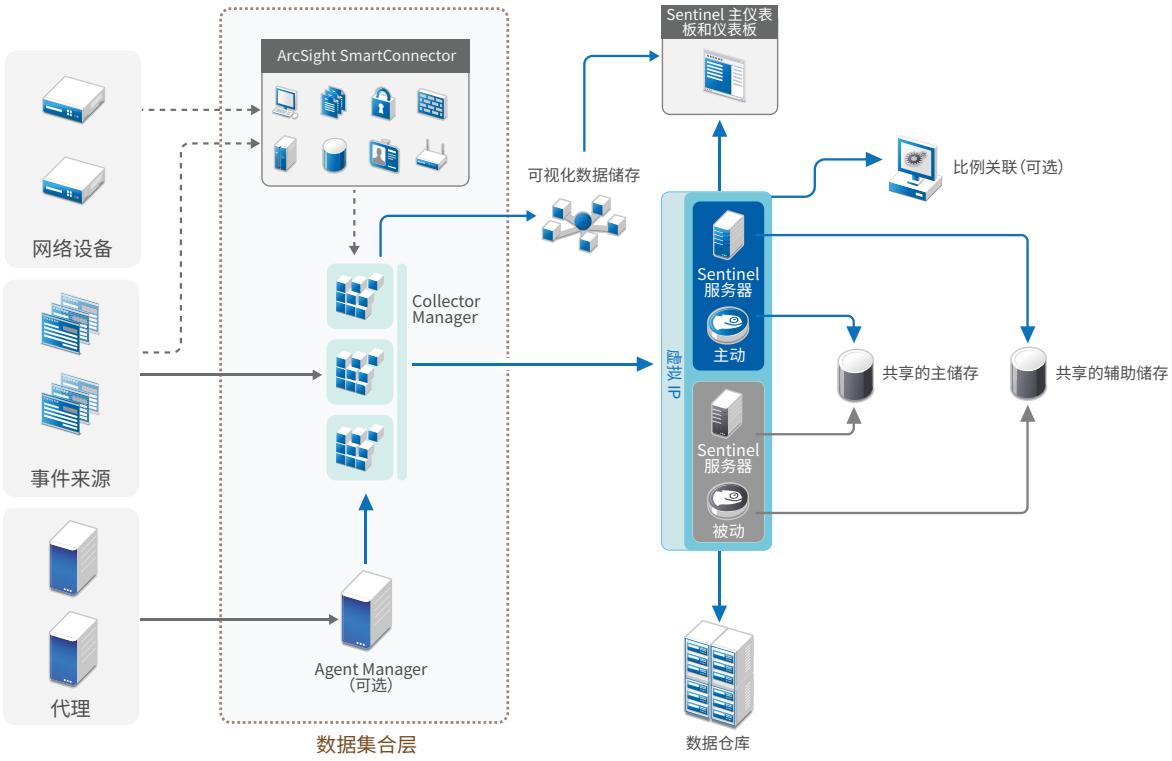
图 6-3 一层分布式部署



具有高可用性的一层分布式部署

一层分布式部署显示它如何能够转变成具有故障转移冗余性的高可用系统。有关部署 Sentinel 为高可用性模式的详细信息，请参见第 VII 部分 “部署 Sentinel 实现高可用性” （第 171 页）。

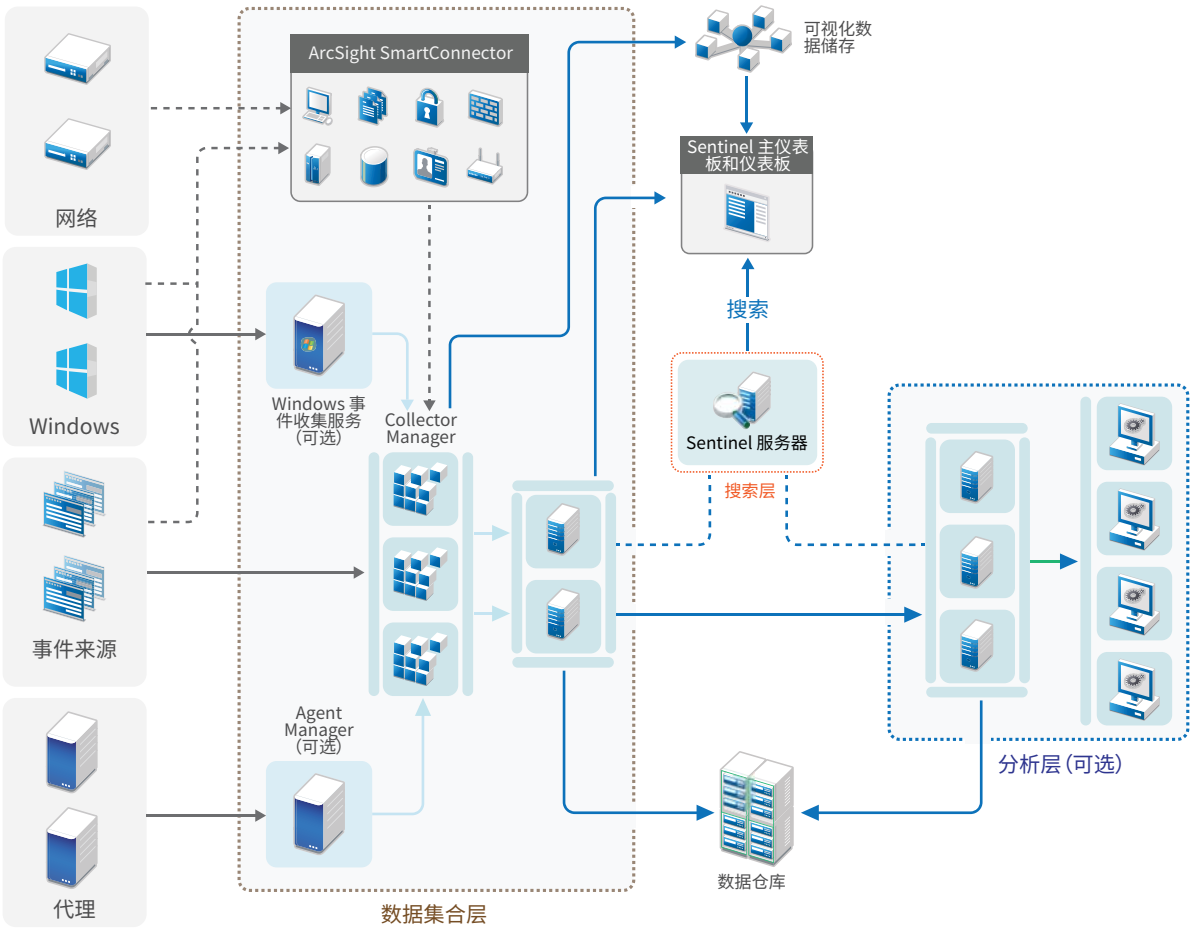
图 6-4 具有高可用性的一层分布式部署



两层和三层分布式部署

使用这些部署，可以通过利用 Sentinel Link 和 Sentinel 数据联合功能来超越单个中心 Sentinel 服务器的负载处理能力，并在多个 Sentinel 实例之间共享处理负载。数据收集在多个 Sentinel 服务器之间进行负载平衡，每个服务器都有多个 Collector Manager，如数据收集层中所示。如果要执行事件关联或安全智能功能，您可以选择使用 Sentinel Link 将数据向上转发到分析层。搜索层提供方便的单一接入点，以便使用 Sentinel 数据联合在其他所有层上的所有系统中进行搜索。由于搜索请求是在 Sentinel 的多个实例上联合处理的，因此该部署还具有在执行缩放以处理较大搜索负载时很有用的搜索负载平衡属性。

图 6-5 两层和三层分布式部署



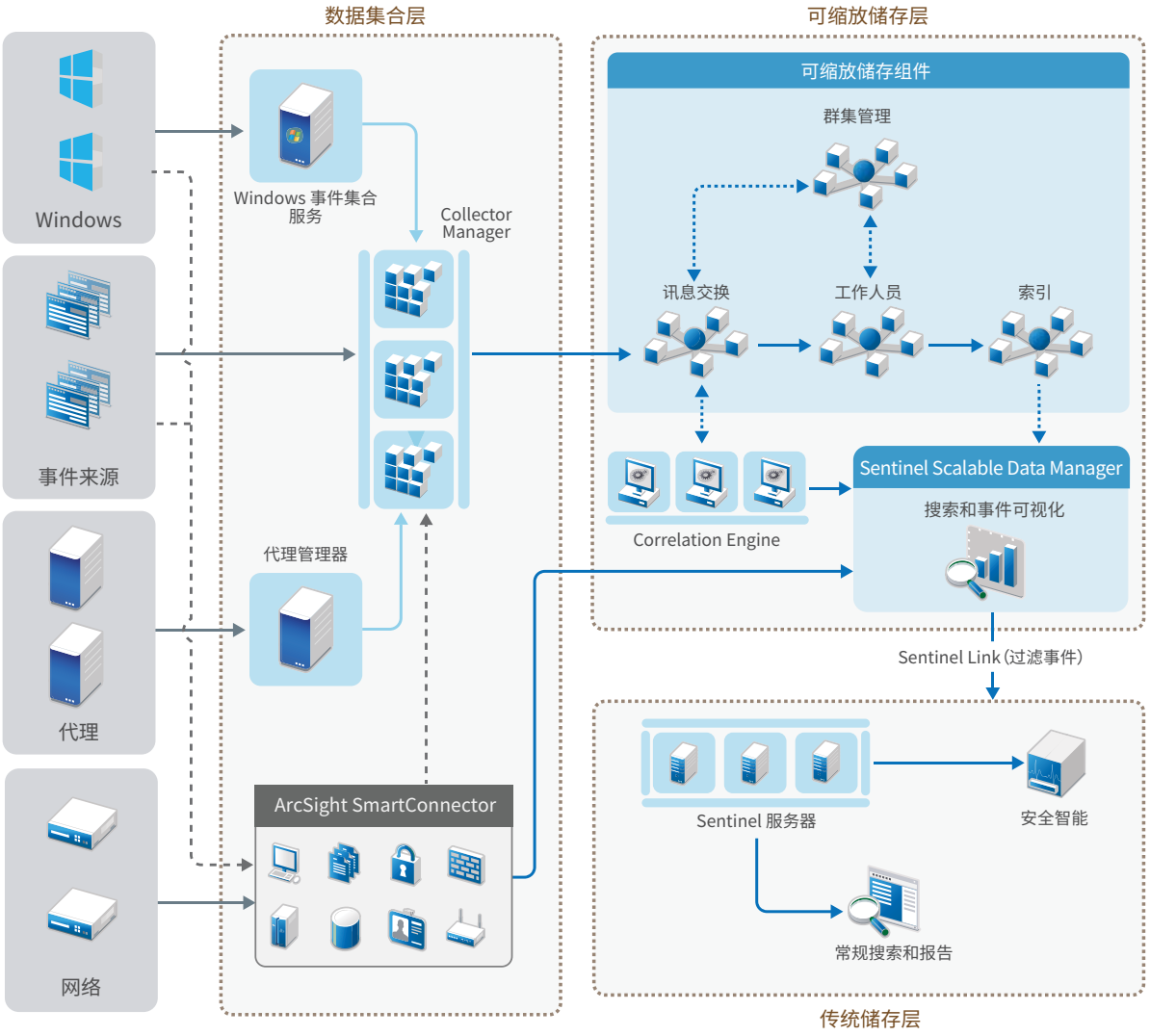
使用可缩放储存进行三层部署

若要满足大规模数据储存和数据处理需求，但又不希望将事件分布在多个 Sentinel 服务器上并在多个实例之间复制配置设置，则可使用可缩放储存设置三层分布式部署。在此部署中，您可以使用带有可缩放储存的单个 Sentinel 服务器而非多个 Sentinel 服务器储存和管理大量数据。

您可以设置带可缩放储存的 Sentinel 服务器或升级现有 Sentinel 服务器以启用可缩放储存。

根据您要使用的 Sentinel 功能，您可以确定如何对您的 Sentinel 部署进行设置。

图 6-6 针对可缩放储存的三层部署



此部署包括以下几层：

- **数据收集层：** 用于从各种事件源收集事件。或者，如果想要在具有传统储存的 Sentinel 中保留现有数据集合设置并且能同时利用可缩放储存功能，可以使用 data_uploader.sh 脚本将所需事件直接从传统储存转发到可缩放储存。有关详细信息，请参见第 32 章“将数据迁移至可缩放储存”（第 163 页）。
- **可缩放储存层：** 用于储存、索引和分析大型数据。您可以使用这层的 SSDM 服务器管理数据集合和数据关联，并提供其他 SSDM 功能。要使用 SSDM 中没有的 Sentinel 功能，您可以设置传统储存层。您还可以将收集的数据转发到任何其他 SIEM 系统或启用其他商业智能工具查询数据，或使用广泛支持的 Hadoop、Kafka、Spark 和 Elasticsearch API 在 Hadoop 分发包上直接进行分析。

- **传统储存层：** 要获得某些 Sentinel 功能，如安全智能、传统搜索以及报告，您必须安装带有传统储存的 Sentinel 的独立实例。您可以配置事件路由规则，以使用 Sentinel Link 将需要的事件从 SSDM 转发到 Sentienl。

  您也可以使用传统储存层中的任一 Sentinel 服务器执行搜索和报告操作。您还可选择设置独立的搜索层，可以提供方便的单一接入点，以便跨传统储存层中所有 Sentinel 服务器搜索和报告。要在可缩放储存中搜索事件，请使用 SSDM 中的搜索选项。

有关安装和设置可缩放储存的详细信息，请参见第 13 章“安装和设置可缩放储存”（第 81 页）。

7 FIPS140-2 模式的部署考虑事项

您可以有选择地将 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，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 Sentinel 服务器、Sentinel 远程 Collector Manager、Sentinel 远程 Correlation Engine、Sentinel 主界面、Sentinel Control Center 和 Sentinel Advisor 服务之间的通讯将使用经过 FIPS 140-2 验证的加密法。

重要： Sentinel 仅支持 FIPS 模式。如果操作系统不是 FIPS 模式，则不支持 Sentinel。

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。

RHEL6.3及更高版本提供的NSS加密模块已经过FIPS140-2验证。SLES11中包括的NSS加密模块尚未经过FIPS140-2正式验证，但是SUSE模块正在接受FIPS140-2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 FIPS 140-2 认证的更多信息，请参见 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2711 和 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1837。

RHEL NSS 包

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

- nspr-*
- nss-sysinit-*
- nss-util-*
- nss-softokn-freebl-*
- nss-softokn-*
- nss-*
- nss-tools-*

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。

SLES NSS 包

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

- libfreebl3-*
- mozilla-nspr-*
- mozilla-nss-*
- mozilla-nss-tools-*

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。

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
  - 检查点 (LEA) 连接器 2011.1r2 和更高版本
  - Syslog 集成器 2011.1r1 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 125 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 130 页）。

- 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）。
- 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 插件的更多信息，请参见 Sentinel 插件网站。如果您要请求任何尚未更新的插件提供 FIPS 支持，请使用 Bugzilla 提交请求。

FIPS 模式影响的数据连接

如果 Sentinel 为 FIPS 140-2 模式，则无法加密连接到 Microsoft SQL Server。此原因将影响下列类型的 Sentinel 操作：

- 与 SQL Server 的数据同步策略
- 与 Agent Manager 数据库通信的 Sentinel 服务器
- 数据库连接器从 SQL Server 收集数据

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。	部署方案（第 55 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。	Sentinel 服务器自定义安装（第 86 页）。 执行无提示安装（第 90 页） 第 23 章“在现有的 Sentinel 安装中启用 FIPS 140-2 模式”（第 121 页）
将 Sentinel 插件配置为在 FIPS 140-2 模式下运行。	将 Sentinel 插件配置为在 FIPS 140-2 模式下运行（第 125 页）。
将证书导入 Sentinel FIPS 密钥存储区。	将证书导入 FIPS 密钥存储区数据库（第 131 页）

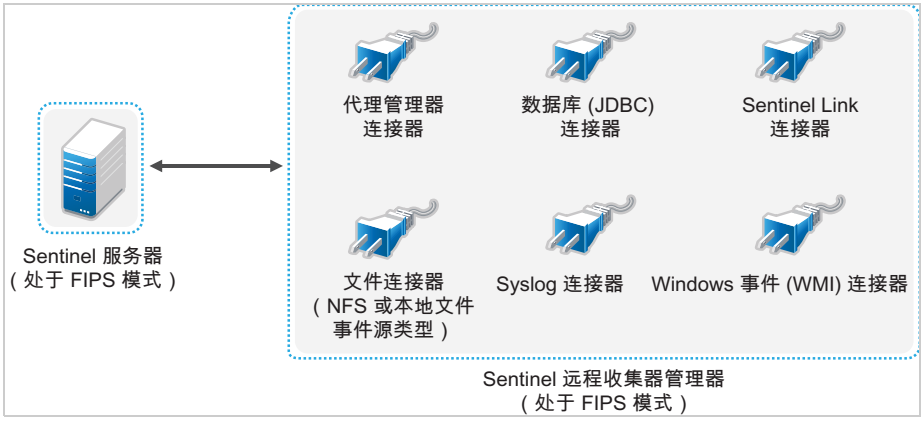
注释： 开始转换为 FIPS 模式前，备份 Sentinel 系统。如果稍后必须将服务器还原为非 FIPS 模式，则只有用于执行此操作的受支持的方法会从备份进行还原。有关还原为非 FIPS 模式的详细信息，请参见将 Sentinel 还原为非 FIPS 模式（第 131 页）。

部署方案

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

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 Collector Manager 收集数据。您可能拥有一个或多个远程 Collector Manager。



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 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 121 页）。

2 必须拥有一个以 FIPS 140-2 模式运行的 Sentinel 远程 Collector Manager。

注释： 如果（全新安装或升级的）远程 Collector Manager 是在非 FIPS 模式下运行的，则必须在该远程 Collector Manager 上启用 FIPS。有关详细信息，请参见在远程 Collector Manager 和 Correlation Engine 上启用 FIPS 140-2 模式（第 122 页）。

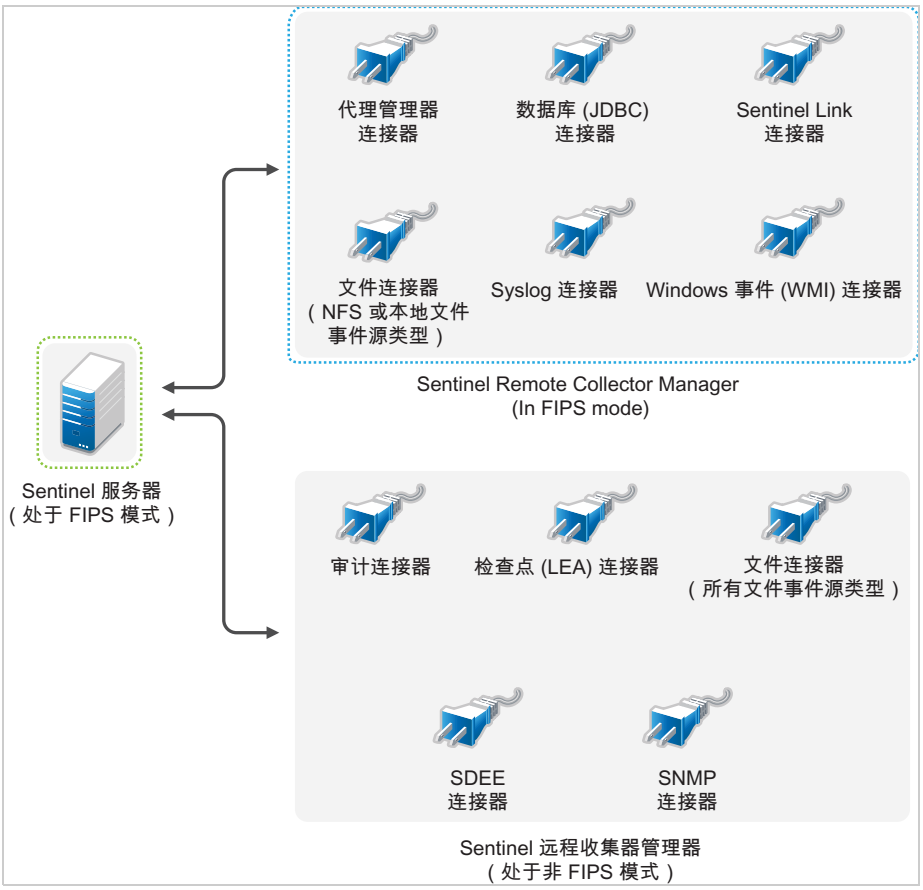
3 确保 FIPS 服务器和远程 Collector Manager 能够互相通讯。

4 将远程 Correlation Engine（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 Collector Manager 和 Correlation Engine 上启用 FIPS 140-2 模式（第 122 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 125 页）。

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。我们假设通过远程 Collector Manager 来收集数据。您可能拥有一个或多个远程 Collector Manager。



若要使用支持和不支持 FIPS 140-2 模式的连接器处理数据收集，您应有两个远程 Collector Manager：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 模式的连接器以及不支持 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 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 121 页）。

---

2 确保一个远程 Collector Manager 在 FIPS 140-2 模式下运行，而另一个远程 Collector Manager 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 Collector Manager，则必须在远程 Collector Manager 上启用 FIPS 模式。有关详细信息，请参见在远程 Collector Manager 和 Correlation Engine 上启用 FIPS 140-2 模式（第 122 页）。

2b 在非 FIPS 远程 Collector Manager 上更新服务器证书。有关详细信息，请参见在远程 Collector Manager 和 Correlation Engine 中更新服务器证书（第 125 页）。

3 确保两个远程 Collector Manager 能够与启用 FIPS 140-2 的 Sentinel 服务器进行通讯。

4 将远程 Correlation Engine（如果有）配置为在 FIPS 140-2 模式下运行。有关详细信息，请参见在远程 Collector Manager 和 Correlation Engine 上启用 FIPS 140-2 模式（第 122 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 125 页）。

5a 在以 FIPS 模式运行的远程 Collector Manager 中部署支持 FIPS 140-2 模式的连接器。

5b 在非 FIPS 远程 Collector Manager 中部署不支持 FIPS 140-2 模式的连接器。

8 使用的端口

Sentinel 使用各种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。

Sentinel 服务器端口

Sentinel 服务器使用以下端口进行内外部通讯。

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	描述
TCP 27017	用于安全智能配置数据库。
TCP 28017	用于安全智能数据库的 Web 控制台。
TCP 32000	用于封装程序进程和服务器进程之间的内部通讯。
TCP 9200	用于与使用 REST 的警报索引服务进行通讯。
TCP 9300	用于与使用其本机协议的警报索引服务进行通讯。

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	必需	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。

端口	方向	必需/可选	描述
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 Collector Manager 和 Correlation Engine 的传入连接。
TCP 10013	入站	必需	由 Sentinel Control Center 和 Solution Designer 使用。
TCP 1468	入站	可选	用于 syslog 讯息。
TCP 10014	入站	可选	远程 Collector Manager 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 Collector Manager 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 更新页面。
TCP 8443	出站	可选	如果使用数据联合，该端口将启动与其他 Sentinel 系统的连接，以执行分布式搜索。
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	如果辅助储存已配置为使用 NFS。
TCP 137、138、139、445	出站	可选	如果辅助储存已配置为使用 CIFS。
TCPJDBC（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。
TCP 9443	入站	可选	此端口允许 Sentinel 系统从其他 SIEM 软件（如 Change Guardian 和 Secure Configuration Manager）接收事件。

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。

端口	方向	必需/可选	描述
TCP 4984	入站	必需	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。
TCP 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 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。
TCP 7630	入站	必需	由 High Availability Web Konsole (Hawk) 使用。
TCP 9443	入站	必需	由 Sentinel 设备管理控制台使用。
TCP 1098 和 2000	入站	必需	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。

Collector Manager 端口

Collector Manager 使用以下端口与其他部件进行通讯。

网络端口

要使 Sentinel Collector Manager 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	必需	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。
TCP 8443	出站	必需	启动与 Sentinel Web 服务器端口的连接。 仅在安装和配置 Collector Manager 时，打开此端口。

Collector Manager 设备特定的端口

除了上述端口之外，还为 Sentinel Collector Manager 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 4984	入站	必需	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	配置数据收集服务器（如 syslog）时使用。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 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。
TCP 9443	入站	必需	由 Sentinel 设备管理控制台使用。
TCP 1098 和 2000	入站	必需	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。

Correlation Engine 端口

Correlation Engine 使用以下端口与其他部件进行通讯。

网络端口

要使 Sentinel Correlation Engine 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	必需	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。
TCP 8443	出站	必需	启动与 Sentinel Web 服务器端口的连接。 仅在安装和配置关联引擎时，打开此端口。

Correlation Engine 设备特定的端口

除了上述端口之外，Sentinel Correlation Engine 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 4984	入站	必需	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 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。
TCP 9443	入站	必需	由 Sentinel 设备管理控制台使用。
TCP 1098 和 2000	入站	必需	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。

可缩放储存端口

要让 SSDM 与 CDH 和 Elasticsearch 成功通讯，请确保除了 Cloudera 所需的端口和Sentinel 服务器端口部分所列的端口外，您在可缩放储存配置期间指定的端口在防火墙上也处于打开状态。

9 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。

传统安装

传统安装方法使用应用程序安装器在现有操作系统上安装 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。
使用默认的评估密钥进行安装。	允许使用默认的评估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。
使用传统储存来储存原始数据和事件。	允许您使用可缩放储存来储存原始数据和事件。
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，请参见执行交互式安装（第 85 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提示安装。有关无提示安装的详细信息，请参见执行无提示安装（第 90 页）。

设备安装

设备安装就是同时安装 SLES 12 SP3 64 位操作系统和 Sentinel。

Sentinel 设备采用以下格式：

- OVF 设备映像
- ISO 设备映像

有关设备安装的详细信息，请参见第 15 章“设备安装”（第 95 页）。

安装 Sentinel

本节将介绍如何安装 Sentinel 和附加的部件。

10 安装概述

默认的 Sentinel 安装将在 Sentinel 服务器中安装以下组件：

- **Sentinel 服务器和 Web 服务器进程：** 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）。

  使用 Sentinel Web 服务器可安全连接到 Sentinel 主仪表板界面。
- **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：** 储存安全智能和警报数据。
- **Elasticsearch：** 索引事件和警报以进行搜索和可视化。
- **Collector Manager：** Collector Manager 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 Collector Manager。
- **Elasticsearch：** 一个储存数据和建立数据索引的可选数据储存组件。默认情况下，Sentinel 包含一个 Elasticsearch 节点。如果预计 EPS 较大，超过 2500，则必须在群集中部署其他 Elasticsearch 节点。
- **Correlation Engine：** Correlation Engine 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“《 Sentinel 管理指南》”中的*检测漏洞和攻击*。
- **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

11 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 37 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 B“卸装”（第 209 页）。
- ❒ 如果您计划安装许可版本，请从 客户关怀中心获取许可证密钥。
- ❒ 确保第 8 章“使用的端口”（第 59 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。
- ❒ 如果您计划部署配置有可缩放储存的 Sentinel，请确保已安装 CDH 和 Elasticsearch。有关部署带有可缩放储存的 Sentinel 的详细信息，请参见安装和设置可缩放储存（第 81 页）。
- ❒ **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：**

  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

- **对于具有传统储存的 Sentinel：**

  要查看事件可视化，通过在 /etc/sysctl.conf 文件中添加属性 vm.max_map_count=262144 设置虚拟内存。

12 安装和配置 Elasticsearch

为了实现事件的可缩放分布式索引，您必须在群集模式下安装 Elasticsearch。为 Sentinel 安装的 Elasticsearch 群集只能用于为 Sentinel 数据编制索引。

先决条件

安装 Elasticsearch 前完成下列前提条件：

- 根据 EPS 率，在群集模式中部署 Elasticsearch，节点数量和副本数量按 Sentinel 技术信息页面中的建议设置。
- 通过在 /etc/security/limits.conf 文件中添加以下属性，设置文件描述符：

  elasticsearch hard nofile 65536

  elasticsearch soft nofile 65536

  elasticsearch soft as unlimited

注释： 满足上述前提条件之后，运行 sysctl -p 命令重新装载文件变更。

安装和配置 Elasticsearch

必须在 Elasticsearch 群集的每个节点上安装 Elasticsearch 和所需插件。

要安装和配置 Elasticsearch，请执行以下操作：

1. 安装 Elasticsearch 支持的 JDK 版本。
2. 下载 Elasticsearch RPM 已认证版本。有关 Elasticsearch 已认证版本和下载 URL 的信息，请参见 Sentinel 技术信息页面。
3. 安装 Elasticsearch：

   rpm -i elasticsearch-<*版本*>.rpm
4. 完成 RPM 安装后说明屏幕上提到的任务。
5. 确保 Elasticsearch 用户可访问 Java。
6. 通过更新或添加以下信息，配置 /etc/elasticsearch/elasticsearch.yml 文件：

属性和值	注释
cluster.name：<*Elasticsearch _cluster_name*>	对于所有节点，指定的群集名称必须相同。
node.name：<*node_name*>	对于每个节点，节点名称必须唯一。
network.host：_<*networkInterface*>:ipv4_	
discovery.zen.ping.unicast.hosts: [<Sentinel 服务器中 elasticsearch 节点的 FQDN>、<*elasticsearch 节点 1 的 FQDN*>、<*elasticsearch 节点 2 的 FQDN*> 等]	
thread_pool.bulk.queue_size: 300	
thread_pool.search.queue_size: 10000	搜索队列大小达到限制后，Elasticsearch 就会丢弃队列中所有未处理的搜索请求。 您可以根据以下公式增加搜索队列大小：calculation:threadpool.search.queue_size = 仪表板中每个用户的平均控件查询次数 x 分区数（每日索引）x 天数（搜索持续时间）
index.codec：best_compression	
path.data：["/<*es1*>", "/<*es2*>"]	让数据分布到多个独立磁盘或位置，以减少磁盘 I/O 延迟。 配置多个路径，用于储存 Elasticsearch 数据。例如 /es1、/es2，等等。 为了实现最佳性能和可管理性，请将每个路径都装入单独的物理磁盘 (JBOD)。

7 更新 /etc/elasticsearch/jvm.options 文件中默认的 Elasticsearch 堆大小。

堆大小必须是服务器内存的 50%。例如，在 24 GB 的 Elasticsearch 节点上，分配 12 GB 作为堆大小，以实现最佳性能。

8 在每个 Elasticsearch 群集节点上重复执行以上所有步骤。

9 在 Sentinel 服务器 Elasticsearch 节点中，按下列方式配置 /etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml：

9a 确保 elasticsearch.yml 文件中 cluster.name 和 discovery.zen.ping.unicast.hosts 的值与外部 Elasticsearch 节点中的 elasticsearch.yml 文件中的相同。

9b 在 network.host 属性中按下列形式指定本地主机 IP 地址后跟本地 Elasticsearch 节点的 IP 地址：

network.host: ["127.0.0.1","<*Sentinel 中 Elasticsearch 节点的 IP 地址*>"]

10 （有条件）对于具有传统储存的 Sentinel，将外部 Elasticsearch 节点 IP 地址添加到/etc/opt/novell/sentinel/config/elasticsearch-index.properties 文件的 ServerList 属性中。

例如：ServerList=<*Elasticsearch IP1*>:<*Port*>,<*Elasticsearch IP2*>:<*Port*>

11 重启动 Sentinel：

rcsentinel 重启动

12 重启动每个 Elasticsearch 节点：

/etc/init.d/elasticsearch start

13 为实现 Sentinel 服务器最优性能和稳定性，将 Sentinel 服务器中的 Elasticsearch 节点配置为专用 master-eligible 节点，这样将在外部 Elasticsearch 节点中索引所有事件可视化数据：

13a 以 novell 用户身份登录到 Sentinel 服务器。

13b 确保所有现有警报数据已移动到外部 Elasticsearch 节点。

13c 打开 /etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml 文件并添加下列信息：

```
node.master: true
node.data: false
node.ingest: false
search.remote.connect: false
```

13d 重启动 Elasticsearch：

rcsentinel stopSIdb

rcsentinel startSIdb

14 继续确保 Elasticsearch 中数据的安全（第 75 页）。

确保 Elasticsearch 中数据的安全

Elasticsearch 群集节点可由不同客户端访问，如：

- Sentinel：提取事件数据并在事件可视化仪表板中显示。
- 在 YARN NodeManager 节点运行的 Spark 作业：对从 Kafka 接收的事件执行批量索引。（针对 SSDM）
- Collector Manager：对具有传统储存的 Sentinel 中的事件执行批量索引。
- 其他外部客户端：执行自定义操作，例如自定义分析。

Sentinel 为 Elasticsearch 提供名为 **elasticsearch-security-plugin** 的安全插件，该插件可鉴定和授予对 Elasticsearch 的访问权限。

根据客户端的连接方式，插件使用 SAML 令牌或白名单进行验证：

- 当客户端与请求一同发送 SAML 令牌时，插件针对 Sentinel 鉴定服务器鉴定令牌。鉴定成功后，插件仅允许客户端访问其具备访问权限的的筛选事件。

  例如，事件可视化仪表板（客户端）仅显示来自 Elasticsearch、用户角色有权查看的那些事件。

  有关角色和权限的相关信息，请参见 *Sentinel 管理指南*中的“创建角色”。
- 客户端无法发送 SAML 令牌时，插件检查其合法客户端的白名单。验证成功后，插件允许访问所有事件，无需筛选。
- 客户端不发送有效 SAML 令牌或白名单不允许此客户端时，插件将其认定为非法客户端并拒绝对此客户端的访问。

此部分提供有关安装和配置 Elasticsearch 安全插件的信息：

- 安装 Elasticsearch 安全插件（第 76 页）
- 提供对其他 Elasticsearch 客户端的安全访问（第 77 页）
- 更新 Elasticsearch 插件配置（第 78 页）

安装 Elasticsearch 安全插件

必须在 Elasticsearch 群集的每个节点以及 Sentinel 中所包含的 Elasticsearch 节点中安装 Elasticsearch 安全插件。

要在 Sentinel 中所包含的 Elasticsearch 节点上安装 Elasticsearch 安全插件：

1. 登录 Sentinel 主仪表板或 SSDM 服务器。
2. 按下列方式设置 JAVA_HOME 环境变量路径：

   ```
   export JAVA_HOME=/<Sentinel_installation_path>/opt/novell/sentinel/jdk/
   ```

3. 安装插件：

   在 Linux 中，以运行 Elasticsearch 的用户身份登录，并运行下列命令：

   ```
   <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/
   elasticsearch-plugin install file://localhost/<Sentinel_installation_path>/
   etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip --
   verbose
   ```

   提示继续安装时，输入 y。

4. （有条件）如果 Elasticsearch 不在侦听默认 HTTP 端口 (9200)，则必须在 <Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt 文件中的每个条目中更新 Elasticsearch 端口号。

   有关详细信息，请参见通过使用白名单提供对 Elasticsearch 客户端的访问权限（第 77 页）。

5. 使用下列命令在 Sentinel 中重启动索引服务：

   ```
   rcsentinel stopSIdb
   rcsentinel startSIdb
   ```

要在外部 Elasticsearch 节点安装 Elasticsearch 安全插件：

在 Elasticsearch 群集的每个节点执行下列步骤：

1. 登录 Sentinel 主仪表板或 SSDM 服务器。
2. 将 <Sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip 文件复制到 Elasticsearch 群集每个节点的临时位置。
3. 安装插件：

   在 Linux 中，以运行 Elasticsearch 的用户身份登录，并运行下列命令：

   ```
   <elasticsearch_install_directory>/bin/elasticsearch-plugin install file://
   localhost/<full path of elasticsearch-security-plugin*.zip file> --verbose
   ```

   提示继续安装时，输入 y。

4 （有条件）如果 Elasticsearch 不在侦听默认 HTTP 端口 (9200)，则必须在 <elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt 文件中的每个条目中更新 Elasticsearch 端口号。

有关详细信息，请参见通过使用白名单提供对 Elasticsearch 客户端的访问权限（第 77 页）。

5 重启动 Elasticsearch。

提供对其他 Elasticsearch 客户端的安全访问

默认情况下，受信客户端如 SSDM服务器（针对事件可视化仪表板）、YARNNodeManager、Sentine服务器（针对事件可视化仪表板）以及 RCM 拥有 Elasticsearch 的访问权限。如果想要使用其他 Elasticsearch 客户端，必须通过使用 SAML 令牌或白名单提供这些其他客户端的安全访问权限。

通过使用 SAML 令牌提供 Elasticsearch REST 客户端的访问权限

如果使用 REST 客户端访问 Elasticsearch，可以按下列方式在请求标题中包含一个 SAML 令牌：

1 从 Sentinel 鉴定服务器获取 SAML 令牌。有关更多信息，请参见 Sentinel 中提供的 REST API 文档。

单击**帮助 > API > 教程 > API 安全性 > 获取 SAML 令牌（登录）**。

2 在后续REST请求中使用SAML令牌：在REST客户端所作的每个请求的授权标题中包含SAML令牌。将标题名称指定为 Authorization，标题值指定为步骤 1 中所获得的 <*SAML 令牌*>。

通过使用白名单提供对 Elasticsearch 客户端的访问权限

默认情况下，Sentinel 用受信 Elasticsearch 客户端，如 SSDM 服务器（针对事件可视化仪表板）、YARNNodeManager、Sentinel服务器（针对事件可视化仪表板）以及RCM的IP地址自动填充白名单。Elasticsearch 安全插件为白名单中所列的所有客户端授予对 Elasticsearch 的访问权限。

要为不发送有效 Sentinel 令牌的其他客户端提供访问权限，则必须以 IP address:port 的格式将客户端的 IP 地址和 Elasticsearch 服务器的 HTTP 端口号添加到白名单中。您必须确保添加到白名单的外部客户端合法且可信，以阻止任意未授权的访问。

要更新白名单：

1 以运行 Elasticsearch 的用户身份登录 Sentinel 服务器或 Elasticsearch 节点。

2 在下列文件中添加条目 <Elasticsearch_Client_IP>:<Target_Elasticsearch_HTTP_Port>：

- Sentinel 所包含的 Elasticsearch 节点的 <Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin//elasticsearch-ip-whitelist.txt。
- 外部 Elasticsearch 节点的 <elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt

如果有多个条目，在新行中添加每个条目并保存文件。

3 在 Elasticsearch 群集的每个节点重复上述步骤。

更新 Elasticsearch 插件配置

如果修改可缩放储存组件的 IP 地址/主机名和端口号或 Elasticsearch 版本和端口号，则必须相应更新 Elasticsearch 插件配置文件。

在 Elasticsearch 群集的每个节点执行下列步骤：

1. 以运行 Elasticsearch 的用户身份登录 Elasticsearch 节点。
2. （有条件）如果修改YARN NodeManager IP地址、SSDM或Sentinel服务器IP地址、RCM IP地址或 Elasticsearch 端口号，则相应更新白名单以确保 Elasticsearch 安全插件授予对 Elasticsearch 客户端的访问权限。

   如果在HA模式中配置 SSDM 或 Sentinel，为 HA 群集的每个活动节点和被动节点的物理 IP 地址添加条目。

   如果修改 HA 群集任意节点的物理 IP 地址或向 HA 群集添加新节点，请用修改或新添加节点的物理 IP 地址更新白名单。

   有关详细信息，请参见通过使用白名单提供对 Elasticsearch 客户端的访问权限（第 77 页）。
3. （有条件）如果修改SSDM IP地址、Sentinel服务器IP地址或Web服务器端口号，更新下列文件中的 authServer.host 和 authServer.port 属性并重启动 Elasticsearch：

   - Sentinel 所包含的 Elasticsearch 节点的 <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-configuration.properties。
   - 外部 Elasticsearch 节点的 <elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-configuration.properties。

   如果在HA模式中配置 SSDM 或 Sentinel，将 authServer.host 属性设置为 HA 群集的虚拟 IP 地址。

   如果修改 HA 群集的虚拟 IP 地址，将 authServer.host 属性更新为修改的虚拟 IP 地址。
4. （有条件）如果已将 Elasticsearch 升级为更新的版本，在下列文件中更新 elasticsearch.version 属性并重启动 Elasticsearch：

   - Sentinel 所包含的 Elasticsearch 节点的 /opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-descriptor.properties。
   - 外部 Elasticsearch 节点的 <elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-descriptor.properties。

Elasticsearch 性能优化

Sentinel 自动配置下表所列 Elasticsearch 设置。您可以根据需要自定义 Elasticsearch 设置。

要自定义默认设置：

对于传统储存： 打开 /etc/opt/novell/sentinel/config/elasticsearch-index.properties 文件并按需要更新表中所列属性。

对于可缩放储存： 在 SSDM 主页中，单击**储存** > **可缩放储存** > **高级属性** > **Elasticsearch**。

表 12-1 Elasticsearch 属性

属性	默认值	注释
elasticsearch.events.lucenefilter（可选）		指定过滤器以仅向 Elasticsearch 发送特定事件进行索引。例如：如果指定值为 sev:[3-5]，则仅严重性值介于 3 到 5 的事件将发送到 Elasticsearch。
index.fields	id,dt,rv171,msg,ei,evt,xdastaxname,xdasoutcomename,sev,vul,rv32,rv39,rv159,dhn,dip,rv98,dp,fn,rv199,dun,tufname,rv84,rv158,shn,sip,rv76,sun,iufname,sp,iudep,rv198,rv62,st,tid,srcgeo,destgeo,obsgeo,rv145,estz,estzmonth,estzdiy,estzdim,estzdiw,estzhour,estzmin,rv24,tudep,pn,xdasclass,xdasid,xdasreg,xdasprov,iuident,tuident	表示您希望 Elasticsearch 索引的事件字段。
es.num.shards	5	表示每个索引的主要分片数量。 当分片大小超过 50 GB 时，您可以提高此默认值。
es.num.replicas	1	表示每个主要分片应有的复本分片数量。 考虑到故障转移和高可用性，建议至少有 2 个节点群集。

部署 Elasticsearch 安全插件

在下列情况下，您必须重新部署，即在 Sentinel 所含 Elasticsearch 节点及外部 Elasticsearch 节点卸装并重新安装 Elasticsearch 安全插件：

- 添加或修改远程 Collector Manager IP 地址。
- 卸装远程 Collector Manager。
- 启用可缩放储存安装后。

要重新部署 Elasticsearch 安全插件：

1. 以运行 Elasticsearch 的用户身份登录 Sentinel 服务器或 Elasticsearch 节点。
2. 使用下列命令卸装插件：
   - 对于 Sentinel 中所含 Elasticsearch：<sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin remove file://localhost/<sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
   - 对于外部 Elasticsearch：<elasticsearch_install_directory> remove file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin

3 重新安装插件：

- 对于 Sentinel 中所含 Elasticsearch：<sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
- 对于外部 Elasticsearch：<elasticsearch_install_directory>/bin/elasticsearch-plugin install file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin

4 使用下列命令重启动 Elasticsearch：

- 对于 Sentinel 中所含 Elasticsearch 节点：

  ```
  rcsentinel stopSIdb
  rcsentinel startSIdb
  ```

- 对于外部 Elasticsearch 节点：

  sudo systemctl restart elasticsearch.service

13 安装和设置可缩放储存

实现下表中所列的先决条件，将可缩放储存设置为 Sentinel 的数据储存选项：

表 13-1 *启用可缩放储存的先决条件*

❒	任务	参见
❒	确定您需要根据所需的EPS大小和副本数配置的Hadoop分布式群集和 Elasticsearch 群集节点的数量。 确定 CDH 和 Elasticsearch 的认证版本。	Sentinel 的技术信息。
❒	CDH、Elasticsearch 和 Sentinel 都有其自己的平台支持一览表。查看以上每种产品的平台支持一览表，确定您要使用的平台。 对于 Elasticsearch，建议安装 RPM，因为 RPM 包含 init 脚本。这会将 Elasticsearch 作为服务进行安装，并使其可在重引导和升级期间自动停止和启动，而不会重写配置文件。 SLES 11 不支持 Elasticsearch RPM 安装。因此，要确定适用于 Elasticsearch 的平台。	CDH 支持 Cloudera 文档中的矩阵。 Elasticsearch 支持 Elasticsearch 文档中的矩阵。 Sentinel 支持矩阵。
❒	在群集模式下安装和配置 CDH。	安装和配置 CDH（第 81 页）。
❒	在群集模式下安装和配置 Elasticsearch。	安装和配置 Elasticsearch（第 73 页）。
❒	在 Sentinel 中启用可缩放储存。	启用可缩放储存（第 83 页）

安装和配置 CDH

本节介绍在安装和配置CDH时Sentinel所需的特定设置。有关安装和配置CDH的详细信息，您必须参考 Cloudera 文档的认证版本。

Sentinel 可与 CDH 的免费版本 Cloudera Express 一起使用。Sentinel 还可与 Cloudera Enterprise 一起使用，后者需要您购买 Cloudera 的许可证，其中包括很多 Cloudera Express 版本所没有的功能。如果您选择一开始就使用 Cloudera Express，但是后来发现需要 Cloudera Enterprise 的功能，则可在购买了 Cloudera 的许可证后升级群集。

先决条件

安装 CDH 前，您必须根据以下先决条件设置主机：

- 实现 Cloudera 文档中提到的先决条件。
- 使用 ext4 或 XFS 文件系统来优化性能。
- CDH 需要多个在默认情况下不安装的操作系统包。因此，您必须装入相应的操作系统 DVD。Cloudera 安装说明将指导您如何安装这些包。
- 对于 SLES 操作系统，CDH 需要 python-psycopg2 包。安装 python-psycopg2 包。有关详细信息，请参见 openSUSE 文档。
- 如果您使用的是虚拟机，请在创建虚拟机节点时在文件系统中保留所需的磁盘空间。例如，在 VMware 中，您可以使用密集供应。
- 确保 Sentinel 和 CDH 群集节点处于同一时区。
- 通过添加以下项，在 /etc/sysctl.conf 文件中将所有主机的交换率设置为 1：

  ```
  vm.swappiness=1
  ```

  要立即应用此设置，请运行以下命令：

  ```
  sysctl -p
  ```

- CDH 中的 JDK 版本必须至少与 Sentinel 中使用的 JDK 版本相同。如果 CDH 中的 JDK 版本低于 Sentinel JDK，则您必须按照说明手动安装 JDK，而不是安装 CDH 储存库中的可用 JDK。

  使用存档二进制文件 (.tar.gz) 安装 JDK，因为使用 manage_spark_jobs.sh 脚本在 YARN 上提交 Spark 工作作业时，JDK RPM 安装会产生问题。

  要确定 Sentinel 中使用的 JDK 版本，请参见 Sentinel 发行说明。

安装和配置 CDH

安装CDH的认证版本。有关CDH已认证版本的信息，请参见Sentinel技术信息页面。有关安装说明，请参考 Cloudera 文档的认证版本。

安装 CDH 时执行以下操作：

- （有条件）如果嵌入式 PostgreSQL 数据库安装失败，执行以下步骤：

  mkdir -p /var/run/postgresql

  sudo chown cloudera-scm:cloudera-scm /var/run/postgresql

- 在**选择储存库**窗口中选择软件安装类型时，请确保选择**使用包**，并在**附加的包**中选择·Kafka。
- 添加服务时，请确保启用以下服务：
  - Cloudera 管理器
  - ZooKeeper
  - HDFS
  - HBase
  - YARN
  - Spark
  - Kafka

注释： Spark History Server 和 HDFS NameNode 必须安装在同一节点上，才能确保系统的可靠性。有关可缩放储存架构的信息，请参见 针对可缩放储存进行规划（第 43 页）。

启用上述服务时，为以下内容配置高可用性：

- HBase HMaster
- HDFS NameNode
- YARN ResourceManager

- （有条件）如果安装程序因缺少 Java 路径而无法部署客户端配置，请打开新的浏览器会话，然后按以下方式手动更新 Java 路径：

  单击**主机** > **所有主机** > **配置**，然后在 **Java 用户主目录**字段中指定正确的路径。

启用可缩放储存

您可以在 Sentinel 安装期间或安装后启用可缩放储存。在安装期间启用可缩放储存时，Sentinel 会使用默认值配置 CDH 组件。其中一些配置是永久性的，不能更改。例如，Kafka 主题的默认分区数是 9，该值不能更改。

如果您要更改默认值，则必须在安装 Sentinel 后启用可缩放储存，然后根据需要设置 CDH 组件的配置。

对于传统安装，您可以在 Sentinel 安装期间或安装后启用可缩放储存。对于设备安装，您只能在安装后启用可缩放储存。

在升级安装版中，只有升级 Sentinel 之后，方能启用可缩放储存。

在继续启用可缩放储存前，请确保 Kafka、HDFS NameNode、YARN NodeManager、ZooKeeper 和 Elasticsearch 节点的 IP 地址或主机名和端口号列表随手可用。启用可缩放储存时，您需要此信息。

要在 Sentinel 安装期间启用可缩放储存，请参见Sentinel 服务器自定义安装（第 86 页）。

要在 Sentinel 安装或升级后启用可缩放储存，请参见 *《Sentinel 管理指南》* 中的“在安装后启用可缩放储存”。

14 传统安装

本章将介绍各种 Sentinel 安装方法。

执行交互式安装

本节将介绍标准安装和自定义安装。

Sentinel 服务器标准安装

使用以下步骤执行标准安装：

1. 从 下载网站下载 Sentinel 安装文件：
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。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>
   ```

5. 指定您希望用于安装的语言数量，然后按 Enter 键。

   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包含的默认评估许可证密钥继续进行。在评估期内或评估期结束后，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 主界面，请在 Web 浏览器中指定下列 URL：

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

其中，*IP_AddressOrDNS_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。

Sentinel 服务器自定义安装

如果您要使用自定义配置安装 Sentinel，则可通过以下方式自定义您的 Sentinel 安装：指定您的许可证密钥，设置不同的口令，指定不同的端口，等等。

1 如果您要启用可缩放储存，请实现第 13 章“安装和设置可缩放储存”（第 81 页）中指定的先决条件。

2 从 下载网站下载 Sentinel 安装文件：

3 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>*。

4 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>
```

5 指定您希望用于安装的语言数量，然后按 Enter 键。

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。

8 指定 2 以执行 Sentinel 的自定义配置。

9 输入 1 以使用默认的评估许可证密钥

或

输入 2 以输入购买的 Sentinel 许可证密钥。

10 指定管理员用户 admin 的口令并再次确认口令。

11 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。

12 指定应用程序用户 appuser 的口令并再次确认口令。

13 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。

14 更改端口之后，指定 7 以完成更改。

15 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 以便使用 LDAP 目录鉴定来鉴定用户。

默认值为 1。

16 ***如果您要在 FIPS 140-2 模式下启用 Sentinel***，请输入 y。

16a 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。

16b 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

16c 执行第 24 章“在 FIPS 140-2 模式下操作 Sentinel”（第 123 页）中所述的任务，以完成 FIPS 140-2 模式配置。

17 ***如果您要启用可缩放储存***，请输入 yes 或 y。

重要： 启用可缩放储存后，您不能还原配置，除非重新安装 Sentinel。

17a 指定可缩放储存组件的 IP 地址或主机名和端口号。

17b （有条件）如果您要退出可缩放储存配置，并继续执行 Sentinel 安装，请输入 no 或 n。

17c Sentinel 安装完成后，完成可缩放储存安装后配置（第 87 页）中介绍的可缩放储存配置。

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 主界面，请在 Web 浏览器中指定下列 URL：

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

其中，*<IP_AddressOrDNS_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。

可缩放储存安装后配置

1 登录 SSDM 服务器。

2 清除浏览器超速缓存以查看您安装的 Sentinel 版本。

3 要查看事件和警报，将 SSDM 中包含的 Elasticsearch 节点添加到为可缩放储存设置的 Elasticsearch 群集：

在本地 Elasticsearch 节点中，打开 /etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml 文件并添加下列信息：

- cluster.name：*<Elasticsearch _cluster_name>*
- node.name：*<node_name>*
- discovery.zen.ping.unicast.hosts：["*<elasticsearch 节点 1 的 FQDN>*", "*<elasticsearch 节点 2 的 FQDN>*", 等等"]

在所有外部 Elasticsearch 节点中，打开 /etc/elasticsearch/elasticsearch.yml 并更新

discovery.zen.ping.unicast.hosts：["*<elasticsearch 节点 1 的 FQDN>*", "*<elasticsearch 节点 2 的 FQDN>*", 等等"]

注释： 确保本地 elasticsearch.yml 文件及外部 Elasticsearch 节点的 elasticsearch.yml 文件的参数值相同，但 network.host 和 node.name 除外，因为这些值对节点来说是唯一值。

---

4 使用下列命令重启动索引服务：

```
rcsentinel stopSIdb
rcsentinel startSIdb
```

5 按下列部分中所述完成可缩放储存配置：

- 确保 Elasticsearch 中数据的安全（第 75 页）
- *Sentinel 管理指南*中的性能优化指南
- *Sentinel 管理指南*中的处理数据

Collector Manager 和 Correlation Engine 安装

默认情况下，Sentinel 将会安装 Collector Manager 和 Correlation Engine。对于生产环境，设置一个分布式部署，因为它可以将数据收集组件隔离到独立的计算机上，这对以最佳系统稳定性处理峰值和其他异常情况很重要。有关安装附加组件优势的详细信息，请参见分布式部署的优势（第 45 页）。

重要： 必须在单独的系统上安装附加的 Collector Manager 或 Correlation Engine。Collector Manager 或 Correlation Engine 不能位于安装了 Sentinel 服务器的同一个系统上。

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，请参见 第 5 章“满足系统要求”（第 37 页）。
- 使用网络时间协议 (NTP) 同步时间。
- 在 Sentinel 服务器上，Collector Manager 需要到讯息总线端口 (61616) 的网络连接。在开始安装 Collector Manager 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。

要安装 Collector Manager 和 Correlation Engine，请使用以下步骤：

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

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

其中，*<IP_AddressOrDNS_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 单击所需安装项目下的**下载安装器**。

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 Collector Manager 或 Correlation Engine：

对于 Collector Manager：

```
./install-cm
```

对于 Correlation Engine：

```
./install-ce
```

或者

如果您希望在多个系统上安装 Collector Manager 或 Correlation Engine，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 安装。要记录您的安装选项，请指定以下命令：

对于 Collector Manager：

```
./install-cm -r <response_filename>
```

对于 Correlation Engine：

```
./install-ce -r <response_filename>
```

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。

安装过程中可能会花几分钟加载安装程序包和提示选择配置类型。

11 提示时，指定相应的选项以继续进行标准或自定义配置。

12 输入已安装 Sentinel 的计算机的默认通讯服务器主机名或 IP 地址。

13 （有条件）如果选择自定义配置，则指定以下内容：

13a Sentinel 服务器通讯通道端口号。

13b Sentinel Web 服务器端口号。

14 系统提示接受证书时，在 Sentinel 服务器中运行以下命令以校验该证书：

对于 FIPS 模式：

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

对于非 FIPS 模式：

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/nonfips_backup/.activemqkeystore.jks
```

将证书输出与步骤 12中显示的 Sentinel 服务器证书进行比较。

注释： 如果证书不匹配，安装将停止。再次运行安装程序，并检查证书。

15 如果证书输出与 Sentinel 服务器证书相匹配，则接受证书。

16 指定任何拥有管理员角色的用户的身份凭证。输入用户名和口令。

17 （有条件）如果选择自定义配置，则输入 yes 或 y 以在 Sentinel 中启用 FIPS 140-2 模式并继续进行 FIPS 配置。

18 （有条件）如果您的环境使用多因素或加强型鉴定，您必须提供 Sentinel 客户端 ID 和 Sentinel 客户端机密。有关鉴定方法的更多信息，请参见 *Sentinel 管理员指南*中的“鉴定方法”。

要检索 Sentinel 客户端 ID 和 Sentinel 客户端机密，请前往以下 URL：

https://*Hostname*:*port*/SentinelAuthServices/oauth/clients

其中：

- *Hostname* 是 Sentinel 服务器的主机名称。
- *Port* 是 Sentinel 使用的端口（通常为 8443）。

指定的 URL 将使用当前 Sentinel 会话检索 Sentinel 客户端 ID 和 Sentinel 客户端机密。

19 （有条件）如果已启用事件可视化，则必须将 Collector Manager 添加到 Elasticsearch 白名单。有关详细信息，请参见通过使用白名单提供对 Elasticsearch 客户端的访问权限（第 77 页）。

20 根据提示继续安装，直到安装完成。

执行无提示安装

如果需要在部署中安装多个 Sentinel 服务器、Collector Manager 或 Correlation Engine，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。

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，请参见 Sentinel 服务器标准安装（第 85 页）或Sentinel 服务器自定义安装（第 86 页）和Collector Manager 和 Correlation Engine 安装（第 88 页）。

要在 FIPS 140-2 模式下启用，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 下载网站下载安装文件。

2 以根身份登录到要安装 Sentinel、Collector Manager 或 Correlation Engine 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，在无提示模式下执行安装：

对于 Sentinel 服务器：

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

对于 Collector Manager：

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

对于 Correlation Engine：

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

将使用储存在响应文件中的值继续安装。

如果安装 Sentinel 服务器，因为系统要执行一次性初始化，所以安装后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。

5 **（有条件）如果对 Sentinel 服务器选择启用 FIPS 140-2 模式，** 执行第 24 章“在 FIPS 140-2 模式下操作 Sentinel”（第 123 页）中所述的任务，以完成 FIPS 140-2 模式配置。

以非 root 用户身份安装 Sentinel

如果组织策略不允许您以 root 身份运行 Sentinel 的完整安装，则可以作为非 root 用户（即 novell 用户）安装 Sentinel。在此安装过程中，将以 root 用户身份执行前几步，然后以 root 用户创建的 novell 用户身份继续安装 Sentinel。最后，根用户完成安装。

以非 root 用户身份安装 Sentinel 时，您应该以 novell 用户身份安装 Sentinel。尽管安装顺利且成功，但不支持除 novell 用户之外的非根安装。

注释： 在现有的非默认目录中安装 Sentinel 时，请确保 novell 用户对此目录拥有所有权权限。运行以下命令以分配所有权权限：

```
chown novell:novell <non-default installation directory>
```

---

1 从 下载网站下载安装文件。

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 root 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 root 用户（即 novell）：

```
su novell
```

7 （有条件）要执行交互式安装：

7a 根据要安装的组件指定相应命令：

组件	命令
Sentinel 服务器	**默认位置：** ./install-sentinel
	非默认位置： ./install-sentinel --location=/foo
Collector Manager	**默认位置：** ./install-cm
	非默认位置： ./install-cm --location=/foo
Correlation Engine	**默认位置：** ./install-ce
	非默认位置： ./install-cm --location=/foo

7b 继续步骤 9。

8 （有条件）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，请参见 Sentinel 服务器标准安装（第 85 页）或Sentinel 服务器自定义安装（第 86 页）。

要执行无提示安装，请执行以下操作：

8a 根据要安装的组件指定相应命令：

组件	命令
Sentinel 服务器	**默认位置：** ./install-sentinel -u <*response_file*>
	非默认位置： ./install-sentinel --location=/foo -u <*response_file*>
Collector Manager	**默认位置：** ./install-cm -u <*response_file*>
	非默认位置： ./install-cm --location=/foo -u <*response_file*>
Correlation Engine	**默认位置：** ./install-ce -u <*response_file*>
	非默认位置： ./install-ce --location=/foo -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Sentinel 服务器标准安装（第 85 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Sentinel 服务器自定义安装（第 86 页）中的步骤 8 到步骤 15。

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 主界面，请在 Web 浏览器中指定下列 URL：

`https://`*`IP_AddressOrDNS_Sentinel_server`*`:`*`8443`*`/sentinel/views/main.html`

其中，*IP_AddressOrDNS_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。

15 设备安装

Sentinel 设备是基于 Micro Focus 通用设备框架的可立即运行的软件设备。该设备将一个强化的 SLES 12 SP 3 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，从而允许您充分利用现有投资。Sentinel 设备提供基于 Web 的用户界面，用于配置和监视设备。

Sentinel 设备映像同时以两种能部署到虚拟环境中的 ISO 和 OVF 格式进行封装。有关支持的虚拟化平台的信息，请参见 Sentinel 技术信息网站。

先决条件

确保您要将 Sentinel 作为 ISO 设备进行安装的环境满足以下先决条件：

- 安装 Sentinel 设备之前，请查看认证的 SLES 发行说明中列出的新功能和已知问题。
- （有条件）如果您正在裸机硬件上安装 Sentinel ISO 设备，请从支持网站下载设备 ISO 磁盘映像，并制作 DVD。
- 确保硬盘空间至少为 50 GB，以便安装程序可以生成自动分区建议。
- 确保系统的最小内存为4GB，以便完成安装。如果内存小于4GB，则安装将失败。如果内存大于 4 GB 但小于建议的 24 GB，安装过程中会显示一条讯息，提醒您内存小于建议值。

安装 Sentinel ISO 设备

本节提供有关使用 ISO 设备映像安装 Sentinel、Collector Manager 和 Correlation Engine 的信息。此映像格式允许您通过使用可引导的 ISO DVD 映像来生成可直接部署到物理硬件（裸机）或虚拟硬件（超级管理程序中卸载的虚拟机）的全盘映像格式。

安装 Sentinel

若要安装 Sentinel ISO 设备，请执行以下操作：

1. 从 下载网站下载 ISO 虚拟设备映像。
2. （有条件）如果您正在使用超级管理程序：

   使用 ISO 虚拟设备映像设置虚拟机并开机。

   或者

将 ISO 映像刻录到 DVD，使用此 DVD 设置虚拟机，然后开机。

3 （条件）如果您正在裸机硬件上安装 Sentinel 设备，请执行以下操作：

3a 从已插入此 DVD 的 DVD 驱动器引导物理计算机。

3b 请按照安装向导的屏幕指导进行操作。

3c 选择**安装 sentinel 服务器 <*版本*>**。

4 选择语言。

5 选择键盘布局。

6 单击**下一页**。

7 阅读并接受 SUSE Enterprise Server 软件许可证协议。单击**下一步**

8 阅读并接受 Sentinel 服务器设备许可证协议。单击**下一步**

9 设置 Sentinel 设备口令、NTP 配置和时区。

设置 vaadmin 用户身份凭证，以便登录到 Sentinel 设备管理控制台。

注释： 安装后，您可以通过以下方式更改 NTP 配置和时区：

- 转到命令提示符并输入 yast->Network Services->NTP Configuration
- 转到 Sentinel 设备管理控制台，然后单击**时间**。

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
```

---

10 在 Sentinel 服务器设备网络设置页面中，指定主机名和域名。选择**静态 IP 地址**或 **DHCP IP 地址**。

11 单击**下一页**。

12 （有条件）如果在步骤 10 中选择了**静态 IP 地址**，需指定网络连接设置。

13 单击**下一步**。

14 设置 Sentinel 用户 admin 的口令，然后单击**下一步**。

设备安装完毕。

15 记录控制台中显示的设备 IP 地址。

16 在控制台以 root 用户身份登录设备。

输入用户名 root，并输入您在步骤 9中设置的口令。

17 继续设备的安装后配置（第 99 页）。

安装 Collector Manager 和 Correlation Engine

除了需要从下载网站下载相应的 ISO 设备文件外，安装 Collector Manager 或 Correlation Engine 的过程与安装 Sentinel 的过程类似。

1 通过 安装 Sentinel（第 95 页） 中的步骤 13 完成步骤 1。

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 1 GB，则安装过程会不允许您继续执行操作，**下一步**按钮会变为灰色。

2 为 Collector Manager 或 Correlation Engine 指定以下配置：

- **Sentinel 服务器主机名或 IP 地址：** 指定 Collector Manager 或 Correlation Engine 应该连接到的 Sentinel 服务器的主机名或 IP 地址。

- **Sentinel 通讯通道端口：** 指定 Sentinel 服务器通讯通道端口号。默认端口号是 61616。
- **Sentinel Web 服务器端口：** 指定 Sentinel Web 服务器端口。默认端口为 8443。
- **拥有管理员角色的用户名：** 指定任何拥有管理员角色的用户的用户名。
- **拥有管理员角色的用户的口令：** 指定与您在以上字段中指定的用户名对应的口令。

3 （有条件）如果您的环境使用多因素或加强型鉴定，您必须提供 Sentinel 客户端 ID 和 Sentinel 客户端机密。有关鉴定方法的更多信息，请参见 *Sentinel 管理员指南*中的“鉴定方法”。

要检索 Sentinel 客户端 ID 和 Sentinel 客户端机密，请前往以下 URL：

https://*Hostname*:*port*/SentinelAuthServices/oauth/clients

其中：

- *Hostname* 是 Sentinel 服务器的主机名称。
- *Port* 是 Sentinel 使用的端口（通常为 8443）。

指定的 URL 将使用当前 Sentinel 会话检索 Sentinel 客户端 ID 和 Sentinel 客户端机密。

4 单击下一步。

5 在提示时接受证书。

6 记录控制台中显示的设备 IP 地址。

控制台显示一条讯息，指出此设备是 Sentinel Collector Manager 或 Correlation Engine（取决于您选择安装的部件），同时还会显示 IP 地址。控制台还会显示 Sentinel 服务器用户界面 IP 地址。

7 通过安装 Sentinel（第 95 页）中的步骤 17完成步骤 16。

安装 Sentinel OVF 设备

本节将介绍如何将 Sentinel、Collector Manager 和 Correlation Engine 安装为 OVF 设备映像。

OVF 格式是标准的虚拟机格式，受到大多数超级管理程序的支持，可直接支持或通过简单的转换进行支持。Sentinel 支持带有两个认证的超级管理程序的 OVF 设备，但您也可以通过其他超级管理程序使用它。

- 安装 Sentinel（第 97 页）
- 安装 Collector Manager 和 Correlation Engine（第 98 页）

安装 Sentinel

若要安装 Sentinel OVF 设备，请执行以下操作：

1 从 下载网站下载 OVF 虚拟设备映像。

2 在您的超级管理程序管理控制台中，将 OVF 映像文件作为新虚拟机导入。如果提示您这样做的话，请允许超级管理程序将 OVF 映像转换为本机格式。

3 查看分配给新虚拟机的虚拟硬件资源，以便确保这些资源满足 Sentinel 的要求。

4 打开虚拟机。

5 选择语言。

6 选择键盘布局。

7 单击下一页。

8 阅读并接受 SUSE Enterprise Server 软件许可证协议。单击**下一步**。

9 阅读并接受 Sentinel 服务器设备许可证协议。单击**下一步**。

10 设置 Sentinel 设备口令、NTP 配置和时区。

设置 vaadmin 用户身份凭证，以便登录到 Sentinel 设备管理控制台。

注释： 安装后，您可以通过以下方式更改 NTP 配置和时区：

- 转到命令提示符并输入 yast->Network Services->NTP Configuration
- 转到 Sentinel 设备管理控制台，然后单击**时间**。

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
```

---

11 在 Sentinel 服务器设备网络设置页面中，指定主机名和域名。选择**静态 IP 地址**或 **DHCP IP 地址**。

12 单击**下一页**。

13 （有条件）如果在步骤 11 中选择了**静态 IP 地址**，需指定网络连接设置。

14 单击**下一页**。

15 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。

16 记录控制台中显示的设备 IP 地址。使用同一 IP 地址访问 Sentinel 主界面。

安装 Collector Manager 和 Correlation Engine

要在 VMware ESX Server 上将 Collector Manager 或 Correlation Engine 安装为 OVF 设备映像，请执行以下操作：

1 通过 安装 Sentinel（第 97 页） 中的步骤 14 完成步骤 1。

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 1 GB，则安装过程会不允许您继续执行操作，**下一步**按钮会变为灰色。

2 指定 Collector Manager 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。默认端口为 61616。

4 指定任何拥有管理员角色的用户的身份凭证。输入用户名和口令。

5 （有条件）如果您的环境使用多因素或加强型鉴定，您必须提供 Sentinel 客户端 ID 和 Sentinel 客户端机密。有关鉴定方法的更多信息，请参见 *Sentinel 管理员指南*中的“鉴定方法”。

要检索 Sentinel 客户端 ID 和 Sentinel 客户端机密，请前往以下 URL：

https://*Hostname*:*port*/SentinelAuthServices/oauth/clients

其中：

- *Hostname* 是 Sentinel 服务器的主机名称。
- *Port* 是 Sentinel 使用的端口（通常为 8443）。

指定的 URL 将使用当前 Sentinel 会话检索 Sentinel 客户端 ID 和 Sentinel 客户端机密。

6 单击**下一步**。

7 接受证书。

8 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 Collector Manager 或 Sentinel Correlation Engine（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。

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。

注册更新

您必须使用设备更新通道注册 Sentinel 设备，才能接收 Sentinel 和最新的操作系统更新。要注册设备，必须先从客户关怀中心获取设备注册代码或设备激活密钥。

使用 Sentinel 设备管理控制台注册

如果您正在使用的是 SLES 12 SP3，则可以使用 Sentinel 设备管理控制台注册更新。

1 通过执行以下任一操作起动 Sentinel 设备：
   - 登录到 Sentinel，单击 **Sentinel Main** > **设备**。
   - 在 Web 浏览器中指定下列 URL：https://<IP_address>:9443。
2 以 vaadmin 或 root 用户身份登录。
3 单击**联机更新** > **立即注册**。
4 在**电子邮件**字段中，指定您想要接收更新的电子邮件 ID。
5 在**激活密钥**字段中，输入注册代码。
6 单击**注册**以完成注册。

使用命令注册

如果使用 SLES 11 SP4 或 SLES 12 SP3，您可以使用命令进行注册。

注册更新

1 以 root 用户身份登录到 Sentinel 服务器。
2 指定以下命令：
   - 要注册服务器，指定：suse_register -a regcode-sentinel="<*registration_code*>" -a email="<*email_ID*>"
   - 要注册 Collector Manager，指定：suse_register -a regcode-sentinel-collector="<*registration_code*>" -a email="<*email_ID*>"

- 要注册 Correlation Engine，指定：suse_register -a regcode-sentinel-correlation ="<*registration_code*>" -a email="<*email_ID*>"
- 要在高可用性模式中注册 Sentinel，指定：suse_register -a regcode-sentinel-ha ="<*registration_code*>" -a email="<*email_ID*>"

关于电子邮件参数，请指定您想要接收更新的电子邮件 ID。

为传统储存创建分区

仅当您要使用传统储存作为数据储存选项时，本节中的信息才适用。

作为一项最佳实践，确保您创建的储存 Sentinel 数据的单独分区与可执行文件、配置文件、操作系统文件所在分区不同。单独储存可变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供附加稳健性。有关如何计划分区的详细信息，请参见 针对传统储存进行规划（第 40 页）。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 Control Center：

   `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。

   有关创建分区的详细信息，请参见 *SLES 11 文档*中的使用 YaST 分区器。
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

配置可缩放储存

要启用可缩放储存并将其配置为数据储存选项，请参见“《 Sentinel 管理指南》”中的*配置可缩放储存*。

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 客户中心相集成的程序包代理系统，可提供主要的 客户中心功能。

先决条件

为设备配置 SMT 前，请确保满足以下先决条件：

- 获取客户中心身份凭证以获取 Sentinel 更新。有关获取身份凭证的更多信息，请联系技术支持。
- 确保在您希望安装 SMT 的计算机上安装 SLES 11 SP3 以及下列包：
  - 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，请参见 SMT 文档中的以下各节内容：
  - 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

执行以下步骤，为设备配置 SMT：

1. 通过在 SMT 服务器中运行以下命令，启用设备储存库：

   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

2. 通过执行 “SMT 文档”的将客户端配置为使用 SMT 一节中的步骤，为设备配置 SMT。

升级设备

有关升级设备的信息，请参见 升级 Sentinel（第 147 页）。

16 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。

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. 在 **Sentinel 主仪表板**中，单击 **Admin** 下拉菜单，然后单击**应用程序**。
3. 单击**起动 Control Center** 以起动 Sentinel Control Center。
4. 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**。
5. 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**。
6. 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 插件网页中特定收集器的文档。

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. 在 **Sentinel 主仪表板**中，单击 **Admin** 下拉菜单，然后单击**应用程序**。
3. 单击**起动 Control Center** 以起动 Sentinel Control Center。
4. 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**。
5. 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**。
6. 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 插件网站中特定连接器的文档。

17 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
  ```

- 验证 Sentinel 服务是在 FIPS 还是在非 FIPS 模式下启动和运行：

  ```
  /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。

- 起动 Sentinel：

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

     ```
     https://IP_AddressOrDNS_Sentinel_server:8443
     ```

     其中，*IP_AddressOrDNS_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。
  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。

IV 配置 Sentinel

本节将介绍如何配置 Sentinel 和即用型插件。

18 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。

理解 Sentinel 中的时间

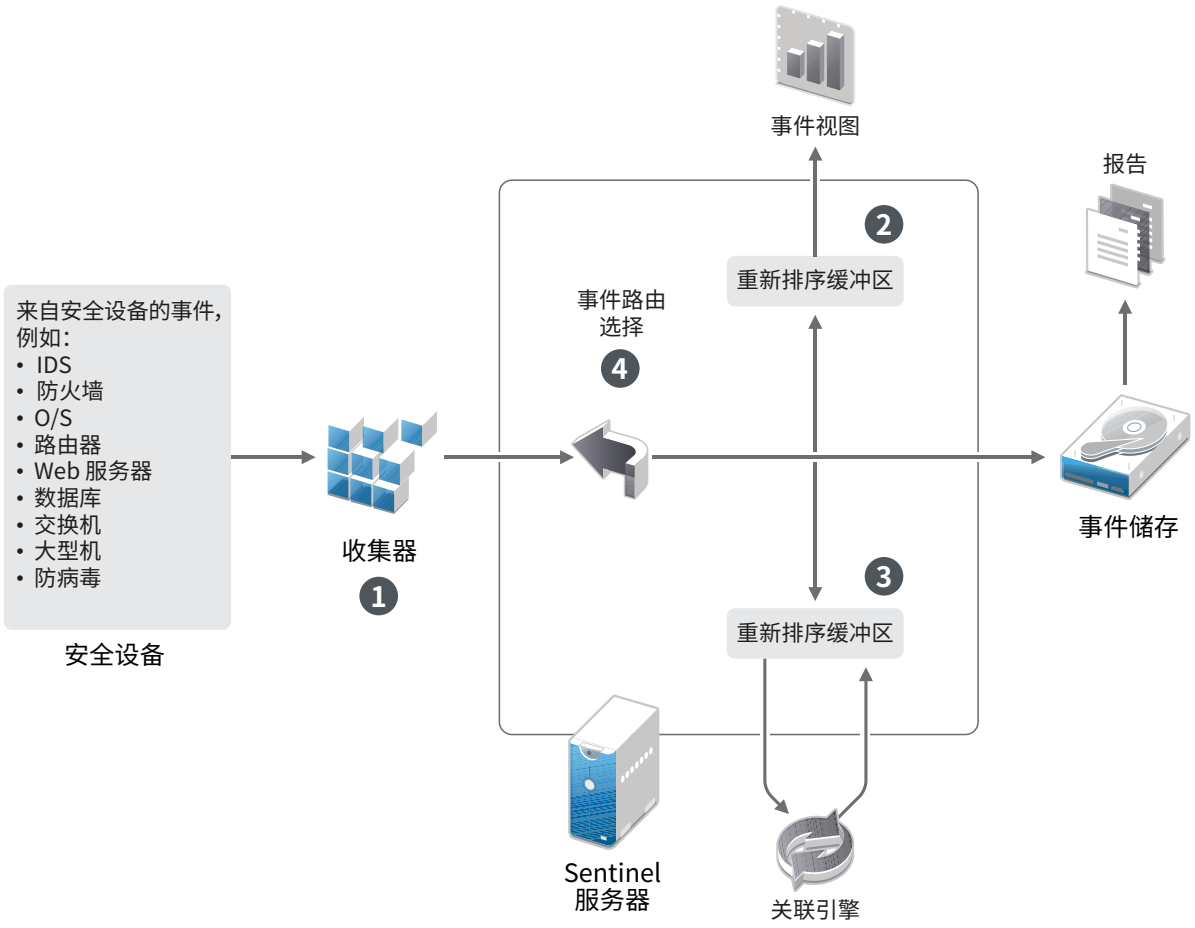
Sentinel 是由分布到您的整个网络中的多个进程组成的分布式系统。此外，事件源可能会引入一定的延迟。为了适应此需求，Sentinel 进程会在处理事件之前将事件重新排序到一个时序流中。

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 Collector Manager 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。

下图说明了 Sentinel 在传统储存设置中是如何做到这一点的：

图 18-1 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”与服务器时间相差不到 5 分钟（早于或晚于服务器时间）的事件通常由事件视图来处理。如果“事件时间”晚于服务器时间 5 分钟以上，则此事件不显示在事件视图中，但会添加到事件储存中。“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 Correlation Engine 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 Correlation Engine 不会处理这些事件。
4. 如果事件时间早于 Collector Manager 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 Correlation Engine 和安全智能等实时系统。

配置 Sentinel 中的时间

Correlation Engine 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 Collector Manager 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 Collector Manager 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 “《 Sentinel 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。

为事件配置延迟时间限制

当 Sentinel 从事件源收到事件时，在事件生成和被 Sentinel 处理时间之间可能有延迟。Sentinel 在独立分区中储存长延迟事件。如果有许多事件出现长时间延迟，这可能表明事件源配置不正确。试图处理延迟事件也可能降低 Sentinel 的性能。既然延迟事件可能是不正确的配置造成的，因此，可能不想它们存储下来，Sentinel 允许您为进来的事件配置可接受的延迟限制。事件路由器会丢弃超过延迟限制的事件。在 configuration.properties 文件的如下属性中指定延迟限制：

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

您也可以拥有一个定期记录 Sentinel 服务器日志文件的列表，用以显示那些超过指定阈值已接收事件的事件源。若要记录该信息，请在 configuration.properties 文件的如下属性中指定阈值：

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

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，Collector Manager 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 Collector Manager 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 Collector Manager 发送到 Sentinel 服务器并储存在事件储存中。Collector Manager 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 浏览器转换为本地时间，因此所有事件都是按本地时区显示给客户端的。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。

19 确保 Elasticsearch 中数据的安全

Sentinel 利用了基于浏览器的分析和搜索仪表板 Kibana，可以帮助您在仪表板中可视化事件和警报。Sentinel 在 Elasticsearch 中储存和索引警报。您也可以将 Sentinel 配置为在 Elasticsearch 中储存和索引事件，以利用事件可视化功能。Sentinel 仪表板访问 Elasticsearch 中的数据，以在仪表板中显示事件和警报。为确保仪表板仅显示用户角色有权查看的数据并阻止 Elasticsearch 中出现未经授权访问数据的情况，必须安装 Elasticsearch 安全插件。有关详细信息，请参见确保 Elasticsearch 中数据的安全（第 75 页）。

20 启用事件可视化

可缩放储存设置中默认包含事件可视化。在传统储存设置中，事件可视化仅在启用可视化数据储存 (Elasticsearch) 来储存数据和建立数据索引后可用。

先决条件

有关生产环境中事件的可缩放和分布式索引，您必须在群集模式中设置其他 Elasticsearch 节点。要在群集模式中安装和配置 Elasticsearch，请参见安装和配置 Elasticsearch（第 73 页）。

启用事件可视化

要启用事件可视化：

1. 以 Novell 用户身份登录 Sentinel 服务器。
2. 打开 /etc/opt/novell/sentinel/config/configuration.properties 文件。
3. 将 eventvisualization.traditionalstorage.enabled 设置为 true。
4. 几分钟后刷新用户界面以查看事件可视化。

   您现在应该可以看到**我的 Sentinel** 用户界面中启用的所有仪表板。起动仪表板，例如 Threat Hunting（威胁狩猎）仪表板，然后单击**搜索**。仪表板显示过去 1 小时内生成的所有事件。
5. （可选)事件可视化仪表板仅显示启用事件可视化后处理的事件。要查看基于文件的储存中的现有事件，必须将数据从基于文件的储存中迁移到 Elasticsearch。有关详细信息，请参见第 33 章 “将数据迁移到 Elasticsearch”（第 167 页）。

注释： 启用或禁用事件可视化将生成异常，因为将重启动 Sentinel 索引服务。此异常为预期情况，可忽略此异常。

---

21 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指派的端口，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. 使用以下命令关闭 Sentinel：

   rcsentinel stop

2. 在命令行指定以下命令来运行 configure.sh 脚本：

   ```
   ./configure.sh
   ```

3. 指定 1 以执行标准配置，或指定 2 以执行自定义 Sentinel 配置。
4. 按空格键以通读许可证协议。
5. 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。
6. 输入 1 以使用默认的评估许可证密钥

   或

   输入 2 以输入购买的 Sentinel 许可证密钥。
7. 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 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。

     admin 用户是一个身份，用于通过 Sentinel 主界面执行管理任务，包括创建其他用户帐户。
8. 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 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。

   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。
9. 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 10。
   - 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 10。

     appuser 帐户是一个内部身份，Sentinel java 进程使用此帐户来建立连接，并与数据库交互。您在此处输入的口令用于执行数据库任务。
10. 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。
11. 更改端口之后，指定 7 以完成更改。
12. 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 以便使用 LDAP 目录鉴定来鉴定用户。

    默认值为 1。

22 配置即用型插件

Sentinel 将与发布 Sentinel 时提供的默认 Sentinel 插件一起预安装。

本章将介绍如何配置即用型插件。

查看预安装的插件

您可以查看 Sentinel 中预安装的插件的列表。您还可以查看插件版本和其他元数据，这可帮助您确定是否已安装最新版本的插件。

要查看已安装在 Sentinel 服务器中的插件，请执行以下操作：

1. 以管理员身份登录到 Sentinel 主界面（https://<*IP 地址*>:8443），其中，8443 是 Sentinel 服务器的默认端口。
2. 单击**插件** > **编目**。

配置数据收集

有关为收集数据配置 Sentinel 的信息，请参见“《 Sentinel 管理指南》”中的*收集和路由事件数据*。

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 “《 Sentinel 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 主界面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 “《 Sentinel 管理指南》”中的*安装和管理解决方案包*。

配置操作和集成器

有关配置即用型插件的信息，请参见 Sentinel 插件网站中特定插件的文档。

23 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。

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. （有条件）如果环境使用多因子鉴定或强鉴定，您必须运行 create_mfa_fips_keys.sh 脚本并按屏幕指导操作。

   注释： 运行脚本时需要 NSS 数据库口令。

6. （有条件）如果您的环境使用多因素或加强型鉴定，您必须提供 Sentinel 客户端 ID 和 Sentinel 客户端机密。有关鉴定方法的更多信息，请参见 *Sentinel 管理员指南*中的“鉴定方法”。

   要检索 Sentinel 客户端 ID 和 Sentinel 客户端机密，请前往以下 URL：

   https://*Hostname*:*port*/SentinelAuthServices/oauth/clients

   其中：

   - *Hostname* 是 Sentinel 服务器的主机名称。
   - *Port* 是 Sentinel 使用的端口（通常为 8443）。

   指定的 URL 将使用当前 Sentinel 会话检索 Sentinel 客户端 ID 和 Sentinel 客户端机密。
7. 重启动 Sentinel 服务器。
8. 执行第 24 章“在 FIPS 140-2 模式下操作 Sentinel”（第 123 页）中所述的任务，以完成 FIPS 140-2 模式配置。

在远程 Collector Manager 和 Correlation Engine 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 Collector Manager 和 Correlation Engine 上启用 FIPS 140-2 模式。

要启用远程 Collector Manager 或 Correlation Engine 以在 FIPS 140-2 模式下运行，请执行以下操作：

1. 登录到远程 Collector Manager 或 Correlation Engine 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. 重启动 Collector Manager 或 Correlation Engine。
6. 执行第 24 章“在 FIPS 140-2 模式下操作 Sentinel”（第 123 页）中所述的任务，以完成 FIPS 140-2 模式配置。

24 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。

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 131 页）。

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 131 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新启动 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>/jdk/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 131 页）。

6 在目标计算机上重新启动 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>/jdk/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 131 页）。

5 在源计算机上重新启动 Sentinel 服务。

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 131 页）。

3 以拥有管理员角色的用户身份导航到 **Sentinel 主界面**，并继续配置 LDAP 鉴定。

有关更多信息，请参见 *Sentinel 管理指南*中的“针对单个 LDAP 服务器或域进行的 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，对在 FIPS 140-2 模式下运行的 Sentinel 服务器配置 LDAP 鉴定。

在远程 Collector Manager 和 Correlation Engine 中更新服务器证书

要将现有远程 Collector Manager 和 Correlation Engine 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 Collector Manager 或 Correlation Engine 保留为非 FIPS 模式。处于 FIPS 模式的远程 Collector Manager 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 Collector Manager 或 Correlation Engine 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 Collector Manager 或 Correlation Engine 能够与 Sentinel 服务器进行通讯。

要在远程 Collector Manager 或 Correlation Engine 中更新 Sentinel 服务器证书，请执行以下操作：

1. 登录到远程 Collector Manager 或 Correlation Engine 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。

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： 如果您已将 Sentinel 安装在 /opt/novell/sentinel 目录下，则将提供这些说明。以 novell 用户身份运行所有命令。

- 代理管理器连接器（第 126 页）
- 数据库 (JDBC) 连接器（第 126 页）
- Sentinel 链接连接器（第 126 页）
- Syslog 连接器（第 127 页）
- Windows 事件 (WMI) 连接器（第 128 页）
- Sentinel Link Integrator（第 129 页）
- LDAP Integrator（第 129 页）
- SMTP 集成器（第 130 页）
- Syslog 集成器（第 130 页）
- 将不启用 FIPS 的连接器与处于 FIPS 140-2 模式的 Sentinel 一起使用（第 130 页）

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 131 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 Collector Manager 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 Collector Manager 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。

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 131 页）。
3. 继续配置连接器。

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 131 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。

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 131 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 Collector Manager 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 Collector Manager 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。

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 131 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 Collector Manager 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 Collector Manager 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 131 页）。

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 Collector Manager 上，则您必须将 /etc/opt/novell/sentinel/config/rcm.cer 文件从接收方远程 Collector Manager 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 131 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。

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 131 页）。

3 继续配置集成器实例。

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。

Syslog 集成器

仅当您在配置 Syslog 集成器的网络设置期间选择了“已加密 (SSL)”选项时，才执行以下过程。

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

1 当 Syslog 集成器处于 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 Syslog 服务器证书导入 Sentinel FIPS 密钥存储区：

- **如果 Syslog 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 服务器复制到发送方 Sentinel 服务器。

  如果连接器部署在远程 Collector Manager 上，则您必须将 /etc/opt/novell/sentinel/config/rcm.cer 文件从接收方远程 Collector Manager 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 Syslog 连接器处于非 FIPS 模式：** 您必须将自定义 Syslog 服务器证书导入发送方 Sentinel FIPS 密钥存储区。

  注释： 当 Syslog 集成器处于 FIPS 140-2 模式而 Syslog 连接器处于非 FIPS 模式时，请使用该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。

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 Collector Manager 上的任意临时位置。
2. 转到 /opt/novell/sentinel/bin 目录。
3. 运行以下命令，将证书导入 FIPS 密钥存储区数据库，然后按照屏幕说明操作：

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. 当提示重新启动 Sentinel 服务器或远程 Collector Manager 时，请输入 yes 或 y。

2 继续配置集成器实例。

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

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 Collector Manager，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 III 部分 “安装 Sentinel” （第 67 页）。
2. 将非 FIPS 连接器专门部署到非 FIPS 远程 Collector Manager。

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 服务器的非 FIPS 远程 Collector Manager 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《Sentinel 发行说明》。

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。在启用了 FIPS 140-2 模式时，您无法使用 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 Collector Manager 的连接器的事件源，您必须将证书导入远程 Collector Manager（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 Collector Manager 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. 当提示重新启动 Sentinel 服务器或远程 Collector Manager 时，请输入 yes 或 y。

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。

- 将 Sentinel 服务器还原为非 FIPS 模式（第 131 页）
- 将远程 Collector Manager 或远程 Correlation Engine 还原为非 FIPS 模式（第 132 页）

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 root 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. 重新启动 Sentinel 服务器。

将远程 Collector Manager 或远程 Correlation Engine 还原为非 FIPS 模式

您可以将远程 Collector Manager 或远程 Correlation Engine 还原为非 FIPS 模式。

要将远程 Collector Manager 或远程 Correlation Engine 还原为非 FIPS 模式，请执行以下操作：

1. 登录到远程 Collector Manager 或远程 Correlation Engine 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. 重新启动远程 Collector Manager 或远程 Correlation Engine。

25 添加同意标题

Sentinel 允许您在登录前显示同意标题。您可以根据要求指定标题内容。添加同意标题后，每次登录 Sentinel 都必须接受同意标题中的条款。

要添加同意标题：

1. 以 Novell 用户身份登录到 Sentinel 服务器。
2. 浏览至 /<Sentinel_installation_path>/var/opt/novell/sentinel/3rdparty/jetty/webapps/ROOT/siemdownloads。
3. 添加名为 USER_AGREEMENT.txt 的文本文件。
4. 输入用户协议文本。
5. 保存文件。
6. 起动 Sentinel 查看同意标题。

现在，Sentinel 在登录屏幕上显示同意标题。

注释： 升级 Sentinel 前必须手动备份 USER_AGREEMENT.txt 文件。

V 升级 Sentinel

本节将介绍如何升级 Sentinel 和其他部件。

26 实现核对清单

在升级 Sentinel 之前，请查看下列核对清单，以确保升级成功：

表 26-1 *实现核对清单*

❒	任务	参见
❒	确保安装 Sentinel 及其部件的计算机满足指定的要求。	Sentinel 技术信息网站
❒	查看支持的操作系统发行说明以了解已知问题。	SUSE 发行说明
❒	查看 Sentinel 发行说明以了解新功能和已知问题。	Sentinel 发行说明
❒	完成“先决条件”中所述的任务。	第 27 章“先决条件”（第 139 页）

27 先决条件

保存自定义配置信息

保存 server.conf 文件设置

如果在 server.conf 文件中设置了任何自定义配置参数值，升级前请将这些值保存在独立文件中。

要保存自定义配置信息，请执行以下操作：

1. 以 novell 用户身份登录到 Sentinel 服务器，然后转到 /etc/opt/novell/sentinel/config/ 目录。
2. 创建名为 server-custom.conf 的配置文件，然后将自定义配置参数添加到此文件中。

在升级过程中，Sentinel 将已保存的自定义配置应用到这些配置文件中。

保存 jetty-ssl 文件设置

Sentinel 8.1 包括更新版 Jetty。更新版 Jetty 包括对其文件结构做出的更改。

如果您已更改 Sentinel 之前版本的 /etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml 文件，如排除所有加密法，请在 Sentinel 升级之前，将这些更改保存到单独文件中。

Sentinel 升级完成之后，将这些更改复制到 /etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl-context.xml 文件并重启 Sentinel。

延长事件关联数据的保留期限

从 Sentinel 7.4.4 开始，事件关联数据的默认保留期限为 14 天。如果您正在升级 Sentinel 7.4.4 之前的版本，升级后您设置的事件关联数据的保留期限将被覆盖为 14 天。为避免这种情况，您可以通过在 configuration.properties 文件中添加属性，将保留期限设置为所需值。有关更多信息，请参见 *《Sentinel 管理指南》*中的“配置事件关联数据的保留期限”。

升级前 SSDM 的配置

升级过程将会更新 Spark 应用程序相关文件。要使用更新文件，您必须重启 Spark 作业，重设置与 Kafka 主题相关的所有 Spark 检查点。要防止数据因重设置 Kafka 主题检查点而丢失，您必须在升级 SSDM 之前，暂停将数据从 Collector Manager 转发到 Kafka。暂停转发数据之后，数据将储存在 Collector Manager 上，直到恢复数据转发。Spark 应用程序处理完转发暂停前转发到 Kafka 的数据后，可安全重设置检查点，不会丢失数据。

要暂停将事件从 Collector Manager 转发至 Kafka：

1. 在 Sentinel 主界面，单击**储存** > **可缩放储存** > **高级配置** > **Kafka**。
2. 添加以下属性，并将其设置为 true：

   pause.events.tokafka
3. 单击**保存**。

Change Guardian 集成

Sentinel 与 Change Guardian 4.2 及其更高版本兼容。要从 Change Guardian 接收事件，您必须先将 Change Guardian 服务器、代理和策略编辑器升级到 4.2 或更高版本，以确保升级后 Sentinel 仍可从 Change Guardian 接收事件。

28 升级 Sentinel 传统安装

升级 Sentinel

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 “《 Sentinel 管理指南》”中的*备份和恢复数据*。
2. （条件）如果您已在 server.xml、collector_mgr.xml 或 correlation_engine.xml 文件中自定义了配置设置，请确保您已经创建了名为 obj-component id 的相应属性文件来确保升级后保留此自定义。有关详细信息，请参见“《 Sentinel 管理指南》”中的*在 XML 文件中维持自定义设置*。
3. 从下载网站下载最新的安装程序。
4. 以 root 身份登录要升级 Sentinel 的服务器。
5. 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>*。
6. 将目录更改为抽取安装文件的位置。
7. 指定以下命令来升级 Sentinel：

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

   最终用户许可证协议将以选定的语言显示。
9. 阅读最终用户许可证协议，输入 yes 或 y 接受许可证，然后继续安装。
10. 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 程序包。该安装完成可能需要几秒钟的时间。
11. 清除 Web 浏览器超速缓存，以查看最新的 Sentinel 版本。
12. 在客户端计算机上清除 Java Web Start 超速缓存，以便使用最新版本的 Sentinel 应用程序。

    可以通过使用 javaws -clearcache 命令或 Java Control Center 来清除 Java Web Start 超速缓存。有关详细信息，请参见 http://www.java.com/en/download/help/plugin_cache.xml。

13 （有条件）如果 PostgreSQL 数据库升级到一个主版本（如 8.0 到 9.0 或者 9.0 到 9.1），请从PostgreSQL数据库清除旧PostgreSQL文件。有关PostgreSQL数据库是否已升级的信息，请参见Sentinel 发行说明。

13a 切换到 novell 用户。

```
su novell
```

13b 浏览至 bin 文件夹：

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

13c 使用以下命令删除所有旧的 PostgreSQL 文件：

```
./delete_old_cluster.sh
```

14 要升级 Collector Manager 系统和 Correlation Engine 系统，请参见升级 Collector Manager 或 Correlation Engine（第 144 页）。

15 （有条件）如果使用 Kerberos 鉴定，请在 Java 运行时环境中启用 AES256，因为在升级过程中，默认文件代替了 java 文件夹。要在 Java 运行时环境中启用 AES256，需完成下列步骤：

15a 从下列位置下载 Java Cryptography Extension (JCE) 8：http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

15b 将两个 *.jar 文件解压缩并将其复制到 /opt/novell/sentinel/jdk/jre/lib/security directory。

15c （有条件）如果在 HA 环境中运行 Sentinel，在群集中的所有节点中重复这些步骤。

15d 重启动 Sentinel。

以非 root 用户身份升级 Sentinel

如果组织策略不允许以 root 用户身份运行完整的 Sentinel 升级，则可以以另一个用户的身份升级 Sentinel。在此升级过程中，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升级 Sentinel。

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 “《 Sentinel 管理指南》”中的 *备份和恢复数据*。

2 （条件）如果您已在 server.xml、collector_mgr.xml 或 correlation_engine.xml 文件中自定义了配置设置，请确保您已经创建了名为 obj-component id 的相应属性文件来确保升级后保留此自定义。有关详细信息，请参见“《 Sentinel 管理指南》”中的 *备份和恢复数据*。

3 可以从 下载网站下载这些安装文件。

4 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>*。

5 以 root 身份登录要升级 Sentinel 的服务器。

6 从 Sentinel 安装文件中提取 squashfs RPM。

7 在 Sentinel 服务器上安装 squashfs。

```
rpm -Uvh <install_filename>
```

8 指定以下命令以更改为新创建的非根 novell 用户：novell：

su novell

9 （有条件）要执行交互式升级，请执行以下操作：

9a 指定以下命令：

```
./install-sentinel
```

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

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

9b 继续执行步骤 11。

10 （有条件）要执行无提示升级，请指定以下命令：

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

将使用储存在响应文件中的值继续安装。Sentinel 升级已完成。

11 指定要用于升级的语言编号。

最终用户许可证协议将以选定的语言显示。

12 阅读最终用户许可证协议并输入 yes 或 y 接受此许可证协议，然后继续升级。

升级将开始安装所有的 RPM 程序包。该安装完成可能需要几秒钟的时间。

13 清除 Web 浏览器超速缓存，以查看最新的 Sentinel 版本。

14 在客户端计算机上清除 Java Web Start 超速缓存，以便使用最新版本的 Sentinel 应用程序。

可以通过使用 javaws -clearcache 命令或 Java Control Center 来清除 Java Web Start 超速缓存。有关详细信息，请参见 http://www.java.com/en/download/help/plugin_cache.xml。

15 （有条件）如果 PostgreSQL 数据库升级到一个主版本（如 8.0 到 9.0 或者 9.0 到 9.1），请从 PostgreSQL数据库清除旧PostgreSQL文件。有关PostgreSQL数据库是否已升级的信息，请参见 Sentinel 发行说明。

15a 切换到 novell 用户。

```
su novell
```

15b 浏览至 bin 文件夹：

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c 使用以下命令删除所有旧的 postgreSQL 文件：

```
./delete_old_cluster.sh
```

16 （有条件）如果使用 Kerberos 鉴定，请在 Java 运行时环境中启用 AES256，因为在升级过程中，默认文件代替了 java 文件夹。要在 Java 运行时环境中启用 AES256，需完成下列步骤：

16a 从下列位置下载 Java Cryptography Extension (JCE) 8：http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

16b 将两个 *.jar 文件解压缩并将其复制到 /opt/novell/sentinel/jdk/jre/lib/security directory。

16c （有条件）如果在 HA 环境中运行 Sentinel，在群集中的所有节点中重复这些步骤。

16d 重启动 Sentinel。

升级 Collector Manager 或 Correlation Engine

使用以下步骤升级 Collector Manager 或 Correlation Engine：

1. 备份您的配置，然后创建 ESM 导出。

   有关详细信息，请参见“《 Sentinel 管理指南》”中的*备份和恢复数据*。
2. 以拥有管理员角色的用户身份导航到 **Sentinel 主界面**。
3. 选择**下载**。
4. 在“Collector Manager 安装程序”部分中，单击**下载安装程序**。
5. 将安装程序文件保存在各自的 Collector Manager 或 Correlation Engine 服务器中。
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 Collector Manager：

   ```
   ./install-cm
   ```

   对于 Correlation Engine：

   ```
   ./install-ce
   ```
9. 按照屏幕上的指导完成安装。
10. （有条件）对于自定义安装，请运行以下命令以在 Sentinel 服务器、Collector Manager 和 Correlation Engine 之间同步配置：

    ```
    /opt/novell/sentinel/setup/configure.sh
    ```

升级操作系统

此版本的 Sentinel 包含一组可在操作系统升级过程中使用的命令。这些命令可确保升级操作系统后 Sentinel 能够正常工作。

注释： 升级操作系统之前，您必须先升级 Sentinel。

使用以下步骤来升级您的操作系统：

1. 在要升级操作系统的 Sentinel 服务器上，以下列用户身份之一登录：
   - root 用户
   - 非 root 用户
2. 打开命令提示符，并转到提取 Sentinel 安装文件的目录。
3. 停止 Sentinel 服务：

   rcsentinel stop
4. （有条件）如果操作系统升级之前 Sentinel 处于 FIPS 模式，必须通过运行以下命令手动升级 NSS 数据库文件：

   certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X

   按照屏幕指导升级 NSS 数据库。

授予 novell 用户以下文件的全部权限：

```
cert9.db
key4.db
pkcs11.txt
```

5 升级您的操作系统。

6 （有条件）如果使用 Mozilla Network Security Services (NSS) 3.29，将不安装两个依赖 RPM 文件 libfreebl3-hmac 和 libsoftokn3-hmac。手动安装下列 RPM 文件：libfreebl3-hmac 和 libsoftokn3-hmac。

7 （有条件）对于 RHEL 7.*x*，运行以下命令检查 RPM 数据库中是否有错误：

rpm -qa --dbpath <*install_location*>/rpm | grep novell

示例：# rpm -qa --dbpath /custom/rpm | grep novell

7a 如有错误，请运行以下命令修复错误：

rpm --rebuilddb --dbpath <*install_location*>/rpm

示例：# rpm --rebuilddb --dbpath /custom/rpm

7b 运行步骤 7 中提到的命令以确保没有错误。

8 对以下组件重复执行此过程：

- Collector Manager
- Correlation Engine
- NetFlow Collector Manager

9 重新启动 Sentinel 服务：

rcsentinel 重启动

此步骤对 Sentinel HA 不适用。

29 升级 Sentinel 设备

此章内容将指导您完成 Sentinel 设备升级。您可以选择在不升级 SLES 操作系统的情况下升级 Sentinel，或同时升级 Sentinel 和 SLES 操作系统。因为 Sentinel 8.2 设备包括 SLES 12 SP 3，SLES 11 更新通道现已弃用，SUSE 结束对 SLES 11 的一般支持时将去除此通道。因此，您应该升级到 Sentinel 8.2 设备，其中包括 SLES 12 SP3 操作系统以继续接收操作系统更新。升级操作系统之前，您需要升级 Sentinel。

升级 Sentinel

通过设备更新通道升级 Sentinel

可使用 Zypper 升级 Sentinel。Zypper 是一个命令行程序包管理器，您可以用来执行设备交互升级。在需要用户交互完成升级的情况下（如终端用户许可证协议更新），您必须使用 Zypper 升级 Sentinel 设备。

要通过设备更新通道升级设备：

1. 备份您的配置，然后创建 ESM 导出。

   有关详细信息，请参见“《 Sentinel 管理指南》”中的*备份和恢复数据*。
2. （条件）如果您已在 server.xml、collector_mgr.xml 或 correlation_engine.xml 文件中自定义了配置设置，请确保您已经创建了名为 obj-component id 的相应属性文件来确保升级后保留此自定义。有关详细信息，请参见“《 Sentinel 管理指南》”中的*在 XML 文件中维持自定义设置*。
3. 以 root 用户身份登录到设备控制台。
4. 运行以下命令：

   ```
   /usr/bin/zypper patch
   ```
5. （有条件）如果安装程序显示一则讯息，要求您必须解析OpenSSH包的依赖项，请输入相应的选项，以降级 OpenSSH 包。
6. （有条件）如果安装程序显示一则讯息，指示 ncgOverlay 体系结构发生更改，请输入相应的选项，以接受体系结构更改。
7. （有条件）如果安装程序显示一则讯息，要求您必须解析某些设备包的依赖项，请输入相应的选项，以卸载依赖项包。
8. 输入 Y 以继续操作。
9. 输入 yes 以接受许可证协议。
10. 重新启动 Sentinel 设备。

11 （有条件）如果·Sentinel·安装在自定义端口上或·Collector·Manager·或 Correlation Engine 处于 FIPS 模式下，则运行以下命令：

```
/opt/novell/sentinel/setup/configure.sh
```

12 清除 Web 浏览器超速缓存，以查看最新的 Sentinel 版本。

13 在客户端计算机上清除 Java Web Start 超速缓存，以便使用最新版本的 Sentinel 应用程序。

可以通过使用 javaws -clearcache 命令或 Java Control Center 来清除 Java Web Start 超速缓存。有关详细信息，请参见 http://www.java.com/en/download/help/plugin_cache.xml。

14 （有条件）如果 PostgreSQL 数据库升级到一个主版本（如 8.0 到 9.0 或者 9.0 到 9.1），请从 PostgreSQL数据库清除旧PostgreSQL文件。有关PostgreSQL数据库是否已升级的信息，请参见 Sentinel 发行说明。

14a 切换到 novell 用户。

```
su novell
```

14b 浏览至 bin 文件夹：

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

14c 使用以下命令删除所有旧的 postgreSQL 文件：

```
./delete_old_cluster.sh
```

15 （有条件）要升级 Collector Manager 或 Correlation Engine，请执行步骤 3 到步骤 11。

16 （有条件）如果使用 Kerberos 鉴定，请在 Java 运行时环境中启用 AES256，因为在升级过程中，默认文件代替了 java 文件夹。要在 Java 运行时环境中启用 AES256，需完成下列步骤：

16a 从下列位置下载 Java Cryptography Extension (JCE) 8：http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

16b 将两个 *.jar 文件解压缩并将其复制到 /opt/novell/sentinel/jdk/jre/lib/security directory。

16c 重启动 Sentinel。

17 （有条件）如果在 HA 环境中运行 Sentinel，在群集中的所有节点中重复这些步骤。

18 （有条件）要升级操作系统，请参见升级操作系统（第 149 页）

19 重启动 Sentinel。

通过使用 SMT 升级 Sentinel

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，请参见使用 SMT 配置设备（第 101 页）。

2 备份您的配置，然后创建 ESM 导出。

有关详细信息，请参见“《 Sentinel 管理指南》”中的*备份和恢复数据*。

3 （条件）如果您已在 server.xml、collector_mgr.xml 或 correlation_engine.xml 文件中自定义了配置设置，请确保您已经创建了名为 obj-component id 的相应属性文件来确保升级后保留此自定义。有关详细信息，请参见“《 Sentinel 管理指南》”中的*在 XML 文件中维持自定义设置*。

4 以 root 用户身份登录到设备控制台。

5 刷新储存库以进行升级：

```
zypper ref -s
```

6 检查是否已启用设备以进行升级：

```
zypper lr
```

7 （可选）检查设备的可用更新：

```
zypper lu
```

8 （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>
```

9 更新设备：

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

10 重新启动设备。

```
rcsentinel restart
```

11 （有条件）如果·Sentinel·安装在自定义端口上或·Collector·Manager·或 Correlation Engine 处于 FIPS 模式下，则运行以下命令：

```
/opt/novell/sentinel/setup/configure.sh
```

12 （有条件）要升级 Collector Manager 或 Correlation Engine，请执行步骤 4 到步骤 11。

13 （有条件）如果使用 Kerberos 鉴定，请在 Java 运行时环境中启用 AES256，因为在升级过程中，默认文件代替了 java 文件夹。要在 Java 运行时环境中启用 AES256，需完成下列步骤：

13a 从下列位置下载 Java Cryptography Extension (JCE) 8：http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

13b 将两个 *.jar 文件解压缩并将其复制到 /opt/novell/sentinel/jdk/jre/lib/security directory。

13c 重启动 Sentinel。

14 （有条件）如果在 HA 环境中运行 Sentinel，在群集中的所有节点中重复这些步骤。

15 （有条件）要升级操作系统，请参见升级操作系统（第 149 页）。

16 重启动 Sentinel。

升级操作系统

升级 Sentinel 后必须升级操作系统。升级操作系统后，必须将设备配置为利用新的 Sentinel Appliance Manager 功能。Sentinel Appliance Manager 提供基于 Web 的简单用户界面，可帮助您配置和管理设备。它取代了现有的 WebYast 功能。

要升级操作系统和配置设备：

1 升级 Sentinel。有关详细信息，请参见升级 Sentinel（第 147 页）。

2 停止 Sentinel 服务：

```
rcsentinel stop
```

3 （有条件）如果操作系统升级之前 Sentinel 处于 FIPS 模式，必须通过运行以下命令手动升级 NSS 数据库文件：

certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X

按照屏幕指导升级 NSS 数据库。

授予 novell 用户以下文件的全部权限：

```
cert9.db
key4.db
pkcs11.txt
```

4 （有条件）如果使用 Mozilla Network Security Services (NSS) 3.29，将不安装两个依赖 RPM 文件 libfreebl3-hmac 和 libsoftokn3-hmac。手动安装下列 RPM 文件：libfreebl3-hmac 和 libsoftokn3-hmac。

5 从 Micro Focus Patch Finder 网站下载 SLES 12 SP3 安装程序以及升级后实用程序。同时，为 Sentinel HA 下载 SLES 12 SP3 HA 文件。

6 按安装提示升级操作系统。对于 Sentinel HA，当提示安装其他外接式附件产品时，选择您存放下载的 SLES 12 SP3 HA 文件的位置并继续进行升级。

有关升级至 SLES 12 SP3 的更多信息，请参见 SLES 文档。

7 升级过程中，SLES 将 /etc/sysctl.conf 文件重命名为 /etc/sysctl.conf.rpmsave（作为备份）并创建一个 new /etc/sysctl.conf 文件。升级后将 /etc/sysctl.conf.rpmsave 文件的内容复制到 /etc/sysctl.conf 文件。打开 sysctl.conf 文件并搜索 # Added by sentinel vm.max_map_count。将此设置移到下一行，如下所示：

将

```
net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

更改为

```
net.core.wmem_max = 67108864
# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

8 （有条件）对于 Sentinel HA，需完成下面各部分中提到的步骤：

- 配置 iSCSI 目标（第 196 页）
- 配置 iSCSI 发起程序（第 196 页）
- 配置 HA 群集（第 197 页）

9 要配置设备，请从命令提示符运行升级后实用程序：

9a 将文件解压缩：

tar -xvf <*升级后实用程序安装程序文件名*>.tar.gz

9b 切换到提取实用程序的目录：

cd <*升级后实用程序安装程序文件名*>

9c 要配置设备，请运行以下脚本：

./appliance_SLESISO_post_upgrade.sh

注释： 不要远程运行此脚本，因为此脚本涉及网络重新配置。

9d 按照屏幕指导完成配置。

此脚本将重新配置安装的软件包并配置软件包以管理设备.

10 使用您现有的注册代码再次注册更新，来接收 Sentinel 和最新操作系统更新。有关详细信息，请参见注册更新（第 99 页）。

30 升级后配置

本章包括升级后配置。

确保 Elasticsearch 中数据的安全

Sentinel 利用了基于浏览器的分析和搜索仪表板 Kibana，可以帮助您在仪表板中可视化事件和警报。Sentinel 在 Elasticsearch 中储存和索引警报。您也可以将 Sentinel 配置为在 Elasticsearch 中储存和索引事件，以利用事件可视化功能。Sentinel 仪表板访问 Elasticsearch 中的数据，以在仪表板中显示事件和警报。为确保仪表板仅显示用户角色有权查看的数据并阻止 Elasticsearch 中出现未经授权访问数据的情况，必须安装 Elasticsearch 安全插件。有关详细信息，请参见确保 Elasticsearch 中数据的安全（第 75 页）。

配置事件可视化

Sentinel 提供以图表、表格和地图形式显示数据的事件可视化。这些可视化使得可视化和分析大量数据，如事件、IP 流事件及警报变得更加容易。您也可以创建自己的可视化和仪表板。

Sentinel 利用了基于浏览器的分析和搜索仪表板 Kibana，可以帮助您搜索和可视化事件。Kibana 访问可视化数据储存 (Elasticsearch) 中的数据，以在仪表板中显示事件。默认情况下，Sentinel 包含一个 Elasticsearch 节点。必须启用事件可视化，才能在 Elasticsearch 中存储和索引事件。有关详细信息，请参见配置“可视化数据储存”（第 42 页）。

注释： 升级至 Sentinel 8.2 后，使用 Kibana 的一些 Sentinel 仪表板无法装载。这是因为 Sentinel 8.2 中升级了 Elasticsearch 和 Kibana 版本，现有 Kibana 索引文件与 Elasticsearch 和 Kibana 升级版本不兼容。要修复此问题，必须手动删除现有 Kibana 索引文件并重创建新的 Kibana 索引文件。有关更多信息，请参见知识库文章 7022736。

配置 IP 流数据集合

Sentinel 现在使用通过收集 IP 流数据和 NetFlow 数据帮助您监视企业网络的 ArcSight SmartConnector。SmartConnector 将 IP 流数据收集为事件，这将允许您：

- 使用现有 Collector Manager 收集 IP 流数据。您将不再需要 NetFlow Collector Manager 收集 NetFlow 数据。
- 在 Sentinel 的多个方面使用 IP 流数据，例如可视化、事件路由选择、数据联合、报告和关联。
- 向 IP 流数据应用数据保留策略，这样您储存数据的时长可按需设置。

升级 Sentinel 后，您可以继续使用 NetFlow 功能或选择配置 IP 流数据集合。但是，可使用 IP 流数据集合和可视化功能后，之前可用的 NetFlow 功能，包括 NetFlow 视图现已弃用，将来将去除这些功能，以优化用户体验。

启用 IP 流数据集合后：

- IP 流数据将收集为事件，因此应为 EPS 计数考虑此类事件。
- 您将失去启用 IP 流前收集的所有 NetFlow 数据。弃用的 NetFlow 系统保留期最长为 3 天。您可以按需要时长保留 IP 流事件。
- 您无法将启用 IP 流之前收集的 NetFlow 数据迁移到 IP 流功能。
- 您无法恢复配置，除非重新安装 Sentinel。
- 您将登出 Sentinel 主仪表板并需要重新登录。

要配置 IP 流数据集合：

1. 安装和配置 ArcSight SmartConnector。配置时，确保配置收集 IP 流数据的相关 SmartConnector。

   关于配置 SmartConnector 的相关信息，请参见 Sentinel 插件网站中的 Generic Universal CEF Collector（一般通用 CEF 收集器）文档。
2. 在 **Sentinel 主仪表板** > **集合** > **IP 流**中，选择**收集 IP 流数据**，然后单击**启用**。

注释： 由于现在 IP 流事件发送至 Collector Manager，您将不再需要使用 NetFlow Collector Manager。因此，可卸装任意现有 NetFlow Collector Manager。有关详细信息，请参见卸载 NetFlow Collector Manager（第 210 页）。

Sentinel Scalable Data Manager 升级后配置

- 安装 Elasticsearch 安全插件（第 155 页）
- 在 YARN 中更新 Spark 应用程序（第 155 页）
- 启用 Sentinel 功能（第 156 页）
- 在 Sentinel Scalable Data Manager 中更新仪表板和可视化项（第 156 页）

安装 Elasticsearch 安全插件

除外部 Elasticsearch 节点外，Sentinel 现在还默认包含一个用于数据可视化的本地 Elasticsearch 节点。因此，您必须为本地 Elasticsearch 安装一个 Elasticsearch 插件。 有关详细信息，请参见安装 Elasticsearch 安全插件（第 76 页）。

由于 Sentinel 中使用的 Elasticsearch 和 Kibanaare 得到升级，您必须重新部署现有 Elasticsearch 节点的所有 Elasticsearch 安全插件。有关重新部署 Elasticsearch 安全插件的更多信息，请参见部署 Elasticsearch 安全插件（第 79 页）。

在 YARN 中更新 Spark 应用程序

Sentinel 升级期间，也会更新一些 Spark 应用程序文件。您必须通过执行以下步骤重新提交含这些更新文件的 Spark 应用程序：

1. 以novell用户身份登录到SSDM服务器并将文件复制到安装了HDFS NameNode的Spark历史服务器：

   cd /etc/opt/novell/sentinel/scalablestore

   scp SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties log4j.properties manage_spark_jobs.sh root@<*hdfs_node*>:<*destination_directory*>

   其中，<*destination_directory*> 是您想要放置复制文件的目录。此外，确保 hdfs 用户具有此目录的全部权限。

2. 以 root user 身份登录到 <*hdfs_node*> 服务器并将复制文件所有权改为 hdfs 用户：

   cd <*destination_directory*>

   chown hdfs SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties log4j.properties manage_spark_jobs.sh

   向 manage_spark_jobs.sh 脚本指派可执行许可权限。

3. 确保 Spark 作业已处理完所有数据：

   转到YARN ResourceManager Web用户界面并查看每个Sentinel Spark应用程序。当通过Kafka处理了所有数据后，Spark Streaming 应用程序数据将显示输入率降为零。

4. 运行以下命令停止数据处理：

   。/manage_spark_jobs.sh stop

5. 清除数据处理检查点：

   ```
   sudo -u hdfs hadoop fs -rm -R -skipTrash  /spark/checkpoint
   ```

   其中 /spark/checkpoint 是检查点目录。

6. 运行以下脚本重新提交 Spark 作业：

   。/manage_spark_jobs.sh start

   上述命令完成提交过程需要一些时间。

7. （可选）运行以下命令以校验提交的 Spark 作业的状态：

   。/manage_spark_jobs.sh status

8. 继续将事件转发到 Kafka 以便 Spark 开始处理事件：

   8a 在 Sentinel 主界面，单击**储存** > **可缩放储存** > **高级配置** > **Kafka**。

   8b 将以下属性设置为 false：

pause.events.tokafka

8c 单击**保存**。

启用 Sentinel 功能

从 SSDM 8.0.*x.x* 升级之后，Sentinel 8.1 及更高版本中添加的某些 Sentinel 功能默认情况下不可用。您必须在 /etc/opt/novell/sentinel/config/ui-configuration.properties 文件中手动启用这些功能。

1. 以 novell 用户身份登录到 Sentinel 服务器。
2. 打开 /etc/opt/novell/sentinel/config/ui-configuration.properties 文件。
3. 将以下属性改为 false：

```
alerts.hideUI
solutionDesigner.launcher.hideUI
correlation.hideUI
scc.configurations.solutionPacks.hideUI
people.hideUI
permission.knowledgeBase.hideUI
scc.menuBarItem.toolsMenu.hideUI
scc.toolBarItem.peopleBrowser.hideUI
integration.hideUI
```

4. 刷新 Sentinel 浏览器。

在 Sentinel Scalable Data Manager 中更新仪表板和可视化项

升级 SSDM后必须更新仪表板和可视化，这样才会应用仪表板和可视化最新版本中所包含的增强功能。

升级 SSDM 后，在默认情况下，将不更新仪表板和可视化项。但是，您可以在升级后手动更新这些内容。您可以通过以下方式更新仪表板和可视化项：删除现有的仪表板和可视化项，然后运行 load_kibana_data.sh 脚本，该脚本将安装最新的仪表板和可视化项。

重要： 在更新仪表板和可视化项时，可能已在仪表板和可视化项中完成的自定义项将会丢失。

要更新仪表板和可视化项，请执行以下操作：

1. 登录到 SSDM Web 界面，然后转到“事件可视化”。
2. 在“事件可视化”中，转到**设置** > **对象** > **仪表板**。
3. 选择要更新的仪表板，然后单击**删除**。
4. 单击**可视化项**。选择要更新的可视化项，然后单击**删除**。
5. 注销 SSDM Web 界面。
6. 以 novell 用户身份登录 SSDM 服务器。
7. 转到 /opt/novell/sentinel/bin 目录。
8. 使用以下命令运行 load_kibana_data.sh：

   。/load_kibana_data.sh http://<ip address>:<port>> <alerts/events/misc>

   例如：

   。/load_kibana_data.sh http://127.0.0.1:9200 alerts

./load_kibana_data.sh http://127.0.0.1:9200 events

9 登录到 SSDM Web 界面，然后转到“事件可视化”，以查看更新的仪表板和可视化项。

添加 JDBC DB2 驱动程序

升级 Sentinel 后，通过执行以下步骤，添加正确的 JDBC 驱动程序并将其配置为数据收集和数据同步：

1 为 /opt/novell/sentinel/lib 文件夹中的 DB2 数据库版本复制正确版本的 IBM DB2 JDBC 驱动程序 (db2jcc-*.jar)。

2 确保您设置了驱动程序文件的必要所有权和许可权限。

3 配置此驱动程序，以便进行数据收集。有关详细信息，请参见数据库连接器文档。

在 Sentinel 设备中配置数据联合属性

升级 Sentinel 设备后执行以下步骤，以便数据联合不会在配置有两个或更多 NIC 的环境中显示任何错误：

1 在授权请求者服务器中，将以下属性添加在 /etc/opt/novell/sentinel/config/configuration.properties 文件中，如下所示：

sentinel.distsearch.console.ip=<授权请求者的 IP 地址之一>

2 在数据源服务器中，将以下属性添加在 /etc/opt/novell/sentinel/config/configuration.properties 文件中，如下所示：

sentinel.distsearch.target.ip=<数据源的 IP 地址之一>

3 重启动 Sentinel：

rcsentinel 重启动

4 登录到授权请求者服务器，然后单击集成。如果您想添加的数据源已经存在，请将其删除，并使用您在步骤 2 中指定的 IP 地址之一重新进行添加。

同样，使用您在步骤 1 中指定的 IP 地址添加授权请求者。

注册 Sentinel 设备以进行更新

如果已升级操作系统，则必须重新注册 Sentinel 设备才能接收 Sentinel 和最新的操作系统更新。可以使用现有的注册密钥重新注册更新。要注册设备，请参见注册更新（第 99 页）。

更新外部数据库以进行数据同步

从 Sentinel 8.x 开始，“讯息 (msg)”事件字段的大小已从 4000 增至 8000 个字符，以使该字段可容纳更多信息。

如果您已在早期版本的 Sentinel 中创建将“讯息 (msg)”事件字段同步到外部数据库的数据同步策略，则必须根据需要增加外部数据库中相应映射列的大小。

注释： 仅当您将早期版本的 Sentinel 升级到 8.x 时，以上步骤才适用。

在多因子鉴定模式下重新鉴定 Sentinel

在 MFA 模式下升级 Sentinel 服务器时，现有 NetFlow Collector Manager 不会自动重新鉴定到 Sentinel 服务器。您必须执行下列步骤以手动重新鉴定 NetFlow Collector Manager 到 Sentinel 服务器。

要在 MFA 模式下重新鉴定 Sentinel：

1. 登录到 NetFlow Collector Manager 计算机。
2. 转到 /opt/novell/sentinel/setup。
3. 运行 configure.sh 脚本。

   系统将提示您登录 Sentinel 服务器。
4. 指定 LDAP 用户名和口令。
5. 提供 Sentinel 客户端 ID 和 Sentinel 客户端机密。

   要检索 Sentinel 客户端 ID 和 Sentinel 客户端机密，请前往以下 URL：

   https://Sentinel_FQDN:port/SentinelAuthServices/oauth/clients

   其中：

   - Sentinel_FQDN 是 Sentinel 服务器的完全限定的域名 (FQDN)。

     例如 abc.netiq.com

     其中 abc 是 Sentinel 服务器主机名，netiq.com 是域名。
   - Port 是 Sentinel 使用的端口（通常为 8443）。

   指定的 URL 将使用当前 Sentinel 会话检索 Sentinel 客户端 ID 和 Sentinel 客户端机密。

31 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（包括解决方案包）将不断上载到 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 从传统储存迁移数据

从带有传统储存的 Sentinel 迁移数据，您不仅利用了已有的 Sentinel 数据，还能让您已经投入的时间再次发挥价值。要从带有传统储存的 Sentinel 迁移数据，源 Sentinel 服务器和目标 Sentinel 服务器的 Sentinel 版本必须相同。例如，如果想要将数据从 Sentinel 8.1（来源）迁移到 Sentinel 8.2（目标），您必须首先将 Sentinel 8.1 升级到 Sentinel 8.2，然后再开始数据迁移过程。

此部分介绍将现有数据迁移到所需数据储存组件的相关信息。

32 将数据迁移至可缩放储存

您可能有一个或多个带有传统储存的 Sentinel 服务器。您需要采用的数据迁移过程取决于想要设置和维护 Sentinel 部署的方式。

表 32-1 *Sentinel 部署的数据迁移过程*

Sentinel 部署	迁移过程
您有一个 Sentinel 服务器且计划将现有的 Sentinel 服务器升级到可缩放储存。	升级 Sentinel 服务器并启用可缩放储存后，将事件数据和原始数据从传统储存迁移到可缩放储存。 有关详细信息，请参见 第 34 章“迁移数据”（第 169 页）。
您只有一个带有传统储存的 Sentinel 服务器，且想要将另一个 Sentinel 服务器设置为可缩放储存，以便使用 Sentinel 中的所有功能。	使用备份和恢复实用程序将带有传统储存的 Sentinel 中的数据迁移到带有可缩放储存的 Sentinel。 有关使用备份和恢复实用程序的详细信息，请参见《*Sentinel 管理指南*》中的“备份和恢复数据”。
您有一个多层安装程序，其中有多个 Sentinel 服务器，您打算设置新的 Sentinel 服务器或将一个现有服务器用于可缩放储存，您需要迁移事件数据、原始数据以及配置数据。	在多层安装程序中，您可以指定一个拥有大部分数据的传统 Sentinel 服务器，然后使用备份和恢复实用程序迁移数据。 如果您需要备份剩余 Sentinel 服务器中的数据，您必须使用本部分后面介绍的不同方法迁移来自这些服务器的配置数据、事件数据和原始数据。您还必须手动重新创建部分配置。 您无法使用备份和恢复实用程序迁移多个服务器的数据，因为恢复数据时，实用程序会覆盖现有数据。例如，如果您已恢复服务器 A 的数据，然后尝试恢复服务器 B 的数据，该实用程序会覆盖服务器 A 中已恢复的数据。 因此，要了解所涉及的数据迁移过程，按相同顺序按下列部分中的说明进行操作： ◆ 您可以迁移的数据 ◆ 迁移配置数据 ◆ 迁移数据 ◆ 迁移警报和 NetFlow 数据 ◆ 更新 Sentinel 客户端 ◆ 导入 ESM 配置

您可以迁移的数据

您可以迁移事件数据、原始数据和部分配置数据。您必须手动重新创建剩余配置，这些配置不可迁移。

表 32-2 *您可以迁移的配置以及需要重新创建的配置*

您可以迁移的配置	需要重新创建的配置
◆ 关联规则 ◆ 操作 ◆ 映射 ◆ 过滤器 ◆ 威胁传递 ◆ ESM 配置 ◆ 除知识库数据以外的警报 ◆ NetFlow	◆ 租户、角色、用户和 LDAP 配置 ◆ 事件和警报路由选择规则 ◆ 数据和警报保留策略 ◆ 仪表板 ◆ 实时视图 ◆ 身份信息 ◆ 传递配置 ◆ 操作和集成商插件配置 ◆ 安全性配置

迁移配置数据

迁移事件数据之前，您必须首先迁移配置数据到 Sentinel 目标服务器。您可以使用 Solution Designer 和事件源管理 (ESM) 中的导入导出选项备份部分配置。您必须手动重新创建其余无法备份或导出的配置数据。

- 在源服务器上备份数据（第 164 页）
- 在目标服务器中恢复数据（第 165 页）

在源服务器上备份数据

您必须通过 Sentinel 中的多个选项备份必要数据。

- 使用解决方案包（第 165 页）
- 使用 ESM 中的导出配置选项（第 165 页）

使用解决方案包

使用 Solution Designer 在源服务器上备份以下配置：

表 32-3 配置数据

	数据	注释
❒	关联规则	为每个 Correlation Engine 创建单独控制，这样您可以将这些规则单独迁移到特定 Correlation Engine。
❒	操作	您只能备份 JavaScript 操作，无法备份旧操作（如动态列表及创建事件）。
❒	事件丰富	Sentinel 还可以备份事件字段的相关映射。因此，在恢复事件丰富数据之后，不需要重新创建相关映射。
❒	过滤器	备份所有自定义过滤器。
❒	传递	解决方案包仅备份传递插件，不备份插件配置。

关于备份 Solution Designer 中数据的信息，请参见*《Sentinel 管理指南》*中的“创建解决方案包”。

使用 ESM 中的导出配置选项

使用 ESM 中的导出配置选项备份数据集合配置。有关更多信息，请参见*《Sentinel 管理指南》*中的“导出配置”。

在目标服务器中恢复数据

- 安装解决方案包中的配置数据（第 165 页）
- 手动重新创建配置（第 165 页）

安装解决方案包中的配置数据

使用 Solution Designer 导入您在源服务器上备份的配置数据。有关更多信息，请参见*《Sentinel 管理指南》*中的“安装解决方案数据包中的内容”。

如果对象（如过滤器、操作和关联规则）的名称有重复，请重新命名。默认情况下，当您在目标服务器上导入过滤结果时，所有过滤器都为“公共”。手动为每个过滤器重指派许可权限。

手动重新创建配置

除了从解决方案包导入的配置数据，您必须手动重新创建所有其他配置。关于您需要手动重新创建的配置的更多信息，请参见 表 32-2“您可以迁移的配置以及需要重新创建的配置”（第 164 页）。

迁移事件数据和原始数据

要迁移事件数据和原始数据，请参见迁移数据。

迁移警报和 NetFlow 数据

您可以使用备份和恢复实用程序，将警报和 NetFlow 数据从源服务器迁移到目标服务器。对于警报，该实用程序会恢复触发警报的事件。但是，该程序不会恢复相关的关联规则以及知识库信息。

使用以下命令备份和恢复警报及 NetFlow 数据：

```
For backing up:
./backup_util.sh -i

For restore:
./backup_util.sh -m restore -f <backup_file_path>
```

对于警报和 NetFlow 数据，您可以选择覆盖或追加现有数据。选择所需的选项。

尽管上述命令备份和恢复安全智能数据，但您无法使用该数据，因为安全智能不可用于 SSDM。

关于使用备份和恢复实用程序的详细信息，请参见*《Sentinel 管理指南》*中的“备份和恢复数据”。

更新 Sentinel 客户端

您必须更新所有现有 Collector Manager、Correlation Engine 和 NetFlow Collector Manager 配置，这样它们就可以与目标 Sentinel 服务器通信。有关更多信息，请参见*《Sentinel 管理指南》*中的“更新 Sentinel 客户端”。

注释： 尽管您已从源服务器迁移了事件数据，但必须重新运行数据迁移脚本以迁移可能在数据迁移过程中或数据迁移过程之后到达的所有事件数据。有关详细信息，请参见 第 34 章“迁移数据”（第 169 页）。

导入 ESM 配置

使用 ESM 用户界面中的导入配置选项，导入您在源服务器上使用的数据集合配置。有关更多信息，请参见*《Sentinel 管理指南》*中的“导入配置”。

33 将数据迁移到 Elasticsearch

默认情况下，Sentinel 将数据储存在基于文件的传统储存中并在 Sentinel 服务器上本地索引数据。启用事件可视化后，除基于文件的传统储存外，Sentinel 还在 Elasticsearch 中储存和索引数据。仪表板仅显示启用事件可视化后处理的事件。要查看基于文件的储存中的现有事件，必须将数据从基于文件的储存中迁移到 Elasticsearch。要将数据迁移至 Elasticsearch，请参见第 34 章“迁移数据”（第 169 页）。

34 迁移数据

您可以使用 data_uploader.sh 脚本将数据迁移到下列任意一个数据储存组件：

- **Kafka：** 您可以将事件数据和原始数据迁移至 Kafka。针对事件数据和原始数据单独运行脚本。脚本将数据迁移至 Kafka 主题。

  您可以指定自定义，例如在迁移过程中压缩数据、分批发送数据等。要指定这些自定义，请创建属性文件，并以健值格式添加所需的属性。比如，您可以按下列方式添加属性：

  compression.type=lz4

  batch.size=20000

  关于 Kafka 属性的信息，请参见 Kafka 文档。自行设置属性和属性值，因为脚本不会验证这些属性。

  注释： 确保 Sentinel 服务器能够将所有 Kafka 中介程序主机名解析对整个 Kafka 群集有效的 IP 地址。如果 DNS 未设置为启用此功能，可将 Kafka 中介程序主机名添加到 Sentinel 服务器的 /etc/hosts 文件中。

- **Elasticsearch：** 您可以仅将事件数据迁移至 Elasticsearch。迁移数据前，确保已启用事件可视化。有关详细信息，请参见启用事件可视化（第 115 页）。

脚本传输您指定日期范围（起止日期）内的数据。运行脚本时，将显示启动数据迁移应指定的必需和可选参数，以及将用于所需数据储存组件的相关属性信息。

必须以 novell 用户身份运行脚本。因此，确保 novell 用户对您指定的数据目录和所有文件具有相应权限。默认的情况下，脚本从主要储存迁移数据。如果想要从二级储存迁移数据，运行脚本时指定二级储存的相应路径。

要迁移数据：

1. 以 Novell 用户身份登录 Sentinel 服务器。
2. 运行以下脚本：

   /opt/novell/sentinel/bin/data_uploader.sh
3. 遵照屏幕指导，用所需参数再次运行脚本。

迁移数据的保留期将如目标服务器中所设置。

数据迁移完成后，脚本将记录状态，例如分区成功迁移、分区迁移失败、迁移的事件数量等。对于具有当前日期及前一天日期的分区，数据传输状态显示 IN_PROGRESS，该状态考虑到稍后可能进来的事件。

数据迁移未成功完成或分区的数据迁移状态仍显示 IN_PROGRESS的情况下重新运行脚本。重新运行脚本时，它将首先检查状态文件以了解已经迁移的分区，然后再继续仅迁移剩余分区。脚本将日志保存在 /var/opt/novell/sentinel/log/data_uploader.log 目录下以方便查错。

VII 部署 Sentinel 实现高可用性

本节介绍如何以主动-被动高可用性模式安装 Sentinel。在此模式下，如果发生硬件或软件故障，允许 Sentinel 故障转移到冗余群集节点。有关在 Sentinel 环境中实现高可用性和灾难恢复的详细信息，请联系 技术支持。

注释： 高可用性 (HA) 配置仅在 Sentinel 服务器上受支持。但是，Collector Manager 和 Correlation Engine 仍然可以与 Sentinel HA 服务器进行通讯。

35 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。

有关高可用性的详细信息，请参见 SUSE 高可用性指南。

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HA解决方案都允许实现者声明应该高度可用的服务之间的相关性，但是，这只适用于在群集本身上运行的服务。Sentinel 外部系统（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（如故障转移事件）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 之间发送和/或接收数据），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 地址配置 Sentinel）。

共享储存

所有HA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。

Sentinel 可对共享储存使用两种基本方法。第一种方法是将所有组件（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。

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。

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新启动。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。

36 系统要求

在分配群集资源以支持高可用性 (HA) 安装时，请考虑以下要求：

- ❒ （有条件）对于 HA 设备的安装，请确保 Sentinel HA 设备有一个有效许可证可用。Sentinel HA 设备是一个 ISO 设备，它包含以下包：
  - 操作系统：SLES 12 SP3
  - SLES 高可用性扩展 (SLES HAE) 包
  - Sentinel 软件（包括 HA rpm）
- ❒ （有条件）进行传统的 HA 安装时，请确保备齐以下项目：
  - 操作系统：SLES 11 SP4 或 SLES 12 SP1 或更高版本
  - 带有效许可证的 SLES HAE ISO 映像
  - Sentinel 安装程序（TAR 文件）
- ❒ （有条件）如果您使用的是内核版本为 3.0.101 或更高版本的 SLES 操作系统，则必须手动加载计算机中的检查包驱动程序。若要找到适合您计算机硬件的检查包驱动程序，请与您的硬件供应商联系。若要加载检查包驱动程序，请执行以下操作：
  1. 在命令提示符中，运行以下命令在当前会话中加载检查包驱动程序：

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. 在 /etc/init.d/boot.local 文件中添加以下行，以确保计算机在每次启动时自动装载检查包驱动程序：

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

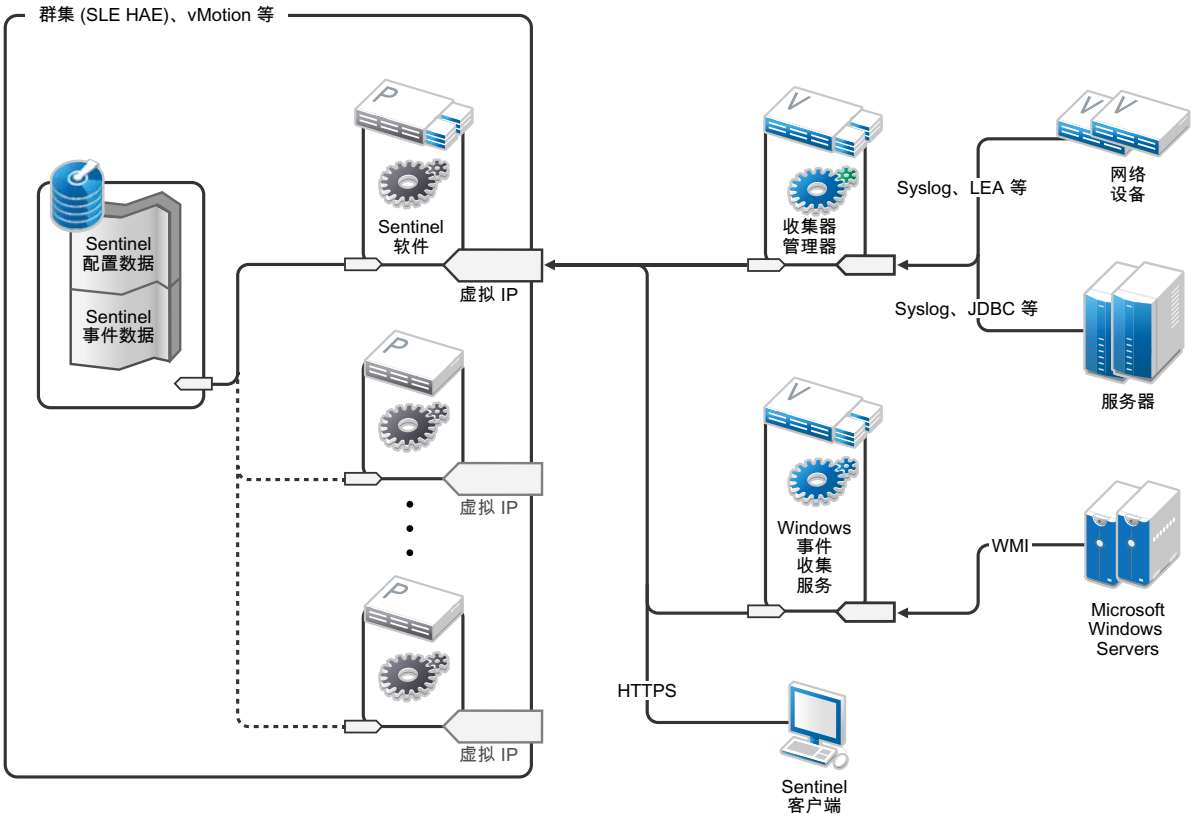
- ❒ 确保托管 Sentinel 服务的每个群集节点都满足第 5 章“满足系统要求”（第 37 页）中指定的要求。
- ❒ 确保为 Sentinel 数据和应用程序提供足够的共享储存。
- ❒ 确保对在发生故障转移时可在节点之间迁移的服务使用虚拟 IP 地址。
- ❒ 确保共享储存设备满足第 5 章“满足系统要求”（第 37 页）中指定的性能和大小特征要求。将配置了 iSCSI Target 的标准 SLES 虚拟机用作共享储存。

  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。如果储存的延迟和带宽慢于建议值，则 Sentinel 可能会遇到问题。
- ❒ 确保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。建议采用两个 SLES 虚拟机。
- ❒ 确保已创建群集节点与共享储存通讯的方法，例如用于 SAN 的 FibreChannel。使用专用 IP 地址连接 iSCSI Target。
- ❒ 确保已拥有的虚拟 IP 地址可在群集节点之间迁移，并可用作 Sentinel 的外部 IP 地址。
- ❒ 确保每个群集节点至少有一个 IP 地址用于内部群集通讯。您可以使用简单的单播 IP 地址，但生产环境使用多路广播更有利。

37 安装和配置

本章提供的步骤用于在高可用性 (HA) 环境中安装和配置 Sentinel。

下图显示了主动-被动 HA 体系结构。



初始设置

根据针对 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。

使用以下核对清单来指导您完成初始设置和配置。

	核对清单项目
❑	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 37 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 37 页）中根据主储存和辅助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 8 章“使用的端口”（第 59 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。
❑	确保所有群集节点的时间是同步的。可以使用 NTP 或类似技术实现此目的。
❑	◆ 该群集需要可靠的主机名解析。将所有内部群集主机名输入到 /etc/hosts 文件中，以确保在 DNS 发生故障的情况下群集继续运行。 ◆ 确保未指派主机名给回写 IP 地址。 ◆ 如果在安装操作系统时配置主机名和域名，请取消选择**指派主机名给回写 IP**。

您可使用下列配置：

- （有条件）对于传统 HA 安装：
  - 运行 SLES 11 SP4、SLES 12 SP1 或更高版本的两个群集节点虚拟机。
  - （有条件）如果您需要GUI配置，可以安装XWindows。将引导脚本设置为在没有X的情况下启动（运行级别 3），因此可以仅在需要的时候启动它们。
- （有条件）对于HA设备安装：两个基于HAISO设备的群集节点虚拟机。有关安装HAISO设备的详细信息，请参见 安装 Sentinel（第 95 页）。
- 节点的一个 NIC 将用于外部访问，而另一个 NIC 将用于 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 SLES 和 SLES HAE 系统要求，以及 Sentinel 应用程序要求。
- 运行SLES 11 SP4、SLES 12 SP1或更高版本的一个虚拟机，已配置iSCSI目标，用于共享储存。
  - （有条件）如果您需要GUI配置，可以安装XWindows。将引导脚本设置为在没有X的情况下启动（运行级别 3），因此可以仅在需要的时候启动它们。
  - 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。
  - 使用允许通过 SSH 或类似协议进行远程访问的 IP 地址配置外部 NIC。例如，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 SLES 系统要求，以及 Sentinel 事件数据储存要求。

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 地址进行内部群集通讯。

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。如果您使用的是FibreChannel和SAN，则可能需要提供物理连接及附加配置。Sentinel 使用此共享储存来储存数据库和事件数据。确保根据预期的事件发生率和数据保留策略，适当地相应调整共享储存的大小。

考虑以下共享储存安装程序示例：

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

注释： 配置共享储存并测试在每个群集节点上安装该储存。但是，群集配置将处理储存的实际装入。

执行以下过程，以创建由 SLES 虚拟机托管的 iSCSI 目标：

1. 连接到 storage03（您在初始设置期间创建的虚拟机），然后启动控制台会话。
2. 运行以下命令，以便按照需要为 Sentinel 主储存创建一个任意大小的空文件：

   dd if=/dev/zero of=/localdata count=<*文件大小*> bs=<*位大小*>

   例如，运行以下命令，创建一个 20GB 的文件，其中填充有从 /dev/zero 伪设备复制的零：

   dd if=/dev/zero of=/localdata count=20480000 bs=1024
3. 重复执行步骤 1 至步骤 2，以同样的方式为辅助储存创建一个文件。

   例如，对辅助储存运行以下命令：

   dd if=/dev/zero of=/networkdata count=20480000 bs=1024

注释： 对于此示例，您创建了两个具有相同大小和性能特征的文件来表示两个磁盘。在生产部署中，您可以将主储存创建在快速 SAN 上，而将辅助储存创建在速度较慢的 iSCSI、NFS 或 CIFS 卷上。

执行以下各节中提供的步骤，以配置 iSCSI 目标和发起程序设备：

- 配置 iSCSI 目标（第 179 页）
- 配置 iSCSI 发起程序（第 181 页）

配置 iSCSI 目标

执行以下过程，将 localdata 和 networkdata 文件配置为 iSCSI 目标。

有关配置 iSCSI 目标的详细信息，请参见 SUSE 文档中的使用 YaST 创建 iSCSI 目标。

1. 从命令行（如果您愿意，可以使用图形用户界面）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·地址。
6. 单击**下一步**，然后单击**确定**。

7 （有条件）在主屏幕上执行以下操作：

- 如果您使用的是 SLES 11 SP4，请选择**网络服务** > **iSCSI 目标**。
- 如果您正在使用的是 SLES 12 SP1 或更高版本，选择**网络服务** > **iSCSI LIO 目标**。

注释： 如果您找不到此选项，请转到 **软件** > **软件管理** > **iSCSI LIO 服务器**，然后安装 iSCSI LIO 包。

---

8 （有条件）如果出现系统提示，请安装所需的软件：

- 对于 SLES 11 SP4：iscsitarget RPM
- 对于 SLES 12 SP1 或更高版本：iscsiliotarget RPM

9 （有条件）如果您正在使用的是SLES12SP1或更高版本，在群集中的所有节点上执行以下步骤：

9a 运行以下命令，打开包含 iSCSI 发起程序名称的文件：

cat /etc/iscsi/initiatorname.iscsi

9b 记录要用于配置 iSCSI 发起程序的发起程序名称：

例如：

InitiatorName=iqn.1996-04.de.suse:01:441d6988994

这些发起程序名称将在配置 iSCSI 目标客户端安装程序时使用。

10 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。

11 选择**全局**选项卡，取消选择**无鉴定**以启用鉴定，然后为入局和出局鉴定指定所需的身份凭证。

默认情况下，**无身份验证**选项处于启用状态。但您应该启用鉴定以确保配置安全。

12 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。

13 单击**添加**以添加新的 LUN。

14 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。

15 重复步骤 13 和步骤 14，并在这次添加 LUN 1 和选择 /networkdata。

16 （有条件）如果您使用的是 SLES 11 SP4，请执行以下步骤：

16a 将其他选项保留为其默认值，单击**确定**，然后单击**下一步**。

16b （有条件）如果您已在步骤 11 中启用鉴定，请提供鉴定身份凭证。

选择客户端，再选择 **Edit Auth（编辑鉴定）** > **Incoming Authentication（入局鉴定）**，然后指定用户名和口令。

17 （有条件）如果您正在使用的是 SLES 12 SP1 或更高版本，执行以下步骤：

17a 将其他选项保留为其默认值，然后单击**下一步**。

17b 单击**添加**。当系统提示输入客户端名称时，请指定您已在步骤 9 中复制的发起程序名称。重复执行此步骤，以添加所有客户端名称，方法是指定发起程序名称。

客户端名称列表将显示在客户端列表中。

17c （有条件）如果您已在步骤 11 中启用鉴定，请提供鉴定身份凭证。

选择客户端，再选择 **Edit Auth（编辑鉴定）** > **Incoming Authentication（入局鉴定）**，然后指定用户名和口令。对所有客户端重复执行此步骤。

18 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。当系统提示重启动 iSCSI 时，接受该要求。

19 退出 YaST。

注释： 此过程在 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。

配置 iSCSI 发起程序

执行以下过程，对 iSCSI 发起程序设备进行格式化。

有关配置 iSCSI 发起程序的详细信息，请参见 SUSE 文档中的配置 iSCSI 发起程序。

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·地址。

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 如果出现系统提示，请安装所需软件 (iscsiclient 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 目标 IP 地址 (10.0.0.3)。

（有条件）如果您已在配置 iSCSI 目标（第 179 页）的步骤 11 中启用鉴定，请取消选择**无鉴定**。在**出局鉴定**字段中，输入您已在 iSCSI 目标配置期间配置的用户名和口令。

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 请执行下列步骤：

13a 切换到**启动**下拉菜单中的“自动”。

13b （有条件）如果您已启用鉴定，请取消选择**无鉴定**。

您已在步骤 11 中指定的用户名和口令应显示在**出局鉴定**部分中。如果不显示这些身份凭证，请在此部分中输入身份凭证。

13c 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，您会在列表中看到以下类型的新硬盘（例如 /dev/sdb 和 /dev/sdc）：

- 在 SLES 11 SP4 中：IET-VIRTUAL-DISK
- 在 SLES 12 SP1 或更高版本中：LIO-ORG-FILEIO

按 Tab 切换到列表中的第一项（应该是主储存），并选择该磁盘，然后按 Enter 键。

18 选择**添加**以将新分区添加到空磁盘。将该磁盘格式化为 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**。

此时，已格式化的磁盘（例如 /dev/sdb1）应准备就绪。在此过程的以下步骤中，我们称之为 /dev/<SHARED1>。

20 重新转到**分区程序**，并针对 /dev/sdc 或与辅助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 （有条件）如果您要执行传统的 HA 安装，请创建一个安装点，并按如下方式测试装入本地分区（确切的设备名称可能因具体实施而异）：

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

您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。

23 （有条件）如果您正在进行传统 HA 安装，则要卸载：

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

24 （有条件）对于 HA 设备安装，请重复执行步骤 1-15，以确保每个群集节点均可装入本地共享储存。对于每个群集节点，将步骤 5 中的节点 IP 地址替换为其他 IP 地址。

25 （有条件）对于传统 HA 安装，请重复执行步骤 1-15、22 和 23，以确保每个群集节点均可装入本地共享储存。对于每个群集节点，将步骤 6 中的节点 IP 地址替换为其他 IP 地址。

Sentinel 安装

有两个选项可用于安装 Sentinel：将 Sentinel 的每一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安装在共享储存中。

在托管 Sentinel 的每个群集节点上安装 Sentinel。首次安装 Sentinel 后，必须执行完整的安装（包括应用程序二进制文件、配置和所有数据储存）。对于其他群集节点上的后续安装，将只安装应用程序。在装入了共享储存后，Sentinel 数据将立即可用。

在第一个节点上安装

- 传统 HA 安装（第 182 页）
- Sentinel HA 设备安装（第 183 页）

传统 HA 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 请执行以下步骤开始安装：

3a 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

3b 提示选择配置方法时，指定 2 选择“自定义配置”。

4 执行完整安装，适当配置产品。

5 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 地址访问本产品。

6 使用下列命令关闭 Sentinel 并卸下共享存储：

```
rcsentinel stop
```

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

此步骤将删除自动启动脚本，使群集可以管理产品。

```
cd /
```

```
insserv -r sentinel
```

Sentinel HA 设备安装

Sentinel HA 设备包括已安装和配置的 Sentinel 软件。若要将 Sentinel 软件配置成 HA 模式，请执行以下步骤：

1 连接到其中一个群集节点 (node01) 并打开控制台窗口。

2 导航到以下目录：

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

3 记录配置信息：

3a 执行以下命令：

```
./configure.sh --record-unattended=/tmp/install.props --no-start
```

该步骤在 install.props 文件中记录配置信息，需要使用 install-resources.sh 脚本配置群集资源。

3b 提示选择配置方法时，指定 2 选择“自定义配置”。

3c 出现口令提示时，指定 2 以输入新口令。

如果您指定 1，该 install.props 文件不会储存口令。

4 使用以下命令关闭 Sentinel：

```
rcsentinel stop
```

此步骤将删除自动启动脚本，使群集可以管理产品。

```
insserv -r sentinel
```

5 使用以下命令将 Sentinel 数据文件夹移至共享存储。该移动将允许节点通过共享存储使用 Sentinel 数据文件夹。

```
mkdir -p /tmp/new
```

```
mount /dev/<SHARED1> /tmp/new
```

```
mv /var/opt/novell/* /tmp/new

umount /tmp/new/
```

6 使用以下命令校验 Sentinel 数据文件夹到共享存储的移动是否成功：

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

umount /var/opt/novell/
```

在后续节点上安装

- 传统 HA 安装（第 184 页）
- Sentinel HA 设备安装（第 184 页）

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。

传统 HA 安装

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

cd sentinel_server*

./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props

insserv -r sentinel
```

Sentinel HA 设备安装

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：

```
insserv -r sentinel
```

3 停止 Sentinel 服务。

```
rcsentinel stop
```

4 删除 Sentinel 目录。

```
rm -rf /var/opt/novell/*
```

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。

群集安装

对于传统的高可用性 (HA) 安装，必须仅安装群集软件。Sentinel HA 设备包含群集软件并且无需手动安装。

按下列步骤设置具有 Sentinel 特定资源代理覆盖的 SLES High Availability Extension：

1 在每个节点上安装群集软件。

2 使用群集管理器注册每个群集节点。

3 校验每个群集节点是否显示在群集管理控制台中。

注释： 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。如果您不使用 OCF 资源代理监视 Sentinel，则必须为本地群集环境开发一个类似的监视解决方案。要开发自己的解决方案，请复查现有的资源代理（储存在 Sentinel 下载包内的 Sentinelha.rpm 文件中）。

---

4 按照SLE HAE文档安装核心SLE HAE软件。有关安装SLES外接式附件的信息，请参见《部署指南》。

5 在所有群集节点上重复执行步骤 4。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。

6 安装附加 RPM 以提供特定于 Sentinel 的附加群集资源代理。HA RPM 可以在安装产品时解包的默认 Sentinel 下载包中储存的 novell-Sentinelha-<*Sentinel_version*>*.rpm 文件内找到。

7 在每个群集节点上，将 novell-Sentinelha-<*Sentinel_version*>*.rpm 文件复制到 /tmp 目录中，然后运行以下命令：

```
cd /tmp
```

```
rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

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。在此配置过程中，您还可以设置隔离和逐出其他节点 (STONITH) 资源，以确保群集的一致性。

重要： 本部分程序使用了 rcopenais 和 openais 命令，这两个命令只适用于 SLES 11 SP4。对于 SLES 12 SP2 及更高版本，使用 systemctl pacemaker.service 命令。

例如，对于 /etc/rc.d/openais start 命令，使用 systemctl start pacemaker.service 命令。

按下列步骤配置群集：

对于本解决方案，必须使用专用 IP 地址进行内部群集通讯，并使用单播以最大程度地减少从网络管理员请求多路广播地址的需要。您还必须使用在托管共享储存的同一个 SLES 虚拟机上配置的 iSCSI 目标，将其作为实现隔离目的的节点分裂检测 (SBD) 设备。

SBD 设置

1. 连接到 storage03 并启动控制台会话。运行以下命令，以便按照需要创建一个任意大小的空文件：

   dd if=/dev/zero of=/sbd count=<*文件大小*> bs=<*位大小*>

   例如，运行以下命令，创建一个 1MB 的文件，其中填充有从 /dev/zero 伪设备复制的零：

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

2. 从命令行或图形用户界面运行 YaST：/sbin/yast
3. 选择**网络服务** > **iSCSI 目标**。
4. 单击**目标**并选择现有目标。
5. 选择**编辑**。UI 将显示可用 LUN（驱动器）的列表。
6. 选择**添加**以添加新的 LUN。
7. 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。
8. 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。
9. 单击**完成**以退出配置。根据需要重新启动服务。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 地址及其主机名（由 hostname 命令报告）的 /etc/hosts 文件中添加每个主机的项。另外，请确保未为回环 IP 地址指派主机名。

执行以下步骤可在 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**启动选项并取消选择**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1MBIET-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. （有条件）执行以下命令之一：
    - 如果您使用的是 SLES 11 SP4：

      sleha-init

    - 如果您使用的是 SLES 12 SP1 或更高版本：

      ha-cluster-init

11. 当系统提示输入要绑定的目标网络地址时，请指定外部 NIC IP 地址 (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 （有条件）出现下列提示时输入 N：

```
Do you wish to configure an administration IP? [y/N]
```

要配置管理 IP 地址，在资源配置（第 188 页）期间提供虚拟 IP 地址

15 完成向导并确保未报告任何错误。

16 启动 YaST。

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

18 在左侧的框中，确保已选择**通讯通道**。

19 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）。

20 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。

21 选择**完成**以完成配置。

22 退出 YaST。

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

连接到每个附加的群集节点 (node02) 并打开控制台：

1 运行 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**启动选项并取消选择**无鉴定**）。

6 选择**确定**以退出 iSCSI 发起程序工具。

7 （有条件）执行以下命令之一：

- 如果您使用的是 SLES 11 SP4：

  sleha-join

- 如果您使用的是 SLES 12 SP1 或更高版本：

  ha-cluster-join

8 输入第一个群集节点的 IP 地址。

（有条件）如果群集未正常启动，请执行以下步骤：

1 运行 crm status 命令查看节点是否已加入。如果节点未加入，重启动群集中的所有节点。

2 手动将 /etc/corosync/corosync.conf 文件从 node01 复制到 node02，在 node01 上运行 csync2 -x -v，或者通过 YaST 在 node02 上手动设置群集。

3 （有条件）如果您在步骤 1 中运行的 csync2 -x -v 命令无法同步所有文件，请执行以下过程：

3a 清除所有节点 /var/lib/csync2 目录中的 csync2 数据库。

3b 在所有节点上更新 csync2 数据库以匹配文件系统，无需将任何项目标记为需要同步至其他服务器：

csync2 -cIr /

3c 在活动节点上，执行下列操作：

3c1 找出活动节点与被动节点之间的所有区别，标记这些区别以进行同步：

csync2 -TUXI

3c2 重设置数据库以强制活动节点覆盖任意冲突：

csync2 -fr /

3c3 开始同步至所有其他节点：

csync2 -xr /

3d 在所有节点上校验所有文件均同步：

csync2 -T

此命令将仅列出未同步的文件。

4 在 node02 上运行以下命令：

对于 SLES 11 SP4：

/etc/rc.d/openais start

对于 SLES 12 SP1 及更高版本：

systemctl start pacemaker.service

（有条件）如果 xinetd 服务未正确添加新的 csync2 服务，该脚本将无法正常运行。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 xinetd 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。

要解决此问题，请执行 kill -HUP `cat /var/run/xinetd.init.pid 命令，然后重新运行 sleha-join 脚本。

5 在每个群集节点上运行 crm_mon，以校验该群集是否正常运行。此外，还可以使用“hawk”（Web 控制台）来校验群集。默认登录名是 hacluster，口令是 linux。

（有条件）根据您的环境，请执行以下任务来修改其他参数：

1 要确保双节点群集中的单个节点出现故障不会使整个群集意外停止，请将全局群集选项 no-quorum-policy 设为 ignore：

crm configure property no-quorum-policy=ignore

注释： 如果您的群集包含两个以上的节点，请勿设置此选项。

2 要确保资源管理器允许资源就地运行和移动，请将全局群集选项 default-resource-stickiness 设为 1：

crm configure property default-resource-stickiness=1。

资源配置

默认情况下，资源代理随SLEHAE一起提供。如果您不想使用SLEHAE，则需要使用替代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 地址对应的 IP 地址资源。
- 用于储存配置和事件元数据的 Postgres 数据库软件。

按下列步骤配置资源：

crm 脚本帮助您进行群集配置。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，则可以使用以下过程相应地编辑该脚本。

1 连接到安装 Sentinel 的原始节点。

注释： 这必须是运行完整 Sentinel 安装的节点。

2 编辑脚本，使其如下所示，其中 <SHARED1> 是之前创建的共享卷：

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

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

./install-resources.sh
```

3 （有条件）您可能会遇到群集中的新资源问题。如果出现此问题，在 node02 上运行以下命令：

对于 SLES 11 SP4：

/etc/rc.d/openais start

对于 SLES 12 SP1：

systemctl start pacemaker.service

4 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 地址，以及共享储存的设备名称），然后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。

5 如果您的环境与 建议的此解决方案不同，您可以编辑 resources.cli 文件（位于同一目录中），并修改该文件中的基元定义。例如，建议的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。

6 在运行外壳脚本后，您可以发出 crm status 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
```

7 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）。

辅助储存配置

执行以下步骤来配置辅助储存，使 Sentinel 可以将事件分区迁移到较便宜的储存：

注释： 此过程是可选的，并且辅助储存的高可用性方式不需要与所配置的系统的其余部分相同。您可以使用从 SAN、非 SAN、NFS 或 CIFS 卷装入的任何目录。

---

1. 在 Sentinel 主界面的顶部菜单栏中，单击**储存**。
2. 选择**配置**。
3. 选择未配置的辅助储存下方的单选按钮之一

将简单 iSCSI Target 用作网络共享储存位置，与主要储存配置基本相同。在生产环境中，储存技术可能会有所不同。

使用以下过程配置辅助储存以供 Sentinel 使用：

注释： 对于 iSCSI Target，目标将安装为目录以用作二级储存。必须将装入配置为文件系统资源，其方式与主储存文件系统的配置方式类似。这未在资源安装脚本中进行自动设置，因为还有其他可能的变量。

---

1. 复查前面的步骤，以确定创建了哪个分区以用作辅助储存（/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 Sentinel 主界面或运行命令：

   ```
   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），并确保已正确装入辅助储存（使用 mount 命令）。
5. 登录到 Sentinel 主界面。
6. 依次选择**储存**和**配置**，然后在“未配置的辅助储存”下选择 **SAN（本地装入）**。
7. 键入辅助储存装入到的路径，例如 /var/opt/netdata。

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）。

38 将 Sentinel HA 配置为 SSDM

本章节介绍将 Sentinel HA 设置配置为 SSDM 的相关信息。这些说明对于传统安装和设备安装均适用。

将 Sentinel HA 设置配置为 SSDM：

1. 安装和配置 Sentinel 可缩放储存。有关详细信息，请参见第 13 章“安装和设置可缩放储存”（第 81 页）。
2. 在活动节点上启用可缩放储存。有关详细信息，请参见“《 Sentinel 管理指南》”中的*在安装后启用可缩放储存*。
3. 在活动节点上运行以下命令：

   csync2 -x -v

   此操作会将 SSDM 配置与所有被动节点同步。
4. （有条件）如果您在步骤 3 中运行的 csync2 -x -v 命令无法同步所有文件，请执行以下操作：

   4a 清除所有节点上的 csync2 数据库（位于 /var/lib/csync2 目录中）。

   4b 在所有服务器上运行以下命令，将 csync2 数据库更新为匹配文件系统，但是不将任何内容标记为需要同步到其他服务器：

   csync2 -cIr /

   4c 运行以下命令，找到授权服务器与远程服务器之间的所有不同之处，并将其标记为需要同步：

   csync2 -TUXI

   4d 运行以下命令，对数据库进行重设置，强制当前服务器在发生任何冲突时忽略相关冲突：

   csync2 -fr /

   4e 运行以下命令，启动同步操作，将内容同步到所有其他的服务器：

   csync2 -xr /

   4f 运行以下命令，校验是否同步了所有文件：

   csync2 -T

   如果同步成功，则此命令将不列出任何文件。

39 在高可用性环境中升级 Sentinel

当您在 HA 环境下升级 Sentinel 时，您应该首先升级群集中的无源节点，然后再升级活动的群集节点。

先决条件

- 从下载网站下载最新的安装程序。
- 如果正在使用内核版本 3.0.101 或更高版本的 SLES 操作系统，您必须手动加载计算机中的检查包驱动程序。若要找到适合您计算机硬件的检查包驱动程序，请与您的硬件供应商联系。若要加载检查包驱动程序，请执行以下操作：
  1. 在命令提示符中，运行以下命令在当前会话中加载检查包驱动程序：

     /sbin/modprobe -v --ignore-install <*检查包驱动程序名称*>
  2. 在 /etc/init.d/boot.local 文件中添加下面一行，以确保计算机在每次引导时自动加载检查包驱动程序：

     /sbin/modprobe -v --ignore-install <*检查包驱动程序名称*>

升级传统 Sentinel HA 安装

本节介绍如何升级传统的 Sentinel 安装，以及如何在传统的 Sentinel 安装过程中升级操作系统。

重要： 本部分程序使用了 rcopenais 和 openais 命令，这两个命令只适用于 SLES 11 SP4。对于 SLES 12 SP2 及更高版本，使用 systemctl pacemaker.service 命令。

例如，对于 /etc/rc.d/openais start 命令，使用 systemctl start pacemaker.service 命令。

升级 Sentinel HA

1 在群集中启用维护模式：

crm configure property maintenance-mode=true

维护模式可以帮助您在更新 Sentinel 时，避免对正在运行的群集资源产生任何干扰。可以从任何群集节点运行此命令。

2 校验维护模式是否处于活动状态：

crm status

群集资源应显示为处于非受管状态。

3 升级被动群集节点：

3a 停止群集堆栈：

rcopenais stop

停止群集堆栈可确保群集资源仍然可以访问，并可避免节点防护。

3b 以 root 身份登录要升级 Sentinel 的服务器。

3c 从 tar 文件提取安装文件：

tar xfz <*install_filename*>

3d 在您提取安装文件的目录中运行以下命令：

。/install-sentinel --cluster-node

3e 在升级完成后，重新启动群集堆栈：

rcopenais start

对所有被动群集节点重复执行步骤 3。

3f 去除自动启动脚本，使群集可以管理产品。

cd /

insserv -r sentinel

4 升级主动群集节点：

4a 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 “《 Sentinel 管理指南》”中的*备份和恢复数据*。

4b 停止群集堆栈：

rcopenais stop

停止群集堆栈可确保群集资源仍然可以访问，并可避免节点防护。

4c 以 root 身份登录要升级 Sentinel 的服务器。

4d 运行以下命令从 tar 文件提取安装文件：

tar xfz <*install_filename*>

4e 在您提取安装文件的目录中运行以下命令：

。/install-sentinel

4f 在升级完成后，启动群集堆栈：

rcopenais start

4g 去除自动启动脚本，使群集可以管理产品。

cd /

insserv -r sentinel

4h 运行以下命令以同步配置文件中的任何更改：

csync2 -x -v

5 在群集中禁用维护模式：

crm configure property maintenance-mode=false

可以从任何群集节点运行此命令。

6 校验维护模式是否处于非活动状态：

crm status

群集资源应显示为处于已启动状态。

7 （可选）校验 Sentinel 升级是否成功：

rcsentinel version

升级操作系统

本节介绍如何在 Sentinel HA 群集中将操作系统升级到主版本，例如从 SLES 11 升级到 SLES 12。升级操作系统时，必须执行几项配置任务，确保在升级该操作系统后 Sentinel HA 可以正常工作。

执行以下各节中所述的步骤：

- 升级操作系统（第 195 页）
- 配置 iSCSI 目标（第 196 页）
- 配置 iSCSI 发起程序（第 196 页）
- 配置 HA 群集（第 197 页）

升级操作系统

要升级操作系统，请执行以下操作:

1 以 root 用户身份登录到 Sentinel HA 群集中的任何节点。

2 运行以下命令，在群集上启用维护模式：

crm configure property maintenance-mode=true

维护模式可帮助您在升级操作系统时避免对正在运行的群集资源产生任何干扰。

3 运行以下命令，校验维护模式是否处于活动状态：

crm status

群集资源应显示为处于非受管状态。

4 确保您已在所有群集节点上将 Sentinel 升级到 8.2 或更高版本。

5 确保所有的群集节点都已在 SLES 和 SLESHA 中注册。

6 执行以下步骤，在被动群集节点上升级操作系统：

6a 运行以下命令，停止群集堆栈：

rcopenais stop

停止群集堆栈可确保群集资源始终不可访问，这样就不需节点防护。

6b 升级操作系统。有关更多信息，请参见操作系统升级。

7 在所有被动节点上重复执行步骤 6，以升级操作系统。

8 在主动节点上重复执行步骤 6，以在主动节点上升级操作系统。

9 重复执行步骤 6b，以在共享储存上升级操作系统。

10 确保所有群集节点上的操作系统均已升级到 SLES12 SP3。

配置 iSCSI 目标

要配置 iSCSI 目标，请执行以下操作：

1. 在共享储存上，检查是否已安装 iSCSI LIO 包。如果尚未安装，请转到“YaST2 软件管理”，然后安装 iSCSI LIO 包 (iscciliotarget RPM)。
2. 在所有群集节点上执行以下步骤：
   - **2a** 运行以下命令，打开包含 iSCSI 发起程序名称的文件：

     cat /etc/iscsi/initiatorname.iscsi
   - **2b** 记录要用于配置 iSCSI 发起程序的发起程序名称：

     例如：

     InitiatorName=iqn.1996-04.de.suse:01:441d6988994

   这些发起程序名称将在配置 iSCSI 目标客户端安装程序时使用。
3. 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。
4. 选择**全局**选项卡，取消选择**无鉴定**以启用鉴定，然后为进来的和出去的鉴定指定用户名称和口令。

   默认情况下，**无身份验证**选项处于启用状态。但您应该启用鉴定以确保配置安全。
5. 单击**目标**，然后单击**添加**以添加新目标。
6. 单击**添加**以添加新的 LUN。
7. 将 LUN 编号保留为 0，然后在**路径**对话框（在 Type=fileio 下面）中浏览，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。
8. 重复步骤 6 和步骤 7，并在这次添加 LUN 1 和选择 /networkdata。
9. 重复步骤 6 和步骤 7，并在这次添加 LUN 2 和选择 /sbd。
10. 将其他选项保留为其默认值。单击**下一步**。
11. 单击**添加**。当系统提示输入客户端名称时，请指定您已在步骤 2 中复制的发起程序名称。重复执行此步骤，以添加所有客户端名称，方法是指定发起程序名称。

    客户端名称列表将显示在客户端列表中。
12. （有条件）如果您已在步骤 4 中启用鉴定，请提供您在步骤 4 中指定的鉴定身份凭证。

    选择客户端，再选择 **Edit Auth（编辑鉴定）** > **Incoming Authentication（入局鉴定）**，然后指定用户名和口令。对所有客户端重复执行此步骤。
13. 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。出现系统提示时，重启动iSCSI。
14. 退出 YaST。

配置 iSCSI 发起程序

要配置 iSCSI 发起程序，请执行以下操作：

1. 连接到其中一个群集节点 (node01) 并启动 YaST。
2. 单击**网络服务** > **iSCSI 发起程序**。
3. 如果出现系统提示，请安装所需软件 (iscsiclient RPM)。
4. 单击**服务**，选择**引导时**，以确保在引导时启动 iSCSI 服务。
5. 单击**已发现的目标**。

注释： 如果显示任何以前就有的 iSCSI 目标，请删除这些目标。

选择**发现**以添加新的 iSCSI 目标。

6 指定 iSCSI 目标 IP 地址 (10.0.0.3)。

（有条件）如果您已在配置 iSCSI 目标（第 196 页）的步骤 4 中启用鉴定，请取消选择**无鉴定**。在**出局鉴定**部分中，输入您在配置 iSCSI 目标时指定的鉴定身份凭证。

单击**下一步**。

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

8 请执行下列步骤：

8a 切换到**启动**下拉菜单中的“自动”。

8b （有条件）如果您已启用鉴定，请取消选择**无鉴定**。

您已指定的用户名和口令应显示在**出局鉴定**部分中。如果不显示这些身份凭证，请在此部分中输入身份凭证。

8c 单击**下一步**。

9 切换到**已连接的目标**选项卡，以确保连接到目标。

10 退出配置。此时，iSCSI 目标应该已作为块设备装入群集节点上。

11 在 YaST 主菜单中，选择**系统** > **分区程序**。

12 在系统视图中，您会在列表中看到 LIO-ORG-FILEIO 类型的新硬盘（例如 /dev/sdb 和 /dev/sdc），以及已格式化的磁盘（例如 /dev/sdb1 或 /dev/<SHARED1）。

13 在所有节点上重复执行步骤 1 至步骤 12。

配置 HA 群集

要配置 HA 群集，请执行以下操作：

1 启动 YaST2，然后转到**高可用性** > **群集**。

2 出现系统提示时，安装 HA 包并解析依赖项。

在安装 HA 包后，将显示群集通讯通道。

3 确保将“单播”选为“传输”选项。

4 选择**添加成员地址**，并指定节点 IP 地址，然后重复执行此操作，以添加所有其他的群集节点 IP 地址。

5 确保选择**自动生成节点 ID**。

6 确保在所有节点上启用 HAWK 服务。如果未启用该服务，请运行以下命令以启用它：

```
service hawk start
```

7 运行以下命令：

```
ls -l /dev/disk/by-id/
```

此时将显示 SBD 分区 ID。例如，scsi-1LIO-ORG_FILEIO:33caaa5a-a0bc-4d90-b21b-2ef33030cc53。

复制该 ID。

8 打开 sbd 文件 (/etc/sysconfig/sbd)，然后使用您已在步骤 7 中复制的 ID 更改 SBD_DEVICE 的 ID。

9 运行以下命令以重启动 pacemaker 服务：

```
rcpacemaker restart
```

10 运行以下命令以去除自动启动脚本，以便群集可以管理本产品。

cd /

insserv -r sentinel

11 在所有群集节点上重复执行步骤 1 至步骤 10。

12 运行以下命令以同步配置文件中的任何更改：

csync2 -x -v

13 运行以下命令，在群集上禁用维护模式：

crm configure property maintenance-mode=false

可以从任何群集节点运行此命令。

14 运行以下命令，校验维护模式是否处于非活动状态：

crm status

群集资源应显示为处于已启动状态。

升级 Sentinel HA 设备安装

可使用 Zypper 补丁升级 Sentinel HA 设备安装。

重要： 本部分程序使用了 rcopenais 和 openais 命令，这两个命令只适用于 SLES 11 SP4。对于 SLES 12 SP2 及更高版本，使用 systemctl pacemaker.service 命令。

例如，对于 /etc/rc.d/openais start 命令，使用 systemctl start pacemaker.service 命令。

- 通过使用 Zypper 升级 Sentinel HA 设备（第 198 页）

通过使用 Zypper 升级 Sentinel HA 设备

升级前必须通过 Sentinel Appliance Manager 注册所有设备节点。有关详细信息，请参见 注册更新（第 99 页）。若您未注册设备，Sentinel 将显示一则黄色警告。

1 在群集上启用维护模式。

crm configure property maintenance-mode=true

维护模式帮助您在升级 Sentinel 软件时避免干扰正在运行的群集资源。可以从任何群集节点运行此命令。

2 校验维护模式是否处于活动状态。

crm status

群集资源应显示为处于非受管状态。

3 升级被动群集节点：

3a 停止群集堆栈。

rcopenais stop

停止群集堆栈可确保群集资源始终不可访问，这样就不需节点防护。

3b 下载 Sentinel HA 设备的更新。

zypper -v patch

3c （有条件）如果安装程序显示一则讯息，要求您必须解析OpenSSH包的依赖项，请输入相应的选项，以降级 OpenSSH 包。

3d （有条件）如果安装程序显示一则讯息，指示ncgOverlay体系结构发生更改，请输入相应的选项，以接受体系结构更改。

3e （有条件）如果安装程序显示一则讯息，要求您必须解析某些设备软件包的依赖项，请输入相应的选项，以卸装依赖项软件包。

3f 在升级完成后，启动群集堆栈。

```
rcopenais start
```

4 对所有无源群集节点重复步骤 3。

5 升级主动群集节点：

5a 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 “《 Sentinel 管理指南》”中的*备份和恢复数据*。

5b 停止群集堆栈。

```
rcopenais stop
```

停止群集堆栈可确保群集资源始终不可访问，这样就不需节点防护。

5c 下载 Sentinel HA 设备的更新。

```
zypper -v patch
```

5d （有条件）如果安装程序显示一则讯息，要求您必须解析OpenSSH包的依赖项，请输入相应的选项，以降级 OpenSSH 包。

5e （有条件）如果安装程序显示一则讯息，指示ncgOverlay体系结构发生更改，请输入相应的选项，以接受体系结构更改。

5f （有条件）如果安装程序显示一则讯息，要求您必须解析某些设备软件包的依赖项，请输入相应的选项，以卸装依赖项软件包。

5g 在升级完成后，启动群集堆栈。

```
rcopenais start
```

5h 运行以下命令以同步配置文件中的任何更改：

```
csync2 -x -v
```

6 禁用群集上的维护模式。

```
crm configure property maintenance-mode=false
```

可以从任何群集节点运行此命令。

7 校验维护模式是否处于非活动状态。

```
crm status
```

群集资源应显示为处于已启动状态。

8 （可选）校验 Sentinel 升级是否成功：

```
rcsentinel version
```

9 （有条件）要升级操作系统，请参见升级操作系统（第 149 页）。

40 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。

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。“《 Sentinel 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。

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。“《 Sentinel 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。

VIII 附录

A 查错

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。

因为错误网络配置导致安装失败

首次引导时，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。

UUID 不是为 Collector Manager 或 Correlation Engine 映像而创建

如果您为 Collector Manager 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 Collector Manager 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 Collector Manager 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 Collector Manager。

   Collector Manager 便会自动生成 UUID。

登录后 Sentinel 主界面在 Internet Explorer 中为空白

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**，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**自动提示文件下载**选项下选择**启用**。

Sentinel 无法在 Windows Server 2012 R2 中的 Internet Explorer 11 中起动

使用 Windows Server 2012 R2 时，因 Internet Explorer 11 的默认安全性配置，Sentinel 在 Internet Explorer 11 中无法起动。您必须在起动 Sentinel 前，将 Sentinel 手动添加到受信站点列表中。

将 Sentinel 添加到受信站点列表中

1. 打开 Internet Explorer 11。
2. 单击**设置**图标 > **Internet 选项** > **安全性**选项卡 > **受信站点** > **站点**
3. 将 Sentinel 主机添加到受信站点列表中。

Sentinel 无法通过默认 EPS 许可证运行本地报告

如果环境拥有默认的 25 个 EPS 许可证并且您运行报告，报告失败，错误为：License for Distributed Search feature is expired

要在与 Sentinel 相同的 JVM 中运行报告，完成下列步骤：

1. 登录 Sentinel 服务器并打开 /etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties 文件。
2. 查找 reporting.process.oktorunstandalone 属性。
3. （有条件）如果文件中无此属性，请添加。
4. 将属性设置为 false。例如：

   reporting.process.oktorunstandalone=false
5. 重启动 Sentinel。

将活动节点转换为 FIPS 140-2 模式后，需要在 Sentinel 高可用性模式中手动启动同步

问题： 在 Sentinel 高可用模式中将活动节点转换为 FIPS 140-2 模式后，未完全执行将所有被动节点转换为 FIPS 140-2 模式的同步操作。您必须手动启动同步。

解决方法： 按以下步骤手动同步被动节点与 FIPS 140-2 模式：

1. 在主动节点上以 root user 身份登录。
2. 打开 /etc/csync2/csync2.cfg 文件。
3. 更改下列行：

   include /etc/opt/novell/sentinel/3rdparty/nss/*;

   更改为

   include /etc/opt/novell/sentinel/3rdparty/nss;
4. 保存 csync2.cfg 文件。
5. 通过运行以下命令手动启动同步：

   csync2 -x -v

转换到 Sentinel 可缩放数据管理器后 Sentinel 主界面显示空白页

问题： 启用 SSDM 后，如果您登录到 Sentinel 主界面，则浏览器将显示空白页。

解决方法： 关闭您的浏览器，然后重新登录到 Sentinel 主界面。在您启用 SSDM 后首次登录到 Sentinel 主界面时，该问题只出现一次。

在编辑某些保存的搜索时，在日程表页中缺少事件字段面板

问题： 在编辑从 Sentinel 7.2 升级到后续版本的已保存搜索时，在日程表页中缺少用于指定搜索报告 CSV 中的输出字段的**事件字段**面板。

解决方法： 在升级 Sentinel 后，重创建并重安排搜索来查看日程表页中的**事件字段**面板。

在您使用默认的 Fire 计数搜索来搜索部署规则的事件时，Sentinel 不返回任何关联事件

问题： 当您通过单击该规则的关联摘要页的**活动统计**面板的 **Fire 计数**旁边的图标，搜索部署或启用该规则后生成的所有关联事件时，Sentinel 不会返回任何关联事件。

解决方法： 将事件搜索页中 **From** 字段的值更改为一个早于此字段中填充时间的时间，并再次单击**搜索**。

当重新生成基线时，安全智能仪表板显示无效的基线持续时间

问题： 在安全智能基线重新生成期间，基线的开始和结束日期不正确，并显示为 1/1/1970。

解决方法： 在基线重新生成完成后，更新正确的日期。

如果单个分区中有大量事件，运行搜索时，Sentinel 服务器会关闭

问题： 如果在单个分区中有大量索引的事件，运行搜索时，Sentinel 服务器会关闭。

解决方法： 通过在一天中至少打开两个分区的方式，创建保留策略。打开多个分区有助于减少分区中索引的事件数量。

您可以基于跟踪一天中小时的 estzhour 字段来创建过滤事件的保留策略。因此，您可以使用 estzhour:[0 TO 11] 作为过滤器来创建一个保留策略，并使用 estzhour:[12 TO 23] 作为过滤器来创建另一个保留策略。

有关详细信息，请参见 *《Sentinel 管理指南》* 中的“配置数据保留策略”。

使用 report_dev_setup.sh 脚本为升级的 Sentinel 设备安装上的防火墙异常配置 Sentinel 端口时，出现错误

问题： 当您使用 report_dev_setup.sh 脚本为防火墙异常配置 Sentinel 端口时，Sentinel 显示错误。

解决方法： 通过以下步骤，为防火墙异常配置 Sentinel 端口：

1. 打开 /etc/sysconfig/SuSEfirewall2 文件。
2. 更改下列行：

   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443 40000:41000 1290 1099 2000 1024 1590"

   更改为

   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443 40000:41000 1290 1099 2000 1024 1590 5432"
3. 重启动 Sentinel。

B 卸装

本附录将介绍如何卸装 Sentinel 以及卸装后的任务。

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 Collector Manager 和 Correlation Engine（如果有）。
- ❒ 执行卸装后的任务以完成 Sentinel 卸装。

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。

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：

   ```
   <sentinel_installation_path>/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。

卸载 Collector Manager 和 Correlation Engine

使用以下步骤卸装 Collector Manager 和 Correlation Engine：

1 以 root 身份登录到 Collector Manager 和 Correlation Engine 计算机。

注释： 如果安装以 root 用户的身份进行，您将无法以非 root 用户的身份卸载远程 Collector Manager 和远程 Correlation Engine。然而，如果安装以非 root 用户身份进行，非 root 用户便可以卸载。

2 转到以下位置：

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

3 运行以下命令：

```
./uninstall-sentinel
```

脚本显示一则警告，告知 Collector Manager 或者 Correlation Engine 以及所有相关数据都将被彻底删除。

4 输入 y 去除 Collector Manager 或 Correlation Engine。

该脚本首先停止服务，然后完全去除它。但是，“Collector Manager 和 Correlation Engine”图标仍会在 Sentinel 主界面中显示为非活动状态。

5 （有条件）如果已启用事件可视化，必须重新部署 Elasticsearch 安全插件。有关详细信息，请参见部署 Elasticsearch 安全插件（第 79 页）。

6 执行以下附加步骤，在 Sentinel 主界面中手动删除 Collector Manager 和 Correlation Engine：

Collector Manager：

1. 访问**事件源管理 > 实时视图**。
2. 右键单击要删除的 Collector Manager，然后单击**删除**。

Correlation Engine：

1. 以管理员身份导航到 **Sentinel 主界面**。
2. 展开**关联**，然后选择您希望删除的 Correlation Engine。
3. 单击**删除**按钮（回收站图标）。

卸载 NetFlow Collector Manager

使用以下步骤卸载 NetFlow Collector Manager：

1 登录到 NetFlow Collector Manager 计算机。

注释： 您必须以与安装 NetFlow Collector Manager 时使用的用户许可权限相同的用户许可权限登录。

2 更改为以下目录：

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

3 运行以下命令：

```
./uninstall-sentinel
```

4 输入 y 卸载 Collector Manager。

脚本首先停止服务，然后将服务彻底卸载。

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、用户主目录以及组。

userdel -r novell

groupdel novell

5 重新启动操作系统。