

Novell Sentinel 6.1 Rapid Deployment SP2 自述文件

2011 年 4 月

Novell®

Sentinel Rapid Deployment 是占市场领先地位的 Novell Sentinel 安全性信息和事件管理解决方案的新打包选项。Sentinel Rapid Deployment 包含 Sentinel 的全部功能，非常适合较小型组织或区域性的安装环境。

Sentinel 6.1 Rapid Deployment SP2 提供了全新安装程序或升级安装程序。升级安装程序会将最新的软件修复程序和增强功能应用于已安装的 Sentinel Rapid Deployment 6.1 SP1。

- ◆ 第 1 节“新功能”（第 1 页）
- ◆ 第 2 节“系统要求”（第 2 页）
- ◆ 第 3 节“安装 Novell Sentinel Rapid Deployment”（第 2 页）
- ◆ 第 4 节“升级到 Sentinel Rapid Deployment SP2”（第 2 页）
- ◆ 第 5 节“访问 Sentinel Rapid Deployment 帮助文件”（第 2 页）
- ◆ 第 6 节“修复的缺陷和增强的功能”（第 3 页）
- ◆ 第 7 节“已知问题”（第 5 页）
- ◆ 第 8 节“文档”（第 6 页）
- ◆ 第 9 节“法律声明”（第 7 页）

1 新功能

- ◆ 第 1.1 节“Sentinel Rapid Deployment 6.1 SP2 中的新功能”（第 1 页）
- ◆ 第 1.2 节“Sentinel Rapid Deployment SP1 中的新功能”（第 2 页）

1.1 Sentinel Rapid Deployment 6.1 SP2 中的新功能

- ◆ 支持 SLES 11 SP1（第 1 页）
- ◆ 对 Legacy 收集器的支持有限（第 1 页）
- ◆ 安全性提升（第 2 页）

1.1.1 支持 SLES 11 SP1

现在，SUSE Linux Enterprise Server (SLES) 11 SP1 64 位平台支持 Sentinel Rapid Deployment。

1.1.2 对 Legacy 收集器的支持有限

Novell 在 Sentinel 产品线中正在逐步淘汰对旧式收集器的支持。在先前版本的 Sentinel Rapid Deployment 中，如果您导入 Legacy 收集器，系统会发出警告。从 SP2 版开始，Sentinel Rapid Deployment 和收集器管理器的全新安装不会运行 Legacy 收集器。不过，升级后的 Sentinel Rapid Deployment 系统和收集器管理器会继续像以前一样运行 Legacy 收集器。

注释： Legacy 收集器是使用 Legacy 收集器构建器应用程序编写的，该应用程序不再随附于 Sentinel 产品中。 Legacy 收集器现由 JavaScript 收集器代替，用户可使用 Sentinel Plug-In SDK 编写此类收集器。 Sentinel 6.1 插件网站 (<http://support.novell.com/products/sentinel/secure/sentinel61.html>) 中提供了 JavaScript 收集器。

1.1.3 安全性提升

Sentinel Rapid Deployment 6.1 SP2 包含多个可提升产品安全性的更新：

- ◆ Java Runtime Environment (JRE) 已升级到版本 1.6.0_24。
- ◆ Apache Tomcat 已升级到版本 6.0.29。
- ◆ PostgreSQL 数据库已升级到版本 8.3.12。

1.2 Sentinel Rapid Deployment SP1 中的新功能

有关 Sentinel Rapid Deployment 6.1 SP1 中的新功能的信息，请参见“[Sentinel Rapid Deployment SP1 自述文件](http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85)” (http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85)。

2 系统要求

有关硬件要求、支持的操作系统和浏览器的详细信息，请参见《*Sentinel Rapid Deployment 安装指南*》中的“[系统要求](#)”。

3 安装 Novell Sentinel Rapid Deployment

安装步骤现已简化，不再需要提供 tar 文件名。您可以下载安装程序，将其提取到某个目录，然后只需运行脚本便能以根用户或非根用户身份进行安装。您还可以指定相应的命令行自变量，只创建用户、安装 Rapid Deployment 服务器、创建服务以在系统启动时自动启动 Sentinel Rapid Deployment，或只安装 Rapid Deployment 服务器而不创建用户或服务。

要安装 Novell Sentinel Rapid Deployment 6.1 SP2，请参见《*Sentinel Rapid Deployment 安装指南*》中的“[安装](#)”。

4 升级到 Sentinel Rapid Deployment SP2

进行升级之前，请确保已在要安装此服务包的系统上安装了 Sentinel 6.1 Rapid Deployment SP1：

要升级到 Sentinel Rapid Deployment 6.1 SP2，请参见《*Sentinel Rapid Deployment 安装指南*》中的“[升级 Sentinel Rapid Deployment](#)”。

5 访问 Sentinel Rapid Deployment 帮助文件

您可以单击 Sentinel 控制中心内的 *帮助* > *帮助* 来访问 Sentinel Rapid Deployment 的联机用户指南。但是，如果您在安全的工作环境下工作，该环境禁止直接访问因特网，您可以一步到位将联机帮助文件下载并提取到 Sentinel Rapid Deployment 服务器上。将帮助文件提取到特定位置后，您便可通过服务器或远程系统访问该文档。您可以通过任何 Web 浏览器查看帮助文件。

注释： 帮助文件只提供英文版本。

下载联机帮助：

- 1 访问 [Sentinel Rapid Deployment 文档网站 \(http://www.novell.com/documentation/sentinel61rd/\)](http://www.novell.com/documentation/sentinel61rd/)。
- 2 单击“可下载用户指南帮助”部分中的 *zip*，然后将 *s61rd_user_help.zip* 文件保存到本地计算机。
- 3 使用以下命令复制并提取下载的文件：

```
cp s61rd_user_help.zip <安装目录>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
cd <安装目录>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
unzip s61rd_user_help.zip
```

重要： 在将 *s61rd_user_help.zip* 文件提取到指定位置前，您无法访问帮助文件。

- 4 执行以下任一操作查看帮助文件：
 - ◆ 在 Sentinel 控制中心内，单击 *帮助* > *帮助*。
 - ◆ 打开 <安装目录>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help/s61rd_user_help/index.html 文件。

Index.html 文件会在导航窗格中列出各主题。单击所需的主题以打开该主题对应的帮助页。

注释： 如果将帮助文件下载并保存到 Sentinel Rapid Deployment 服务器上的指定位置，则单击 Sentinel 控制中心内的 *帮助* 菜单会始终列出服务器上存放的已下载帮助内容。

如果要让 *帮助* 菜单重定向到联机《*Sentinel Rapid Deployment 用户指南*》，请去除 Sentinel Rapid Deployment 服务器上 <安装目录>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help 文件夹中的 *s61rd_user_help*。

6 修复的缺陷和增强的功能

- ◆ [第 6.1 节“修复的缺陷”（第 3 页）](#)
- ◆ [第 6.2 节“增强功能”（第 4 页）](#)

6.1 修复的缺陷

下表列出了 Sentinel Rapid Deployment 6.1 SP2 中存在的缺陷的编号，以及针对这些缺陷所提供的解决方案：

错误编号	解决方案
451892	现在，Sentinel WebStart 应用程序将在必要时自动下载所需的字体。
497131	现在，最新的 eDirectory Collector 可以在报告功能中处理双字节日语字符。
531114	现在，当使用报告 Web 用户界面上载任何非报告 (.zip) 文件时，浏览器将显示一条错误讯息，指出从 package.xml 获取 PluginPackage 时出错。
556730	关联引擎不再将超过 30 秒的未来事件存储到未来类别中，因此不会显示内存不足错误。

错误编号	解决方案
566973	现在,“关联引擎管理器”窗口将会显示关联引擎的列表,即使该窗口是在先前保存的 Sentinel 控制中心会话中打开也是如此。
569849	现在, Sentinel Rapid Deployment 捆绑了最新的 Apache Tomcat 版本 6.0.29,以解决安全漏洞。
573181	对于 Sentinel 进程,现在将以百分比分配内存。另外,还支持通过 memory.conf 文件覆盖内存分配。
600604	性能已得到改善,系统在运行大型报告时不会耗尽内存。
607145	现已创建额外的审计事件,用于监视 Sentinel 管理活动,以及对数据映射、过滤器、关联规则、操作和事件源管理 (ESM) 所做的配置更改。
621509	现在,当用户选择事件 (event)、创建事件 (incident) 以及将事件 (event) 保存为事件 (incident) 的一部分时,新建事件窗口将显示事件 (event)。
623834	仅当使用空间达到根据实际文件系统磁盘空间计算的上限阈值时,才显示磁盘空间用量达到上限阈值讯息。
625930	RulePerformanceSummary 事件中的规则名称不再显示为空。
626402	在 ESM 中重新启动包含多个事件源的连接器不再导致超时异常。
629716	Sentinel 控制中心 (SCC) 实例不再因为死锁问题而冻结。
641087	现在, Sentinel Rapid Deployment 捆绑了最新的 PostgreSQL 增补程序版本 8.3.12,以解决安全漏洞。
644821	ESM 中拥有查看许可权限的用户无法通过在键盘上按 Delete 键来删除节点 (“事件源”、“收集器”、“收集器管理器”)。
648554	现在, Sentinel 数据管理器 (SDM) 配置文件将在用户主目录中创建,而不是在启动 SDM 的位置创建。
651181	运行大型报告时,将使用 Jasper 虚拟化程序来缩短查询时间。
651524	现在,可以使用代理服务器下载 Advisor 传递文件,代理口令将通过下载管理器更新。
656595	与数据库的连接不会泄漏任何连接,因为长时间空闲的开放事务的锁将被释放。
656715	现在,将会压缩通过 ActiveMQ 传输的数据,以改善网络带宽。
662213	现在,可在电子邮件事件 (event) 操作和电子邮件事件 (incident) 操作中向多个收件人地址发送电子邮件。
668443	现在,除了可以通过 pgadmin 连接 PostgreSQL 数据库外,还可以通过命令行进行连接。
672058	当您重新启动一个配置为在指定时间内未收到数据时发出警报的事件源时,该事件源不再生成重复事件 (NoDataAlert) 和日志讯息。
682235	现在, Sentinel Rapid Deployment 捆绑了最新的 Java 版本 1.6.0_24,以解决安全漏洞。

6.2 增强功能

下表列出了为改善可用性而对 Sentinel Rapid Deployment 6.1 SP2 所做的增强:

错误编号	说明
547390	现在,您可以通过在 das_core.xml 文件中设置最大事件数属性来配置脱机查询限制。

错误编号	说明
642690	脱机查询已得到增强，允许在 <code>das_core.xml</code> 文件中配置子区间查询时间。
642691	现在，脱机查询信息的更新状态存储在 <code>das_core</code> 日志文件中。
648108	现在，“Advisor 状态”窗口将显示有关所有传递文件的信息。
673362	JasperPrint 对象文件（即名为 <code>results</code> 的原始结果文件）不再捆绑在报告结果中。Sentinel 并不使用该文件，因此去除它可以改善报告性能，节省磁盘空间。
680054	在 Sentinel Rapid Deployment 服务器中，已添加对绑定 IP 地址的支持，作为一种故障转移机制。

7 已知问题

错误编号	说明
486932	问题： 用户可以删除与某个正在运行的 iTRAC 进程关联的活动。 解决方法： 无。
517568	问题： 尝试单独安装解决方案设计器无法成功。 解决方法： 请使用 Sentinel 控制中心或 Sentinel 数据管理器安装解决方案设计器。
525334	问题： “身份浏览器”显示 Active Directory 域的冗余数据。 解决方法： 无。
598473	问题： 通过非英文系统启动 ESM 用户界面时，6r9 文件连接器不会按预期使用 SCP 协议检索远程文件。 解决方法： 无。将在文件连接器 6r10 版本中解决此问题。
674008	问题： 在 Linux 计算机上，Installshield 向导中不显示 Novell 图标和版权信息。 解决方法： 无。
674720	问题： 尽管 Sentinel 6.1 Rapid Deployment SP2 未包含对收集器构建器选项的支持，但许可协议中仍显示收集器构建器信息。 解决方法： 无。

错误编号	说明
679830	<p>问题：对于 Windows 收集器管理器，映射功能有时无法按预期工作。</p> <p>解决方法：请遵循以下步骤：</p> <ol style="list-style-type: none"> 1. 停止收集器管理器： <ul style="list-style-type: none"> < 安装目录 >/bin/sentinel.bat stop 2. 打开 < 安装目录 >/log 目录中的收集器管理器日志文件 collector_mgr0.0.log。 3. 搜索有无类似于下面的错误： <pre>System temporary directory (java.io.tmpdir property) of C:\Windows\system32\config\systemprofile\AppData\Local\Temp\ appears to be invalid.</pre> 4. 在以下位置创建一个名为 Temp 的文件夹： <p>Windows 64 位系统： C:\Windows\syswow64\config\systemprofile\AppData\Local\</p> <p>Windows 32 位系统： C:\Windows\system32\config\systemprofile\AppData\Local\</p> 5. 重新启动收集器管理器： <ul style="list-style-type: none"> < 安装目录 >/bin/sentinel.bat start
680054	<p>问题：Sentinel Rapid Deployment 服务器无法自动确定 IP 地址。</p> <p>解决方法：请遵循以下步骤：</p> <ol style="list-style-type: none"> 1. 在 < 安装目录 >/sentinel_rd/config 下创建 start_tomcat.properties 文件。 <p>确保运行 Sentinel Rapid Deployment 服务器的用户拥有该文件，并具有执行许可权限。</p> 2. 在新建的文件中添加下行以指定 IP 地址： <pre>SERVER_IP=<ip_address_value></pre> 3. 保存文件。 4. 以 Sentinel 安装文件的所有者身份登录，并使用以下命令重新启动服务器： <pre>sentinel.sh restart</pre> 5. 检查以下位置的 IP 地址，以确定是否使用了覆盖后的 IP 地址： <pre>\$ESEC_HOME/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads</pre> 中的 jnlp 文件
680154	<p>问题：Sentinel 数据管理器上的表空间/选项卡显示错误的已使用空间和可用空间。已使用空间和可用空间是根据 sendata1 表空间计算的，而不是根据实际磁盘空间计算的。</p> <p>解决方法：无。</p>
685187	<p>问题：尝试通过控制台模式安装远程收集器管理器时，安装程序无法从服务器导入中介程序证书。</p> <p>解决方法：要在远程系统上以控制台模式安装收集器管理器，可以在图形模式下使用 ssh 连接到该系统。例如，ssh -x < 系统 IP >。</p>

8 文档

要查看更新的文档和发行说明，请访问 [Sentinel Rapid Deployment 文档网站 \(http://www.novell.com/documentation/sentinel61rd/index.html\)](http://www.novell.com/documentation/sentinel61rd/index.html)。

9 法律声明

Novell, Inc. 对于本文档的内容或使用不做任何陈述或保证，特别是对用于任何特定目的的适销性或适用性不做任何明示或暗示的保证。另外，Novell, Inc. 保留随时修订本出版物和更改其内容的权利，并且没有义务将这些修订或更改通知任何个人或实体。

另外，Novell, Inc. 对任何软件不做任何声明或保证，特别是对用于任何特定目的的适销性或适用性不做任何明示或暗示的保证。另外，Novell, Inc. 保留随时更改 Novell 软件全部或部分内容的权利，并且没有义务将这些更改通知任何个人或实体。

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

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

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

所有第三方商标均是其各自所有者的财产。