Novell Sentinel Log Manager 1.1 发行说明

2010 年 7 月 8 日

Novell

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

- 第 1 节 “Sentinel Log Manager 1.1 的新功能”（第 1 页）
- 第 2 节 “Sentinel Log Manager 1.0.0.5 的新功能”（第 3 页）
- 第 3 节 “系统要求”（第 4 页）
- 第 4 节 “安装 Novell Sentinel Log Manager 1.1”（第 4 页）
- 第 5 节 “Sentinel Log Manager 1.1 中解决的缺陷”（第 4 页）
- 第 6 节 “已知问题”（第 5 页）
- 第 7 节 “文档”（第 7 页）
- 第 8 节 “法律声明”（第 8 页）

1 Sentinel Log Manager 1.1 的新功能

- 第 1.1 节 “角色”（第 1 页）
- 第 1.2 节 “分布式搜索”（第 2 页）
- 第 1.3 节 “标记”（第 2 页）
- 第 1.4 节 “设备”（第 2 页）
- 第 1.5 节 “LDAP 鉴定的增强功能”（第 3 页）
- 第 1.6 节 “报告的增强功能”（第 3 页）
- 第 1.7 节 “数据恢复”（第 3 页）

1.1 角色

管理员现在可以创建角色，并将其指派给任意数量的用户。可以为每个角色指派一组不同的许可权限，而属于某个角色的用户将继承他们所处的角色的许可权限。

Sentinel Log Manager 包含一些具有必需许可权限的默认角色。但是，您可以根据自己的需要修改许可权限并创建更多角色。

有关组权限的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 管理指南》*中的 *“配置用户和角色”*(http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bjxveru.html)。

1.2 分布式搜索

“分布式搜索”功能使您不仅可以在本地 Sentinel Log Manager 服务器上搜索事件，还可以在分布于全球的其他 Sentinel Log Manager 服务器上进行搜索。当您设置分布式搜索配置以将多个服务器与本地服务器 （搜索启动程序）链接后，即可在本地服务器上执行搜索，并可以选择让搜索引擎同时在链接的服务器上执行搜索。系统会检索来自所有选定服务器的相应事件，并将其显示在搜索结果中。搜索结果中的每个事件都会显示服务器信息，事件即从这些信息中检索而出。

使用这一新功能时，还可以导出搜索结果、将搜索结果发送给某个操作和检索原始数据事件。同时，报告引擎也进行了改进，现在将使用同一个基础搜索引擎，这样报告就可以包含来自多个 Sentinel Log Manager 服务器的数据。

有关分布式搜索的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 管理指南》*中的“在分布式环境中搜索和报告事件”(http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bp5lx14.html)。

1.3 标记

“标记”功能可让您创建一个或多个可搜索的标记属性，并将其指派给事件管理系统 (ESM) 节点 （例如事件源、事件源服务器、收集器管理器和收集器插件）和报告。来自这些 ESM 节点的所有事件也会进行标记。您可以通过标记功能对这些 ESM 节点、事件本身和报告进行逻辑分组。

可以根据应用于事件的标记来搜索这些事件，还可以根据事件源和报告带有的标记来对它们进行过滤。

Sentinel Log Manager 包含一些默认标记；不过，您可以根据自己的需要创建新标记。

有关标记的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 管理指南》*中的“配置标记”(http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bp62o80.html)。

1.4 设备

Sentinel Log Manager 设备是一种可直接运行的软件设备，它使用 Novell SUSE Linux Enterprise Server (SLES) 11 操作系统和 Novell Sentinel Log Manager 软件，同时提供更新服务。此设备提供了增强的基于浏览器的用户界面，支持对来自众多设备和应用程序以及各种协议的日志数据进行收集、储存、报告和搜索。

Sentinel Log Manager 1.1 设备支持以下格式：

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

注释：Sentinel Log Manager 1.0 用户可以按照 *《Novell Sentinel Log Manager 1.1 安装指南》*的第 6.4 节 “从 1.0 迁移到 1.1 设备”(http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bq9ckex.html) 中的说明将其安装迁移到 Sentinel Log Manager 1.1 设备。

有关 Sentinel Log Manager 设备安装的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 安装指南》*(http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html) 中的 “安装设备”。

1.5 LDAP 鉴定的增强功能

- *用户*选项卡下提供了新的用户界面，可用于将 Sentinel Log Manager 服务器配置为使用 LDAP 鉴定。
- 可通过或不通过匿名搜索在 LDAP 目录上执行 LDAP 鉴定。

有关 LDAP 鉴定的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 管理指南》*中的 “LDAP 鉴定”(http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bpfef67.html)。

1.6 报告的增强功能

报告功能已进行了改进，能够向下钻取组成报告的事件。此向下钻取选项可让您能够使用用于生成报告的相同查询和时间范围来起动搜索，以便用户可以查看用于生成报告的事件的细节。

一次可以导出多个报告定义和报告结果，并且一次可以从报告定义导出压缩文件或收集器程序包文件中导入多个报告定义。

有关这些增强功能的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 管理指南》*中的 “报告”(http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bjxdi87.html)。

系统会添加新报告模板并更新现有报告模板。还会删除一些未使用的报告模板。有关可用的报告模板的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 管理指南》*中的 “Sentinel Log Manager 报告”(http://wwwtest.provo.novell.com/documentation/novelllogmanager11/log_manager_admin/index.html?page=/documentation/novelllogmanager11/log_manager_admin/data/bl5jfoz.html)。

1.7 数据恢复

新的数据恢复功能可以恢复旧的、已丢失的或已删除的事件数据。您还可以对恢复的事件数据执行搜索。

新的*数据恢复*部分已添加到*储存* > *配置*用户界面中。您可以选择特定的事件分区来恢复事件数据，还可以配置恢复的事件分区再次失效的时间。

有关数据恢复的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 管理指南》*中 “配置数据储存”(http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/) 中的*恢复事件数据*。

2 Sentinel Log Manager 1.0.0.5 的新功能

- 第 2.1 节 “Sentinel Log Manager 的 500 EPS 版本”（第 4 页）
- 第 2.2 节 “新的最终用户许可证协议”（第 4 页）

2.1 Sentinel Log Manager 的 500 EPS 版本

Novell Sentinel Log Manager 现在提供了 500 EPS （每秒的事件数）版本。 500 EPS 版本适用于只有一个 Sentinel Log Manager 服务器并且事件率较低的小型部署。在大型部署中，它还可以用作向其他 Sentinel 或 Sentinel Log Manager 服务器报告的低容量节点。

2.2 新的最终用户许可证协议

此版本中更新了最终用户许可证协议 (EULA) 条款。您必须先接受新条款才能继续应用最新的增补程序。最终用户许可证协议中的一些更改如下：

- Novell Sentinel Log Manager 现在提供了 500 EPS 版本。
- 更新了非生产实例的定义。
- 更新了类型 I 设备的定义。

3 系统要求

自 Sentinel Log Manager 1.0 发布以来，系统要求中就没有重大更改了。

有关硬件要求以及支持的操作系统、浏览器和事件源的详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 安装指南》*(http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html)。

4 安装 Novell Sentinel Log Manager 1.1

要安装 Novell Sentinel Log Manager 1.1，请参阅 *《Novell Sentinel Log Manager 1.1 安装指南》*(http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html)。

5 Sentinel Log Manager 1.1 中解决的缺陷

错误编号	说明
617478	入侵检测系统的前 10 个报告现在可以创建为 *DeviceAttackName* 字段，并且现在包含在“事件”字段中。
609811	当用户的口令更改时， *TargetUserName* 和 *InitiatorIP* 字段现在会按预期填入值。
609814	当用户登录 Sentinel Log Manager 时， *InitiatorIP* 字段现在会按预期填入值。
607143	新报告已创建，可用于对内部事件执行审计。
606861	您现在可以对包含大写字符的事件执行通配符搜索。
592503	您在*简化*面板中添加的其他搜索查询现在显示相应的结果。
587831	当 *CustomerVar22* 字段添加为要显示的额外字段时，*简化*面板现在显示该字段的事件数。
567082	口令中含有非标准字符的用户现在可以按预期登录 Web 用户界面和 ESM 界面。

错误编号	说明
565777	“信任管理”报告现在包含 DEASSOC_TRUST 事件，这些事件是在去除用户帐户时生成的。
526062	Web 用户界面中的*配置*链接现在已更换为齿轮图标，这表示该图标旁边的链接是配置链接。
524575	所有 JavaScript 弹出式窗口 （例如 “搜索提示”、“运行”和 “删除”）现在按预期显示在法语版、西班牙语版和意大利语版的 Internet Explorer 8 上。
503808	当 Sentinel Log Manager 初次安装在它以前从未安装过的某台服务器上时， ESM 现在会按预期起动。
545436	内部审计事件字段 （例如 initUserName、 initIP 和 targetUserNamedetails）现在填入了相应的值，并且显示在搜索结果中。

6 已知问题

错误编号	说明
620681	**问题：**在 ESM 中，“收集器”节点在重新启动服务器期间被错误地设置为已停止状态。但是，这是个别问题。 **解决方法：**在重新启动服务器之后，登录 ESM，并确保应该运行的收集器设置为启动状态。

620100	**问题：**远程收集器管理器对旧收集器不起作用。
	
	解决方法：修改远程收集器管理器计算机中的 ESEC_HOME/config/collector_mgr.xml 文件。
	
	1. 在任何编辑器中打开 ESEC_HOME/config/collector_mgr.xml 文件。
	2. 更改以下行：
	
	`<property name="workbench.home">..</property>`
	`<property name="properties.file">../config/`
	`collector_mgr.properties</property>`
	`<property name="esecurity.home">..</property>`
	
	更改为
	
	`<property name="workbench.home">${user.dir}/..</property>`
	`<property name="properties.file">../config/`
	`collector_mgr.properties</property>`
	`<property name="esecurity.home">${user.dir}/..</property>`
	
	3. 重新启动远程收集器管理器服务。

617318	**问题：**在您将较早版本的 Sentinel Log Manager 升级为 Sentinel Log Manager 1.1 之后，*另存为报告* > *可视化*下拉列表应该只包含报告模板。但是，一些特定于收集器的报告可能仍然显示在*可视化*列表中，因为如果这些报告在升级之前正在使用，则可能在升级期间无法删除。 **解决方法：**出现这种情况是因为列表中显示的特定于收集器的报告在升级期间没有自动更新。从 Sentinel 6.1 内容网站 (http://support.novell.com/products/sentinel/sentinel61.html) 下载更新的收集器程序包，然后使用 Sentinel Log Manager 报告上载选项上载该程序包。

错误编号	说明
617663	**问题：**在*集合* > *事件源服务器*页面上，当您修改事件源的多个字段并单击*保存*刷新该页面时，只有一个字段进行了更新，而其他字段显示旧值。 **解决方法：**一次更改一个字段的值。在修改完每个字段后，单击*保存*。
617477	**问题：**在搜索结果的事件字段上单击 Alt+ 向左键头以将 NOT 子句添加到空查询时没有起到预期的作用，因为不允许进行纯 NOT 条件的查询。 **解决方法：**如果您使用 sev:[0 TO 5] 查询而不是空查询开始搜索，则单击 Alt+ 向左键头就会起到预期的作用。这两种查询检索到的事件都是一样的。
618294	**问题：**当主字段为空时，“事件摘要”、“前 10 个报告”和 “前 10 个仪表板”基本报告显示值为 -0-（而不是空值）的事件。 **解决方法：**对于 “事件摘要”和 “前 10 个报告”报告，不要选择没有数据 （为空）的主字段。对于 “前 10 个仪表板”报告，忽略将 -0- 用作 X 轴中的值的字段图。
617103	**问题：**如果较大报告在运行过程中配置了 NFS 存档，则 server_wrapper.log 文件中会记录异常。 **解决方法：**在 EPS 处于最低值时 （例如夜晚或周末）运行较大报告。本地存储 RAID 阵列中的磁盘增多可能也会有帮助。
614686	**问题：**当较大报告在拥有大约 2 亿个事件的系统上运行时，搜索查询超时并且记录异常。 **解决方法：**在执行大型搜索时，避免运行较大报告。
613960	**问题：**远程收集器管理器 Installshield 向导显示 Sentinel 6.1 而不是 Sentinel Log Manager。 **解决方法：**无。这是用户界面问题。
608905	**问题：**在您添加许可证密钥之后， Sentinel Log Manager 用户界面未提示重新启动 Sentinel 服务，并且没有按预期执行某些操作。 **解决方法：**在添加许可证密钥之后，重新启动 Sentinel Log Manager 服务器。
606567	**问题：**在设备上，平台版本每两分钟通过内核讯息记录到 syslog （位于 /var/log/messages）中。 **解决方法：**这些讯息都是特意发送的，以便操作系统可以将其版本告知 Sentinel Log Manager。如果这些讯息出于某些原因而导致出现问题，请禁用 wtmpmon 脚本以防止生成这些讯息。
593435	**问题：**如果 Sentinel Log Manager 1.1 安装重新定位到路径中含有空格的基本目录中，则 Sentinel Log Manager 服务器不按预期运行。例如， /home/user/Sentinel Log Manager。 **解决方法：**请确保目录的路径中不包含空格。
560966	**问题：**在配置文件连接器时，如果您单击*浏览*添加事件源，则文件浏览器不显示，并且控制中心日志文件中记录了异常。 **解决方法：**指定所需文件路径，或者将该文件路径复制 / 粘贴到字段中，而不是使用*浏览*按钮。

错误编号	说明
577073	当事件源数目大约有 3000 个时，如果原始数据分区从打开状态转为记录状态，则 EPS 率下降到 0。 **解决方法：**安装其他的 Sentinel Log Manager 实例，以使每个实例的事件源总数小于系统要求中指定的建议设备数上限。有关详细信息，请参阅 *《Novell Sentinel Log Manager 1.1 安装指南》*中的 “系统要求”(http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bjx8zq7.html)。
617350	**问题：**在安装增补程序更新时， WebYaST 报告 DBus.Error.LimitsExceeded 错误。 **解决方法：**重新启动 yastws 服务： `/etc/init.d/yastws restart` 或者，单击控制面板中的*重引导*来重新启动计算机。
607684	**问题：**当您从 ISO 设备映象引导计算机（即将 ISO 作为 Live CD/DVD 运行）时，如果通过 “WebYast” > “更新”运行增补程序更新，则系统会转为非响应状态。 **解决方法：**将 Live DVD 安装到硬件中，然后运行增补程序更新。
609187	**问题：**在超过一百万个事件的系统上，在您开始生成报告并单击*取消*以取消报告生成后，报告生成仍在进行中，并没有取消。 **解决方法：**无。
593788	**问题：**安装之后， Sentinel Log Manager 初次登录 Web 用户界面大约需要 5 分钟时间。 **解决方法：**无。
510824	**问题：**在您单击各个搜索结果的*细节* ++ 链接之后，*所有细节* ++ 和*所有细节* -- 链接没有按预期的那样对前 25 个事件起作用。 **解决方法：**无。
548515	**问题：**Sentinel Log Manager 中的示例报告显示 Sentinel Log Manager 中未提供的用户数据，例如全名、部门和职员 ID。 **解决方法：**无。
509549	**问题：**在具有 75,000 多个事件的 “搜索结果”页面上，当您向下滚动鼠标以查看事件时，滚动条不在滚动点停止，并且频繁地改变其位置。 **解决方法：**无。
615572	**问题：**Sentinel Log Manager 可让您在编辑目标服务器细节时更改目标服务器的 IP 地址，但不显示任何表示 “指定的 IP 地址不一样”的讯息。 **解决方法：**无。
545436	**问题：**当您停止收集器时， stopcollector 内部事件在事件日志中生成了两次。生成的第二个 stopcollector 事件没有显示正确的 initUserName、initIP 和 targetUserNamedetails 事件字段值。 **解决方法：**无。

7 文档

要查看更新的文档和发行说明，请访问 Sentinel Log Manager 文档网站 (http://www.novell.com/documentation/novelllogmanager11/)。

8 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/)。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。

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)。

所有第三方商标均是其各自所有者的财产。