Sentinel 8.5 发行说明

2021 年 8 月

Sentinel 8.5 解决了以前的几个问题，并增加了一些新功能。

其中的很多改进都是直接按照我们客户提供的建议做出的。非常感谢您在百忙之中为我们提供宝贵的意见。我们衷心希望您继续为我们提供意见，以确保我们产品满足您的一切需求。您可以在 Sentinel 论坛中发布反馈，这一论坛是我们的线上社区，其中还有产品信息、博客和有用资源的链接。您还可以在 Ideas Portal （想法门户）中共享改善产品的想法。

我们在一个公开网页 （无需登录）上以 HTML 和 PDF 格式提供了此产品的相关文档。如果您对文档改进有任何建议，请单击发布在 Sentinel 文档页的 HTML 版本文档的任一页上的评论图标。要下载本产品，请参见产品下载网站。

- 新增功能？ （第 1 页）
- 系统要求 （第 3 页）
- 许可证和采购信息 （第 3 页）
- 安装 Sentinel 8.5 （第 4 页）
- 升级到 Sentinel 8.5 （第 4 页）
- 已知问题 （第 4 页）
- 联系 Micro Focus （第 10 页）
- 法律声明 （第 10 页）

新增功能？

以下几节概述了此版本提供的主要功能，以及此版本解决的问题：

- ArcSight Intelligence 与 Sentinel 集成 （第 2 页）
- MITRE ATT&CK （第 2 页）
- JDK 升级 （第 2 页）
- 储存来自连接器的原始事件 （第 2 页）
- TLS 支持 （第 2 页）
- 操作系统 (OS) 版本 （第 3 页）
- 软件修复 （第 3 页）

ArcSight Intelligence 与 Sentinel 集成

通过此版本， Sentinel 客户能够集成 ArcSight Intelligence 卓越的分析技术。因此， Sentinel 用户几乎可以实时获得风险得分，并将其用于自身关联规则的进一步分析等。这样 Sentinel 可以获得许多威胁搜寻经验。

ArcSight Intelligence 是一种用户和实体行为分析解决方案，使用数据科学和高级分析来识别组织中风险最高的实体和行为。 Intelligence 首先为您的组织实体建立正常的行为，然后使用高级分析识别任何实体的异常行为，并为各此类实体提供相应的风险得分。

Sentinel 提供了一种与 ArcSight Intelligence 6.3 集成的方法。这种集成有助于 Sentinel 用户将其数据发送到 ArcSight Intelligence 进行分析，并且提供了从 Intelligence 接收实体风险得分细节的方法。这样 Sentinel 能够检测到组织中任何可能危害整个系统并造成潜在威胁的风险较高的用户和实体。

MITRE ATT&CK

MITRE ATT&CK 有助于网络安全团队评估其安全运营中心 (SOC) 进程和防御措施的有效性，以确定需要改进的方面。 MITRE ATT&CK 是基于实际监测到的网络安全对抗策略和技术的全球可访问知识库。私人部门、政府、网络安全产品和服务社区将 MITRE ATT&CK 知识库用作开发特定威胁模型和方法的基础。

从此 Sentinel 版本开始，管理员可以映射关联规则与 MITRE ATT&CK ID。 MITRE ATT&CK 代表 MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)。 MITRE ATT&CK 框架是基于实际监测到的威胁参与者策略和技术的通用行业语言。

Sentinel 管理员现在可以直接将自己的即用型关联规则或自定义关联规则与 MITRE ATT&CK ID 映射。因此，提供大量触手可及的数据分析，这样管理员能够可视化触发了哪些规则以及用户使用了哪些策略和 MITRE 技术。 Sentinel 为管理员提供了一套工具集，通过这些工具集，他们可以立即查看网络以及需要阻止的最重要的攻击。

如果触发了与 MITRE ATT&CK ID 映射的关联规则，则触发的事件将具有 MITRE ATT&CK ID 和 MITRE ATT&CK 名称。将通过默认安全状态仪表板中的控件分析这些事件。此仪表板中显示排名前十的 MITRE ATT&CK 名称，时间范围为 1 天，显示间隔为 1 小时。

JDK 升级

为了避免安全漏洞 （CVE-2021-2161、 CVE-2021-2163、 CVE-2021-2341、 CVE-2021-2432、 CVE-2021-2369、 CVE-2021-2388），以及为了利用 JDK 新标准的安全功能， JDK 从 1.8.0_update242 升级为 1.8.0_update302

储存来自连接器的原始事件

从 2021.1r1 版开始， Sentinel Syslog 连接器将开始储存通过 ArcSight Smart Connector 进来的原始事件。这些事件是终端设备直接生成的未经改动、未处理的事件。可通过勾选相应的 Smart Connector 中的 **Preserve Raw Event** （保留原始事件）选项启用此设置。

TLS 支持

已去除对 TLS 1.0 和 TLS 1.1 的支持。

操作系统 (OS) 版本

传统安装：Sentinel 现在也在以下新平台上获得认证：

- Red Hat Enterprise Linux (RHEL) 8.3

已弃用 OS：以下 OS 已弃用，因为 RHEL 和 SLES 支持已从这些 OS 中去除：

- RHEL 7.6 和 7.7
- SLES 15 SP1

软件修复

Sentinel 8.5 包括能够解决以下问题的软件修复：

- 转换为 Sentinel 服务器上的 FIPS 会将协议 TLS 1.2 更改为 1.1 （第 3 页）
- 升级 Sentinel Java 客户端后， Sentinel REST 调用失败 （第 3 页）
- 生成新报告时出错 （第 3 页）

转换为 Sentinel 服务器上的 FIPS 会将协议 TLS 1.2 更改为 1.1

问题：当转换为 Sentinel 服务器上的 FIPS 时，协议会从 TLS 1.2 更改为 1.1，这会导致 SAM 和 Sentinel 服务器之间的连接终止。但是，客户必须使用 TLS 1.2

修复：现在，当转换为 FIPS 时， TLS 版本不会从 1.2 更改为 1.1

升级 Sentinel Java 客户端后， Sentinel REST 调用失败

问题：将 Sentinel Java 客户端从 8.1 升级到 8.2 后， REST 调用失败。

修复：将 Sentinel Java 客户端从 8.1 升级到 8.2 后， REST 调用正常。

生成新报告时出错

问题：生成新报告时出错。错误的主要问题可能是篡改了密钥存储区或口令错误。

修复：生成新报告时不会出错。

系统要求

关于硬件要求、支持的操作系统和浏览器的更多信息，请参见 Sentinel System Requirements （Sentinel 系统要求）。

许可证和采购信息

要购买企业许可证或升级现有许可证，请致电 1-800-529-3400，发送电子邮件至 info@microfocus.com 或访问 https://www.microfocus.com/en-us/products/netiq-sentinel/contact。

安装 Sentinel 8.5

有关安装 Sentinel 8.5 的信息，请参见 *Sentinel Installation and Configuration Guide （《Sentinel 安装和配置指南》）*。

注释：用于 Sentinel 服务器及其组件的所有主机都必须在双向 DNS 可解析环境 （主机名到 IP 和 IP 到主机名）中设置。

升级到 Sentinel 8.5

您可以从任何先前版本的 Sentinel （从 Sentinel 8.2 及更高版本）升级到 Sentinel 8.5。

重要：由于最新的 JDK 升级，为了配置 LDAPS 和 SDK，用户需要使用主机名而不是 IP 地址，而且主机名必须可解析。

重要：传统安装和设备安装的升级过程发生了变化。请参阅 Settings in Elasticsearch for Secure Cluster Communication （Elasticsearch 中用于确保群集通讯安全的设置），并遵循步骤。仅适用于将 Sentinel 从 8.3.1 和之前的版本升级到最新版本时。

重要：您可以通过下载每个设备的脱机补丁 ISO 执行脱机更新。有关更多信息，请参阅 Performing Offline Updates （执行脱机更新）。

警告：如果您从 Sentinel 8.3 之前的版本升级到 8.3，必须手动为将事件或附件发送到 Sentinel 的非管理员用户指派 **Send events and attachments** （发送事件和附件）许可权限。如果不指派此许可权限，Sentinel 将不再接收来自 Change Guardian 和 Secure Configuration Manager 的事件和附件。

对于传统安装，请参阅 *Sentinel Installation and Configuration Guide* （《Sentinel 安装和配置指南》）中的 Upgrading the Operating System （升级操作系统）。

已知问题

Micro Focus 力求确保我们的产品提供高品质的解决方案，以满足贵企业的软件需求。以下已知问题目前正在研究中。如果需要有关任何问题的进一步帮助，请联系技术支持。

Sentinel 中包含的 Java 8 更新可能会影响以下插件：

- Cisco SDEE 连接器
- SAP (XAL) 连接器
- Remedy 集成商

有关这些插件的任何问题，我们将根据标准的缺陷处理策略优先考虑和修复这些问题。有关支持策略的更多信息，请参见支持策略。

- 无法查看储存容量预测图表 （第 5 页）
- 升级 Sentinel 后起动 Kibana 仪表板时出错 （第 5 页）

- 无法复制 Mozilla Firefox 和 Microsoft Edge 中警报视图中所有警报的警报链接 （第 6 页）
- 将 Sentinel、收集器管理器和关联引擎安装为 OVF 设备映像不显示登录屏幕 （第 6 页）
- 重引导时， Microsoft Hyper-V Server 2016 中的 Sentinel 8.2 设备不启动 （第 6 页）
- 升级至 Sentinel 8.2 HA 设备时出现错误 （第 6 页）
- MFA 模式下以非英语安装收集器管理器和关联引擎设备失败 （第 7 页）
- 设备安装屏幕中的可用性问题 （第 7 页）
- 如果 Open-vm-tools 中启用时间同步，收集器管理器内存不足 （第 7 页）
- 启用 FIPS 140-2 模式时，代理管理器要求进行 SQL 鉴定 （第 7 页）
- 在非 FIPS 140-2 模式下进行 Sentinel 高可用性安装会显示错误 （第 7 页）
- Keytool 命令显示警告 （第 8 页）
- 在 FIPS 模式下， Sentinel 不处理威胁智能源 （第 8 页）
- 在多因子鉴定模式下，从 Sentinel Main 注销不会使您从仪表板注销，反之亦然 （第 8 页）
- 升级到 Sentinel 8.3.1 后， Kibana 自定义仪表板不显示 （第 8 页）
- 当您起动 Kibana 时，显示冲突错误讯息 （第 8 页）
- 当您重引导 OS Redhat 8.1 和 8.2 时， Sentinel 未自动启动 （第 8 页）
- 当您打开 Sentinel 设备管理控制台时，显示一条错误讯息 （第 9 页）
- 具有隐藏可视化管理许可权限的用户仍可以在 Kibana 页面中看到管理选项卡 （第 9 页）
- 管理员更改警报的用户角色后， Kibana 页面中的更改不会立即更新 （第 9 页）
- 当您以租户用户的身份起动可视化仪表板时，显示一条错误讯息 （第 9 页）
- 在 RHEL 中，当启用 CRL 时， RCM 和 RCE 没有连接到服务器 （第 9 页）
- 当启用事件可视化、 FIPS 和 CRL 时， RCM 不会将事件转发到 Sentinel 服务器 （第 9 页）
- 将 OS 从任何旧版本升级到最新版本后，事件报告因异常而失败 （第 9 页）
- 首次尝试重新建立索引时记录异常 （第 10 页）
- 在 Sentinel 8.5 RCM/RCE 设备版本中运行 `convert_to_fips.sh` 时出错 （第 10 页）

无法查看储存容量预测图表

问题：在 **Sentinel Main** > **储存** > **运行状况**中，**储存容量预测**图表不可用。这是因为 Zulu OpenJDK 中没有必要的字体。

解决方法：使用以下命令安装字体：

- yum install fontconfig
- yum install dejavu

升级 Sentinel 后起动 Kibana 仪表板时出错

问题：起动 Kibana 仪表板显示以下讯息：No default index pattern.You must select or create one to continue.

解决方法：要将 Kibana 索引模式设置为默认索引模式：

1. 选择下列任意选项：
   - alerts.alerts
   - security.events.normalized_*
2. 单击 **Set as Default** （设置为默认）。

无法复制 Mozilla Firefox 和 Microsoft Edge 中警报视图中所有警报的警报链接

问题：选择所有 < *警报数* > 个警报 > 复制警报链接选项在 Firefox 和 Edge 中不可用。

解决方法：请执行下列步骤：

1. 使用允许您选择所有警报的复选框手动选择警报视图每页中的所有警报。
2. 单击**复制警报链接**。
3. 将其粘贴到目标应用程序中。

将 Sentinel、收集器管理器和关联引擎安装为 OVF 设备映像不显示登录屏幕

问题：进度屏幕中安装程序停止安装，即使安装完成也不会显示登录屏幕。

解决方法：重引导虚拟机，然后起动 Sentinel、收集器管理器或关联引擎。

重引导时， Microsoft Hyper-V Server 2016 中的 Sentinel 8.2 设备不启动

问题：在 Hyper-V Server 2016 中重新启动 Sentinel 设备时，设备不启动并显示下列讯息：

```
A start job is running for dev-disk-by\..
```

出现此问题是因为操作系统在安装期间修改了磁盘 UUID。因此重新启动时，设备找不到磁盘。

解决方法：手动修改磁盘 UUID。有关更多信息，请参见知识库文章 7023143。

升级至 Sentinel 8.2 HA 设备时出现错误

问题：升级至 Sentinel 8.2 HA 设备时， Sentinel 显示下列错误：

```
Installation of novell-SentinelSI-db-8.2.0.0-<version> failed:
with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Command exited
with status 1.
Abort, retry, ignore? [a/r/i] (a):
```

解决方法：响应上述提示前，执行下列操作：

1. 使用 PuTTY 或其他类似软件在运行升级的主机上再打开一个会话。
2. 在 /etc/csync2/csync2.cfg 文件中添加下列条目：

   /etc/opt/novell/sentinel/config/configuration.properties

3 从 /var/opt/novell 去除 sentinel 文件夹：

rm -rf /var/opt/novell/sentinel

4 返回至启动升级的会话并输入 r 继续升级。

MFA 模式下以非英语安装收集器管理器和关联引擎设备失败

问题：如果操作系统语言为非英语，在 MFA 模式下安装收集器管理器和关联引擎设备失败。

解决方法：以英语安装收集器管理器和关联引擎设备。安装完成后再将语言改为所需语言。

设备安装屏幕中的可用性问题

问题：设备安装屏幕中的下一步和返回按钮在某些情况下不显示或为禁用状态，例如：

- 在 Sentinel 预检查屏幕中单击返回以编辑或查看 Sentinel 服务器设备网络设置屏幕中的信息时，没有下一步按钮以继续执行安装。配置按钮仅允许您编辑指定的信息。
- 如果指定了错误的网络设置，“Sentinel 预检查 ” 屏幕将指示由于网络信息不正确而无法继续安装。没有返回按钮进入上一屏幕以修改网络设置。

解决方法：重新开始安装设备。

如果 Open-vm-tools 中启用时间同步，收集器管理器内存不足

问题：如果手动安装 open-vm-tools 并启用其中的时间同步，它们将定期同步 Sentinel 设备 (guest) 和 VMware ESX 服务器 （主机）间的时间。这些时间同步将导致 guest 时间早于或晚于 ESX 服务器时间。Sentinel 设备 (guest) 和 ESX 服务器 （主机）间时间同步前， Sentinel 不处理任何事件。这样一来，收集器管理器中会有大量事件排队，最终可能导致达到阈值后丢失事件。为避免这种情况， Sentinel 默认禁用 Sentinel 中可用版本 open-vm-tools 的时间同步。

解决方法：禁用时间同步。有关禁用时间同步的更多信息，请参见禁用时间同步。

启用 FIPS 140-2 模式时，代理管理器要求进行 SQL 鉴定

问题：在 Sentinel 中启用 FIPS 140-2 模式时，对 Agent Manager 使用 Windows 鉴定，会导致与 Agent Manager 数据库同步失败。

解决方法：为 Agent Manager 使用 SQL 鉴定。

在非 FIPS 140-2 模式下进行 Sentinel 高可用性安装会显示错误

问题：在非 FIPS 140-2 模式下成功完成了 Sentinel 高可用性安装，但会显示以下错误两次：

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

解决方法：应该显示该错误，您可以安全地将其忽略。虽然安装程序会显示错误，但 Sentinel 高可用性配置将在非 FIPS 140-2 模式下成功地正常工作。

Keytool 命令显示警告

问题：使用 Keytool 命令时，显示以下警告：

```
The JKS keystore uses a proprietary format. It is recommended to migrate to
PKCS12which is an
industry standard format using "keytool -importkeystore -srckeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -destkeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -deststoretype pkcs12".
```

解决方法：应该显示该警告，您可以安全地将其忽略。虽然已显示警告， Keytool 命令仍按预期运作。

在 FIPS 模式下， Sentinel 不处理威胁智能源

问题：在 FIPS 模式下，处理来自 URL 的现成可用威胁智能源时， Sentinel 显示以下错误：Received fatal alert: protocol_version （收到严重警报：protocol_version）。 This issue occurs because the out-of-the-box threat feeds now support only TLS 1.2, which does not work in FIPS mode. （出现此问题是因为即用型威胁源现在只支持 TLS 1.2，但 TLS 1.2 在 FIPS 模式下不起作用。）

解决方法：执行以下操作：

1. 单击 **Sentinel Main** > **集成** > **威胁智能来源**。
2. 编辑每个 URL 以将协议从 http 改为 https。

在多因子鉴定模式下，从 Sentinel Main 注销不会使您从仪表板注销，反之亦然

问题：在多因子鉴定模式中，如果您从 **Sentinel Main** 注销，不会使您从 Sentinel 仪表板注销，反之亦然。这是由 Advanced Authentication Framework 中的一个问题造成的。

解决方法：Advanced Authentication Framework 中提供修复前，刷新屏幕以查看登录屏幕。

升级到 Sentinel 8.3.1 后， Kibana 自定义仪表板不显示

问题：当您从 Sentinel 8.3 或更早版本升级到 Sentinel 8.3.1 时， Kibana 自定义仪表板不显示。

解决方法：在升级 Sentinel 后，请确保重新创建自定义仪表板。

当您起动 Kibana 时，显示冲突错误讯息

问题：安装或升级 Sentinel 后，当您首次起动 Kibana 时，显示冲突错误讯息。

解决方法：忽略冲突错误讯息，因为不会影响功能。

当您重引导 OS Redhat 8.1 和 8.2 时， Sentinel 未自动启动

问题：在 OS Redhat 8.1 和 8.2 上安装 Sentinel 后，重引导后未自动启动 Sentinel （服务器、 RCM 或 RCE）。

解决方法：在文件 /etc/selinux/config 中将 SELINUX 值更改为 **SELINUX=disabled**。

当您打开 Sentinel 设备管理控制台时，显示一条错误讯息

问题：升级到 Sentinel 8.3 后，当您尝试打开 HA （高可用性）服务器的 CE （关联引擎）或 CM （收集器管理器）的 Sentinel 设备管理控制台时，显示错误讯息 Error 404 - Not found （错误 404 - 未找到）。

解决方法：有关更多信息，请参阅 Micro Focus Knowledge Base document （Micro Focus 知识库文档）。

具有隐藏可视化管理许可权限的用户仍可以在 Kibana 页面中看到管理选项卡

问题：升级到 Sentinel 8.4 后，具有隐藏可视化管理权限的用户仍然可以在 Kibana 页面上看到管理选项卡，但无法访问管理选项卡的功能。

管理员更改警报的用户角色后， Kibana 页面中的更改不会立即更新

问题：现有用户无法立即在 Kibana 页面上看到任何警报，尽管管理员已更新了查看警报的许可权限。

解决方法：当用户许可权限更新时，您需要注销然后重新登录。

当您以租户用户的身份起动可视化仪表板时，显示一条错误讯息

问题：当非默认租户用户起动可视化仪表板时，显示一条错误讯息已禁止。每当仪表板由非默认租户（对管理选项具有 View-only （只读）许可权限，该租户下没有用户具有管理选项的编辑许可权限）起动时，就会显示此错误讯息。

解决方法：忽略错误讯息，因为不会影响功能。

在 RHEL 中，当启用 CRL 时， RCM 和 RCE 没有连接到服务器

问题：在 RHEL 中启用 CRL 时，远程收集器管理器 (RCM) 和远程关联引擎 (RCE) 无法连接到服务器。

解决方法：将计算机上的 cURL 版本升级到 7.60 或更高版本。

当启用事件可视化、 FIPS 和 CRL 时， RCM 不会将事件转发到 Sentinel 服务器

问题：在新安装分布式安装中，启用事件可视化、 FIPS 和 CRL 服务后，远程收集器管理器 (RCM) 不会将事件转发到 Sentinel 服务器。

解决方法：如果启用了事件可视化和 FIPS 或事件可视化和 CRL，那么 RCM 会将事件转发到 Sentinel 服务器。

将 OS 从任何旧版本升级到最新版本后，事件报告因异常而失败

问题：当您升级操作系统，从旧版本升级到最新版本时，事件报告因异常而失败。

首次尝试重新建立索引时记录异常

问题：首次运行重新建立索引操作时记录异常。

在 Sentinel 8.5 RCM/RCE 设备版本中运行 convert_to_fips.sh 时出错

问题：当系统管理员在 Sentinel 8.5 RCM/RCE 设备版本中运行 convert_to_fips.sh 时，在持续循环中提供正确的身份凭证后，会显示以下错误讯息：

```
ERROR: Failed to connect to <Sentinel server IP>:
Failed to retrieve token for communication channel.
```

解决方法：请执行下列步骤：

1. 退出脚本执行。
2. 转至 <Sentinel RCM/RCE installation>/etc/opt/novell/sentinel/config/configuration.properties
3. 将 rest.endpoint.port 值设为相应的网络服务器端口。

   例如， rest.endpoint.port=8443
4. 重新运行 convert_to_fips.sh

联系 Micro Focus

如果遇到特定的产品问题，请通过 https://www.microfocus.com/support-and-services/ 联系 Micro Focus 支持人员。

可从多种来源获取其他技术信息或建议：

- 产品文档、知识库文章和视频：https://www.microfocus.com/support-and-services/
- Micro Focus 社区网页：https://www.microfocus.com/communities/

法律声明