

# vRealize Log Insight 8.1.1 发行说明

## 发行说明内容

本说明包含以下主题：

- [关于 vRealize Log Insight](#)
- [新增功能](#)
- [兼容性](#)
- [限制](#)
- [从先前版本升级](#)
- [国际化支持](#)
- [已解决的问题](#)
- [已知问题](#)

## 关于 vRealize Log Insight

vRealize Log Insight 专为 VMware 环境提供最佳的实时存档日志管理功能。利用基于机器学习的智能分组和高性能搜索功能，可以更快地在物理、虚拟和云环境中进行故障排除。vRealize Log Insight 可以使用现代 Web 界面分析数太字节的日志、发现非结构化数据中的结构，以及提供企业范围的可见性。

有关详细信息，请参见 vRealize Log Insight 产品文档，网址为 <https://docs.vmware.com/cn/vRealize-Log-Insight/index.html>。

## 新增功能

vRealize Log Insight 8.1.1 是一个维护版本，其中修复了一些安全问题。此版本还有助于您利用社区支持的内容包所具有的优势。您可以从 VMware Sample Exchange 下载这些内容包，并将其导入 vRealize Log Insight。

## 兼容性

vRealize Log Insight 8.1.1 支持以下 VMware 产品和版本：

- vRealize Log Insight 可以从 VMware vCenter Server 6.0 或更高版本中提取事件、任务和警报数据。
- 您可以将 vRealize Log Insight 8.1.1 与 vRealize Operations Manager 8.0.1 或更高版本相集成。

## 浏览器支持

vRealize Log Insight 8.1.1 支持以下浏览器版本。较新的浏览器版本也可以与 vRealize Log Insight 一起使用，但是尚未经过验证。

- Mozilla Firefox 72.0 及更高版本
- Google Chrome 78.0 及更高版本
- Safari 11.1 及更高版本
- Internet Explorer 11.0 及更高版本

**注意：**Internet Explorer 文档模式必须用于**标准模式**中。不支持其他模式。不支持“兼容性视图”浏览器模式。

支持的浏览器分辨率最低为 1280 x 800 像素。

**重要信息：**必须在浏览器中启用 Cookie。

## **vRealize Log Insight Windows 代理支持**

vRealize Log Insight 8.1.1 Windows 代理支持以下版本：

- Windows 7、Windows 8、Windows 8.1 和 Windows 10
- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016 和 Windows Server 2019

## **vRealize Log Insight Linux 代理支持**

vRealize Log Insight Linux 代理支持以下分发和版本：

- RHEL 5、RHEL 6、RHEL 7 和 RHEL 8
- SUSE Enterprise Linux (SLES 11 SP3) 和 SLES 12 SP1
- Ubuntu 14.04 LTS、Ubuntu 16.04 LTS 和 Ubuntu 18.04
- VMware Photon 版本 1 修订版本 2、版本 2 和版本 3

## **限制**

vRealize Log Insight 8.1.1 具有以下限制：

### **常规**

- vRealize Log Insight 无法正确处理非可打印 ASCII 字符。
- vRealize Log Insight 不支持打印。但是，您可以使用浏览器的“打印”选项。打印的结果可能有所不同，具体取决于所使用的浏览器。我们建议使用 Internet Explorer 或 Firefox 打印 vRealize Log Insight 用户界面的各个部分。
- 主机表可能会将设备显示多次，并且每次以不同的格式显示，包括 IP 地址、主机名和 FQDN 的组合。例如，名为 foo.bar.com 的设备可能同时显示为 foo 和 foo.bar.com。  
主机表将使用 syslog RFC 中定义的 hostname 字段。如果设备通过 syslog 协议发送的事件没有主机名，则 vRealize Log Insight 将使用源作为主机名。这可能会导致多次列出该设备，原因是 vRealize Log Insight 无法确定两种格式是否指向同一设备。
- 要添加新数据分区或删除现有数据分区，需要重新启动集群（逐个重新启动集群节点），才能使新配置生效。但是，对现有数据分区的路由筛选器、已启用状态和保留期限所做的更改将会立即应用（不需要重新启动集群）。

## vRealize Log Insight Windows 和 Linux 代理

- 当 vRealize Log Insight Windows 和 Linux 代理以 syslog 模式运行时，无法正确传递 hostname 和 source 字段中的非 ASCII 字符。

## vRealize Log Insight Windows 代理

- vRealize Log Insight Windows 代理是 32 位应用程序，它发出的从 C:\Windows\System32 子目录打开文件的所有请求都将被 WOW64 重定向到 C:\Windows\SysWOW64。但是，您可以配置 vRealize Log Insight Windows 代理以使用特殊别名 C:\Windows\Sysnative 从 C:\Windows\System32 中收集。例如，要从 MS DHCP 服务器的默认位置收集日志，请将以下行添加到 vRealize Log Insight Windows 代理配置文件的相应部分：`=C:\Windows\Sysnative\dhcp`。

## vRealize Log Insight Linux 代理

- 由于操作系统限制，vRealize Log Insight Linux 代理在配置为通过 syslog 发送事件时，不会检测网络中断。
- vRealize Log Insight Linux 代理不支持在字段或标记名称中使用非英语 (UTF-8) 符号。
- 默认情况下，vRealize Log Insight Linux 代理会收集隐藏文件和目录。要阻止此行为，您必须将 `exclude=.*` 选项添加到每个配置部分。选项 `exclude` 使用 glob 模式 `.*`，它表示隐藏文件格式。
- 当文件的标准输出重定向用于生成日志时，vRealize Log Insight 代理可能无法正确识别此类日志文件中的事件边界。

## vRealize Log Insight 集成

如果虚拟机的 IP 地址对 vRealize Operations 实例不可见，并且 vCenter 未将该 IP 地址显示在虚拟机的**虚拟机摘要**选项卡中，则无法从 vRealize Log Insight 和 vRealize Operations 中对该虚拟机执行“在环境中启动”操作。由于缺少 vmware-tools 实用程序，IP 地址可能不可用。不受支持的旧版本或发生故障的 vmware-tools 也可能导致 IP 地址变得不可用。

确保虚拟机上安装了正确版本的 VMware Tools，并且 vCenter 的**虚拟机摘要**选项卡显示了虚拟机的 IP 地址。

## 从 vRealize Log Insight 的先前版本升级

在升级到此版本的 vRealize Log Insight 时，请记住以下注意事项。

### 升级途径

您可以从 vRealize Log Insight 8.1、8.0 或 4.8 升级到 8.1.1。

### 有关升级的重要说明

- 要升级到 vRealize Log Insight 8.1.1，您必须正在运行 vRealize Log Insight 8.1、8.0 或 4.8。
- 执行手动升级时，必须一次升级一个工作线程。同时升级多个工作线程会导致升级失败。将主节点升级到 vRealize Log Insight 8.1.1 时，除非专门禁用，否则将进行滚动升级。
- 必须从主节点的 FQDN 执行升级。不支持使用集成负载均衡器 IP 地址进行升级。

- vRealize Log Insight 不支持双节点集群。在执行升级之前，需先添加与两个现有节点相同版本的第三个 vRealize Log Insight 节点。
- 如果 vRealize Log Insight 升级 (.pak 文件) 具有一个新的 JRE 版本，则用户在 vRealize Log Insight 设置中安装的证书 (例如，用于事件转发的证书) 会在升级后消失不见。
- 如果集成目标为 SSL 连接提供了不受信任的证书，则在升级后与 vRealize Log Insight 的集成将无法正常工作，因为这些证书未添加到信任存储区中。这些集成目标包括 vSphere、vRealize Operations Manager、事件转发器、Active Directory 和 SMTP。作为解决办法，请在每个集成配置页面中，测试连接并接受不受信任的 SSL 证书 (如果显示了一个包含该证书详细信息的对话框)。接受证书即会将其添加到信任存储区中。
- Photon OS 改进了安全策略，在成功升级到 Photon OS 后，您可能需要更改 root 密码。在 SLES 中，仅当 root 密码已过期时才会发生这种情况，但与 Photon OS 不同的是，SLES OS 不会强制执行更新。
- 将基于 SLES 的 vRealize Log Insight 4.8 升级到基于 Photon 的最新版 vRealize Log Insight 时，sshd 自定义服务配置 (/etc/ssh/sshd\_config) 将重置为默认值。作为解决办法，请在升级前保存 /etc/ssh/sshd\_config 配置，然后在升级后重新进行手动配置。
- Photon OS 对并发 ssh 连接数实施了严格的规则。由于默认将 /etc/ssh/sshd\_config 文件中的 MaxAuthtries 值设置为 2，所以，在存在多个连接的情况下，使用 ssh 连接到 vRealize Log Insight 虚拟设备可能会失败，并显示以下消息：“从 xx.xx.xx.xxx 端口 22:2 收到断开连接信息: 身份验证失败次数过多 (Received disconnect from xx.xx.xx.xxx port 22:2: Too many authentication failures)”。
- 您可以使用以下任一解决办法来解决此问题：
  - 通过 ssh 连接时，使用 IdentitiesOnly=yes 选项：`#ssh -o IdentitiesOnly=yes user@ip`
  - 更新 ~/.ssh/config 文件以添加以下内容：`Host* IdentitiesOnly yes`
  - 通过修改 /etc/ssh/sshd\_config 文件并重新启动 sshd 服务来更改 MaxAuthtries 值。
- 在开始从 vRealize Log Insight 4.8 集群升级到 8.1.1 之前，请确认每个节点在根分区中具有足够的可用空间。有关详细信息，请参见 <https://kb.vmware.com/s/article/76282>。
- 将 vRealize Log Insight 从 4.8 升级到 8.1.1 后，设备默认采用 SLES 引导选项，而不是 Photon OS。有关解决办法，请按照 <https://kb.vmware.com/s/article/79592> 中的说明进行操作。

## 国际化支持

vRealize Log Insight 8.1.1 具有以下本地化功能。

- vRealize Log Insight 服务器 Web 用户界面已本地化为日语、法语、西班牙语、德语、简体中文、繁体中文和韩语。
- vRealize Log Insight 服务器 Web 用户界面支持 Unicode 数据，包括机器学习功能。
- vRealize Log Insight 代理可在非英语本机 Windows 中运行。

## 限制

- 代理安装程序和内容包尚未本地化。vRealize Log Insight 服务器 Web 用户界面的某些部分可能仍显示未本地化的字符串，且可能存在布局问题。
- vRealize Log Insight 可与 vCenter Server 和 vRealize Operations Manager 的本地化版本进行互操作。不过，内容包依赖匹配的非本地化日志消息。将从默认区域设置中检索 vCenter Server 事件，因此默认区域设置应设置为 en\_US。有关详细信息，请参见 <http://kb.vmware.com/kb/2121646>。
- 对于包含非 ASCII 字符的用户名，不支持与 Active Directory、vSphere 和 vRealize Operations Manager 集成。

- 不支持事件日志本地化。事件日志仅支持 UTF-8 和 UTF-16 字符编码。
- vRealize Log Insight 8.1.1 的全新部署仅显示英文版的最终用户许可协议 (EULA)。

## 已解决的问题

有关此版本中已解决的安全漏洞列表，请参见 <https://kb.vmware.com/s/article/79258>。

## 已知问题

此版本中存在以下已知问题。

- **Virtual Center (VC) 事件收集延迟**  
重新启动 vRealize Log Insight 服务或升级集群后，如果集成了大量 Virtual Center (VC)，则 VC 事件收集可能会延迟。  
  
**解决办法：**经过一段足够长的时间后，事件会自动恢复为已收集状态。具体时间长短取决于您的环境。例如，对于包含 4 个节点的集群上的 80 个 VC，延迟将为一小时。
- **删除 vRealize Operations 集成失败**  
如果 vRealize Log Insight 先前与某个 vRealize Operations 实例相集成，但该集成后来变得不可访问，则不能强制移除该集成。  
  
**解决办法：**进行刷新，并再次尝试移除该集成。
- **配置了双向信任关系时，vRealize Log Insight 无法从第二个受信任的 Active Directory 对用户和组进行身份验证**  
如果某个 Active Directory 与另一个 Active Directory 配置为双向信任关系，则 vRealize Log Insight 无法从第二个受信任的 Active Directory 对用户和组进行身份验证。  
  
**解决办法：**使用 vIDM，它直接与两个 Active Directory 相集成。
- **对于在代理启动或重新配置事件之前创建的某些目录，将无法从中收集信息**  
如果在重新配置代理后创建新目录，则不会从新创建的目录中收集信息。  
  
**解决办法：**要启动目录监控，请重新启动该服务，或者使用 liagent.ini 文件或从“服务器管理代理”页面更新代理配置。
- **Photon OS 上的 vRealize Log Insight 代理无法执行自动升级**  
无法对 Photon OS 上的 vRealize Log Insight 代理执行自动升级，因为 Photon OS 不支持 gpg 命令。  
  
**解决办法：**执行手动升级。
- **SMTP 配置可能不适用于使用 IPv6 的公共邮件服务器**  
SMTP 配置可能不适用于 Google 和 Yahoo 等公共电子邮件服务，因为这些服务可能会使用较为严格的 IPv6 限制策略。  
  
**解决办法：**使用备用邮件服务器（如企业邮件服务器）或启动专用服务器。

- **通过 IPv4 将 VMware Identity Manager 与 vRealize Log Insight 集成时会将重定向 URL 主机更改为 IPv6 地址**

如果您在部署 vRealize Log Insight 虚拟设备时选择首选 IPv6 地址的选项，则在与不支持 IPv6 的 VMware Identity Manager 集成时，重定向 URL 主机列表中会填充 IPv6 节点地址。

**解决办法：**创建一个备用 IPv4 VIP，以便在将 vRealize Log Insight 与 VMware Identity Manager 集成时使用。

- **无法使用默认任务名称导出超过 20,000 个事件**

导出超过 20,000 个事件时，无法使用显示的默认导出任务名称。

**解决办法：**使用包含字母数字字符的自定义导出任务名称。

- **Internet Explorer 11.0 中存在布局问题**

在 Internet Explorer 11.0 中，**仪表板**和**交互式分析**选项卡上的标题和图表图例列表显示中的用户图标存在布局问题。

**解决办法：**有关解决办法，请参见 <https://kb.vmware.com/s/article/78592>。