

vRealize Log Insight 8.4 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和存档日志管理功能。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

以下是 vRealize Log Insight 8.4 的一些主要功能亮点，可帮助您比以往更快、更准确、更有力地利用日志数据：

- **日志源**：现在，可以配置 Fluentd 以从各种源（如 Docker、Kubernetes、Tanzu Kubernetes Grid 和 OpenShift）收集日志，然后将其转发给 vRealize Log Insight。Fluentd 是一个开源的日志处理器和转发器，它允许您从不同的源收集日志数据，并使用筛选器处理这些数据。它是 Kubernetes 等容器化环境的首要之选。可以在 vRealize Log Insight 用户界面中找到 Fluentd 日志源的配置步骤。
- **日志屏蔽**：日志数据包含可能被视为敏感的信息。特定日志消息可能包含用户名、电子邮件地址、URL 参数以及其他您不希望披露的信息。借助日志屏蔽功能，可以通过修改用于处理您视为敏感的信息的配置，来屏蔽任何信息。
- **日志丢弃**：有时，基础架构生成的日志事件量可能过大或者有明显波动。在这种情况下，可能需要选择要发送到日志管理解决方案的日志以及要丢弃的日志。借助日志丢弃功能，可以通过修改相应的配置来丢弃某些日志。
- **自定义 Webhook**：现在可利用 vRealize Log Insight Webhook 连接将警示中的通知发送到 Slack 和 PagerDuty。此外，还可以通过定义相应的负载，向自定义 Webhook 发送通知。
- **基于分区的存档**：数据存档可保留由于存储限制可能会从 vRealize Log Insight 虚拟设备中移除的旧日志。vRealize Log Insight 可以将数据分区的已存档数据存储到 NFS 挂载中。
- **警示管理**：使用升级后的警示管理，可以在一个环境中查看组织范围内的整个警示列表。现在，警示以组织为中心，而不是以用户为中心，这样便可以更灵活地控制组织警示。管理基于查询的警示的权限已

更新。现在，用户需要具有“交互式分析”权限才能查看警示，需要具有“编辑共享内容”权限才能创建和管理警示。

- **使用新的大小调整计算器简化了大小调整：**正确调整 vRealize Log Insight 集群的大小，对于获得最佳的日志搜索和分析性能以及确保集群具有所需的资源至关重要。大小调整计算器可根据服务器和设备日志记录的类型、预期的载入速率和日志保留要求来确定所需的节点大小。
- **NSX Data Center 版本：**vRealize Log Insight 现在随以下新的 NSX Data Center 版本一起提供。有关详细信息，请参见 [VMware NSX Data Center 产品介绍](#)。
 - NSX Firewall
 - 具有 Advanced Threat Prevention 的 NSX Firewall
- **内容包更新：**已更新以下内容包。
 - VMware NSX-v 4.2.1（与字段提取相关的更新）
 - VMware NSX-T v4.0.1（新增了仪表板支持“统一安全流量日志”）
 - VMware vRA 8.3 及更高版本（支持 vRA 8.3 及更高版本产品系列）
 - Microsoft IIS v3.4（改进了“设置说明”部分，以介绍如何从日志中提取自定义字段。）
 - VMware Horizon v4.0.1
 - vSphere 8.4
 - vRops v4.2
 - vSAN（支持 vSAN 70u2）
 - 已验证的其他内容包：
 - NPE Servers v1.1.1
 - Mongo DB v2.4
 - Solarwinds v1.1
 - Oracle DB v1.1
 - NPE Nimble v1.1

兼容性

vRealize Log Insight 8.4 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。在 FIPS 模式下，vRealize Log Insight 可与 VMware vCenter Server 6.0 U1 或更高版本集成。
- 您可以将 vRealize Log Insight 8.4 与 vRealize Operations Manager 8.0.1 或更高版本相集成。

浏览器支持

vRealize Log Insight 8.4 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 8.4 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 8.4 存在以下限制：

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）。
- FIPS 模式在激活后将无法再禁用。

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 8.3 或 8.2 升级到 8.4。

有关升级的重要说明

- 要升级到 vRealize Log Insight 8.4，您必须正在运行 vRealize Log Insight 8.3 或 8.2。
- 从命令行执行手动升级时，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。
- 从用户界面中将主节点升级到 vRealize Log Insight 8.4 时，除非明确禁用，否则将执行滚动升级。
- 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。
- 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。

国际化支持

vRealize Log Insight 8.4 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。

已解决的问题

此版本中没有已解决的问题。

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。
- **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，则将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。

- **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>。

- **REST API 调用“POST /api/v1/sessions”失败**

如果将 vRealize Log Insight 8.2 或 8.3 中新部署的节点加入从 4.8 或更低版本升级的旧集群，则对新工作节点发起的 REST API 调用“POST /api/v1/sessions”将失败并引发以下错误：

Error: write EPROTO 1319245176:error:100000f7:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER:../third_party/boringssl/src/ssl/tls_record.cc:242:

您可以在 REST 客户端中找到相关日志。由于此错误，您无法获取该节点的会话。

解决办法：通过在受影响的节点上运行“service loginsight restart”命令，重新启动 vRealize Log Insight 服务。

- **在 FIPS 模式下测试配置了 STARTTLS 的自定义 SMTP 服务器时，引发证书错误**

在 FIPS 模式下使用 STARTTLS 选项配置自定义 SMTP 服务器时，单击发送测试电子邮件会显示一个弹出窗口，提示接受自签名证书。接受证书时，将显示以下错误：

找不到所请求目标的有效证书路径 (Unable to find valid certification path to requested target)

解决办法：通过运行“service loginsight restart”命令，重新启动 vRealize Log Insight 服务。

- **vRealize Log Insight 在没有可信证书的情况下使用自定义 SMTP 服务器发送电子邮件通知**

使用自定义 SMTP 服务器时，即使未接受自定义证书，vRealize Log Insight 也会通过电子邮件发送警示和系统通知。

解决办法：无。

- **以 FIPS 模式部署的全新 vRealize Log Insight 8.3 设置的升级失败**

在启用 FIPS 模式的情况下部署全新的 vRealize Log Insight 8.3 设置后，该设置的升级失败。

解决办法：在部署后启用 FIPS 模式。请参见 <https://kb.vmware.com/s/article/83360>。

- **即使升级成功，vRealize Log Insight 也显示“升级未确认 (Upgrade unconfirmed)”消息**

在升级到 vRealize Log Insight 8.4 时，可能显示一则消息，说明升级状态未确认。此消息对整体升级状态没有影响，最终升级会成功。

解决办法：无。

- **双堆栈或 IPv6 设置的升级失败**

将双堆栈或 IPv6 设置升级到 vRealize Log Insight 8.4 失败。

解决办法：无。