

# vRealize Log Insight 入门

2022 年 5 月 24 日

vRealize Log Insight 8.4

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**威睿信息技术（中国）有  
限公司**  
北京办公室  
北京市  
朝阳区新源南路 8 号  
启皓北京东塔 8 层 801  
[www.vmware.com/cn](http://www.vmware.com/cn)

上海办公室  
上海市  
淮海中路 333 号  
瑞安大厦 804-809 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

广州办公室  
广州市  
天河路 385 号  
太古汇一座 3502 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

版权所有 © 2022 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

# 目录

vRealize Log Insight 入门	4
<b>1 安装 vRealize Log Insight 之前</b>	<b>5</b>
vRealize Log Insight 中支持的日志文件和存档格式	5
安全要求	6
产品兼容性	6
最低要求	7
规划 vRealize Log Insight 部署	9
调整 vRealize Log Insight 虚拟设备的大小	10
将 vRealize Log Insight 与 vRealize Operations Manager 集成	12
<b>2 事件生命周期</b>	<b>13</b>
事件生命周期的主要方面	14
<b>3 安装 vRealize Log Insight</b>	<b>15</b>
部署 vRealize Log Insight 虚拟设备	15
启动新 vRealize Log Insight 部署	17
加入现有部署	19
<b>4 客户体验提升计划</b>	<b>21</b>

# vRealize Log Insight 入门

《vRealize Log Insight 入门》提供了有关部署和配置 VMware® vRealize™ Log Insight™ 的信息，包括如何调整 vRealize Log Insight 虚拟设备的大小以接收日志消息。

您可以在希望计划或安装部署时使用此信息。此信息的目标读者为熟悉虚拟机技术和数据中心操作且具有丰富经验的 Linux 和 Windows 系统管理员。

# 安装 vRealize Log Insight 之前

# 1

要开始在您的环境中使用 vRealize Log Insight，必须部署 vRealize Log Insight 虚拟设备并应用多个基本配置。

本章讨论了以下主题：

- vRealize Log Insight 中支持的日志文件和存档格式
- 安全要求
- 产品兼容性
- 最低要求
- 规划 vRealize Log Insight 部署
- 调整 vRealize Log Insight 虚拟设备的大小
- 将 vRealize Log Insight 与 vRealize Operations Manager 集成

## vRealize Log Insight 中支持的日志文件和存档格式

可以使用 vRealize Log Insight 分析非结构化或结构化的日志数据。

vRealize Log Insight 接受来自以下源的数据：

- 支持通过 syslog 协议发送日志流的源。
- 写入日志文件并可以运行 vRealize Log Insight 代理的源。
- 可以通过 REST API 使用 HTTP 或 HTTPS 发布日志数据的源。API 文档可从位于 [https://<vRLI\\_host>/rest-api](https://<vRLI_host>/rest-api) 的 vRealize Log Insight 界面获取。
- 由 vRealize Log Insight 存档的历史数据。

vSphere 日志分析程序允许您在 vRealize Log Insight 中导入 vSphere 日志包。

---

**注** 虽然 vRealize Log Insight 可以同时处理历史数据和实时数据，但还是建议您部署 vRealize Log Insight 的单独实例以处理导入的日志文件。

---

请参见管理 vRealize Log Insight 中的[将 Log Insight 存档导入到 vRealize Log Insight 中](#)。

## 安全要求

为保护虚拟环境免遭外部攻击，必须遵循特定规则。

- 始终在可信网络中安装 vRealize Log Insight。
- 始终将 vRealize Log Insight 支持包保存在安全位置。

IT 决策者、架构师、管理员以及必须自行熟悉 vRealize Log Insight 安全组件的其他人员都必须阅读管理 vRealize Log Insight 中的安全主题。

这些主题提供了对 vRealize Log Insight 安全功能的简明参考。主题包括产品外部接口、端口、身份验证机制和用于配置和管理安全功能的选项。

有关保护虚拟环境安全的信息，请参见《VMware vSphere 安全性指南》和 VMware 网站上的“安全中心”。

## 产品兼容性

vRealize Log Insight 通过 syslog 协议和 HTTP 收集数据，可以连接到 vCenter Server 以收集事件、任务和警报数据，并且还可以与 vRealize Operations Manager 集成以发送通知事件和启用“在环境中启动”。有关受支持产品版本的最新更新，请查看《VMware vRealize Log Insight 发行说明》。

## 虚拟设备部署

必须使用 vSphere 部署 vRealize Log Insight 虚拟设备。始终使用 vSphere Client 连接到 vCenter Server。vRealize Log Insight 虚拟设备部署在由 vCenter Server 5.0 或更高版本管理的 ESX/ESXi 主机 5.0 或更高版本上。

## Syslog 源

vRealize Log Insight 通过以下端口和协议收集和分析 syslog 数据。

- 514/UDP
- 514/TCP
- 1514/TCP (SSL)

必须配置诸如操作系统、应用程序、存储、防火墙和网络设备等环境组件才能将其 syslog 源推送到 vRealize Log Insight。

## API 源

vRealize Log Insight 数据获取 API 通过以下端口和协议收集数据。

- 9000/TCP
- 9543/TCP (SSL)

## vSphere 集成

可以配置 vRealize Log Insight 以提取一个或多个 vCenter Server 实例中出现的任务、事件和警报的数据。vRealize Log Insight 使用 vSphere API 连接到 vCenter Server 系统并收集数据。

可以配置 ESXi 主机以将 syslog 数据转发到 vRealize Log Insight。

有关 vCenter Server 和 ESXi 特定版本的兼容性信息，请参见 [VMware 产品互操作性列表](#)。

有关连接到 vSphere 环境的信息，请参见将 [vRealize Log Insight 连接到 vSphere 环境](#)。

## vRealize Operations Manager 集成

可以通过两种独立的方法集成 vRealize Log Insight 和 vRealize Operations Manager vApp 或 Installable。

所有支持的 vCenter Operations Manager 版本均支持通知以及“在环境中启动”。

- vRealize Log Insight 可以向 vRealize Operations Manager 发送通知事件。  
请参见将 [vRealize Log Insight 配置为向 vRealize Operations Manager 发送通知事件](#)。
- vRealize Operations Manager 的“在环境中启动”菜单可以显示与 vRealize Log Insight 相关的操作。  
请参见在 [vRealize Operations Manager 中为 vRealize Log Insight 启用“在环境中启动”](#)。

## 最低要求

VMware 将 vRealize Log Insight 作为虚拟设备以 OVA 文件格式进行分发。各种资源和应用程序必须可用，此虚拟设备才能成功运行。有关要求的最新信息，请参见最新发行说明。

## 虚拟硬件

在部署 vRealize Log Insight 虚拟设备期间，您可以根据环境的载入要求选择预配置大小。这些预设是经过认证的计算和磁盘资源大小组合，但您可以在以后添加额外的资源。小型配置（如下表所述）消耗最少的资源，同时保持受支持状态。还可以使用超小型配置，但该配置仅适用于演示目的。

有关基于载入要求的完整资源要求，请参见 [调整 vRealize Log Insight 虚拟设备的大小](#)。

表 1-1. 小型配置的预设值

资源	最低要求
内存	8 GB
vCPU	4
存储空间	530 GB

## 支持的浏览器

可以使用以下浏览器之一连接到 vRealize Log Insight Web 用户界面。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。

**重要事项** 必须在浏览器中启用 Cookie。

- Mozilla Firefox 45.0 及更高版本
- Google Chrome 51.0 及更高版本
- Safari 9.1 及更高版本
- Internet Explorer 11.0 及更高版本

### 注

- Internet Explorer 文档模式必须设置为**标准模式**。不支持其他模式。
- **浏览器模式**：不支持兼容性视图。
- 要在 Internet Explorer 上使用 vRealize Log Insight Web 客户端，必须将 Windows 本地存储完整性级别配置为“低”。

## 帐户密码

类型	要求
root	除非您在部署 OVA 期间指定 root 密码或使用客户机自定义，否则 vRealize Log Insight 虚拟设备上的 root 用户的默认凭据为 <b>root/blank</b> 。在首次访问 vRealize Log Insight 虚拟设备控制台时，系统会提示您更改 root 帐户密码。  <b>注</b> 在设置 root 密码之前，SSH 一直处于禁用状态。
用户帐户	在 vRealize Log Insight 3.3 及更高版本中创建的用户帐户需要强密码。密码长度必须至少为 8 个字符，并且包含一个大写字符、一个小写字符、一个数字和一个特殊字符。

## 集成要求

产品	要求
vCenter Server	要从 vCenter Server 提取事件、任务和警报数据，您必须提供该 vCenter Server 的一组用户凭据。在 vCenter Server 中注册和取消注册 vRealize Log Insight 所需的最低角色为 <b>只读</b> 。必须在 vCenter Server 级别设置该角色并将其传播到子对象。要配置 vCenter Server 管理的 ESXi 主机，vRealize Log Insight 需要其他特权。
vSphere ESXi	需要使用 vSphere ESXi 6.0 Update 1 或更高版本才能与 vRealize Log Insight 建立 SSL 连接。
vRealize Operations Manager	要在 vRealize Operations Manager 实例中启用通知事件和在环境中启动功能，您必须为该 vRealize Operations Manager 实例提供用户凭据。

## 网络端口要求

以下网络端口必须可在外部访问。

端口	协议
22/TCP	SSH
80/TCP	HTTP
443/TCP	HTTPS
514/UDP, 514/TCP	Syslog
1514/TCP	仅通过 SSL 的 Syslog 载入
9000/TCP	vRealize Log Insight 数据获取 API
9543/TCP	vRealize Log Insight 数据获取 API (SSL)

## 规划 vRealize Log Insight 部署

您可以使用单节点、单集群或带转发器的集群部署 vRealize Log Insight。

**注** 不支持将外部负载均衡器用于 vRealize Log Insight，包括 vRealize Log Insight 群集。

## 通过 vRealize Suite Lifecycle Manager 进行安装

vRealize Suite Lifecycle Manager 自动执行套件产品的安装、配置、升级、修补、配置管理、偏移修复以及运行状况监控。作为 vRealize Log Insight 安装的替代方法，您可以通过 vRealize Suite Lifecycle Manager 安装 vRealize Log Insight。您必须使用 vRealize Suite Lifecycle Manager 1.2 或更高版本以及 vRealize Log Insight 4.5.1 或更高版本。有关详细信息，请参见 [vRealize Suite Lifecycle Manager 文档](#)。

## 单个节点

一个基本的 vRealize Log Insight 配置包含单个节点。日志源可以是应用程序、操作系统日志、虚拟机日志、主机、vCenter Server、虚拟或物理交换机和路由器、存储硬件，等等。使用 syslog（UDP、TCP、TCP+SSL）或 CFAPI（通过 HTTP 或 HTTPS 的 vRealize Log Insight 本地载入协议），直接由应用程序、syslog 集中器或安装在源上的 vRealize Log Insight 代理将日志流传输到 vRealize Log Insight 节点。

单节点部署的最佳做法是使用 vRealize Log Insight 集成负载均衡器 (Integrated Load Balancer, ILB)，并将查询和载入流量发送到 ILB。如果打算将来为您的部署添加节点以创建集群，这可简化配置，而不会产生开销。

最佳做法是，不要在生产环境中使用单个节点。

## 集群

生产环境通常需要使用集群。集群必须满足以下要求：

- 集群中的节点必须全部具有相同大小并位于同一数据中心。
- 用于集群的 ILB 要求节点位于同一 L2 层网络。
- 必须从 VMware NSX 分布式防火墙保护中排除 vRealize Log Insight 虚拟机。

这是因为集群的虚拟 IP 使用处于服务器直接返回模式的 Linux 虚拟服务器 (LVS-DR) 进行负载均衡。服务器直接返回比通过单个集群成员路由所有响应流量更高效。但是，这种响应流量还与虚假的流量相似，因此 NSX 分布式防火墙会阻止这种流量。

## 调整集群大小

vRealize Log Insight 单集群配置可以包含 3 到 18 个节点，并且使用 ILB。一个集群最少需要三个正常节点才能正常运行。

生产环境要求节点至少为中等大小。如果预计要处理大量并发查询（包括警示），请考虑使用大型节点。有关大小调整的信息，请参见[调整 vRealize Log Insight 虚拟设备的大小](#)。

虽然 vRealize Log Insight 集群中的最小节点数为三个，但如果节点出现故障，包含的正常节点数少于三个的集群将无法完全正常运行。此外，集群中的正常节点数必须大于集群节点总数的一半。例如，如果您有一个包含六个节点的集群，其中的三个节点变得不可用，则该集群将无法完全正常运行，直到您从该集群中移除不可正常运行的节点。不支持移除和重新引入集群节点。

## 具有转发器的集群

具有转发器的 vRealize Log Insight 集群配置包含主索引、存储以及具有 3 至 18 个节点并使用 ILB 的查询集群。对于单集群，仅在主集群中的一个位置存在单个日志消息。

通过在远程站点或集群添加多个转发器集群来扩展设计。每个转发器集群配置为将其所有日志消息转发到主集群，并且用户连接到主集群，从而利用 CFAPI 在转发路径上提供压缩和恢复能力。配置为机架置顶式的转发器集群可以配置较大的本地保留。

## 提供冗余的交叉转发

此 vRealize Log Insight 部署方案包括经扩展和镜像的带转发器的集群。两个主集群用于索引、存储和查询。在每个数据中心具有一个主集群。每个数据中心的前端是一对专用的转发器集群。来自所有机架置顶式聚合的所有日志源集中在转发器集群。您可以在两个保留集群上独立查询相同的日志。

## vRealize Log Insight 集成负载均衡器

要在集群中的节点之间正确均衡流量并最大限度减少管理开销，请在所有部署中使用集成负载均衡器 (ILB)。这可确保接受传入载入流量，即使某些 vRealize Log Insight 节点不可用。

## 调整 vRealize Log Insight 虚拟设备的大小

默认情况下，vRealize Log Insight 虚拟设备在小型配置中使用预设值。

## 独立部署

您可以更改设备设置，以满足要在部署期间收集日志的环境需求。

vRealize Log Insight 提供了预设虚拟机大小，您可以从中选择满足您环境载入要求的相应大小。这些预设是经过认证的计算和磁盘资源大小组合，但您可以在以后添加额外的资源。小型配置消耗最少的资源，同时保持受支持状态。超小型配置仅适用于演示目的。

预设大小	日志载入速率	虚拟 CPU	内存	IOPS	syslog 连接（活动的 TCP 连接）	每秒事件数
超小型	6 GB/天	2	4GB	75	20	400
小型	30 GB/天	4	8 GB	500	100	2000
中型	75 GB/天	8	16 GB	1000	250	5000
大型	225 GB/天	16	32GB	1500	750	15,000

可以使用 syslog 聚合器增加向 vRealize Log Insight 发送事件的 syslog 连接数。但是，每秒的最大事件数是固定的，并不取决于是否使用 syslog 聚合器。vRealize Log Insight 实例无法用作 syslog 聚合器。

大小调整基于以下假定条件。

- 每个虚拟 CPU 至少为 2 GHz。
- 每个 ESXi 主机每秒发送最多 10 条消息，平均消息大小为 170 个字节/消息，大致相当于 150 MB/天/主机。

**注** 对于大型安装，必须升级 vRealize Log Insight 虚拟机的虚拟硬件版本。vRealize Log Insight 支持虚拟硬件版本 7 或更高版本。虚拟硬件版本 7 最多可以支持 8 个虚拟 CPU。因此，如果打算置备 16 个虚拟 CPU，您必须将 ESXi 5.x 的虚拟硬件升级到版本 8 或更高版本。您可以使用 vSphere Client 升级虚拟硬件。如果要升级虚拟硬件至最新版本，请阅读并了解 VMware 知识库文章[将虚拟机升级至最新硬件版本 \(1010675\)](#) 中的信息。

## 集群部署

对于 vRealize Log Insight 集群中的主节点和工作线程节点，使用中型或较大型配置。每秒事件数随节点数呈线性增长。例如，在包含 3 到 18 个节点的集群中（集群必须最少具有三个节点），包含 18 个节点的集群中的载入每秒事件数 (Events Per Second, EPS) 为 270,000，或每天事件数为 4 TB。

## 减少内存大小

在概念证明或测试环境中使用超小型版本的设备，但不要在生产环境中使用此版本。此配置最多支持 20 个 ESXi 主机（约 200 个事件/秒或约 3 GB/天）。

## vRealize Log Insight 大小调整计算器

该计算器可以帮助您确定是否可以调整 vRealize Log Insight 以及网络和存储利用率的大小。此计算器仅用于提供相关指导。很多环境输入因站点而异，因此，该计算器需要在某些领域中使用估计值。请参见 <https://www.vmware.com/go/loginsight/calculator>。

**注** 如果为具有涉及正则表达式的复杂条件或多个条件的文本字段（例如，“`text=~"Deleting the machine"`”）定义了转发器，vRealize Log Insight 的总体性能可能会下降。在这些情况下，尤其是当集群上的总体负载较高时，性能可能会出现延迟，并且磁盘块可能会在集群的每个节点上累积。

## 将 vRealize Log Insight 与 vRealize Operations Manager 集成

要启用 vRealize Log Insight 和 vRealize Operations Manager 之间的集成，必须在两个产品中都执行配置。

### 步骤

- 1 将 vRealize Log Insight 管理包安装到 vRealize Operations Manager 中。

对于两个产品之间的“在环境中启动”功能，需要 vRealize Log Insight 管理包。vRealize Log Insight 管理包随 vRealize Operations Manager 下载文件提供或者可在 VMware Solution Exchange 网站上获得。

- 2 配置 vRealize Log Insight 以连接到 vRealize Operations Manager。

- 3 配置 vRealize Log Insight 警示以将信息转发到 vRealize Operations Manager。

请参见《管理 vRealize Log Insight》中的[将 vRealize Log Insight 配置为向 vRealize Operations Manager 发送通知事件](#)。

- 4 启用 vRealize Operations “在环境中启动” 以在 vRealize Log Insight 中查询日志。

请参见《管理 vRealize Log Insight》中的[在 vRealize Operations Manager 中为 vRealize Log Insight 启用“在环境中启动”](#)。

# 事件生命周期

## 2

了解 vRealize Log Insight 如何处理消息和事件对于有效使用 vRealize Log Insight 至关重要。

日志消息或事件的生命周期分为多个阶段，包括读取、分析、载入、编制索引、生成警示、查询应用程序、存档和删除。

事件和消息通过以下阶段进行转换。

- 1 在设备上生成事件（在 vRealize Log Insight 外部）。
- 2 选择事件并通过以下方法之一将事件发送到 vRealize Log Insight:
  - 通过使用数据获取 API 或 syslog 的 vRealize Log Insight 代理
  - 通过使用 syslog 的第三方代理（例如 rsyslog、syslog-ng 或 log4j）
  - 以自定义方式写入到数据获取 API（如 log4j 附加程序）
  - 以自定义方式写入到 syslog（如 log4j 附加程序）
- 3 vRealize Log Insight 接收事件。
  - 如果使用集成的负载均衡器 (Integrated Load Balancer, ILB)，事件将传送到负责处理该事件的单个节点。
  - 如果拒绝了事件，客户端将通过 UDP 丢弃、具有协议设置的 TCP 或具有磁盘支持的队列的 CFAPI 处理拒绝问题。
  - 如果接受了事件，则会通知客户端。
- 4 通过 vRealize Log Insight 数据获取管道传送事件，将在其中执行以下步骤。
  - 创建或更新一个关键字索引。该索引以专有格式存储在本地磁盘上。
  - 将机器学习应用于集群事件。
  - 事件以压缩专有格式存储在本地磁盘上的段中。
- 5 查询事件。
  - 根据关键字索引匹配关键字和通配符匹配操作符查询。
  - 根据压缩事件匹配正则表达式。
- 6 将事件移至段并存档。
  - 段达到 0.5 GB 时，会被密封并存档。

## 7 删除事件。

- 按 FIFO 顺序删除段。

## 了解详细信息

有关详细信息，请参见 VMware 技术出版物视频：



vRealize Log Insight 中的日志事件生命周期。

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_horp849x/uiConfId/50138843/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_horp849x/uiConfId/50138843/))

本章讨论了以下主题：

- 事件生命周期的主要方面

## 事件生命周期的主要方面

随着事件存在的时间增加，需要在事件生命周期内注意事件存储和管理方面的一些重要问题。

### 事件存储

事件存储在磁盘上的单个段中。在使用段时，请注意以下行为和特性。

- 段可以达到的最大大小为 0.5 GB。段达到 0.5 GB 时，会被密封并排入存档队列。在存档密封的段后，将标记为已存档。事件可以同时保留在本地和存档中。
- 不会跨 vRealize Log Insight 节点复制段。如果丢失一个节点，则会丢失该节点上的数据。
- 所有段都存储在 /storage/core 分区上。
- 如果 /storage/core 分区上的可用空间少于 3%，vRealize Log Insight 将删除旧段。删除操作将遵循 FIFO 模式。

---

**注** /storage/core 分区达到几乎全满的状态很常见，也是预期结果。该分区应始终不会达到 100%，因为该分区由 vRealize Log Insight 管理。但是，请勿尝试将数据存储在该分区上，因为它可能会干扰旧段删除。

---

### 事件管理

在您设置和配置产品时，熟悉 vRealize Log Insight 事件和事件管理的以下特点和行为会很有帮助。

- 在本地删除某个事件后，便不能再查询该事件，除非使用命令行界面从存档中导入该事件。
- 从 vRealize Log Insight 删除了机器学习群集的所有事件后，则会移除该群集。
- vRealize Log Insight 会在群集中的各节点之间公平地重新平衡所有入站事件。例如，即使已将节点明确发送到某个事件，该节点也可能不是载入该事件的节点。
- 事件元数据以专有格式存储在单个 vRealize Log Insight 节点中，而不是存储在数据库中。
- 事件可以存在于节点本地以及存档中。

# 安装 vRealize Log Insight

# 3

vRealize Log Insight 作为虚拟设备提供，您应将其部署到 vSphere 环境中。

在查看调整 vRealize Log Insight 虚拟设备的大小后，转到部署 vRealize Log Insight 虚拟设备。无论您拥有的是单节点部署还是群集形式的部署，都请按照本部分中所述的标准 OVF 部署过程操作。

---

**注** 您可以使用 vRealize Suite Lifecycle Manager 1.2 或更高版本安装 vRealize Log Insight 4.5.1 和更高版本。有关详细信息，请参见 [vRealize Suite 文档](#)。

---

本章讨论了以下主题：

- 部署 vRealize Log Insight 虚拟设备
- 启动新 vRealize Log Insight 部署
- 加入现有部署

## 部署 vRealize Log Insight 虚拟设备

下载 vRealize Log Insight 虚拟设备。VMware 将 vRealize Log Insight 虚拟设备作为 .ova 文件进行分发。使用 vSphere Client 部署 vRealize Log Insight 虚拟设备。

### 前提条件

- 验证您是否拥有 vRealize Log Insight 虚拟设备 .ova 文件的副本。
- 验证您是否有权将 OVF 模板部署至清单。
- 验证您的环境是否拥有足够资源来满足 vRealize Log Insight 虚拟设备的最低要求。请参见[最低要求](#)。
- 确保已阅读并了解虚拟设备大小调整建议。请参见[调整 Log Insight 虚拟设备的大小](#)。

### 步骤

- 1 在 vSphere Client 中，选择文件 > 部署 OVF 模板。
- 2 按照部署 OVF 模板向导中的提示进行操作。
- 3 在“选择配置”页面上，根据要收集日志的环境的大小选择 vRealize Log Insight 虚拟设备的大小。  
小型是生产环境的最低要求。

vRealize Log Insight 提供了预设虚拟机大小，您可以从中选择满足您环境载入要求的相应大小。这些预设是经过认证的计算和磁盘资源大小组合，但您可以在以后添加额外的资源。小型配置消耗最少的资源，同时保持受支持状态。超小型配置仅适用于演示目的。

预设大小	日志载入速率	虚拟 CPU	内存	IOPS	syslog 连接（活动的 TCP 连接）	每秒事件数
超小型	6 GB/天	2	4GB	75	20	400
小型	30 GB/天	4	8 GB	500	100	2000
中型	75 GB/天	8	16 GB	1000	250	5000
大型	225 GB/天	16	32GB	1500	750	15,000

可以使用 syslog 聚合器增加向 vRealize Log Insight 发送事件的 syslog 连接数。但是，每秒的最大事件数是固定的，并不取决于是否使用 syslog 聚合器。vRealize Log Insight 实例无法用作 syslog 聚合器。

**注** 如果选择**大型**，必须在部署后升级 vRealize Log Insight 虚拟机上的虚拟硬件。

#### 4 在“选择存储”页面上，选择磁盘格式。

- **厚置备延迟置零**以默认的厚格式创建虚拟磁盘。创建虚拟磁盘时分配虚拟磁盘所需的空間。创建时不会擦除物理设备上保留的数据，但是以后首次从虚拟设备写入时会按需要将其置零。
- **厚置备置零**创建一种厚虚拟磁盘类型，可支持 Fault Tolerance 等群集功能。在创建时为虚拟磁盘分配所需的空間。与平面格式相反，创建虚拟磁盘时，会将物理设备上保留的数据置零。创建这种格式的磁盘所需的时间可能会比创建其他类型的磁盘长。

**重要事项** 尽可能使用厚置备置零磁盘部署 vRealize Log Insight 虚拟设备，以获得更佳性能以及保证虚拟设备的运行。

- **精简置备**创建精简格式的磁盘。磁盘会随其上保存的数据量增加而扩展。如果存储设备不支持厚置备磁盘或您希望节省 vRealize Log Insight 虚拟设备上的未使用磁盘空间，请使用精简置备磁盘部署虚拟设备。

**注** 不支持压缩 vRealize Log Insight 虚拟设备上的磁盘，并且该操作可能导致数据损坏或数据丢失。

#### 5 （可选）在“选择网络”页面上，设置 vRealize Log Insight 虚拟设备的网络连接参数。您可以选择 IPv4 或 IPv6 协议。

如果不提供网络设置，如 IP 地址、DNS 服务器和网关信息，vRealize Log Insight 会使用 DHCP 设置这些设置。

**小心** 请勿指定超过两个域名服务器。如果指定超过两个域名服务器，将会忽略 vRealize Log Insight 虚拟设备中的所有已配置域名服务器。

使用以逗号分隔的列表指定域名服务器。

- 6 （可选） 如果使用的不是 DHCP，则在“自定义模板”页面上设置网络属性。

如果要在双堆栈网络中运行虚拟机，请在“应用程序”下选中**优先使用 IPv6 地址**复选框。

**小心** 如果尽管您的网络支持 IPv6 但您仍希望使用纯 IPv4，那么请不要选中**优先使用 IPv6 地址**复选框。仅当您的网络支持双堆栈或纯堆栈 IPv6 时，才选中该复选框。

- 7 （可选） 在“自定义模板”页面上，选择**其他属性**，然后为 vRealize Log Insight 虚拟设备设置根密码。

SSH 需要根密码。您还可以通过 VMware Remote Console 设置此密码。

- 8 按照提示完成部署。

有关部署虚拟设备的信息，请参见《部署 vApp 和虚拟设备用户指南》。

在打开虚拟设备电源后，将开始初始化进程。初始化进程需要几分钟时间完成。在进程结束时，将重新启动虚拟设备。

- 9 导航到**控制台**选项卡，然后验证 vRealize Log Insight 虚拟设备的 IP 地址。

IP 地址前缀	描述
https://	虚拟设备上的 DHCP 配置正确。
http://	虚拟设备上的 DHCP 配置失败。 a 关闭 vRealize Log Insight 虚拟设备的电源。 b 右键单击虚拟设备，然后选择 <b>编辑设置</b> 。 c 为虚拟设备设置静态 IP 地址。

### 后续步骤

- 如果要配置独立的 vRealize Log Insight 部署，请参见[配置新的 Log Insight 部署](#)。

vRealize Log Insight Web 界面的网址为 `https://log-insight-host/`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

## 启动新 vRealize Log Insight 部署

在虚拟设备部署或从集群中移除工作节点后首次访问 vRealize Log Insight Web 界面时，必须完成初始配置步骤。

在初始配置期间修改的所有设置均会在管理 Web 用户界面中提供。

有关您参与客户体验提升计划时，vRealize Log Insight 可能收集并发送到 VMware 的跟踪数据的信息，请参见第 4 章 [客户体验提升计划](#)。

### 前提条件

- 在 vSphere Client 中，记录 vRealize Log Insight 虚拟设备的 IP 地址。有关查找 IP 地址的信息，请参见[部署 vRealize Log Insight 虚拟设备](#)。
- 验证使用的浏览器是否受支持，请参见[最低要求](#)。

- 验证您是否具有有效的许可证密钥。可以通过 My VMware™ (<https://my.vmware.com/>) 帐户请求评估或永久许可证密钥。
- 如果要使用本地、vCenter Server 或 Active Directory 凭据将 vRealize Log Insight 与 vRealize Operations Manager 相集成，请验证在 vRealize Operations Manager 自定义用户界面中是否已导入这些用户。有关配置 LDAP 的说明，请参见 [vRealize Operations Manager 文档](#)。

## 步骤

- 1 使用受支持的浏览器导航到 vRealize Log Insight 的 Web 用户界面。  
URL 格式为 `https://log_insight-host/`，其中，`log_insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。  
初始配置向导将打开。
- 2 单击**启动新部署**。
- 3 设置管理员用户的密码，然后单击**保存并继续**。  
或者，也可以提供管理员用户的电子邮件地址。
- 4 输入许可证密钥，单击**添加许可证密钥**，然后单击**保存并继续**。
- 5 在“常规配置”页面上，输入从 vRealize Log Insight 接收系统通知的电子邮件地址。
- 6 如果使用 Webhook 向 vRealize Operations Manager 或第三方应用程序发送通知，请在**将 HTTP Post 系统通知发送到**文本框中输入以空格分隔的 URL 列表。
- 7 （可选）要退出客户体验提升计划，请取消选中**加入 VMware 客户体验计划**选项。单击**保存并继续**。
- 8 在“时间配置”页面上，设置在 vRealize Log Insight 虚拟设备上同步时间的方式，然后单击**测试**。

选项	描述
<b>NTP 服务器 (建议)</b>	默认情况下，vRealize Log Insight 已配置为与公用 NTP 服务器同步时间。如果由于防火墙设置无法访问外部 NTP 服务器，可以使用您组织中的内部 NTP 服务器。 使用逗号分隔多个 NTP 服务器。
<b>ESX/ESXi 主机</b>	如果没有 NTP 服务器可用，可以与在其中部署 vRealize Log Insight 虚拟设备的 ESXi 主机同步时间。

- 9 单击**保存并继续**。
- 10 （可选）要启用出站警示和系统通知电子邮件，请指定 SMTP 服务器的属性。  
要验证 SMTP 配置是否正确，请输入有效的电子邮件地址，然后单击**测试**。vRealize Log Insight 会向您所提供的地址发送测试电子邮件。
- 11 （可选）要提供自定义 SSL 证书，请将 PEM 格式的证书文件上传到集群。您还可以查看现有证书的详细信息。  
系统会将该证书添加到集群中所有节点的信任库，并将其保存起来以备后用。  
有关自定义 SSL 证书的必备条件的信息，请参见[安装自定义 SSL 证书](#)。
- 12 单击**保存并继续**。

## 结果

在 vRealize Log Insight 进程重新启动后，您将重定向至 vRealize Log Insight 的**仪表盘**选项卡。

## 后续步骤

- 导航到**管理**选项卡。从 **vSphere 集成** 页面中，配置 vRealize Log Insight 以从 vCenter Server 实例中提取任务、事件和警示，并配置 ESXi 主机以向 vRealize Log Insight 发送 syslog 源。
- 向 vRealize Log Insight 分配永久许可证。请参见《管理 vRealize Log Insight》中的[向 Log Insight 分配永久许可证](#)。
- 配置 vRealize Operations Manager 中的 vRealize Log Insight 适配器以启用“在环境中启动”。请参见《vRealize Operations Manager 配置指南》中的使用 vRealize Operations Manager 配置 vRealize Log Insight。
- 安装 vRealize Log Insight Windows 代理以收集 Windows 事件通道、Windows 目录和纯文本日志文件中的事件。请参见《使用 vRealize Log Insight 代理》中的[安装 Windows 代理](#)。

## 加入现有部署

在部署和设置独立 vRealize Log Insight 节点后，可以部署新的 vRealize Log Insight 实例，然后将其添加到现有节点以形成 vRealize Log Insight 集群。

vRealize Log Insight 可以通过在集群中使用多个虚拟设备实例来进行扩展。集群能够实现载入吞吐量的线性扩展、提高查询性能，并实现高可用性载入。在集群模式下，vRealize Log Insight 会提供主节点和工作线程节点。主节点和工作线程节点均负责处理数据子集。主节点可以查询所有数据子集并聚合结果。您可能需要更多节点来支持站点需求。您可以在一个集群中使用 3 到 18 个节点。这意味着完全正常运行的集群必须至少具有三个正常节点。在较大集群中，必须有大多数节点处于正常状态。例如，如果包含六个节点的集群中有三个节点出现故障，则在移除故障节点之前，任何节点均无法完全正常运行。

## 前提条件

- 在 vSphere Client 中，记下工作 vRealize Log Insight 虚拟设备的 IP 地址。
- 确认知晓主 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 确认拥有主 vRealize Log Insight 虚拟设备的管理员帐户。
- 确认 vRealize Log Insight 主节点和工作线程节点的版本已同步。请勿将旧版本的 vRealize Log Insight 工作线程添加到较新版本的 vRealize Log Insight 主节点。
- 必须将 vRealize Log Insight 虚拟设备上的时间与 NTP 服务器同步。请参见[同步 Log Insight 虚拟设备上的时间](#)。
- 有关支持的浏览器版本的信息，请参见《vRealize Log Insight 发行说明》。

## 步骤

- 1 使用受支持的浏览器导航到 vRealize Log Insight 工作线程的 Web 用户界面。

URL 格式为 `https://log_insight-host/`，其中，`log_insight-host` 是 vRealize Log Insight 工作线程节点虚拟设备的 IP 地址或主机名。

初始配置向导将打开。

- 2 单击**加入现有部署**。
- 3 输入 vRealize Log Insight 主节点的 IP 地址或主机名，然后单击**转到**。  
工作线程节点会向 vRealize Log Insight 主节点发送加入现有部署的请求。
- 4 单击**单击此处访问“集群管理”**页面。
- 5 以管理员身份登录。  
将加载“集群”页面。
- 6 单击**[允许]**。

工作线程节点加入现有部署，然后 vRealize Log Insight 开始在集群中运行。

## 后续步骤

- 根据需要，添加更多工作线程节点。该集群必须具有至少三个节点。

# 客户体验提升计划

# 4

该产品加入了 VMware 客户体验提升计划 (CEIP)。

有关通过 CEIP 收集的数据以及 VMware 使用该数据的用途的详细信息，请参见 Trust & Assurance Center 中的规定：<https://www.vmware.com/solutions/trustvmware/ceip.html>。

要加入或退出该产品的 CEIP，请参见《管理 vRealize Log Insight》中的“加入或退出 VMware 客户体验计划”。