Red Hat Virtualization 4.4

规划和前提条件指南

规划 Red Hat Virtualization 4.4 的安装和配置。

Last Updated: 2023-09-08

Red Hat Virtualization 4.4 规划和前提条件指南

规划 Red Hat Virtualization 4.4 的安装和配置。

Red Hat Virtualization Documentation Team
Red Hat Customer Content Services
rhev-docs@redhat.com

法律通告

摘要

本文档为 Red Hat Virtualization 环境提供要求、选项和建议。

目录

前言

Red Hat Virtualization 由连接的组件组成，每个组件在环境中都扮演不同的角色。提前计划并准备自己的要求有助于这些组件进行通信和高效运行。

本指南涵盖了：

- 硬件和安全要求
- 用于不同组件的选项
- 优化环境的建议

第 1 章 RED HAT VIRTUALIZATION 架构

Red Hat Virtualization 可以作为自托管引擎部署，也可以部署为单机管理器。自托管引擎是推荐的部署选项。

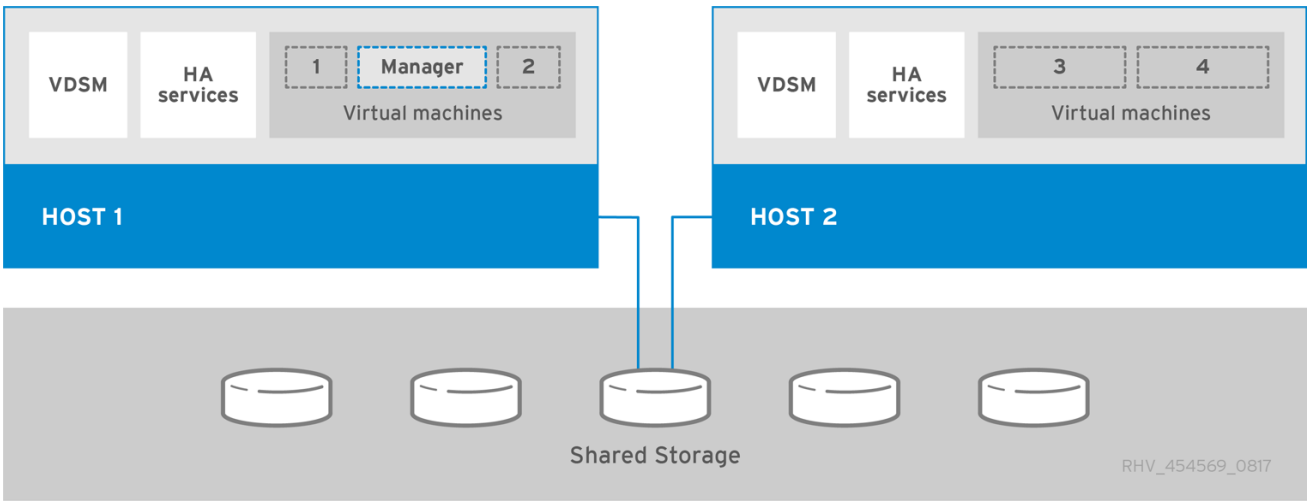
1.1. 自托管引擎架构

Red Hat Virtualization Manager 在它管理的同一环境中的自托管引擎节点（专用主机）上作为虚拟机运行。自托管引擎环境所需要的物理服务器会少一个，但需要更多的管理开销来部署和管理。管理器本身具有高可用性，无需外部 HA 管理。

自托管引擎环境的最小设置包括：

- 一个在自托管引擎节点上托管的 Red Hat Virtualization Manager 虚拟机。RHV-M 设备用于自动安装 Red Hat Enterprise Linux 8 虚拟机和该虚拟机上的 Manager。
- 至少两个自托管引擎节点以实现虚拟机高可用性。您可以使用 Red Hat Enterprise Linux 主机或 Red Hat Virtualization Manager 主机 (RHVH)。VDSM（主机代理）需要在所有主机上运行，以便与 Red Hat Virtualization Manager 进行通信。HA 服务在所有自托管引擎节点上运行，以管理管理器虚拟机的高可用性。
- 一个存储服务，可根据所使用的存储类型，运行在本地或远程服务器上。存储服务必须能被所有主机访问。

图 1.1. 自托管引擎 Red Hat Virtualization 架构



1.2. 独立管理器架构

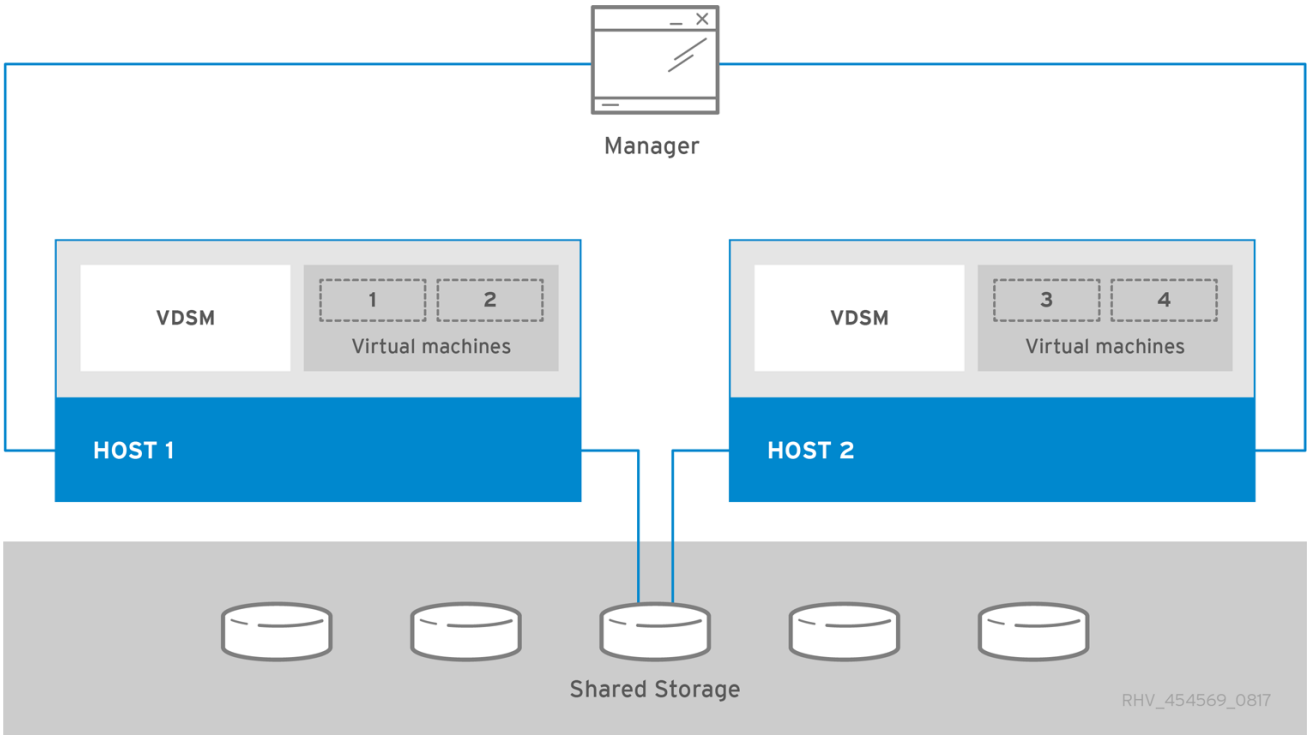
Red Hat Virtualization Manager 在物理服务器或单独虚拟化环境中托管的虚拟机上运行。单机管理器更易于部署和管理，但需要额外的物理服务器。管理器只有在外部使用产品（如红帽的高可用性附加组件）进行管理时才高度可用。

独立管理器环境的最小设置包括：

- 一个 Red Hat Virtualization Manager 机器。管理器通常部署在物理服务器上。但是，它也可以部署到虚拟机上，只要该虚拟机托管在单独的环境中。Manager 必须在 Red Hat Enterprise Linux 8 上运行。
- 至少两个用于虚拟机高可用性的主机。您可以使用 Red Hat Enterprise Linux 主机或 Red Hat Virtualization Manager 主机 (RHVH)。VDSM（主机代理）需要在所有主机上运行，以便与 Red Hat Virtualization Manager 进行通信。

- 一个存储服务，可根据所使用的存储类型，运行在本地或远程服务器上。存储服务必须能被所有主机访问。

图 1.2. 独立管理器 Red Hat Virtualization 架构



第 2 章 要求

2.1. RED HAT VIRTUALIZATION MANAGER 要求

2.1.1. 硬件要求

此处概述的最低硬件要求和推荐的硬件要求基于典型的中小型安装。根据大小和负载，部署的确切要求会有所不同。

Red Hat Enterprise Linux 的硬件认证涵盖了 Red Hat Enterprise Linux 的硬件认证。如需更多信息，请参阅 Red Hat Virtualization 是否也具有硬件认证？要确认特定硬件项目是否已经过 Red Hat Enterprise Linux 认证，请参阅红帽认证硬件。

表 2.1. Red Hat Virtualization Manager 硬件要求

资源	最小值	推荐的
CPU	一个双核 x86_64 CPU。	一个四核 x86_64 CPU 或多个双核 x86_64 CPU.
内存	如果没有安装数据仓库，并且现有进程没有使用内存，则有 4 GB 的可用系统 RAM。	16 GB 系统内存。
硬盘	25 GB 本地可访问、可写入磁盘空间。	50 GB 本地可访问、可写入磁盘空间。 您可以使用 RHV Manager History Database Size Calculator 计算管理器历史记录数据库大小的适当磁盘空间。
网络接口	1 个网络接口卡 (NIC)，带宽至少为 1 Gbps.	1 个网络接口卡 (NIC)，带宽至少为 1 Gbps.

2.1.2. 浏览器要求

以下浏览器版本和操作系统可用于访问管理门户和虚拟机门户。

浏览器支持分为几个层次：

- 1 级：经过全面测试且完全支持的浏览器和操作系统组合。红帽工程致力于修复此一级浏览器的问题。
- 2 级：浏览器和操作系统组合经过部分测试，可能起作用。为此级的浏览器提供有限的支持。红帽工程将尝试修复此级浏览器的问题。
- 3 级：浏览器和操作系统组合未经测试，但可能有效.对这个级的浏览器提供最少的支持。红帽工程将尝试仅修复此级别的浏览器上的小问题。

表 2.2. 浏览器要求

支持级别	操作系统系列	浏览器
1 级	Red Hat Enterprise Linux	Mozilla Firefox 扩展支持版本 (ESR)
	任意	Google Chrome、Mozilla Firefox 或 Microsoft Edge 的最新版本
2 级		
3 级	任意	Google Chrome 或 Mozilla Firefox 的早期版本
	任意	其他浏览器

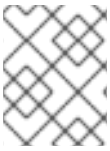
2.1.3. 客户端要求

虚拟机控制台只能使用 Red Hat Enterprise Linux 和 Windows 上的受支持的远程查看器 (**virt-viewer**) 客户端访问。要安装 **virt-viewer**，请参阅*虚拟机管理指南*中的在客户端机器上安装支持组件部分。安装 **virt-viewer** 需要管理员特权。

您可以使用 SPICE、VNC 或 RDP（仅限 Windows）协议访问虚拟机控制台。您可以在客户机操作系统中安装 QXLDOD 图形驱动程序以提高 SPICE 的功能。SPICE 目前支持最大分辨率 2560x1600 像素。

客户端操作系统 SPICE 支持

Red Hat Enterprise Linux 7.2 及更新的版本以及 Windows 10 上提供了受支持的 QXLDOD 驱动程序。



注意

SPICE 可以使用 QXLDOD 驱动程序与 Windows 8 或 8.1 配合使用，但它并没有经过认证或测试。

2.1.4. 操作系统要求

Red Hat Virtualization Manager 必须安装在 Red Hat Enterprise Linux 8.6 的基本安装中。

不要在基础安装后安装任何其他软件包，因为它们在尝试安装管理器所需的软件包时可能会导致依赖项问题。

不要启用管理器安装所需的额外软件仓库。

2.2. 主机要求

Red Hat Enterprise Linux 的硬件认证涵盖了 Red Hat Enterprise Linux 的硬件认证。如需更多信息，请参阅 Red Hat Virtualization 是否也具有硬件认证？要确认特定硬件项目是否已经过 Red Hat Enterprise Linux 认证，请查看 查找认证解决方案。

有关适用于客户机的要求和限制的更多信息，请参阅 Red Hat Enterprise Linux 技术能力和限制 以及支持的限制。

2.2.1. CPU 要求

所有 CPU 必须支持 Intel® 64 或 AMD64 CPU 扩展，并且已启用 AMD-V™ 或 Intel VT® 硬件虚拟化扩展。还需要支持 No eXecute 标志 (NX)。

支持以下 CPU 型号：

- AMD
  - Opteron G4
  - Opteron G5
  - EPYC
- Intel
  - Nehalem
  - Westmere
  - SandyBridge
  - IvyBridge
  - Haswell
  - Broadwell
  - Skylake Client
  - Skylake Server
  - Cascadelake Server
- IBM
  - POWER8
  - POWER9

对于带有安全更新的每个 CPU 型号，**CPU Type** 会列出基本类型和安全类型。例如：

- **Intel Cascadelake Server 系列**
- **Secure Intel Cascadelake Server 系列**

Secure CPU 类型包含最新的更新。详情请参阅 BZ#1731395

2.2.1.1. 检查处理器是否支持所需的标记

您必须在 BIOS 中启用虚拟化。关闭并在进行此更改后重新启动主机，以确保更改已被应用。

流程

1. 在 Red Hat Enterprise Linux 或 Red Hat Virtualization Host 引导屏幕中，按任意键，然后从列表中选择 **Boot** 或 **Boot with serial console** 条目。

2. 按 **Tab** 编辑所选选项的内核参数。
3. 确保列出的最后一个内核参数后有一个空格，并附加参数 **rescue**。
4. 按 **Enter** 键引导进入救援模式。
5. 在提示符处，确定您的处理器有所需的扩展，并通过运行以下命令启用它们：

```
# grep -E 'svm|vmx' /proc/cpuinfo | grep nx
```

如果显示任何输出，处理器将支持硬件虚拟化。如果没有显示输出，您的处理器可能仍然支持硬件虚拟化；在某些情况下，制造商会禁用 BIOS 中的虚拟化扩展。如果您认为情况确实如此，请查阅系统 BIOS 和制造商提供的主板手册。

2.2.2. 内存要求

RAM 的最小要求为 2 GB。对于集群级别 4.2 到 4.5，Red Hat Virtualization Host 中每个虚拟机的最大支持 RAM 为 6 TB。对于集群级别 4.6 到 4.7，Red Hat Virtualization Host 中每个虚拟机的最大支持 RAM 为 16 TB。

但是，所需的 RAM 量因客户机操作系统要求、客户机应用程序要求以及客户机内存活动与使用情况而异。KVM 还可以为虚拟客户机过量使用物理 RAM，允许您配置 RAM 要求大于实际存在的客户机，假设客户机并非全部在高峰负载同时工作。KVM 仅根据需要为 guest 分配 RAM，并将利用率不足的 guest 转移至交换。

2.2.3. 存储要求

主机需要存储来存储配置、日志、内核转储，并用作交换空间。存储可以是本地存储，也可以基于网络.Red Hat Virtualization Host (RHVH) 可以使用在网络存储中默认分配的一个或多个进行引导。如果出现断网的情况，则从网络存储引导可能会导致冻结。添加置入多路径配置文件可帮助解决网络连接中断的问题。如果 RHVH 从 SAN 存储引导并丢失连接，则文件将变为只读，直到网络连接恢复为止。使用网络存储可能会导致性能下降。

RHVH 的最低存储要求记录在本节中。Red Hat Enterprise Linux 主机的存储要求根据其现有配置所使用的磁盘空间量而有所不同，但应该大于 RHVH。

下方列出了主机安装的最低存储要求：但是，使用默认分配，这将使用更多存储空间。

- / (root) - 6 GB
- /home - 1 GB
- /tmp - 1 GB
- /boot - 1 GB
- /var - 5 GB
- /var/crash - 10 GB
- /var/log - 8 GB
- /var/log/audit - 2 GB
- /var/tmp - 10 GB

- swap - 1 GB.详情请查看 Red Hat 平台推荐的 swap 大小是什么？
- Anaconda 在卷组中保留 20% 的精简池大小，以便将来进行元数据扩展。这是为了避免开箱即用的配置在正常使用条件下耗尽空间。还不支持在安装过程中过度置备精简池。
- **最小总量 - 64 GiB**

如果您还安装了用于自托管引擎安装的 RHV-M 设备，**/var/tmp** 必须至少为 10 GB。

如果您计划使用内存过量分配功能，请添加足够的交换空间为所有虚拟机提供虚拟内存。请参阅内存优化。

2.2.4. PCI 设备要求

主机必须至少有一个网络接口，最小带宽为 1 Gbps。每个主机应具有两个网络接口，一个专用于支持网络密集型活动，如虚拟机迁移。此类操作的性能受可用带宽的限制。

有关如何使用 PCI Express 和传统 PCI 设备及基于 Intel Q35 的虚拟机的信息，请参阅 *使用 PCI Express 和带有 Q35 虚拟机的约定 PCI 设备*。

2.2.5. 设备分配要求

如果您计划实施设备分配和 PCI 直通，以便虚拟机可以使用主机中的特定 PCIe 设备，请确保满足以下要求：

- CPU 必须支持 IOMMU（如 VT-d 或 AMD-Vi）。IBM POWER8 默认支持 IOMMU。
- 固件必须支持 IOMMU。
- 使用的 CPU 根端口必须支持 ACS 或 ACS 等效功能。
- PCIe 设备必须支持 ACS 或 ACS 等效功能。
- PCIe 设备和根端口之间的所有 PCIe 交换机和网桥都应支持 ACS。例如，如果交换机不支持 ACS，该交换机后面的所有设备共享同一个 IOMMU 组，并且只能分配到同一虚拟机。
- 对于 GPU 支持，Red Hat Enterprise Linux 8 支持 PCIe 的基于 PCIe 的 NVIDIA K-Series Quadro（model 2000 系列或更高版本）、GRID 和 Tesla 作为非 VGA 图形设备分配。目前，除其中一个标准模拟 VGA 接口外，还最多可将两个 GPU 附加到虚拟机。模拟的 VGA 用于预引导和安装，在加载 NVIDIA 图形驱动程序时，NVIDIA GPU 将接管。请注意，不支持 NVIDIA Quadro 2000 卡，也不支持 Quadro K420 卡。

检查供应商规格和产品规格说明，以确认您的硬件是否满足这些要求。**lspci -v** 命令可用于打印系统上已安装的 PCI 设备的信息。

2.2.6. vGPU 要求

主机必须满足以下要求才能使该主机上的虚拟机使用 vGPU：

- vGPU-compatible GPU
- 启用 GPU 的主机内核
- 安装了带有正确驱动程序的 GPU

- 在**管理**门户中的虚拟机**主机**设备选项卡中的 **管理 vGPU** 对话框中，选择这个虚拟机要使用的 vGPU 类型以及实例数量。
- 在集群中的每个主机上安装支持 vGPU 的驱动程序
- 安装了 vGPU 驱动程序的 vGPU 支持的虚拟机操作系统

2.3. 网络要求

2.3.1. 常规要求

Red Hat Virtualization 要求在运行 Manager 的物理或虚拟机中保持 IPv6 处于启用状态。不要在 Manager 机器上禁用 IPv6，即使您的系统没有使用它。

2.3.2. 自托管引擎部署的网络范围

自托管引擎部署流程临时使用 **192.168** 下的 **/24** 网络地址。默认为 **192.168.222.0/24**，如果使用此地址，它将尝试 **192.168** 下的其他 **/24** 地址，直到找到不使用的地址。如果此范围内找不到未使用的网络地址，部署会失败。

使用命令行安装自托管引擎时，您可以将部署脚本设置为使用备用 **/24** 网络范围，选项为 **--ansible-extra-vars=he_ipv4_subnet_prefix=*PREFIX***，其中 ***PREFIX*** 是默认范围的前缀。例如：

```
# hosted-engine --deploy --ansible-extra-vars=he_ipv4_subnet_prefix=192.168.222
```

注意

您只能通过使用命令行将 Red Hat Virtualization 安装为自托管引擎来设置另一个范围。

2.3.3. DNS、NTP 和 IPMI 隔离的防火墙要求

以下所有主题的防火墙要求都是需要单独考虑的特例。

DNS 和 NTP

Red Hat Virtualization 不会创建 DNS 或 NTP 服务器，因此防火墙不需要开放端口用于传入流量。

默认情况下，Red Hat Enterprise Linux 允许到任何目标地址上的 DNS 和 NTP 的出站流量。如果您禁用传出流量，请为发送到 DNS 和 NTP 服务器的请求定义例外。

重要

- Red Hat Virtualization Manager 和所有主机（Red Hat Virtualization Host 和 Red Hat Enterprise Linux 主机）必须具有完全限定域名和完整、完全对齐和反向名称解析。
- 不支持在 Red Hat Virtualization 环境中将 DNS 服务作为虚拟机运行。Red Hat Virtualization 环境使用的所有 DNS 服务都必须托管在环境之外。
- 使用 DNS 而不是 **/etc/hosts** 文件进行名称解析。使用主机文件通常需要更多工作，并且更容易出错。

IPMI 和其他隔离机制（可选）

对于 IPMI（智能平台管理接口）和其他隔离机制，防火墙不需要开放传入流量的端口。

默认情况下，Red Hat Enterprise Linux 允许到任何目标地址上的端口出站 IPMI 流量。如果您禁用传出流量，请对发送到 IPMI 或隔离服务器的请求进行例外处理。

集群中的每个 Red Hat Virtualization Host 和 Red Hat Enterprise Linux 主机都必须能够连接到集群中所有其他主机的隔离设备。如果集群主机遇到错误（网络错误，存储错误……）且无法作为主机运行，它们必须能够连接到数据中心中的其他主机。

具体端口号取决于您使用的隔离代理的类型以及配置方式。

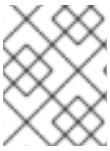
以下部分中的防火墙要求表不代表这个选项。

2.3.4. Red Hat Virtualization Manager 防火墙要求

Red Hat Virtualization Manager 要求打开多个端口以允许通过系统的防火墙网络流量。

engine-setup 脚本可以自动配置防火墙。

此处记录的防火墙配置假定默认配置。



注意

这些防火墙要求图请参考 https://access.redhat.com/articles/3932211。您可以使用表中的 ID 来查找图中的连接。

表 2.3. Red Hat Virtualization Manager 防火墙要求

ID	端口	协议	源	目的地	用途	默认加密
M1	-	ICMP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	Red Hat Virtualization Manager	可选。 可以帮助诊断.	否
M2	22	TCP	用于维护管理器的系统，包括后端配置和软件升级。	Red Hat Virtualization Manager	SSH 访问。 可选。	是
M3	2222	TCP	访问虚拟机串行控制台的客户端.	Red Hat Virtualization Manager	SSH 访问，以启用与虚拟机串行控制台的连接。	是

ID	端口	协议	源	目的地	用途	默认加密
M4	80, 443	TCP	管理门户客户端 虚拟机门户客户端 Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机 REST API 客户端	Red Hat Virtualization Manager	提供对 Manager 的 HTTP（端口 80，未加密）和 HTTPS（端口 443、加密）访问。HTTP 将连接重定向到 HTTPS。	是
M5	6100	TCP	管理门户客户端 虚拟机门户客户端	Red Hat Virtualization Manager	当 websocket 代理在 Manager 上运行时，为基于 Web 的控制台客户端 **noVNC** 提供 websocket 代理访问。	否
M6	7410	UDP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	Red Hat Virtualization Manager	如果在主机上启用了 Kdump，在 Manager 中为 fence_kdump 侦听程序打开此端口。请参阅 fence_kdump 高级配置。**fence_kdump** 不提供加密连接的方法。但是，您可以将此端口手动配置为阻止来自不符合条件的主机的访问。	否

ID	端口	协议	源	目的地	用途	默认加密
M7	54323	TCP	管理门户客户端	Red Hat Virtualization Manager（**ovirt-imageio** 服务）	与 **ovirt-imageo** 服务通信需要此项。	是
M8	6642	TCP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	开放虚拟网络 (OVN) 南向数据库	连接到开放虚拟网络 (OVN) 数据库	是
M9	9696	TCP	OVN 外部网络提供程序的客户端	OVN 的外部网络供应商	OpenStack 网络 API	是，使用 engine-setup 生成的配置。
M10	35357	TCP	OVN 外部网络提供程序的客户端	OVN 的外部网络供应商	OpenStack Identity API	是，使用 engine-setup 生成的配置。
M11	53	TCP, UDP	Red Hat Virtualization Manager	DNS 服务器	从 1023 以上端口到端口 53 的 DNS 查找请求，以及响应。默认打开。	否
M12	123	UDP	Red Hat Virtualization Manager	NTP 服务器	从 1023 以上端口到端口 123 的 NTP 请求，以及响应. 默认打开。	否

注意

- OVN 北向数据库 (6641) 的端口没有列出，因为在默认配置中，OVN 北向数据库 (6641) 的唯一客户端是 **ovirt-provider-ovn**。由于它们在同一主机上运行，因此它们的通信对网络不可见。
- 默认情况下，Red Hat Enterprise Linux 允许到任何目标地址上的 DNS 和 NTP 的出站流量。如果您禁用传出流量，请为 Manager 异常向 DNS 和 NTP 服务器发送请求。其他节点可能还需要 DNS 和 NTP。在这种情况下，请查看这些节点的要求并相应地配置防火墙。

2.3.5. 主机防火墙要求

Red Hat Enterprise Linux 主机和 Red Hat Virtualization 主机 (RHVH) 需要打开多个端口，以允许通过系统的防火墙网络流量。在向 Manager 添加新主机时，默认自动配置防火墙规则，覆盖任何预先存在的防火墙配置。

要在添加新主机时禁用自动防火墙配置，请清除 **Advanced Parameters** 下的 **Automatically configure host firewall** 复选框。

要自定义主机防火墙规则，请参阅 RHV：如何自定义主机的防火墙规则？

注意

Red Hat Virtualization: Firewall Requirements Diagram 为这些防火墙要求图。您可以使用表中的 ID 来查找图中的连接。

表 2.4. 虚拟化主机防火墙要求

ID	端口	协议	源	目的地	用途	默认加密
H1	22	TCP	Red Hat Virtualization Manager	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	SSH 访问。 可选。	是
H2	2223	TCP	Red Hat Virtualization Manager	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	SSH 访问，以启用与虚拟机串行控制台的连接。	是
H3	161	UDP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	Red Hat Virtualization Manager	简单的网络管理协议 (SNMP)。只有在您想要简单网络管理协议从主机发送到一个或多个外部 SNMP 管理器时才需要。 可选。	否

ID	端口	协议	源	目的地	用途	默认加密
H4	111	TCP	NFS 存储服务器	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	NFS 连接。 可选。	否
H5	5900 - 6923	TCP	管理门户客户端 虚拟机门户客户端	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	通过 VNC 和 SPICE 访问远程客户机控制台.必须打开这些端口，以便于客户端访问虚拟机。	是（可选）
H6	5989	TCP, UDP	Common Information Model Object Manager (CIMOM)	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	CIMOM 用于监控主机上运行的虚拟机。只有在您想要使用 CIMOM 监控虚拟化环境中的虚拟机时才需要。 可选。	否
H7	9090	TCP	Red Hat Virtualization Manager 客户端机器	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	需要此项以访问 Cockpit Web 界面（如果已安装）。	是
H8	16514	TCP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	使用 **libvirt** 进行虚拟机迁移。	是

ID	端口	协议	源	目的地	用途	默认加密
H9	49152 - 49215	TCP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	使用 VDSM 进行虚拟机迁移和隔离. 这些端口必须处于打开状态，以促进虚拟机的自动化和手动迁移。	是。根据隔离代理，通过 libvirt 进行迁移。
H10	54321	TCP	Red Hat Virtualization Manager Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	VDSM 与管理器和其他虚拟化主机的通信。	是
H11	54322	TCP	Red Hat Virtualization Manager **ovirt-imageio** 服务	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	与 **ovirt-imageo** 服务通信需要此项。	是
H12	6081	UDP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	当将开放虚拟网络 (OVN) 用作网络提供程序时，需要允许 OVN 在主机之间创建隧道。	否
H13	53	TCP, UDP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	DNS 服务器	从 1023 以上端口到端口 53 的 DNS 查找请求，以及响应。此端口是必需的并默认打开。	否

ID	端口	协议	源	目的地	用途	默认加密
H14	123	UDP	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	NTP 服务器	从 1023 以上端口到端口 123 的 NTP 请求，以及响应.此端口是必需的并默认打开。	
H15	4500	TCP, UDP	Red Hat Virtualization 主机	Red Hat Virtualization 主机	Internet 安全协议 (IPSec)	是
H16	500	UDP	Red Hat Virtualization 主机	Red Hat Virtualization 主机	Internet 安全协议 (IPSec)	是
H17	-	AH, ESP	Red Hat Virtualization 主机	Red Hat Virtualization 主机	Internet 安全协议 (IPSec)	是

注意

默认情况下，Red Hat Enterprise Linux 允许到任何目标地址上的 DNS 和 NTP 的出站流量。如果您禁用传出流量，请对 Red Hat Virtualization 主机进行例外处理

Red Hat Enterprise Linux 主机向 DNS 和 NTP 服务器发送请求。其他节点可能还需要 DNS 和 NTP。在这种情况下，请查看这些节点的要求并相应地配置防火墙。

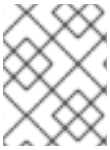
2.3.6. 数据库服务器防火墙要求

Red Hat Virtualization 支持将远程数据库服务器用于管理器数据库（**引擎**）和数据仓库数据库 (**ovirt-engine-history**)。如果您计划使用远程数据库服务器，则必须允许与管理器和数据仓库服务（它们可以独立于管理器）的连接。

同样，如果您计划从外部系统访问本地或远程数据仓库数据库，数据库必须允许来自该系统的连接。

重要

不支持从外部系统访问 Manager 数据库。



注意

这些防火墙要求图请参考 https://access.redhat.com/articles/3932211。您可以使用表中的 ID 来查找图中的连接。

表 2.5. 数据库服务器防火墙要求

ID	端口	协议	源	目的地	用途	默认加密
D1	5432	TCP, UDP	Red Hat Virtualization Manager 数据仓库服务	管理器（**引擎**）数据库服务器 数据仓库 (**ovirt-engine-history**) 数据库服务器	PostgreSQL 数据库连接的默认端口。	否，但可以启用。
D2	5432	TCP, UDP	外部系统	数据仓库 (**ovirt-engine-history**) 数据库服务器	PostgreSQL 数据库连接的默认端口。	默认禁用此选项。否，但可以启用。

2.3.7. 最大传输单元要求

部署期间，推荐的主机最大传输单位(MTU)设置是 1500。在环境设置为不同的 MTU 后，可以更新此设置。如需有关更改 MTU 设置的更多信息，请参阅如何更改托管引擎虚拟机网络 MTU。

第 3 章 注意事项

本章介绍了各种 Red Hat Virtualization 组件的优点、限制和可用选项。

3.1. 主机类型

使用最适合您环境的主机类型。如果需要，您也可以在同一集群中同时使用这两种类型的主机。

集群内的所有受管主机都必须具有相同的 CPU 类型。Intel 和 AMD CPU 无法在同一集群中共存。

有关支持的最大限制和限制信息，如 Red Hat Virtualization Manager 可以支持的最大主机数量，请参阅 Red Hat Virtualization 支持的限制。

3.1.1. Red Hat Virtualization 主机

Red Hat Virtualization 主机 (RHVH) 与 Red Hat Enterprise Linux 主机相比有以下优点：

- RHVH 包含在 Red Hat Virtualization 订阅中。Red Hat Enterprise Linux 主机可能需要额外订阅。
- RHVH 部署为单个镜像。这会产生一个简化的更新过程，整个镜像都会作为一个整体更新，而不是单独更新的软件包。
- 仅包含托管虚拟机或管理主机本身所需的软件包和服务。这简化了操作并减少总体攻击向量；因为不会部署不必要的软件包和服务，所以不会被安全攻击所利用。
- Cockpit Web 界面默认可用，包括特定于 Red Hat Virtualization 的扩展，包括虚拟机监控工具和自托管引擎的 GUI 安装程序。Cockpit 支持 Red Hat Enterprise Linux 主机，但必须手动安装。

3.1.2. Red Hat Enterprise Linux 主机

Red Hat Enterprise Linux 主机与 Red Hat Virtualization 主机相比有以下优点：

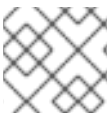
- Red Hat Enterprise Linux 主机是高度定制的，因此如果主机需要特定的文件系统布局，则可能是一个最好的选择。
- Red Hat Enterprise Linux 主机更适合频繁更新，特别是在安装了其他软件包时。单个软件包可以更新，而不是整个镜像。

3.2. 存储类型

每个数据中心必须至少有一个数据存储域。另外，还建议每个数据中心有一个 ISO 存储域。导出存储域已被弃用，但在需要时仍可创建。

存储域可以由块设备（iSCSI 或光纤通道）或者文件系统组成。

默认情况下，GlusterFS 域和本地存储域支持 4K 块大小。4k 块大小可以提供更好的性能，特别是在使用大型文件时，在使用需要 4K 兼容性的工具时（如 VDO）也需要这样做。



注意

GlusterFS 存储已弃用，并将在以后的发行版本中删除。

重要

Red Hat Virtualization 目前不支持块大小为 4K 的块存储。您必须以旧模式（512b 块）配置块存储。

以下部分中描述的存储类型支持用作数据存储域。ISO 和导出存储域仅支持基于文件的存储类型。ISO 域在本地存储数据中心中使用时支持本地存储。

请参阅：

- *管理指南*中的存储。
- *Red Hat Enterprise Linux 存储管理指南*

3.2.1. NFS

Red Hat Virtualization 4 支持 NFS 版本 3 和 4。生产工作负载需要企业级 NFS 服务器，除非 NFS 仅用作 ISO 存储域。当企业 NFS 部署通过 10GbE、且与 VLAN 分隔的网络进行，并且将各个服务配置为使用特定端口时，则部署过程既快且安全。

随着 NFS 导出的增长以适应更多存储需求，Red Hat Virtualization 可以立即识别更大的数据存储。主机或 Red Hat Virtualization 不需要其他配置。这从扩展和运营角度而言，提供了与块存储相比的 NFS 边缘。

请参阅：

- *Red Hat Enterprise Linux 存储管理指南* 中的网络文件系统(NFS)
- *管理指南*中的准备和添加 NFS 存储.

3.2.2. iSCSI

生产工作负载需要企业级 iSCSI 服务器。当企业 iSCSI 部署通过 10GbE、与 VLAN 分隔并使用 CHAP 验证的网络进行时，它既快速且安全。iSCSI 也可以使用多路径来实现高可用性。

Red Hat Virtualization 每个基于块的存储域支持 1500 个逻辑卷。不允许超过 300 个 LUN。

请参阅：

- *Red Hat Enterprise Linux Storage 管理指南* 中的在线存储管理.
- *管理指南*中的添加 iSCSI 存储。

3.2.3. Fibre Channel

Fibre Channel 是快速安全的，如果已在目标数据中心中使用它，则应该使用它。与 iSCSI 和 NFS 相比，它还具有低 CPU 开销优势。Fibre Channel 也可以使用多路径来提高高可用性。

Red Hat Virtualization 每个基于块的存储域支持 1500 个逻辑卷。不允许超过 300 个 LUN。

请参阅：

- *Red Hat Enterprise Linux Storage 管理指南* 中的在线存储管理.
- *管理指南*中的添加 FCP 存储。

3.2.4. 通过以太网光纤通道

要在 Red Hat Virtualization 中使用 Fibre Channel over Ethernet(FCoE)，您必须在 Manager 上启用 **fcoe** 密钥，并在主机上安装 *vdsm-hook-fcoe* 软件包。

Red Hat Virtualization 每个基于块的存储域支持 1500 个逻辑卷。不允许超过 300 个 LUN。

请参阅：

- *Red Hat Enterprise Linux Storage 管理指南* 中的在线存储管理.
- *管理指南* 中的如何将 Red Hat Virtualization Manager 设置为使用 FCoE 。

3.2.5. Red Hat Hyperconverged Infrastructure

Red Hat Hyperconverged Infrastructure (RHHI) 将 Red Hat Virtualization 和 Red Hat Gluster Storage 整合到同一基础架构上，而不是将 Red Hat Virtualization 连接到远程 Red Hat Gluster Storage 服务器。这个紧凑选项可减少运营开支和开销。

请参阅：

- *部署 Red Hat Hyperconverged Infrastructure for Virtualization*
- *在单节点上部署 Red Hat Hyperconverged Infrastructure for Virtualization*
- *Automating RHHI for Virtualization Deployment*

3.2.6. POSIX-Compliant FS

其他与 POSIX 兼容的文件系统可作为 Red Hat Virtualization 中的存储域使用，只要它们是集群的文件系统，如 Red Hat Global File System 2(GFS2)，并且支持稀疏文件和直接 I/O。例如，通用 Internet 文件系统(CIFS)不支持直接 I/O，使它与 Red Hat Virtualization 不兼容。

请参阅：

- *Red Hat Enterprise Linux 全局文件系统 2*
- *管理指南*中的添加 POSIX Compliant 文件系统存储。

3.2.7. 本地存储

本地存储在单独的主机上使用主机自己的资源进行设置。当您将主机设置为使用本地存储时，它会自动添加到新的数据中心，并在没有其他主机的集群可以添加到其中。在单主机集群中创建的虚拟机无法迁移、隔离或调度。

对于 Red Hat Virtualization 主机，应该始终在独立于 /(root)的文件系统上定义本地存储。使用单独的逻辑卷或磁盘。

请参见*管理指南*中的准备和添加本地存储。

3.3. 网络注意事项

在 Red Hat Virtualization 环境中规划和设置网络时，强烈建议先熟悉网络概念及其使用。有关管理网络的更多信息，请阅读您的网络硬件供应商指南。

可以使用物理设备（如 NIC）或逻辑设备（如网络绑定）支持逻辑网络。绑定提高了高可用性，并提供容错能力，因为绑定中的所有网络接口卡都必须失败。绑定模式 1、2、3 和 4 支持虚拟机和非虚拟机网络类型。模式 0、5 和 6 仅支持非虚拟机网络。Red Hat Virtualization 默认使用模式 4。

不需要为每个逻辑网络有一个设备，因为多个逻辑网络可以使用虚拟 LAN(VLAN)标记共享单个设备来隔离网络流量。要使用这个功能，还必须在交换机级别支持 VLAN 标记。

应用到在 Red Hat Virtualization 环境中定义的逻辑网络数量的限制是：

- 附加到主机的逻辑网络数量限制为可用网络设备的数量，以及最大虚拟 LAN(VLAN)的数量，即 4096。
- 单个操作中可以附加到主机的网络数量当前限制为 50。
- 集群中的逻辑网络数量仅限于可附加到主机（因为网络）对于集群中所有主机的逻辑网络数量。
- 数据中心中的逻辑网络数量仅限于它所包含的集群数量，与每个集群允许的逻辑网络数量相结合。

重要

修改管理网络属性(**ovirtmgmt**)时请格外小心。对 **ovirtmgmt** 网络属性的更改不正确，可能会导致主机变得不可访问。

重要

如果您计划使用 Red Hat Virtualization 为其他环境提供服务，请记住，如果 Red Hat Virtualization 环境停止运行，该服务将停止。

Red Hat Virtualization 与 Cisco Application Centric Infrastructure(ACI)完全集成，它提供全面的网络管理功能，从而减少了手动配置 Red Hat Virtualization 网络基础架构的需要。该集成是通过根据 Cisco 的文档在 Cisco 的应用策略基础架构控制器(APIC)版本 3.1(1)及之后的版本上配置红帽虚拟化来进行集成。

3.4. 目录服务器支持

在安装过程中，Red Hat Virtualization Manager 会在默认 **internal** 域中创建一个默认的 **admin** 用户。此帐户供初始配置环境和故障排除时使用。您可以使用 **ovirt-aaa-jdbc-tool** 在 **interna** 域中创建其他用户。在本地域中创建的用户帐户称为本地用户。请参阅 *管理指南*中的从命令行管理用户任务。

您还可以将外部目录服务器附加到 Red Hat Virtualization 环境中，并将其用作外部域。在外部域中创建的用户帐户称为目录用户。还支持将多个目录服务器附加到管理器。

以下目录服务器支持与 Red Hat Virtualization 搭配使用。有关安装和配置受支持的目录服务器的详情，请查看厂商的文档。

- Microsoft Active Directory
- Red Hat Enterprise Linux Identity Management
- Red Hat Directory Server
- OpenLDAP
- IBM Security(Tivoli)目录服务器

重要

必须在目录服务器中创建有权读取所有用户和组的用户，专门用于作为 Red Hat Virtualization 管理用户使用。**不要**将目录服务器的管理用户用作 Red Hat Virtualization 管理用户。

请参见 *管理指南* 中的用户和角色。

3.5. 基础架构注意事项

3.5.1. 本地或远程主机

以下组件可以托管在 Manager 或远程机器上。在 Manager 计算机上保留所有组件变得更加简单且需要较少的维护，因此当性能不是问题时，最好这样做。将组件移动到远程机器中需要更多维护，但可提高 Manager 和 Data Warehouse 的性能。

数据仓库数据库和服务

要在 Manager 上托管数据仓库，请在 **engine-setup** 提示时选择 **Yes**。
要在远程机器上托管数据仓库，请选择 **No**（当由 **engine-setup** 提示时），并请参阅 *安装 Red Hat Virtualization 作为一个单独的 Manager，使用远程数据库* 中的在一个独立的机器上安装并配置 Data Warehouse。

要在安装后迁移数据仓库，请参阅 *Data Warehouse 指南* 中的将数据仓库迁移到一个独立的机器。

您还可以将数据仓库服务和数据仓库数据库分别托管在不同的系统中。

Manager 数据库

要在 Manager 上托管 Manager 数据库，请在 **engine-setup** 提示时选择 **Local**。
要在远程机器上托管 Manager 数据库，请首先参阅 *安装 Red Hat Virtualization 作为一个独立的 Manager，使用远程数据库* 中的准备一个远程的 PostgreSQL 数据库部分，然后再在 Manager 上运行 **engine-setup**。

要在安装后迁移 Manager 数据库，请参阅 *管理指南* 中的将引擎数据库迁移到远程服务器数据库。

Websocket 代理

要在 Manager 上托管 websocket 代理，请在 **engine-setup** 提示时选择 **Yes**。

重要

自托管引擎环境使用设备来安装和配置管理器虚拟机，因此数据仓库、管理器数据库和 websocket 代理只能进行外部安装后。

3.5.2. 仅限远程主机

以下组件必须托管在远程机器上：

DNS

由于在 Red Hat Virtualization 环境中广泛使用 DNS，因此不支持将环境的 DNS 服务作为环境中托管的虚拟机运行。

存储

除本地存储外，存储服务不得与管理器或任何主机位于同一个机器上。

身份管理

IdM (**ipa-server**) 与 **mod_ssl** 软件包不兼容，后者是 Manager 所需的。

第 4 章 建议

本章介绍了一些并不是严格要求的配置，但这些配置可能会提高您的环境的性能或稳定性。

4.1. 常规建议

- 部署完成后就立即进行完整备份，并将它存储在单独的位置。稍后进行常规备份。请参见*管理指南*中的备份和迁移。
- 避免运行 Red Hat Virtualization 依赖于同一环境中的虚拟机的任何服务。如果出现这种情况，则必须仔细规划，如果包含该服务的虚拟机停机，则需要仔细规划。
- 确保安装 Red Hat Virtualization Manager 的裸机主机或虚拟机有充足的熵。200 值可能会导致 Manager 设置失败。要检查熵值，请运行 **cat /proc/sys/kernel/random/entropy_avail**。要提高熵，请安装 **rng-tools** 软件包，并遵循如何自定义 rngd 服务启动的步骤？
- 您可以使用 PXE、Kickstart、Satellite、CloudForms、Ansible 或结合使用来自动部署主机和虚拟机。但是，不支持使用 PXE 安装自托管引擎。请参阅：
  - 使用 PXE 和 Kickstart 自动部署 Red Hat Virtualization Host Deployment 以实现自动化 RHVH 部署的额外要求。
  - *执行标准 RHEL 安装*中的准备您的安装。
  - *执行高级 RHEL 安装*中的使用 Kickstart 执行自动安装.
  - *Red Hat Satellite 6.2 置备指南*。
  - *Red Hat CloudForms 5.0 置备虚拟机和主机*。
  - *管理指南*中的使用 Ansible 自动化配置任务。
- 将部署中的所有机器的系统时区设置为 UTC。这样可确保数据收集和连接不会因您的本地时区的不同而中断，比如夏时制时间。
- 在环境中，使用所有主机和虚拟机上的网络时间协议(NTP)来同步时间。身份验证和证书对时间偏移特别敏感。在以前的版本中，NTP 可使用 **chrony** (**chrony**)或 **ntp** (**ntpd**)，但在 Red Hat Enterprise Linux 8 中只支持 **chrony**。
  有关从 **ntp** 迁移到 **chrony** 的详情，请参考迁移到 **chrony**。

  有关 **chrony** 的更多信息，请参阅使用 Chrony 套件配置 NTP。
- 记录下所有内容，以便使用环境的任何人都可以了解其当前状态和所需程序。

4.2. 安全建议

- 不要在主机或虚拟机上禁用任何安全功能（如 HTTPS、SELinux 和防火墙）。
- 将所有主机和 Red Hat Enterprise Linux 虚拟机注册到 Red Hat Content Delivery Network 或 Red Hat Satellite，以便获得最新的安全更新和勘误。
- 创建单独的管理员帐户，而不是允许很多人使用默认的 **admin** 帐户，以正确跟踪活动。
- 限制主机的访问权限并创建单独的登录。不要创建一个单独的 **root** 登录为每个人使用。有关管理用户、组和 root 权限的具体信息，请参阅*配置基本系统设置*。

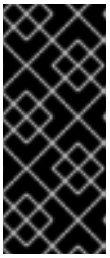
- 不要在主机上创建不受信任的用户。
- 部署 Red Hat Enterprise Linux 主机时，只安装满足虚拟化、性能、安全和监控要求所需的软件包和服务。生产主机不应具有额外的软件包，如 analyzers、编译器或其他组件，它们添加了不必要的安全风险。

4.3. 主机建议

- 标准化同一集群中的主机。这包括具有一致的硬件型号和固件版本。在同一集群中混合不同的服务器硬件可能会导致从主机到主机的性能不一致。
- 虽然您可以在同一个集群中同时使用 Red Hat Enterprise Linux 主机和 Red Hat Virtualization Host，但只有在满足特定业务或技术要求时才应使用此配置。
- 在部署时配置隔离设备。高可用性需要隔离设备。
- 为隔离流量使用单独的硬件交换机。如果监控和隔离在同一个交换机中，则该交换机就成为高可用性的单一故障点。

4.4. 网络建议

- 绑定网络接口，特别是生产主机上。绑定可提高服务的整体可用性，以及网络带宽。请参见 *管理指南*中的网络绑定。
- 配置 DNS 和 DHCP 记录的稳定网络基础架构。
- 如果绑定将与其他网络流量共享，则需要正确的服务质量(QoS)用于存储和其他网络流量。
- 为了获得最佳性能和简化的故障排除，请使用 VLAN 来分隔不同的流量类型，并尽可能使用 10 GbE 或 40 GbE 网络。
- 如果底层交换机支持巨型帧，请将 MTU 设置为底层交换机支持的最大值（如 **9000**）。对于大多数应用程序，这个设置启用了最佳吞吐量，且带宽较低并降低 CPU 使用率。默认 MTU 由底层交换机支持的最小大小决定。如果您启用了 LLDP，您可以在 **Setup Host Networks** 窗口中看到 NIC 工具提示中每个主机的对等点支持的 MTU。

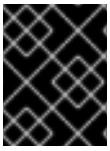


重要

如果更改网络的 **MTU** 设置，您必须将此更改传播到网络中的正在运行的虚拟机：Hot unplug 和 replug each virtual machine 的 vNIC（应该应用 MTU 设置），或重启虚拟机。否则，当虚拟机迁移到另一台主机时，这些接口会失败。如需更多信息，请参阅 网络 MTU 更改后，一些虚拟机和网桥有旧的 MTU，查看数据包丢弃和 BZ#1766414。

- 1 GbE 网络应该只用于管理流量。将 10 GbE 或 40 GbE 用于虚拟机和基于以太网的存储。
- 如果向主机添加了额外的物理接口以供存储使用，请清除 **VM 网络**，以便直接将 VLAN 分配给物理接口。

配置主机网络的建议做法



重要

始终使用 RHV Manager 来修改集群中的主机的网络配置。否则，您可能创建不受支持的配置。详情请查看 Network Manager Stateful Configuration (nmstate)。

如果您的网络环境比较复杂，您可能需要在将主机添加到 Red Hat Virtualization Manager 之前手动配置主机网络。

在配置主机网络时请考虑以下做法：

- 使用 Cockpit 配置网络。或者，您可以使用 **nmtui** 或 **nmcli**。
- 如果自托管引擎部署或将主机添加到管理器时不需要网络，请在将主机添加到管理器后在管理门户中配置网络。请参阅在数据中心或集群中创建新逻辑网络。
- 使用以下命名约定：
  - VLAN 设备：***VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD***
  - VLAN 接口：***physical_device.VLAN_ID*** (例如 **eth0.23**, **eth1.128**, **enp3s0.50**)
  - 绑定接口：**bond*number*** (for example, **bond0**, **bond1**)
  - 绑定接口上的 VLAN：**bond*number.VLAN_ID*** (例如，**bond0.50**, **bond1.128**)
- 使用网络绑定.Red Hat Virtualization 不支持网络合作，如果主机用于部署自托管引擎或添加到管理器，则会导致错误。
- 使用推荐的绑定模式：
  - 如果虚拟机不使用 **ovirtmgmt** 网络，则网络可以使用任何支持的绑定模式。
  - 如果虚拟机使用了 **ovirtmgmt** 网络，请参阅 *哪种绑定模式与虚拟机客户机或容器连接的网桥一起使用？*。
  - Red Hat Virtualization 的默认绑定模式是 **(Mode 4)Dynamic Link Aggregation**。如果您的交换机不支持链路聚合控制协议 (LACP)，请使用 **(Mode 1)Active-Backup**。详情请查看绑定模式。
- 如以下示例所示，在物理 NIC 上配置 VLAN（尽管使用了 **nmcli**，但您可以使用任何工具）：

```
# nmcli connection add type vlan con-name vlan50 ifname eth0.50 dev eth0 id 50
# nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24 +ipv4.gateway
123.123.0.254
```

- 在绑定上配置 VLAN，如下例中所示（尽管使用了 **nmcli**，但您可以使用任何工具）：

```
# nmcli connection add type bond con-name bond0 ifname bond0 bond.options
"mode=active-backup,miimon=100" ipv4.method disabled ipv6.method ignore
# nmcli connection add type ethernet con-name eth0 ifname eth0 master bond0 slave-type
bond
# nmcli connection add type ethernet con-name eth1 ifname eth1 master bond0 slave-type
bond
# nmcli connection add type vlan con-name vlan50 ifname bond0.50 dev bond0 id 50
# nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24 +ipv4.gateway
123.123.0.254
```

- 不要禁用 **firewalld**。
- 将主机添加到管理器后，自定义管理门户中的防火墙规则。请参阅配置主机防火墙规则。

4.5. 自托管引擎建议

- 为 Red Hat Virtualization Manager 和其他基础架构级服务创建单独的数据中心和集群（如果环境足以允许它）。虽然管理器虚拟机可以在常规群集的主机上运行，但与生产虚拟机分离有助于备份调度、性能、可用性和安全性。
- 在自托管引擎部署期间创建专用于 Manager 虚拟机的存储域。请勿将此存储域用于任何其他虚拟机。
- 如果您正在预见繁重的存储工作负载，请将迁移、管理和存储网络分隔开，以减少对 Manager 虚拟机的运行状况的影响。
- 虽然每个集群的主机数量在技术上没有硬性限制，但将自托管引擎节点限制为每个集群的 7 个节点。以改进弹性的方式分发服务器，例如在不同机架中。
- 所有自托管引擎节点应具有相等的 CPU 系列，以便 Manager 虚拟机可以在它们之间安全迁移。如果您打算拥有多个系列，请使用最低系列开始安装。
- 如果 Manager 虚拟机关闭或需要迁移，则必须在自托管引擎节点上有足够的内存供 Manager 虚拟机重新启动或迁移到该虚拟机。

附录 A. 法律通知