



Red Hat Virtualization 4.4

使用本地数据库将 Red Hat Virtualization 安装为 独立管理器

在同一服务器上安装 Red Hat Virtualization Manager 及其数据库

Red Hat Virtualization 4.4 使用本地数据库将 Red Hat Virtualization 安装为独立管理器

在同一服务器上安装 Red Hat Virtualization Manager 及其数据库

Red Hat Virtualization Documentation Team

Red Hat Customer Content Services

rhev-docs@redhat.com

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

本文档论述了如何安装单机管理器环境 - 在与管理器相同的机器上安装 Red Hat Virtualization Manager 或另一个环境中的虚拟机上。如果这不是您要使用的配置，请参阅 产品指南 中的其他安装选项。

目录

前言	4
RED HAT VIRTUALIZATION KEY 组件	4
独立管理器架构	4
第 1 章 安装概述	6
第 2 章 要求	7
2.1. RED HAT VIRTUALIZATION MANAGER 要求	7
2.2. 主机要求	8
2.3. 网络要求	12
第 3 章 安装 RED HAT VIRTUALIZATION MANAGER	20
3.1. 准备 RED HAT VIRTUALIZATION MANAGER 机器	20
3.2. 启用 RED HAT VIRTUALIZATION MANAGER 存储库	20
3.3. 安装和配置 RED HAT VIRTUALIZATION MANAGER	22
3.4. 连接到管理门户	27
第 4 章 为 RED HAT VIRTUALIZATION 安装主机	28
4.1. RED HAT VIRTUALIZATION 主机	28
4.2. RED HAT ENTERPRISE LINUX 主机	39
4.3. 配置主机网络的建议做法	41
4.4. 在 RED HAT VIRTUALIZATION MANAGER 中添加标准主机	42
第 5 章 为 RED HAT VIRTUALIZATION 准备存储	44
5.1. 准备 NFS 存储	44
5.2. 准备 ISCSI 存储	45
5.3. 准备 FCP 存储	46
5.4. 准备兼容 POSIX 的文件系统存储	47
5.5. 准备本地存储	47
5.6. 准备 RED HAT GLUSTER STORAGE	48
5.7. 为 SAN 供应商自定义多路径配置	48
5.8. 推荐的 MULTIPATH.CONF 设置	49
第 6 章 为 RED HAT VIRTUALIZATION 添加存储	51
6.1. 添加 NFS 存储	51
6.2. 添加 ISCSI 存储	51
6.3. 添加 FCP 存储	53
6.4. 添加兼容 POSIX 的文件系统存储	54
6.5. 添加本地存储域	55
6.6. 添加 RED HAT GLUSTER STORAGE	56
附录 A. 为 RED HAT VIRTUALIZATION MANAGER 安装配置本地仓库	57
启用 Red Hat Virtualization Manager 存储库	57
配置离线存储库	58
附录 B. 准备本地手动配置 POSTGRESQL 数据库	61
启用 Red Hat Virtualization Manager 存储库	61
初始化 PostgreSQL 数据库	62
附录 C. 为 PCI PASSTHROUGH 配置主机	65
附录 D. 删除独立 RED HAT VIRTUALIZATION MANAGER	67
附录 E. 防止内核模块自动载入	68

E.1. 临时删除模块	69
附录 F. 防止内核模块自动载入	71
F.1. 临时删除模块	72
附录 G. 保护 RED HAT VIRTUALIZATION	74
G.1. 在基于 RHEL 的主机和独立管理器中应用 DISA STIG 配置集	74
G.2. 在 RHV 主机和独立管理器中应用 PCI-DSS 配置集	75
附录 H. 法律通知	76

前言

独立管理器安装是手动的，并可自定义。您必须安装 Red Hat Enterprise Linux 机器，然后运行配置脚本 (**engine-setup**) 并提供有关如何配置 Red Hat Virtualization Manager 的信息。在管理器运行后添加主机和存储。虚拟机高可用性至少需要两个主机。

在本地数据库环境中，管理器数据库和数据仓库数据库可以由管理器配置脚本自动创建。或者，在运行 **engine-setup** 前，您可以在 Manager 机器上手动创建这些数据库。

有关环境选项和推荐配置的信息，请参阅 [规划和前提条件指南](#)。

RED HAT VIRTUALIZATION KEY 组件

组件名称	描述
Red Hat Virtualization Manager	此服务提供图形用户界面和 REST API，用于管理环境中的资源。Manager 安装在运行 Red Hat Enterprise Linux 的物理或虚拟机上。
主机	Red Hat Enterprise Linux 主机 (RHEL 主机) 和 Red Hat Virtualization 主机 (基于镜像的 hypervisor) 是两种受支持的主机类型。主机使用基于内核的虚拟机 (KVM) 技术，并提供用于运行虚拟机的资源。
共享存储	存储服务用于存储与虚拟机关联的数据。
Data Warehouse (数据仓库)	从管理器收集配置信息和统计数据的服务。

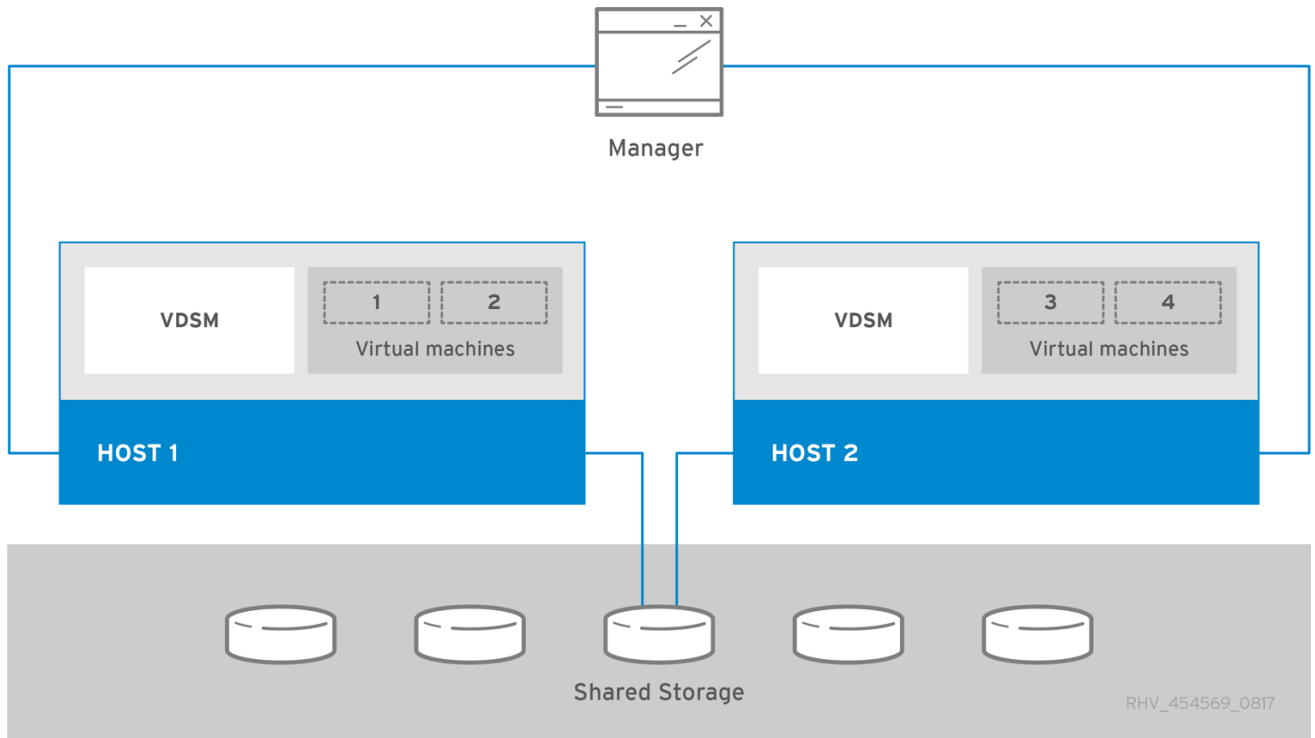
独立管理器架构

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. 独立管理器 Red Hat Virtualization 架构



第 1 章 安装概述

使用本地数据库安装单机管理器环境涉及以下步骤：

1. 安装和配置 Red Hat Virtualization Manager:
 - a. 为管理器安装 Red Hat Enterprise Linux 机器。
 - b. 在 Content Delivery Network 中注册 Manager 机器并启用 Red Hat Virtualization Manager 软件仓库。
 - c. 使用 **engine-setup** 安装并配置 Red Hat Virtualization Manager。
 - d. 连接到管理门户，以添加主机和存储域。
2. 安装主机以运行虚拟机：
 - a. 使用主机类型，或两者：
 - Red Hat Virtualization Host
 - Red Hat Enterprise Linux
 - b. 将主机添加到管理器。
3. 准备要用于存储域的存储。您可以使用以下存储类型之一：
 - NFS
 - iSCSI
 - Fibre Channel (FCP)
 - 兼容 POSIX 的文件系统
 - 本地存储
 - Red Hat Gluster Storage
4. 添加存储域到管理器。



重要

使环境保持最新。如需更多信息，请参阅[如何更新我的 Red Hat Virtualization 系统？](#) 由于常见问题的程序错误修复频繁发布，因此请使用计划中的任务来更新主机和管理器。

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

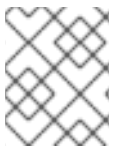
2.1.3. 客户端要求

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 QXLDDOD 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 QXLDDOD 驱动程序。



注意

SPICE 可以使用 QXLDDOD 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 必须安装到 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 仅根据需要在 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` 必须是 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

- 选择 vGPU 类型以及您要通过虚拟机的 **Administration Portal Host Devices** 选项卡中的 **Manage vGPU** 对话框用于此虚拟机的实例数量。
- 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。

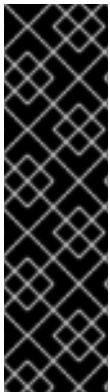
2.3.2. DNS、NTP 和 IPMI 隔离的防火墙要求

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。

2.3.3. 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
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

ID	端口	协议	源	目的地	用途	默认加密
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
M7	54323	TCP	管理门户客户端	Red Hat Virtualization Manager (ovirt-imageio 服务)	与 ovirt-imageio 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。

ID	端口	协议	源	目的地	用途	默认加密
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。

2.3.4. 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
----	----	----	---	-----	----	------

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
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)

ID	端口	协议	源	目的地	用途	默认加密
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
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

ID	端口	协议	源	目的地	用途	默认加密
H11	54322	TCP	Red Hat Virtualization Manager ovirt-imageio 服务	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	与 ovirt-imageio 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
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。

2.3.5. 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。

2.3.6. 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 安装 RED HAT VIRTUALIZATION MANAGER

安装 Red Hat Virtualization Manager 涉及以下步骤：

1. [准备 Red Hat Virtualization Manager 机器](#)
2. [启用 Red Hat Virtualization Manager 存储库](#)
3. [安装和配置 Red Hat Virtualization Manager](#)
4. [连接到管理门户](#)

3.1. 准备 RED HAT VIRTUALIZATION MANAGER 机器

Red Hat Virtualization Manager 必须在 Red Hat Enterprise Linux 8 中运行。有关详情请参考 [执行标准 RHEL 安装](#)。

此机器必须满足最低 [管理器硬件要求](#)。

要在无法访问 Content Delivery Network [的系统中安装 Red Hat Virtualization Manager](#)，请参阅 [配置 Red Hat Virtualization Manager 安装的离线 仓库](#)。

默认情况下，Red Hat Virtualization Manager 的配置脚本 **engine-setup** 会自动创建并配置管理器数据库和数据仓库数据库。要手动设置数据库，或手动设置数据库，请参阅 [配置管理器前准备本地手动配置 PostgreSQL 数据库](#)。

3.2. 启用 RED HAT VIRTUALIZATION MANAGER 存储库

您需要使用 Red Hat Subscription Manager 登录并注册 Manager 机器，附加 **Red Hat Virtualization Manager** 订阅并启用 Manager 存储库。

流程

1. 使用 Content Delivery Network 注册您的系统，在提示时输入您的客户门户网站用户名和密码：

```
# subscription-manager register
```



注意

如果您使用 IPv6 网络，请使用 IPv6 转换机制来访问 Content Delivery Network 和 subscription Manager。

2. 查找 **Red Hat Virtualization Manager** 订阅池并记录池 ID：

```
# subscription-manager list --available
```

3. 使用池 ID 将订阅附加到系统：

```
# subscription-manager attach --pool=pool_id
```




注意

查看当前附加的订阅：

```
# subscription-manager list --consumed
```

列出所有启用的软件仓库：

```
# dnf repolist
```

4. 配置存储库：

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-8-for-x86_64-baseos-eus-rpms \
  --enable=rhel-8-for-x86_64-appstream-eus-rpms \
  --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms \
  --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
  --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
  --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
  --enable=rhel-8-for-x86_64-appstream-tus-rpms \
  --enable=rhel-8-for-x86_64-baseos-tus-rpms
```

5. 将 RHEL 版本设置为 8.6:

```
# subscription-manager release --set=8.6
```

6. 启用 **pki-deps** 模块。

```
# dnf module -y enable pki-deps
```

7. 启用 **postgresql** 模块的版本 12。

```
# dnf module -y enable postgresql:12
```

8. 启用 **nodejs** 模块的版本 14:

```
# dnf module -y enable nodejs:14
```

9. 同步安装的软件包，将它们更新至最新可用版本。

```
# dnf distro-sync --nobest
```

其它资源

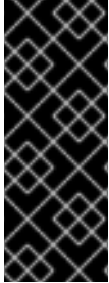
有关模块和模块流的详情，请参考 [安装](#)、[管理](#)和[删除用户空间组件](#)中的以下部分。

- [模块流](#)
- [安装软件包前选择流](#)
- [重置模块流](#)

- [切换到更新的流](#)

3.3. 安装和配置 RED HAT VIRTUALIZATION MANAGER

安装 Red Hat Virtualization Manager 的软件包和依赖项，并使用 **engine-setup** 命令进行配置。该脚本将要求您回答一系列问题，并在提供所有问题所需的值后，应用该配置并启动 **ovirt-engine** 服务。



重要

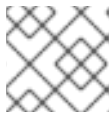
engine-setup 命令指导您完成几个不同的配置阶段，每个阶段需要用户输入的几个步骤。建议的配置默认值在方括号中提供；如果给定步骤接受推荐的值，请按 **Enter** 以接受该值。

您可以运行 **engine-setup --accept-defaults** 来自动接受具有默认答案的所有问题。这个选项时应谨慎使用，只有在您熟悉 **engine-setup** 时才应使用。

流程

1. 请确定所有软件包是最新的：

```
# dnf upgrade --nobest
```



注意

如果任何与内核相关的软件包已更新，请重新启动机器。

2. 安装 **rhvm** 软件包和依赖项。

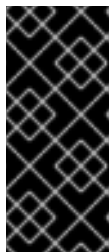
```
# dnf install rhvm
```

3. 运行 **engine-setup** 命令以开始配置 Red Hat Virtualization Manager：

```
# engine-setup
```

4. 可选：输入 **Yes** 并按 **Enter** 在此机器上设置 Cinderlib 集成：

```
Set up Cinderlib integration
(Currently in tech preview)
(Yes, No) [No]:
```



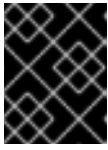
重要

Cinderlib 只是一个技术预览功能。技术预览功能不包括在红帽生产服务级别协议（SLA）中，且其功能可能并不完善。因此，红帽不建议在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。有关红帽技术预览功能支持范围的更多信息，请参阅 [Red Hat 技术预览功能支持范围](#)。

5. 按 **Enter** 键配置这个机器上的 Manager：

```
Configure Engine on this host (Yes, No) [Yes]:
```

6. 可选：安装 Open Virtual Network(OVN)。选择 **Yes** 在 Manager 机器上安装 OVN 服务器，并将其添加到 Red Hat Virtualization 中作为外部网络供应商。此操作还会将 Default 集群配置为使用 OVN 作为其默认网络提供程序。



重要

另外，请参阅 [管理指南](#) 中 [添加 Open Virtual Network\(OVN\) 作为外部网络提供者](#) 中的“下一步”步骤。

Configuring ovirt-provider-ovn also sets the Default cluster's default network provider to ovirt-provider-ovn.

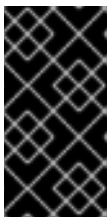
Non-Default clusters may be configured with an OVN after installation.

Configure ovirt-provider-ovn (Yes, No) [Yes]:

有关在 Red Hat Virtualization 中使用 OVN 网络的更多信息，请参阅 [管理指南](#) 中的 [添加开放虚拟网络\(OVN\) 作为外部网络提供程序](#)。

7. 可选：允许 **engine-setup** 配置 WebSocket Proxy 服务器，允许用户通过 **noVNC** 控制台连接到虚拟机：

Configure WebSocket Proxy on this machine? (Yes, No) [Yes]:



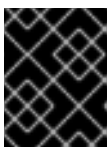
重要

WebSocket 代理和 noVNC 只是一个技术预览功能。技术预览功能不被红帽产品服务级别协议(SLA)支持，且可能无法完成。红帽不建议在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。如需更多信息，请参阅 [红帽技术预览功能支持范围](#)。

8. 选择是否在此机器上配置数据仓库。

Please note: Data Warehouse is required for the engine. If you choose to not configure it on this host, you have to configure it on a remote host, and then configure the engine on this host so that it can access the database of the remote Data Warehouse host.

Configure Data Warehouse on this host (Yes, No) [Yes]:



重要

红帽只支持在彼此相同的机器上安装数据仓库数据库、Data Warehouse 服务和 Grafana。

9. 按 **Enter** 在 Manager 中配置 Grafana：

Configure Grafana on this host (Yes, No) [Yes]:

10. 可选：从命令行访问虚拟机的串行控制台。

Configure VM Console Proxy on this host (Yes, No) [Yes]:

客户端机器上需要其他配置才能使用此功能。请参阅 [虚拟机管理指南](#) 中的 [打开串行控制台到虚拟机](#)。

- 按 **Enter** 接受自动检测到的主机名，或者输入备用主机名，然后按 **Enter** 键。请注意，如果您使用虚拟主机，自动检测的主机名可能不正确。

Host fully qualified DNS name of this server [*autodetected host name*]:

- engine-setup** 命令检查您的防火墙配置，并可以打开 Manager 用于外部通信的端口，如端口 80 和 443。如果您没有允许 **engine-setup** 修改防火墙配置，则必须手动打开由管理器使用的端口。**firewalld** 配置为防火墙管理器。

Setup can automatically configure the firewall on this system.

Note: automatic configuration of the firewall may overwrite current settings.

Do you want Setup to configure the firewall? (Yes, No) [Yes]:

如果您选择自动配置防火墙，且没有防火墙管理器处于活动状态，系统会提示您从支持的选项列表中选择您所选的防火墙管理器。输入防火墙管理器的名称，然后按 **Enter**。即使只列出了一个选项，也是如此。

- 指定是否在此机器上配置数据仓库数据库，或在其它机器上配置：

Where is the DWH database located? (Local, Remote) [Local]:

- 如果您选择 **Local**，则 **engine-setup** 脚本可以自动配置数据库（包括添加用户和数据库）或者它连接到预配置的本地数据库：

Setup can configure the local postgresql server automatically for the DWH to run. This may conflict with existing applications.

Would you like Setup to automatically configure postgresql and create DWH database, or prefer to perform that manually? (Automatic, Manual) [Automatic]:

- 如果您通过按 **Enter** 来选择 **Automatic**，则不需要进一步的操作。
- 如果选择 **Manual**，请为手动配置的本地数据库输入以下值：

DWH database secured connection (Yes, No) [No]:

DWH database name [ovirt_engine_history]:

DWH database user [ovirt_engine_history]:

DWH database password:



注意

engine-setup 在下一步中配置 Manager 数据库后请求这些值。

- 如果您选择 **Remote**（例如，如果您在 Manager 机器上安装 Data Warehouse 服务，但已配置了远程数据仓库数据库），请为远程数据库服务器输入以下值：

DWH database host [localhost]:

DWH database port [5432]:

DWH database secured connection (Yes, No) [No]:

DWH database name [ovirt_engine_history]:

DWH database user [ovirt_engine_history]:

DWH database password:

**注意**

engine-setup 在下一步中配置 Manager 数据库后请求这些值。

- 如果选择 **Remote**，系统会提示您输入 Grafana 数据库用户的用户名和密码：

```
Grafana database user [ovirt_engine_history_grafana]:
Grafana database password:
```

14. 指定是否在此机器上配置 Manager 数据库，还是在另一台机器上：

```
Where is the Engine database located? (Local, Remote) [Local]:
```

- 如果选择 **Local**，**engine-setup** 命令可以自动配置数据库（包括添加用户和数据库）或者它连接到预配置的本地数据库：

```
Setup can configure the local postgresql server automatically for the engine to run. This
may conflict with existing applications.
Would you like Setup to automatically configure postgresql and create Engine database,
or prefer to perform that manually? (Automatic, Manual) [Automatic]:
```

- 如果您通过按 **Enter** 来选择 **Automatic**，则不需要进一步的操作。
- 如果选择 **Manual**，请为手动配置的本地数据库输入以下值：

```
Engine database secured connection (Yes, No) [No]:
Engine database name [engine]:
Engine database user [engine]:
Engine database password:
```

15. 为 Red Hat Virtualization Manager 自动创建的管理员用户设置密码：

```
Engine admin password:
Confirm engine admin password:
```

16. 选择 **Gluster**, **Virt**, 或 **Both**:

```
Application mode (Both, Virt, Gluster) [Both]:
```

- **Both** - 提供最大的灵活性。在大多数情况下，选择 **Both**。
- **virt** - 允许您在环境中运行虚拟机。
- **Gluster** - 只允许从管理门户管理 GlusterFS。

**注意**

GlusterFS 存储已弃用，并将在以后的发行版本中删除。

17. 如果安装了 OVN 供应商，您可以选择使用默认凭证，或者指定替代方案。

Use default credentials (admin@internal) for ovirt-provider-ovn (Yes, No) [Yes]:
 oVirt OVN provider user[admin@internal]:
 oVirt OVN provider password:

18. 为 **wipe_after_delete** 标志设置默认值，它会在删除磁盘时擦除虚拟磁盘的块。

Default SAN wipe after delete (Yes, No) [No]:

19. Manager 使用证书与其主机安全通信。此证书也可以选择用来保护与 Manager 的 HTTPS 通信。为证书提供机构名称：

Organization name for certificate [*autodetected domain-based name*]:

20. (可选) 允许 **engine-setup** 将 Manager 的登录页面设置为 Apache Web 服务器提供的默认页面：

Setup can configure the default page of the web server to present the application home page. This may conflict with existing applications.
 Do you wish to set the application as the default web page of the server? (Yes, No) [Yes]:

21. 默认情况下，与 Manager 进行通信的外部 SSL(HTTPS) 通讯会与配置前面创建的自签名证书进行保护，以安全地与主机通信。或者，为外部 HTTPS 连接选择另一个证书；这不会影响 Manager 与主机通信的方式：

Setup can configure apache to use SSL using a certificate issued from the internal CA.
 Do you wish Setup to configure that, or prefer to perform that manually? (Automatic, Manual) [Automatic]:

22. 您可以为 Grafana admin 用户指定唯一密码，或者使用与 Manager admin 密码相同的密码：

Use Engine admin password as initial Grafana admin password (Yes, No) [Yes]:

23. 选择数据仓库将保留所收集数据的时长：

Please choose Data Warehouse sampling scale:

(1) Basic

(2) Full

(1, 2)[1]:

Full 使用 [Data Warehouse Guide](#) 中列出的数据存储设置的默认值（当远程服务器上安装数据仓库时，发送）。

Basic 会将 **DWH_TABLES_KEEP_HOURLY** 的值减小到 **720**，**DWH_TABLES_KEEP_DAILY** 的值减小到 **0**，从而减轻了 Manager 集群的负载。在同一机器上安装 Manager 和数据仓库时，请使用 **Basic**。

24. 查看安装设置，点 **Enter** 接受值并继续安装：

Please confirm installation settings (OK, Cancel) [OK]:

配置您的环境后，**engine-setup** 会显示有关如何访问您的环境的详细信息。

后续步骤

如果您选择手动配置防火墙，**engine-setup** 提供了一个需要打开的端口的自定义列表，具体取决于设置过程中选择的选项。**engine-setup** 还会将您的回答保存到一个文件，该文件可用于使用相同的值重新配置管理器，并输出 Red Hat Virtualization Manager 配置过程中的日志文件位置。

- 如果要将在 Red Hat Virtualization 环境与目录服务器链接，请将日期和时间配置为与目录服务器使用的系统时钟同步，以避免意外的帐户到期问题。如需更多信息，请参阅 [Red Hat Enterprise Linux 系统管理员指南](#) 中的 [使用远程服务器同步系统时钟](#)。
- 根据浏览器提供的说明安装证书颁发机构。您可以导航到 <http://<manager-fqdn>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>，将 <manager-fqdn> 替换为安装过程中提供的 FQDN。

登录到管理门户，您可以在其中添加主机和存储到环境中：

3.4. 连接到管理门户

使用 Web 浏览器访问管理门户。

1. 在 Web 浏览器中，导航到 <https://manager-fqdn/ovirt-engine>，将 *manager-fqdn* 替换为您在安装过程中提供的 FQDN。



注意

您可以使用备用主机名或 IP 地址访问管理门户。为此，您需要在 `/etc/ovirt-engine/engine.conf.d/` 下添加一个配置文件。例如：

```
# vi /etc/ovirt-engine/engine.conf.d/99-custom-ssso-setup.conf
SSO_ALTERNATE_ENGINE_FQDNS="alias1.example.com
alias2.example.com"
```

备用主机名列表需要用空格分开。您还可以将 Manager 的 IP 地址添加到列表中，但不建议使用 IP 地址而不是 DNS 可解析的主机名。

2. 单击 **Administration Portal**。将显示 SSO 登录页面。通过 SSO 登录，您可以同时登录管理和虚拟机门户。
3. 输入您的**用户名和密码**。如果您是第一次登录，请使用用户名 **admin** 以及安装期间指定的密码。
4. 选择要对其进行身份验证的**域**。如果使用内部 **admin** 用户名进行登录，请选择 **internal** 域。
5. 点 **Log In**。
6. 您可以使用多种语言查看管理门户。默认选择会根据 Web 浏览器的区域设置进行选择。如果要使用非默认语言查看管理门户，请从欢迎页面的下拉列表中选择您首选的语言。

要从 Red Hat Virtualization 管理门户注销，请单击标题栏中的用户名并单击 **Sign Out**。您已注销所有门户，并显示 Manager 欢迎屏幕。

第 4 章 为 RED HAT VIRTUALIZATION 安装主机

Red Hat Virtualization 支持两种类型的主机：[Red Hat Virtualization Hosts\(RHVH\)](#) 和 [Red Hat Enterprise Linux 主机](#)。根据您的环境，您可能只使用一种类型，或两者都使用。迁移和高可用性功能至少需要两个主机。

有关为网络信息 [配置主机网络](#)，请参阅 [推荐的实践](#)。



重要

安装时 SELinux 处于 enforcing 模式。要进行验证，请运行 **getenforce**。SELinux 必须在所有主机和管理器上处于 enforcing 模式，才能支持您的 Red Hat Virtualization 环境。

表 4.1. 主机类型

主机类型	其他名称	描述
Red Hat Virtualization Host	RHVH，一个精简的主机	这是基于 Red Hat Enterprise Linux 的最小操作系统。它作为 ISO 文件从客户门户分发，仅包含计算机充当主机所需的软件包。
Red Hat Enterprise Linux 主机	RHEL 主机，一个完全的主机	附加了适当订阅的 Red Hat Enterprise Linux 系统可用作主机。

主机兼容性

创建新数据中心时，您可以设置兼容性版本。选择适合数据中心所有主机的兼容性版本。设置之后，不允许版本回归。对于全新的 Red Hat Virtualization 安装，在默认数据中心和默认集群中设置了最新的兼容性版本；要使用较早的兼容性版本，您必须创建额外的数据中心和集群。有关兼容性版本的更多信息，请参阅 [Red Hat Virtualization 生命周期](#) 中的 [Red Hat Virtualization Manager 兼容性](#)。

4.1. RED HAT VIRTUALIZATION 主机

4.1.1. 安装 Red Hat Virtualization 主机

Red Hat Virtualization Host (RHVH) 是一个基于 Red Hat Enterprise Linux 的最小操作系统，旨在提供一种简单的方法来设置物理机以充当 Red Hat Virtualization 的 hypervisor。最小操作系统仅包含计算机充当虚拟机监控程序所需的软件包，并提供 Cockpit Web 界面来监控主机和执行管理任务。有关最低浏览器要求，请参阅 [运行 Cockpit](#)。

RHVH 支持 NIST 800-53 分区要求以提高安全性。RHVH 默认使用 NIST 800-53 分区布局。

主机必须满足[最低主机要求](#)。



警告

安装或重新安装主机的操作系统时，红帽强烈建议您先分离附加到主机的任何现有非 OS 存储，以避免意外初始化这些磁盘，从而避免意外初始化这些磁盘，并可能会丢失数据。

流程

1. 请访问红帽客户门户上的 [Red Hat Virtualization 入门](#) 并登录。
2. 单击 **Download Latest** 以访问产品下载页面。
3. 从列表中选择适当的 **Hypervisor Image for RHV**，然后单击 **Download Now**。
4. 启动您要安装 RHVH 的机器，从准备的安装介质启动。
5. 在引导菜单中选择 **Install RHVH 4.4** 并按 **Enter**。



注意

您还可以按 **Tab** 键编辑内核参数。内核参数必须以空格分开，您可以通过按 **Enter** 键使用指定的内核参数引导系统。按 **Esc** 键清除对内核参数的任何更改并返回到引导菜单。

6. 选择语言，点 **Continue**。
7. 从键盘布局屏幕中选择 **键盘布局**，然后点 **Done**。
8. 从 **Installation Destination** 屏幕中选择要在其上安装 RHV 的设备。（可选）启用加密。点 **Done**。



重要

使用 **Automatically configure partitioning** 选项。

9. 从 **Time & Date** 屏幕中选择一个时区，然后点 **Done**。
10. 从 **Network & Host Name** 屏幕选择一个网络，然后单击 **Configure...** 来配置连接详情。



注意

要在系统每次启动时使用连接，请选择 **Connect automatically with priority** 复选框。如需更多信息，请参阅 *Red Hat Enterprise Linux 8 安装指南* 中的 [配置网络和主机名选项](#)。

在 **Host Name** 字段中输入主机名，然后单击 **Done**。

11. 可选：**配置安全策略和 Kdump**。有关安装 **概述** 屏幕中的每个部分的更多信息，请参阅 [为 Red Hat Enterprise Linux 8 执行标准 RHEL 安装中的 GUI 定制您的 RHEL 安装](#)。

- 点 **Begin Installation**。
- 设置 **root** 密码，并选择性地为 RHVH 安装时创建额外的用户。



警告

不要在 RHVH 上创建不受信任的用户，因为这可能导致利用本地安全漏洞。

- 单击 **Reboot** 以完成安装。



注意

当 RHVH 重新启动时，**nodectl check** 会在主机上执行健康检查，并在您在命令行中登录时显示结果。消息 **node status: OK** 或 **node status: DEGRADED** 代表了健康状态。运行 **nodectl check** 以了解更多信息。



注意

如有必要，您可以[防止内核模块自动载入](#)。

4.1.2. 启用 Red Hat Virtualization 主机存储库

注册系统以接收更新。Red Hat Virtualization Host 只需要一个软件仓库。本节提供有关将 RHVH 注册到[内容交付网络](#)或[Red Hat Satellite 6](#)的说明。

将 RHVH 注册到内容交付网络

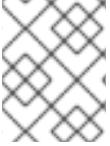
- 启用 **Red Hat Virtualization Host 8** 存储库，以便以后更新 Red Hat Virtualization 主机：

```
# subscription-manager repos --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

将 RHVH 注册到 Red Hat Satellite 6

- 登录位于 **https://HostFQDNorIP:9090** 的 Cockpit Web 界面。
- 点 **Terminal**。
- 使用 Red Hat Satellite 6 注册 RHVH:

```
# rpm -Uvh http://satellite.example.com/pub/katello-ca-consumer-latest.noarch.rpm
# subscription-manager register --org="org_id"
# subscription-manager list --available
# subscription-manager attach --pool=pool_id
# subscription-manager repos \
  --disable='*' \
  --enable=rhvh-4-for-rhel-8-x86_64-rpms
```



注意

您还可以使用 `virt-who` 在 Red Hat Satellite 中配置虚拟机订阅。请参阅[使用 virt-who 管理基于主机的订阅](#)。

4.1.3. 高级安装

4.1.3.1. 自定义分区

不建议在 Red Hat Virtualization Host (RHVH) 上自定义分区。在 **Installation Destination** 窗口中使用 **Automatically configure partitioning** 选项。

如果您的安装需要自定义分区，在安装过程中选择 **I will configure partitioning** 选项，请注意这有以下限制：

- 确定在 **Manual Partitioning** 窗口中选择了默认 **LVM Thin Provisioning** 选项。
- 以下目录是必需的，且必须在精简置备的逻辑卷中：
 - `root (/)`
 - `/home`
 - `/tmp`
 - `/var`
 - `/var/crash`
 - `/var/log`
 - `/var/log/audit`



重要

不要为 `/usr` 创建单独的分区。这样做将导致安装失败。

`/usr` 必须位于可以更改版本与 RHVH 的逻辑卷中，因此应保留在 `root (/)` 上。

有关每个分区所需的 [存储大小的详情](#)，请参考[存储要求](#)。

- `/boot` 目录应定义为标准分区。
- `/var` 目录必须位于单独的卷或磁盘中。
- 仅支持 XFS 或 Ext4 文件系统。

在 Kickstart 文件中配置手动分区

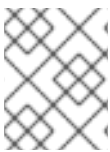
以下示例演示了如何在 Kickstart 文件中配置手动分区。

```
clearpart --all
part /boot --fstype xfs --size=1000 --ondisk=sda
part pv.01 --size=42000 --grow
volgroup HostVG pv.01 --reserved-percent=20
logvol swap --vgname=HostVG --name=swap --fstype=swap --recommended
```

```

logvol none --vgname=HostVG --name=HostPool --thinpool --size=40000 --grow
logvol / --vgname=HostVG --name=root --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=6000 --grow
logvol /var --vgname=HostVG --name=var --thin --fstype=ext4 --poolname=HostPool
--fsoptions="defaults,discard" --size=15000
logvol /var/crash --vgname=HostVG --name=var_crash --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=10000
logvol /var/log --vgname=HostVG --name=var_log --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=8000
logvol /var/log/audit --vgname=HostVG --name=var_audit --thin --fstype=ext4 --poolname=HostPool -
-fsoptions="defaults,discard" --size=2000
logvol /home --vgname=HostVG --name=home --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=1000
logvol /tmp --vgname=HostVG --name=tmp --thin --fstype=ext4 --poolname=HostPool --
fsoptions="defaults,discard" --size=1000

```



注意

如果使用 **logvol --thinpool --grow**，还必须包含 **volgroup --reserved-space** 或 **volgroup --reserved-percent**，以在卷组中保留空间，以便精简池增长。

4.1.3.2. 在没有安装程序支持的主机上安装 DUD 驱动程序

安装 Red Hat Virtualization Host(RHVM)有时需要一个 Driver Update Disk(DUD)，比如使用 RHVM 默认配置不支持的硬件 RAID 设备。与 Red Hat Enterprise Linux 主机相比，RHVM 并不完全支持使用 DUD。因此，主机在安装后无法正常引导，因为它没有看到 RAID。相反，它引导进入紧急模式。

输出示例：

```

Warning: /dev/test/rhvh-4.4-20210202.0+1 does not exist
Warning: /dev/test/swap does not exist
Entering emergency mode. Exit the shell to continue.

```

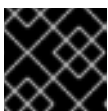
在这种情况下，您可以在完成安装前手动添加驱动程序。

先决条件

- 您要在其上安装 RHVM 的计算机。
- 一个 DUD。
- 如果您将 USB 驱动器用于 DUD 和 RHVM，则必须至少有两个可用的 USB 端口。

流程

1. 在主机上加载 DUD。
2. 安装 RHVM。请参阅 [使用命令行将 Red Hat Virtualization 安装为自托管引擎中的安装 Red Hat Virtualization 主机](#)。



重要

安装完成后，请勿重启系统。

提示

如果要使用 SSH 访问 DUD，请执行以下操作：

- 在内核命令行中添加字符串 **inst.sshd**：

```
<kernel_command_line> inst.sshd
```

- 在安装过程中启用网络。

3. 按 **Ctrl + Alt + F3** 进入控制台模式。或者，您也可以使用 SSH 连接到它。

4. 挂载 DUD：

```
# mkdir /mnt/dud
# mount -r /dev/<dud_device> /mnt/dud
```

5. 将 DUD 中的 RPM 文件复制到目标机器的磁盘中：

```
# cp /mnt/dud/rpms/<path>/<rpm_file>.rpm /mnt/sysroot/root/
```

例如：

```
# cp /mnt/dud/rpms/x86_64/kmod-3w-9xxx-2.26.02.014-5.el8_3.elrepo.x86_64.rpm
/mnt/sysroot/root/
```

6. 将根目录改为 **/mnt/sysroot**：

```
# chroot /mnt/sysroot
```

7. 备份当前的 initrd 镜像。例如：

```
# cp -p /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img /boot/initramfs-4.18.0-
240.15.1.el8_3.x86_64.img.bck1
# cp -p /boot/rhvh-4.4.5.1-0.20210323.0+1/initramfs-4.18.0-240.15.1.el8_3.x86_64.img
/boot/rhvh-4.4.5.1-0.20210323.0+1/initramfs-4.18.0-240.15.1.el8_3.x86_64.img.bck1
```

8. 从您之前创建的副本中为驱动程序安装 RPM 文件。

例如：

```
# dnf install /root/kmod-3w-9xxx-2.26.02.014-5.el8_3.elrepo.x86_64.rpm
```



注意

在重新引导安装环境后，此软件包在系统中不可见。因此，如果您需要它才能重新构建 **initramfs**，您需要再次安装该软件包，之后该软件包仍会保留。

如果使用 **dnf** 更新主机，驱动程序更新会保留，因此您不需要重复此过程。

提示

如果您没有互联网连接，请使用 **rpm** 命令而不是 **dnf**：

```
# rpm -ivh /root/kmod-3w-9xxx-2.26.02.014-5.el8_3.elrepo.x86_64.rpm
```

9. 创建新镜像，强制添加驱动程序：

```
# dracut --force --add-drivers <module_name> --kver <kernel_version>
```

例如：

```
# dracut --force --add-drivers 3w-9xxx --kver 4.18.0-240.15.1.el8_3.x86_64
```

10. 检查结果。新镜像应该更大，并且包含驱动程序。例如，比较原始备份镜像文件的大小和新镜像文件的大小。

在本例中，新镜像文件是 88739013 字节，大于原始 88717417 字节：

```
# ls -ltr /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img*
-rw-----. 1 root root 88717417 Jun  2 14:29 /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img.bck1
-rw-----. 1 root root 88739013 Jun  2 17:47 /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img
```

新驱动程序应该是镜像文件的一部分。例如，应包含 3w-9xxx 模块：

```
# lsinitrd /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img | grep 3w-9xxx
drwxr-xr-x  2 root  root      0 Feb 22 15:57 usr/lib/modules/4.18.0-240.15.1.el8_3.x86_64/weak-updates/3w-9xxx
lrwxrwxrwx  1 root  root      55 Feb 22 15:57 usr/lib/modules/4.18.0-240.15.1.el8_3.x86_64/weak-updates/3w-9xxx/3w-9xxx.ko-../../4.18.0-240.el8.x86_64/extra/3w-9xxx/3w-9xxx.ko
drwxr-xr-x  2 root  root      0 Feb 22 15:57 usr/lib/modules/4.18.0-240.el8.x86_64/extra/3w-9xxx
-rw-r--r--  1 root  root    80121 Nov 10 2020 usr/lib/modules/4.18.0-240.el8.x86_64/extra/3w-9xxx/3w-9xxx.ko
```

11. 将镜像复制到 **/boot** 下的目录中，其中包含正在安装的层中使用的内核，例如：

```
# cp -p /boot/initramfs-4.18.0-240.15.1.el8_3.x86_64.img /boot/rhvh-4.4.5.1-0.20210323.0+1/initramfs-4.18.0-240.15.1.el8_3.x86_64.img
```

12. 退出 **chroot**。
13. 退出 **shell**。
14. 如果您使用 **Ctrl + Alt + F3** 访问虚拟终端，则请按 **Ctrl + Alt + F_<n>**，通常为 **F1** 或 **F5** 来返回到安装程序。
15. 在安装程序屏幕中，重新启动。

验证

计算机应成功重新引导。

4.1.3.3. 自动执行 Red Hat Virtualization Host 部署

您可以在没有物理介质设备的情况下安装 Red Hat Virtualization Host (RHVH)，方法是使用包含安装问题的答案的 Kickstart 文件通过网络从 PXE 服务器引导。



警告

安装或重新安装主机的操作系统时，红帽强烈建议您先分离附加到主机的任何现有非 OS 存储，以避免意外初始化这些磁盘，从而避免意外初始化这些磁盘，并可能会丢失数据。

[Red Hat Enterprise Linux 安装指南](#) 中提供了使用 Kickstart 文件从 PXE 服务器安装的一般说明，因为 RHVH 的安装方式与 Red Hat Enterprise Linux 非常相似。下面介绍了 RHVH 的特定说明，以及使用 Red Hat Satellite 部署 RHVH 的示例。

自动化 RHVH 部署有 3 个阶段：

- [准备安装环境](#)
- [配置 PXE 服务器和 Boot Loader](#)
- [创建并运行 Kickstart 文件](#)

4.1.3.3.1. 准备安装环境

1. 请访问红帽客户门户上的 [Red Hat Virtualization 入门](#) 并登录。
2. 单击 **Download Latest** 以访问产品下载页面。
3. 从列表中选择适当的 **Hypervisor Image for RHV**，然后单击 **Download Now**。
4. 通过网络提供 RHVH ISO 镜像。请参阅 [Red Hat Enterprise Linux 安装指南](#) 中的 [网络安装源](#)。
5. 从 RHVH ISO 中提取 `squashfs.img` 虚拟机监控程序镜像文件：

```
# mount -o loop /path/to/RHVH-ISO/mnt/rvh
# cp /mnt/rvh/Packages/redhat-virtualization-host-image-update* /tmp
# cd /tmp
# rpm2cpio redhat-virtualization-host-image-update* | cpio -idmv
```



注意

此 `squashfs.img` 文件位于 `/tmp/usr/share/redhat-virtualization-host/image/` 目录中，名为 `redhat-virtualization-host-version_number_version.squashfs.img`。它包含用于在物理机上安装的虚拟机监控程序镜像。它不应与 `/LiveOS/squashfs.img` 文件（由 Anaconda `inst.stage2` 选项使用）混淆。

4.1.3.3.2. 配置 PXE 服务器和引导装载程序

1. 配置 PXE 服务器。请参阅 *Red Hat Enterprise Linux 安装指南* 中的 [准备网络安装](#)。
2. 将 RHVH 引导镜像复制到 `/tftpboot` 目录中：

```
# cp mnt/rhvh/images/pxeboot/{vmlinuz,initrd.img} /var/lib/tftpboot/pxelinux/
```

3. 创建一个 `rhvh` 标签，在引导装载程序配置中指定 RHVH 引导镜像：

```
LABEL rhvh
MENU LABEL Install Red Hat Virtualization Host
KERNEL /var/lib/tftpboot/pxelinux/vmlinuz
APPEND initrd=/var/lib/tftpboot/pxelinux/initrd.img inst.stage2=URL/to/RHVH-ISO
```

Red Hat Satellite 的 RHVH 引导装载程序配置示例

如果您使用 Red Hat Satellite 中的信息来置备主机，您必须创建一个名为 `rhvh_image` 的全局或主机组级别参数，并使用挂载或提取 ISO 的目录 URL 填充它：

```
<%=#
kind: PXELinux
name: RHVH PXELinux
%>
# Created for booting new hosts
#

DEFAULT rhvh

LABEL rhvh
KERNEL <%= @kernel %>
APPEND initrd=<%= @initrd %> inst.ks=<%= foreman_url("provision") %> inst.stage2=<%=
@host.params["rhvh_image"] %> intel_iommu=on console=tty0 console=ttyS1,115200n8
ssh_pwauth=1 local_boot_trigger=<%= foreman_url("built") %>
IPAPPEND 2
```

4. 使 RHVH ISO 的内容在本地可用，并使用 HTTPD 服务器将其导出到网络中：

```
# cp -a /mnt/rhvh/ /var/www/html/rhvh-install
# curl URL/to/RHVH-ISO/rhvh-install
```

4.1.3.3.3. 创建并运行 Kickstart 文件

1. 创建 Kickstart 文件，并使其可通过网络使用。请参阅 *Red Hat Enterprise Linux 安装指南* 中的 [Kickstart 安装](#)。
2. 确保 Kickstart 文件满足以下 RHV 特定要求：
 - RHVH 不需要 `%packages` 部分。使用 `liveimg` 选项并指定 RHVH ISO 镜像中的 `redhat-virtualization-host-version_number_version.squashfs.img` 文件：

```
liveimg --url=example.com/tmp/usr/share/redhat-virtualization-host/image/redhat-
virtualization-host-version_number_version.squashfs.img
```


- 强烈建议自动分区，但请谨慎操作：确保首先检测到本地磁盘，包含 **ignoredisk** 命令，并指定要忽略的本地磁盘，如 **sda**。为确保使用特定的驱动器，红帽建议使用 **ignoredisk --only-use=/dev/disk/<path>** 或 **ignoredisk --only-use=/dev/disk/<ID>**：

```
autopart --type=thinp
ignoredisk --only-use=sda
ignoredisk --only-use=/dev/disk/<path>
ignoredisk --only-use=/dev/disk/<ID>
```



注意

自动分区需要精简配置。

--no-home 选项无法在 RHVH 中工作，因为 **/home** 是一个必需的目录。

如果您的安装需要手动分区，请参阅 [Custom Partitioning](#) 以了解适用于分区的限制列表，并在 Kickstart 文件中手动分区示例。

- 需要一个调用 **nodedctl init** 命令的 **%post** 部分：

```
%post
nodedctl init
%end
```



注意

确保 **nodedctl init** 命令位于 **%post** 部分的结尾，但如果存在，则在重新引导代码之前。

自行部署 RHVH 的 Kickstart 示例

此 Kickstart 示例演示了如何部署 RHVH。您可以根据需要包含其他命令和选项。



警告

本例假定所有磁盘均为空，可以初始化。如果您使用数据附加了磁盘，请将其删除或添加到 **ignoredisks** 属性中。

```
liveimg --url=http://FQDN/tmp/usr/share/redhat-virtualization-host/image/redhat-
virtualization-host-version_number_version.squashfs.img
clearpart --all
autopart --type=thinp
rootpw --plaintext ovirt
timezone --utc America/Phoenix
zerombr
text

reboot
```

```
%post --erroronfail
nodedctl init
%end
```

Kickstart 示例，部署来自 Satellite 的注册和网络配置的 RHVH。

此 Kickstart 示例使用 Red Hat Satellite 中的信息来配置主机网络，并将主机注册到 Satellite 服务器。您必须创建一个名为 **rhvh_image** 的全局或主机组级别参数，并为它填充 **squashfs.img** 文件的目录 URL。**ntp_server1** 也是全局或主机组级别变量。



警告

本例假定所有磁盘均为空，可以初始化。如果您使用数据附加了磁盘，请将其删除或添加到 **ignoredisks** 属性中。

```
<%#
kind: provision
name: RHVH Kickstart default
oses:
- RHVH
%>
install
liveimg --url=<%= @host.params['rhvh_image'] %>squashfs.img

network --bootproto static --ip=<%= @host.ip %> --netmask=<%= @host.subnet.mask
%> --gateway=<%= @host.subnet.gateway %> --nameserver=<%=
@host.subnet.dns_primary %> --hostname <%= @host.name %>

zerombr
clearpart --all
autopart --type=thinp

rootpw --iscrypted <%= root_pass %>

# installation answers
lang en_US.UTF-8
timezone <%= @host.params['time-zone'] || 'UTC' %>
keyboard us
firewall --service=ssh
services --enabled=sshd

text
reboot

%post --log=/root/ks.post.log --erroronfail
nodedctl init
<%= snippet 'subscription_manager_registration' %>
<%= snippet 'kickstart_networking_setup' %>
/usr/sbin/ntpdate -sub <%= @host.params['ntp_server1'] || '0.fedora.pool.ntp.org' %>
/usr/sbin/hwclock --systohc
```

```
/usr/bin/curl <%= foreman_url('built') %>
```

```
sync
systemctl reboot
%end
```

3. 将 Kickstart 文件位置添加到 PXE 服务器的引导装载程序配置文件中：

```
APPEND initrd=/var/ftptboot/pxelinux/initrd.img inst.stage2=URL/to/RHVH-ISO
inst.ks=URL/to/RHVH-ks.cfg
```

4. 按照 *Red Hat Enterprise Linux 安装指南* 中的[使用 PXE 从网络引导](#)中的内容，安装 RHVH。

4.2. RED HAT ENTERPRISE LINUX 主机

4.2.1. 安装 Red Hat Enterprise Linux 主机

Red Hat Enterprise Linux 主机基于在物理服务器中的 Red Hat Enterprise Linux 8 的标准基本安装，并附加 **Red Hat Enterprise Linux Server** 和 **Red Hat Virtualization** 订阅。

有关详细的安装说明，请参阅[执行标准 RHEL 安装](#)。

主机必须满足[最低主机要求](#)。



警告

安装或重新安装主机的操作系统时，红帽强烈建议您先分离附加到主机的任何现有非 OS 存储，以避免意外初始化这些磁盘，从而避免意外初始化这些磁盘，并可能会丢失数据。



重要

虚拟化必须在主机的 BIOS 设置中启用。有关更改主机的 BIOS 设置的详情，请参考主机的硬件文档。



重要

不要在 Red Hat Enterprise Linux 主机上安装第三方 watchdog 系统。它们可能会干扰 VDSM 提供的 watchdog 守护进程。

4.2.2. 启用 Red Hat Enterprise Linux 主机存储库

要使用 Red Hat Enterprise Linux 机器作为主机，需要为主机注册 Content Delivery Network，附加 **Red Hat Enterprise Linux Server** 和 **Red Hat Virtualization** 订阅，并启用主机仓库。

流程

1. 使用 Content Delivery Network 注册您的系统，在提示时输入您的客户门户网站用户名和密码：

-

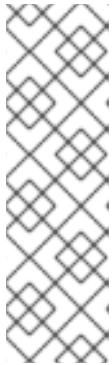
```
# subscription-manager register
```

2. 查找 **Red Hat Enterprise Linux Server** 和 **Red Hat Virtualization** 订阅池，并记录池 ID：

```
# subscription-manager list --available
```

3. 使用池 ID 将订阅附加到系统：

```
# subscription-manager attach --pool=poolid
```



注意

查看当前附加的订阅：

```
# subscription-manager list --consumed
```

列出所有启用的软件仓库：

```
# dnf repolist
```

4. 配置存储库：

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-8-for-x86_64-baseos-eus-rpms \
  --enable=rhel-8-for-x86_64-appstream-eus-rpms \
  --enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms \
  --enable=advanced-virt-for-rhel-8-x86_64-rpms \
  --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
  --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
  --enable=rhel-8-for-x86_64-appstream-tus-rpms \
  --enable=rhel-8-for-x86_64-baseos-tus-rpms
```

对于 Red Hat Enterprise Linux 8 主机、little endian、IBM POWER8 或 IBM POWER9 硬件：

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhv-4-mgmt-agent-for-rhel-8-ppc64le-rpms \
  --enable=rhv-4-tools-for-rhel-8-ppc64le-rpms \
  --enable=advanced-virt-for-rhel-8-ppc64le-rpms \
  --enable=rhel-8-for-ppc64le-appstream-rpms \
  --enable=rhel-8-for-ppc64le-baseos-rpms \
  --enable=fast-datapath-for-rhel-8-ppc64le-rpms \
```

5. 将 RHEL 版本设置为 8.6:

```
# subscription-manager release --set=8.6
```

6. 确保当前安装的所有软件包都为最新版本：

```
# dnf upgrade --nobest
```

7. 重启机器。



注意

如有必要，您可以[防止内核模块自动载入](#)。

4.2.3. 在 Red Hat Enterprise Linux 主机上安装 Cockpit

您可以安装 Cockpit 来监控主机的资源并执行管理任务。

流程

1. 安装仪表盘软件包：

```
# dnf install cockpit-ovirt-dashboard
```

2. 启用并启动 **cockpit.socket** 服务：

```
# systemctl enable cockpit.socket
# systemctl start cockpit.socket
```

3. 检查 Cockpit 是否在防火墙中是活跃的服务：

```
# firewall-cmd --list-services
```

您应看到 **Cockpit** 列出。如果没有，使用 root 权限输入以下内容，将 **cockpit** 添加为服务到防火墙：

```
# firewall-cmd --permanent --add-service=cockpit
```

使用 **--permanent** 选项可在重新启动后保持 **cockpit** 服务处于活动状态。

您可以在 <https://HostFQDNorIP:9090> 上登录到 Cockpit Web 界面。

4.3. 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：***bondnumber*** (for example, ***bond0***, ***bond1***)
 - 绑定接口上的 VLAN：***bondnumber.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）：

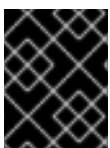
```
# nmcli connection add type vlan con-name vlan50 ifname eth0.50 dev eth0 id 50
# nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24 +ipv4.gateway 123.123.0.254
```

- 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](#)。

4.4. 在 RED HAT VIRTUALIZATION MANAGER 中添加标准主机




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 \(nmstate\)](#)。

在您的 Red Hat Virtualization 环境中添加主机可能需要一些时间，因为平台将完成下列步骤：虚拟化检查、软件包安装和创建网桥。

流程

1. 在管理门户中，单击 **Compute** → **Hosts**。
2. 点 **New**。
3. 使用下拉列表为新主机选择 **Data Center** 和 **Host Cluster**。
4. 输入新主机的**名称和地址**。标准 SSH 端口（端口 22）在 **SSH Port** 字段中自动填充。
5. 选择用于管理器以访问主机的身份验证方法。
 - 输入 root 用户的密码以使用密码身份验证。
 - 或者，将 **SSH PublicKey** 字段中显示的密钥复制到主机上的 `/root/.ssh/authorized_keys` 以使用公钥身份验证。
6. （可选）点 **Advanced Parameters** 按钮更改以下高级主机设置：
 - 禁用自动防火墙配置。
 - 添加主机 SSH 指纹以提高安全性。您可以手动添加，或自动获取。
7. （可选）配置电源管理，其中主机有一个受支持的电源管理卡。有关电源管理配置的详情，请参阅 [管理指南中的主机电源管理设置说明](#)。
8. 点击 **确定**。

新主机显示在主机列表中，状态为 **Installing**，您可以在 **通知 Drawer** 的 **Events** 部分查看安装进度()。在短暂延迟主机状态变为 **Up** 后。

第 5 章 为 RED HAT VIRTUALIZATION 准备存储

您需要准备要用于新环境中的存储域的存储。Red Hat Virtualization 环境必须至少有一个数据存储域，但建议添加更多存储域。



警告

安装或重新安装主机的操作系统时，红帽强烈建议您先分离附加到主机的任何现有非 OS 存储，以避免意外初始化这些磁盘，从而避免意外初始化这些磁盘，并可能会丢失数据。

数据域保管数据中心中所有虚拟机和模板的虚拟硬盘和 OVF 文件，并且在激活的情况下无法在数据中心间共享（但可以在数据中心之间迁移）。多个存储类型的数据域可以添加到同一数据中心，只要它们都是共享的，而不是本地域。

您可以使用以下存储类型之一：

- [NFS](#)
- [iSCSI](#)
- [Fibre Channel \(FCP\)](#)
- [兼容 POSIX 的文件系统](#)
- [本地存储](#)
- [Red Hat Gluster Storage](#)

5.1. 准备 NFS 存储

在您的文件存储或远程服务器上设置 NFS 共享，以充当 Red Hat Enterprise Virtualization 主机系统上的存储域。在远程存储上导出共享并在 Red Hat Virtualization Manager 中配置共享后，将在 Red Hat Virtualization 主机上自动导入共享。

有关设置、配置、挂载和导出 NFS 的详情，请参考为 Red Hat Enterprise Linux 8 [管理文件系统](#)。

Red Hat Virtualization 需要特定的系统用户帐户和系统用户组，以便管理器可以将数据存储在与导出的目录表示的存储域中。以下流程为一个目录设置权限。您必须为 Red Hat Virtualization 中用作存储域的所有目录重复 **chown** 和 **chmod** 步骤。

先决条件

1. 安装 NFS **utils** 软件包。

```
# dnf install nfs-utils -y
```

2. 检查启用的版本：

```
# cat /proc/fs/nfsd/versions
```


3. 启用以下服务：

```
# systemctl enable nfs-server
# systemctl enable rpcbind
```

流程

1. 创建组 **kvm**：

```
# groupadd kvm -g 36
```

2. 在组 **kvm** 中创建用户 **vdsmd**：

```
# useradd vdsmd -u 36 -g kvm
```

3. 创建 **storage** 目录并修改访问权限。

```
# mkdir /storage
# chmod 0755 /storage
# chown 36:36 /storage/
```

4. 将 **storage** 目录添加到具有相关权限的 **/etc/exports** 中。

```
# vi /etc/exports
# cat /etc/exports
/storage *(rw)
```

5. 重启以下服务：

```
# systemctl restart rpcbind
# systemctl restart nfs-server
```

6. 查看哪个导出可用于特定 IP 地址：

```
# exportfs
/nfs_server/srv
    10.46.11.3/24
/nfs_server    <world>
```



注意

如果在启动服务后 **/etc/exports** 中进行了更改，则可以使用 **exportfs -ra** 命令重新加载更改。执行上述所有阶段后，导出目录应已就绪，并可在其他主机上进行测试，以检查其是否可用。

5.2. 准备 iSCSI 存储

Red Hat Virtualization 支持 iSCSI 存储，这是从由 LUN 组成的卷组创建的存储域。卷组和 LUN 一次不能附加到多个存储域。

有关设置和配置 iSCSI 存储的详情，请参考为 Red Hat Enterprise Linux 8 [管理存储设备](#) 中的 [配置 iSCSI 目标](#)。



重要

如果您使用的是块存储，并且打算在裸设备上部署虚拟机或直接 LUN 并用逻辑卷管理器 (LVM) 管理它们，您必须创建一个过滤器来隐藏 guest 逻辑卷。这将防止在主机引导时激活 guest 逻辑卷，这种情况可能会导致逻辑卷过时并导致数据崩溃。使用 **vdsm-tool config-lvm-filter** 命令创建 LVM 的过滤器。请参阅 [创建 LVM 过滤器](#)



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。



重要

如果您的主机从 SAN 存储引导并丢失与存储的连接，则存储文件系统将变为只读并在恢复连接后保持此状态。

要防止这种情况，请在 SAN 的根文件系统中为引导 LUN 添加下拉多路径配置文件以确保它在连接时已在队列中：

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
  multipath {
    wwid boot_LUN_wwid
    no_path_retry queue
  }
}
```

5.3. 准备 FCP 存储

Red Hat Virtualization 通过从由预先存在的 LUN 的卷组创建存储域来支持 SAN 存储。卷组和 LUN 不可同时附加到多个存储域。

Red Hat Virtualization 系统管理员需要对存储区域网络 (SAN) 概念有较好的了解。SAN 通常使用光纤通道协议 (FCP) 作为主机和共享外部存储之间的通信。因此，SAN 有时可能会被称为 FCP 存储。

有关在 Red Hat Enterprise Linux 上设置和配置 FCP 或多路径的详情，请参考 [存储管理指南](#) 和 [DM 多路径指南](#)。



重要

如果您使用的是块存储，并且打算在裸设备上部署虚拟机或直接 LUN 并用逻辑卷管理器 (LVM) 管理它们，您必须创建一个过滤器来隐藏 guest 逻辑卷。这将防止在主机引导时激活 guest 逻辑卷，这种情况可能会导致逻辑卷过时并导致数据崩溃。使用 **vdsm-tool config-lvm-filter** 命令创建 LVM 的过滤器。请参阅 [创建 LVM 过滤器](#)



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。

重要

如果您的主机从 SAN 存储引导并丢失与存储的连接，则存储文件系统将变为只读并在恢复连接后保持此状态。

要防止这种情况，请在 SAN 的根文件系统中为引导 LUN 添加下拉多路径配置文件以确保它在连接时已在队列中：

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
  multipath {
    wwid boot_LUN_wwid
    no_path_retry queue
  }
}
```

5.4. 准备兼容 POSIX 的文件系统存储

POSIX 文件系统支持允许您使用与从命令行手动挂载时所用的相同挂载选项挂载文件系统。这个功能旨在允许访问没有使用 NFS、iSCSI 或 FCP 公开的存储。

所有用作 Red Hat Virtualization 中的存储域的所有 POSIX 兼容文件系统都必须是集群文件系统，如全局文件系统 2(GFS2)，并且必须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。

有关设置和配置 POSIX 兼容文件系统存储的详情，请参考 [Red Hat Enterprise Linux Global File System 2](#)。

重要

不要通过创建兼容 POSIX 的文件系统存储域来挂载 NFS 存储。始终创建 NFS 存储域。

5.5. 准备本地存储

在 Red Hat Virtualization Host(RHVM)上，应始终在独立于 / (root)的文件系统上定义本地存储。使用单独的逻辑卷或磁盘，在升级过程中防止可能丢失数据。

Red Hat Enterprise Linux 主机的步骤

1. 在主机上，创建要用于本地存储的目录：

```
# mkdir -p /data/images
```

2. 确保该目录具有允许对 **vds**m 用户(UID 36)和 **kvm** 组(GID 36)的读/写访问权限：

```
# chown 36:36 /data /data/images
# chmod 0755 /data /data/images
```

Red Hat Virtualization 主机的步骤

在逻辑卷中创建本地存储：

1. 创建本地存储目录：

```
# mkdir /data
# lvcreate -L $SIZE rhvh -n data
# mkfs.ext4 /dev/mapper/rhvh-data
# echo "/dev/mapper/rhvh-data /data ext4 defaults,discard 1 2" >> /etc/fstab
# mount /data
```

2. 挂载新的本地存储：

```
# mount -a
```

3. 确保该目录具有允许对 **vds**m 用户(UID 36)和 **kvm** 组(GID 36)的读/写访问权限：

```
# chown 36:36 /data /rhvh-data
# chmod 0755 /data /rhvh-data
```

5.6. 准备 RED HAT GLUSTER STORAGE

有关设置和配置 Red Hat Gluster Storage 的信息，请参阅 [Red Hat Gluster Storage 安装指南](#)

有关 Red Hat Virtualization 支持的 Red Hat Gluster Storage 版本，请参阅 [Red Hat Gluster Storage 版本兼容性和支持](#)。

5.7. 为 SAN 供应商自定义多路径配置

如果您的 RHV 环境配置为使用 SAN 的多路径连接，您可以自定义多路径配置设置以满足您的存储供应商指定的要求。这些自定义可覆盖 **/etc/multipath.conf** 中指定的默认设置和设置。

要覆盖多路径设置，请不要自定义 **/etc/multipath.conf**。因为 VDSM 拥有 **/etc/multipath.conf**，因此安装或升级 VDSM 或 Red Hat Virtualization 可能会覆盖此文件，包括其包含的任何自定义。这种覆盖可能会导致严重存储失败。

取而代之，您可以在 **/etc/multipath/conf.d** 目录中创建一个文件，其中包含您要自定义或覆盖的设置。

VDSM 按字母顺序执行 **/etc/multipath/conf.d** 中的文件。因此，为了控制执行顺序，您可以从使文件名进入最后一个的数字开始。例如：**/etc/multipath/conf.d/90-myfile.conf**。

要避免造成严重的存储失败，请遵循以下准则：

- 不要修改 **/etc/multipath.conf**。如果文件包含用户修改，且文件被覆盖，则可能会导致意外的存储问题。
- 不要覆盖 **user_friendly_names** 和 **find_multipaths** 设置。详情请参阅 [Multipath.conf 的建议设置](#)。
- 除非存储供应商特别要求您这样做，否则请避免覆盖 **no_path_retry** 和 **poll_interval** 设置。详情请参阅 [Multipath.conf 的建议设置](#)。

**警告**

不遵循上述准则可能会导致灾难性存储错误。

先决条件

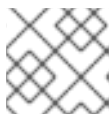
- VDSM 配置为使用 multipath 模块。要验证这一点，请输入：

```
# vdsmd-tool is-configured --module multipath
```

流程

1. 在 `/etc/multipath/conf.d` 目录中创建新的配置文件。
2. 将您要从 `/etc/multipath.conf` 中覆盖的单独设置复制到 `/etc/multipath/conf.d/<my_device>.conf` 中的新配置文件。删除任何注释标记、编辑设置值并保存您的更改。
3. 输入以下内容应用新的配置设置：

```
# systemctl reload multipathd
```

**注意**

不要重启 multipathd 服务。这样做会在 VDSM 日志中生成错误。

验证步骤

1. 测试新配置是否在各种故障场景中在非生产集群中按预期执行。例如，禁用所有存储连接。
2. 一次启用一个连接，并验证这样做是否使存储域可访问。

其它资源

- [推荐的 Multipath.conf 设置](#)
- [Red Hat Enterprise Linux DM 多路径](#)
- [配置 iSCSI 多路径](#)
- [如何自定义 RHVH 虚拟机监控程序上的 /etc/multipath.conf？哪些值不能改变，为什么？](#)

5.8. 推荐的 MULTIPATH.CONF 设置

不要覆盖以下设置：

```
user_friendly_names no
```

设备名称在所有管理程序之间必须一致。例如：`/dev/mapper/{WWID}`。此设置的默认值 `no` 可防止在不同虚拟机监控程序上分配任意和不一致的设备名称，如 `/dev/mapper/mpath{N}`，这会导致系统行为不可预测。



警告

不要将此设置更改为 `user_friendly_names yes`。用户友好的名称可能会导致系统行为或故障无法预测，且不受支持。

`find_multipaths no`

此设置控制 RHVH 是否仅在有多条路径可用时尝试通过多路径访问设备。当前值 `no` 允许 RHV 通过多条路径访问设备，即使只有一个路径可用。



警告

不要覆盖此设置。

除非存储系统厂商需要，否则请避免覆盖以下设置：

`no_path_retry 4`

此设置控制无路径可用时尝试重试的轮询数量。在 RHV 版本 4.2 之前，`no_path_retry` 的值为 `fail`，因为在没有路径可用时，QEMU 和 I/O 队列可能会遇到问题。`fail` 值使其快速失败并暂停虚拟机。RHV 版本 4.2 将此值更改为 `4`，因此当多路径检测到最后一个路径失败时，它会检查所有路径四次。假设默认的 5 秒轮询间隔，这个检查路径的过程需要 20 秒。如果没有启动路径，`multipathd` 会告知内核停止排队并出现故障，直到路径恢复。恢复路径后，下次所有路径都失败时重置 20 秒延迟。如需了解更多详细信息，请参阅[更改此设置的提交](#)。

`polling_interval 5`

此设置决定了轮询尝试检测路径是打开还是失败之间的秒数。除非供应商提供了增加这个值的明确原因，请保留 VDSM 生成的默认值，以便系统更快地响应路径失败。

第 6 章 为 RED HAT VIRTUALIZATION 添加存储

在新环境中添加存储作为数据域。Red Hat Virtualization 环境必须至少有一个数据域，但建议添加更多。

添加您之前准备的存储：

- NFS
- iSCSI
- Fibre Channel (FCP)
- 兼容 POSIX 的文件系统
- 本地存储
- Red Hat Gluster Storage

6.1. 添加 NFS 存储

此流程演示了如何将现有 NFS 存储附加到 Red Hat Virtualization 环境作为数据域。

如果您需要 ISO 或导出域，请使用此流程，但从 **Domain Function** 列表中选择 **ISO** 或 **Export**。

流程

1. 在管理门户中，点 **Storage** → **Domains**。
2. 点 **New Domain**。
3. 输入存储域的**名称**。
4. 接受 **Data Center**, **Domain Function**, **Storage Type**, **Format**, 和 **Host** 列表的默认值。
5. 输入要用于存储域的**导出路径**。导出路径的格式应为 `123.123.0.10:/data` (IPv4), `[2001:0:0:0:0:0:5db1]/data` (IPv6), 或 `domain.example.com:/data`。
6. 另外，您可以配置高级参数：
 - a. 点 **Advanced Parameters**。
 - b. 在 **Warning Low Space Indicator** 字段中输入一个百分比值。如果存储域中的可用空间低于这个百分比，则会向用户显示警告消息并记录日志。
 - c. 在 **Critical Space Action Blocker** 字段中输入一个 GB 值。如果存储域中可用的可用空间低于此值，则会向用户和记录错误消息显示，并且任何占用空间的新操作（即便是临时使用）都会被阻止。
 - d. 选中 **Wipe After Delete** 复选框以启用 `wipe after delete` 选项。可以在创建域后编辑此选项，但是这样做不会在删除已存在的磁盘属性后更改擦除。
7. 点击 **确定**。

新 NFS 数据域的状态为 **Locked**，直到准备好磁盘为止。然后，数据域将自动附加到数据中心。

6.2. 添加 iSCSI 存储

此流程演示了如何将现有 iSCSI 存储附加到 Red Hat Virtualization 环境中作为数据域。

流程

1. 点 **Storage** → **Domains**。
2. 点 **New Domain**。
3. 输入新存储域的名称。
4. 从下拉列表中选择**数据中心**。
5. 选择 **Data** 作为 **Domain Function**，**iSCSI** 作为 **Storage Type**。
6. 选择活动主机作为**主机**。



重要

与存储域的通信来自选定的主机，而不是直接从管理器通信。因此，所有主机都必须有权访问存储设备，然后才能配置存储域。

7. 管理器可以将 iSCSI 目标映射到 LUN 或 LUN，以将 iSCSI 目标映射到 iSCSI 目标。当选择了 iSCSI 存储类型时，**新建域**窗口会自动显示已知带有未使用的 LUN 的目标。如果没有显示您要添加存储的目标，您可以使用目标发现来查找它；否则，继续下一步。
 - a. 单击 **Discover Targets** 以启用目标发现选项。发现目标并登录后，**新建域**窗口将自动显示环境未使用的目标。



注意

外部用于环境的 LUN 也会显示。

您可以使用 **发现目标** 选项在多个目标或同一 LUN 的多个路径中添加 LUN。



重要

如果您使用 REST API 方法 **discoveriscsi** 发现 iscsi 目标，您可以使用 FQDN 或 IP 地址，但您必须使用发现的目标结果中的 iscsi 详细信息才能使用 REST API 方法 **iscsilogin** 进行登录。如需更多信息，请参阅 *REST API 指南* 中的 [发现iscsi](#)。

- b. 在 **Address** 字段中输入 iSCSI 主机的 FQDN 或 IP 地址。
- c. 在 **Port** 字段中，输入在浏览目标时要连接到主机的端口。默认值为 **3260**。
- d. 如果使用 CHAP 保护存储，请选中 **User Authentication** 复选框。输入 **CHAP 用户名** 和 **CHAP 密码**。



注意

您可以使用 REST API 为特定主机的 iSCSI 目标定义凭据。如需更多信息，请参阅 *REST API 指南* 中的 [StorageServerConnectionExtensions : add](#)。

- e. 点 **Discover**。
- f. 从发现结果中选择一个或多个目标，再点 **Login**（一个目标）或 **Login All**（多个目标）。



重要

如果需要多个路径访问，您必须通过所有必要的路径发现并登录到目标。目前不支持修改存储域以添加其他路径。



重要

在使用 REST API **iscsilogin** 方法登录时，您必须使用发现的目标中的 iscsi 详细信息生成 **discoveriscsi** 方法。如需更多信息，请参阅 *REST API 指南* 中的 [iscsilogin](#)。

8. 点所需目标旁边的 **+** 按钮。这会展开条目并显示附加到目标的所有未使用的 LUN。
9. 选中您正在使用的每个 LUN 的复选框，以创建存储域。
10. 另外，您可以配置高级参数：
 - a. 点 **Advanced Parameters**。
 - b. 在 **Warning Low Space Indicator** 字段中输入一个百分比值。如果存储域中的可用空间低于这个百分比，则会向用户显示警告消息并记录日志。
 - c. 在 **Critical Space Action Blocker** 字段中输入一个 GB 值。如果存储域中可用的可用空间低于此值，则会向用户和记录错误消息显示，并且任何占用空间的新操作（即便是临时使用）都会被阻止。
 - d. 选中 **Wipe After Delete** 复选框以启用 wipe after delete 选项。可以在创建域后编辑此选项，但是这样做不会在删除已存在的磁盘属性后更改擦除。
 - e. 选中 **Discard After Delete** 复选框，以在删除后启用丢弃选项。可在创建域后编辑此选项。此选项仅适用于块存储域。
11. 点击 **确定**。

如果您已配置了多个存储连接路径到同一目标，请按照[配置 iSCSI 多路径](#)以完成 iSCSI 绑定的步骤进行操作。

如果要将当前存储网络迁移到 iSCSI 绑定，请参阅[将逻辑网络迁移到 iSCSI Bond](#)。

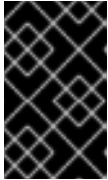
6.3. 添加 FCP 存储

此流程演示了如何将现有 FCP 存储附加到 Red Hat Virtualization 环境作为数据域。

流程

1. 点 **Storage** → **Domains**。
2. 点 **New Domain**。
3. 输入存储域的**名称**。

4. 从下拉列表中选择 **FCP Data Center**。
如果您还没有适当的 FCP 数据中心，请选择 **(none)**。
5. 从下拉列表中选择 **Domain Function** 和 **Storage Type**。与所选数据中心不兼容的存储域类型不可用。
6. 在 **Host** 字段中选择一个活动主机。如果这不是数据中心中的第一个数据域，您必须选择数据中心的 SPM 主机。



重要

与存储域的所有通信均通过选定的主机进行，而不是直接从 Red Hat Virtualization Manager 进行。系统中必须至少有一个活动主机，并附加到所选的数据中心。所有主机都必须有权访问存储设备，然后才能配置存储域。

7. 当选择 **Fibre Channel** 作为存储类型时，**新建域** 窗口会自动显示已知带有未使用的 LUN 的目标。选择 **LUN ID** 复选框来选择所有可用的 LUN。
8. 另外，您还可以配置高级参数。
 - a. 点 **Advanced Parameters**。
 - b. 在 **Warning Low Space Indicator** 字段中输入一个百分比值。如果存储域中的可用空间低于这个百分比，则会向用户显示警告消息并记录日志。
 - c. 在 **Critical Space Action Blocker** 字段中输入一个 GB 值。如果存储域中可用的可用空间低于此值，则会向用户和记录错误消息显示，并且任何占用空间的新操作（即便是临时使用）都会被阻止。
 - d. 选中 **Wipe After Delete** 复选框以启用 wipe after delete 选项。可以在创建域后编辑此选项，但是这样做不会在删除已存在的磁盘属性后更改擦除。
 - e. 选中 **Discard After Delete** 复选框，以在删除后启用丢弃选项。可在创建域后编辑此选项。此选项仅适用于块存储域。
9. 点击 **确定**。

新的 FCP 数据域在准备使用时仍然处于 **Locked** 状态。准备就绪后，它将自动附加到数据中心。

6.4. 添加兼容 POSIX 的文件系统存储

此流程演示了如何将现有的 POSIX 兼容文件系统存储作为数据域附加到 Red Hat Virtualization 环境中。

流程

1. 点 **Storage → Domains**。
2. 点 **New Domain**。
3. 输入存储域的名称。
4. 选择要与存储域关联的**数据中心**。所选数据中心必须是 **POSIX (POSIX 兼容 FS)** 的类型。或者，选择 **(none)**
5. 从 **Domain Function** 下拉列表中选择 **Data**，从 **Storage Type** 下拉列表中选择 **POSIX 兼容 FS**。

- 如果适用，从下拉菜单中选择 **Format**。
6. 从主机下拉列表选择一个**主机**。
 7. 输入 **POSIX** 文件系统的路径，因为您通常会将其提供给 **mount** 命令。
 8. 输入 **VFS 类型**，因为您通常会使用 **-t** 参数将其提供给 **mount** 命令。有关有效 VFS 类型的列表，请参阅 **man mount**。
 9. 输入其他 **挂载选项**，因为您通常使用 **-o** 参数将它们提供给 **mount** 命令。挂载选项应以逗号分隔列表形式提供。有关有效挂载选项列表，请参阅 **man mount**。
 10. 另外，您还可以配置高级参数。
 - a. 点 **Advanced Parameters**。
 - b. 在 **Warning Low Space Indicator** 字段中输入百分比值。如果存储域中的可用空间低于这个百分比，则会向用户显示警告消息并记录日志。
 - c. 在 **Critical Space Action Blocker** 字段中输入 GB 值。如果存储域中可用的可用空间低于此值，则会向用户和记录错误消息显示，并且任何占用空间的新操作（即便是临时使用）都会被阻止。
 - d. 选中 **Wipe After Delete** 复选框以启用 **wipe after delete** 选项。可以在创建域后编辑此选项，但是这样做不会在删除已存在的磁盘属性后更改擦除。
 11. 点击 **确定**。

6.5. 添加本地存储域

将本地存储域添加到主机时，设置本地存储目录的路径会自动创建并将主机放置到本地数据中心、本地集群和本地存储域中。


流程

1. 单击 **Compute** → **Hosts**，再选择 **主机**。
2. 点 **Management** → **Maintenance** 和 **OK**。主机的状态更改为 **Maintenance**。
3. 单击 **Management** → **Configure Local Storage**。
4. 单击 **Data Center**、**Cluster** 和 **Storage** 字段旁边的**编辑按钮**，以配置和命名本地存储域。
5. 在文本条目字段中设置本地存储的路径。
6. 如果适用，点 **Optimization** 选项卡为新的本地存储集群配置内存优化策略。
7. 点击 **确定**。

Manager 使用本地集群本地存储域设置本地数据中心。它还将主机的状态更改为 **Up**。

验证

1. 点 **Storage** → **Domains**。
2. 找到您刚刚添加的本地存储域。

域的状态应当是 **Active** (), **Storage Type** 列中的值应该是 **Local on Host**。

现在, 您可以在新的本地存储域中上传磁盘镜像。

6.6. 添加 RED HAT GLUSTER STORAGE

要在 Red Hat Virtualization 中使用 Red Hat Gluster Storage, 请参阅 [配置 Red Hat Virtualization 使用 Red Hat Gluster Storage](#)。

有关 Red Hat Virtualization 支持的 Red Hat Gluster Storage 版本, 请参阅 [Red Hat Gluster Storage 版本兼容性和支持](#)。

附录 A. 为 RED HAT VIRTUALIZATION MANAGER 安装配置本地仓库

要在没有与 Content Delivery Network 直接连接的系统中安装 Red Hat Virtualization Manager，请在有互联网访问的系统中下载所需软件包，然后创建一个可与离线管理器机器共享的软件仓库。托管存储库的系统必须连接到与要安装的软件包的客户端系统相同的网络。

先决条件

- 在可访问 Content Delivery Network 的系统中安装 Red Hat Enterprise Linux 8 服务器。这个系统下载所有必要的软件包，并将其分发到离线系统中。
- 有大量可用磁盘空间。这个过程下载大量软件包，并最多需要 50GB 的可用磁盘空间。

首先，在在线系统中启用 Red Hat Virtualization Manager 软件仓库：

启用 Red Hat Virtualization Manager 存储库

您需要登录并使用 Red Hat Subscription Manager 注册在线机器，附加 **Red Hat Virtualization Manager** 订阅并启用 Manager 软件仓库。

流程

1. 使用 Content Delivery Network 注册您的系统，在提示时输入您的客户门户网站用户名和密码：

```
# subscription-manager register
```



注意

如果您使用 IPv6 网络，请使用 IPv6 转换机制来访问 Content Delivery Network 和 subscription Manager。

2. 查找 **Red Hat Virtualization Manager** 订阅池并记录池 ID：

```
# subscription-manager list --available
```

3. 使用池 ID 将订阅附加到系统：

```
# subscription-manager attach --pool=pool_id
```



注意

查看当前附加的订阅：

```
# subscription-manager list --consumed
```

列出所有启用的软件仓库：

```
# dnf repolist
```

4. 配置存储库：

```
# subscription-manager repos \
--disable='*' \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms \
--enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
--enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
--enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
--enable=rhel-8-for-x86_64-appstream-tus-rpms \
--enable=rhel-8-for-x86_64-baseos-tus-rpms
```

- 将 RHEL 版本设置为 8.6:

```
# subscription-manager release --set=8.6
```

- 启用 **pki-deps** 模块。

```
# dnf module -y enable pki-deps
```

- 启用 **postgresql** 模块的版本 12。

```
# dnf module -y enable postgresql:12
```

- 启用 **nodejs** 模块的版本 14:

```
# dnf module -y enable nodejs:14
```

- 同步安装的软件包，将它们更新至最新可用版本。

```
# dnf distro-sync --nobest
```

其它资源

有关模块和模块流的详情，请参考 [安装](#)、[管理](#)和[删除用户空间组件](#)中的以下部分。

- [模块流](#)
- [安装软件包前选择流](#)
- [重置模块流](#)
- [切换到更新的流](#)

配置离线存储库

- 未连接到互联网的服务器可以使用文件传输协议(FTP)访问其他系统上的软件存储库。要创建 FTP 软件仓库，在预期的管理器机器中安装和配置 **vsftpd** :

- 安装 **vsftpd** 软件包 :

```
# dnf install vsftpd
```

- b. 启用匿名用户的 FTP 访问权限，以便从预期管理器计算机访问 rpm 文件，并保证其安全，禁用 ftp 服务器上的写入操作。编辑 `/etc/vsftpd/vsftpd.conf` 文件并更改 `anonymous_enable` 和 `write_enable` 的值，如下所示：

```
anonymous_enable=YES
write_enable=NO
```

- c. 启动 `vsftpd` 服务，并确保该服务在引导时启动：

```
# systemctl start vsftpd.service
# systemctl enable vsftpd.service
```

- d. 创建一条防火墙规则来允许 FTP 服务并重新载入 `firewalld` 服务以应用更改：

```
# firewall-cmd --permanent --add-service=ftp
# firewall-cmd --reload
```

- e. Red Hat Enterprise Linux 8 默认强制 SELinux，因此配置 SELinux 以允许 FTP 访问：

```
# setsebool -P allow_ftp_full_access=1
```

- f. 在 `/var/ftp/pub/` 目录中创建一个子目录，其中下载的软件包可用：

```
# mkdir /var/ftp/pub/rhvrepo
```

2. 从所有配置的软件存储库下载软件包到 `rhvrepo` 目录。这包括附加到系统的所有 Content Delivery Network 订阅池以及任何本地配置的软件仓库：

```
# reposync -p /var/ftp/pub/rhvrepo --download-metadata
```

此命令会下载大量软件包及其元数据，并且需要很长时间才能完成。

3. 创建库文件，并将其复制到预期管理器计算机上的 `/etc/yum.repos.d/` 目录中。您可以手动或通过脚本创建配置文件。在托管存储库的机器上运行以下脚本，将 `baseurl` 中的 `ADDRESS` 替换为托管该存储库的机器的 IP 地址或 FQDN：

```
#!/bin/sh

REPOFILE="/etc/yum.repos.d/rhev.repo"
echo -e " " > $REPOFILE

for DIR in $(find /var/ftp/pub/rhvrepo -maxdepth 1 -mindepth 1 -type d);
do
    echo -e "[$(basename $DIR)]" >> $REPOFILE
    echo -e "name=$(basename $DIR)" >> $REPOFILE
    echo -e "baseurl=ftp://__ADDRESS__/pub/rhvrepo/'$(basename $DIR)'" >> $REPOFILE
    echo -e "enabled=1" >> $REPOFILE
    echo -e "gpgcheck=0" >> $REPOFILE
    echo -e "\n" >> $REPOFILE
done
```

[返回到配置管理器](#)。软件包是从本地存储库而不是从 Content Delivery Network 中安装的软件包。

故障排除

在运行 `reposync` 时，会出现以下出错信息

No available modular metadata for modular package "package_name_from_module" it cannot be installed on the system

解决方案

确保已安装 `yum-utils-4.0.8-3.el8.noarch` 或更高版本，以便 `reposync` 正确下载所有软件包。如需更多信息，请参阅[使用 Red Hat Enterprise Linux 8 创建本地仓库](#)。

附录 B. 准备本地手动配置 PostgreSQL 数据库

使用这个步骤设置 Manager 数据库。在配置管理器前设置这个数据库；您必须在 **engine-setup** 中提供数据库凭证。



注意

engine-setup 和 **engine-backup --mode=restore** 命令只支持 **en_US.UTF8** 区域中的系统错误消息，即使系统区域设置不同。

postgresql.conf 文件中的区域设置必须设置为 **en_US.UTF8**。



重要

数据库名称必须包含数字、下划线和小写字母。

启用 Red Hat Virtualization Manager 存储库

您需要使用 Red Hat Subscription Manager 登录并注册 Manager 机器，附加 **Red Hat Virtualization Manager** 订阅并启用 Manager 存储库。

流程

1. 使用 Content Delivery Network 注册您的系统，在提示时输入您的客户门户网站用户名和密码：

```
# subscription-manager register
```



注意

如果您使用 IPv6 网络，请使用 IPv6 转换机制来访问 Content Delivery Network 和 subscription Manager。

2. 查找 **Red Hat Virtualization Manager** 订阅池并记录池 ID：

```
# subscription-manager list --available
```

3. 使用池 ID 将订阅附加到系统：

```
# subscription-manager attach --pool=pool_id
```



注意

查看当前附加的订阅：

```
# subscription-manager list --consumed
```

列出所有启用的软件仓库：

```
# dnf repolist
```

4. 配置存储库：

```
# subscription-manager repos \
--disable='*' \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms \
--enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
--enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
--enable=rhceph-4-tools-for-rhel-8-x86_64-rpms \
--enable=rhel-8-for-x86_64-appstream-tus-rpms \
--enable=rhel-8-for-x86_64-baseos-tus-rpms
```

5. 将 RHEL 版本设置为 8.6:

```
# subscription-manager release --set=8.6
```

6. 启用 **postgresql** 模块的版本 12。

```
# dnf module -y enable postgresql:12
```

7. 启用 **nodejs** 模块的版本 14:

```
# dnf module -y enable nodejs:14
```

8. 同步安装的软件包，将它们更新至最新可用版本。

```
# dnf distro-sync --nobest
```

其它资源

有关模块和模块流的详情，请参考 [安装、管理和删除用户空间组件中的以下部分](#)。

- [模块流](#)
- [安装软件包前选择流](#)
- [重置模块流](#)
- [切换到更新的流](#)

初始化 PostgreSQL 数据库

1. 安装 PostgreSQL 服务器软件包：

```
# dnf install postgresql-server postgresql-contrib
```

2. 初始化 PostgreSQL 数据库实例：

```
# postgresql-setup --initdb
```

3. 启动 **postgresql** 服务，并确保这个服务在引导时启动：

```
# systemctl enable postgresql
# systemctl start postgresql
```

- 4. 以 **postgres** 用户身份连接到 **psql** 命令行界面：

```
# su - postgres -c psql
```

- 5. 创建默认用户。Manager 的默认用户是 **engine**，Data Warehouse 的默认用户是 **ovirt_engine_history**：

```
postgres=# create role user_name with login encrypted password 'password';
```

- 6. 创建数据库。Manager 的默认数据库名称为 **engine**，Data Warehouse 的默认数据库名称为 **ovirt_engine_history**：

```
postgres=# create database database_name owner user_name template template0
encoding 'UTF8' lc_collate 'en_US.UTF-8' lc_ctype 'en_US.UTF-8';
```

- 7. 连接到新数据库：

```
postgres=# \c database_name
```

- 8. 添加 **uuid-osspl** 扩展：

```
database_name=# CREATE EXTENSION "uuid-osspl";
```

- 9. 如果 **plpgsql** 语言不存在，请添加 **plpgsql** 语言：

```
database_name=# CREATE LANGUAGE plpgsql;
```

- 10. 退出 **psql** 接口：

```
database_name=# \q
```

- 11. 编辑 **/var/lib/pgsql/data/pg_hba.conf** 文件以启用 md5 客户端身份验证，以便引擎在本地访问数据库。在文件底部以 **local** 开头的行下添加以下行：

```
host database_name user_name 0.0.0.0/0 md5
host database_name user_name ::0/0 md5
```

- 12. 更新 PostgreSQL 服务器配置。编辑 **/var/lib/pgsql/data/postgresql.conf** 文件，并在文件的底部添加以下行：

```
autovacuum_vacuum_scale_factor=0.01
autovacuum_analyze_scale_factor=0.075
autovacuum_max_workers=6
maintenance_work_mem=65536
max_connections=150
work_mem=8192
```

- 13. 重启 **postgresql** 服务：

```
# systemctl restart postgresql
```

14. （可选）将 [SSL](#) 设置为安全数据库连接。

返回 [配置管理器](#)，并在系统询问有关数据库时回答 **Local** 和 **Manual**。

附录 C. 为 PCI PASSTHROUGH 配置主机



注意

这是显示如何在 Red Hat Virtualization 上设置和配置 SR-IOV 的一系列主题中的一个。如需更多信息，请参阅[设置和配置 SR-IOV](#)

启用 PCI 透传 (passthrough) 可让虚拟机使用主机上的设备，就好像设备直接附加到虚拟机一样。要启用 PCI passthrough 功能，您必须启用虚拟化扩展和 IOMMU 功能。以下流程要求您重新引导主机。如果主机已附加到管理器，请务必先将主机置于维护模式。

先决条件

- 确保主机硬件满足 PCI 设备直通和分配的要求。如需更多信息，请参阅[PCI 设备要求](#)。

为 PCI Passthrough 配置主机

1. 在 BIOS 中启用虚拟化扩展和 IOMMU 扩展。如需更多信息，请参阅 *Red Hat Enterprise Linux 虚拟化部署和管理指南* 中的[在 BIOS 中启用 Intel VT-x 和 AMD-V 虚拟化硬件扩展](#)。
2. 在将主机添加到 Manager 或手动编辑 `grub` 配置文件时，选择 **Hostdev Passthrough & SR-IOV** 复选框，在内核中启用 IOMMU 标志。
 - 要从管理门户中启用 IOMMU 标志，请参阅[将标准主机添加到 Red Hat Virtualization Manager](#) 和[内核设置说明](#)。
 - 要手动编辑 `grub` 配置文件，请参阅[手动启用 IOMMU](#)。
3. 对于 GPU 直通，您需要在主机和客户机系统上运行其他配置步骤。请参阅[GPU device passthrough: Assigning a host GPU to a single virtual machine](#) in *Setting up an NVIDIA GPU for a virtual machine in Red Hat Virtualization*。

手动启用 IOMMU

1. 通过编辑 `grub` 配置文件启用 IOMMU。



注意

如果您使用 IBM POWER8 硬件，请跳过此步骤，因为默认启用 IOMMU。

- 对于 Intel，引导计算机，并在 `grub` 配置文件中的 `GRUB_CMDLINE_LINUX` 行的末尾附加 `intel_iommu=on`。

```
# vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on
...
```

- 对于 AMD，引导计算机，并将 `amd_iommu=on` 附加到 `grub` 配置文件中的 `GRUB_CMDLINE_LINUX` 行的末尾。

```
# vi /etc/default/grub
...
```

```
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... amd_iommu=on
```

```
...
```



注意

如果检测到 **intel_iommu=on** 或 AMD IOMMU，您可以尝试添加 **iommu=pt**。**pt** 选项只为用于透传的设备启用 IOMMU，并提供更好的主机性能。但是，该选项可能并不在所有硬件上受到支持。如果 **pt** 选项不适用于您的主机，则恢复先前的选项。

如果因为硬件不支持中断重新映射而导致 passthrough 失败，您可以考虑启用 **allow_unsafe_interrupts** 选项（如果虚拟机受信任）。默认情况下不启用 **allow_unsafe_interrupts**，因为它可能会使主机暴露于来自虚拟机的 MSI 攻击。启用该选项：

```
# vi /etc/modprobe.d
options vfio_iommu_type1 allow_unsafe_interrupts=1
```

2. 刷新 **grub.cfg** 文件并重启主机以使这些更改生效：

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

```
# reboot
```

附录 D. 删除独立 RED HAT VIRTUALIZATION MANAGER

engine-cleanup 命令可删除 Red Hat Virtualization Manager 的所有组件，并自动备份以下内容：

- Grafana 数据库，位于 `/var/lib/grafana/`
- `/var/lib/ovirt-engine/backups/` 中的 Manager 数据库
- 在 `/var/lib/ovirt-engine/backups/` 中的 PKI 密钥和配置压缩的存档

备份文件名包括日期和时间。



警告

您应该只在 Red Hat Virtualization Manager 的独立安装中使用这个步骤。

流程

1. 在 Manager 机器中运行以下命令：

```
# engine-cleanup
```

2. 在继续之前，必须停止管理器服务。系统将提示您确认。输入 **OK** 继续操作：

```
During execution engine service will be stopped (OK, Cancel) [OK]:
```

3. 系统将提示您确认要删除所有管理器组件。输入 **OK** 删除所有组件，或 **Cancel** 以退出 **engine-cleanup**：

```
All the installed ovirt components are about to be removed, data will be lost (OK, Cancel) [Cancel]: OK
```

engine-cleanup 详细说明已删除的组件，以及备份文件的位置。

4. 删除 Red Hat Virtualization 软件包：

```
# dnf remove rhvm* vds-m-bootstrap
```

附录 E. 防止内核模块自动载入

您可以防止自动加载内核模块，无论是直接加载模块，还是在引导过程中作为依赖项载入。

流程

1. 模块名称必须添加到 **modprobe** 实用程序的配置文件中。此文件必须位于配置目录 **/etc/modprobe.d** 中。
有关此配置目录的更多信息，请参阅 man page **modprobe.d**。

2. 确保该模块没有配置为在以下任意位置载入：

- **/etc/modprobe.conf**
- **/etc/modprobe.d/***
- **/etc/rc.modules**
- **/etc/sysconfig/modules/***

```
# modprobe --showconfig <_configuration_file_name_>
```

3. 如果模块出现在输出中，请确保它被忽略且没有加载：

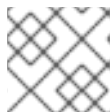
```
# modprobe --ignore-install <_module_name_>
```

4. 如果载入了正在运行的系统，从正在运行的系统中卸载该模块：

```
# modprobe -r <_module_name_>
```

5. 通过将 **blacklist** 行添加到系统专用的配置文件（如 **/etc/modprobe.d/local-dontload.conf**）来防止直接加载模块：

```
# echo "blacklist <_module_name_> >> /etc/modprobe.d/local-dontload.conf"
```



注意

如果模块是另一个模块的必需依赖项或可选依赖项，则此步骤不会阻止模块加载。

6. 防止根据需要载入可选模块：

```
# echo "install <_module_name_>/bin/false" >> /etc/modprobe.d/local-dontload.conf"
```



重要

如果其他硬件需要排除的模块，则排除该模块可能会导致意外的副作用。

7. 生成 **initramfs** 的备份副本：

```
# cp /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.$(date +%m-%d-%H%M%S).bak
```


8. 如果内核模块是 **initramfs** 的一部分，重建初始 **ramdisk** 镜像，省略该模块：

```
# dracut --omit-drivers <_module_name_> -f
```

9. 获取当前的内核命令行参数：

```
# grub2-editenv - list | grep kernelopts
```

10. 将 **<_module_name_>.blacklist=1 rd.driver.blacklist=<_module_name_>** 附加到生成的输出中：

```
# grub2-editenv - set kernelopts="<> <_module_name_>.blacklist=1 rd.driver.blacklist=
<_module_name_>"
```

例如：

```
# grub2-editenv - set kernelopts="root=/dev/mapper/rhel_example-root ro crashkernel=auto
resume=/dev/mapper/rhel_example-swap rd.lvm.lv=rhel_example/root
rd.lvm.lv=rhel_example/swap <_module_name_>.blacklist=1 rd.driver.blacklist=
<_module_name_>"
```

11. 生成 **kdump initramfs** 的备份副本：

```
# cp /boot/initramfs-$(uname -r)kdump.img /boot/initramfs-$(uname -r)kdump.img.$(date
+%m-%d-%H%M%S).bak
```

12. 将 **rd.driver.blacklist=<_module_name_>** 附加到 **/etc/sysconfig/kdump** 文件中的 **KDUMP_COMMANDLINE_APPEND** 设置中，以从 **kdump initramfs** 中忽略它：

```
# sed -i '/^KDUMP_COMMANDLINE_APPEND=/s/"$/ rd.driver.blacklist=module_name"/'
/etc/sysconfig/kdump
```

13. 重启 **kdump** 服务以获取对 **kdump initrd** 的更改：

```
# kdumpctl restart
```

14. 重建 **kdump** 初始 **ramdisk** 镜像：

```
# mkdumprd -f /boot/initramfs-$(uname -r)kdump.img
```

15. 重启系统：

E.1. 临时删除模块

您可以临时删除模块。

流程

1. 运行 **modprobe** 以删除任何当前加载的模块：

```
# modprobe -r <module name>
```

2. 如果模块无法卸载，则进程或其他模块可能仍在使用该模块。如果是，终止进程并运行在其他时间上写入的 **modprobe** 命令以卸载该模块。

附录 F. 防止内核模块自动载入

您可以防止自动加载内核模块，无论是直接加载模块，还是在引导过程中作为依赖项载入。

流程

1. 模块名称必须添加到 **modprobe** 实用程序的配置文件中。此文件必须位于配置目录 **/etc/modprobe.d** 中。
有关此配置目录的更多信息，请参阅 man page **modprobe.d**。

2. 确保该模块没有配置为在以下任意位置载入：

- **/etc/modprobe.conf**
- **/etc/modprobe.d/***
- **/etc/rc.modules**
- **/etc/sysconfig/modules/***

```
# modprobe --showconfig <_configuration_file_name_>
```

3. 如果模块出现在输出中，请确保它被忽略且没有加载：

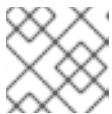
```
# modprobe --ignore-install <_module_name_>
```

4. 如果载入了正在运行的系统，从正在运行的系统中卸载该模块：

```
# modprobe -r <_module_name_>
```

5. 通过将 **blacklist** 行添加到系统专用的配置文件（如 **/etc/modprobe.d/local-dontload.conf**）来防止直接加载模块：

```
# echo "blacklist <_module_name_> >> /etc/modprobe.d/local-dontload.conf"
```

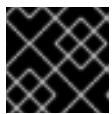


注意

如果模块是另一个模块的必需依赖项或可选依赖项，则此步骤不会阻止模块加载。

6. 防止根据需要载入可选模块：

```
# echo "install <_module_name_>/bin/false" >> /etc/modprobe.d/local-dontload.conf"
```



重要

如果其他硬件需要排除的模块，则排除该模块可能会导致意外的副作用。

7. 生成 **initramfs** 的备份副本：

```
# cp /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.$(date +%m-%d-%H%M%S).bak
```

8. 如果内核模块是 **initramfs** 的一部分，重建初始 **ramdisk** 镜像，省略该模块：

```
# dracut --omit-drivers <_module_name_> -f
```

9. 获取当前的内核命令行参数：

```
# grub2-editenv - list | grep kernelopts
```

10. 将 **<_module_name_>.blacklist=1 rd.driver.blacklist=<_module_name_>** 附加到生成的输出中：

```
# grub2-editenv - set kernelopts="<> <_module_name_>.blacklist=1 rd.driver.blacklist=
<_module_name_>"
```

例如：

```
# grub2-editenv - set kernelopts="root=/dev/mapper/rhel_example-root ro crashkernel=auto
resume=/dev/mapper/rhel_example-swap rd.lvm.lv=rhel_example/root
rd.lvm.lv=rhel_example/swap <_module_name_>.blacklist=1 rd.driver.blacklist=
<_module_name_>"
```

11. 生成 **kdump initramfs** 的备份副本：

```
# cp /boot/initramfs-$(uname -r)kdump.img /boot/initramfs-$(uname -r)kdump.img.$(date
+%m-%d-%H%M%S).bak
```

12. 将 **rd.driver.blacklist=<_module_name_>** 附加到 **/etc/sysconfig/kdump** 文件中的 **KDUMP_COMMANDLINE_APPEND** 设置中，以从 **kdump initramfs** 中忽略它：

```
# sed -i '/^KDUMP_COMMANDLINE_APPEND=/s/"$/ rd.driver.blacklist=module_name"/'
/etc/sysconfig/kdump
```

13. 重启 **kdump** 服务以获取对 **kdump initrd** 的更改：

```
# kdumpctl restart
```

14. 重建 **kdump** 初始 **ramdisk** 镜像：

```
# mkdumprd -f /boot/initramfs-$(uname -r)kdump.img
```

15. 重启系统：

F.1. 临时删除模块

您可以临时删除模块。

流程

1. 运行 **modprobe** 以删除任何当前加载的模块：

```
# modprobe -r <module name>
```

2. 如果模块无法卸载，则进程或其他模块可能仍在使用该模块。如果是，终止进程并运行在其他时间上写入的 **modprobe** 命令以卸载该模块。

附录 G. 保护 RED HAT VIRTUALIZATION

此信息特定于 Red Hat Virtualization。它不涵盖与以下任何方面相关的基本安全实践：

- 禁用不必要的服务
- 身份验证
- 授权
- Accounting
- 非 RHV 服务的渗透测试和强化
- 加密敏感应用程序数据

先决条件

- 您应精通机构的安全标准和实践。如果可能，请咨询机构的负责安全的人员。
- 在部署 RHEL 主机前，请参阅 Red Hat Enterprise Linux [安全强化](#)。

G.1. 在基于 RHEL 的主机和独立管理器中应用 DISA STIG 配置集

安装 RHV 时，您可以使用 UI 安装程序选择 DISA STIG 配置集，这是 RHEL 8 提供的配置集。



重要

Red Hat Virtualization Host(RHVH)不支持 DISA STIG 配置集。

流程

1. 在 **安装概述** 屏幕中选择 **安全策略**。
2. 在 **Security Policy** 屏幕中，将 **Apply security policy** 设置为 **On**。
3. 为 Red Hat Enterprise Linux 8 选择 **DISA STIG**
4. 点击 **Select profile**。此操作在配置集旁边添加一个绿色勾号，并将软件包添加到**已完成或需要完成的更改**列表中。如果它们指示您进行任何更改，请按照屏幕说明进行操作。
5. 点 **Done**。
6. 在**安装概述**屏幕上，验证 **Security Policy** 的状态是否为 **Everything**。
7. 重启主机。

G.1.1. 在自托管引擎中启用 DISA STIG

您可以在部署使用命令行时在自托管引擎中启用 DISA STIG。

流程

1. 启动自托管引擎部署脚本。使用命令行将 Red Hat Virtualization 安装为自托管引擎。

2. 当部署脚本提示 **是否要应用 OpenSCAP 安全配置集**时，请输入 **Yes**。
3. 当部署脚本提示 **Please 提供您要使用的安全配置集**时，请输入 **stig**。

G.2. 在 RHV 主机和独立管理器中应用 PCI-DSS 配置集

安装 RHVH 时，您可以使用 UI 安装程序选择 PCI-DSS 配置集，这是 RHEL 8 提供的配置集。

流程

1. 在 **安装概述** 屏幕中选择 **安全策略**。
2. 在 **Security Policy** 屏幕中，将 **Apply security policy** 设置为 **On**。
3. 为 Red Hat Enterprise Linux 8 选择 **PCI-DSS v3.2.1 Control Baseline**
4. 点击 **Select profile**。此操作在配置集旁边添加一个绿色勾号，并将软件包添加到**已完成或需要完成的更改**列表中。如果它们指示您进行任何更改，请按照屏幕说明进行操作。
5. 点 **Done**。
6. 在 **安装概述** 屏幕中，验证 **安全策略的状态是一切正常**。
7. 重启主机。

G.2.1. 在自托管引擎中启用 PCI-DSS

您可以在部署使用命令行时在自托管引擎中启用 PCI-DSS。

流程

1. 启动自托管引擎部署脚本。使用命令行将 **Red Hat Virtualization** 安装为自托管引擎。
2. 当部署脚本提示 **是否要应用 OpenSCAP 安全配置集**时，请输入 **Yes**。
3. 当部署脚本提示 **Please 提供要使用的安全配置集**时，请输入 **pci-dss**。

附录 H. 法律通知

Copyright © 2022 Red Hat, Inc.

Licensed under the ([Creative Commons Attribution–ShareAlike 4.0 International License](#)).从(oVirt Project)的文档衍生而来。如果您发布本文档或对其进行改编，您必须提供原始版本的 URL。

修改后的版本必须删除所有红帽商标。

Red Hat、Red Hat Enterprise Linux、Red Hat 商标、Shadowman 商标、JBoss、OpenShift、Fedora、Infinity 商标以及 RHCE 都是在美国及其他国家的注册商标。

Linux® 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Java® 是 Oracle 和/或其附属公司的注册商标。

XFS® 是 Silicon Graphics International Corp. 或其子公司在美国和/或其他国家的商标。

MySQL® 是 MySQL AB 在美国、欧盟和其他国家/地区的注册商标。

Node.js® 是 Joyent 的官方商标。Red Hat Software Collections 与官方 Joyent Node.js 开源或商业项目没有正式关联或被正式认可。

The OpenStack® Word Mark 和 OpenStack 标识是 OpenStack Foundation 在美国及其他国家的注册商标/服务标记或商标/服务标记，可根据 OpenStack Foundation 授权使用。我们不附属于 OpenStack Foundation 或 OpenStack 社区。

所有其他商标均由其各自所有者所有。