



## Red Hat Virtualization 4.3

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

其他方法安装 Red Hat Virtualization Manager 及其数据库在同一服务器上



## Red Hat Virtualization 4.3 使用本地数据库将 Red Hat Virtualization 安装为独立管理器

---

其他方法安装 Red Hat Virtualization Manager 及其数据库在同一服务器上

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

## 法律通告

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Installing\_Red\_Hat\_Virtualization\_as\_a\_standalone\_Manager\_with\_local\_databases.ent file |.

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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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

本文档描述了如何安装单机管理器环境，其中 Red Hat Virtualization Manager 在带有 Manager 数据库以及安装在与管理器相同的计算机上的另一个环境中的物理服务器或虚拟机上安装。如果这不是您想要使用的配置，请参阅产品指南中的其他安装选项。

# 目录

前言 .....	4
独立管理器架构 .....	4
<b>第 1 章 安装概述 .....</b>	<b>6</b>
<b>第 2 章 要求 .....</b>	<b>7</b>
2.1. RED HAT VIRTUALIZATION MANAGER 要求 .....	7
2.1.1. 硬件要求 .....	7
2.1.2. 浏览器要求 .....	7
2.1.3. 客户端要求 .....	8
2.1.4. 操作系统要求 .....	8
2.2. 主机要求 .....	9
2.2.1. CPU 要求 .....	9
2.2.1.1. 检查处理器是否支持所需的标记 .....	9
2.2.2. 内存要求 .....	10
2.2.3. 存储要求 .....	10
2.2.4. PCI 设备要求 .....	11
2.2.5. 设备分配要求 .....	11
2.2.6. vGPU 要求 .....	11
2.3. 网络要求 .....	12
2.3.1. 常规要求 .....	12
2.3.2. DNS、NTP、IPMI 隔离和指标存储的防火墙要求 .....	12
2.3.3. Red Hat Virtualization Manager 防火墙要求 .....	12
2.3.4. 主机防火墙要求 .....	15
2.3.5. 数据库服务器防火墙要求 .....	18
<b>第 3 章 安装 RED HAT VIRTUALIZATION MANAGER .....</b>	<b>20</b>
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 .....	21
3.4. 连接到管理门户 .....	25
<b>第 4 章 为 RED HAT VIRTUALIZATION 安装主机 .....</b>	<b>27</b>
4.1. RED HAT VIRTUALIZATION 主机 .....	27
4.1.1. 安装 Red Hat Virtualization 主机 .....	27
4.1.2. 启用 Red Hat Virtualization 主机存储库 .....	29
4.1.3. 高级安装 .....	29
4.1.3.1. 自定义分区 .....	30
4.1.3.2. 自动部署 Red Hat Virtualization 主机 .....	31
4.1.3.2.1. 准备安装环境 .....	31
4.1.3.2.2. 配置 PXE 服务器和 Boot Loader .....	32
4.1.3.2.3. 创建并运行 Kickstart 文件 .....	32
4.2. RED HAT ENTERPRISE LINUX 主机 .....	34
4.2.1. 安装 Red Hat Enterprise Linux 主机 .....	34
4.2.2. 启用 Red Hat Enterprise Linux 主机存储库 .....	35
4.2.3. 在 Red Hat Enterprise Linux 主机上安装 Cockpit .....	36
4.3. 配置主机网络的建议做法 .....	36
4.4. 在 RED HAT VIRTUALIZATION MANAGER 中添加标准主机 .....	38
<b>第 5 章 为 RED HAT VIRTUALIZATION 准备存储 .....</b>	<b>39</b>
5.1. 准备 NFS 存储 .....	39
5.2. 准备 ISCSI 存储 .....	40

5.3. 准备 FCP 存储	40
5.4. 准备兼容 POSIX 的文件系统存储	41
5.5. 准备本地存储	41
5.6. 准备 RED HAT GLUSTER STORAGE	42
5.7. 为 SAN 供应商自定义多路径配置	42
5.8. 推荐的 MULTIPATH.CONF 设置	43
<b>第 6 章 为 RED HAT VIRTUALIZATION 添加存储</b>	<b>45</b>
6.1. 添加 NFS 存储	45
6.2. 添加 ISCSI 存储	45
6.3. 添加 FCP 存储	47
6.4. 添加兼容 POSIX 的文件系统存储	48
6.5. 添加本地存储	49
6.6. 添加 RED HAT GLUSTER STORAGE	49
<b>附录 A. 为 RED HAT VIRTUALIZATION MANAGER 安装配置本地仓库</b>	<b>50</b>
启用 Red Hat Virtualization Manager 存储库	50
配置离线存储库	51
<b>附录 B. 准备本地手动配置 POSTGRESQL 数据库</b>	<b>53</b>
启用 Red Hat Virtualization Manager 存储库	53
初始化 PostgreSQL 数据库	54
<b>附录 C. 为 PCI PASSTHROUGH 配置主机</b>	<b>56</b>
<b>附录 D. 删除 RED HAT VIRTUALIZATION MANAGER</b>	<b>58</b>
<b>附录 E. 保护 RED HAT VIRTUALIZATION</b>	<b>59</b>
E.1. RED HAT LINUX 7 的 DISA STIG	59
E.2. 为 RED HAT LINUX 7 PROFILE 应用 DISA STIG	60



## 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](#)。

表 1. 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

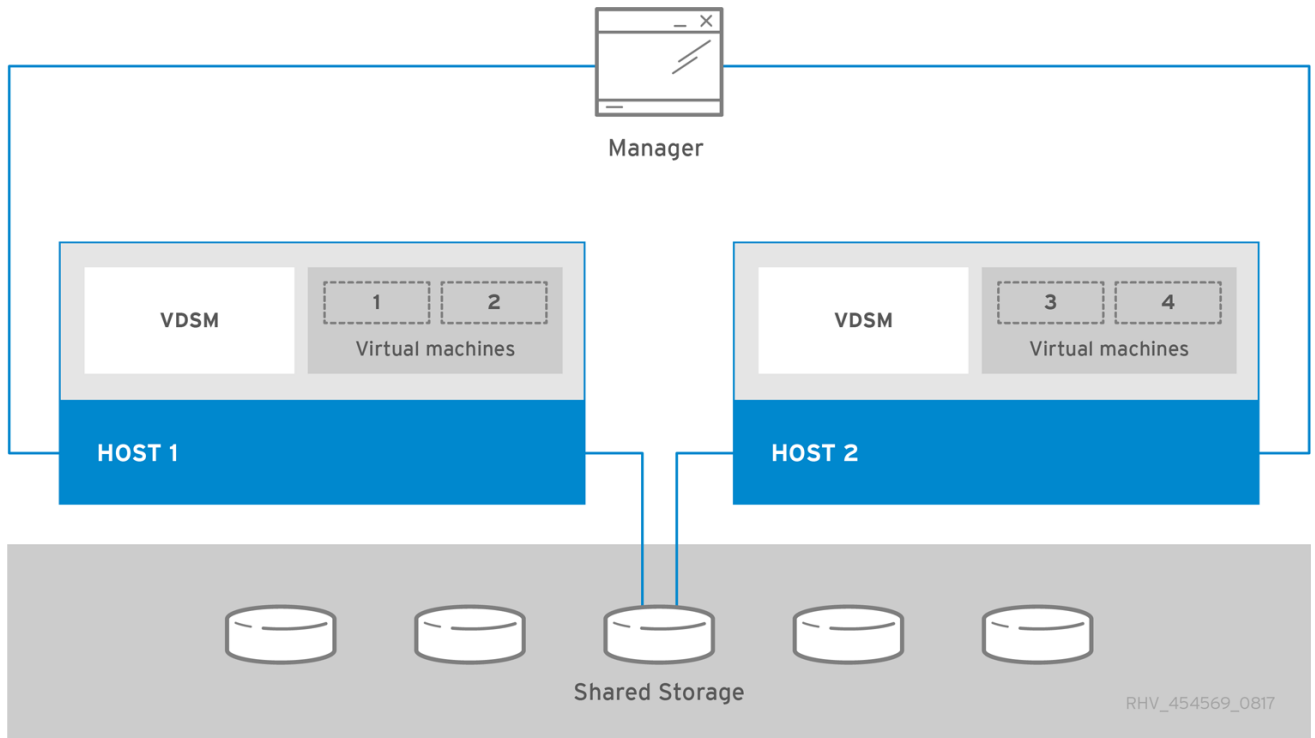
Red Hat Virtualization Manager 在物理服务器或单独虚拟化环境中托管的虚拟机上运行。单机管理器更易于部署和管理，但需要额外的物理服务器。管理器只有在外部使用产品（如红帽的高可用性附加组件）进行管理时才高度可用。

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。管理器必须在 Red Hat Enterprise Linux 7 中运行。
- 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 <https://access.redhat.com/articles/2974891>。由于对已知问题的程序错误修复会频繁发布，因此红帽建议使用调度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 <https://access.redhat.com/solutions/725243>。要确认特定的硬件项目是否已认证可与 Red Hat Enterprise Linux 一起使用，请参阅 <https://access.redhat.com/ecosystem/#certifiedHardware>。

表 2.1. Red Hat Virtualization Manager 硬件要求

资源	最小值	推荐的
CPU	双核 CPU。	四核 CPU 或多个双核 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 <a href="#">RHV Manager History Database Size Calculator</a> 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](#)。安装 **virt-viewer** 需要管理员特权。

虚拟机控制台可通过 SPICE、VNC 或 RDP（仅限 Windows）协议访问。可以在客户端操作系统中安装 QXL 图形驱动程序，以便改进/增强的 SPICE 功能。SPICE 目前支持最大分辨率 2560x1600 像素。

Red Hat Enterprise Linux、Windows XP 和 Windows 7 提供了受支持的 QXL 驱动程序。

SPICE 支持分为几个级别：

- 第 1 层：完全测试了远程查看器（Remote Viewer）并被支持的操作系统。
- 第 2 层：被部分测试的远程查看器的操作系统，可能可以正常工作。为此级的浏览器提供有限的支持。红帽工程团队将尝试修复此层上 remote-viewer 的问题。

表 2.3. 客户端操作系统 SPICE 支持

支持级别	操作系统
1 级	Red Hat Enterprise Linux 7.2 及更新的版本
	Microsoft Windows 7
2 级	Microsoft Windows 8
	Microsoft Windows 10

### 2.1.4. 操作系统要求

Red Hat Virtualization Manager 必须在 Red Hat Enterprise Linux 7 的基本安装上安装，该安装已更新至最新的次版本。

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 <https://access.redhat.com/solutions/725243>。要确认特定的硬件项目是否已认证可与 Red Hat Enterprise Linux 一起使用，请参阅 <https://access.redhat.com/ecosystem/#certifiedHardware>。

有关适用于客户机的要求和限制的详情请参考 <https://access.redhat.com/articles/rhel-limits> 和 <https://access.redhat.com/articles/906543>。

### 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
  - Haswell
  - Haswell-noTSX
  - Broadwell
  - Broadwell-noTSX
  - Skylake (client)
  - Skylake (server)
- IBM POWER8

#### 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。

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。Red Hat Virtualization Host 中每个虚拟机最多支持 4 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，红帽建议使用默认分配，这会使用更多存储空间。

- / (root) - 6 GB
- /home - 1 GB
- /tmp - 1 GB
- /boot - 1 GB
- /var - 15 GB
- /var/crash - 10 GB
- /var/log - 8 GB
- /var/log/audit - 2 GB
- swap - 1 GB（推荐的 swap 大小，请参阅 <https://access.redhat.com/solutions/15244>）
- 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。

- 最小总数 - 55 GB

如果您还安装用于自托管引擎安装的 RHV-M 设备，`/var/tmp` 必须至少为 5 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。红帽建议，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。
- 红帽建议在 PCIe 设备和 root 端口支持 ACS 间的所有 PCIe 交换机和桥接。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 7 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
- 预定义的 `mdev_type` 设置为与设备支持的其中一个 `mdev` 类型对应
- 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（也称为“Manager 机器”）的计算机或虚拟机上保持启用 IPv6。不要在 Manager 机器上禁用 IPv6，即使您的系统没有使用它。

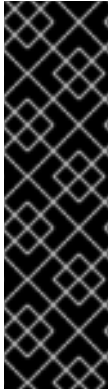
### 2.3.2. DNS、NTP、IPMI 隔离和指标存储的防火墙要求

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。
- 红帽强烈建议使用 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。

#### Metrics Store, Kibana, 和 ElasticSearch

有关 Metrics Store、Kibana 和 ElasticSearch，请参阅 [Metrics Store 虚拟机的网络配置](#)。

### 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，但如果您使用 `iptables`，则会覆盖任何已存在的防火墙配置。如果要保留现有的防火墙配置，则必须手动插入 Manager 所需的防火墙规则。`engine-setup` 命令会保存在 `/etc/ovirt-engine/iptables.example` 文件中需要的 `iptables` 规则列表。如果您使用



firewalld, engine-setup 不会覆盖现有的配置。

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 2.4. 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
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 <b>noVNC</b> 提供 websocket 代理访问。如果 websocket 代理在不同主机上运行，则不会使用此端口。	否

ID	端口	协议	源	目的地	用途	默认加密
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 <a href="#">fence_kdump 高级配置</a> 。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 (ImageIO 代理服务器)	与 ImageIO 代理通信需要此项 ( <b>ovirt-imageio-proxy</b> )。	是
M8	6442	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。

### 2.3.4. 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 <https://access.redhat.com/solutions/2772331>。



### 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. 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

ID	端口	协议	源	目的地	用途	默认加密
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)
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

ID	端口	协议	源	目的地	用途	默认加密
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
H11	54322	TCP	Red Hat Virtualization Manager (ImagelO 代理服务器)	Red Hat Virtualization 主机 Red Hat Enterprise Linux 主机	与 ImagelO 守护进程 (ovirt-imageio-daemon) 进行通信需要。	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

ID	端口	协议	源	目的地	用途	默认加密
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



### 注意

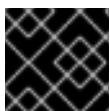
默认情况下，Red Hat Enterprise Linux 允许到任何目标地址上的 DNS 和 NTP 的出站流量。如果您禁用传出流量，请对 Red Hat Virtualization 主机进行例外处理

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 2.6. 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。

ID	端口	协议	源	目的地	用途	默认加密
D2	5432	TCP, UDP	外部系统	数据仓库 ( <b>ovirt-engine-history</b> ) 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。

## 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 7 中运行。有关安装 Red Hat Enterprise Linux 的详情，请查看 [Red Hat Enterprise Linux 7 安装指南](#)。

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，请在配置管理器前参考 [附录 A, 为 Red Hat Virtualization Manager 安装配置本地仓库](#)。

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。要设置数据库，或两者，请在配置管理器前参阅 [附录 B, 准备本地手动配置 PostgreSQL 数据库](#)。

### 3.2. 启用 RED HAT VIRTUALIZATION MANAGER 存储库

在 Red Hat Subscription Manager 中注册系统，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：

```
# yum repolist
```

#### 4. 配置存储库：

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-7-server-rpms \
  --enable=rhel-7-server-supplementary-rpms \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=rhel-7-server-rhv-4-manager-tools-rpms \
  --enable=rhel-7-server-ansible-2.9-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms
```

### 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：

```
# yum update
```



### 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。

```
# yum install rhvm
```

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

```
# engine-setup
```

- 按 **Enter** 键配置这个机器上的 Manager :

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

- (可选) 安装 Open Virtual Network(OVN)。选择 **Yes** 将在 Manager 机器上安装 OVN 中央服务器, 并将其作为外部网络提供程序添加到 Red Hat Virtualization 中。默认集群将使用 OVN 作为其默认网络提供程序, 添加的主机会自动配置为与 OVN 通信。

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

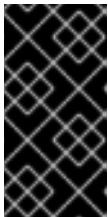
有关在 Red Hat Virtualization 中使用 OVN 网络的更多信息, 请参阅 [管理指南](#) 中的 [添加开放虚拟网络\(OVN\)作为外部网络提供程序](#)。

- (可选) 允许 **engine-setup** 配置镜像 I/O 代理(**ovirt-imageio-proxy**), 以允许 Manager 将虚拟磁盘上传到存储域。

```
Configure Image I/O Proxy on this host? (Yes, No) [Yes]:
```

- (可选) 允许 **engine-setup** 配置 websocket 代理服务器, 以便允许用户通过 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](#)。

- 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]:
```

- (可选) 允许通过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]:
```

11. **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；**iptables** 已被弃用。

```
Setup can automatically configure the firewall on this system.
Note: automatic configuration of the firewall may overwrite current settings.
NOTICE: iptables is deprecated and will be removed in future releases
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。

12. 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：

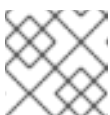
```
Where is the DWH database located? (Local, Remote) [Local]:
```

- 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。

13. 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:

14. 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:

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

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

**Both**都提供最大的灵活性。在大多数情况下，选择 **两者**。**virt** 允许您在环境中运行虚拟机；**Gluster** 仅允许从管理门户管理 GlusterFS。

16. 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:

17. 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]:

18. 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*]:

19. (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]:

20. 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]:
```

21. 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**。

22. 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。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。

23. 如果要将 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*。
24. 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* 替换为您在安装过程中提供的 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-ss0-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。

如需更多信息，请参阅 [第 4.3 节“配置主机网络的建议做法”](#)。



### 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。有关浏览器的最低要求，请查看 <http://cockpit-project.org/running.html>。

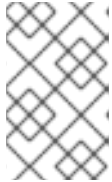
RHVH 支持 NIST 800-53 分区要求以提高安全性。RHVH 默认使用 NIST 800-53 分区布局。

主机必须满足最低[主机要求](#)。

### 流程

1. 从客户门户网站下载 RHVH ISO 镜像：
  - a. 登录到客户门户网站 <https://access.redhat.com>。
  - b. 点菜单栏中的 **Downloads**。

- c. 点 **Red Hat Virtualization**。向上滚动并点 **Download Latest** 以访问产品下载页面。
  - d. 进入 **Hypervisor Image for RHV 4.3**并点 **Download Now**。
  - e. 创建可引导介质设备。如需更多信息，请参阅 *Red Hat Enterprise Linux 安装指南*中的[复制介质](#)。
2. 启动您要安装 RHVH 的机器，从准备的安装介质启动。
  3. 在引导菜单中，选择 **Install RHVH 4.3**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。

4. 选择语言，然后点 **Continue**。
5. 从 **Date & Time** 屏幕中选择一个时区，然后点 **Done**。
6. 从键盘菜单中选择 **键盘布局**，再单击 **Done**。
7. 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

红帽强烈建议使用 **Automatically configure partitioning** 选项。

8. 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

要在每次系统引导时使用连接，选择 **Automatically connect to this network when it is available** 复选框。如需更多信息，请参阅 *Red Hat Enterprise Linux 7 安装指南*中的[编辑网络连接](#)。

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

9. （可选）配置语言支持、安全策略和 Kdump。有关安装概述界面中的每个部分的更多信息，请参阅 *Red Hat Enterprise Linux 7 安装指南*中的[使用 Anaconda 进行安装](#)。
10. 点 **Begin Installation**。
11. 设置 root 密码，并选择性地在 RHVH 安装时创建额外的用户。





### 警告

红帽建议不要在 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。

12. 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。该服务默认启用。

## 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

1. 登录位于 **https://HostFQDNorIP:9090** 的 Cockpit Web 界面。
2. 进入 **Subscriptions**，点 **Register System**，并输入您的客户门户网站用户名和密码。**Red Hat Virtualization Host** 订阅会自动附加到系统。
3. 点 **Terminal**。
4. 启用 **Red Hat Virtualization Host 7** 软件仓库，以便稍后对 Red Hat Virtualization 主机进行更新：

```
# subscription-manager repos --enable=rhel-7-server-rvh-4-rpms
```

### 将 RHVH 注册到 Red Hat Satellite 6

1. 登录位于 **https://HostFQDNorIP:9090** 的 Cockpit Web 界面。
2. 点 **Terminal**。
3. 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=rhel-7-server-rvh-4-rpms
```

## 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。红帽强烈建议在 **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 [第 2.2.3 节“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. 自动部署 Red Hat Virtualization 主机

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。

[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：

- [第 4.1.3.2.1 节 “准备安装环境”](#)
- [第 4.1.3.2.2 节 “配置 PXE 服务器和 Boot Loader”](#)
- [第 4.1.3.2.3 节 “创建并运行 Kickstart 文件”](#)

### 4.1.3.2.1. 准备安装环境

1. [登录客户门户网站](#)。
2. 点菜单栏中的 **Downloads**。
3. 点 **Red Hat Virtualization**。向上滚动并点 **Download Latest** 以访问产品下载页面。
4. 进入 **Hypervisor Image for RHV 4.3** 并点 **Download Now**。
5. 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](#)。
6. 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/rhvh
# cp /mnt/rhvh/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。

### 4.1.3.2.2. 配置 PXE 服务器和 Boot Loader

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 Boot Loader 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
```

### 4.1.3.2.3. 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
```

- 强烈推荐自动分区：

```
autopart --type=thinp
```

**注意**

精简配置必须与自动分区一起使用。

**--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 [第 4.1.3.1 节“自定义分区”](#) 了解适用于分区的限制列表以及 Kickstart 文件中的手动分区示例。

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

```
%post
nodectl init
%end
```

**在其上部署 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。

```
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
nodectl init
%end
```

**从 Satellite 部署 RHVH 的 Kickstart 示例**

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。

```
<%#
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
nodectl 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 7 的标准基本安装，并附加 **Red Hat Enterprise Linux Server** 和 **Red Hat Virtualization** 订阅。

有关具体安装说明，请参阅 [执行标准 {enterprise-linux-shortname} 安装](#)。

主机必须满足最低[主机要求](#)。



### 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

第三方 watchdog 不应安装在 Red Hat Enterprise Linux 主机上，因为它们可能会影响到 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：

```
# yum repolist
```

4. 配置存储库：

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-7-server-rpms \
  --enable=rhel-7-server-rhv-4-mgmt-agent-rpms \
  --enable=rhel-7-server-ansible-2.9-rpms
```

对于 Red Hat Enterprise Linux 7 主机、little endian、在 IBM POWER8 硬件上：

```
# subscription-manager repos \
--disable='*' \
--enable=rhel-7-server-rhv-4-mgmt-agent-for-power-le-rpms \
--enable=rhel-7-for-power-le-rpms
```

对于 Red Hat Enterprise Linux 7 主机, little endian 在 IBM POWER9 硬件上：

```
# subscription-manager repos \
--disable='*' \
--enable=rhel-7-server-rhv-4-mgmt-agent-for-power-9-rpms \
--enable=rhel-7-for-power-9-rpms
```

5. 确保当前安装的所有软件包都为最新版本：

```
# yum update
```

6. 重启机器。

### 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：

```
# yum 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

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。



红帽建议通过以下实践来配置主机网络：

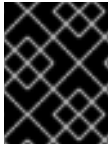
- 使用 Cockpit 配置网络。或者，您可以使用 **nmtui** 或 **nmcli**。
- 如果自托管引擎部署或将主机添加到管理器时不需要网络，请在将主机添加到管理器后在管理门户中配置网络。请参阅[在数据中心或集群中创建新逻辑网络](#)。
- 使用以下命名约定：
  - VLAN 设备：**VLAN\_NAME\_TYPE\_RAW\_PLUS\_VID\_NO\_PAD**
  - VLAN 接口：**physical\_device.VLAN\_ID** (例如 **eth0.23**, **eth1.128**, **enp3s0.50**)
  - 绑定接口：**bondnumber** (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**。详情请参阅[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](#)。

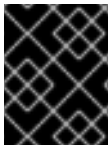


### 重要

在创建使用静态 IPv6 地址的管理网桥时，请在添加主机前禁用其接口配置(ifcfg)文件中的网络管理器控制。如需更多信息，请参阅 <https://access.redhat.com/solutions/3981311>。

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

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。




### 重要

在创建使用静态 IPv6 地址的管理网桥时，请在添加主机前禁用其接口配置(ifcfg)文件中的网络管理器控制。如需更多信息，请参阅 <https://access.redhat.com/solutions/3981311>。

### 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

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。

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。

有关设置和配置 NFS 的详情，请参考 *Red Hat Enterprise Linux 7 存储管理指南* 中的[网络文件系统 \(NFS\)](#)。

有关如何导出"NFS"共享的信息，请参阅[如何在 Red Hat Virtualization 中从 NetApp Storage / EMC SAN 导出"NFS"共享](#)

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到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。

#### 流程

1. 创建组 **kvm**：

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

2. 在组 **kvm** 中创建用户 **vdsm**：

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

3. 将导出的目录的所有权设置为 36:36，这提供了 **vdsmd:kvm** 所有权：

```
# chown -R 36:36 /exports/data
```

4. 更改目录的模式，以便所有者授予读和写访问权限，以便向组和其他用户授予读和执行权限：

■

```
# chmod 0755 /exports/data
```

## 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 *Red Hat Enterprise Linux 7 存储管理指南* 中的 [在线存储管理](#)。

### 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。详情请查看 <https://access.redhat.com/solutions/2662261>。

### 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，红帽推荐在 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

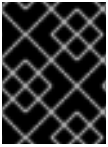
Red Hat Virtualization 通过从由预先存在的 LUN 的卷组创建存储域来支持 SAN 存储。卷组和 LUN 不可同时附加到多个存储域。

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。详情请查看 <https://access.redhat.com/solutions/2662261>。

**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，红帽推荐在 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：

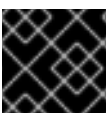
```
# cat /etc/multipath/conf.d/host.conf
multipaths {
  multipath {
    wwid boot_LUN_wwid
    no_path_retry queue
  }
}
```

## 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

可以在主机上设置本地存储域。当您将主机设置为使用本地存储时，主机会自动添加到新的数据中心，并且没有其他主机的集群可以添加到其中。多主机集群要求所有主机都能够访问所有存储域，这些存储域对本地存储不可能。在单主机集群中创建的虚拟机无法迁移、隔离或调度。

**重要**

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。红帽建议使用单独的逻辑卷或磁盘，以防止在升级过程中丢失数据。

## 为 Red Hat Enterprise Linux 主机准备本地存储

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
```

## 为 Red Hat Virtualization 主机准备本地存储

红帽建议在逻辑卷中创建本地存储，如下所示：

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，然后修改权限和所有权：

```
# mount -a
# 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 <https://access.redhat.com/articles/2356261>。

## 5.7. 为 SAN 供应商自定义多路径配置

要自定义多路径配置设置，请不要修改 **/etc/multipath.conf**。而是应该创建新的配置文件，它会覆盖 **/etc/multipath.conf**。



### 警告

升级虚拟桌面和服务器管理器(VDSM)会覆盖 **/etc/multipath.conf** 文件。如果 **multipath.conf** 包含自定义项，则覆盖它可能会触发存储问题。

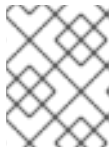
### 先决条件

- 本主题只适用于已经配置为使用多路径连接存储域的系统，带有一个 **/etc/multipath.conf** 文件。

- 不要覆盖 `user_friendly_names` 和 `find_multipaths` 设置。如需更多信息，请参阅 [ref-Recommended\\_Settings\\_for\\_Multipath.conf\\_SM\\_localDB\\_deploy](#)
- 除非存储厂商需要，否则请避免覆盖 `no_path_retry` 和 `polling_interval`。如需更多信息，请参阅 [ref-Recommended\\_Settings\\_for\\_Multipath.conf\\_SM\\_localDB\\_deploy](#)

## 流程

1. 要覆盖 `/etc/multipath.conf` 中的设置值，请在 `/etc/multipath/conf.d/` 目录中创建一个新配置文件。



### 注意

`/etc/multipath/conf.d/` 中的文件按字母顺序执行。按照文件命名惯例，在文件名称的开头加上数字。例如：`/etc/multipath/conf.d/90-myfile.conf`。

2. 将您要覆盖的设置从 `/etc/multipath.conf` 复制到 `/etc/multipath/conf.d/` 中的新配置文件。编辑设置值并保存您的更改。
3. 输入 `systemctl reload multipathd` 命令来应用新的配置设置。



### 注意

避免重启 `multipathd` 服务。这样做会在 `VDSM` 日志中生成错误。

## 验证步骤

如果您覆盖 `/etc/multipath.conf` 中的 `VDSM` 生成的设置，请验证在各种失败场景中新配置按预期执行。

例如，禁用所有存储连接。然后，一次启用一个连接，并验证存储域可以被访问。

## 故障排除

如果 Red Hat Virtualization 主机访问共享存储时遇到问题，请检查 `/etc/multipath/conf.d/` 下的 `/etc/multipath.conf` 和文件，以便与 `SAN` 不兼容的值。

## 其他资源

- RHEL 文档中的 [Red Hat Enterprise Linux DM 多路径](#)。
- 管理指南中的 [配置 iSCSI 多路径](#)。
- [如何自定义 RHVH 虚拟机监控程序上的 /etc/multipath.conf？什么值不能更改及不能更改的原因](#)，它包括一个 `multipath.conf` 示例文件，它是一个基础。

## 5.8. 推荐的 MULTIPATH.CONF 设置

在覆盖 `/etc/multipath.conf` 时，不要覆盖以下设置：

### `user_friendly_names no`

此设置会控制除了实际设备名称外，是否会将用户友好的名称分配给设备。多个主机必须使用相同的名称来访问设备。禁用此设置可防止因为使用用户友好的名称而破坏了这个要求。

### `find_multipaths no`



此设置控制 RHVH 是否在仅有一个路径可用时也会通过多路径访问所有设备。禁用此设置可防止 RHV 出现启用此设置时的一些行为。

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**。

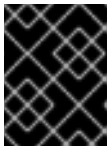
新 NFS 数据域的状态为 **Locked**，直到准备好磁盘为止。然后，数据域将自动附加到数据中心。

### 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

在环境外部使用的 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。

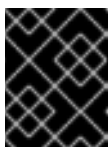
- b. 在 **Address** 字段中输入 iSCSI 主机的 FQDN 或 IP 地址。
- c. 在 **Port** 字段中，输入在浏览目标时要连接到主机的端口。默认值为 **3260**。
- d. 如果使用 CHAP 保护存储，请选中 **User Authentication** 复选框。输入 **CHAP 用户名**和 **CHAP 密码**。



### 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。

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。

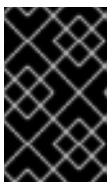
如果要将当前存储网络迁移到 iSCSI 绑定，请参阅[将逻辑网络迁移到 iSCSI Bond](#)。

### 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. 从主机下拉列表中选择**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**，因为您通常会使用 **-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

在主机中添加本地存储会将主机放置在新的数据中心和集群中。本地存储配置窗口将数据中心的创建、集群和存储合并到一个过程中。

### 流程

1. 单击 **Compute** → **Hosts**，再选择 主机。
2. 点 **Management** → **Maintenance** 并点 **OK**。
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**。

您的主机在其所在的数据中心上线。

## 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 <https://access.redhat.com/articles/2356261>。

## 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 7 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。

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

在 Red Hat Subscription Manager 中注册系统，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

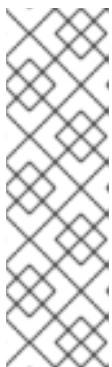
如果您使用 IPv6 网络，请使用 IPv6 转换机制来访问 Content Delivery Network 和 subscription Manager。

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：

```
# yum repolist
```

4. 配置存储库：

```
# subscription-manager repos \
--disable='*' \
--enable=rhel-7-server-rpms \
--enable=rhel-7-server-supplementary-rpms \
--enable=rhel-7-server-rhv-4.3-manager-rpms \
--enable=rhel-7-server-rhv-4-manager-tools-rpms \
--enable=rhel-7-server-ansible-2.9-rpms \
--enable=jb-eap-7.2-for-rhel-7-server-rpms
```

## 配置离线存储库

1. 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 存储库，请安装和配置 **vsftpd**：

- a. 安装 **vsftpd** 软件包：

```
# yum install vsftpd
```

- b. 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
```

- c. 在 `/var/ftp/pub/` 目录中创建一个子目录。这是下载的软件包可用位置：

```
# 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 -l -p /var/ftp/pub/rhvrepo
```

此命令会下载大量软件包，需要很长时间才能完成。`-l` 选项启用 yum 插件支持。

3. 安装 **createrepo** 软件包：

```
# yum install createrepo
```

4. 为在 `/var/ftp/pub/rhvrepo` 中下载软件包的每个子目录创建存储库元数据：

```
# for DIR in $(find /var/ftp/pub/rhvrepo -maxdepth 1 -mindepth 1 -type d); do createrepo $DIR; done
```

5. 创建仓库文件，并将其复制到您要安装 Manager 的离线机器上的 `/etc/yum.repos.d/` 目录。配置文件可以手动创建，也可以使用脚本创建。在托管该程序库的系统中运行该脚本，将 `baseurl` 中的 `ADDRESS` 替换为托管该存储库的系统的 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 [第 3.3 节“安装和配置 Red Hat Virtualization Manager”](#)。软件包是从本地存储库而不是从 Content Delivery Network 中安装的软件包。



## 附录 B. 准备本地手动配置 PostgreSQL 数据库

按照此流程使用自定义值设置 Manager 数据库或数据仓库数据库。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

在 Red Hat Subscription Manager 中注册系统，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：

```
# yum repolist
```

4. 配置存储库：

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-7-server-rpms \
  --enable=rhel-7-server-supplementary-rpms \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=rhel-7-server-rhv-4-manager-tools-rpms \
  --enable=rhel-7-server-ansible-2.9-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms
```

## 初始化 PostgreSQL 数据库

1. 安装 PostgreSQL 服务器软件包：

```
# yum install rh-postgresql10 rh-postgresql10-postgresql-contrib
```

2. 初始化 PostgreSQL 数据库，启动 **postgresql** 服务，并确保该服务在引导时启动：

```
# scl enable rh-postgresql10 -- postgresql-setup --initdb
# systemctl enable rh-postgresql10-postgresql
# systemctl start rh-postgresql10-postgresql
```

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

```
su - postgres -c 'scl enable rh-postgresql10 -- psql'
```

4. 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';
```

5. 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';
```

6. 连接到新数据库：

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

7. 添加 **uuid-osp** 扩展：

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

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

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

9. 退出 **psql** 接口：

```
database_name=# \q
```

10. 通过启用 md5 客户端身份验证来确保可以远程访问数据库。编辑 `/var/opt/rh/rh-postgresql10/lib/pgsql/data/pg_hba.conf` 文件，并在文件底部以 `local` 开头的行立即添加以下行，将 `X.X.X.X` 替换为 Manager 或 Data Warehouse 机器的 IP 地址，将 `0-32` 或 `0-128` 替换为 CIDR 掩码长度：

```
host database_name user_name X.X.X.X/0-32 md5
host database_name user_name X.X.X.X::/0-128 md5
```

11. 更新 PostgreSQL 服务器配置。编辑 `/var/opt/rh/rh-postgresql10/lib/pgsql/data/postgresql.conf` 文件，并将以下行添加到文件的底部：

```
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
```

12. 重启 `postgresql` 服务：

```
# systemctl restart rh-postgresql10-postgresql
```

13. 另外，还可使用 <http://www.postgresql.org/docs/10/static/ssl-tcp.html#SSL-FILE-USAGE> 中的说明将 SSL 设置为安全数据库连接。

返回到 [第 3.3 节“安装和配置 Red Hat Virtualization Manager”](#)，并在询问数据库时回答 **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

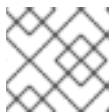
- 确保主机硬件满足 PCI 设备直通和分配的要求。如需更多信息，请参阅[PCI 设备要求](#)。

### 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 `intel_iommu=on` 或 `amd_iommu=on` 可以正常工作，您可以尝试添加 `iommu=pt` 或 `amd_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，则恢复为上一选项。

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
```

要启用 SR-IOV 并将专用虚拟 NIC 分配给虚拟机，请参阅 <https://access.redhat.com/articles/2335291>。

## 附录 D. 删除 RED HAT VIRTUALIZATION MANAGER

您可以使用 **engine-cleanup** 命令删除 Red Hat Virtualization Manager 的特定组件或所有组件。



### 注意

总是自动创建 Manager 数据库和 PKI 密钥的压缩存档和配置。这些文件保存在 **/var/lib/ovirt-engine/backups/** 下，并分别在相应的文件名中包含 **engine-** 和 **engine-pki-** 数据。

### 流程

1. 在 Manager 机器中运行以下命令：

```
# engine-cleanup
```

2. 系统将提示您删除所有 Red Hat Virtualization Manager 组件：

- 输入 **Yes** 并按 **Enter** 删除所有组件：

```
Do you want to remove all components? (Yes, No) [Yes]:
```

- 键入 **No**，然后按 **Enter** 键选择要删除的组件。您可以选择单独保留或删除每个组件：

```
Do you want to remove Engine database content? All data will be lost (Yes, No) [No]:
```

```
Do you want to remove PKI keys? (Yes, No) [No]:
```

```
Do you want to remove PKI configuration? (Yes, No) [No]:
```

```
Do you want to remove Apache SSL configuration? (Yes, No) [No]:
```

3. 您会给另一个机会更改您的想法，并取消删除 Red Hat Virtualization Manager。如果选择继续，则 **ovirt-engine** 服务将停止，并且根据您选择的选项删除您的环境配置。

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

```
ovirt-engine is about to be removed, data will be lost (OK, Cancel) [Cancel]:OK
```

4. 删除 Red Hat Virtualization 软件包：

```
# yum remove rhvm* vdsm-bootstrap
```

## 附录 E. 保护 RED HAT VIRTUALIZATION

此主题包括如何保护 Red Hat Virtualization 的有限信息。此信息随着时间的推移会增加。

这些信息特定于 Red Hat Virtualization，它不包括与以下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

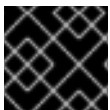
### 先决条件

- 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。
- 部署 RHEL 主机前，请参阅 Red Hat Enterprise Linux [安全指南](#)。

## E.1. RED HAT LINUX 7 的 DISA STIG

国防信息系统局(DISA)为各种平台和操作系统发布安全技术实施指南(STIG)。

安装 Red Hat Virtualization 主机 (RHVH) 时，**DISA STIG for Red Hat Linux 7**是可用的安全策略之一。在安装过程中启用此配置集不再需要重新生成 SSH 密钥、SSL 证书，或者稍后在部署过程中重新配置主机。



### 重要

DISA STIG 安全策略是红帽官方测试和认证的唯一安全策略。

DISA STIG 是 DOD IA 和支持 IA 的设备/系统的配置标准自 1998 年以来，DISA 通过提供安全技术实施指南 (STIG) 在增强国防部安全系统的安全形象方面发挥了重要作用。STIG 含有有关"锁定"信息系统/软件的技术指导，否则可能容易遭受恶意计算机攻击"。

这些 STIG 基于国家标准与技术协会 (NIST) 800-53 提出的要求，这是美国联邦信息系统安全控制目录（美国联邦信息系统除外）。

要确定哪些配置文件重叠，红帽指的是云安全联盟的云控制矩阵(CCM)。此 CCM 指定一组全面的云安全控制，并将每一控制映射到领先标准、最佳实践和法规的要求。

为了帮助您验证安全策略，红帽为各种红帽平台（包括 RHEL 和 RHV）提供了 OpenSCAP 工具和安全内容自动化协议 (SCAP) 配置集。

红帽的 OpenSCAP 项目为管理员和审计员提供开源工具，用于评估、测量和执行 SCAP 基准。NIST 于 2014 年向 OpenSCAP 授予 SCAP 1.2 认证。

NIST 维护 SCAP 标准。SCAP 兼容配置集提供有关设置操作系统和应用程序安全配置的详细低级别指导。

红帽将各种产品和平台的 SCAP 基准发布到两个位置：

- NIST 国家检查清单 (NCP)，是公开提供的安全检查清单（或基准测试）美国政府存储库。
- Department of Defense (DoD) Cyber Exchange

#### 其他资源

- [红帽的 NIST 国家检查计划存储库](#)
- [Unix/Linux 相关 STIG 的国防部 Exchange 下载页面](#)
- [NIST 特殊发布 800-53 Rev. 4](#)
- [NIST 特殊发布 800-53 Rev. 5 \(DRAFT\)](#)
- [OpenSCAP 项目](#)
- [云安全联盟：云控制列表](#)

## E.2. 为 RED HAT LINUX 7 PROFILE 应用 DISA STIG

本节介绍如何在安装 Red Hat Virtualization (RHV) 管理器 ("Manager")、Red Hat Virtualization 主机 (RHVH) 和 Red Hat Enterprise Linux 主机时为 *Red Hat Linux 7 安全配置集* 启用 DISA STIG。

### 为 RHVH Red Hat Linux 7 启用 DISA STIG

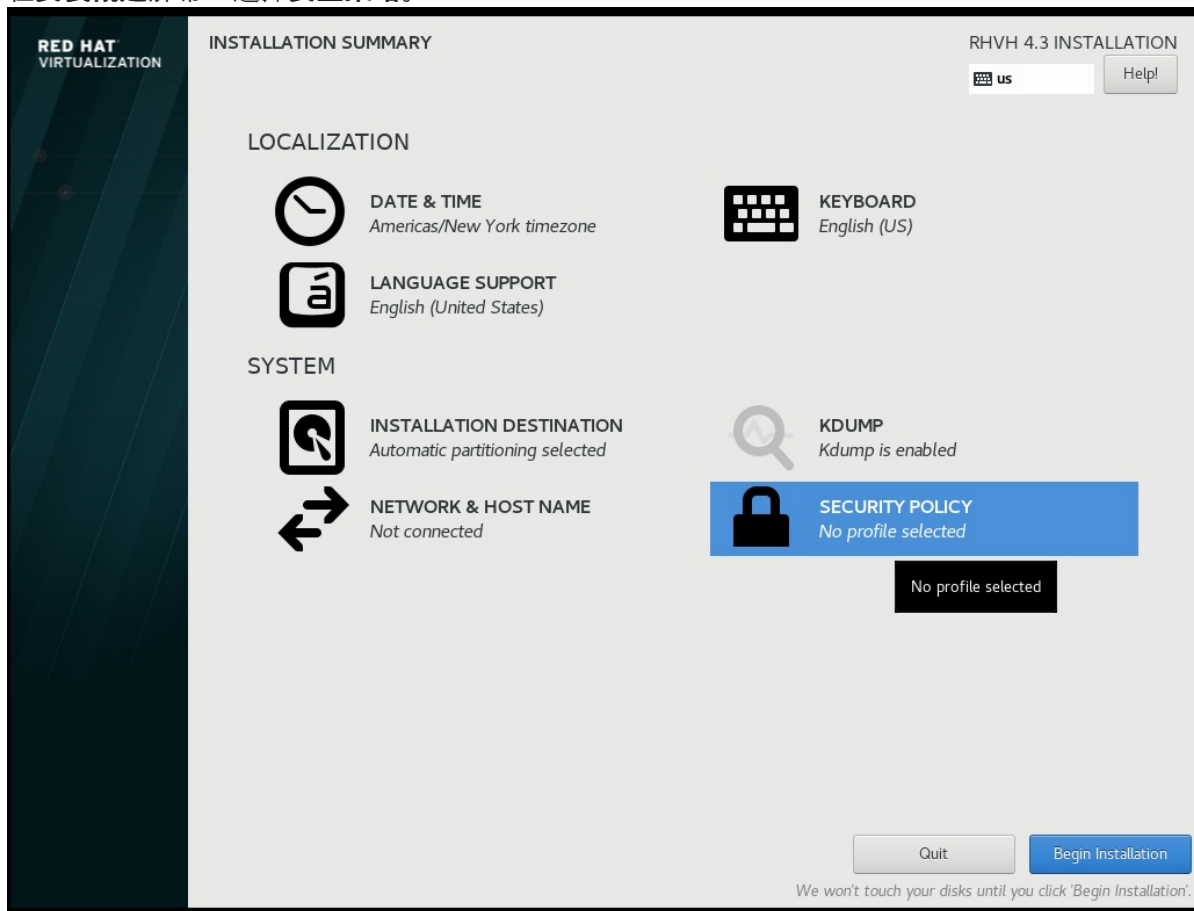
以下流程适用于为两个不同的目的安装 Red Hat Virtualization Host (RHVH)：

- 将 Manager 部署为自托管引擎时，使用 RHVH 作为 Manager 虚拟机的宿主。
- 在 RHV 集群中将 RHVH 用作普通主机。

如果您使用 Anaconda 安装程序安装 RHVH:



1. 在安装概述屏幕上选择安全策略。

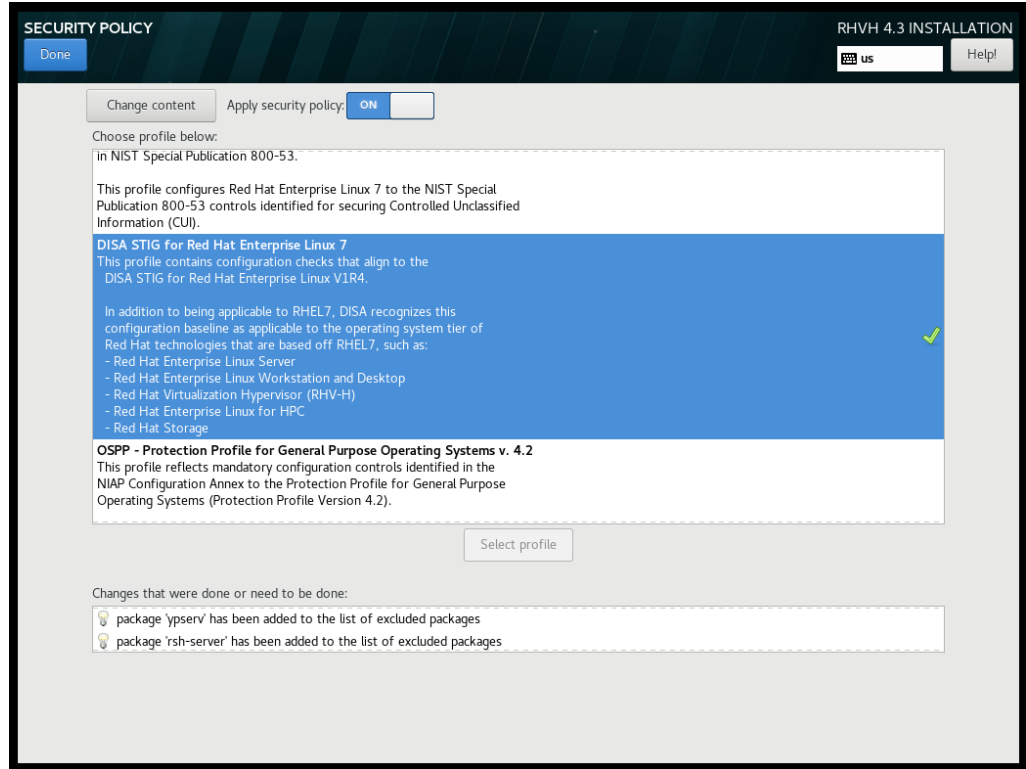


2. 在打开的 Security Policy 屏幕上，将 Apply security policy 设置切换为 On。
3. 在 profiles 滚动列表中选择 DISA STIG for Red Hat Linux 7
4. 点 Select profile 按钮。此操作在配置集旁边添加一个绿色勾号，并将软件包添加到已完成或需要完成的更改列表中。



### 注意

这些软件包已经是 RHVH 镜像的一部分。RHVH 作为单一系统镜像提供。安装不属于 RHVH 镜像的其他所选安全配置集所需的软件包可能无法安装。有关所含软件包的列表，请参阅 RHVH 软件包清单。



5. 点 Done。
6. 在安装概述屏幕上，验证 Security Policy 的状态是否为 Everything。

7. 稍后，当您登录 RHVH 时，命令行会显示以下信息。

```
You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls)
to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE
or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or services
by attorneys, psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See User
Agreement for details.

localhost login:
```



### 注意

如果您使用命令行将 RHV 部署为自托管引擎，在一系列提示中输入 **ovirt-hosted-engine-setup** 后的，您会被提问 **Do you want to apply a default OpenSCAP security profile?** 输入 **Yes**，并按照说明选择 *DISA STIG for Red Hat Linux 7* 配置集。

### 其他资源

- [在安装过程中配置和应用 SCAP 策略](#)