



Red Hat Virtualization 4.4

管理指南

Red Hat Virtualization 中的管理任务

Red Hat Virtualization 4.4 管理指南

Red Hat Virtualization 中的管理任务

Red Hat Virtualization Documentation Team

Red Hat Customer Content Services

rhev-docs@redhat.com

法律通告

Copyright © 2023 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

本文档提供与 Red Hat Virtualization 管理员相关的信息和程序。

目录

第 1 章 管理和维护 RED HAT VIRTUALIZATION	4
1.1. 全局配置	4
1.2. DASHBOARD	26
1.3. 搜索	31
1.4. 书签	46
1.5. TAGS	47
第 2 章 管理资源	50
2.1. 服务质量	50
2.2. DATA CENTERS	55
2.3. 集群	61
2.4. 逻辑网络	85
2.5. 主机	139
2.6. 存储	192
2.7. 池	243
2.8. 虚拟磁盘	259
2.9. 外部供应商	279
第 3 章 管理环境	299
3.1. 管理自托管引擎	299
3.2. 备份和迁移	311
3.3. 使用 RED HAT SATELLITE 设置勘误查看	384
3.4. 在证书过期前续订证书	385
3.5. 使用 ANSIBLE 自动化配置任务	387
3.6. 用户和角色	390
3.7. 配额和服务等级协议政策	432
3.8. 事件通知	441
3.9. 工具	454
第 4 章 收集有关环境的信息	475
4.1. 监控和可观察性	475
4.2. 日志文件	485
附录 A. VDSM 服务和 HOOK	494
A.1. 安装 VDSM HOOK	494
A.2. 支持的 VDSM 事件	495
A.3. VDSM HOOK 环境	497
A.4. VDSM HOOK 域 XML 对象	498
A.5. 定义自定义属性	498
A.6. 设置虚拟机自定义属性	500
A.7. 在 VDSM HOOK 中评估虚拟机自定义属性	501
A.8. 使用 VDSM HOOKING 模块	501
A.9. VDSM HOOK 执行	502
A.10. VDSM HOOK 返回代码	503
A.11. VDSM HOOK 示例	503
附录 B. 自定义网络属性	506
B.1. BRIDGE_OPTS 参数的说明	506
B.2. 如何设置 RED HAT VIRTUALIZATION MANAGER 以使用 ETHTOOL	507
B.3. 如何设置 RED HAT VIRTUALIZATION MANAGER 以使用 FCOE	508
附录 C. RED HAT VIRTUALIZATION USER INTERFACE PLUGINS	510
C.1. ABOUT RED HAT VIRTUALIZATION USER INTERFACE PLUG-INS	510

C.2. RED HAT VIRTUALIZATION USER INTERFACE PLUGIN LIFECYCLE	510
C.3. 用户界面插件相关的文件和位置	512
C.4. 用户界面插件部署示例	513
附录 D. 在 RED HAT VIRTUALIZATION 中启用 FIPS	515
D.1. 在自托管引擎中启用 FIPS	515
D.2. 在 RHV 主机和独立管理器中启用 FIPS	516
D.3. 其他资源	516
附录 E. RED HAT VIRTUALIZATION 和加密通信	517
E.1. 替换 RED HAT VIRTUALIZATION MANAGER CA 证书	517
E.2. 在 MANAGER 和 LDAP 服务器间设置加密通信	521
E.3. 为 FIPS 启用加密的 VNC 控制台	523
附录 F. 代理	528
F.1. SPICE 代理	528
F.2. SQUID PROXY	530
F.3. WEBSOCKET 代理	534
附录 G. BRANDING	535
G.1. BRANDING	535
附录 H. 系统帐户	540
H.1. RED HAT VIRTUALIZATION MANAGER USER ACCOUNTS	540
H.2. RED HAT VIRTUALIZATION MANAGER GROUPS	540
H.3. 虚拟化主机用户帐户	540
H.4. 虚拟化主机组	541
附录 I. 法律通知	543

第 1 章 管理和维护 RED HAT VIRTUALIZATION

Red Hat Virtualization 环境需要管理员保持它的运行。作为管理员，您的任务包括：

- 管理物理和虚拟资源，如主机和虚拟机。这包括升级和添加主机、导入域、转换外部虚拟机监控程序 (hypervisors) 上创建的虚拟机，以及管理虚拟机池。
- 监控整体系统资源以了解潜在的问题，如其中一个主机上高负载、内存或磁盘空间不足，以及执行任何必要的操作（例如，将虚拟机迁移到其他主机，以通过关闭机器减少负载或释放资源）。
- 响应对虚拟机的新要求（例如，升级操作系统或分配更多内存）。
- 使用标签管理自定义对象属性。
- 管理保存为公共书签的搜索。
- 管理用户设置和设置权限级别。
- 为特定用户或虚拟机提供整体系统功能的故障排除。
- 生成常规和特定报告。

1.1. 全局配置

通过单击 **Administration → Configure**，**Configure** 窗口允许您为 Red Hat Virtualization 环境配置多个全局资源，如用户、角色、系统权限、调度策略、实例类型和 MAC 地址池。此窗口允许您自定义用户与环境中资源交互的方式，并为配置可应用到多个集群的选项提供一个中央位置。

1.1.1. 角色

角色是可从 Red Hat Virtualization Manager 配置的预定义权限集。角色提供对数据中心中不同级别资源以及特定物理和虚拟资源的访问权限和管理权限。

通过多级管理，适用于容器对象的任何权限也适用于该容器中的所有单个对象。例如，当主机管理员角色分配给特定主机上的用户时，该用户将获得执行任何可用主机操作的权限，但只能在分配的主机上获得。但是，如果主机管理员角色分配给数据中心上的用户，该用户将获得在数据中心集群中的所有主机上执行主机操作的权限。

1.1.1.1. 创建新角色

如果您需要的角色不在 Red Hat Virtualization 的默认角色列表中，您可以创建新角色并对其进行自定义以满足您的需要。

流程

1. 单击 **Administration → Configure**。这将打开 **Configure** 窗口。默认情况下会选择 **Roles** 选项卡，显示默认用户和管理员角色以及任何自定义角色的列表。
2. 单击 **New**。
3. 输入新角色的名称和描述。
4. 选择 **Admin** 或 **User** 作为帐户类型。

5. 使用 **Expand All** 或 **Collapse All** 按钮，在 **Check Boxes to Allow Action** 列表中查看所列对象的一个或多个权限。您还可以扩展或折叠每个对象的选项。
6. 对于每个对象，为您要设置的角色选择或清除您想要允许的操作或拒绝的操作。
7. 单击**确定**以应用更改。新角色显示在角色列表中。

1.1.1.2. 编辑或复制角色

您可以更改已创建角色的设置，但无法更改默认角色。要更改默认角色，请克隆并修改它们以符合您的要求。

流程

1. 单击 **Administration** → **Configure**。这将打开 **Configure** 窗口，其中显示默认用户和管理员角色以及任何自定义角色的列表。
2. 选择您要更改的角色。
3. 点 **Edit** 或 **Copy**。这将打开 **Edit Role** 或 **Copy Role** 窗口。
4. 如有必要，编辑角色的 **Name** 和 **Description**。
5. 使用 **Expand All** 或 **Collapse All** 按钮查看列出对象的一个或多个权限。您还可以扩展或折叠每个对象的选项。
6. 对于每个对象，选择或清除您希望允许或拒绝您要编辑的角色的操作。
7. 单击 **OK** 以应用您所做的更改。

1.1.1.3. 用户角色和授权示例

以下示例演示了如何使用本章中描述的授权系统的不同功能，针对各种场景应用授权控制。

例 1.1. 集群权限

Sarah 是公司帐户部门的系统管理员。她所在部门的所有虚拟资源都在一个称为 **Accounts** 的 Red Hat Virtualization **集群**。她被分配了 accounts 集群上的 **ClusterAdmin** 角色。这使她能够管理集群中的所有虚拟机，因为虚拟机是集群的子对象。管理虚拟机包括编辑、添加或删除磁盘等虚拟资源，以及执行快照。这些权限并不允许她管理此集群之外的任何资源。由于 **ClusterAdmin** 是管理员角色，因此它允许她使用管理门户或虚拟机门户来管理这些资源。

例 1.2. VM PowerUser 权限

John 是财务部门的软件开发人员。他使用虚拟机来构建和测试其软件。Sarah 已为他创建了一个名为 **johndesktop** 的虚拟桌面。John 被分配了 **johndesktop** 虚拟机上的 **UserVmManager** 角色。这允许他使用虚拟机门户访问此单一虚拟机。由于他具有 **UserVmManager** 权限，因此可以修改虚拟机。由于 **UserVmManager** 是用户角色，因此不允许他使用管理门户。

例 1.3. 数据中心 Power 用户角色权限

Penelope 是办事处经理。除了她自己的职责外，她偶尔还帮助人力资源经理完成各种任务，如安排访谈和跟进参考检查。根据公司政策，Penelope 需要使用特定的应用程序来完成招聘任务。

虽然 Penelope 拥有自己的机器来执行办公室管理任务，但她希望创建单独的虚拟机来运行该规范应用。为她被分配了新虚拟机的数据中心的 **PowerUserRole** 权限。这是因为要创建新虚拟机，她需要在数据中心内对多个组件进行更改，包括在存储域中创建虚拟磁盘。

请注意，这与为 Penelope 分配 **DataCenterAdmin** 权限不同。作为数据中心的 **PowerUser**，Penelope 可以登录虚拟机门户，并对数据中心内的虚拟机执行特定于虚拟机的操作。她无法执行数据中心级别的操作，如将主机或存储附加到数据中心。

例 1.4. 网络管理员权限

Chris 担任 IT 部门的网络管理员。她的日常职责包括创建、操作和删除部门 Red Hat Virtualization 环境中的网络。对于她的角色，她需要资源以及每个资源的网络上的管理权限。例如，如果 Chris 对 IT 部门的数据中心具有 **NetworkAdmin** 权限，她可以在数据中心中添加和删除网络，并为属于数据中心的所有虚拟机附加和分离网络。

例 1.5. 自定义角色权限

Rachel 在 IT 部门工作，负责管理 Red Hat Virtualization 中的用户帐户。她需要添加用户帐户并为它们分配适当的角色和权限的权限。她不会自行使用任何虚拟机，并且不应有权管理主机、虚拟机、集群或数据中心。没有向她提供这一特定权限集的内置角色。必须创建自定义角色，以定义适合 Rachel 位置的权限集合。

图 1.1. UserManager 自定义角色

The screenshot shows a 'New Role' dialog box with the following configuration:

- Name:** UserManager
- Description:** (empty)
- Account Type:** Admin (selected)
- Check Boxes to Allow Action:**
 - Expand All
 - Collapse All
 - System
 - Configure System
 - Manipulate Users
 - Manipulate Permissions
 - Add users and groups from directory while adding permissions
 - Manipulate Roles
 - Login Permissions
 - Tag management Permissions
 - Bookmark management Permissions

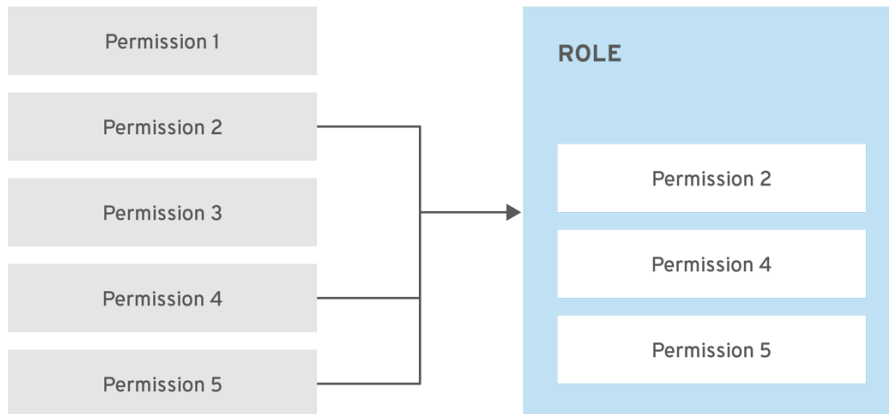
- Buttons:** OK, Reset, Cancel

上面显示的 **UserManager** 自定义角色允许操作用户、权限和角色。这些操作在 **System** - 层次结构中显示的顶层对象下 [进行组织](#)。这意味着它们应用到系统的所有其他对象。该角色设置为帐户类型为 **Admin**。这意味着，当她被分配了此角色时，Rachel 可以同时使用管理门户和虚拟机门户。

1.1.2. 系统权限

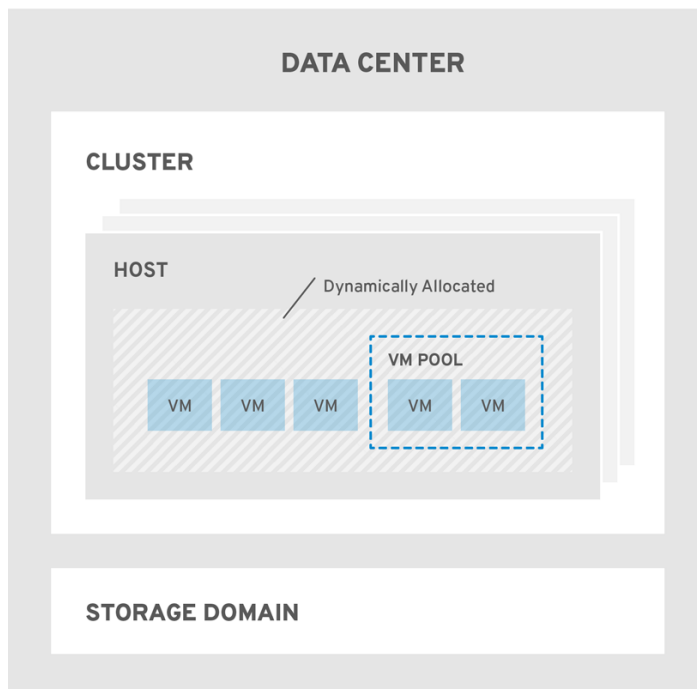
权限允许用户对对象执行操作，其中对象可以是单个对象或容器对象。适用于容器对象的任何权限也适用于该容器的所有成员。

图 1.2. 权限和角色



RHV_453537_0219

图 1.3. Red Hat Virtualization 对象层次结构



RHV_453537_0219

1.1.2.1. 用户属性

角色和权限是用户的属性。角色是预定义的特权集合，允许访问不同级别的物理和虚拟资源。多级管理提供了精细的权限层次。例如，数据中心管理员具有管理数据中心所有对象的权限，而主机管理员则对单个物理主机具有系统管理员权限。一个用户可以具有使用单一虚拟机的权限，但不会对虚拟机配置进行任何更改，而另一用户则可分配给虚拟机的系统权限。

1.1.2.2. 用户和管理员角色

Red Hat Virtualization 提供一系列预配置的角色，从具有系统范围权限的管理员到有权访问单个虚拟机的最终用户。虽然您无法更改或删除默认角色，但您可以克隆和自定义它们，或者根据您的要求创建新角色。角色有两种类型：

- Administrator 角色：允许使用管理门户来管理物理和虚拟资源。管理员角色限制要在虚拟机门户中执行的操作的权限；但是，它不涉及用户在虚拟机门户中可以看到的内容。
- 用户角色：允许使用虚拟机门户来管理和访问虚拟机和模板。用户角色决定了用户在虚拟机门户中可以看到的内容。授予具有管理员角色的用户的权限反映在虚拟机门户中可供该用户使用的操作中。

1.1.2.3. 用户角色介绍

下表描述了基本用户角色，这些角色授予在虚拟机门户中访问和配置虚拟机的权限。

表 1.1. Red Hat Virtualization 用户角色 - 基础

角色	权限	备注
UserRole	可以访问和使用虚拟机和池。	可以登录虚拟机门户，使用分配的虚拟机和池，查看虚拟机状态和详细信息。
PowerUserRole	可以创建和管理虚拟机和模板。	使用 Configure 窗口，或针对特定数据中心或集群，将这个角色应用到整个环境的用户。例如，如果在数据中心级别上应用 PowerUserRole，PowerUser 可以在数据中心中创建虚拟机和模板。
UserVmManager	虚拟机的系统管理员。	可以管理虚拟机并创建和使用快照。在虚拟机门户中创建虚拟机的用户会自动被分配机器上的 UserVmManager 角色。

下表描述了高级用户角色，允许您进一步微调虚拟机门户中的资源的权限。

表 1.2. Red Hat Virtualization 用户角色 - 高级

角色	权限	备注
UserTemplateBasedVm	有限的权限，仅能使用模板。	可以使用模板创建虚拟机。
DiskOperator	虚拟磁盘用户。	可以使用、查看和编辑虚拟磁盘。继承使用虚拟磁盘所附加虚拟机的权限。

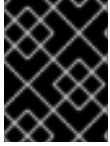
角色	权限	备注
VmCreator	可以在虚拟机门户中创建虚拟机。	此角色不适用于特定的虚拟机；使用 Configure 窗口将此角色应用到整个环境的用户。另外，也可以将此角色应用到特定的数据中心或集群。当将此角色应用到集群时，还必须对整个数据中心或特定存储域应用 DiskCreator 角色。
TemplateCreator	可以在分配的资源内创建、编辑、管理和删除虚拟机模板。	此角色不适用于特定的模板；使用 Configure 窗口将此角色应用到整个环境的用户。另外，也可以将这个角色应用到特定的数据中心、集群或存储域。
DiskCreator	可以在分配的集群或数据中心内创建、编辑、管理和移除虚拟磁盘。	此角色不适用于特定的虚拟磁盘；使用 Configure 窗口将此角色应用到整个环境的用户。另外，也可以将这个角色应用到特定的数据中心或存储域。
TemplateOwner	可以编辑和删除模板，为模板分配和管理用户权限。	此角色自动分配给创建模板的用户。其他对模板没有 TemplateOwner 权限的用户无法查看或使用模板。
VnicProfileUser	虚拟机和模板的逻辑网络和网络接口用户。	可以将网络接口从特定逻辑网络附加或分离。

1.1.2.4. 管理员角色已说明

下表描述了基本管理员角色，这些角色授予访问管理门户中配置资源的权限。

表 1.3. Red Hat Virtualization 系统管理员角色 - 基础

角色	权限	备注
SuperUser	Red Hat Virtualization 环境的系统管理员。	具有所有对象和级别的完全权限，可以管理所有数据中心中的所有对象。
ClusterAdmin	集群管理员。	拥有特定集群下所有对象的管理权限。
DataCenterAdmin	数据中心管理员。	拥有特定数据中心下除存储之外的所有对象的管理权限。



重要

不要将目录服务器的管理用户用作 Red Hat Virtualization 管理用户。在目录服务器中创建一个用户，专门用于 Red Hat Virtualization 管理用户。

下表描述了高级管理员角色，允许您对管理门户中的资源的权限进行进一步微调。

表 1.4. Red Hat Virtualization 系统管理员角色 - 高级

角色	权限	备注
TemplateAdmin	虚拟机模板的管理员。	可以创建、删除和配置模板的存储域和网络详细信息，并在域之间移动模板。
StorageAdmin	存储管理员。	可以创建、删除、配置和管理分配的存储域。
HostAdmin	主机管理员。	可以连接、删除、配置和管理特定主机。
NetworkAdmin	网络管理员。	可以配置和管理特定数据中心或集群的网络。数据中心或集群的网络管理员继承集群中虚拟池的网络权限。
VmPoolAdmin	虚拟池系统管理员。	可以创建、删除和配置虚拟池；分配和删除虚拟池用户；可以对池中的虚拟机执行基本操作。
GlusterAdmin	Gluster 存储管理员。	可以创建、删除、配置和管理 Gluster 存储卷。
VmImporterExporter	导入和导出虚拟机的管理员。	可以导入和导出虚拟机。能够查看其他用户导出的所有虚拟机和模板。

1.1.2.5. 将管理员或用户角色分配给资源

将管理员或用户角色分配到资源，以允许用户访问或管理该资源。

流程

1. 查找并单击资源名称。这会打开详情视图。
2. 单击 **Permissions** 选项卡，以列出分配的用户、每个用户的角色以及所选资源的继承权限。
3. 点 **Add**。
4. 在搜索文本框中输入现有用户的名称或用户名，然后单击 **Go**。从生成的可能匹配项列表中选择用户。
5. 从 **Role to Assign** 下拉列表中选择角色。

6. 点击 **OK**。

用户现在为该资源启用了该角色的继承权限。

重要

避免将全局权限分配给集群等资源的常规用户，因为权限由系统层次结构中较低资源自动继承。设置 **UserRole** 以及对特定资源（如虚拟机、池或虚拟机池）的所有其他用户角色权限，特别是后者。

分配全局权限可能会导致两个问题，因为权限继承：

- 普通用户可自动获得控制虚拟机池的权限，即使管理员分配权限并非有意这样做。
- 虚拟机门户可能会与池意外发生。

因此，强烈建议仅对特定资源设置 **UserRole** 和所有其他用户角色权限，特别是虚拟机池资源，而不设置其他资源从中继承权限的资源。

1.1.2.6. 从资源中删除管理员或用户角色

从资源中删除管理员或用户角色；用户丢失与该资源的角色关联的继承权限。

流程

1. 查找并单击资源名称。这会打开详情视图。
2. 单击 **Permissions** 选项卡，以列出分配的用户、用户的角色以及所选资源的继承权限。
3. 选择要从资源中删除的用户。
4. 单击 **Remove**。
5. 点击 **OK**。

1.1.2.7. 管理系统权限

作为 **SuperUser**，系统管理员可以管理管理门户的所有方面。可以为其他用户分配更具体的管理角色。这些受限管理员角色可用于授予用户管理特权，以限制它们仅具有特定资源。例如，**DataCenterAdmin** 角色仅对分配的数据中心具有管理员特权，但该数据中心的存储除外，**ClusterAdmin** 则仅对分配的群集具有管理员特权。

数据中心管理员仅仅是特定数据中心的系统管理角色。这在具有多个数据中心（每个数据中心需要管理员）的虚拟化环境中非常有用。**DataCenterAdmin** 角色是一种分层模型；分配了数据中心管理员角色的用户可以管理数据中心中的所有对象，但该数据中心的存储除外。使用标题栏中的 **Configure** 按钮，为环境中所有数据中心分配数据中心管理员。

数据中心管理员角色允许执行以下操作：

- 创建和删除与数据中心关联的集群。
- 添加和删除与数据中心关联的主机、虚拟机和池。
- 编辑与数据中心关联的虚拟机的用户权限。

**注意**

您只能将角色和权限分配给现有用户。

您可以通过删除现有系统管理员并添加新系统管理员来更改数据中心的系统管理员。

1.1.2.8. 数据中心管理员角色说明**数据中心权限角色**

下表描述了适用于数据中心管理的管理员角色和特权。

表 1.5. Red Hat Virtualization 系统管理员角色

角色	权限	备注
DataCenterAdmin	数据中心管理员	可以使用、创建、删除、管理特定数据中心内的所有物理和虚拟资源，但存储除外，包括集群、主机、模板和虚拟机。
NetworkAdmin	网络管理员	可以配置和管理特定数据中心的网络。数据中心的网络管理员还继承数据中心内虚拟机的网络权限。

1.1.2.9. 管理系统权限

作为 **SuperUser**，系统管理员可以管理管理门户的所有方面。可以为其他用户分配更具体的管理角色。这些受限管理员角色可用于授予用户管理特权，以限制它们仅具有特定资源。例如，**DataCenterAdmin** 角色仅对分配的数据中心具有管理员特权，但该数据中心的存储除外，**ClusterAdmin** 则仅对分配的群集具有管理员特权。

集群管理员仅是特定集群的系统管理角色。这在具有多个集群的数据中心中很有用，每个集群都需要系统管理员。**ClusterAdmin** 角色是一种层次结构模型：被分配了集群管理员角色的用户可以管理群集中的所有对象。使用标题栏中的 **Configure** 按钮，为环境中所有群集分配集群管理员。

集群管理员角色允许执行以下操作：

- 创建和删除关联的集群。
- 添加和删除与集群关联的主机、虚拟机和池。
- 编辑与集群关联的虚拟机的用户权限。

**注意**

您只能将角色和权限分配给现有用户。

您还可以删除现有系统管理员并添加新系统管理员来更改集群的系统管理员。

1.1.2.10. 集群管理员角色已说明**集群权限角色**

下表描述了适用于集群管理的管理角色和特权。

表 1.6. Red Hat Virtualization 系统管理员角色

角色	权限	备注
ClusterAdmin	Cluster Administrator	<p>可以使用、创建、删除、管理特定集群中的所有物理和虚拟资源，包括主机、模板和虚拟机。可以在集群中配置网络属性，如指定显示网络，或者将网络标记为必需或非必需网络。</p> <p>但是，ClusterAdmin 没有从集群附加或分离网络的权限，因此需要 NetworkAdmin 权限。</p>
NetworkAdmin	网络管理员	<p>可以配置和管理特定群集的网络。集群的网络管理员还继承集群中虚拟机的网络权限。</p>

1.1.2.11. 管理系统权限

作为 **SuperUser**，系统管理员可以管理管理门户的所有方面。可以为其他用户分配更具体的管理角色。这些受限管理员角色可用于授予用户管理特权，以限制它们仅具有特定资源。例如，**DataCenterAdmin** 角色仅对分配的数据中心具有管理员特权，但该数据中心的存储除外，**ClusterAdmin** 则仅对分配的群集具有管理员特权。

网络管理员是一种系统管理角色，可应用于特定网络，或数据中心、群集、主机、虚拟机或模板上的所有网络。网络用户可以执行有限的管理角色，如在特定虚拟机或模板上查看和附加网络。您可以使用标题栏中的 **Configure** 按钮为环境中的所有网络分配网络管理员。

网络管理员角色允许执行以下操作：

- 创建、编辑和删除网络。
- 编辑网络的配置，包括配置端口镜像。
- 在资源（包括集群和虚拟机）上附加和分离网络。

系统会自动为创建网络的用户分配所创建网络上的 **NetworkAdmin** 权限。您还可以删除现有管理员并添加新管理员来更改网络的管理员。

1.1.2.12. 网络管理员和用户角色说明

网络权限角色

下表描述了适用于网络管理的管理员、用户角色和特权。

表 1.7. Red Hat Virtualization 网络管理员和用户角色

角色	权限	备注
----	----	----

角色	权限	备注
NetworkAdmin	数据中心、集群、主机、虚拟机或模板的网络管理员。系统会自动为创建网络的用户分配所创建网络上的 NetworkAdmin 权限。	可以配置和管理特定数据中心、集群、主机、虚拟机或模板的网络。数据中心或集群的网络管理员继承集群中虚拟池的网络权限。要在虚拟机网络上配置端口镜像，请在网络上应用 NetworkAdmin 角色，并在虚拟机上应用 UserVmManager 角色。
VnicProfileUser	虚拟机和模板的逻辑网络和网络接口用户。	可以将网络接口从特定逻辑网络附加或分离。

1.1.2.13. 管理系统权限

作为 **SuperUser**，系统管理员可以管理管理门户的所有方面。可以为其他用户分配更具体的管理角色。这些受限管理员角色可用于授予用户管理特权，以限制它们仅具有特定资源。例如，**DataCenterAdmin** 角色仅对分配的数据中心具有管理员特权，但该数据中心的存储除外，**ClusterAdmin** 则仅对分配的群集具有管理员特权。

主机管理员仅仅是特定主机的系统管理角色。这在有多个主机的集群中很有用，每个主机都需要系统管理员。您可以使用标题栏中的 **Configure** 按钮为环境中所有主机分配主机管理员。

主机管理员角色允许执行以下操作：

- 编辑主机的配置。
- 设置逻辑网络。
- 删除主机。

您还可以删除现有系统管理员并添加新系统管理员来更改主机的系统管理员。

1.1.2.14. 主机管理员角色已说明

主机权限角色

下表描述了适用于主机管理的管理角色和特权。

表 1.8. Red Hat Virtualization 系统管理员角色

角色	权限	备注
HostAdmin	主机管理员	可以配置、管理和删除特定主机。还可以在特定主机上执行网络相关的操作。

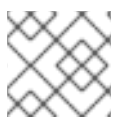
1.1.2.15. 为存储域管理系统权限

作为 **SuperUser**，系统管理员可以管理管理门户的所有方面。可以为其他用户分配更具体的管理角色。这些受限管理员角色可用于授予用户管理特权，以限制它们仅具有特定资源。例如，**DataCenterAdmin** 角色仅对分配的数据中心具有管理员特权，但该数据中心的存储除外，**ClusterAdmin** 则仅对分配的群集具有管理员特权。

存储管理员只是特定存储域的系统管理角色。这在具有多个存储域的数据中心中很有用，每个存储域都需要系统管理员。使用标题栏中的 **Configure** 按钮，为环境中所有存储域分配存储管理员。

存储域管理员角色允许执行以下操作：

- 编辑存储域的配置。
- 将存储域移至维护模式。
- 删除存储域。



注意

您只能将角色和权限分配给现有用户。

您还可以删除现有系统管理员并添加新系统管理员来更改存储域的系统管理员。

1.1.2.16. 存储管理员角色已说明

存储域权限角色

下表描述了适用于存储域管理的管理角色和特权。

表 1.9. Red Hat Virtualization 系统管理员角色

角色	权限	备注
StorageAdmin	存储管理员	可以创建、删除、配置和管理特定的存储域。
GlusterAdmin	Gluster 存储管理员	可以创建、删除、配置和管理 Gluster 存储卷。

1.1.2.17. 为虚拟机池管理系统权限

作为 **SuperUser**，系统管理员可以管理管理门户的所有方面。可以为其他用户分配更具体的管理角色。这些受限管理员角色可用于授予用户管理特权，以限制它们仅具有特定资源。例如，**DataCenterAdmin** 角色仅对分配的数据中心具有管理员特权，但该数据中心的存储除外，**ClusterAdmin** 则仅对分配的群集具有管理员特权。

虚拟机池管理员是数据中心中虚拟机池的系统管理角色。此角色可以应用到特定的虚拟机池、数据中心或整个虚拟化环境；这对于允许不同的用户管理某些虚拟机池资源非常有用。

虚拟机池管理员角色允许执行以下操作：

- 创建、编辑和删除池。
- 将虚拟机从池中添加和分离。

**注意**

您只能将角色和权限分配给现有用户。

1.1.2.18. 虚拟机池管理员角色说明**池权限角色**

下表描述了适用于池管理的管理角色和特权。

表 1.10. Red Hat Virtualization 系统管理员角色

角色	权限	备注
VmPoolAdmin	虚拟池的系统管理员角色.	可以创建、删除和配置虚拟池，分配和删除虚拟池用户，以及对虚拟机执行基本操作。
ClusterAdmin	Cluster Administrator	可以使用、创建、删除、管理特定集群中的所有虚拟机池。

1.1.2.19. 为虚拟磁盘管理系统权限

作为 **SuperUser**，系统管理员可以管理管理门户的所有方面。可以为其他用户分配更具体的管理角色。这些受限管理员角色可用于授予用户管理特权，以限制它们仅具有特定资源。例如，**DataCenterAdmin** 角色仅对分配的数据中心具有管理员特权，但该数据中心的存储除外，**ClusterAdmin** 则仅对分配的群集具有管理员特权。

Red Hat Virtualization Manager 提供两个默认虚拟磁盘用户角色，但没有默认的虚拟磁盘管理员角色。其中一个用户角色 **DiskCreator** 角色允许从虚拟机门户管理虚拟磁盘。此角色可应用于特定的虚拟机、数据中心、特定存储域或整个虚拟化环境；这对于允许不同的用户管理不同的虚拟资源非常有用。

虚拟磁盘创建者角色允许执行以下操作：

- 创建、编辑和删除与虚拟机或其他资源关联的虚拟磁盘。
- 编辑虚拟磁盘的用户权限。

**注意**

您只能将角色和权限分配给现有用户。

1.1.2.20. 虚拟磁盘用户角色已说明**虚拟磁盘用户权限角色**

下表描述了适用于在虚拟机门户中使用和管理虚拟磁盘的用户角色和特权。

表 1.11. Red Hat Virtualization 系统管理员角色

角色	权限	备注
----	----	----

角色	权限	备注
DiskOperator	虚拟磁盘用户。	可以使用、查看和编辑虚拟磁盘。继承使用虚拟磁盘所附加虚拟机的权限。
DiskCreator	可以在分配的集群或数据中心内创建、编辑、管理和移除虚拟磁盘。	此角色不适用于特定的虚拟磁盘；使用 Configure 窗口将此角色应用到整个环境的用户。另外，也可以将这个角色应用到特定的数据中心、集群或存储域。

1.1.2.20.1. 设置传统 SPICE 密码

SPICE 控制台默认使用 FIPS 兼容加密和密码字符串。默认的 SPICE 密码字符串为：
kECDHE+FIPS:kDHE+FIPS:kRSA+FIPS:!eNULL:!aNULL:!aNULL

此字符串通常已足够。但是，如果您的虚拟机具有较旧的操作系统或 SPICE 客户端，其中一个或另一个不支持 FIPS 兼容的加密，则必须使用更弱的密码字符串。否则，如果您在现有集群中安装新集群或新主机并尝试连接到该虚拟机，则可能会出现连接安全错误。

您可以使用 Ansible playbook 更改密码字符串。

更改密码字符串

1. 在 Manager 计算机上，在 **/usr/share/ovirt-engine/playbooks** 目录中创建文件。例如：

```
# vim /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

2. 在文件中输入以下内容并保存它：

```
name: oVirt - setup weaker SPICE encryption for old clients
hosts: hostname
vars:
  host_deploy_spice_cipher_string: 'DEFAULT:-RC4:-3DES:-DES'
roles:
  - ovirt-host-deploy-spice-encryption
```

3. 运行您刚才创建的文件：

```
# ansible-playbook -i hostname /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

或者，您可以使用带有变量 **host_deploy_spice_cipher_string** 的 **--extra-vars** 选项的 Ansible playbook **ovirt-host-deploy** 重新配置主机：

```
# ansible-playbook -i hostname \
--extra-vars host_deploy_spice_cipher_string="DEFAULT:-RC4:-3DES:-DES" \
/usr/share/ovirt-engine/playbooks/ovirt-host-deploy.yml
```

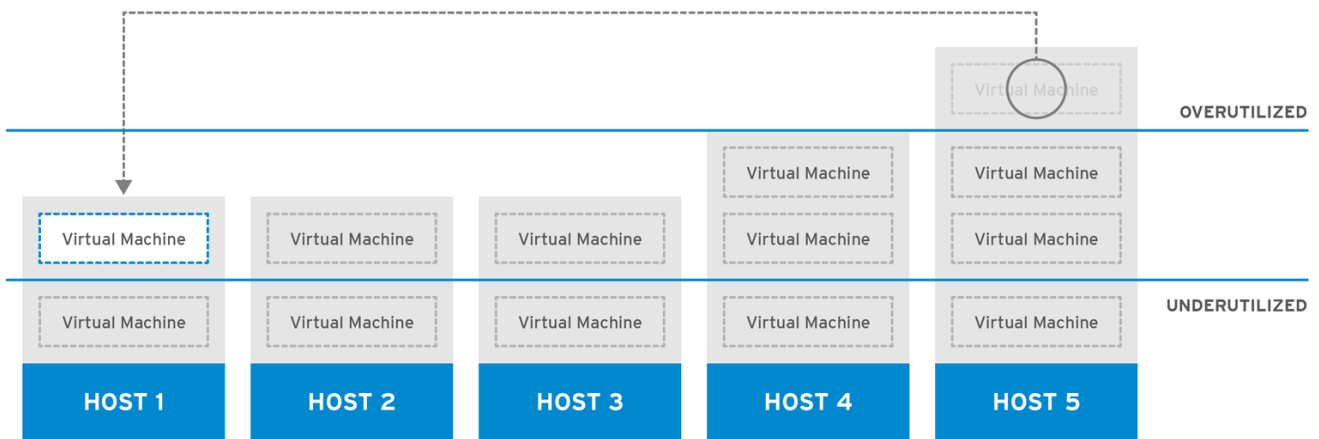
1.1.3. 调度策略

调度策略是一组规则，用于定义在群集中应用调度策略的主机之间分发虚拟机的逻辑。调度策略通过过滤器、权重和负载均衡策略的组合来确定此逻辑。过滤器模块应用硬实施，并过滤掉不符合该过滤器指定条件的主机。weights 模块应用软实施，用于控制决定集群中可以运行虚拟机的主机时所考虑因素的相对优先级。

Red Hat Virtualization Manager 提供了五种默认的调度策略：**Evenly_Distributed**, **Cluster_Maintenance**, **None**, **Power_Saving**, 和 **VM_Evenly_Distributed**。您还可以定义新的调度策略，对虚拟机的分发提供精细的控制。无论调度策略如何，虚拟机都不会在 CPU 过载的主机上启动。默认情况下，如果主机的 CPU 的负载超过 80% 达到 5 分钟，则主机 CPU 被视为过载，但这些值可以使用调度策略来更改。如需有关每个调度策略属性的更多信息，请参阅 [管理指南](#) 中的 [调度策略](#)。

如需有关调度策略的工作方式的详细信息，请参阅 [集群调度策略如何工作？](#)

图 1.4. 平均分布式调度策略

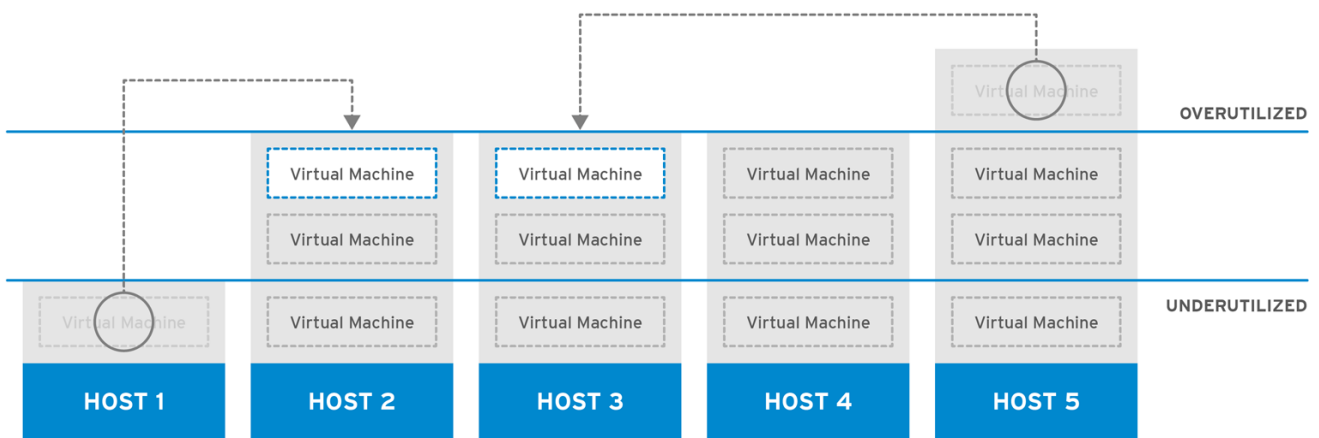


RHV_ 444396_0417

Evenly_Distributed 调度策略在集群中的所有主机上平均分配内存和 CPU 处理负载。如果主机已达到定义的 **CpuOverCommitDurationMinutes**、**HighUtilization**、**VCpuToPhysicalCpuRatio** 或 **MaxFreeMemoryForOverUtilized**，则附加到主机的其他虚拟机将不会启动。

VM_Evenly_Distributed 调度策略根据虚拟机的数量在主机之间均匀分布虚拟机。如果任何主机运行的虚拟机数量超过 **HighVmCount**，且至少有一个主机具有超出 **MigrationThreshold** 范围的虚拟机数，则该集群被视为未平衡。

图 1.5. 节能调度策略



RHV_ 444396_0417

Power_Saving 调度策略在可用主机子集之间分配内存和 CPU 处理负载，以减少利用率不足的主机上的功耗。CPU 负载低于低利用率值的主机将超过定义的时间间隔，将所有虚拟机迁移到其他主机，以便将其关闭。如果主机已达到定义的高利用率值，则附加到主机的其他虚拟机将不会启动。

将 **None** 策略设置为主机之间没有用于运行虚拟机的负载或电源共享。这是默认的模式。当虚拟机启动时，内存和 CPU 处理负载会在集群中的所有主机上均匀分布。如果主机已达到定义的 **CpuOverCommitDurationMinutes**、**HighUtilization** 或 **MaxFreeMemoryForOverUtilized**，则附加到主机的其他虚拟机将不会启动。

Cluster_Maintenance 调度策略在维护任务期间限制集群中的活动。设置 **Cluster_Maintenance** 策略时，除了高可用性虚拟机外，无法启动新的虚拟机。如果发生主机故障，高可用性虚拟机将正确重新启动，任何虚拟机都可以迁移。

1.1.3.1. 创建调度策略

您可以创建新的调度策略，以控制将虚拟机分布到 Red Hat Virtualization 环境中的给定集群中的逻辑。

流程

1. 单击 **Administration** → **Configure**。
2. 单击调度策略选项卡。
3. 单击 **New**。
4. 输入调度策略的 **Name** 和 **Description**。
5. 配置过滤器模块：
 - a. 在 **Filter Modules** 部分中，将要应用到 **Disabled Filters** 部分中的调度策略的首选过滤器模块拖放到 **Enabled Filters** 部分中。
 - b. 也可以将特定过滤器模块设置为**第一个**，被赋予最高优先级（或 **Last**），从而获得最低的优先级，以进行基本的优化。要设置优先级，请右键单击任何过滤器模块，将光标悬停在位置上，然后选择 **First** 或 **Last**。
6. 配置权重模块：
 - a. 在 **Weights** 模块部分中，将应用于 **Disabled Weights** 部分的首选权重模块拖放到 **Enabled Weights & Factors** 部分。
 - b. 使用已启用的权重模块左侧的 **+** 和 **-** 按钮来增加或减少这些模块的权重。
7. 指定负载平衡策略：
 - a. 从 **Load Balancer** 部分的下拉菜单中选择要应用到调度策略的负载平衡策略。
 - b. 从 **Properties** 部分的下拉菜单中，选择要应用到调度策略的负载平衡属性，并使用该属性右侧的文本字段来指定值。
 - c. 使用 **+** 和 **-** 按钮来添加或删除其他属性。
8. 单击 **OK**。

1.1.3.2. 新调度策略和编辑调度策略窗口中的设置说明

下表详述了新建调度策略和编辑调度策略窗口中可用的选项。

表 1.12. 新调度策略和编辑调度策略设置

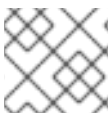
字段名称	Description
Name	调度策略的名称。这是用于引用 Red Hat Virtualization Manager 中的调度策略的名称。
Description	调度策略的描述信息。建议使用此字段，但不强制设置。
Filter Modules	<p>用于控制集群中虚拟机可以运行的主机的一组过滤器。启用过滤器将过滤不满足该过滤器指定条件的主机，如下所示：</p> <ul style="list-style-type: none"> ● ClusterInMaintenance：在没有为高可用性配置的主机上启动虚拟机会过滤出主机。 ● CpuPinning：无法满足 CPU 固定定义的主机。 ● 迁移：防止迁移到同一主机。 ● CPUOverloaded：CPU 用量高于定义的 CpuOverCommitDurationMinutes 阈值（间隔由 CpuOverCommitDurationMinutes 定义）的主机。 ● PinToHost：虚拟机要固定到的主机以外的主机。 ● CPU-Level：不符合虚拟机的 CPU 拓扑的主机。 ● VmAffinityGroups：不满足为虚拟机定义的关联性规则的主机。 ● NUMA：没有 NUMA 节点的主机，可在资源方面容纳虚拟机 vNUMA 节点。 ● InClusterUpgrade：运行的操作系统版本早于当前运行虚拟机的主机。 ● MDevice：不提供所需介质设备(mDev)的主机。 ● memory：没有足够的内存来运行虚拟机的主机。 ● CPU：CPU 数量少于分配给虚拟机的主机。 ● HostedEnginesSpares：在指定数量的自托管引擎节点上为管理器虚拟机保留空间。 ● 交换：在阈值中不交换的主机。 ● 虚拟机租用就绪：不支持配置有存储租期的虚拟机的主机。 ● VmToHostsAffinityGroups：不符合关联性组成员虚拟机指定条件的主机组。例如，关联性组中的虚拟机必须在组中的一个

字段名称	Description 主机上运行，或者在组中排除的独立主机上运行。
	<ul style="list-style-type: none"> ● HostDevice : 不支持虚拟机所需主机设备的主机。 ● HA : 将管理器虚拟机置于自托管引擎环境中，使其仅在具有良好高可用性分数的主机上运行。 ● Emulated-Machine: 不支持适当模拟计算机的主机。 ● hugepages : 不满足虚拟机内存所需数量的 Huge Pages 的主机。 ● migration-Tsc-Frequency : 没有虚拟机的主机与当前运行虚拟机的主机相同。 ● Network: 未在其上安装虚拟机的网络接口控制器所需的网络的主机，或者没有安装集群的显示网络。 ● Label: 没有所需关联性标签的主机。 ● Compatibility-Version : 不支持正确的集群兼容性版本的主机。
Weights Modules	<p>用于控制在决定虚拟机可以运行集群中的主机时所考虑因素的相对优先级的一组权重。</p> <ul style="list-style-type: none"> ● VmAffinityGroups : 根据为虚拟机定义的关联性组，Weights 主机。此权重模块根据该关联性组的参数，确定关联性组中虚拟机将如何在同一主机或单独的主机上运行。 ● InClusterUpgrade: Weight 主机根据其操作系统版本而有所不同。权重使具有较早操作系统的主机数量超过与当前运行虚拟机所运行的主机相同的操作系统的主机。这可确保始终将优先级提供给具有后续操作系统的主机。 ● OptimalForCpuEvenDistribution : 根据 CPU 使用率了解主机，并根据 CPU 使用率低的主机提供优先级。 ● CPU 用于高性能虚拟机 : 请参考虚拟机的数量或数量相等的插槽、内核和线程的主机。 ● HA : 根据主机的高可用性分数来放置主机。 ● OptimalForCpuPowerSaving: Weights hosts 根据 CPU 使用率增加，为具有更高 CPU 用量的主机赋予优先级。 ● OptimalForMemoryPowerSaving: 根据内存使用情况，为可用内存较低的主机赋予优先级。 ● CPU 和 NUMA 固定兼容性 : 根据固定兼容性，确保主机安全.当虚拟机同时定义了

字段名称	Description
	<p>vNUMA 和固定时，这个权重模块会优先考虑 CPU 固定 CPU 固定的主机。</p> <ul style="list-style-type: none"> ● VmToHostsAffinityGroups : 根据为虚拟机定义的关联性组，Weights 主机。此权重模块决定了关联性组中虚拟机在组中某一台主机上运行或独立于组的独立主机上运行的可能性。 ● OptimalForEvenGuestDistribution : 根据这些主机上运行的虚拟机数量，Weights 主机。 ● OptimalForHaReservation : 根据主机的高可用性分数。 ● OptimalForMemoryEvenDistribution : 根据内存使用情况，为具有更高可用内存的主机赋予优先级。 ● Fit VM to single host NUMA node: 根据虚拟机是否适合单一 NUMA 节点对主机进行权重。当虚拟机没有定义 vNUMA 时，这种权重模块会优先选择将虚拟机适合单一物理 NUMA 的主机。 ● PreferredHosts : 首选主机在虚拟机设置期间具有优先级。
Load Balancer	此下拉菜单允许您选择要应用的负载均衡模块。负载均衡模块决定了用于将虚拟机从高使用量较高的主机迁移到利用率较低的主机的逻辑。
Properties	此下拉菜单允许您为负载均衡模块添加或删除属性，并且仅在您为调度策略选择负载均衡模块时才可用。默认情况下不定义任何属性，可用的属性特定于所选的负载均衡模块。使用 + 和 - 按钮向负载均衡模块添加或删除其他属性。

1.1.4. 实例类型

实例类型可用于定义虚拟机的硬件配置。创建或编辑虚拟机时选择实例类型将自动填写硬件配置字段。这使得用户可以使用相同硬件配置创建多个虚拟机，而无需手动填写每个字段。



注意

对实例类型的支持现已弃用，并将在以后的发行版本中删除。



下表中所示，默认提供了一组预定义的实例类型：

表 1.13. 预定义的实例类型

Name	内存	VCPU
tiny	512 MB	1

Name	内存	VCPU
small	2 GB	1
Medium	4 GB	2
Large	8 GB	2
xlarge	16 GB	4

管理员还可以从 **Configure** 窗口的 **Instance Types** 选项卡创建、编辑和删除实例类型。

新虚拟机和**编辑虚拟机**窗口中绑定到实例类型的字段旁边有一个链链接镜像 ()。如果更改了其中一个字段的值，则虚拟机将从实例类型分离，更改为 **Custom**，并且链会出现中断()。但是，如果值被更改回，链将重新链接，实例类型将移回所选类型。

1.1.4.1. 创建实例类型

管理员可以创建新的实例类型，用户可在创建或编辑虚拟机时选择这些类型。

流程

1. 单击 **Administration** → **Configure**。
2. 单击 **Instance Types** 选项卡。
3. 单击 **New**。
4. 输入实例类型的 **Name** 和 **Description**。
5. 单击 **Show Advanced Options**，再根据需要配置实例类型的设置。**New Instance Type** 窗口中出现的设置与 **New Virtual Machine** 窗口中出现的设置相同，但仅与相关字段相同。请参阅 *虚拟机管理指南* 中的 **新虚拟机和编辑虚拟机 Windows 中的设置说明**。
6. 单击 **OK**。

新实例类型将显示在 **Configure** 窗口中的 **Instance Types** 选项卡中，可以在创建或编辑虚拟机时从 **Instance Type** 下拉列表中选择。

1.1.4.2. 编辑实例类型

管理员可以从 **Configure** 窗口编辑现有的实例类型。

流程

1. 单击 **Administration** → **Configure**。
2. 单击 **Instance Types** 选项卡。
3. 选择要编辑的实例类型。
4. 点 **Edit**。

5. 根据需要更改设置。
6. 点击 **OK**。

实例类型的配置已更新。创建基于此实例类型的新虚拟机时，或者更新基于此实例类型的现有虚拟机时，会应用新的配置。

基于此实例类型的现有虚拟机将显示标记为链图标 的字段，该字段将更新。如果现有虚拟机在实例类型发生更改时正在运行，则它们旁边将显示 orange Pending Changes 图标，并且在下次重启时将更新链图标 的字段。

1.1.4.3. 删除实例类型

流程

1. 单击 **Administration** → **Configure**。
2. 单击 **Instance Types** 选项卡。
3. 选择要删除的实例类型。
4. 单击 **Remove**。
5. 如果任何虚拟机都基于要删除的实例类型，则将显示一个警告窗口，列出附加的虚拟机。若要继续删除实例类型，可选中 **Approve Operation** 复选框。否则，单击 **取消**。
6. 点击 **OK**。

实例类型从 **Instance Types** 列表中删除，在创建新虚拟机时无法再使用。任何附加到已移除实例类型的虚拟机现在都将附加到自定义（无实例类型）。

1.1.5. MAC 地址池

MAC 地址池定义为每个集群分配的 MAC 地址范围。为每个集群指定一个 MAC 地址池。通过使用 MAC 地址池，Red Hat Virtualization 可以自动生成 MAC 地址并为新的虚拟网络设备分配，这有助于防止 MAC 地址重复。当与集群相关的所有 MAC 地址都超出所分配的 MAC 地址池的范围时，MAC 地址池的内存池会提高内存效率。

同一 MAC 地址池可由多个集群共享，但每个集群分配了一个 MAC 地址池。Red Hat Virtualization 创建默认 MAC 地址池，并在未分配其他 MAC 地址池时使用。有关为集群分配 MAC 地址池的更多信息，[请参阅创建新集群](#)。



注意

如果多个 Red Hat Virtualization 集群共享一个网络，则不要只依赖默认的 MAC 地址池，因为每个集群的虚拟机都将尝试使用相同的 MAC 地址范围，从而导致冲突。为避免 MAC 地址冲突，请检查 MAC 地址池范围，以确保为每个集群分配唯一的 MAC 地址范围。

MAC 地址池分配返回到池的最后一个地址之后的下一个可用 MAC 地址。如果范围中没有剩余地址，则搜索将从范围的开头重新开始。如果有多个 MAC 地址范围中定义了可用 MAC 地址，则范围将以与选择可用 MAC 地址相同的方式为传入的请求提供服务。

1.1.5.1. 创建 MAC 地址池

您可以创建新的 MAC 地址池。

流程

1. 单击 **Administration → Configure**。
2. 单击 **MAC Address Pools** 选项卡。
3. 点 **Add**。
4. 输入新 MAC 地址池的**名称和描述**。
5. 选中 **Allow Duplicates** 复选框，以允许池中多次使用 MAC 地址。MAC 地址池不会自动使用重复的 MAC 地址，但启用重复选项意味着用户可以手动使用重复的 MAC 地址。



注意

如果一个 MAC 地址池被禁用，并且另一个 MAC 地址启用了重复，则池中可以多次使用重复项并禁用重复，但可以在启用了重复功能的池中多次使用。

6. 输入所需的 **MAC Address Ranges**。若要输入多个范围，可单击 **From** 和 **To** 字段旁边的加号按钮。
7. 单击 **OK**。

1.1.5.2. 编辑 MAC 地址池

您可以编辑 MAC 地址池来更改详细信息，包括池中可用的 MAC 地址范围以及是否允许重复。

流程

1. 单击 **Administration → Configure**。
2. 单击 **MAC Address Pools** 选项卡。
3. 选择要编辑的 MAC 地址池。
4. 点 **Edit**。
5. 根据需要更改 **Name, Description, Allow Duplicates**, 和 **MAC Address Ranges** 字段。



注意

更新 MAC 地址范围时，不会重新分配现有 NIC 的 MAC 地址。已分配但位于新 MAC 地址范围之外的 MAC 地址作为用户指定的 MAC 地址添加，仍然由 MAC 地址池跟踪。

6. 单击 **OK**。

1.1.5.3. 编辑 MAC 地址池权限

创建 MAC 地址池后，您可以编辑其用户权限。用户权限控制哪些数据中心可以使用 MAC 地址池。有关添加新用户权限的更多信息，请参阅 [角色](#)。

流程

1. 单击 **Administration** → **Configure**。
2. 单击 **MAC Address Pools** 选项卡。
3. 选择所需的 MAC 地址池。
4. 编辑 MAC 地址池的用户权限：
 - 在 MAC 地址池中添加用户权限：
 - a. 在 **Configure** 窗口底部的用户权限窗格中，单击 **Add**。
 - b. 搜索并选择所需用户。
 - c. 从 **Role to Assign** 下拉列表中选择所需的角色。
 - d. 单击 **确定** 以添加用户权限。
 - 从 MAC 地址池删除用户权限：
 - a. 在 **Configure** 窗口底部的用户权限窗格中，选择要删除的用户权限。
 - b. 单击 **Remove** 以删除用户权限。

1.1.5.4. 删除 MAC 地址池

如果池没有与集群关联，您可以删除创建的 MAC 地址池，但无法删除默认的 MAC 地址池。

流程

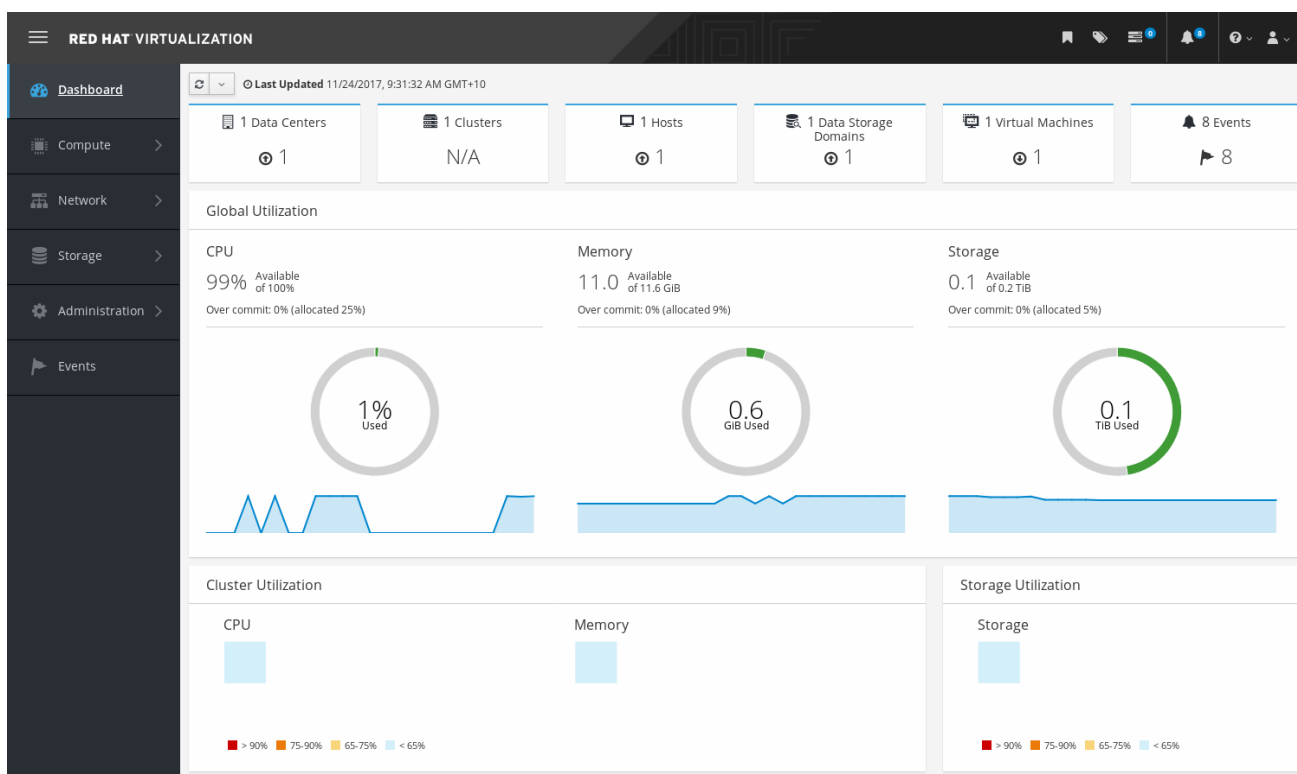
1. 单击 **Administration** → **Configure**。
2. 单击 **MAC Address Pools** 选项卡。
3. 选择要删除的 MAC 地址池。
4. 单击 **Remove**。
5. 单击 **OK**。

1.2. DASHBOARD

控制面板通过显示 Red Hat Virtualization 资源及利用率的概要来提供 Red Hat Virtualization 系统状态的概述。此概述可能会提醒您问题，并允许您分析问题区域。

默认情况下，仪表板中的信息会从 Data Warehouse 每 15 分钟更新一次，Manager API 默认每 15 秒更新一次，或者每当仪表板被刷新时。当用户从另一个页面更改或手动刷新时，控制面板会被刷新。控制面板不会自动刷新。库存卡信息由 Manager API 提供，利用率信息则由数据仓库提供。控制面板是作为 UI 插件组件实施的，与 Manager 一起自动安装和升级。

图 1.6. 控制面板



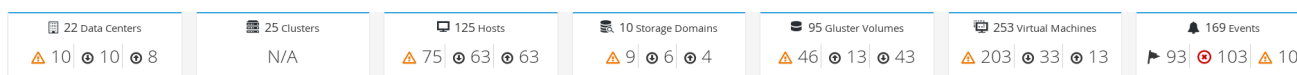
1.2.1. 前提条件

控制面板要求安装和配置数据仓库。请参阅 [数据仓库指南](#) 中的 [安装和配置数据仓库](#)。

1.2.2. 全局清单

控制面板的顶部部分提供 Red Hat Virtualization 资源的全局清单，包括数据中心、集群、主机、存储域、虚拟机和事件的项。图标显示每个资源的状态，数字则显示具有该状态的每个资源的数量。

图 1.7. 全局清单



标题显示资源类型的数量，其状态显示在标题下方。单击资源标题可导航到 Red Hat Virtualization Manager 中的相关页面。**集群的状态始终显示为 N/A。**

表 1.14. 资源状态

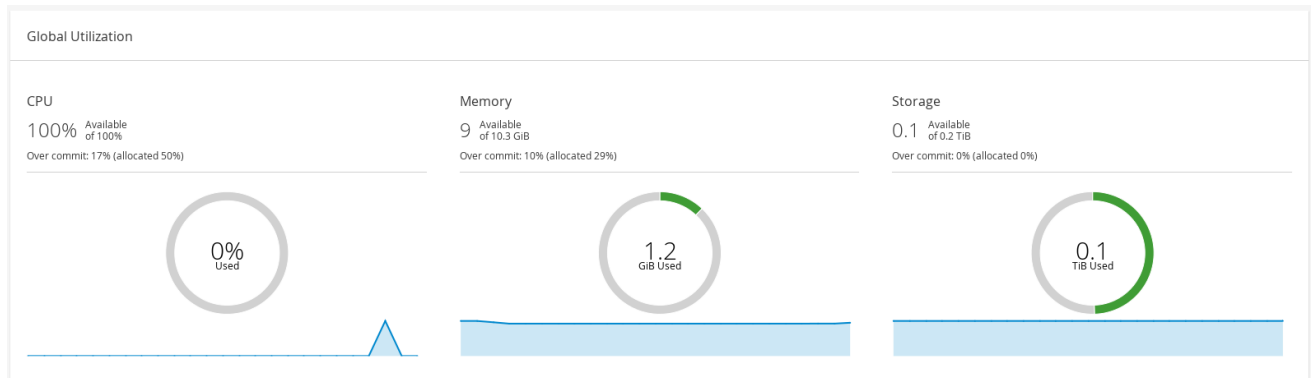
图标	状态
	这些资源都不添加到 Red Hat Virtualization 中。

图标	状态
	<p>显示具有警告状态的资源数。单击图标可导航到相应的页面，搜索范围仅限于该资源，且具有警告状态。每个资源的搜索都会有所不同：</p> <ul style="list-style-type: none"> ● Data Centers: 搜索仅限于不正常运行或不响应的数据中心。 ● Gluster 卷： 搜索仅限于正在启动、暂停、迁移、等待、暂停或关机的 gluster 卷。 ● 主机： 搜索仅限于未分配、处于维护模式、安装、重新启动、准备维护、待处理批准或连接的主机。 ● 存储域： 搜索仅限于未初始化、未附加、不活动、处于维护模式、准备维护、分离或激活的存储域。 ● 虚拟机： 搜索仅限于正在启动、暂停、迁移、等待、暂停或关机的虚拟机。 ● Events： 搜索仅限于严重性为 warning 的事件。
	<p>显示具有 up 状态的资源数。单击图标可导航到相应的页面，搜索范围仅限于启动的资源。</p>
	<p>显示状态为 down 的资源数量。单击图标可导航到相应的页面，搜索范围仅限于 down 状态的资源。每个资源的搜索都会有所不同：</p> <ul style="list-style-type: none"> ● 数据中心： 搜索仅限于未初始化、维护模式或处于 down 状态的数据中心。 ● Gluster 卷： 搜索仅限于分离或不活跃的 gluster 卷。 ● hosts： 搜索仅限于不响应、出错、安装错误、无法运行、初始化或停机的主机。 ● 存储域： 搜索仅限于分离或不活动的存储域。 ● 虚拟机： 搜索仅限于关闭、不响应或重新启动的虚拟机。
<p>images:images/Dashboard_Alert.png[title="Alert icon"]</p>	<p>显示具有警报状态的事件数。单击该图标，导航到 Events，搜索仅限于具有警报严重性的事件。</p>
<p>images:images/Dashboard_Error.png[title="Error icon"]</p>	<p>显示具有错误状态的事件数。单击该图标可导航到 Events，搜索仅限于具有错误严重性的事件。</p>

1.2.3. 全局利用率

Global Utilization 部分显示 CPU、内存和存储的系统利用率。

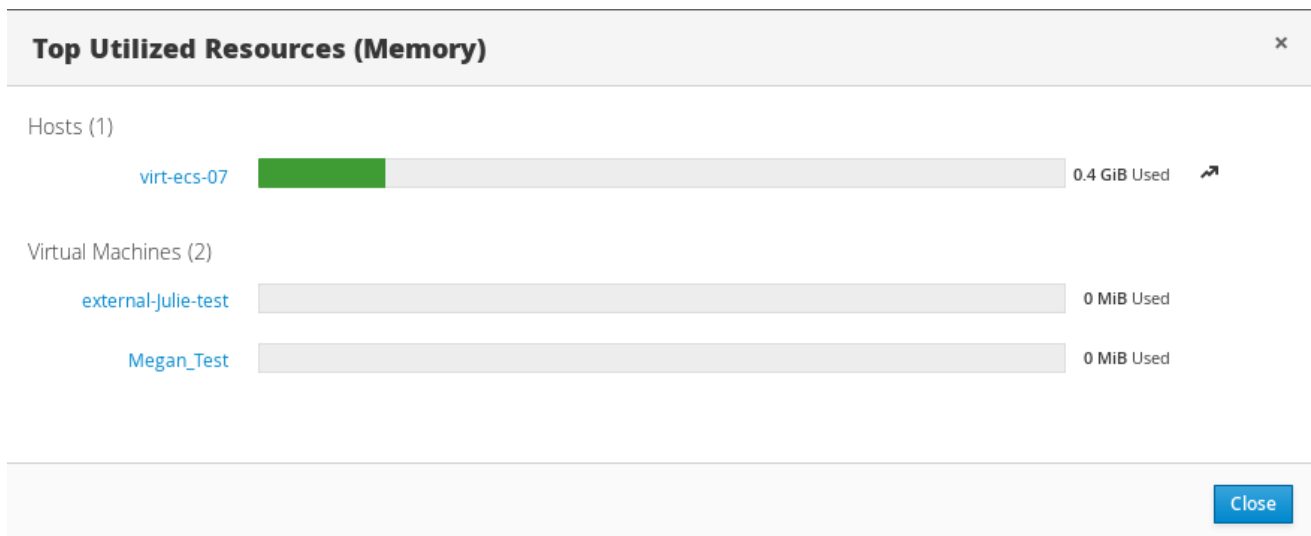
图 1.8. 全局利用率



- top 部分显示可用 CPU、内存或存储的百分比，以及过量提交比率。例如，CPU 的过量提交比率是通过根据数据仓库中最新数据将虚拟内核数除以可用于运行的虚拟机的物理内核数来计算的。
- 圈图以百分比为单位显示 CPU、内存或存储的使用情况，并根据最后 5 分钟的平均使用量显示所有主机的平均使用情况。将鼠标悬停在圆环的某一部分上，将显示所选部分的值。
- 底部的行图在最后 24 小时内显示趋势。每个数据点都显示针对特定小时的平均使用量。将鼠标悬停在图形上的点上可显示 CPU 图形使用的百分比以及内存和存储图的使用情况量。

1.2.3.1. top Utilized Resources

图 1.9. top Utilized Resources (Memory)

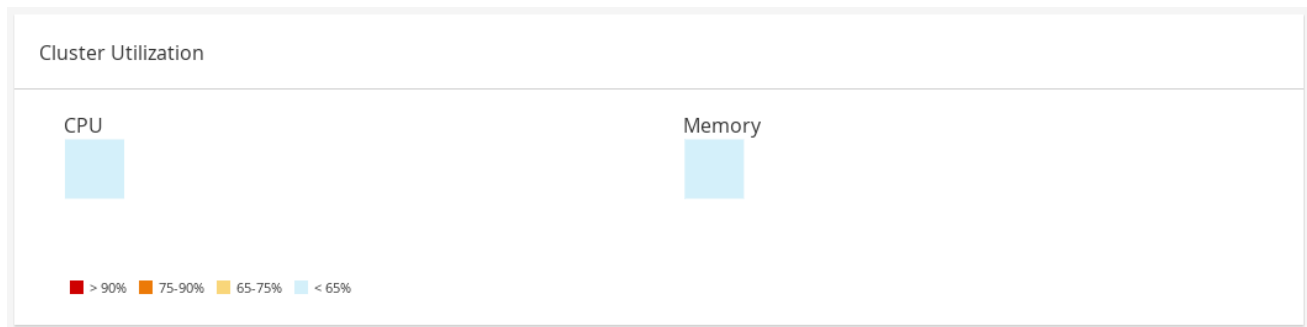


点控制面板的全局使用部分中的圆环，将显示 CPU、内存或存储占用最多的资源的列表。对于 CPU 和内存，弹出框显示使用率最高的十个主机和虚拟机列表。对于存储，弹出显示占用的十大存储域和虚拟机的列表。使用栏右侧的箭头显示该资源在最后一分钟内的使用情况。

1.2.4. Cluster Utilization

Cluster Utilization 部分显示 heatmap 中 CPU 和内存的集群利用率。

图 1.10. Cluster Utilization



1.2.4.1. CPU

特定集群的 CPU 使用率 heatmap，显示最后 24 小时 CPU 的平均利用率。将鼠标悬停在热图上会显示集群名称。点热图进入 **Compute** → **Hosts**，并显示特定集群的搜索结果（按 CPU 使用率排序）。用于计算集群 CPU 的使用情况的公式是集群中平均主机 CPU 利用率。这通过使用上 24 小时内每个主机的平均主机 CPU 利用率计算得出的，以确定集群的 CPU 总数。

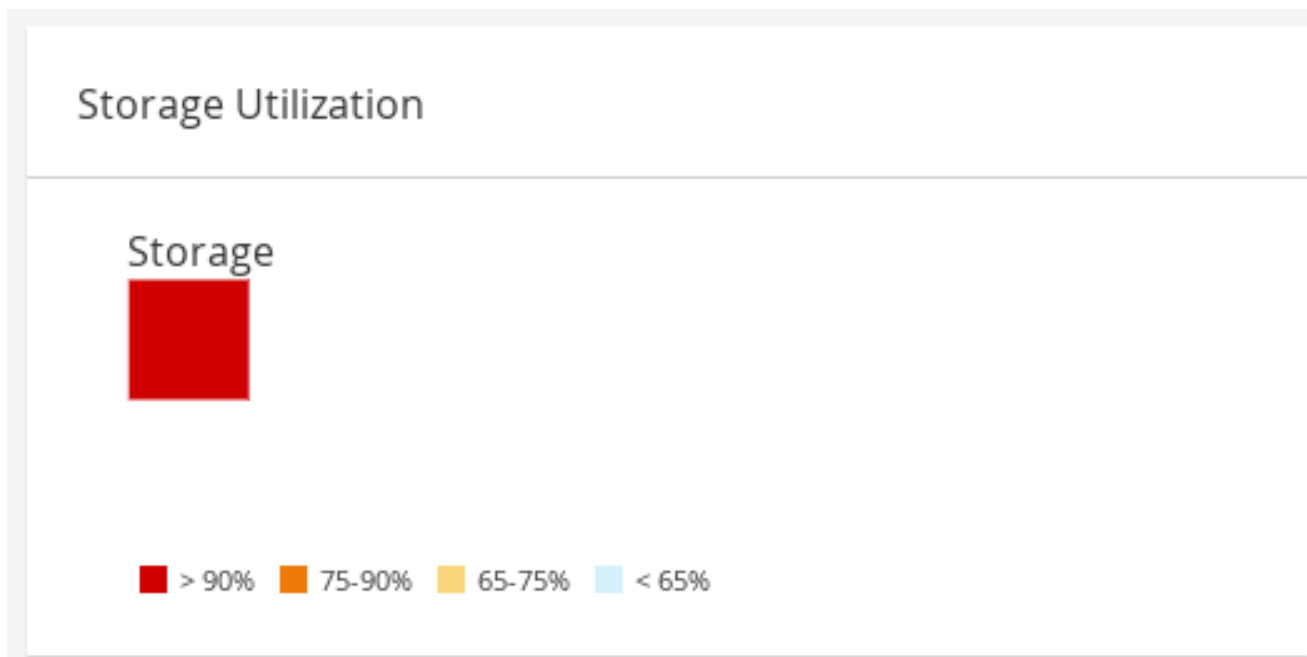
1.2.4.2. 内存

特定集群内存使用率的 heatmap，显示最后 24 小时的内存平均利用率。将鼠标悬停在热图上会显示集群名称。点热图进入 **Compute** → **Hosts**，并显示特定集群的搜索结果（按内存使用率排序）。用于计算集群内存使用的公式是集群中内存的总使用（以 GB 为单位）。这通过使用上 24 小时内每个主机的平均主机内存利用率计算得出的，以确定集群的内存的总平均使用量。

1.2.5. Storage Utilization

Storage Utilization 部分显示 heatmap 中的存储利用率。

图 1.11. Storage Utilization



热图显示最后 24 小时的存储的平均利用率。用于计算集群存储使用情况的公式是集群中的存储总利用率。这通过使用上 24 小时内每个主机的平均主机存储利用率计算得出的，以确定集群的存储总数。将鼠标悬停在热图上可显示存储域名称。单击 heatmap 将使用按利用率排序的存储域导航到 **存储** → **域**。

1.3. 搜索

1.3.1. 在 Red Hat Virtualization 中执行搜索

管理门户允许您管理数千资源，如虚拟机、主机、用户等。要执行搜索，请在搜索栏中输入搜索查询（自由文本或语法），可在每个资源的主页中找到。搜索查询可以保存为书签以供以后重复使用，因此您不必在每次需要特定搜索结果时重新设置搜索查询。搜索不区分大小写。

1.3.2. 搜索语法和示例

对 Red Hat Virtualization 资源的搜索查询的语法如下：

结果类型 : {criteria} [sortby sort_spec]

语法示例

以下示例描述了如何使用搜索查询，并帮助您了解 Red Hat Virtualization 如何协助构建搜索查询。

表 1.15. Search Queries 示例

Example	结果
Hosts: Vms.status = up page 2	显示正在运行虚拟机的所有主机的列表（第 2 页）。
VM: domain = qa.company.com	显示在指定域中运行的所有虚拟机的列表。
VM: users.name = Mary	显示属于用户名称 Mary 的所有虚拟机的列表。
events: severity > normal sortby time	显示所有严重性高于 Normal 的事件的列表，按时间排序。

1.3.3. 搜索 Auto-Completion

管理门户提供自动完成功能，可帮助您创建有效且强大的搜索查询。当您输入搜索查询的每个部分时，搜索的下一部分的下拉列表会在搜索栏下打开。您可以从列表中选择，然后继续键入/选择搜索的下一部分，或者忽略选项并继续手动输入查询。

下表指定，管理门户自动完成有助于构建查询的示例：

Hosts: Vms.status = down

表 1.16. 使用 Auto-Completion 的搜索查询示例

输入	列出显示的项目	操作
h	Hosts (仅 1 个选项)	选择 Hosts 或 type Hosts
Hosts :	所有主机属性	类型 v
Hosts: v	从 v 开始的主机属性	选择 Vms 或 type Vms

输入	列出显示的项目	操作
Hosts: Vms	所有虚拟机属性	类型 s
Hosts : Vms.s	以 s 开头的所有虚拟机属性	选择 状态 或类型 状态
Hosts: Vms.status	= !=	选择或类型 =
Hosts: Vms.status =	所有状态值	选择或类型 关闭

1.3.4. 搜索结果类型选项

通过结果类型，您可以搜索任何类型的资源：

- Vms 虚拟机列表
- Host 主机列表
- Pools 池列表
- Template 模块列表
- Events 事件列表
- Users 用户列表
- Cluster 集群列表
- DataCenter 数据中心列表
- Storage 存储域列表

因为每种类型的资源都有一组独特的属性，以及与之关联的一组其他资源类型，因此每个搜索类型都有一组有效的语法组合。您还可以使用自动完成功能轻松创建有效的查询。

1.3.5. 搜索标准

您可以在查询中的冒号后指定搜索条件。{criteria} 的语法如下：

<prop><operator><value>

或者

<obj-type><prop><operator><value>

例子

下表描述了语法的部分：

表 1.17. 搜索条件示例

Part	Description	值	Example	备注
prop	search-for 资源的属性。也可以是资源类型的属性（请参阅 obj-type ）或 tag (custom tag)。	将搜索范围限制为带有特定属性的对象。例如，搜索具有 status 属性的对象。	状态	N/A
obj-type	与搜索资源关联的资源类型。	它们是系统对象，如数据中心和虚拟机。	用户	N/A
operator	比较运算符。	= != (not equal) > < >= <=	N/A	值选项取决于属性。
值	哪些表达式与以下内容进行比较：	字符串 整数 等级 日期（根据区域设置格式化）	jones 256 normal	<ul style="list-style-type: none"> 通配符可以在字符串中使用。 ""（两个一组没有空格的引号），可用于表示未初始化（空字符串）字符串。 双引号应该在包含空格的字符串或日期后面使用

1.3.6. 搜索：多个标准和通配符

通配符可用于字符串语法的 **<value>** 部分。例如，要查找以 **m** 开头的所有用户，请输入 **m***。

您可以使用布尔值运算符和 **OR** 执行具有两个 **条件** 的搜索。例如：

VM: users.name = m* AND status = Up

此查询返回所有正在运行的虚拟机，适用于其名称以"m"开头的用户。

Vms: users.name = m* AND tag = "paris-loc"

对于名称以"m"开头的用户，此查询会返回带有"paris-loc"标记的所有虚拟机。

在没有使用 **AND** 或 **OR** 的情况下指定了两个条件，代表 **AND**。**AND** 的优先级高于 **OR**，**OR** 的优先级高于没有明确指定的 **AND**。

1.3.7. 搜索：确定搜索顺序

您可以使用 **sortby** 确定返回的信息的排序顺序。可以包括排序方向（**asc** 代表升序，**desc** 代表降序）。

例如：

events: severity > normal sortby time desc

此查询会返回所有严重性高于 Normal 的事件，按时间排序（降序）。

1.3.8. 搜索数据中心

下表描述了数据中心的所有搜索选项。

表 1.18. 搜索数据中心

属性（资源或资源类型）	类型	描述（参考）
cluster.cluster-prop	取决于属性类型	与数据中心关联的集群属性。
name	字符串	数据中心的名称。
description	字符串	数据中心的描述。
type	字符串	数据中心的类型。
status	list	数据中心的可用性。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

datacenter: type = nfs and status != up

这个示例返回类型为 NFS 的数据中心列表，以及除 up 以外的状态。

1.3.9. 搜索集群

下表描述了集群的所有搜索选项。

表 1.19. 搜索集群

属性（资源或资源类型）	类型	描述（参考）
Datacenter.<i>datacenter-prop</i>	取决于属性类型	与集群关联的数据中心的属性。
数据中心	字符串	集群所属的数据中心。
name	字符串	标识网络上的集群的唯一名称。
description	字符串	集群的描述。
初始化	字符串	判断集群的状态的 True 或 False。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

clusters: initialized = true 或 name = Default

本例返回初始化或名为 Default 的集群列表。

1.3.10. 搜索主机

下表描述了主机的所有搜索选项。

表 1.20. 搜索主机

属性（资源或资源类型）	类型	描述（参考）
vm.<i>Vms-prop</i>	取决于属性类型	与主机关联的虚拟机的属性。
templates.<i>templates-prop</i>	取决于属性类型	与主机关联的模板的属性。
events.<i>events-prop</i>	取决于属性类型	与主机关联的事件的属性。
users.<i>users-prop</i>	取决于属性类型	与主机关联的用户的属性。
name	字符串	主机的名称。
status	list	主机的可用性。
external_status	字符串	外部系统和插件报告的主机的健康状况。
cluster	字符串	主机所属的集群。

属性（资源或资源类型）	类型	描述（参考）
address	字符串	标识网络主机上主机的唯一名称。
cpu_usage	整数	使用的处理能力百分比。
mem_usage	整数	使用的内存百分比。
network_usage	整数	网络使用量的百分比。
load	整数	在给定时间片段中的每个处理器的 run-queue 中执行的作业。
version	整数	操作系统的版本号。
cpus	整数	主机上的 CPU 数量。
内存	整数	可用的内存量。
cpu_speed	整数	CPU 的处理速度。
cpu_model	字符串	CPU 的类型。
active_vms	整数	当前运行的虚拟机数量。
migrating_vms	整数	当前迁移的虚拟机数量。
committed_mem	整数	已提交的内存百分比。
tag	字符串	分配给主机的标签。
type	字符串	主机的类型。
datacenter	字符串	主机所属的数据中心。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

Hosts: cluster = Default 和 Vms.os = rhel6

这个示例返回作为默认集群的一部分的主机列表，以及运行 Red Hat Enterprise Linux 6 操作系统的主机。

1.3.11. 搜索网络

下表描述了网络的所有搜索选项。

表 1.21. 搜索网络

属性（资源或资源类型）	类型	描述（参考）
Cluster_network.clusternetw ork-prop	取决于属性类型	与网络关联的集群的属性。
Host_Network.hostnetwork- prop	取决于属性类型	与网络关联的主机的属性。
name	字符串	标识网络的人类可读名称。
description	字符串	描述网络的关键字或文本（在创建网络时可选使用）。
vlanid	整数	网络的 VLAN ID。
stp	字符串	网络是否启用或禁用生成树协议 (STP)。
mtu	整数	逻辑网络的最大传输单元。
vmnetwork	字符串	网络是否仅用于虚拟机流量。
datacenter	字符串	附加网络的数据中心。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

Network: mtu > 1500 and vmnetwork = true

这个示例会返回一个最大传输单元大于 1500 字节的网络列表，仅用于虚拟机使用。

1.3.12. 搜索存储

下表描述了存储的所有搜索选项。

表 1.22. 搜索存储

属性（资源或资源类型）	类型	描述（参考）
主机.host-prop	取决于属性类型	与存储关联的主机的属性。

属性 (资源或资源类型)	类型	描述 (参考)
cluster.cluster-prop	取决于属性类型	与存储关联的集群的属性。
name	字符串	标识网络上存储的唯一名称。
status	字符串	存储域的状态。
external_status	字符串	外部系统和插件报告的存储域的健康状况。
datacenter	字符串	存储所属的数据中心。
type	字符串	存储的类型。
free-size	整数	可用存储的大小(GB)。
used-size	整数	使用的存储量(GB)。
total_size	整数	可用存储的总量(GB)。
committed	整数	提交的存储量(GB)。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

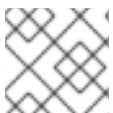
Example

Storage: free_size > 6 GB 和 total_size < 20 GB

这个示例返回一个存储空间大于 6 GB 的存储列表，或者存储空间总量小于 20 GB。

1.3.13. 搜索磁盘

下表描述了磁盘的所有搜索选项。



注意

您可以使用 **Disk Type** 和 **Content Type** 过滤选项来减少显示的虚拟磁盘数量。

表 1.23. 搜索磁盘

属性 (资源或资源类型)	类型	描述 (参考)
Datacenters.datacenters-prop	取决于属性类型	与磁盘关联的数据中心的属性。

属性 (资源或资源类型)	类型	描述 (参考)
Storages.storages-prop	取决于属性类型	与磁盘关联的存储的属性。
alias	字符串	标识网络上存储的人类可读名称。
description	字符串	描述磁盘时使用的关键字或文本 (可选)。
provisioned_size	整数	磁盘的虚拟大小。
size	整数	磁盘大小。
actual_size	整数	分配给磁盘的实际大小。
creation_date	整数	创建磁盘的日期。
bootable	字符串	磁盘是否可以引导。有效值为 0, 1, yes, 或 no 之一。
shareable	字符串	磁盘是否能一次连接到多个虚拟机。有效值为 0, 1, yes, 或 no 之一。
格式	字符串	磁盘格式。可以是 unused, unassigned, cow, 或 raw 之一。
status	字符串	磁盘状态。可以是 unassigned, ok, locked, invalid, 或 illegal 之一。
disk_type	字符串	磁盘的类型。可以是 镜像 之一或 lun 。
number_of_vms	整数	附加磁盘的虚拟机数量。
vm_names	字符串	附加磁盘的虚拟机的名称。
quota	字符串	虚拟磁盘强制配额的名称。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

disks: format = cow 和 provisioned_size > 8

这个示例返回带有 QCOW 格式和分配的磁盘大小大于 8 GB 的虚拟磁盘列表。

1.3.14. 搜索卷

下表描述了卷的所有搜索选项。

表 1.24. 搜索卷

属性（资源或资源类型）	类型	描述（参考）
集群	字符串	与卷关联的集群名称。
cluster.cluster-prop	取决于属性类型（示例：名称、描述、注释、架构）	与卷关联的集群的属性。
name	字符串	标识卷的人类可读名称。
type	字符串	可以是分发、复制、distributed_replicate、stripe 或 distributed_stripe 中的一个。
transport_type	整数	可以是 TCP 或 RDMA 之一。
replica_count	整数	副本数。
stripe_count	整数	条带数。
status	字符串	卷的状态。可以是 Up 或 Down 之一。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

volume: transport_type = rdma 和 stripe_count >= 2

这个示例返回有传输类型设置为 RDMA 的卷列表，以及 2 个或更多条带。

1.3.15. 搜索虚拟机

下表描述了虚拟机的所有搜索选项。



注意

目前，Network Label, Custom Emulated Machine 和 Custom CPU Type 属性不支持搜索参数。

表 1.25. 搜索虚拟机

属性 (资源或资源类型)	类型	描述 (参考)
主机 . <i>host-prop</i>	取决于属性类型	与虚拟机关联的主机的属性。
templates . <i>templates-prop</i>	取决于属性类型	与虚拟机关联的模板的属性。
events . <i>events-prop</i>	取决于属性类型	与虚拟机关联的事件的属性。
users . <i>users-prop</i>	取决于属性类型	与虚拟机关联的用户的属性。
storage . <i>storage-prop</i>	取决于属性类型	与虚拟机关联的存储设备的属性。
vNIC . <i>vnic-prop</i>	取决于属性类型	与虚拟机关联的 vNIC 属性。
name	字符串	虚拟机的名称。
status	list	虚拟机的可用性。
ip	整数	虚拟机的 IP 地址。
uptime	整数	虚拟机运行了几分钟的时间。
domain	字符串	对这些机器进行分组的域 (通常为 Active Directory 域)。
os	字符串	创建虚拟机时选择的操作系统。
creationdate	Date	创建虚拟机的日期。
address	字符串	标识网络上的虚拟机的唯一名称。
cpu_usage	整数	使用的处理能力百分比。
mem_usage	整数	使用的内存百分比。
network_usage	整数	使用的网络的百分比。
内存	整数	定义的最大内存。
apps	字符串	当前在虚拟机上安装的应用程序。
cluster	list	虚拟机所属的集群。
pool	list	虚拟机所属的虚拟机池。

属性（资源或资源类型）	类型	描述（参考）
loggedinuser	字符串	当前登录到虚拟机的用户的名称。
tag	list	虚拟机所属的标签。
datacenter	字符串	虚拟机所属的数据中心。
type	list	虚拟机类型（服务器或桌面）。
quota	字符串	与虚拟机关联的配额名称。
description	字符串	描述虚拟机的关键字或文本，可以选择创建虚拟机时使用。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。
next_run_configuration_exists	布尔值	虚拟机有待处理的配置更改。

Example

VMs: template.name = Win* and user.name = ""

本例返回其基础模板名称以 Win 开头的虚拟机列表，并分配给任何用户。

Example

VM: cluster = Default and os = windows7

这个示例返回属于 Default 集群且正在运行 Windows 7 的虚拟机列表。

1.3.16. 搜索池

下表描述了池的所有搜索选项。

表 1.26. 搜索池

属性（资源或资源类型）	类型	描述（参考）
name	字符串	池的名称。
description	字符串	池的描述。
type	list	池的类型。

属性（资源或资源类型）	类型	描述（参考）
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

pool: type = automatic

这个示例返回了类型为 **automatic** 的池列表。

1.3.17. 搜索模板

下表描述了模板的所有搜索选项。

表 1.27. 搜索模板

属性（资源或资源类型）	类型	描述（参考）
vm.Vms-prop	字符串	与模板关联的虚拟机的属性。
主机.host-prop	字符串	与模板关联的主机的属性。
events.events-prop	字符串	与模板关联的事件的属性。
users.users-prop	字符串	与模板关联的用户的属性。
name	字符串	模板的名称。
domain	字符串	模板的域。
os	字符串	操作系统的类型。
creationdate	整数	创建模板的日期。 日期格式是 mm/dd/yy。
childcount	整数	从模板创建的虚拟机数量。
mem	整数	定义的内存。
description	字符串	模板的描述。
status	字符串	模板的状态。
cluster	字符串	与模板关联的集群。

属性（资源或资源类型）	类型	描述（参考）
datacenter	字符串	与模板关联的数据中心。
quota	字符串	与模板关联的配额。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

template: Events.severity >= normal and Vms.uptime > 0

本例返回模板列表，其中事件是从模板派生的虚拟机上发生正常或更大严重性的事件，并且虚拟机仍在运行。

1.3.18. 搜索用户

下表描述了用户的所有搜索选项。

表 1.28. 搜索用户

属性（资源或资源类型）	类型	描述（参考）
vm.Vms-prop	取决于属性类型	与用户关联的虚拟机的属性。
主机.host-prop	取决于属性类型	与用户关联的主机的属性。
templates.templates-prop	取决于属性类型	与用户关联的模板的属性。
events.events-prop	取决于属性类型	与用户关联的事件的属性。
name	字符串	用户名称。
lastname	字符串	用户的姓氏。
username	字符串	用户的唯一名称。
department	字符串	用户所属的部门。
group	字符串	用户所属的组。
title	字符串	用户标题。
status	字符串	用户的状态。

属性（资源或资源类型）	类型	描述（参考）
role	字符串	用户的角色。
tag	字符串	用户所属的标签。
pool	字符串	用户所属的池。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

Users: Events.severity > normal and Vms.status = up or Vms.status = pause

此示例返回一个用户列表，其中事件超过正常严重性的事件已发生在虚拟机，并且虚拟机仍在运行中；或者用户的虚拟机已暂停。

1.3.19. 搜索事件

下表描述了可用于搜索事件的所有搜索选项。根据情况提供许多选项的自动完成功能。

表 1.29. 搜索事件

属性（资源或资源类型）	类型	描述（参考）
vm.Vms-prop	取决于属性类型	与事件关联的虚拟机的属性。
主机.host-prop	取决于属性类型	与事件关联的主机的属性。
templates.templates-prop	取决于属性类型	与事件关联的模板的属性。
users.users-prop	取决于属性类型	与事件关联的用户的属性。
cluster.cluster-prop	取决于属性类型	与事件关联的集群的属性。
volumes.Volumes-prop	取决于属性类型	与事件关联的卷的属性。
type	list	事件的类型。
severity	list	事件的严重性： Warning/Error/Normal。
message	字符串	事件类型的描述。

属性（资源或资源类型）	类型	描述（参考）
time	list	事件发生一天。
username	字符串	与事件关联的用户名。
event_host	字符串	与事件关联的主机。
event_vm	字符串	与事件关联的虚拟机。
event_template	字符串	与事件关联的模板。
event_storage	字符串	与事件关联的存储。
event_datacenter	字符串	与事件关联的数据中心。
event_volume	字符串	与事件关联的卷。
correlation_id	整数	事件的标识号。
sortby	list	根据其中一个资源属性对返回的结果进行排序。
page	整数	要显示的结果的页面数。

Example

Events: Vms.name = testdesktop and Hosts.name = gonzo.example.com

本例返回事件列表，其中事件发生在名为 **testdesktop** 的虚拟机上，同时在主机 **gonzo.example.com** 上运行。


1.4. 书签

1.4.1. 将查询字符串保存为书签

书签可用于记住搜索查询，并与其他用户共享。

流程


1. 在搜索栏中输入所需的搜索查询，并执行搜索。
2. 点搜索栏右侧的星形形状的书签按钮。此时将打开 **New Bookmark** 窗口。
3. 输入书签的 **Name**。
4. 如果需要，编辑 **Search string** 字段。
5. 点击 **OK**。

点击标题栏中的 **书签** 图标  来查找并选择书签。

1.4.2. 编辑书签

您可以修改书签的名称和搜索字符串。


流程

1. 点击标题栏中的 **书签** 图标 .
2. 选择书签并点击 **Edit**。
3. 根据需要更改 **Name** 和 **Search 字符串** 字段。
4. 点击 **OK**。

1.4.3. 删除书签

当不再需要书签时，将其删除。

流程


1. 点击标题栏中的 **书签** 图标 .
2. 选择书签并单击 **删除**。
3. 点击 **OK**。

1.5. TAGS

1.5.1. 使用标签来自定义 Red Hat Virtualization

在为您的要求设置并配置了 Red Hat Virtualization 平台后，您可以使用标签自定义它的工作方式。标记允许将系统资源分组或类别。当虚拟化环境中存在很多对象时，这很有用，而管理员想要专注于一组特定的对象。


本节论述了如何创建和编辑标签，将它们分配到主机或虚拟机，并使用标签作为条件进行搜索。可将标签按照与结构匹配的层次结构来排列，以满足企业的需求。

要创建、修改和删除管理门户标签，请点击标题栏中的 **标签** 图标 .

1.5.2. 创建标签

创建标签，以便您可以使用标签过滤搜索结果。

流程


1. 点标题栏中的 **标签** 图标()。
2. 单击 **Add** 以创建新标签，或者选择标签，然后单击 **New** 以创建下级标签。
3. 输入新标签的**名称**和**描述**。

4. 点击 **OK**。

1.5.3. 修改标签

您可以编辑标签的名称和描述。


修改标签

1. 点标题栏中的 **标签** 图标()。
2. 选择要修改的标签并点击 **Edit**。
3. 根据需要更改 **Name** 和 **Description** 字段。
4. 点击 **OK**。

1.5.4. 删除标签

当不再需要某个标签时，将它删除。

流程


1. 点标题栏中的 **标签** 图标()。
2. 选择您要删除的标签，然后单击 **Remove**。消息会警告，删除标签也会同时删除标签的所有后代。
3. 点击 **OK**。

您已删除标签及其所有子代。该标签也会从它所附加的所有对象中删除。

1.5.5. 为对象添加和删除标签

您可以分配标签到并从主机、虚拟机和用户中删除标签。

流程

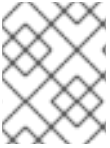
1. 选择您要标记或取消标记的对象。
2. 点 **More Actions** ()，然后点 **Assign Tags**。
3. 选中复选框，以分配标签到对象，或者清除要从对象中分离标签的复选框。
4. 点击 **OK**。

指定的标签现在将添加或删除为所选对象的自定义属性。

1.5.6. 使用标签搜索对象

使用 **tag** 作为属性以及所需值或值集作为搜索条件输入搜索查询。

带有指定条件的对象列在结果列表中。




注意

如果您在搜索对象时使用 **tag** 作为属性以及不相等运算符 (**!=**), 例如 **Host: Vms.tag!=server1**, 则结果列表不包括没有带有 tag 的对象。

1.5.7. 使用标签自定义主机

您可以使用标签存储主机的相关信息。然后, 您可以基于标签搜索主机。有关搜索的更多信息, 请参阅 [搜索](#)。

流程

1. 单击 **Compute** → **Hosts** 并选择一个主机。
2. 点 **More Actions** (), 然后点 **Assign Tags**。
3. 选中适用标签的复选框。
4. 单击 **OK**。

您已添加有关主机的额外可搜索信息作为标签。

第 2 章 管理资源

2.1. 服务质量

Red Hat Virtualization 允许您定义服务质量条目，对环境资源的输入和输出、处理和网络功能提供精细的控制。服务条目的质量在数据中心级别上定义，并分配到集群和存储域下创建的配置集。然后，这些配置集被分配到集群中独立的资源和创建配置集的存储域中。

2.1.1. 存储服务质量

存储服务质量为存储域的虚拟磁盘定义最大吞吐量级别和输出操作级别。通过为虚拟磁盘分配存储服务质量，您可以对存储域的性能进行微调，并防止与一个虚拟磁盘关联的存储操作影响到同一存储域上托管的其他虚拟磁盘的可用存储功能。

2.1.1.1. 创建存储服务质量服务条目

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **QoS** 选项卡。
4. 在 **Storage** 下，单击 **New**。
5. 为服务质量输入输入 **QoS Name** 和 **Description**。
6. 选择以下选项之一来指定服务的**吞吐量**质量：
 - **None**
 - **Total** - 在 **MB/s** 字段中输入允许的最大吞吐量。
 - **Read/Write** - 在左面的 **MB/s** 字段中输入读操作的最大允许吞吐量，在右面的 **MB/s** 字段中输入写操作的最大吞吐量。
7. 点击其中一个单选按钮来指定服务的**输入和输出(I/Ops)**质量：
 - **None**
 - **total** - 在 **I/Ops** 字段中，输入数上限和输出操作数每秒输入数。
 - **Read/Write** - 在左面的 **I/Ops** 字段中输入允许的最大输入操作数，在右面的 **I/Ops** 字段中输入每秒允许的最大操作数。
8. 单击 **OK**。

您已创建了服务条目的存储质量，并根据属于数据中心的数据存储域中的该条目创建磁盘配置文件。

2.1.1.2. 删除存储服务质量服务条目

删除现有存储服务质量条目。

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **QoS** 选项卡。
4. 在 **Storage** 下，选择 **storage quality of service** 条目，再单击 **Remove**。
5. 单击 **OK**。

如果有任何磁盘配置集基于该条目，则这些配置集的服务条目的存储质量会自动设置为 **[无限]**。

2.1.2. 虚拟机网络服务质量

虚拟机网络服务质量的功能允许您创建配置文件来限制单个虚拟网络接口控制器的入站和出站流量。通过此功能，您可以限制多个层中的带宽，从而控制网络资源的消耗。

2.1.2.1. 创建虚拟机网络服务质量服务条目

在应用到虚拟网络接口控制器(vNIC)配置集（也称为虚拟网络接口接口配置文件）时，创建用于注册网络流量的虚拟机网络服务质量。

创建虚拟机网络服务质量服务条目

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **QoS** 选项卡。
4. 在 **VM Network** 下，单击 **New**。
5. 为虚拟机网络服务质量输入 **Name**。
6. 输入 **Inbound** 和 **Outbound** 网络流量的限制。
7. 单击 **OK**。

您已创建了虚拟机网络服务质量，它可在虚拟网络接口控制器中使用。

2.1.2.2. New Virtual Machine Network QoS 和 Edit Virtual Machine Network QoS Windows 中的设置说明

虚拟机网络服务质量设置允许您在三个不同级别上为入站和出站流量配置带宽限制。

表 2.1. 虚拟机网络 QoS 设置

字段名称	Description
数据中心	要添加虚拟机网络 QoS 策略的数据中心。此字段会根据所选数据中心自动配置。
Name	代表 Manager 中的虚拟机网络 QoS 策略的名称。

字段名称	Description
入站	<p>应用到入站流量的设置。选择或取消选择 Inbound 复选框来启用或禁用这些设置。</p> <ul style="list-style-type: none"> ● 平均：入站流量的平均速度。 ● 峰值：高峰期间入站流量速度。 ● burst：激增期间入站流量速度。
出站	<p>应用到出站流量的设置。选择或清除 Outbound 复选框，以启用或禁用这些设置。</p> <ul style="list-style-type: none"> ● 平均：出站流量的平均速度。 ● 峰值：高峰期间出站流量速度。 ● 激增：激增期间出站流量速度。

要更改 **Average**、**Peak** 或 **Burst** 字段允许的最大值，使用 **engine-config** 命令更改 **MaxAverageNetworkQoSValue**、**MaxPeakNetworkQoSValue** 或 **MaxBurstNetworkQoSValue** 配置键的值。您必须重新启动 **ovirt-engine** 服务，才能使任何更改生效。例如：

```
# engine-config -s MaxAverageNetworkQoSValue=2048
# systemctl restart ovirt-engine
```

2.1.2.3. 删除虚拟机网络服务质量服务条目

删除服务条目的现有虚拟机网络质量。

流程

1. 单击 **Compute** → **Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **QoS** 选项卡。
4. 在 **VM Network** 下，选择虚拟机网络质量的 service 条目，再单击 **Remove**。
5. 单击 **OK**。

2.1.3. 主机网络服务质量

主机网络质量配置主机上的网络，从而通过物理接口控制网络流量。主机网络服务质量可通过控制同一物理网络接口控制器上的网络资源消耗来微调网络性能。这有助于防止一个网络使其他网络附加到同一物理网络接口控制器时，因为负载过重的流量不再起作用。通过配置主机网络质量服务，这些网络现在可以在同一物理网络接口控制器上正常工作，而不会出现各种问题。

2.1.3.1. 创建主机网络服务质量服务条目

创建主机网络服务质量服务条目。

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **QoS** 选项卡。
4. 在 **主机网络**下，单击**新建**。
5. 输入 **QoS Name**，以及服务质量条目的描述。
6. 为 **Weighted Share**、**Rate Limit [Mbps]**和 **Committed Rate [Mbps]** 输入所需的值。
7. 单击 **OK**。

2.1.3.2. New Host Network Quality of Service and Edit Host Network Quality of Service Windows 中的内容

通过主机网络服务质量设置，您可以为出站流量配置带宽限制。

表 2.2. 主机网络 QoS 设置

字段名称	Description
数据中心	要添加到主机网络 QoS 策略的数据中心。此字段会根据所选数据中心自动配置。
QoS Name	代表 Manager 中的主机网络 QoS 策略的名称。
Description	主机网络 QoS 策略的描述。
出站	<p>应用到出站流量的设置。</p> <ul style="list-style-type: none"> ● 加权共享：指定应分配特定网络的逻辑链接的容量量，相对于附加到同一逻辑链接的其他网络。确切共享取决于该链接上所有网络共享的总和。默认情况下，这是 1 到 100 范围内的数字。 ● 速率限制 [Mbps]：网络要使用的最大带宽。 ● 提交率 [Mbps]：网络所需的最小带宽。请求的提交率不能保证，并根据网络基础架构和同一逻辑链路上其他网络请求的提交率不同。

要更改 **Rate Limit [Mbps]** 或 **Committed Rate [Mbps]** 字段允许的最大值，请使用 **engine-config** 命令更改 **MaxAverageNetworkQoSValue** 配置键的值。您必须重新启动 **ovirt-engine** 服务，才能使更改生效。例如：

```
# engine-config -s MaxAverageNetworkQoSValue=2048
# systemctl restart ovirt-engine
```

2.1.3.3. 删除主机网络服务质量条目

删除现有的服务质量。

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **QoS** 选项卡。
4. 在 **Host Network** 下，选择主机网络服务质量服务条目，再单击 **Remove**。
5. 提示时点 **确定**。

2.1.4. CPU 服务质量

CPU 服务质量定义虚拟机可在其上运行的主机上的最大处理能力，以对该主机可用的总处理能力百分比表示。通过为虚拟机分配 CPU 质量，您可以防止集群中的一个虚拟机上的工作负载影响集群中可供其他虚拟机的处理资源。

2.1.4.1. 创建 CPU 服务质量条目

创建服务条目的 CPU 质量。

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **QoS** 选项卡。
4. 在 **CPU** 下，单击 **New**。
5. 为服务质量输入输入 **QoS Name** 和 **Description**。
6. 在 **Limit (%)** 字段中输入服务条目允许的最大处理能力。不要包含 % 符号。
7. 单击 **OK**。

您已创建了服务条目的 CPU 质量，并可以根据属于该数据中心的集群中的该条目创建 CPU 配置集。

2.1.4.2. 删除 CPU 服务质量条目

删除服务条目的现有 CPU 质量。

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **QoS** 选项卡。

4. 在 CPU 下，选择 CPU 质量的服务条目，然后单击 **Remove**。

5. 单击 **OK**。

如果任何 CPU 配置集都基于该条目，则这些配置集的服务条目的 CPU 质量会自动设置为 **[unlimited]**。

2.2. DATA CENTERS

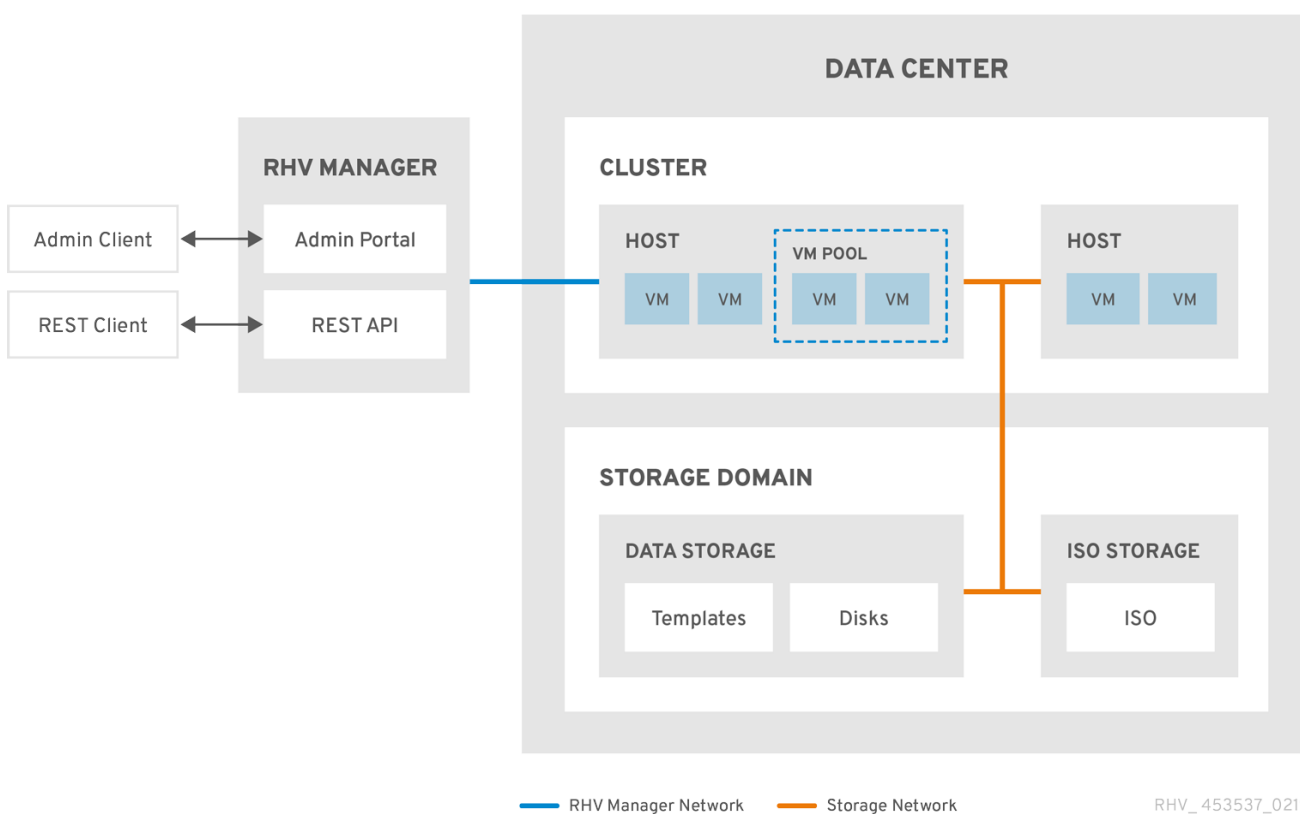
2.2.1. 数据中心介绍

数据中心是一个逻辑实体，用于定义特定环境中使用的资源集合。数据中心被视为容器资源，其中由逻辑资源组成，其格式为集群和主机；网络资源，格式为逻辑网络和物理 NIC；以及存储资源，格式为存储域。

数据中心可以包含多个集群，可以包含多个主机；可以关联多个存储域；它可以支持每个主机上的多个虚拟机。Red Hat Virtualization 环境可以包含多个数据中心；数据中心基础架构允许您分别保持这些中心。

所有数据中心都通过单一管理门户管理。

图 2.1. Data Centers



Red Hat Virtualization 在安装过程中创建一个默认数据中心。您可以配置默认数据中心，或者相应地设置新命名数据中心。

2.2.2. 存储池管理程序

存储池管理程序 (SPM) 是提供给数据中心中某一主机的角色，使其能够管理数据中心的存储域。SPM 实体可以在数据中心的任何主机上运行；红帽虚拟化管理器将角色授予其中一个主机。SPM 不会从其标准操作中排除主机；作为 SPM 运行的主机仍然可以托管虚拟资源。

SPM 实体通过协调存储域的元数据来控制对存储的访问。这包括创建、删除和操作虚拟磁盘（镜像）、快照和模板，以及为稀疏块设备（在 SAN 上）分配存储。这是一个拍它的责任：只有一个主机可以是一个数据中心的 SPM，以确保元数据的完整性。

Red Hat Virtualization Manager 确保 SPM 始终可用。如果 SPM 主机在访问存储时遇到问题，则管理器会将 SPM 角色移到其他主机。当 SPM 启动时，它会确保它是唯一授予该角色的主机，因此它将获得以存储为中心的租用。这个过程可能需要一些时间。

2.2.3. SPM 优先级

SPM 角色使用部分主机的可用资源。主机的 SPM 优先级设置将更改被分配 SPM 角色的主机的可能性：在具有高 SPM 优先级的主机将在主机具有低 SPM 优先级前分配 SPM 角色。具有低 SPM 优先级的主机上的关键虚拟机不必与主机资源的 SPM 操作相交。

您可以在 **Edit Host** 窗口的 **SPM** 选项卡中更改主机的 SPM 优先级。

2.2.4. 数据中心任务

2.2.4.1. 创建新数据中心

此流程在您的虚拟化环境中创建一个数据中心。数据中心需要一个正常工作的集群、主机和存储域才能运行。



注意

设置 **Compatibility Version** 后，您无法降低版本号。不支持版本回归。

您可以为集群指定 MAC 池范围。不再支持设置 MAC 池范围。

流程

1. 单击 **Compute** → **Data Centers**。
2. 单击 **New**。
3. 输入数据中心的**名称**和**描述**。
4. 从下拉菜单中选择 **Storage Type**、**Compatibility Version** 和 **Quota Mode**。
5. 点 **OK** 创建数据中心并打开 **Data Center - Guide Me** 窗口。
6. **Guide Me** 窗口列出了需要为数据中心配置的实体。点 **Configure Later** 按钮配置这些实体或 postpone 配置。通过选择数据中心并点 **More Actions** (⋮) 来恢复配置，然后点 **Guide Me**。

新数据中心将保持**未初始化**状态，直到为其配置了集群、主机和存储域；使用 **Guide Me** 来配置这些实体。

2.2.4.2. New Data Center 和 Edit Data Center Windows 中的设置说明

下表描述了**新建数据中心**和**编辑数据中心**窗口中显示的数据中心的设置。当您单击 **OK** 时，无效的条目会在 orange 中列出，从而禁止接受更改。另外，字段提示指定预期的值或值范围。

表 2.3. 数据中心属性


字段	description/Action
Name	数据中心的名称。此文本字段的限制为 40 个字符，且必须是唯一的名称，其中含有大写字母和小写字母、数字、连字符和下划线的任意组合。
Description	数据中心的描述。建议使用此字段，但不强制设置。
存储类型	<p>选择共享或本地存储类型。</p> <p>可将不同类型的存储域(iSCSI、NFS、FC、POSIX 和 Gluster)添加到同一数据中心。但是，本地和共享域不能混合使用。</p> <p>您可在数据中心初始化后更改存储类型。请参阅 更改数据中心存储类型。</p>
兼容性版本	<p>Red Hat Virtualization 的版本。</p> <p>升级 Red Hat Virtualization Manager 后，主机、集群和数据中心可能仍然在更早的版本。在升级数据中心的兼容性等级前，请确保已升级所有主机，然后集群。</p>
配额模式	<p>配额是 Red Hat Virtualization 提供的资源限制工具。选择以下之一：</p> <ul style="list-style-type: none"> ● 禁用：如果您不想实现配额，则选择该选项 ● 审核：如果您要编辑定额设置，则选择该选项 ● 强制：选择该选项实施定额
注释	(可选) 添加有关数据中心的纯文本注释。

2.2.4.3. 重新初始化数据中心：恢复过程

此恢复过程将数据中心的 **master** 数据域替换为新的 **master** 数据域。如果 **主** 数据损坏，您必须重新初始化主数据域。通过重新初始化数据中心，您可以恢复与数据中心关联的所有其他资源，包括集群、主机和非问题存储域。

您可以将任何备份或导出的虚拟机或模板导入到新的 **master** 数据域中。

流程

1. 点 **Compute** → **Data Centers** 并选择数据中心。
2. 确定附加到数据中心的任何存储域都处于维护模式。
3. 点 **More Actions** ()，然后点 **Re-Initialize Data Center**。

4. **数据中心重新初始化** 窗口将列出所有可用的（已达到维护模式；在维护模式中）存储域。点您要添加到数据中心的存储域的单选按钮。
5. 选择 **Approve operation** 复选框。
6. 点击 **OK**。

存储域作为 **master** 数据域连接到数据中心，并已激活。现在，您可以将任何备份或导出的虚拟机或模板导入到新的 **master** 数据域中。

2.2.4.4. 删除数据中心

删除数据中心需要活跃的主机。删除数据中心不会删除关联的资源。

流程

1. 确保附加到数据中心的存储域处于维护模式。
2. 点 **Compute → Data Centers** 并选择要删除的数据中心。
3. 单击 **Remove**。
4. 点击 **OK**。


2.2.4.5. 强制删除数据中心

如果附加的存储域已损坏或者主机变为 **Non Responsive**，则数据中心将变为 **Non Responsive**。您不能在这两种情况下 **删除** 数据中心。

强制删除 不需要活跃的主机。它还永久删除附加的存储域。

可能需要先销毁损坏的存储域，然后才能**强制删除**数据中心。

流程

1. 点 **Compute → Data Centers** 并选择要删除的数据中心。
2. 点 **More Actions** (), 然后点 **Force Remove**。
3. 选择 **Approve operation** 复选框。
4. 点 **OK**

数据中心和附加存储域从 Red Hat Virtualization 环境中永久删除。

2.2.4.6. 更改数据中心存储类型

您可在初始化后更改数据中心的存储类型。这可用于移动虚拟机或模板的数据域。

限制

- 与本地共享 - 对于不含多个主机和多个集群的数据中心，因为本地数据中心不支持它。
- local to Shared - 对于不包含本地存储域的数据中心。

流程

1. 单击 **Compute** → **Data Centers**，再选择要更改的数据中心。
2. 点 **Edit**。
3. 将 **Storage Type** 更改为所需的值。
4. 单击 **OK**。

2.2.4.7. 更改数据中心兼容性版本

Red Hat Virtualization 数据中心具有兼容性版本。兼容性版本指明了数据中心要与之兼容的 Red Hat Virtualization 版本。数据中心中的所有集群都必须支持所需的兼容性级别。

先决条件

- 要更改数据中心兼容性级别，您必须首先更新数据中心的集群和虚拟机的兼容性版本。

流程

1. 在管理门户中，点 **Compute** → **Data Centers**。
2. 选择要更改的数据中心，再单击 **Edit**。
3. 将 **Compatibility Version** 更改为所需的值。
4. 单击 **确定**。此时会打开 **Change Data Center Compatibility Version** 确认对话框。
5. 点 **OK** 确认。

2.2.5. 数据中心和存储域

2.2.5.1. 将现有数据域附加到数据中心

未连接的数据域可以附加到数据中心。可向同一数据中心添加多种类型的共享存储域(iSCSI、NFS、FC、POSIX 和 Gluster)。

流程

1. 单击 **Compute** → **Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **Storage** 选项卡列出已附加到数据中心的存储域。
4. 点 **Attach Data**。
5. 选中要附加到数据中心的数据域的复选框。您可以选择多个复选框来附加多个数据域。
6. 单击 **OK**。

数据域已附加到数据中心，并自动激活。

2.2.5.2. 将现有的 ISO 域附加到数据中心

未附加的 ISO 域可以附加到数据中心。ISO 域必须是与数据中心相同的 **存储类型**。

只能将一个 ISO 域附加到数据中心。

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **Storage** 选项卡列出已附加到数据中心的存储域。
4. 点 **Attach ISO**。
5. 点相应 ISO 域的单选按钮。
6. 单击 **OK**。

ISO 域连接到数据中心，并自动激活。

2.2.5.3. 将现有导出域附加到数据中心



注意

导出存储域已弃用。存储数据域可以从数据中心取消附加，并导入到同一环境中或不同环境中的其他数据中心。然后，可以将虚拟机、浮动虚拟磁盘和模板从导入的存储域上传到所连接的数据中心。有关 [导入存储域的信息](#)，请参阅导入现有存储域。

附加 **未连接** 的导出域可以附加到数据中心。只能将一个导出域附加到数据中心。

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **Storage** 选项卡列出已附加到数据中心的存储域。
4. 点 **Attach Export**。
5. 单击相应导出域的单选按钮。
6. 单击 **OK**。

导出域连接到数据中心，并自动激活。

2.2.5.4. 将存储域从数据中心分离

将存储域从数据中心分离开来，将阻止数据中心与该存储域相关联。存储域不会从 Red Hat Virtualization 环境中删除；它可以附加到另一个数据中心。

虚拟机和模板等数据仍然附加到存储域。



警告

虽然可以分离最后一个主存储域，但不建议这样做。

如果分离主存储域，必须重新初始化。

如果重新初始化存储域，您的所有数据都将丢失，存储域可能无法再次找到您的磁盘。

流程

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点 **Storage** 选项卡列出附加到数据中心的存储域。
4. 选择要分离的存储域。如果存储域是 **Active**，请单击 **Maintenance**。
5. 单击 **OK** 以启动维护模式。
6. 单击 **Detach**。
7. 单击 **OK**。

存储域可能需要几分钟才能从详情视图中消失。

2.3. 集群

2.3.1. 集群简介

集群是共享相同存储域且相同类型的 CPU (Intel 或 AMD) 的主机的逻辑分组。如果主机具有不同的 CPU 模型生成，则只使用所有模型中的功能。

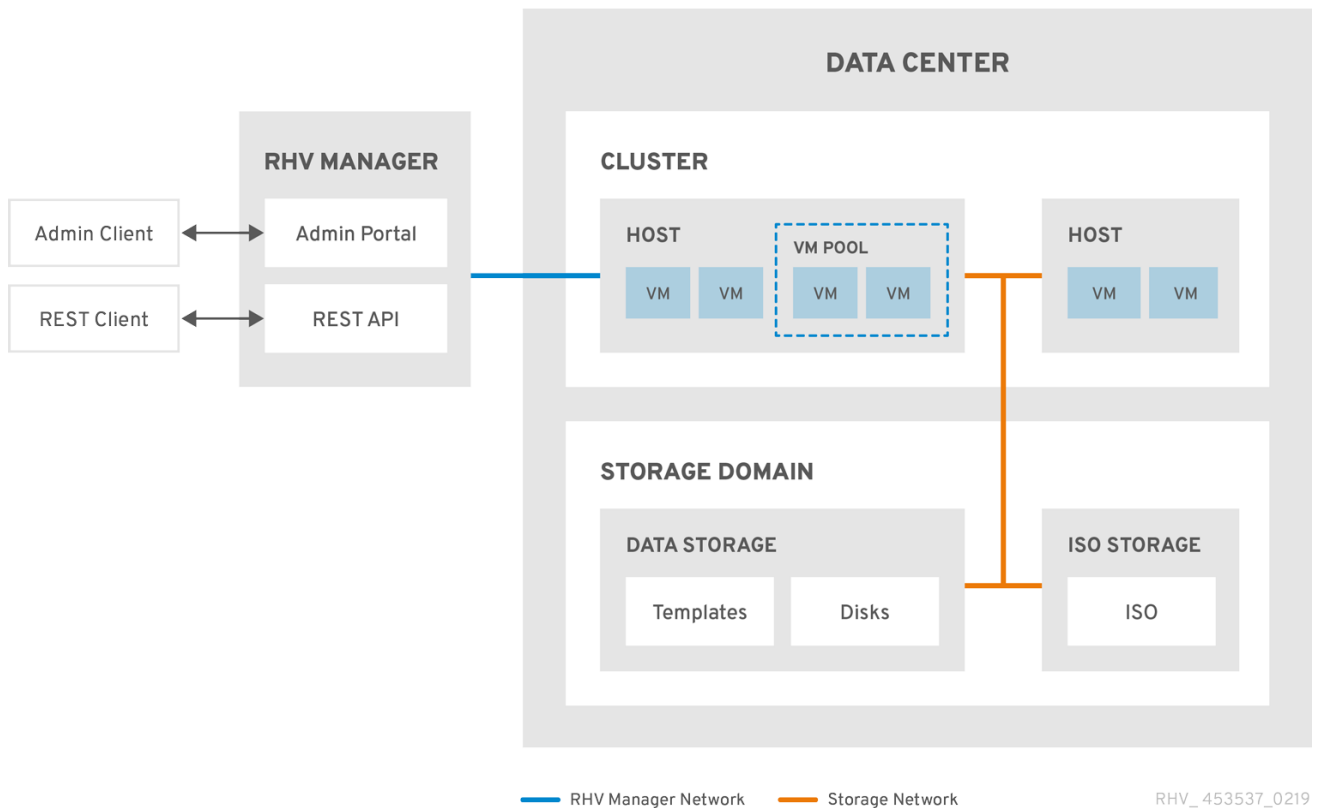
系统中的每个集群都必须属于一个数据中心，系统中的每一主机都必须属于一个集群。虚拟机会动态分配到集群中的任何主机，并根据虚拟机中定义的策略在它们之间进行迁移。集群是可定义电源和加载共享策略的最高级别。

属于集群的主机和虚拟机数量分别显示在 **Host Count** 和 **VM Count** 下的结果列表中。

集群运行虚拟机或 Red Hat Gluster Storage 服务器。这两个目的是相互排斥的：单个集群无法支持虚拟化和存储主机。

Red Hat Virtualization 在安装过程中在默认数据中心创建一个默认集群。

图 2.2. 集群



2.3.2. 集群任务



注意

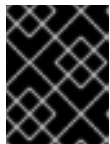
有些集群选项不适用于 Gluster 集群。有关在 Red Hat Virtualization 中使用 Red Hat Gluster Storage 的更多信息，请参阅使用 [Red Hat Gluster Storage 配置 Red Hat Virtualization](#)。

2.3.2.1. 创建新集群

数据中心可以包含多个集群，一个集群可以包含多个主机。集群中的所有主机都必须具有相同的 CPU 架构。要优化 CPU 类型，请在创建集群时创建主机。创建集群后，您可以使用 [引导我按钮配置主机](#)。

流程

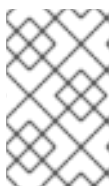
1. 单击 **Compute → Clusters**。
2. 单击 **New**。
3. 从下拉列表中选择集群将属于的**数据中心**。
4. 输入集群的**名称和描述**。
5. 从 **Management Network** 下拉列表选择一个网络来分配管理网络角色。
6. 选择 **CPU 架构**。
7. 对于 **CPU Type**，请在要属于此群集的主机中选择**最旧的 CPU 处理器系列**。CPU 类型按顺序从最旧的到最新的列出。



重要


其 CPU 处理器系列的主机早于您为 **CPU 类型指定的主机** 不能是此集群的一部分。详情请查看 [RHEV3 或 RHV4 集群应该设置为哪个 CPU 系列？](#)

8. 从下拉列表中选择集群的 **FIPS Mode**。
9. 从下拉列表中选择集群的 **Compatibility Version**。
10. 从下拉列表中选择 **Switch Type**。
11. 选择 **集群中主机的防火墙类型**，可以是 **Firewalld**（默认）或 **iptables**。



注意

只有在具有兼容性版本 4.2 或 4.3 的集群中的 Red Hat Enterprise Linux 7 主机才支持 **iptables**。您只能将 Red Hat Enterprise Linux 8 主机添加到使用防火墙类型为 **firewalld** 的集群

12. 选中 **Enable Virt Service** 或 **Enable Gluster Service** 复选框，以定义集群是否用虚拟主机填充或启用了 Gluster 的节点。
13. （可选）选择 **Enable to set VM Maintenance reason** 复选框，以便在从 Manager 关闭虚拟机时启用可选的 reason 字段，让管理员能够为维护提供说明。
14. （可选）选择 **Enable to set Host maintenance reason** 复选框，以便在主机从 Manager 放置到维护模式时启用可选的 reason 字段，让管理员能够针对维护提供说明。
15. （可选）选择 **/dev/hwrng source**（外部硬件设备）复选框来指定集群中所有主机要使用的随机数生成器设备。默认启用 **/dev/urandom 源**（Linux 提供的设备）。
16. 单击 **Optimization** 选项卡，以选择集群的内存页面共享阈值，并选择性地集群中的主机上启用 CPU 线程处理和内存膨胀。
17. 单击 **Migration Policy** 选项卡定义集群的虚拟机迁移策略。
18. 单击 **Scheduling Policy** 选项卡，以选择性地配置调度策略，配置调度程序优化设置，为集群中的主机启用可信服务，启用 HA Reservation，然后选择序列号策略。
19. 单击 **Console** 选项卡可以选择性地覆盖全局 SPICE 代理（如果有），并为集群中的主机指定 SPICE 代理地址。
20. 单击 **隔离策略** 选项卡在集群中启用或禁用隔离，然后选择隔离选项。
21. 单击 **MAC Address Pool** 选项卡，为集群指定默认池的 MAC 地址池。有关创建、编辑或删除 MAC 地址池的更多信息，请参阅 [MAC 地址池](#)。
22. 单击 **OK** 创建集群并打开 **Cluster - Guide Me** 窗口。
23. **Guide Me** 窗口列出了需要为集群配置的实体。单击 **Configure Later** 按钮配置这些实体或 postpone 配置。通过选择集群并单击 **More Actions** () 来恢复配置，然后单击 **Guide Me**。

2.3.2.2. 常规集群设置说明

下表描述了新集群和编辑集群窗口中常规选项卡的设置。当您单击 **OK** 时，无效的条目会在 orange 中列出，从而禁止接受更改。另外，字段提示指定预期的值或值范围。

表 2.4. 常规集群设置

字段	description/Action
数据中心	将包含集群的数据中心。必须在添加集群前创建数据中心。
Name	集群的名称。此文本字段的限制为 40 个字符，且必须是唯一的名称，其中含有大写字母和小写字母、数字、连字符和下划线的任意组合。
描述/评论	集群的描述或其他备注。建议使用这些字段，但不强制要求。
管理网络	<p>将被分配管理网络角色的逻辑网络。默认为 ovirtmgmt。如果迁移网络没有正确附加到源或目标主机，则此网络也将用于迁移虚拟机。</p> <p>在现有集群中，只有使用详情视图中的 Logical Networks 标签页中的 Manage Networks 按钮可以更改管理网络。</p>
CPU 架构	<p>集群的 CPU 架构。集群中的所有主机都必须运行您指定的架构。不同的 CPU 类型取决于选择哪个 CPU 架构。</p> <ul style="list-style-type: none"> ● 未定义：所有其他 CPU 类型。 ● x86_64：对于 Intel 和 AMD CPU 类型。 ● ppc64：用于 IBM POWER CPU 类型。
CPU Type	<p>集群中最旧的 CPU 系列。有关 CPU 类型列表，请参阅《<i>规划和前提条件指南</i>》中的 CPU 要求。在不发生重大中断的情况下创建集群后，您无法更改它。将 CPU 类型设置为集群中最旧的 CPU 模型。只能使用所有模型中的功能。对于 Intel 和 AMD CPU 类型，列出的 CPU 型号从最旧的到最新状态的顺序排列。</p>

字段	description/Action
芯片组/固件类型	<p>只有当集群的 CPU 架构 设置为 x86_64 时，此设置才可用。此设置指定芯片组和固件类型。选项是：</p> <ul style="list-style-type: none"> ● 自动检测：此设置自动检测芯片组和固件类型。选择了 Auto Detect 时，芯片组和固件由集群中的第一个主机决定。 ● 带有 BIOS 的 I440FX Chipset：使用固件类型 BIOS 指定到 I440FX 的芯片组。 ● 带有 BIOS 的 Q35 Chipset：使用没有 UEFI 的固件类型的 BIOS 指定 Q35 芯片组（默认为兼容版本 4.4 的集群）。 ● Q35 Chipset with UEFI 指定 Q35 芯片组，使用 UEFI 固件类型的 BIOS 指定 Q35 芯片组。（对于兼容版本 4.7 的集群的默认） ● Q35 Chipset 与 UEFI SecureBoot 一起指定 Q35 芯片组，该芯片组为 Q35 芯片组使用 SecureBoot，它验证引导装载程序的数字签名。 <p>如需更多信息，请参阅 管理指南 中的 UEFI 和 Q35 芯片组。</p>
使用 Bios 将现有 VM/Templates 从 I440fx 改为 Q35 Chipset	<p>当集群的芯片组从 I440FX 改为 Q35 时，选择此复选框来更改现有工作负载。</p>
FIPS 模式	<p>集群使用的 FIPS 模式。集群中的所有主机都必须运行您指定的 FIPS 模式，或者它们将无法操作。</p> <ul style="list-style-type: none"> ● auto Detect：此设置会自动检测到启用了 FIPS 模式还是禁用。当选择了 Auto Detect 时，FIPS 模式由集群中的第一个主机决定。 ● disabled：此设置在集群中禁用 FIPS。 ● 启用：此设置在集群中启用 FIPS。
兼容性版本	<p>Red Hat Virtualization 的版本。您将无法选择比为数据中心指定的版本更早的版本。</p>
切换类型	<p>集群使用的交换机类型。Linux Bridge 是标准 Red Hat Virtualization 交换机。OVS 支持 Open vSwitch 网络功能。</p>
防火墙类型	<p>指定集群中主机的防火墙类型，即 firewalld（默认）或 iptables。只有在具有兼容性版本 4.2 或 4.3 的集群中的 Red Hat Enterprise Linux 7 主机才支持 iptables。您只能将 Red Hat Enterprise Linux 8 主机添加到类型为 firewalld 的集群中。如果更改现有集群的防火墙类型，您必须 重新安装集群中的所有主机 以应用更改。</p>

字段	description/Action
默认网络提供程序	<p>指定集群要使用的默认外部网络供应商。如果您选择 Open Virtual Network (OVN)，则添加到集群的主机会自动配置为与 OVN 供应商通信。</p> <p>如果更改默认网络供应商，您必须重新安装集群中的所有主机以应用更改。</p>
最大日志内存阈值	<p>以百分比或绝对值（以 MB 为单位）形式指定最大内存消耗的日志记录阈值。如果主机的内存用量超过百分比，或者主机可用内存低于写值，则会记录消息。默认值为 95%。</p>
启用 Virt Service	<p>如果选中此复选框，则此集群中的主机将用于运行虚拟机。</p>
启用 Gluster 服务	<p>如果选中此复选框，则此集群中的主机将用作 Red Hat Gluster Storage Server 节点，而不适用于运行虚拟机。</p>
导入现有的 gluster 配置	<p>只有选择了 Enable Gluster Service 单选按钮时，此复选框才可用。通过此选项，您可以将当前启用了 Gluster 的集群及其所有附加的主机导入到 Red Hat Virtualization Manager。</p> <p>集群中被导入的每个主机都需要以下选项：</p> <ul style="list-style-type: none"> ● 主机名：输入 Gluster 主机服务器的 IP 或完全限定域名。 ● 主机 ssh 公钥(PEM)：Red Hat Virtualization Manager 获取主机的 SSH 公钥，以确保您使用正确的主机进行连接。 ● 密码：输入与主机通信所需的 root 密码。
额外的随机数字生成器源	<p>如果选中了复选框，集群中的所有主机都有额外的随机数生成器设备。这可实现从随机数生成器设备到虚拟机传递熵。</p>
Gluster Tuned 配置集	<p>只有选择了 Enable Gluster Service 复选框时，此复选框才可用。此选项指定 virtual-host 调优配置文件，以便提高脏内存页面的主动写回，这将使主机性能受益。</p>

2.3.2.3. 优化设置说明

内存注意事项

内存页面共享可让虚拟机利用其他虚拟机中未使用的内存，最多使用 200% 的分配内存。此过程基于您 Red Hat Virtualization 环境中的虚拟机不会全部同时运行容量，允许将未使用的内存临时分配给特定虚拟机。

CPU 注意事项

- 对于非 CPU 密集型工作负载，您可以使用大于主机内核数（单个虚拟机的处理器内核数）的处理器内核总数来运行虚拟机。可以实现以下优点：
 - 您可以运行更多虚拟机，从而降低硬件要求。
 - 您可以使用原本无法实现的 CPU 拓扑配置虚拟机，例如，虚拟内核的数量在主机内核数和主机线程数量之间。
- 为了获得最佳性能，尤其是 CPU 密集型工作负载，您应该在虚拟机中使用与主机中相同的拓扑，因此主机和虚拟机预计同样的缓存使用量。主机启用了超线程后，QEMU 会将主机的超线程视为内核，因此虚拟机不知道它在具有多个线程的单一核心上运行。此行为可能会影响虚拟机的性能，因为实际对应于主机核心中的超线程的虚拟核心可能会与同一主机核心中的另一个超线程共享一个缓存，而虚拟机则将其视为一个单独的核心。

下表描述了新集群和编辑集群窗口中优化选项卡的设置。

表 2.5. 优化设置

字段	description/Action
Memory Optimization	<ul style="list-style-type: none"> ● None - Disable memory overcommit : 禁用内存页面共享。 ● 对于服务器负载 - 允许调度 150% 物理内存 : 将内存页共享阈值设置为每个主机的系统内存的 150%。 ● 对于桌面负载 - 允许调度 200% 物理内存 : 将每个主机上系统内存内存的内存页面共享阈值设置为 200%。
CPU 线程	<p>选择 Count Threads As Cores 复选框可让主机运行虚拟机，处理器内核总数大于主机中的内核数（单个虚拟机的处理器内核数不得超过主机中的内核数）。</p> <p>选择了此复选框后，公开的主机线程将被视为虚拟机可以使用的内核。例如，一个有 24 个内核，每个内核有 2 个线程的核系统（总共 48 个线程）可以运行最多 48 个虚拟机，用于计算主机 CPU 负载的算法会与潜在的内核的两倍相比。</p>

字段	description/Action
内存 Balloon	<p>选择 Enable Memory Balloon Optimization 复选框可在此集群中运行的虚拟机上启用内存过量使用。选择了此复选框后，内存过量使用管理器(MoM)会尽可能启动膨胀，但会限制每个虚拟机的保证内存大小。</p> <p>要运行气球功能，虚拟机需要有一个带有相关驱动程序的气球设备。每个虚拟机都包含 balloon 设备，除非特别删除。此集群中的每个主机在状态更改为 启动 时会收到 balloon 策略更新。如果需要，您可以手动更新主机上的 balloon 策略，而无需更改状态。请参阅在集群的主机上更新 MoM 策略。</p> <p>务必要清楚，在某些情况下，ballooning 可能会与 KSM 冲突。在这种情况下，MoM 将尝试调整气球的大小，以最大程度减少冲突。此外，在某些情况下，ballooning 可能会导致虚拟机的最优性能。建议管理员小心使用膨胀优化。</p>
KSM 控制	<p>选择 启用 KSM 复选框可让 MoM 在需要时运行 Kernel Same-page Merging (KSM)，并且当它生成内存可节省能降低其 CPU 的成本时。</p>

2.3.2.4. 迁移策略设置说明

迁移策略定义了主机发生故障时实时迁移虚拟机的条件。这些条件包括迁移期间虚拟机的停机时间、网络带宽以及虚拟机优先级方式。

表 2.6. 迁移策略详细说明

策略	Description
Cluster default (Minimal downtime)	vdsm.conf 中的覆盖仍在应用。客户机代理 hook 机制已被禁用。
Minimal downtime	允许虚拟机在典型的情况下迁移的策略。虚拟机不应遇到任何显著的停机时间。如果虚拟机迁移经过长时间后还没有被聚合，则迁移过程会被终止（取决于 QEMU 的迭代，最长为 500 millisecond）。客户机代理 hook 机制已启用。

策略	Description
post-copy migration	<p>使用后复制迁移时，将暂停源主机上的迁移虚拟机 vCPU，仅传输最小内存页面，激活目标主机上的虚拟机 vCPU，并在虚拟机运行目标时传输其余内存页面。</p> <p>后复制策略首先尝试预复制，以验证是否可能发生聚合。如果虚拟机迁移在很长时间后没有聚合，迁移会切换到后复制。</p> <p>这可显著减少迁移的虚拟机停机时间，还可以确保无论源虚拟机的内存页面变化速度如何快。对于迁移大量连续使用的虚拟机来说，这是最佳选择，无法使用标准预复制迁移进行迁移。</p> <p>此策略的缺点在于，在复制后阶段，虚拟机可能会显著下降，因为主机之间缺少内存部分传输。</p> <div style="background-color: #fff9c4; padding: 10px; margin-top: 10px;"> <p style="text-align: center;"> 警告</p> <p>如果在完成后复制进程前网络连接中断，管理器将暂停，然后终止正在运行的虚拟机。如果虚拟机可用性至关重要，或者迁移网络不稳定，请不要使用复制后迁移。</p> </div>
如果需要，挂起工作负载	<p>允许虚拟机在大多数情况下迁移的策略，包括运行繁重工作负载的虚拟机。因此，与某些其他设置相比，虚拟机可能会出现停机时间更大。迁移可能仍然针对极端工作负载中止。客户机代理 hook 机制已启用。</p>

带宽设置定义每个主机传出和传入迁移的最大带宽。

表 2.7. 带宽详细说明

策略	Description
auto	<p>带宽从数据中心主机网络 QoS 中的 Rate Limit [Mbps] 设置中复制。如果尚未定义速率限制，则会计算为发送和接收网络接口最少的链接速度。如果没有设置速率限值，且链路速度不可用，将由发送主机上的本地 VDSM 设置确定。</p>
Hypervisor 默认	<p>带宽由发送主机上的本地 VDSM 设置控制。</p>

策略	Description
Custom	<p>由用户（以 Mbps）定义。这个值被并发迁移数量除以 2 个，以考虑正在进行和传出的迁移。因此，用户定义的带宽必须足够大，以适应所有并发迁移。</p> <p>例如，如果 自定义 带宽定义为 600 Mbps，则虚拟机迁移的最大带宽实际为 300 Mbps。</p>

弹性策略定义了虚拟机在迁移中的优先级。

表 2.8. 弹性策略设置

字段	description/Action
迁移虚拟机	按照其定义的优先级迁移所有虚拟机。
只迁移高度可用的虚拟机	仅迁移高度可用的虚拟机，以防止超载其他主机。
不迁移虚拟机	防止虚拟机被迁移。

表 2.9. 其他属性设置

字段	description/Action
启用迁移加密	<p>允许在迁移过程中对虚拟机进行加密。</p> <ul style="list-style-type: none"> ● 集群默认 ● 加密 ● 不加密
并行迁移	<p>允许您指定是否使用多少并行迁移连接。</p> <ul style="list-style-type: none"> ● 禁用：虚拟机使用单一的非并行连接迁移。 ● auto：自动决定并行连接数量。此设置可能会自动禁用并行连接。 ● auto Parallel：自动确定并行连接数量。 ● Custom：允许您指定首选的并行连接数，实际数量可能较低。
VM 迁移连接数	此设置仅在选择 Custom 时可用。自定义并行迁移的首选数量，2 到 255 之间。

2.3.2.5. 调度策略设置说明

通过调度策略，您可以指定可用主机之间虚拟机的使用和分配。定义调度策略，以启用集群中主机之间自动负载平衡。无论调度策略如何，虚拟机都不会在 CPU 过载的主机上启动。默认情况下，如果主机的 CPU 的负载超过 80% 达到 5 分钟，则主机 CPU 被视为过载，但这些值可以使用调度策略来更改。如需更多信息，请参阅 [管理指南](#) 中的 [调度策略](#)。

表 2.10. 调度策略选项卡属性

字段	description/Action
选择 Policy	<p>从下拉列表中选择策略。</p> <ul style="list-style-type: none"> ● 无：禁用已在正在运行的虚拟机的主机间的负载平衡或节能功能。这是默认的模式。当虚拟机启动时，内存和 CPU 处理负载会在集群中的所有主机上均匀分布。如果主机已达到定义的 CpuOverCommitDurationMinutes、HighUtilization 或 MaxFreeMemoryForOverUtilized，则附加到主机的其他虚拟机将不会启动。 ● evenly_distributed：分配内存和 CPU 处理在集群中的所有主机间平均负载。如果主机已达到定义的 CpuOverCommitDurationMinutes、HighUtilization、VCpuToPhysicalCpuRatio 或 MaxFreeMemoryForOverUtilized，则附加到主机的其他虚拟机将不会启动。 ● cluster_maintenance：限制维护任务期间集群中的活动。除了高可用性虚拟机外，可能不会启动新的虚拟机。如果发生主机故障，高可用性虚拟机将正确重新启动，任何虚拟机都可以迁移。 ● power_saving：将内存和 CPU 处理负载分散到可用主机子集中，以减少未被充分利用的主机的功耗。CPU 负载低于低利用率值的主机将超过定义的时间间隔，将所有虚拟机迁移到其他主机，以便将其关闭。如果主机已达到定义的高利用率值，则附加到主机的其他虚拟机将不会启动。 ● vm_evenly_distributed：根据虚拟机数量在主机之间平均分配虚拟机。如果任何主机运行的虚拟机数量超过 HighVmCount，且至少有一个主机具有超出 MigrationThreshold 范围的虚拟机数，则该集群被视为未平衡。
Properties	<p>根据所选的策略，会出现以下属性：如果需要，编辑它们：</p> <ul style="list-style-type: none"> ● HighVmCount：设置每个主机必须运行的最小虚拟机数量，以启用负载平衡。默认值为在单一主机上运行的虚拟机 10。只有集群中至少有 HighVmCount 运行虚拟机时，才会启用负载平衡。 ● MigrationThreshold：定义在从主机迁移虚拟机前的缓冲区。它是最高利用的主机和最低利用率主机之间的虚拟机数量的最大差值。当集群中的每个主机都有不处于迁移阈值内的虚拟机数时，集群处于平衡状态。默认值为 5。 ● SpmVmGrace：定义要在 SPM 主机上保留虚拟机的插槽数量。SPM 主机的负载比其他主机更低的负载，因此此变量定义了 SPM 主机与其他主机相比可以要运行的虚拟机数量。默认值为 5。 ● CpuOverCommitDurationMinutes：设置主机可以在调度策略采取操作前运行 CPU 负载的时间（以分钟为单位）。定义的时间间隔可防止 CPU 负载激活调度策略和产生不必要的虚拟机迁移的临时激增。最多两个字符。默认值为 2。 ● HighUtilization：以百分比表示。如果主机使用 CPU 使用率高于定义的时间间隔高利用率值运行，则 Red Hat Virtualization Manager 会将虚拟机迁移到集群中的其他主机，直到主机的 CPU 负载低于最大服务阈值。默认值为 80。

字段	description/Action
	<ul style="list-style-type: none"> ● LowUtilization : 以百分比表示。如果主机以 CPU 使用率低于定义的时间间隔保持 CPU 运行, 则 Red Hat Virtualization Manager 会将虚拟机迁移到集群中的其他主机。管理器将关闭原始主机机器, 并在负载均衡需要或集群中没有足够的可用主机时再次重新启动。默认值为 20。 ● scaleDown : 由于 HA Reservation weight 功能的影响, 按指定数量划分主机的分数。这是一个可选属性, 可添加到任何策略, 包括 none。 ● HostsInReserve : 指定很多主机来继续运行, 即使其中没有运行虚拟机。这是一个可选属性, 可添加到 power_saving 策略中。 ● EnableAutomaticHostPowerManagement : 为集群中的所有主机启用自动电源管理。这是一个可选属性, 可添加到 power_saving 策略中。默认值为 true。 ● MaxFreeMemoryForOverUtilized : 指定主机应具有的最小可用内存, 以 MB 为单位。如果主机可用内存小于这个数量, 则 RHV Manager 会认为主机被过度使用。例如, 如果您将此属性设置为 1000, 则的内存少于 1 GB 的可用内存被过度使用。 有关此属性如何与 power_saving 和 evenly_distributed 策略交互的详情, 请参阅 MaxFreeMemoryForOverUtilized 和 MinFreeMemoryForUnderUtilized 集群调度策略属性。 您可以将此属性添加到 power_saving 和 evenly_distributed 策略。虽然它出现在 vm_evenly_distributed 策略的属性列表中, 但它不适用于该策略。 ● MinFreeMemoryForUnderUtilized : 指定主机应具有的最大可用内存量 (以 MB 为单位)。如果主机可用内存超过这个数量, 则 RHV Manager 调度程序将主机视为使用率不足。例如, 如果您将此参数设置为 10000, 则有超过 10 GB 的可用内存的主机使用不足。 有关此属性如何与 power_saving 和 evenly_distributed 策略交互的详情, 请参阅 MaxFreeMemoryForOverUtilized 和 MinFreeMemoryForUnderUtilized 集群调度策略属性。 您可以将此属性添加到 power_saving 和 evenly_distributed 策略。虽然它出现在 vm_evenly_distributed 策略的属性列表中, 但它不适用于该策略。 ● HeSparesCount : 设置额外的自托管引擎节点数量, 必须保留足够可用内存, 以便在迁移或关机的情况下启动管理器虚拟机。如果这样做, 则其他虚拟机无法在自托管引擎节点上启动 (如果这样做) 不会为 Manager 虚拟机保留足够的可用内存。这是一个可选属性, 可以添加到 power_saving, vm_evenly_distributed, 和 evenly_distributed 策略。默认值为 0。
调度程序优化	<p>为主机权衡/订购优化调度。</p> <ul style="list-style-type: none"> ● 优化 Utilization : 在调度中包括权重模块, 以允许选择最佳。 ● 优化 Speed : 在有超过十个待处理请求的情况下跳过主权重。
启用信任服务	<p>启用与 OpenAttestation 服务器集成。启用此选项之前, 使用 engine-config 工具输入 OpenAttestation 服务器的详细信息。重要信息 : 不再提供 OpenAttestation 和 Intel Trusted Execution Technology (Intel TXT)。</p>
启用 HA 保留	<p>启用 Manager 以监控高可用性虚拟机的集群容量。Manager 确保集群中存在适当的容量, 以便在现有主机意外发生故障时将其指定为高度可用的虚拟机来迁移。</p>

字段	description/Action
序列号策略	<p>配置策略，以将序列号分配给集群中的每个新虚拟机：</p> <ul style="list-style-type: none"> ● 系统默认：使用 Manager 数据库中的系统范围默认值。要配置这些默认值，请使用 engine 配置工具 设置 DefaultSerialNumberPolicy 和默认 CustomSerialNumber 的值。这些键值对保存在 Manager 数据库的 vdc_options 表中。 对于 DefaultSerialNumberPolicy: <ul style="list-style-type: none"> ○ 默认值：HOST_ID ○ 可能的值有：HOST_ID,VM_ID,CUSTOM ○ 命令行示例：engine-config --set DefaultSerialNumberPolicy=VM_ID ○ 重要：重启 Manager 以应用配置。 对于 默认的CustomSerialNumber： <ul style="list-style-type: none"> ○ 默认值：Dummy serial number ○ 可能的值：任何字符串（最大长度为 255 个字符） ○ 命令行示例：engine-config --set DefaultCustomSerialNumber="My very special string value" ○ 重要：重启 Manager 以应用配置。 ● 主机 ID：将每个新虚拟机的序列号设置为主机的 UUID。 ● 虚拟机 ID：将每个新虚拟机的序列号设置为虚拟机的 UUID。 ● 自定义序列号：将每个新虚拟机的序列号设置为您在以下自定义序列号参数中指定的值。
自定义序列号	指定要应用到集群中的新虚拟机的自定义序列号。

当主机的可用内存低于 20% 时，如 **mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580** 的气球命令会记录到 `/var/log/vdsm/mom.log`。`/var/log/vdsm/mom.log` 是 Memory Overcommit Manager 日志文件。

2.3.2.6. MaxFreeMemoryForOverUtilized 和 MinFreeMemoryForUnderUtilized 集群调度策略属性

调度程序有一个后台进程，它根据当前的集群调度策略及其参数迁移虚拟机。根据策略中的各种条件及其相对权重，调度程序持续将主机归类为 *源主机* 或 *目标主机*，并将个别虚拟机从前迁移到后者。

以下描述解释了 `evenly_distributed` 和 `power_saving` 集群调度策略如何与 `MaxFreeMemoryForOverUtilized` 和 `MinFreeMemoryForUnderUtilized` 属性进行交互。虽然两个策略都考虑 CPU 和内存负载，但 CPU 负载与 `MaxFreeMemoryForOverUtilized` 和 `MinFreeMemoryForUnderUtilized` 属性无关。

如果您将 `MaxFreeMemoryForOverUtilized` 和 `MinFreeMemoryForUnderUtilized` 属性定义为 `evenly_distributed` 策略的一部分：

- 可用内存低于 `MaxFreeMemoryForOverUtilized` 的可用内存较少，并成为源主机。
- 具有比 `MinFreeMemoryForUnderUtilized` 可用内存更大且成为目标主机的主机。
- 如果没有定义 `MaxFreeMemoryForOverUtilized`，调度程序不会根据内存负载迁移虚拟机。（它会根据策略的其他条件（如 CPU 负载）继续迁移虚拟机。）
- 如果没有定义 `MinFreeMemoryForUnderUtilized`，调度程序会认为所有主机有资格成为目标主机。

如果您将 `MaxFreeMemoryForOverUtilized` 和 `MinFreeMemoryForUnderUtilized` 属性定义为 `power_saving` 策略的一部分：

- 可用内存低于 `MaxFreeMemoryForOverUtilized` 的可用内存较少，并成为源主机。
- 具有比 `MinFreeMemoryForUnderUtilized` 可用内存更高且成为源主机的主机。
- 超过 `MaxFreeMemoryForOverUtilized` 的可用内存数量超过 `MaxFreeMemoryForOverUtilized` 并不被过度利用，并成为目标主机。
- 低于 `MinFreeMemoryForUnderUtilized` 的可用内存较少，并未被充分利用且成为目标主机。
- 调度程序更喜欢将虚拟机迁移到既不被过度利用或未被充分利用的主机。如果这些主机没有足够的主机，调度程序可将虚拟机迁移到使用率低的主机。如果不需要充分利用主机来实现这一目的，调度程序就可以关闭它们。
- 如果没有定义 `MaxFreeMemoryForOverUtilized`，则没有主机被过度使用。因此，只有利用率不足的主机是源主机，目标主机包括集群中的所有主机。
- 如果没有定义 `MinFreeMemoryForUnderUtilized`，则只有过度利用的主机是源主机，不是被过度利用的主机。
- 要防止主机过度使用所有物理 CPU，请在 0.1 和 2.9 之间定义虚拟 CPU 到物理 CPU 比率 - `VCpuToPhysicalCpuRatio`。当设置此参数时，在调度虚拟机时首选使用较低 CPU 的主机。如果添加虚拟机会导致比例超过限制，则考虑 `VCpuToPhysicalCpuRatio` 和 CPU 使用率。

在运行的环境中，如果主机 `VCpuToPhysicalCpuRatio` 超过 2.5，一些虚拟机可能会平衡负载，并移到具有较低 `VCpuToPhysicalCpuRatio` 的主机。

其他资源

- [集群调度策略设置](#)

2.3.2.7. 集群控制台设置说明

下表描述了 `New Cluster` 和 `Edit Cluster` 窗口中的 `Console` 选项卡的设置。

表 2.11. 控制台设置

字段	description/Action
为集群定义 SPICE 代理	选中此复选框可覆盖全局配置中定义的 SPICE 代理。当用户（例如，通过虚拟机门户进行连接）位于虚拟机监控程序所在的网络之外时，此功能很有用。

字段	description/Action
覆盖的 SPICE 代理地址	SPICE 客户端连接到虚拟机时使用的代理。地址必须采用以下格式： protocol://[host]:[port]

2.3.2.8. 隔离策略设置说明

下表描述了新集群和编辑集群窗口中的隔离策略选项卡的设置。

表 2.12. 隔离策略设置

字段	description/Action
启用隔离	在集群中启用隔离功能。默认情况下启用隔离，但可以根据需要禁用；例如，如果临时网络问题发生或预期，管理员可以禁用隔离，直到诊断或维护活动完成为止。请注意，如果禁用隔离，在不响应的主机中运行的高可用性虚拟机不会在其他位置重启。
如果主机在存储上有实时租用，则跳过围栏	如果选中此复选框，则集群中任何不响应且仍然连接到存储的主机都不会被隔离。
在集群连接问题中跳过隔离	如果选中此复选框，如果遇到连接问题的主机百分比大于或等于定义的 Threshold ，则隔离将临时禁用。 Threshold 值可以从下拉列表中选择，有效值为 25, 50, 75, 和 100。
如果 gluster brick 已启动，则跳过隔离	只有在启用 Red Hat Gluster Storage 功能时，这个选项才可用。如果选中此复选框，则在 brick 正在运行并且可以从其他同级服务器访问时将跳过隔离。请参阅 Chapter 2. 使用隔离策略配置高可用性 和 以及 维护 Red Hat Hyperconverged Infrastructure 中的 Red Hat Gluster 存储附录 A. 隔离策略 以获得更多信息。
如果没有满足 gluster 仲裁，请跳过隔离	只有在启用 Red Hat Gluster Storage 功能时，这个选项才可用。如果选中此复选框，在 brick 正在运行并关闭主机时将跳过隔离，则主机将会导致仲裁丢失。请参阅 Chapter 2. 使用隔离策略配置高可用性 和 以及 维护 Red Hat Hyperconverged Infrastructure 中的 Red Hat Gluster 存储附录 A. 隔离策略 以获得更多信息。

2.3.2.9. 为集群中的主机设置负载和电源管理策略

`evenly_distributed` 和 `power_saving` 调度策略允许您指定可接受的内存和 CPU 用量值，以及虚拟机必须迁移到主机或从主机中的点。`vm_evenly_distributed` 调度策略根据虚拟机数量在主机之间平均分配虚拟机。定义调度策略，以启用集群中主机之间自动负载平衡。有关每个调度策略的详细说明，请参阅 [集群](#)

调度策略设置。

流程

1. 点 **Compute** → **Clusters** 并选择集群。
2. 点 **Edit**。
3. 单击 **Scheduling Policy** 选项卡。
4. 选择以下策略之一：
 - **none**
 - **vm_evenly_distributed**
 - a. 设置必须至少在一台主机上运行的虚拟机数量，以便在 **HighVmCount** 字段中启用负载均衡。
 - b. 在 **MigrationThreshold** 字段中定义最高利用率主机上的虚拟机数量和最低利用主机的虚拟机数量之间可接受的最大区别。
 - c. 在 **SpmVmGrace** 字段中定义要在 SPM 主机上保留虚拟机的插槽数量。
 - d. （可选）在 **HeSparesCount** 字段中，输入额外自托管引擎节点的数量，以便保留足够的可用内存，以便在 Manager 虚拟机迁移或关闭时启动它。如需更多信息，请参阅[为自托管引擎配置 Memory Slots Reserved](#)。
 - **evenly_distributed**
 - a. 在调度策略在 **CpuOverCommitDurationMinutes** 字段中采取行动前，设置主机可在定义的使用值外运行 CPU 负载的时间（以分钟为单位）。
 - b. 在 **HighUtilization** 字段中输入虚拟机开始迁移到其他主机的 CPU 使用率百分比。
 - c. （可选）在 **HeSparesCount** 字段中，输入额外自托管引擎节点的数量，以便保留足够的可用内存，以便在 Manager 虚拟机迁移或关闭时启动它。如需更多信息，请参阅[为自托管引擎配置 Memory Slots Reserved](#)。
 - d. 另外，为了避免主机过度利用所有物理 CPU，请定义虚拟 CPU 到物理 CPU 比例 - **VCpuToPhysicalCpuRatio**，其值介于 0.1 和 2.9 之间。当设置此参数时，在调度虚拟机时首选使用较低 CPU 的主机。
如果添加虚拟机会导致比例超过限制，则考虑 **VCpuToPhysicalCpuRatio** 和 CPU 使用率。

在运行的环境中，如果主机 **VCpuToPhysicalCpuRatio** 超过 2.5，一些虚拟机可能会平衡负载，并移到具有较低 **VCpuToPhysicalCpuRatio** 的主机。
 - **power_saving**
 - a. 在调度策略在 **CpuOverCommitDurationMinutes** 字段中采取行动前，设置主机可在定义的使用值外运行 CPU 负载的时间（以分钟为单位）。
 - b. 在 **LowUtilization** 字段中输入主机的 CPU 使用率百分比。
 - c. 在 **HighUtilization** 字段中输入虚拟机开始迁移到其他主机的 CPU 使用率百分比。
 - d. （可选）在 **HeSparesCount** 字段中，输入额外自托管引擎节点的数量，以便保留足够的可用内存，以便在 Manager 虚拟机迁移或关闭时启动它。如需更多信息，请参阅[为自托管引擎配置 Memory Slots Reserved](#)。

- d. (可选) 在 `HeSparesCount` 字段中, 输入额外目标引擎节点的数重, 以便保留足够的可用内存, 以便在 Manager 虚拟机迁移或关闭时启动它。如需更多信息, 请参阅[为自托管引擎配置 Memory Slots Reserved](#)。
5. 选择以下之一作为集群的调度程序优化 :
 - 选择 **Optimize for Utilization** 在调度中包含权重模块, 以允许选择最佳。
 - 如果请求超过十个, 选择 **Optimize for Speed** 以跳过主机权重。
 6. 如果您使用 OpenAttestation 服务器验证您的主机, 并使用 `engine-config` 工具设置服务器详情, 请选择 **Enable Trusted Service** 复选框。

OpenAttestation 和 Intel Trusted Execution Technology (Intel TXT)不再可用。

1. (可选) 选择 **启用 HA Reservation** 复选框, 使 Manager 能够监控高可用性虚拟机的集群容量。
2. (可选) 为集群中的虚拟机选择 **Serial Number 策略** :
 - **System Default** : 使用系统范围的默认值, 该默认值 [使用引擎配置工具和 DefaultSerialNumberPolicy](#) 和 `DefaultCustomSerialNumber` 密钥名称在 Manager 数据库中进行配置。`DefaultSerialNumberPolicy` 的默认值是使用 Host ID。如需更多信息, 请参阅[管理指南中的调度策略](#)。
 - **主机 ID** : 将每个虚拟机的序列号设置为主机的 UUID。
 - **虚拟机 ID** : 将每个虚拟机的序列号设置为虚拟机的 UUID。
 - **自定义序列号** : 将每个虚拟机的序列号设置为您在以下**自定义序列号**参数中指定的值。
3. 点击 **OK**。

2.3.2.10. 更新集群中的主机上的 MoM 策略

Memory Overcommit Manager 处理主机上的内存 balloon 和 KSM 功能。下一次主机重启后, 对这些功能的更改会传递到主机, 或处于维护模式后进入 **Up** 状态。但是, 如果需要, 您可以对一个主机立刻应用重要的变化, 方法是在主机状态为 **Up** 时同步 MoM 策略。以下过程必须单独在每个主机上执行。

流程

1. 单击 **Compute → Clusters**。
2. 点集群名称。这会打开详情视图。
3. 单击 **Hosts** 选项卡, 再选择需要更新的 MoM 策略的主机。
4. 单击 **Sync MoM Policy**。

主机上的 MoM 策略可以在不必将主机移至维护模式任何在重新变为 **Up** 的情况下进行更新。

2.3.2.11. 创建 CPU 配置集

CPU 配置文件定义集群中的一个虚拟机在其上运行的主机上可以访问的最大处理能力, 以对该主机可用的总处理能力的百分比表示。CPU 配置集基于数据中心的 CPU 配置集创建, 且不会自动应用到集群中的所有虚拟机; 它们必须手动分配给各个虚拟机才能使配置文件生效。

此流程假设您已在集群所属的数据中心下定义了一个或多个服务条目的 CPU 质量。

流程

1. 单击 **Compute → Clusters**。
2. 点集群名称。这会打开详情视图。
3. 点 **CPU Profiles** 选项卡。
4. 单击 **New**。
5. 为 CPU 配置集输入 **Name** 和 **Description**。
6. 从 **QoS** 列表中选择要应用到 CPU 配置集的服务质量。
7. 单击 **OK**。

2.3.2.12. 删除 CPU 配置集

从 Red Hat Virtualization 环境中删除现有 CPU 配置集。

流程

1. 单击 **Compute → Clusters**。
2. 点集群名称。这会打开详情视图。
3. 单击 **CPU Profiles** 选项卡，再选择要删除的 CPU 配置集。
4. 单击 **Remove**。
5. 单击 **OK**。

如果 CPU 配置集被分配给任何虚拟机，则这些虚拟机会自动 **分配默认** CPU 配置集。

2.3.2.13. 导入现有的 Red Hat Gluster Storage 集群

您可以将一个 Red Hat Gluster Storage 集群和属于集群的所有主机都导入到 Red Hat Virtualization Manager。

当您提供集群中任何主机的 IP 地址或主机名等详情时，**gluster peer status** 命令将通过 SSH 在那个主机上执行，然后显示属于集群一部分的主机列表。您必须手动验证每个主机的指纹，并为它们提供密码。如果集群中的一个主机停机或无法访问，您将无法导入集群。当新导入的主机没有安装 VDSM 时，bootstrap 脚本会在主机上安装所有需要的 VDSM 软件包，并重新启动它们。

流程

1. 单击 **Compute → Clusters**。
2. 单击 **New**。
3. 选择集群将属于的**数据中心**。
4. 输入集群的**名称和描述**。
5. 选中 **Enable Gluster Service**复选框，再选择 **Import existing gluster configuration**复选框。

只有在选择了 **Enable Gluster Service** 时，才会显示 **Import existing gluster configuration** 字段。

6. 在 **Hostname** 字段中，输入集群中任何服务器的主机名或 IP 地址。
显示主机 **SSH 指纹**，以确保您使用正确的主机进行连接。如果主机无法访问，或者有网络错误，则在 **Fingerprint** 字段中会显示一个 **Error in fetching fingerprint** 错误。
7. 输入服务器的**密码**，然后单击**确定**。
8. 这时将打开 **Add Hosts** 窗口，并显示属于集群一部分的主机列表。
9. 对于每个主机，输入 **Name** 和 **Root Password**。
10. 如果要对所有主机使用相同的密码，请选择 **Use a Common Password** 复选框，以在提供的文本字段中输入密码。
单击 **Apply** 以设置输入的密码 all hosts。

单击 **OK**，验证指纹是否有效，并提交您的更改。

引导脚本会在主机上安装所有必需的 VDSM 软件包，并重新启动它们。现在，您已成功将现有的 Red Hat Gluster Storage 集群导入到 Red Hat Virtualization Manager。

2.3.2.14. Add Hosts 窗口中的设置信息

通过 **Add Hosts** 窗口，您可以指定导入为支持 Gluster 的集群一部分的主机的详细信息。在选择了 **New Cluster** 窗口中的 **Enable Gluster Service** 复选框后，将显示此窗口并提供必要的主机详细信息。

表 2.13. 添加 Gluster 主机设置

字段	Description
使用常用密码	选择此复选框，对属于一个集群中的所有主机使用相同的密码。在 密码 字段中输入密码，然后单击 应用 按钮以在所有主机上设置密码。
Name	输入主机的名称。
hostname/IP	此字段会自动填充您在 New Cluster 窗口中提供的主机的完全限定域名或 IP。
Root 密码	在此字段中输入密码，为每个主机使用不同的 root 密码。此字段覆盖为集群中的所有主机提供的通用密码。
指纹	此时会显示主机指纹，以确保您使用正确的主机进行连接。此字段会自动填充您在 New Cluster 窗口中提供的主机的指纹。

2.3.2.15. 删除集群

在删除前，将所有主机从集群移出。



注意

您无法删除 **Default** 集群，因为它包含 **空白模板**。但是，您可以重命名 **Default** 集群，并将其添加到新数据中心。

流程

1. 点 **Compute** → **Clusters** 并选择集群。
2. 确保集群中没有主机。
3. 单击 **Remove**。
4. 点 **OK**

2.3.2.16. Memory Optimization

要增加主机上的虚拟机数量，您可以使用 *内存过量使用*，在其中为虚拟机分配的内存超过 RAM，并依赖于交换空间。

但是，内存过量使用有潜在的问题：

- 交换性能 - 交换空间较慢，消耗的 CPU 资源比 RAM 多，会影响虚拟机性能。过量交换会导致 CPU 增大。
- 内存不足 (OOM) killer - 如果主机耗尽交换空间，新进程无法启动，内核的 OOM 终止程序守护进程开始关闭活跃的进程，如虚拟机客户机。

为了帮助克服这些不足，您可以执行以下操作：

- 使用 *内存优化* 设置和 *内存过量使用管理器 (MoM)* 限制内存过量使用。
- 使交换空间足够大，以适应虚拟内存的最大潜力需求，并且剩余安全利润。
- 通过启用 *内存气球* 和 *内核同页合并 (KSM)* 减少虚拟内存大小。

2.3.2.17. 内存优化和内存过量使用

您可以通过选择其中一个 *内存优化* 设置来限制内存过量使用：**None (0%)**, **150%**, or **200%**。

每个设置代表 RAM 百分比。例如，有一个具有 64 GB RAM 的主机，选择 **150%** 表示您可以增加 32 GB 的内存，总内存为 96 GB。如果主机使用总共 4 GB 的 4 GB，则剩余的 92 GB 可用。您可以将其大部分分配给虚拟机 (**System** 标签页中的 **Memory Size**)，但应该考虑保留一些空间以减少出问题的可能。

对虚拟内存的需求激增可能会影响 M、内存膨胀和 KSM 重新定义虚拟内存的时间。要减少这个影响，请选择适合您运行的应用程序和工作负载的限制：

- 对于内存需求递增的工作负载，请选择较高的百分比，如 **200%** 或 **150%**。
- 对于更关键的应用程序或工作负载在内存需求增加时增加，请选择 **150%** 或 **None (0%)** 百分比。选择 **None** 有助于防止内存过量使用，但允许 MoM、内存 balloon 设备和 KSM 继续优化虚拟内存。



重要

在将配置部署到生产环境之前，请始终通过对各种条件进行测试来测试您的 **内存优化** 设置。

要配置 **Memory Optimization** 设置，点 **New Cluster** 或 **Edit Cluster** 窗口中的 **Optimization** 选项卡。请参阅 [集群优化设置说明](#)。

其他评论：

- [Host Statistics](#) 视图显示 有用的历史信息，以调整过量使用比率。
- 实际可用的内存无法实时确定，因为 KSM 和内存膨胀更改达到的内存大小。
- 当虚拟机达到虚拟内存限制时，新的应用程序无法启动。
- 当您计划在主机上运行的虚拟机数量时，请使用最大虚拟内存（物理内存大小和 **内存优化** 设置）作为起点。不要因内存优化而实现的较小的虚拟内存中因素，如内存膨胀和 KSM。

2.3.2.18. swap Space 和 Memory Overcommitment

红帽为配置交换空间 提供了这些建议。

在应用这些建议时，请按照指导将交换空间大小调整为“最后工作量内存”以获得最糟糕的情况。使用物理内存大小和 **内存优化** 设置作为估算总虚拟内存大小的基础。MoM、内存膨胀和 KSM 禁止虚拟内存的优化减少。



重要

为帮助防止 OOM 条件，使交换空间足够大，以处理最糟糕的情况，并且仍然具有安全利润。在部署到生产环境之前，始终在各种条件下测试您的配置。

2.3.2.19. Memory Overcommit Manager (MoM)

Memory Overcommit Manager (MoM) 分为两个事务：

- 它通过将 **Memory Optimization** 设置应用到集群中的主机来限制内存过量使用，如上一节中所述。
- 它通过管理 *内存 ballooning* 和 *KSM* 来优化内存，具体如以下部分所述。

您不需要启用或禁用 MoM。

当主机的可用内存低于 20% 时，像 **mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580** 的气球命令会记录到 Memory Overcommit Manager 日志文件 (`/var/log/vdsm/mom.log`)。

2.3.2.20. 内存膨胀

虚拟机从您分配给它们的完整虚拟内存数量开始。由于虚拟内存使用量超过 RAM，因此主机需要更多 swap 空间。如果启用，*内存膨胀* 可让虚拟机提供该内存中未使用的部分。空闲的内存可以被主机上的其他进程和虚拟机重复使用。减少内存占用率会降低交换的可能性，并提高性能。

virtio-balloon 软件包提供了内存膨胀设备和驱动程序，作为可加载的内核模块(LKM)。默认情况下，它被配置为自动加载。将模块添加到 `denylist` 或卸载时禁用 `ballooning`。

内存膨胀设备不直接协调；它们依赖于主机的 Memory Overcommit Manager (MoM) 流程来持续监控每个虚拟机的需求，并指示 balloon 设备增加或降低虚拟内存。

性能考虑：

- 对于需要持续高性能和低延迟的工作负载，红帽不推荐使用内存膨胀和过量使用。请参阅[配置高性能虚拟机、模板和池](#)。
- 当增加虚拟机密度（经济）比性能更重要时，使用内存膨胀。
- 内存膨胀不会影响 CPU 使用率。（KSM 消耗一些 CPU 资源，但消耗会保持在压力下的一致性。）

要启用内存膨胀，请单击 **New Cluster** 或 **Edit Cluster** 窗口中的 **Optimization** 选项卡。然后选择 **Enable Memory Balloon Optimization** 复选框。这个设置可在此集群中运行的虚拟机上启用内存使用过量。选择此复选框后，M 会尽可能启动膨胀，但会限制每个虚拟机的保证内存大小。请参阅[集群优化设置说明](#)。

此集群中的每个主机在状态更改为开机时会收到 balloon 策略更新。如果需要，您可以手动更新主机上的 balloon 策略，而无需更改状态。请参阅[在集群的主机上更新 MoM 策略](#)。

2.3.2.21. 内核同页合并(KSM)

当虚拟机运行时，它通常会为常见库和高使用数据等项目创建重复的内存页面。另外，运行类似客户机操作系统和应用程序的虚拟机会在虚拟内存中生成重复的内存页面。

启用后，*内核同页合并* (KSM) 检查主机上的虚拟内存，消除了重复内存页面，并在多个应用程序和虚拟机间共享剩余的内存页面。这些共享内存页面标记为写时复制；如果虚拟机需要向该页面写入更改，它会首先进行复制，然后再将其修改写入到该副本。

启用 KSM 时，M 会管理 KSM。您不需要手动配置或控制 KSM。

KSM 通过两种方式增加虚拟内存性能：由于更频繁地使用共享内存页面，因此主机更有可能将其存储在缓存中或主内存中，从而提高了内存访问速度。另外，有内存过量使用，KSM 会减少虚拟内存空间，从而减少交换性能的可能性。

KSM 消耗的 CPU 资源超过内存膨胀。在压力下，CPU KSM 消耗量保持一致性。在主机上运行相同的虚拟机和应用程序，与运行相同虚拟机和应用程序相比，KSM 有机会合并内存页面。如果您运行大多数不同的虚拟机和应用程序，使用 KSM 的 CPU 成本可能会降低其好处。

性能考虑：

- 在 KSM 守护进程合并大量内存后，内核内存核算统计最终可能会相互冲突。如果您的系统有大量可用内存，可以通过禁用 KSM 来提高性能。
- 对于需要持续高性能和低延迟的工作负载，红帽不推荐使用 KSM 和过量使用。请参阅[配置高性能虚拟机、模板和池](#)。
- 在增加虚拟机密度（经济）时，使用 KSM 比性能更重要。

要启用 KSM，请单击 **New Cluster** 或 **Edit Cluster** 窗口中的 **Optimization** 选项卡。然后选择“**启用 KSM**”复选框。此设置可让 MoM 在需要时运行 KSM，并在生成内存时可以降低其 CPU 的成本。请参阅[集群优化设置说明](#)。

2.3.2.22. UEFI 和 Q35 芯片组

Intel Q35 芯片组（新虚拟机的默认芯片组）包括支持统一可扩展固件接口(UEFI)，取代传统的 BIOS。

或者，您可以将虚拟机或集群配置为使用旧的 Intel i440fx 芯片组，该芯片组不支持 UEFI。

UEFI 与旧的 BIOS 相比提供了几个优势，包括：

- 现代引导装载程序
- SecureBoot，用于验证引导装载程序的数字签名
- GUID 分区表(GPT)，它启用大于 2 TB 的磁盘

要在虚拟机上使用 UEFI，您必须将虚拟机的集群配置为 4.4 或更高版本。然后，您可以为任何现有虚拟机设置 UEFI，或者设置为集群中新虚拟机的默认 BIOS 类型。可用的选项如下：

表 2.14. 可用的 BIOS 类型

BIOS 类型	Description
带有传统 BIOS 的 Q35 Chipset	没有 UEFI 的旧 BIOS（用于兼容版本 4.4 的集群的默认设置）
使用 UEFI BIOS 的 Q35 Chipset	使用 UEFI 的 BIOS
带有 SecureBoot 的 Q35 Chipset	带有 SecureBoot 的 UEFI，它验证引导装载程序的数字签名
legacy	带有传统 BIOS 的 i440fx 芯片组

在安装操作系统前设置 BIOS 类型

在安装操作系统前，您可以将虚拟机配置为使用 Q35 芯片组和 UEFI。在安装操作系统后，不支持将虚拟机从旧的 BIOS 转换为 UEFI。

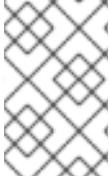
2.3.2.23. 配置集群以使用 Q35 Chipset 和 UEFI

将集群升级到 Red Hat Virtualization 4.4 后，集群中的所有虚拟机都运行 4.4 版本 VDSM。您可以配置集群的默认 BIOS 类型，该类型决定了集群中您创建的任何新虚拟机的默认 BIOS 类型。如果需要，您可以在创建虚拟机时指定不同的 BIOS 类型来覆盖集群的默认 BIOS 类型。

流程

1. 在虚拟机门户或管理门户中，点 **Compute → Clusters**。
2. 选择一个集群并点 **Edit**。
3. 点 **General**。
4. 点 BIOS 类型下拉菜单在集群中的新虚拟机定义默认 **BIOS 类型**，并选择以下任一操作：
 - legacy
 - 带有传统 BIOS 的 Q35 Chipset
 - 使用 UEFI BIOS 的 Q35 Chipset

- 带有 SecureBoot 的 Q35 Chipset
5. 从 **兼容性版本** 下拉菜单中选择 **4.4**。Manager 检查所有正在运行的主机是否都与 4.4 兼容，如果兼容，则 Manager 使用 4.4 功能。
 6. 如果集群中的任何现有虚拟机应该使用新的 BIOS 类型，请将它们配置为这样做。现在，集群中配置为使用 BIOS 类型 **Cluster default** 的新虚拟机现在使用您选择的 BIOS 类型。如需更多信息，请参阅[配置虚拟机以使用 Q35 Chipset 和 UEFI](#)。



注意

由于只能在安装操作系统前更改 BIOS 类型，所以对于配置为使用 BIOS 类型 **Cluster default** 的任何现有虚拟机，请将 BIOS 类型更改为之前的默认集群 BIOS 类型。否则，虚拟机可能无法引导。或者，您可以重新安装虚拟机的操作系统。

2.3.2.24. 配置虚拟机以使用 Q35 Chipset 和 UEFI

在安装操作系统前，您可以将虚拟机配置为使用 Q35 芯片组和 UEFI。将虚拟机从旧的 BIOS 转换为 UEFI，或从 UEFI 转换为旧 BIOS 可能会阻止虚拟机引导。如果更改现有虚拟机的 BIOS 类型，请重新安装操作系统。



警告

如果虚拟机的 BIOS 类型设为 **Cluster default**，更改集群的 BIOS 类型会更改虚拟机的 BIOS 类型。如果虚拟机安装了操作系统，更改集群 BIOS 类型可能会导致引导虚拟机失败。

流程

配置虚拟机以使用 Q35 芯片组和 UEFI：

1. 在虚拟机门户或管理门户中点 **Compute → Virtual Machines**。
2. 选择虚拟机并点 **Edit**。
3. 在 **General** 选项卡中，单击 **Show Advanced Options**。
4. 单击 **System → Advanced Parameters**。
5. 从 **BIOS 类型** 下拉菜单中选择 以下内容之一：
 - 集群默认
 - 带有传统 BIOS 的 Q35 Chipset
 - 使用 UEFI BIOS 的 Q35 Chipset
 - 带有 SecureBoot 的 Q35 Chipset
6. 单击 **OK**。

7. 在 Virtual Machine Portal 或 Administration Portal 中关闭虚拟机。下次启动虚拟机时，它将使用您选择的新 BIOS 类型运行。

2.3.2.25. 更改集群兼容性版本

Red Hat Virtualization 集群有一个兼容版本。集群兼容性版本表示集群中所有主机支持的 Red Hat Virtualization 的功能。集群兼容性根据集群中功能最低的主机操作系统版本来设置。

先决条件

- 要更改集群兼容性级别，您必须首先将集群中的所有主机更新为支持您需要的兼容性级别。检查主机旁边是否存在指示有可用的更新的图标。

限制

- 在将集群兼容性级别升级到 4.6 后，virtio NIC 会作为不同的设备枚举。因此，可能需要重新配置 NIC。红帽建议您在升级集群前测试虚拟机，方法是在虚拟机上将集群兼容性级别设置为 4.6 并验证网络连接。
如果虚拟机的网络连接失败，在升级集群前，使用与当前模拟机器匹配的自定义模拟机器配置虚拟机，例如 pc-q35-rhel8.3.0 适用于 4.5 兼容性版本。


流程

1. 在管理门户中，点 **Compute** → **Clusters**。
2. 选择要更改的集群并点击 **Edit**。
3. 在 **General** 选项卡中，将 **Compatibility Version** 更改为所需的值。
4. 点击 **确定**。此时会打开 **Change Cluster Compatibility Version** 确认对话框。
5. 点 **OK** 确认。



重要

错误消息可能会警告某些虚拟机和模板配置不正确。要修复此错误，请手动编辑每个虚拟机。**Edit Virtual Machine**窗口提供了额外的验证和警告来显示正确的内容。有时问题会自动解决，虚拟机的配置只需要再次保存。编辑完每个虚拟机后，您将能够更改集群兼容性版本。

在更新了集群兼容性版本后，您必须通过从管理门户重启或使用 REST API 来更新所有正在运行的或暂停虚拟机的集群兼容性版本，或使用客户端操作系统中的 REST API 更新它们。需要重启的虚拟机将标记为待处理更改图标()。您无法更改处于预览的虚拟机快照的集群兼容性版本。您必须首先提交或撤销预览。

在自托管引擎环境中，管理器虚拟机不需要重新启动。

虽然您可以在以后方便的时候重新启动虚拟机，但强烈建议您立即重新启动，以便虚拟机使用最新的配置。旧配置没有更新运行的虚拟机，在重启前，如果对虚拟机进行其他更改，新的配置会被覆盖。

在更新了数据中心中所有集群和虚拟机的兼容性版本后，您可以更改数据中心本身的兼容性版本。

2.4. 逻辑网络

2.4.1. 逻辑网络任务

2.4.1.1. 执行网络任务

Network → **Networks** 为用户提供一个中央位置，供用户执行逻辑网络相关的操作，并根据每个网络的属性或与其他资源关联搜索逻辑网络。通过**新建**、**编辑**和**删除**按钮，您可以在数据中心内创建、更改的属性或删除逻辑网络。

点击每个网络名称，并使用详情视图中的标签页执行功能，包括：

- 将网络附加到集群和主机
- 从虚拟机和模板中删除网络接口
- 为用户添加或删除权限以访问和管理网络

这些功能也可以通过每个单独的资源访问。



警告

如果有任何主机正在运行，则不要更改数据中心或集群中的网络，因为这可能导致主机变得不可访问。

重要

如果您计划使用 Red Hat Virtualization 节点提供任何服务，请记住，如果 Red Hat Virtualization 环境停止操作，该服务将停止。

这适用于所有服务，但您应该特别意识到在 Red Hat Virtualization 上运行以下内容：

- 目录服务
- DNS
- 存储

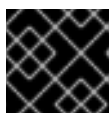
2.4.1.2. 在数据中心或集群中创建新的逻辑网络

创建逻辑网络并在数据中心或数据中心内定义其使用。

流程

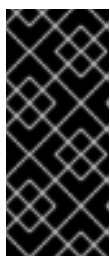
1. 点 **Compute** → **Data Centers** 或 **Compute** → **Clusters**。
2. 点数据中心或集群名称。**Details** 视图将打开。
3. 单击 **逻辑网络** 选项卡。
4. 打开 **New Logical Network** 窗口：
 - 从数据中心详情视图中，单击 **New**。

- 在集群详情视图中点 **Add Network**。
5. 输入逻辑网络的 **Name**、**Description** 和注释。
 6. 可选：启用 **VLAN** 标记。
 7. 可选：禁用 **VM Network**。
 8. 可选：选择 **Create on external provider** 复选框。这可禁用网络标签和 VM 网络。有关详细信息，请参阅 [外部提供程序](#)。
 - a. 选择 **External Provider**。**External Provider** 列表不包含处于只读模式下的外部提供程序。
 - b. 要创建内部隔离网络，请在 **External Provider** 列表上选择 **ovirt-provider-ovn**，并**保持连接到物理网络** 已清除。
 9. 输入新标签，或者在 **Network Label** 文本字段中为逻辑网络选择现有标签。
 10. 对于 **MTU**，可选择 **Default (1500)**，或者选择 **Custom** 并指定自定义值。



重要

在外部提供程序上创建网络后，您无法更改网络的 MTU 设置。



重要

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

11. 如果您从 **External Provider** 下拉列表选择了 **ovirt-provider-ovn**，请定义网络是否应该实施安全组。有关详细信息，请参阅 [逻辑网络常规设置说明](#)。
12. 在 **Cluster** 选项卡中，选择将网络分配到的集群。您还可以指定逻辑网络是否是必需的网络。
13. 如果选中 **Create on external provider** 复选框，则会看到 **Subnet** 选项卡。从 **子网** 选项卡中，选择 **创建子网** 并输入 **名称**、**CIDR** 和 **网关地址**，然后为逻辑网络提供的子网选择 **IP 版本**。您还可以根据需要添加 DNS 服务器。
14. 在 **vNIC Profiles** 选项卡中，根据需要 **将 vNIC 配置集** 添加到逻辑网络中。
15. 点击 **OK**。

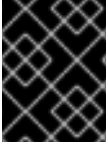
如果您为逻辑网络输入标签，则会自动添加到具有该标签的所有主机网络接口。



注意

当创建新逻辑网络或更改用作显示网络的现有逻辑网络时，必须在网络可用或应用更改前重启使用该网络的任何正在运行的虚拟机。

2.4.1.3. 编辑逻辑网络

**重要**

如果没有与主机上的网络配置同步，则无法编辑或移动逻辑网络。请参阅 [编辑主机网络接口](#)，并在[如何在如何同步您的网络时将逻辑网络分配给主机](#)。

**重要**

当更改用作显示网络的现有逻辑网络的虚拟机网络属性时，无法在已在运行的虚拟机的主机上启动新的虚拟机。只有更改 **VM Network** 属性后没有运行虚拟机的主机才能启动新虚拟机。

流程

1. 单击 **Compute** → **Data Centers**。
2. 点数据中心名称。这会打开详情视图。
3. 单击 **Logical Networks** 选项卡，再选择逻辑网络。
4. 点 **Edit**。
5. 编辑必要的设置。

**注意**

您可以编辑新网络或现有网络的名称，但默认网络除外，而无需停止虚拟机。

6. 单击 **OK**。

**注意**

多主机网络配置会自动将更新的网络设置应用到分配到网络的所有主机。只有在使用网络的虚拟机停机时，才能应用更改。您不能重命名已在主机上配置的逻辑网络。在使用该网络的虚拟机或模板运行时，您无法禁用 **VM Network** 选项。

2.4.1.4. 删除逻辑网络

您可以从 **Network** → **Networks** 或 **Compute** → **Data Centers** 中删除一个逻辑网络。以下步骤演示了如何删除与数据中心关联的逻辑网络。对于 **Red Hat Virtualization** 环境，您必须至少有一个逻辑网络用作 **ovirtmgmt** 管理网络。

流程

1. 单击 **Compute** → **Data Centers**。
2. 点数据中心的名称。这会打开详情视图。
3. 点逻辑网络 选项卡，以列出数据中心的逻辑网络。
4. 选择逻辑网络，然后单击删除。
5. (可选) 从提供程序选择 **Remove external network (s)** 和复选框，以便在外部提供者提供网络时从 **Manager** 中删除逻辑网络或从外部供应商中删除。如果外部供应商处于只读模式，则勾选框将灰显。
6. 单击 **OK**。

逻辑网络已从 **Manager** 中删除，且不再可用。

2.4.1.5. 将非管理逻辑网络配置为默认路由

集群中主机使用的默认路由通过管理网络(**ovirtmgmt**)。以下流程提供将非管理逻辑网络配置为默认路由的说明。

先决条件：

- 如果使用 **default_route** 自定义属性，则需要从所有附加的主机清除自定义属性，然后按照以下步骤操作。

配置默认路由角色

1. 单击 **Network** → **Networks**。
2. 点非管理逻辑网络的名称，将其配置为默认路由，以访问其详细信息。
3. 点 **Clusters** 选项卡。
4. 单击 **Manage Network**。这将打开 **Manage Network** 窗口。
5. 为适当的集群选择默认路由复选框。
6. 单击 **OK**。

当网络附加到主机时，将在您选择的网络上设置主机的默认路由。建议您在将任何主机添加到集群中前配置默认路由角色。如果集群已经包含主机，则它们可能会不同步，直到您将更改同步至它们。

IPv6 的重要限制

- 对于 IPv6，Red Hat Virtualization 仅支持静态寻址。
- 如果两个网络共享一个网关（在同一子网中），您可以将默认路由角色从管理网络 (ovirtmgmt) 移到另一个逻辑网络。
- 如果主机和管理器不在同一子网中，则管理器将断开与主机的连接，因为删除了 IPv6 网关。
- 将默认路由角色移到非管理网络中，会从网络接口中删除 IPv6 网关，并生成警报：“On cluster *clustername* the 'Default Route Role' network is no longer network ovirtmgmt.IPv6 网关正在从此网络中删除”。

2.4.1.6. 在主机上添加静态路由

您可以使用 `nmstate` 为主机添加静态路由。此方法要求您直接配置主机，而无需使用 Red Hat Virtualization Manager。

只要相关的路由网桥、接口或绑定存在并且具有 IP 地址，您添加的 `static-route` 就会保留。否则，系统会移除静态路由。



重要

除了在主机上添加或删除静态路由外，请务必使用 RHV Manager 在集群中配置主机网络设置。详情请查看 [Network Manager Stateful Configuration \(nmstate\)](#)。



注意

自定义 `static-route` 会保留，只要其 `interface/bond` 存在且具有 IP 地址。否则，它将被删除。

因此，VM 网络的行为与非 VM 网络不同：

- VM 网络基于网桥。将网络从一个接口/`bond` 移动到另一个接口不会影响虚拟机网络上的路由。
- 非 VM 网络基于接口。将网络从一个接口/`bond` 移到另一个接口，会删除与 Non-VM 网络相关的路由。

前提条件

这个过程需要 `nmstate`，这只在您的环境使用时可用：

- Red Hat Virtualization Manager 版本 4.4
- 基于 Red Hat Enterprise Linux 8 的 Red Hat Enterprise Linux 主机和 Red Hat Virtualization 主机

流程

1. 连接到您要配置的主机。
2. 在主机上，创建一个 `static_route.yml` 文件，其中包含以下示例内容：

```
routes:
  config:
  - destination: 192.168.123.0/24
    next-hop-address: 192.168.178.1
    next-hop-interface: eth1
```

3. 将示例值替换为您的网络实际值。
4. 要将流量路由到添加的二级网络，请使用 `next-hop-interface` 指定接口或网络名称。

- 要使用非虚拟机网络，请指定 `eth1` 等接口。
- 要使用虚拟机网络，请指定同时是网桥名称（如 `net1`）的网络名称。

5. 运行这个命令：

```
$ nmstatectl set static_route.yml
```

验证步骤

- 使用您在 `static_route.yml` 中设置的目的地参数值运行 IP route 命令 `ip route`。这应该会显示所需的路由。例如，运行以下命令：

```
$ ip route | grep 192.168.123.0`
```

其他资源

- [Network Manager Stateful Configuration \(nmstate\)](#)
- [删除主机上的静态路由](#)

2.4.1.7. 删除主机上的静态路由

您可以使用 `nmstate` 从主机中删除静态路由。此方法要求您直接配置主机，而无需使用 Red Hat Virtualization Manager。



重要

除了在主机上添加或删除静态路由外，请务必使用 RHV Manager 在集群中配置主机网络设置。详情请查看 [Network Manager Stateful Configuration \(nmstate\)](#)。



注意

自定义 `static-route` 会保留，只要其 `interface/bond` 存在且具有 IP 地址。否则，它将被删除。

因此，VM 网络的行为与非 VM 网络不同：

- VM 网络基于网桥。将网络从一个接口/`bond` 移动到另一个接口不会影响虚拟机网络上的路由。
- 非 VM 网络基于接口。将网络从一个接口/`bond` 移到另一个接口，会删除与 Non-VM 网络相关的路由。

前提条件

这个过程需要 `nmstate`，这只在您的环境使用时可用：

- Red Hat Virtualization Manager 版本 4.4
- 基于 Red Hat Enterprise Linux 8 的 Red Hat Enterprise Linux 主机和 Red Hat Virtualization 主机

流程

1. 连接到您要重新配置的主机。

2. 在主机上，编辑 `static_route.yml` 文件。
3. 插入行 `state: absent`，如下例所示。
4. 在 `interfaces: []` 的括号间添加 `next-hop-interface`。其结果应当类似于此处显示的示例。

```
routes:
  config:
    - destination: 192.168.123.0/24
      next-hop-address: 192.168.178.
      next-hop-interface: eth1
      state: absent
  interfaces: [{"name": eth1}]
```

5. 运行这个命令：

```
$ nmstatectl set static_route.yml
```

验证步骤

- 使用您在 `static_route.yml` 中设置的目的地参数值运行 IP route 命令 `ip route`。这应该不再显示所需的路由。例如，运行以下命令：

```
$ ip route | grep 192.168.123.0`
```

其他资源

- [Network Manager Stateful Configuration \(nmstate\)](#)
- [在主机上添加静态路由](#)

2.4.1.8. 查看或编辑逻辑网络的网关

用户可以为逻辑网络定义网关以及 IP 地址和子网掩码。当主机上存在多个网络，并且流量应通过指定的网络而不是默认网关进行路由时需要这样做。

如果主机上存在多个网络，且未定义网关，返回的流量将通过默认网关路由，该网关可能无法到达预

期的目的地。这会导致用户无法 ping 主机。

当接口上线或停机时，Red Hat Virtualization 会自动处理多个网关。

流程

1. 单击 **Compute** → **Hosts**。
2. 单击主机的名称。这会打开详情视图。
3. 单击 **Network Interfaces** 选项卡，以列出附加到主机的网络接口，以及它们的配置。
4. 单击 **Setup Host Networks**。
5. 将光标悬停在分配的逻辑网络上，然后点铅笔图标。此时将打开 **Edit Management Network** 窗口。

Edit Management Network 窗口显示网络名称、引导协议以及 IP、子网掩码和网关地址。可以通过选择 **静态** 引导协议来手动编辑地址信息。

2.4.1.9. 逻辑网络常规设置说明

下表描述了新逻辑网络和编辑逻辑网络窗口的常规选项卡的设置。

表 2.15. New Logical Network 和 Edit Logical Network 设置

字段名称	Description
Name	<p>逻辑网络的名称。此文本字段必须是唯一名称，包含大写字母和小写字母、数字、连字符和下划线的任意组合。</p> <p>请注意，尽管逻辑网络的名称可能超过 15 个字符，并且可以包含非 ASCII 字符，但 on-host 标识符 (<code>vdsm_name</code>) 将与您定义的名称不同。有关显示这些名称映射的信息，请参阅 将 VDSM 名称映射到逻辑网络名称。</p>

字段名称	Description
Description	逻辑网络的描述。此文本字段具有 40 个字符的限值。
注释	用于添加与逻辑网络相关的纯文本可读注释的字段。
在外部供应商上创建	<p>允许您将逻辑网络创建到作为外部提供者添加到 Manager 的 OpenStack 网络实例中。</p> <p>external Provider - 允许您选择要在其上创建逻辑网络的外部供应商。</p>
启用 VLAN 标记	VLAN 标记是一种安全功能，可为逻辑网络上传输的所有网络流量具有特殊特征。标记为 VLAN 的流量无法通过没有该特征的接口读取。在逻辑网络上使用 VLAN 还支持单个网络接口与多个网络接口关联，不同的是 VLAN 标记的逻辑网络。如果启用了 VLAN 标记，在文本条目字段中输入数字值。
VM Network	如果只有虚拟机使用此网络，则选择这个选项。如果网络用于不涉及虚拟机（如存储通讯）的流量，请不要选中此复选框。
端口隔离	如果已设置此项，则同一主机上的虚拟机会被禁止在此逻辑网络上相互通信和查看。要使此选项在不同的虚拟机监控程序上工作，交换机需要在连接到虚拟机监控程序的相应端口/VLAN 上配置使用 PVLAN/Port 隔离，而不用任何 hairpin 设置重新显示帧。
MTU	选择“默认”，这会将最大传输单元(MTU)设置为父括号 () 给出的值，或者 Custom 来为逻辑网络设置自定义 MTU。您可以使用它来将新逻辑网络支持的 MTU 与它接口的硬件支持的 MTU 匹配。如果选择了 Custom ，在文本条目字段中输入数字值。 重要 ：如果更改网络的 MTU 设置，您必须将此更改传播到网络中的正在运行的虚拟机：Hot unplug 和 replug each virtual machine 的 vNIC（应该应用 MTU 设置），或重启虚拟机。否则，当虚拟机迁移到另一台主机时，这些接口会失败。如需更多信息，请参阅 网络 MTU 更改后，一些虚拟机和网桥有旧的 MTU，查看数据包丢弃 和 BZ#1766414 。
Network Label	允许您为网络指定一个新标签，或者从已附加到主机网络接口的现有标签中选择。如果您选择了现有标签，则逻辑网络将自动分配给具有该标签的所有主机网络接口。

字段名称	Description
安全组	允许您将安全组分配给此逻辑网络上的端口。 禁用 禁用安全组功能。 Enabled 启用功能。当端口创建并附加到这个网络时，它将通过启用端口安全性进行定义。这意味着，对/虚拟机的访问/虚拟机的访问会受到当前调配的安全组约束。 从 Configuration 继承，端口可继承 为所有网络定义的配置文件中的行为。默认情况下，该文件将禁用安全组。详情请参阅 将安全组分配给逻辑网络 。

2.4.1.10. 逻辑网络集群设置说明

下表描述了新建逻辑网络窗口的集群选项卡的设置。

表 2.16. 新的逻辑网络 设置

字段名称	Description
Attach/Detach Network to/from Cluster(s)	<p>允许您从数据中心中的集群附加或分离逻辑网络，并指定逻辑网络是否为单个集群必需的网络。</p> <p>Name - 设置要应用到的集群名称。此值无法编辑。</p> <p>Attach All - 允许您向数据中心的所有集群附加或分离逻辑网络。或者，选择或清除要附加或从给定集群分离的每个集群名称旁边的 Attach 复选框。</p> <p>必需所有 - 允许您指定逻辑网络是所有集群中需要的网络。或者，选择或清除每个集群名称旁边的 Required 复选框，以指定逻辑网络是给定集群的所需网络。</p>

2.4.1.11. 逻辑网络 vNIC 配置文件设置说明

下表描述了新建逻辑网络窗口的 vNIC Profiles 选项卡的设置。

表 2.17. 新的逻辑网络 设置

字段名称	Description
------	-------------

字段名称	Description
vNIC 配置集	<p>允许您指定一个或多个逻辑网络的 vNIC 配置集。您可以通过点击 vNIC 配置集旁边的加号或减去按钮，向逻辑网络添加或删除 vNIC 配置集。第一个字段用于输入 vNIC 配置集的名称。</p> <p>public - 允许您指定配置集是否可供所有用户使用。</p> <p>QoS - 允许您指定 vNIC 配置集的网络服务质量(QoS)配置集。</p>

2.4.1.12. 使用 Manage Networks Window 为逻辑网络指定特定流量类型

指定逻辑网络的流量类型，以优化网络流量流。

流程

1. 单击 **Compute** → **Clusters**。
2. 点集群名称。这会打开详情视图。
3. 单击 **逻辑网络** 选项卡。
4. 单击 **Manage Networks**。
5. 选中适当的复选框和单选按钮。
6. 单击 **OK**。



注意

外部提供者提供的逻辑网络必须用作虚拟机网络；不能分配显示或迁移等特殊集群角色。

2.4.1.13. Manage Networks 窗口中的 Settings 解释

下表描述了 **Manage Networks** 窗口的设置。

表 2.18. 管理网络设置

字段	description/Action
分配	将逻辑网络分配到集群中的所有主机。
必需	标记为"required"的网络必须保持正常运行状态，以便它能够正常工作。如果需要网络功能，则与它关联的任何主机都无法运行。
VM Network	标记为"VM Network"的逻辑网络承载与虚拟机网络相关的网络流量。
显示网络	标记为"显示网络"的逻辑网络承载与 SPICE 和虚拟网络控制器相关的网络流量。
迁移网络	标记为"Migration Network"的逻辑网络执行虚拟机和存储迁移流量。如果此网络上发生中断，则改为使用管理网络（默认情况下 <code>ovirtmgmt</code> ）。

2.4.1.14. 在 NIC 上配置虚拟功能



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](#)

单根 I/O 虚拟化(SR-IOV)使您能够使用物理功能(PF)和虚拟功能(VF)将每个 PCIe 端点用作多个单独的设备。PCIe 卡可以有一个到 8 个 PF。每个 PF 都可以有多个 VF。可以拥有的 VF 数量取决于具体类型的 PCIe 设备。

要配置支持 SR-IOV 的网络接口控制器(NIC)，您可以使用 **Red Hat Virtualization Manager**。您可以在每个 NIC 上配置 VF 数量。

您可以配置 VF，如您要配置独立 NIC，包括：

- 将一个或多个逻辑网络分配给 VF。


- 使用 VF 创建绑定接口。
- 为直接设备透传分配 vNIC。

默认情况下，所有虚拟网络都可以访问虚拟功能。您可以禁用此默认值，并指定哪些网络有权访问虚拟功能。

前提条件

- 要将 vNIC 附加到 VF，必须启用其 `passthrough` 属性。详情请查看 [enable _Passthrough_on_a_vNIC_Profile](#)。

流程

1. 单击 **Compute** → **Hosts**。
2. 单击支持 SR-IOV 的主机的名称。这会打开详情视图。
3. 单击 **Network Interfaces** 选项卡。
4. 单击 **Setup Host Networks**。
5. 选择一个支持 SR-IOV 的 NIC，标记为 ，然后点铅笔图标。
6. 可选：要更改虚拟功能的数量，请点 **Number of VFs setting** 下拉菜单，并编辑 **Number of VFs** 文本字段。



重要

更改 VF 的数量会在创建新 VF 前删除网络接口上所有之前的 VF。这包括直接附加虚拟机的任何 VF。

7. 可选：要限制哪些虚拟网络可以访问虚拟功能，请选择 **Specific network**。
 - a. 选择应有权访问 VF 的网络，或者使用 **Labels** 根据其网络标签选择网络。
8. 点击 **OK**。
9. 在 **Setup Host Networks** 窗口中，单击 **OK**。

2.4.2. 虚拟网络接口卡(vNIC)

2.4.2.1. vNIC 配置文件概述

虚拟网络接口卡(vNIC)配置集是可应用于 **Manager** 中的独立虚拟网络接口卡的设置集合。vNIC 配置集允许您将 **Network QoS** 配置集应用到 vNIC，启用或禁用端口镜像，并添加或删除自定义属性。vNIC 配置集还提供新增的管理权限层，以授予这些配置集供特定用户使用（假设）这些配置集。这样，您可以控制不同用户从给定网络接收的服务质量。

2.4.2.2. 创建或编辑 vNIC 配置集

创建或编辑 **Virtual Network Interface Controller (vNIC)**配置集，以注册用户和组的网络带宽。



注意

如果您要启用或禁用端口镜像，在编辑前，使用相关配置集的所有虚拟机都必须处于 **down** 状态。

流程

1. 单击 **Network** → **Networks**。

2. 点逻辑网络的名称。这会打开详情视图。
3. 点 **vNIC Profiles** 选项卡。
4. 点 **New** 或 **Edit**。
5. 输入配置文件的名称和描述。
6. 从 **QoS** 列表中选择相关的服务质量策略。
7. 从下拉列表中选择 **Network Filter**，以管理进出虚拟机的网络数据包的流量。有关网络过滤器的更多信息，请参阅 *Red Hat Enterprise Linux Virtualization Deployment and Administration Guide* 中的[应用网络过滤](#)。
8. 选择 **Passthrough** 复选框，以启用 vNIC 的透传并允许直接分配虚拟功能。启用 **passthrough** 属性将禁用 **QoS**、网络过滤和端口镜像，因为它们不兼容。有关 **passthrough** 的更多信息，请参阅在 [vNIC Profile](#) 上启用 **Passthrough**。
9. 如果选择了 **Passthrough**，可以选择选择 **Migratable** 复选框，以禁用使用这个配置集的 vNIC 迁移。如果保留此复选框，请参阅[虚拟机管理指南](#)中的[带有 SR-IOV-Enabled vNIC 的虚拟机的其他先决条件](#)。
10. 使用 **Port Mirroring** 和 **Allow all users to use this Profile** 复选框来切换这些选项。
11. 从自定义属性列表中选择自定义属性，它默认显示 **Please select a key...**。使用 **+** 和 **-** 按钮添加或删除自定义属性。
12. 点击 **OK**。

将这个配置集应用到用户和组，以规范其网络带宽。如果您编辑了 vNIC 配置集，则必须重启虚拟机或热拔，如果客户机操作系统支持 vNIC 热插和热拔，则热插拔 vNIC。

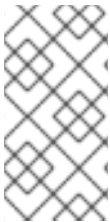
2.4.2.3. VM Interface Profile 窗口中的设置信息

表 2.19. VM Interface Profile 窗口

字段名称	Description
Network	要将 vNIC 配置集应用到的可用网络下拉列表。
Name	vNIC 配置集的名称。这必须是一个唯一名称，其任意组合使用大写和小写字母、数字、连字符和下划线(1 到 50 个字符)。
Description	vNIC 配置集的描述。建议使用此字段，但不强制设置。
QoS	可用的网络服务质量策略的下拉列表，以应用到 vNIC 配置集。QoS 策略规定了 vNIC 的入站和出站网络流量。
网络过滤器	<p>适用于 vNIC 配置集的可用网络过滤器的下拉列表。网络过滤器通过过滤可发送到虚拟机的数据包类型以及从虚拟机来改善网络安全性。默认过滤器是 vdsm-no-mac-spoofing，它是一个 no-mac-spoofing 和 no-arp-mac-spoofing 的组合。有关 libvirt 提供的网络过滤器的更多信息，请参阅 <i>Red Hat Enterprise Linux Virtualization 部署和管理指南</i> 的 预先存在的网络过滤器 部分。</p> <p>将 <No Network Filter> 用于虚拟机 VLAN 和绑定。在可信虚拟机上，选择不使用网络过滤器可提高性能。</p> <div style="display: flex; align-items: flex-start;">  <div> <p>注意</p> <p>红帽不再支持使用 engine-config 工具将 EnableMACAntiSpoofingFilterRules 参数设置为 false 来禁用过滤器。使用 <No Network Filter> 选项替代。</p> </div> </div>
Passthrough	<p>切换 passthrough 属性的复选框。直通允许 vNIC 直接连接到主机 NIC 的虚拟功能。如果 vNIC 配置集附加到虚拟机，则无法编辑 passthrough 属性。</p> <p>如果启用了 passthrough，则 vNIC 配置集中禁用了 QoS、网络过滤器和端口镜像。</p>
Migratable	<p>一个复选框来切换是否使用这个配置集的 vNIC。在常规 vNIC 配置集中默认启用迁移；选择复选框且无法更改。选择了 Passthrough 复选框后，Migratable 变为可用状态，并在需要时可以取消选择以禁用 passthrough vNIC 的迁移。</p>

字段名称	Description
故障切换	一个下拉菜单，用于选择充当故障切换设备的可用 vNIC 配置集。仅在选中 Passthrough 和 Migratable 复选框时才可用。
端口镜像	切换端口镜像的复选框。端口镜像将逻辑网络上的第 3 层网络流量复制到虚拟机上的虚拟接口。默认没有选择它。详情请查看 技术参考中的端口镜像 。
设备自定义属性	一个下拉菜单，用于选择应用到 vNIC 配置集的可用自定义属性。使用 + 和 - 按钮分别添加和删除属性。
允许所有用户使用这个配置集	将配置集可用性切换为环境中的所有用户的复选框。默认会被选择。

2.4.2.4. 在 vNIC 配置文件中启用 Passthrough



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](#)

vNIC 配置集的 **passthrough** 属性可让 vNIC 直接连接到支持 SR-IOV 的 NIC 的虚拟功能(VF)。然后，vNIC 将绕过软件网络虚拟化，直接连接到 VF 进行直接设备分配。

如果 vNIC 配置集已附加到 vNIC，则无法启用 **passthrough** 属性，这个过程会创建一个新配置集来避免这种情况。如果 vNIC 配置集启用了 **passthrough**，则同一配置集无法启用 **passthrough**、**QoS**、**网络过滤器**和**端口镜像**。

有关 SR-IOV、直接设备分配以及在 Red Hat Virtualization 中实现这些 [硬件注意事项的更多信息](#)，请参阅 [实施 SR-IOV 的硬件注意事项](#)。

流程

1. 单击 **Network** → **Networks**。
2. 点逻辑网络的名称。这会打开详情视图。

3. 单击 **vNIC Profiles** 选项卡，以列出该逻辑网络的所有 vNIC 配置集。
4. 单击 **New**。
5. 输入配置文件的名称和描述。
6. 选择 **Passthrough** 复选框。
7. (可选) 选择 **Migratable** 复选框，以使用这个配置集禁用 vNIC 的迁移。如果保留此复选框，请参阅[虚拟机管理指南](#)中的[带有 SR-IOV-Enabled vNIC 的虚拟机的其他先决条件](#)。
8. 如有必要，从自定义属性列表中选择自定义属性，它默认会显示 **Please select a key...**。使用 **+** 和 **-** 按钮添加或删除自定义属性。
9. 单击 **OK**。

vNIC 配置集现在具有 **passthrough** 功能。要使用此配置集将虚拟机直接连接到 NIC 或 PCI VF，请将逻辑网络附加到 NIC，并在使用 **passthrough vNIC** 配置集的所需虚拟机上创建一个新的 **PCI Passthrough vNIC**。有关这些步骤的更多信息，请参阅[虚拟机管理指南](#)中的[编辑主机网络接口和将逻辑网络分配到主机](#)，以及[添加一个新网络接口](#)。

2.4.2.5. 为使用故障转移的 SR-IOV 迁移启用 vNIC 配置集

故障转移允许选择在需要分离 VF 时作为虚拟机迁移期间的故障切换设备，从而保留虚拟机通信并最小化中断。



注意

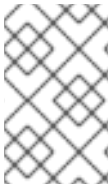
故障转移只是一个技术预览功能。技术预览功能不被红帽产品服务级别协议(SLA)支持，且可能无法完成。红帽不建议在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。如需更多信息，请参阅[红帽技术预览功能支持范围](#)。

前提条件

- 选择配置集的 **Passthrough** 和 **Migratable** 复选框。
- 故障转移网络附加到主机。
- 要使 vNIC 配置集充当故障切换可编辑，您必须首先删除所有故障切换引用。
- 作为故障转移的 vNIC 配置集是没有选择为 **Passthrough** 的配置集，或者没有连接到外部网络。

流程

1. 在管理门户中，进入 **Network** → **VNIC 配置集**，选择 vNIC 配置集，点 **Edit**，然后从下拉列表中选择 **Failover vNIC 配置集**。
2. 单击 **OK** 以保存配置文件设置。



注意

附加两个 vNIC 配置集，在 libvirt 中引用同一故障切换 vNIC 配置集将会失败。

2.4.2.6. 删除 vNIC 配置集

删除 vNIC 配置集，将其从虚拟环境中删除。

流程

1. 单击 **Network** → **Networks**。
2. 点逻辑网络的名称。这会打开详情视图。
3. 单击 **vNIC Profiles** 选项卡，以显示可用的 vNIC 配置集。

4. 选择一个或多个配置集并点 **Remove**。
5. 点击 **OK**。

2.4.2.7. 为 vNIC 配置集分配安全组



注意

只有将 `ovirt-provider-ovn` 添加为外部网络提供程序时，此功能才可用。安全组不能通过 Red Hat Virtualization Manager 创建。您必须通过 `ovirt-provider-ovn` 上的 OpenStack Networking 创建安全组。如需更多信息，请参阅 *Red Hat OpenStack Platform Users and Identity Management Guide* 中的 [Project Security Management](#)。

您可以将安全组分配给从 OpenStack Networking 实例导入的网络的 vNIC 配置集，以及使用 Open vSwitch 插件。安全组是严格强制规则的集合，允许您通过网络接口过滤入站和出站流量。以下流程概述了如何将安全组附加到 vNIC 配置集。



注意

安全组使用在 Open Virtual Network (OVN) External Network Provider 中注册的安全组 ID 标识。您可以使用 OpenStack Networking API 查找给定租户的安全组 ID，请参阅 *OpenStack API* 参考中的 [列出安全组](#)。

流程

1. 单击 **Network** → **Networks**。
2. 点逻辑网络的名称。这会打开详情视图。
3. 点 **vNIC Profiles** 选项卡。
4. 点 **New**，或者选择现有的 vNIC 配置集并点 **Edit**。
5. 从自定义属性下拉列表中，选择 **SecurityGroups**。使自定义属性下拉列表应用默认安全设置，允许所有出站流量和相互连接，但拒绝来自默认安全组外的所有入站流量。请注意，稍后删

除 **SecurityGroups** 属性不会影响应用的安全组。

6. 在文本字段中，输入要附加到 vNIC 配置集的安全组 ID。
7. 点击 **OK**。

您已将安全组附加到 vNIC 配置集。根据针对该安全组定义的规则，将过滤该配置集附加到的逻辑网络的所有流量。

2.4.2.8. vNIC 配置集的用户权限

配置用户权限以将用户分配到特定的 vNIC 配置集。将 **VnicProfileUser** 角色分配给用户，使其能够使用配置集。通过删除该配置集的权限来限制特定配置集的用户。

vNIC 配置集的用户权限

1. 单击 **Network** → **vNIC Profile**。
2. 点 vNIC 配置集的名称。这会打开详情视图。
3. 点 **Permissions** 选项卡显示配置集的当前用户权限。
4. 点 **Add** 或 **Remove** 更改 vNIC 配置集的用户权限。
5. 在 **Add Permissions to User** 窗口中，点 **My Groups** 以显示您的用户组。您可以使用这个选项为组中的其他用户授予权限。

您已为 vNIC 配置集配置了用户权限。

2.4.3. 外部提供商网络

2.4.3.1. 从外部提供程序导入网络

要使用 Open Virtual Network (OVN)的网络，请通过 Manager 注册该提供程序。如需更多信息，请参阅[添加外部网络提供程序](#)。然后，按照以下流程将该提供程序提供的网络导入到 Manager，以便虚拟机可以使用网络。

流程

1. 单击 **Network** → **Networks**。
2. 单击 **Import**。
3. 从 **Network Provider** 下拉列表选择一个外部供应商。该提供程序提供的网络会自动发现并列在 **Provider Networks** 列表中。
4. 使用复选框，选择要在 **Provider Networks** 列表中导入的网络，然后单击向下箭头，将这些网络移到 **Networks to Import** 列表中。
5. 您可以自定义您要导入的网络的名称。要自定义名称，请单击 **Name** 列中的网络名称，并更改文本。
6. 从 **Data Center** 下拉列表中，选择将导入网络的数据中心。
7. 可选：清除 **Allow All** 复选框，以防止该网络可供所有用户使用。
8. 单击 **Import**。

所选网络导入到目标数据中心，并可附加到虚拟机。如需更多信息，请参阅[虚拟机管理指南中的添加新网络接口](#)。

2.4.3.2. 使用外部提供程序网络的限制

以下限制适用于在 Red Hat Virtualization 环境中使用从外部提供程序导入的逻辑网络。

- 外部提供者提供的逻辑网络必须用作虚拟机网络，不能用作显示网络。
- 同一逻辑网络可以导入一次，但只能导入不同的数据中心。
- 您无法编辑 Manager 中外部提供者提供的逻辑网络。要编辑外部提供者提供的逻辑网络的详细信息，您必须直接从提供该逻辑网络的外部供应商编辑逻辑网络。
- 端口镜像不适用于连接到外部提供者提供的逻辑网络的虚拟网络接口卡。
- 如果虚拟机使用外部提供者提供的逻辑网络，那么当逻辑网络仍在被虚拟机使用时，无法从 Manager 中删除该提供者。
- 外部提供者提供的网络不是必需网络。因此，在主机选择期间，调度已导入此类逻辑网络的集群不会将这些逻辑网络考虑在内。此外，用户负责确保逻辑网络在已导入此类逻辑网络的集群中主机上可用。

2.4.3.3. 在外部提供程序逻辑网络上配置子网

如果该逻辑网络上定义了一个或多个子网，则外部提供者提供的逻辑网络只能为虚拟机分配 IP 地址。如果没有定义子网，则不会为虚拟机分配 IP 地址。如果有一个子网，虚拟机将从该子网分配一个 IP 地址，如果存在多个子网，则虚拟机将从任何可用子网中分配一个 IP 地址。托管逻辑网络的外部网络提供商提供的 DHCP 服务负责分配这些 IP 地址。

虽然 Red Hat Virtualization Manager 会自动发现导入的逻辑网络上的预定义子网，但您也可以从 Manager 内向逻辑网络添加或删除子网。

如果您将 Open Virtual Network (OVN) (ovirt-provider-ovn) 添加为外部网络提供程序，则路由器可以互相连接多个子网。要管理这些路由器，您可以使用 [OpenStack 网络 API v2.0](#)。但请注意，ovirt-provider-ovn 有一个限制：Source NAT (OpenStack API 中的 `enable_snat`) 没有实现。

2.4.3.4. 将子网添加到外部提供程序逻辑网络

在由外部提供者提供的逻辑网络上创建子网。

流程

1. 单击 **Network** → **Networks**。
2. 点逻辑网络的名称。这会打开详情视图。
3. 单击 **子网**选项卡。
4. 单击 **New**。
5. 输入新子网的 **Name** 和 **CIDR**。
6. 从 **IP Version** 下拉列表中，选择 **IPv4** 或 **IPv6**。
7. 单击 **OK**。



注意

对于 **IPv6**，**Red Hat Virtualization** 仅支持静态寻址。

2.4.3.5. 从外部提供程序逻辑网络中删除子网

从外部提供者提供的逻辑网络中删除子网。

流程

1. 单击 **Network** → **Networks**。
2. 点逻辑网络的名称。这会打开详情视图。
3. 单击 **子网**选项卡。

4. 选择子网，再单击删除。
5. 单击 OK。

2.4.3.6. 为逻辑网络和端口分配安全组



注意

只有将 Open Virtual Network (OVN) 添加为外部网络提供程序（作为 `ovirt-provider-ovn`）时，此功能才可用。安全组不能通过 Red Hat Virtualization Manager 创建。您必须通过 OpenStack Networking API v2.0 或 Ansible 创建安全组。

安全组是严格强制规则的集合，允许您通过网络过滤入站和出站流量。您还可以使用安全组在端口级别上过滤流量。

在 Red Hat Virtualization 4.2.7 中，安全组默认为禁用。

流程

1. 单击 **Compute** → **Clusters**。
2. 点集群名称。这会打开详情视图。
3. 单击 **逻辑网络** 选项卡。
4. 点 **Add Network** 并定义属性，确保从 **External Providers** 下拉列表中选择 `ovirt-provider-ovn`。如需更多信息，请参阅 [在数据中心或集群中创建新的逻辑网络](#)。
5. 从 **Security Group** 下拉列表中，选择 **Enabled**。详情请查看 [逻辑网络常规设置说明](#)。
6. 单击 OK。

7. 使用 [OpenStack Networking API v2.0](#) 或 [Ansible](#) 创建安全组。
8. 使用 [OpenStack Networking API v2.0](#) 或 [Ansible](#) 创建安全组规则。
9. 使用 [OpenStack Networking API v2.0](#) 或 [Ansible](#) 定义的安全组更新端口。
10. 可选。定义在端口级别是否启用了安全功能。目前，这只能使用 [OpenStack 网络 API](#)。如果没有设置 `port_security_enabled` 属性，它将默认为它所属的网络指定的值。

2.4.4. 主机和网络

2.4.4.1. Network Manager Stateful Configuration (nmstate)

Red Hat Virtualization 版本 4.4 使用 *Network Manager Stateful Configuration (nmstate)* 为基于 RHEL 8 的 RHV 主机配置网络。RHV 版本 4.3 及更早版本使用接口配置(`ifcfg`)网络脚本来管理主机网络。

要使用 `nmstate`，请升级 Red Hat Virtualization Manager 和主机，如 [RHV Upgrade Guide](#) 所述。

作为管理员，您不需要安装或配置 `nmstate`。它默认启用，并在后台运行。



重要

始终使用 RHV Manager 修改集群中主机的网络配置。否则，您可能创建不受支持的配置。

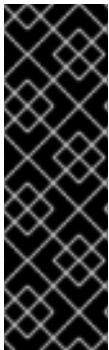
对 `nmstate` 的更改几乎是透明的。它仅通过以下方法更改配置主机网络：

- 将主机添加到集群中后，请始终使用 RHV Manager 修改主机网络。
- 在不使用 Manager 的情况下修改主机网络可以创建不受支持的配置。
-

要修复不支持的配置，您可以使用 **Manager** 来同步主机网络，将其替换为支持的一个配置。详情请参阅 [同步主机网络](#)。

- 修改 **Manager** 之外的主机网络的唯一情形是在主机上配置静态路由。如需了解更多详细信息，请参阅[在主机中添加静态路由](#)。

对 **nmstate** 的更改改进了 **RHV Manager** 在将主机添加到管理器前如何应用您在 **Cockpit** 和 **Anaconda** 中进行的配置更改。在这个版本中，[如果 NM 管理接口，则 BZ#1680970 静态 IPv6 地址会在主机上丢失](#)。



重要

如果您使用 **dnf** 或 **yum** 手动更新 **nmstate** 软件包，请在主机上重启 **vdsmd** 和 **supervdsmd**。例如：

```
# dnf update nmstate
# systemctl restart vdsmd supervdsmd
```



重要

如果您使用 **dnf** 或 **yum** 手动更新 **Network Manager** 软件包，请在主机上重启 **NetworkManager**。例如：

```
# dnf update NetworkManager
# systemctl restart NetworkManager
```

2.4.4.2. 刷新主机功能

当将网络接口卡添加到主机时，必须刷新主机的功能来显示 **Manager** 中的网络接口卡。

流程

1. 单击 **Compute** → **Hosts** 并选择一个主机。
2. 单击 **Management** → **Refresh Capabilities**。

所选主机的 **Network Interfaces** 选项卡中的网络接口卡列表会被更新。现在，所有新的网络接口卡都可以在 **Manager** 中使用。

2.4.4.3. 编辑主机网络接口并将逻辑网络分配给主机

您可以更改物理主机网络接口的设置，将管理网络从一个物理主机网络接口移到另一个，并将逻辑网络分配到物理主机网络接口。也支持 `bridge` 和 `ethtool` 自定义属性。



警告

更改 Red Hat Virtualization 中主机的 IP 地址的唯一方法是移除该主机，然后再次添加它。

要更改主机的 VLAN 设置，请参阅 [编辑 VLAN Settings](#)。



重要

您无法将外部提供者提供的逻辑网络分配给物理主机网络接口；此类网络会动态分配到主机，因为虚拟机需要它们。



注意

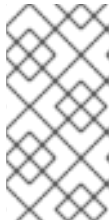
如果切换已配置为提供链路层发现协议(LLDP)信息，您可以将光标悬停于物理网络接口上，以查看交换机端口的当前配置。这有助于防止配置不正确。在分配逻辑网络前检查以下信息：

- **Port Description (TLV type 4) 和 System Name (TLV type 5) 有助于检测主机的接口是否已修补至哪些端口和切换。**
- **端口 VLAN ID 显示在未标记以太网帧的交换机端口上配置的原生 VLAN ID。交换机端口上配置的所有 VLAN 都显示为 VLAN Name 和 VLAN ID 组合。**

流程

1. 单击 **Compute → Hosts**。

2. 单击主机的名称。这会打开详情视图。
3. 单击 **Network Interfaces** 选项卡。
4. 单击 **Setup Host Networks**。
5. (可选) 将光标悬停在主机网络接口上，以查看交换机提供的配置信息。
6. 通过选择逻辑网络并将其拖到物理主机网络接口旁边的已分配逻辑网络区域，将逻辑网络附加到物理主机网络接口，从而将其附加到物理主机网络接口。



注意

如果 NIC 连接到多个逻辑网络，则只有其中一个网络可以是非 VLAN。所有其他逻辑网络都必须是唯一的 VLAN。

7. 配置逻辑网络：
 - a. 将光标悬停在分配的逻辑网络上，然后点铅笔图标。此时将打开 **Edit Management Network** 窗口。
 - b. 在 IPv4 标签页中，选择一个 **Boot Protocol** (None, DHCP, 或 Static)。如果您选择了 **Static**，请输入 **IP**、**Netmask/ Routing Prefix** 和 **Gateway**。



注意

对于 IPv6，只支持静态 IPv6 地址。要配置逻辑网络，请选择 IPv6 选项卡并添加以下条目：

- 将 **Boot Protocol** 设置为 **Static**。
- 对于 **ForRouting Prefix**，使用正斜杠和十进制输入前缀长度。
例如：`/48`
- **IP**：主机网络接口的完整 IPv6 地址。例如：`2001:db8::1:0:0:6`
- **网关**：源路由器的 IPv6 地址。例如：`2001:db8::1:0:0:1`



注意

如果更改主机的管理网络 IP 地址，则必须 **重新安装主机**，以便能配置新的 IP 地址。

每个逻辑网络都可以有一个独立的网关，由管理网络网关定义。这样可以保证使用逻辑网络上的流量将使用逻辑网络的网关进行转发，而不是管理网络使用的默认网关。



重要

将群集中的所有主机都设置为将相同的 IP 堆栈用于其管理网络；仅 IPv4 或 IPv6。不支持双堆栈。

c.

使用 **QoS** 选项卡覆盖默认主机网络服务质量。选择 **Override QoS**，然后在以下字段中输入所需的值：

- **加权共享**：指定应分配特定网络的逻辑链接的容量量，相对于附加到同一逻辑链接的其他网络。确切共享取决于该链接上所有网络共享的总和。默认情况下，这是 1 到 100 范围内的数字。

- 速率限制 [Mbps] : 网络要使用的最大带宽。
 - 提交率 [Mbps] : 网络所需的最小带宽。请求的提交率不能保证, 并根据网络基础架构和同一逻辑链路上其他网络请求的提交率不同。
- d. 要配置网络桥接, 请点击 **Custom Properties** 选项卡, 然后从下拉列表中选择 **bridge_opts**。输入有效的键和值, 语法如下: *key=value*。使用空格字符分隔多个条目。以下键有效, 且值为示例提供的值。有关这些参数的更多信息, 请参阅 [bridge_opts 参数说明](#)。

```
forward_delay=1500
group_addr=1:80:c2:0:0:0
group_fwd_mask=0x0
hash_max=512
hello_time=200
max_age=2000
multicast_last_member_count=2
multicast_last_member_interval=100
multicast_membership_interval=26000
multicast_querier=0
multicast_querier_interval=25500
multicast_query_interval=13000
multicast_query_response_interval=1000
multicast_query_use_ifaddr=0
multicast_router=1
multicast_snooping=1
multicast_startup_query_count=2
multicast_startup_query_interval=3125
```

- e. 要配置以太网属性, 请单击 **Custom Properties** 选项卡, 然后从下拉列表中选择 **ethtool_opts**。使用 **ethtool** 的命令行参数格式输入有效值。例如:

```
--coalesce em1 rx-usecs 14 sample-interval 3 --offload em2 rx on lro on tso off --
change em1 speed 1000 duplex half
```

此字段可以接受通配符。例如, 要将相同的选项应用到所有网络的接口, 请使用:

```
--coalesce * rx-usecs 14 sample-interval 3
```

ethtool_opts 选项默认不可用, 您需要使用 **engine** 配置工具来添加它。如需更多信息, 请参阅[如何设置 Manager 以使用 Ethtool](#)。有关 **ethtool** 属性的更多信息, 请在命令行中输入 `man ethtool` 来查看 `man page`。

f.

要通过以太网配置光纤通道 (FCoE)，请点 **Custom Properties** 选项卡，从下拉菜单中选择 **fcoe**。输入有效的键和值，语法如下：**key=value**。至少 **enable=yes**。您还可以添加 **dcb=[yes|no]** 和 **'auto_vlan=[yes|no]**。使用空格字符分隔多个条目。**fcoe** 选项默认不可用，您需要使用 **engine** 配置工具来添加它。如需更多信息，请参阅[如何设置 Manager 以使用 FCoE](#)。



注意

建议使用单独的专用逻辑网络与 FCoE 一起使用。

g.

要将主机从管理网络 (**ovirtmgmt**) 使用的默认网络改为非管理网络，请配置非管理网络的默认路由。如需更多信息，请参阅[配置 默认路由](#)。

h.

如果您的逻辑网络定义没有与主机上的网络配置同步，请选择 **Sync network** 复选框。有关未同步主机以及如何同步它们的更多信息，请参阅[同步主机网络](#)。

8.

选择 **Verify connectivity between Host and Engine** 复选框，以选中网络连接。此操作仅在主机处于维护模式时才有效。

9.

点击 **OK**。



注意

如果没有显示主机的所有网络接口卡，请单击 **Management** → **Refresh Capabilities** 以更新可用于该主机的网络接口卡列表。

故障排除

在某些情况下，使用 **Setup Host Networks** 窗口或 **setupNetwork** 命令对主机网络配置进行多个并发更改会失败，并显示 **Operation failed: [Cannot setup Networks]**。主机上进行另一个设置网络或主机刷新过程。请稍后尝试。] 错误。此错误表示主机上尚未配置一些更改。这是因为为了保持配置状态的完整性，一次只能处理单个设置网络命令。其他并发配置命令排队，使其默认超时为 20 秒。为了帮助防止出现上述故障，请使用 **engine-config** 命令将 **SetupNetworksWaitTimeoutSeconds** 的超时时间增加到 20 秒。例如：

```
# engine-config --set SetupNetworksWaitTimeoutSeconds=40
```

其他资源

- [engine-config 命令的语法](#)
- [setupnetworks POST](#)

2.4.4.4. 同步主机网络

当主机上的接口的定义与 Manager 存储的定义不同，管理器将把网络接口定义为非同步。

内存不足网络出现在主机网络接口选项卡中



的 Out-of-sync 图标，并在 Setup Host Networks 窗口中使用此图标



。

当主机的网络不同步时，您只能在 Setup Host Networks 窗口中对未同步的网络执行的活动将从网络接口中分离逻辑网络或同步网络。

了解主机如何变为同步

如果出现以下情况，主机将变得不同步：

- 您在主机上进行配置更改，而不是使用 Edit Logical Networks 窗口，例如：
 - 更改物理主机上的 VLAN 标识符。
 - 更改物理主机上的自定义 MTU。
- 您可以将主机移动到具有相同网络名称的不同数据中心，但使用不同的值/参数。
- 您可以通过从主机中手动删除桥接来更改网络 VM Network 属性。



重要

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

防止主机无法同步

遵循这些最佳实践将阻止您的主机变得未同步：

1. 使用管理门户进行更改，而不是在主机上进行本地更改。
2. 根据编辑 VLAN 设置中的说明 [编辑 VLAN 设置](#)。

同步主机

同步主机网络接口定义涉及使用 Manager 中的定义并将其应用到主机。如果这些不是您需要的定义，则在同步主机从管理门户中更新其定义。您可以在三个级别同步主机的网络：

- 每个逻辑网络
- 每个主机
- per cluster

在逻辑网络级别同步主机网络

1. 单击 **Compute** → **Hosts**。
2. 单击主机的名称。这会打开详情视图。
3. 单击 **Network Interfaces** 选项卡。

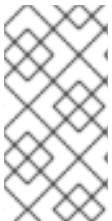
4. 单击 **Setup Host Networks**。
5. 将光标悬停在未同步网络上，然后点铅笔图标。此时将打开 **Edit Network** 窗口。
6. 选中 **Sync network** 复选框。
7. 单击确定以 保存网络更改。
8. 单击 **OK**，以关闭 **Setup Host Networks** 窗口。

在主机级别上同步主机的网络

- 单击主机的 **Network Interfaces** 选项卡中的 **Sync All Networks** 按钮，以同步所有主机的未同步网络接口。

在集群级别同步主机的网络

- 点集群逻辑网络选项卡中的 **Sync All Networks** 按钮，以同步整个集群的所有未同步逻辑网络定义。



注意

您还可以通过 **REST API** 同步主机的网络。请参阅 *REST API 指南* 中的 [syncallnetworks](#)。

2.4.4.5. 编辑主机的 VLAN 设置

要更改主机的 **VLAN** 设置，必须从 **Manager** 中删除主机、重新配置并重新添加到管理器。

要保持网络同步，请执行以下操作：

1. 将主机置于维护模式。

2. 从主机中手动删除管理网络。这将使主机能够通过新的 VLAN 访问。
3. 将主机添加到集群。在主机间可以安全地迁移没有直接连接到管理网络的虚拟机。

当管理网络的 VLAN ID 被改变时，会出现以下警告信息：

Changing certain properties (e.g. VLAN, MTU) of the management network could lead to loss of connectivity to hosts in the data center, if its underlying network infrastructure isn't configured to accommodate the changes. Are you sure you want to proceed?

继续会导致数据中心中的所有主机丢失与 Manager 的连接，并导致主机迁移到新的管理网络失败。管理网络将报告为 "out-of-sync"。



重要

如果更改管理网络的 VLAN ID，则必须 [重新安装主机](#) 以应用新的 VLAN ID。

2.4.4.6. 使用逻辑网络在单一网络接口中添加多个 VLAN

多个 VLAN 可以添加到单一网络接口中，以分隔一个主机上的流量。



重要

您必须已创建了多个逻辑网络，它们都在 **New Logical Network** 或 **Edit Logical Network** 窗口中选中 **Enable VLAN tagging** 复选框。

流程

1. 单击 **Compute** → **Hosts**。
2. 单击主机的名称。这会打开详情视图。
3. 单击 **Network Interfaces** 选项卡。

4. 单击 **Setup Host Networks**。
5. 将 **VLAN** 标记的逻辑网络拖放到物理网络接口旁边的已分配逻辑网络区域。物理网络接口可能会因为 **VLAN** 标记而分配多个逻辑网络。
6. 编辑逻辑网络：
 - a. 将光标悬停在分配的逻辑网络上，然后点铅笔图标。
 - b. 如果您的逻辑网络定义没有与主机上的网络配置同步，请选择 **Sync network** 复选框。
 - c. 选择引导协议：
 - **None**
 - **DHCP**
 - **Static**
 - d. 提供 **IP** 和子网掩码。
 - e. 单击 **OK**。
7. 选择 **Verify connectivity between Host and Engine** 复选框来运行网络检查。这只有在主机处于维护模式时才能正常工作。
8. 单击 **OK**。

通过编辑集群中的每个主机上的 **NIC**，将逻辑网络添加到集群中的每个主机。完成后，网络将变为可操作。

此过程可以重复多次，在每次主机上选择并编辑相同的网络接口，以将具有不同 VLAN 标签的逻辑网络添加到单个网络接口。

2.4.4.6.1. 复制主机网络

要节省时间，您可以将源主机的网络配置复制到同一集群中的目标主机。

复制网络配置包括：

- 附加到主机的逻辑网络，但 `ovirtmgmt` 管理网络除外
- 附加到接口的绑定

限制

- 不要复制包含静态 IP 地址的网络配置。这样做会将目标主机中的引导协议设置为 `none`。
- 将配置复制到与源主机相同的接口名称，但不同的物理网络连接会产生错误的配置。
- 目标主机必须与源主机相等或大于多个接口。否则，操作会失败。
- 不支持复制 QoS、DNS 和 `custom_properties`。
- 网络接口标签不会被复制。



警告

复制主机网络将替换目标主机上的 ALL 网络设置，除了将其附加到 `ovirtmgmt` 管理网络外。

前提条件

- 目标主机上的 **NIC** 数量必须相等或大于源主机上的 **NIC** 数量。否则，操作会失败。
- 主机必须位于同一集群中。

流程

1. 在管理门户中，点 **Compute** → **Hosts**。
2. 选择您要复制的配置的源主机。
3. 单击 **Copy Host Networks**。此时将打开 **Copy Host Networks** 窗口。
4. 使用 **Target Host** 选择应接收配置的主机。列表仅显示同一集群中的主机。
5. 单击 **Copy Host Networks**。
6. 验证目标主机的网络设置

提示

- 选择多个主机将禁用 **Copy Host Networks** 按钮和上下文菜单。
- 您可以右键单击主机并从上下文菜单中选择 **Copy Host Networks** 按钮，而不是使用 **Copy Host Networks** 按钮。
- "复制主机网络"按钮也可在任何主机的详细信息视图中使用。

2.4.4.7. 为主机网络分配额外的 IPv4 地址

在最初设置时，仅使用一个 IP 地址创建主机网络，如 **ovirtmgmt** 管理网络。这意味着，如果 **NIC** 的配置文件配置了多个 IP 地址，则只有第一个列出的 IP 地址分配给主机网络。如果连接到存储或者使用相

同的 NIC 单独专用子网上的服务器，则可能需要额外的 IP 地址。

`vdsm-hook-extra-ipv4-addr`s hook 允许您为主机网络配置额外的 IPv4 地址。有关 hook 的更多信息，请参阅 [VDSM](#) 和 [Hook](#)。

在以下步骤中，必须在要为其配置额外 IP 地址的每个主机上执行特定于主机的任务。

流程

1. 在您要为其配置额外 IPv4 地址的主机上，安装 VDSM hook 软件包。软件包需要在 Red Hat Enterprise Linux 主机和 Red Hat Virtualization 主机上手动安装。

```
# dnf install vsdm-hook-extra-ipv4-addr
```

2. 在 Manager 中运行以下命令添加密钥：

```
# engine-config -s 'UserDefinedNetworkCustomProperties=ipv4_addr=.'
```

3. 重启 `ovirt-engine` 服务：

```
# systemctl restart ovirt-engine.service
```

4. 在管理门户中，点 **Compute** → **Hosts**。

5. 单击主机的名称。这会打开详情视图。

6. 单击 **Network Interfaces** 选项卡，再单击 **Setup Host Networks**。

7. 将光标悬停在分配的逻辑网络上，然后点铅笔图标，以编辑主机网络接口。

8. 从 **Custom Properties** 下拉列表中选择 `ipv4_addr` 并添加额外 IP 地址和前缀（如 5.5.5/24）。必须用逗号分开多个 IP 地址。

9. 单击 **OK** 以关闭 **Edit Network** 窗口。
10. 单击 **OK**，以关闭 **Setup Host Networks** 窗口。

额外的 IP 地址不会在 Manager 中显示，但您可以在主机上运行 `ip addr show` 命令，以确认它们已被添加。

2.4.4.8. 在主机网络接口中添加网络标签

通过使用网络标签，您可以大大简化与分配逻辑网络关联的管理工作负载，以托管网络接口。在角色网络中设置标签（例如，迁移网络或显示网络）会导致在所有主机上大规模地部署该网络。这种大规模网络通过利用 DHCP 来实现。这种批量部署的方法是通过在静态地址中键入的方法来选择，因为很多静态 IP 地址中键入任务无法可扩展。

在主机网络接口中添加标签的方法有两种：

- 在管理门户中手动进行
- 自动通过 LLDP Labeler 服务

流程

1. 单击 **Compute** → **Hosts**。
2. 单击主机的名称。这会打开详情视图。
3. 单击 **Network Interfaces** 选项卡。
4. 单击 **Setup Host Networks**。
5. 点 **Labels**，右键单击 **[New Label]**。选择要标记的物理网络接口。

6. 在 Label 文本字段中输入网络标签的名称。
7. 点击 OK。

流程

您可以使用 LLDP Labeler 服务，自动化在集群列表中分配标签到主机网络接口的过程。

2.4.4.8.1. 配置 LLDP Labeler

默认情况下，LLDP Labeler 作为每小时服务运行。如果您进行硬件更改（如 NIC、交换机或电缆）或更改交换机配置，这个选项很有用。

前提条件

- 接口必须连接到 Juniper 交换机。
- 必须将 Juniper 开关配置为使用 LLDP 来提供 端口 VLAN。

流程

1. 在 `/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf` 中配置用户名和密码：
 - `username` - Manager 管理员的用户名。默认值为 `admin@internal`。
 - `Password` - Manager 管理员密码。默认值为 `123456`。
2. 通过更新 `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf` 中的下列值来配置 LLDP Labeler 服务：
 - `Clusters` - 应该运行该服务的以逗号分隔的集群列表。支持通配符。例如，`Cluster*` 定义在所有以词 `Cluster` 开始的集群中运行 LLDP Labeler。要在数据中心的所有集群中运行该服务，请输入 `*`。默认值为 `Def*`。
 -

api_url - Manager API 的完整 URL。默认值为 `https://Manager_FQDN/ovirt-engine/api`

- **ca_file** - 自定义 CA 证书文件的路径。如果不使用自定义证书，请保留这个值为空。默认值为空。
- **auto_bonding** - 启用 LLDP Labeler 的绑定功能。默认值是 `true`。
- **auto_labeling** - 启用 LLDP Labeler's 标签功能。默认值是 `true`。

3.

另外，您可以通过更改 `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer` 中的 `OnUnitActiveSec` 的值，将服务配置为以不同的间隔运行。默认值为 `1h`。

4.

输入以下命令将服务配置为默认启动和引导时：

```
# systemctl enable --now ovirt-lldp-labeler
```

要手动调用服务，请输入以下命令：

```
# /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
```

您已在主机网络接口中添加网络标签。新创建的具有相同标签的逻辑网络将自动分配给具有该标签的所有主机网络接口。从逻辑网络中删除标签会自动从所有带有该标签的主机网络接口中删除该逻辑网络。

2.4.4.9. 更改主机的 FQDN

使用以下步骤更改主机的完全限定域名。

流程

1.

将主机置于维护模式，以便虚拟机实时迁移到其他主机。如需更多信息，请参阅 [将主机移动到维护模式](#)。或者，手动关闭或将所有虚拟机迁移到另一主机。如需更多信息，请参阅 [虚拟机管理指南中的手动迁移虚拟机](#)。

2. 单击 **Remove**，再单击 **OK** 以将主机从管理门户中删除。
3. 使用 `hostnamectl` 工具更新主机名。如需了解更多选项，请参阅 *Red Hat Enterprise Linux 7 网络指南* 中的 [配置主机名](#)。

```
# hostnamectl set-hostname NEW_FQDN
```

4. 重启主机。
5. 使用 **Manager** 重新注册主机。如需更多信息，请参阅在 **Manager** 中添加标准主机。

2.4.4.9.1. IPv6 网络支持

Red Hat Virtualization 在大多数环境中支持静态 IPv6 网络。



注意

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。

IPv6 的限制

- 仅支持静态 IPv6 地址。不支持使用 DHCP 或无状态地址自动配置动态 IPv6 地址。
- 不支持 IPv4 和 IPv6 的双栈寻址。
- OVN 网络只能与 IPv4 或 IPv6 一起使用。
- 不支持将集群从 IPv4 切换到 IPv6。
- 每个主机只能为 IPv6 设置单个网关。
-

如果两个网络共享一个网关（在同一子网中），您可以将默认路由角色从管理网络 (ovirtmgmt) 移到另一个逻辑网络。主机和管理器应该具有相同的 IPv6 网关。如果主机和管理器不在同一子网中，则管理器将断开与主机的连接，因为删除了 IPv6 网关。

- 不支持使用带有 IPv6addressed gluster 服务器的 glusterfs 存储域。

2.4.4.9.2. 设置和配置 SR-IOV

本主题总结了设置和配置 SR-IOV 的步骤，以及详细论述每个步骤的主题。

前提条件

根据 [实施 SR-IOV 的硬件注意事项](#) 设置硬件注意事项

流程

要设置和配置 SR-IOV，请完成以下任务。

1. [为 PCI 直通配置主机。](#)
2. [编辑 NIC 上的虚拟功能配置。](#)
3. [在 vNIC 配置文件中启用透传。](#)
4. [在迁移过程中，使用 SR-IOV 启用 vNIC 配置虚拟机到 Red Hat User Network Outage。](#)

备注

- 'passthrough' vNIC 的数量取决于主机上可用的虚拟功能(VF)的数量。例如，要运行具有三个 SR-IOV 卡(vNIC)的虚拟机，主机必须启用三个或更多 VF。
- 支持热插拔和拔下。
- 支持实时迁移。

- 要迁移虚拟机，目标主机还必须有足够的可用 VF 来接收虚拟机。在迁移过程中，虚拟机在源主机上释放了很多 VF，并在目标主机上占用相同的 VF 数量。
- 在主机上，您将看到一个设备、链接或是否像任何其他接口一样。当设备附加到虚拟机时，该设备会消失，并在它被释放后重新显示。
- 避免将主机设备直接附加到虚拟机以获取 SR-IOV 功能。
- 要将 VF 用作多个 VLAN 的中继端口并配置客户机内的 VLAN，请参阅[无法在虚拟机中的 SR-IOV VF 接口上配置 VLAN](#)。

以下是接口的 libvirt XML 示例：

```

----
<interface type='hostdev'>
  <mac address='00:1a:yy:xx:vv:xx'/>
  <driver name='vfio'/>
  <source>
    <address type='pci' domain='0x0000' bus='0x05' slot='0x10' function='0x0'/>
  </source>
  <alias name='ua-18400536-5688-4477-8471-be720e9efc68'/>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
</interface>
----

```

故障排除

以下示例演示了如何获取有关附加到接口的 VF 的诊断信息。

```
# ip -s link show dev enp5s0f0
```

```

1: enp5s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc mq state UP mode
DEFAULT qlen 1000
  link/ether 86:e2:ba:c2:50:f0 brd ff:ff:ff:ff:ff:ff
  RX: bytes  packets  errors  dropped  overrun  mcast
30931671 218401 0      0      0      19165434
  TX: bytes  packets  errors  dropped  carrier  collsns
997136   13661  0      0      0      0
  vf 0 MAC 02:00:00:00:00:01, spoof checking on, link-state auto, trust off, query_rss off
  vf 1 MAC 00:1a:4b:16:01:5e, spoof checking on, link-state auto, trust off, query_rss off
  vf 2 MAC 02:00:00:00:00:01, spoof checking on, link-state auto, trust off, query_rss off

```

2.4.4.9.2.1. 其它资源

- [如何为 RHV 虚拟机配置 SR-IOV 透传？](#)
- [如何在 RHV 中通过 SR-IOV VF（虚拟功能）配置绑定](#)
- [如何启用主机设备透传和 SR-IOV，以允许为 RHV 中的虚拟机分配专用虚拟 NIC](#)

2.4.5. 网络绑定

2.4.5.1. 绑定方法

网络绑定将多个 NIC 组合到一个绑定设备中，具有以下优点：

- 绑定 NIC 的传输速度大于单个 NIC 的传输速度。
- 网络绑定提供容错功能，因为绑定设备不会失败，除非其所有 NIC 都失败。

使用相同 make 和 模型的 NIC 可确保它们支持相同的绑定选项和模式。



重要

Red Hat Virtualization 的默认绑定模式 (Mode 4) 动态链路聚合 需要支持 802.3ad 的交换机。

绑定的逻辑网络必须兼容。绑定只支持 1 个非 VLAN 逻辑网络。其余的逻辑网络必须具有唯一的 VLAN ID。

必须为交换机端口启用绑定。有关具体说明，请参考您的厂商提供的手册。

您可以使用以下方法之一创建网络绑定设备：

- [在管理门户中 手动特定主机](#)

- 自动使用 **LLDP Labeler** 作为群集或数据中心中所有主机的未绑定 NIC

如果您的环境使用 iSCSI 存储并且您要实现冗余性，请按照 [配置 iSCSI 多路径](#) 的说明进行操作。

2.4.5.2. 在管理门户中创建绑定设备

您可以在管理门户的特定主机上创建绑定设备。绑定设备可以同时执行 VLAN 标记和未标记的流量。

流程

1. 单击 **Compute** → **Hosts**。
2. 单击主机的名称。这会打开详情视图。
3. 点 **Network Interfaces** 选项卡，以列出附加到主机的物理网络接口。
4. 单击 **Setup Host Networks**。
5. 检查交换机配置。如果切换已配置为提供 Link Layer Discovery Protocol (LLDP)信息，请将光标悬停于物理 NIC 上，以查看交换机端口的聚合配置。
6. 将 NIC 拖放到另一个 NIC 或一个绑定中。



注意

两个 NIC 形成新绑定。NIC 和一个绑定将 NIC 添加到现有绑定中。

如果逻辑网络**不兼容**，则绑定操作会被阻断。

7. 从下拉菜单中选择 **Bond Name** 和 **Bonding Mode**。有关详细信息，请参阅 [绑定模式](#)。

如果选择 **Custom bonding** 模式，您可以在文本字段中输入绑定选项，如下例所示：

- 如果您的环境没有通过 **ethtool** 报告链接状态，则可以通过输入 **mode=1 arp_interval=1 arp_ip_target=192.168.0.2** 来设置 **ARP** 监控。
- 您可以通过输入 **mode=1 primary=eth0**，将具有更高吞吐量的 **NIC** 指定为主接口。

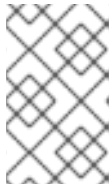
有关绑定选项及其描述的完整列表，请参阅 [Kernel.org](#) 上的 [Linux 以太网绑定驱动程序 HOWTO](#)。

8.

点击 **OK**。

9.

将逻辑网络附加到新绑定并进行配置。具体步骤请参阅[编辑主机网络接口和将逻辑网络分配到主机](#)。



注意

您不能直接将逻辑网络附加到绑定中的独立 **NIC**。

10.

另外，如果主机处于维护模式，您可以选择 **Verify connectivity between Host and Engine**。

11.

点击 **OK**。

2.4.5.3. 使用 LLDP Labeler 服务创建绑定设备

LLDP Labeler 服务可让您为一个或多个集群或整个数据中心中的所有主机自动使用未绑定 **NIC** 创建绑定设备。绑定模式为 [\(Mode 4\) Dynamic Link Aggregation \(802.3ad\)](#)。

带有 [不兼容逻辑网络的 NIC](#) 无法绑定。

2.4.5.3.1. 配置 LLDP Labeler

默认情况下，LLDP Labeler 作为每小时服务运行。如果您进行硬件更改（如 NIC、交换机或电缆）或更改交换机配置，这个选项很有用。

前提条件

- 接口必须连接到 Juniper 交换机。
- 必须使用 LLDP 为链路聚合控制协议(LACP)配置 Juniper 交换机。

流程

1.

在 `/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf` 中配置用户名和密码：

- **username** - Manager 管理员的用户名。默认值为 `admin@internal`。
- **Password** - Manager 管理员密码。默认值为 `123456`。

2.

通过更新 `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf` 中的下列值来配置 LLDP Labeler 服务：

- **Clusters** - 应该运行该服务的以逗号分隔的集群列表。支持通配符。例如，`Cluster*` 定义在所有以词 `Cluster` 开始的集群中运行 LLDP Labeler。要在数据中心的所有集群中运行该服务，请输入 `*`。默认值为 `Def*`。
- **api_url** - Manager API 的完整 URL。默认值为 `https://Manager_FQDN/ovirt-engine/api`
- **ca_file** - 自定义 CA 证书文件的路径。如果不使用自定义证书，请保留这个值为空。默认值为空。
- **auto_bonding** - 启用 LLDP Labeler 的绑定功能。默认值是 `true`。
- **auto_labeling** - 启用 LLDP Labeler's 标签功能。默认值是 `true`。

3.

另外，您可以通过更改 `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer` 中的 `OnUnitActiveSec` 的值，将服务配置为以不同的间隔运行。默认值为 1h。

4.

输入以下命令将服务配置为默认启动和引导时：

```
# systemctl enable --now ovirt-lldp-labeler
```

要手动调用服务，请输入以下命令：

```
# /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
```

1.

将逻辑网络附加到新绑定并进行配置。[具体步骤请参阅编辑主机网络接口和将逻辑网络分配到主机。](#)



注意

您不能直接将逻辑网络附加到绑定中的独立 NIC。

2.4.5.4. 绑定模式

数据包分布算法由绑定模式决定。（请参阅 [Linux 以太网绑定驱动程序 HOWTO](#)）。Red Hat Virtualization 的默认绑定模式是 (Mode 4) Dynamic Link Aggregation (802.3ad)。

Red Hat Virtualization 支持以下绑定模式，因为它们可用于虚拟机（桥接）网络：

(模式 1) Active-Backup

一个 NIC 处于活跃状态。如果活跃 NIC 失败，则备份 NIC 之一会将其替换为绑定中唯一的活跃 NIC。此绑定的 MAC 地址仅在网络适配器端口中可见。这可防止在绑定 MAC 地址更改时发生 MAC 地址混淆，这反映了新活跃 NIC 的 MAC 地址。

(模式 2) 负载均衡(balance-xor)

通过对源 MAC 地址和目的地 MAC 地址执行 XOR 操作来选择传输数据包的 NIC，乘以 NIC 总数的 modulo。此算法确保为每个目标 MAC 地址选择相同的 NIC。

(模式 3) 广播

数据包传输到所有 NIC。

(模式 4) 动态链路聚合(802.3ad) (默认)

NIC 聚合成共享相同速度和双工设置的组中。使用活跃聚合组中的所有 NIC。

注意

(模式 4) 动态链路聚合(802.3ad) 需要支持 802.3ad 的交换机。

绑定 NIC 必须具有相同的聚合器 ID。否则，管理器在 **Network Interfaces** 选项卡中显示绑定的警告感叹号图标，绑定的 `ad_partner_mac` 值报告为 `00:00:00:00:00:00`。您可以输入以下命令来检查聚合器 ID：

```
# cat /proc/net/bonding/bond0
```

[与虚拟客户机或容器连接到的网桥一起使用时，请查看哪些绑定模式工作？](#)

以下绑定模式与虚拟机逻辑网络不兼容，因此只能使用非VM 逻辑网络附加到绑定中：

(模式 0) Round-Robin

NIC 按顺序传输数据包。在以绑定中的第一个可用 NIC 开头的循环中传输数据包，并以绑定中最后一个可用 NIC 结束。后续循环从第一个可用 NIC 开始。

(模式 5) Balance-TLB, 也称为 Transmit Load-Balance

传出流量会根据绑定中的所有 NIC 的负载进行分发。入站流量由活跃 NIC 接收。如果 NIC 接收传入流量失败，则会分配另一个 NIC。

(模式 6) balance-ALB, 也称为 Adaptive Load-Balance

(模式 5) Balance-TLB 与 IPv4 流量接收负载均衡相结合。ARP 协商用于平衡接收负载。

2.5. 主机

2.5.1. 主机简介

主机也称为虚拟机监控程序，是运行虚拟机的物理服务器。使用称为基于内核的虚拟机(KVM)的可加载 Linux 内核模块提供完全虚拟化。

KVM 可以同时托管运行 Windows 或 Linux 操作系统的多个虚拟机。虚拟机作为独立 Linux 进程和线程在主机上运行，并由 Red Hat Virtualization Manager 远程管理。Red Hat Virtualization 环境连接有一个或多个主机。

Red Hat Virtualization 支持两种方法安装主机。您可以使用 Red Hat Virtualization Host (RHVH)安装介质，或者在标准 Red Hat Enterprise Linux 安装中安装虚拟机监控程序软件包。



注意

您可以通过选择主机名来识别 Red Hat Virtualization Manager 中的独立主机类型。这会打开详情视图。然后，查看 软件 下的 OS 描述。

主机使用 tuned 配置集，提供虚拟化优化。有关 tuned 的更多信息，请参阅 *Red Hat Enterprise Linux 监控和管理系统状态和性能* 中的 [Tuned 配置集](#)。

Red Hat Virtualization Host 启用了安全功能。Security Enhanced Linux (SELinux)和防火墙是完全配置且默认打开的。选定主机上的 SELinux 状态会在详情视图中常规标签页的 SELinux 模式下报告。当管理器添加到环境中时，该管理器可以在 Red Hat Enterprise Linux 主机上打开所需的端口。

主机是具有 Intel VT 或 AMD-V 扩展运行 Red Hat Enterprise Linux 7 AMD64/Intel 64 版本的物理 64 位服务器。

Red Hat Virtualization 平台上的物理主机：

- 必须在系统中只属于一个集群。
- 必须有支持 AMD-V 或 Intel VT 硬件虚拟化扩展的 CPU。
- 必须具有支持由集群创建时所选虚拟 CPU 类型公开的所有功能的 CPU。

- 至少 2 GB RAM。
- 具有具有系统权限的系统管理员。

管理员可以从 Red Hat Virtualization 监视列表接收最新的安全公告。订阅 Red Hat Virtualization 监视列表，通过电子邮件接收 Red Hat Virtualization 产品的新安全公告。通过填写此表单来订阅：

<https://www.redhat.com/mailman/listinfo/rhsa-announce>

2.5.2. Red Hat Virtualization Host

Red Hat Virtualization Host (RHVH)使用特殊构建的 Red Hat Enterprise Linux 安装，且只有托管虚拟机所需的软件包。它使用一个基于 Red Hat Enterprise Linux 主机使用的 Anaconda 安装界面，并可通过 Red Hat Virtualization Manager 或 yum 更新。使用 yum 命令是安装附加软件包的唯一方法，并在升级后保留它们。

RHVH 提供了一个 Cockpit Web 界面，用于监控主机的资源并执行管理任务。不支持通过 SSH 或控制台直接访问 RHVH，因此 Cockpit Web 界面为主机添加到 Red Hat Virtualization Manager 之前执行的任务提供了一个图形用户界面，比如通过 Terminal 子选项卡配置网络或运行终端命令。

在 Web 浏览器中，访问 <https://HostFQDNorIP:9090> 的 Cockpit Web 界面。适用于 RHVH 的 Cockpit 包含自定义虚拟化仪表盘，显示主机健康状态、SSH 主机密钥、自托管引擎状态、虚拟机和虚拟机统计信息。

从 Red Hat Virtualization 版本 4.4 SP1 开始，RHVH 使用 systemd-coredump 收集、保存和处理核心转储。如需更多信息，请参阅 [内核转储存储配置文件和 systemd-coredump 服务](#) 的文档。

在 Red Hat Virtualization 4.4 及更早的 RHVH 中，使用自动错误报告工具(ABRT)来收集有关应用程序崩溃的有意义的调试信息。如需更多信息，请参阅 [Red Hat Enterprise Linux 系统管理员指南](#)。



注意

可以使用 grubby 工具将自定义启动内核参数添加到 Red Hat Virtualization Host 中。grubby 工具对 grub.cfg 文件进行持久更改。导航到主机的 Cockpit Web 界面中的 Terminal 子选项卡，以使用 grubby 命令。如需更多信息，请参阅 [Red Hat Enterprise Linux 系统管理员指南](#)。

**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。

2.5.3. Red Hat Enterprise Linux 主机

您可以使用 Red Hat Enterprise Linux 7 作为主机在功能的硬件中安装。Red Hat Virtualization 支持运行 Red Hat Enterprise Linux 7 Server AMD64/Intel 64 版本（带有 Intel VT 或 AMD-V 扩展）的主机。要使用 Red Hat Enterprise Linux 机器作为主机，还必须附加 Red Hat Enterprise Linux 服务器和 Red Hat Virtualization 订阅。

添加主机可能需要一些时间，因为以下步骤由平台完成：虚拟化检查、安装软件包以及创建桥接。使用详情视图监控进程作为主机和管理系统建立连接。

另外，您可以安装一个 Cockpit Web 界面来监控主机的资源并执行管理任务。Cockpit Web 界面为在主机添加到 Red Hat Virtualization Manager 之前执行的任务提供了一个图形用户界面，如配置网络或通过 Terminal 子选项卡运行终端命令。

**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。

2.5.4. Satellite 主机提供程序主机

Satellite 主机提供程序提供的主机也可以用作 Red Hat Virtualization Manager 的虚拟化主机。在将 Satellite 主机提供程序作为外部提供者添加到管理器后，它所提供的任何主机都可添加到 Red Hat Virtualization 中，方式与 Red Hat Virtualization 主机(RHVH)和 Red Hat Enterprise Linux 主机相同。

2.5.5. 主机任务

2.5.5.1. 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. 单击 **OK**。

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。

2.5.5.2. 添加 Satellite 主机提供程序主机

添加 **Satellite** 主机的过程与添加 **Red Hat Enterprise Linux** 主机的过程几乎相同，但该主机在 **Manager** 中标识的方法几乎相同。以下流程概述了如何添加由 **Satellite** 主机提供程序提供的主机。

流程

1. 单击 **Compute** → **Hosts**。
2. 单击 **New**。
3. 使用下拉菜单为新主机选择 **Host Cluster**。
4. 选中 **Foreman/Satellite** 复选框，以显示添加 **Satellite** 主机提供程序主机的选项，然后选择要为其添加主机的供应商。
5. 选择 **Discovered Hosts** 或 **Provisioned Hosts**。
 - **discovered Hosts**（默认选项）：从下拉列表中选择主机、主机组和计算资源。
 - **调配的主机**：从 **Providers Hosts** 下拉列表中选择主机。

有关可以从外部供应商检索的主机的任何详情都会自动设置，并可以根据需要编辑。

6. 输入新主机的 **Name** 和 **SSH Port** (只适用于置备的主机)。
7. 选择用于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。
 - 将 **SSH PublicKey** 字段中显示的密钥复制到主机上的 `/root/.ssh/authorized_hosts` 中, 以使用公钥身份验证 (仅限会话) 。
8. 您现在已完成添加 **Red Hat Enterprise Linux** 主机的强制步骤。单击 **Advanced Parameters** 下拉菜单按钮以显示高级主机设置。
 - a. (可选) 禁用自动防火墙配置。
 - b. (可选) 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。
9. 您可以使用适用的选项卡配置 **Power Management, SPM, Console, 和 Network Provider** ; 但是, 由于这些选项卡对于添加 **Red Hat Enterprise Linux** 主机不是基本, 所以此流程中不涉及这些选项卡。
10. 点 **OK** 添加主机并关闭窗口。

新主机显示在主机列表中, 状态为 **Installing**, 您可以在详情视图中查看安装的进度。安装完成后, 状态将更新为 **Reboot**。必须激活该主机, 才能使状态变为 **Up**。

2.5.5.3. 为主机设置卫星勘误表查看

在管理门户中, 您可以配置主机来查看 **Red Hat Satellite** 中的勘误。将主机与 **Red Hat Satellite** 供应商相关联后, 您可以在主机配置仪表板中接收有关可用勘误表及其重要性的更新, 并决定何时应用更新。

Red Hat Virtualization 4.4 支持使用 **Red Hat Satellite 6.6** 查看勘误。

前提条件

- **Satellite 服务器必须添加为外部提供程序。**
- **您要查看勘误表的 Manager 及任何主机都必须通过对应的 FQDN 在卫星服务器中注册。这样可确保外部内容主机 ID 无需在 Red Hat Virtualization 中维护。**



重要

使用 IP 地址添加的主机无法报告勘误表。

- **管理主机的 Satellite 帐户必须具有 Administrator 权限和默认的组织设置。**
- **主机必须注册到卫星服务器。**
- **使用 Red Hat Satellite 远程执行来管理主机上的软件包。**



注意

Katello 代理已弃用，并将在以后的 Satellite 版本中删除。迁移进程以使用远程执行功能远程更新客户端。

流程

1. **单击 Compute → Hosts，再选择 主机。**
2. **点 Edit。**
3. **选中 Use Foreman/Satellite 复选框。**
4. **从下拉列表中选择所需的 Satellite 服务器。**

5. 点击 OK。

现在，主机被配置为显示可用的勘误表及其重要信息，它们在用于管理主机的配置的同仪表板中。

其他资源

- [为主机调配添加 Red Hat Satellite 实例](#)
- 在 Red Hat Satellite 文档中没有 [Goferd](#) 和 [Katello Agent](#) 的**主机管理**

2.5.5.3.1. 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。

前提条件

- 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](#)。

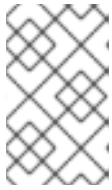
为 PCI Passthrough 配置主机

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
```

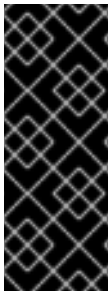
2.

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
```

2.5.5.3.2. 为所有虚拟机启用嵌套虚拟化



重要

使用 `hook` 启用嵌套虚拟化是一项技术预览功能。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](#)。

嵌套虚拟化可让虚拟机托管其他虚拟机。为清楚起见，我们将这些称为**父虚拟机**和**嵌套虚拟机**。

子虚拟机仅对具有父虚拟机权限的用户查看和管理。它们对 **Red Hat Virtualization (RHV)** 管理员不可见。

默认情况下，RHV 中不启用嵌套虚拟化。要启用嵌套虚拟化，您需要在集群中的所有主机上安装 `VDSM hook vdsm-hook-nestedvt`。然后，在这些主机上运行的所有虚拟机都可以作为父虚拟机运行。

您应该只在支持嵌套虚拟化的主机上运行父虚拟机。如果父虚拟机迁移到不支持嵌套虚拟化的主机，则其子虚拟机将失败。要防止这种情况，请将集群中的所有主机配置为支持嵌套虚拟化。否则，限制父虚拟机迁移到不支持嵌套虚拟化的主机。



警告

采取预防措施，防止父虚拟机迁移到不支持嵌套虚拟化的主机。

流程

1. 在管理门户中，点 **Compute** → **Hosts**。
2. 选择您要启用嵌套虚拟化的集群中的主机，然后点 **Management** → **Maintenance** 和 **OK**。
3. 再次选择主机，单击 **Host Console**，然后登录主机控制台。

4. 安装 **VDSM hook**：

```
# dnf install vds-hook-nestedvt
```

5. 重启主机。

6. 再次登录到主机控制台并验证是否启用了嵌套虚拟化：

```
$ cat /sys/module/kvm*/parameters/nested
```

如果这个命令返回 **Y** 或 **1**，则表示启用了该功能。

7. 对集群中的所有主机重复此步骤。

VDSM hook

2.5.5.3.3. 为单独的虚拟机启用嵌套虚拟化



重要

嵌套虚拟化是技术预览功能。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](#)。

嵌套虚拟化可让虚拟机托管其他虚拟机。为清楚起见，我们将这些称为**父虚拟机**和**嵌套虚拟机**。

子虚拟机仅对具有父虚拟机权限的用户查看和管理。它们对 Red Hat Virtualization (RHV)管理员不可见。

要在**特定虚拟机上**（而非所有虚拟机）启用嵌套虚拟化，您要将主机或主机配置为支持嵌套虚拟化。然后，您可以在这些特定主机上运行虚拟机或虚拟机并启用**传递主机 CPU**。此选项可让虚拟机使用您刚刚在主机上配置的嵌套虚拟设置。这个选项还限制虚拟机可在哪些主机上运行并且需要手动迁移。

否则，要为**集群中的所有虚拟机**启用嵌套虚拟化，请参阅[为所有虚拟机启用嵌套虚拟化](#)

仅在支持嵌套虚拟化的主机上运行父虚拟机。如果您将父虚拟机迁移到不支持嵌套虚拟化的主机，则其子虚拟机将失败。



警告

不要将父虚拟机迁移到不支持嵌套虚拟化的主机。

避免实时迁移运行子虚拟机的父虚拟机。即使源和目标主机都相同，并且支持嵌套虚拟化，实时迁移也会导致子虚拟机失败。相反，请在迁移前关闭虚拟机。

流程

将主机配置为支持嵌套虚拟化：

1. 在管理门户中，点 **Compute** → **Hosts**。
2. 选择您要启用嵌套虚拟化的集群中的主机，然后点 **Management** → **Maintenance** 和 **OK**。
3. 再次选择主机，单击 **Host Console**，然后登录主机控制台。
4. 在 **Edit Host** 窗口中，选择 **Kernel** 选项卡。
5. 在 **内核引导参数** 下，如果复选框问候，请单击 **RESET**。
6. 选择嵌套虚拟化并单击确定。

此操作在 **Kernel** 命令行中显示一个 `kvm-<architecture>.nested=1` 参数。以下步骤将这个参数添加到 **Current kernel CMD** 行。

7. 点 **Installation** → **Reinstall**。
8. 当主机状态变为 **Up** 时，点 **Power Management** or **SSH Management** 下的 **Management** → **Restart**。
9. 验证嵌套虚拟化是否已启用。登录到主机控制台并输入：

```
$ cat /sys/module/kvm*/parameters/nested
```

如果这个命令返回 **Y** 或 **1**，则表示启用了该功能。

10. 对运行父虚拟机的所有主机重复此步骤。

在特定虚拟机中启用嵌套虚拟化：

1. 在管理门户中，点 **Compute** → **Virtual Machines**。
2. 选择虚拟机并点 **Edit**
3. 在 **Edit Virtual Machine** 窗口中，点 **Show Advanced Options** 并选择 **Host** 选项卡。
4. 在 **Start Running On** 下，点 **Specific Host**，再选择您配置为支持嵌套虚拟化的主机或主机。
5. 在 **CPU** 选项下，选择 **Pass-Through Host CPU**。此操作会自动将 **Migration** 模式设置为只允许手动迁移。



注意

在 RHV 版本 4.2 中，当选择 不允许迁移时，您只能启用 **Pass-Through Host CPU**。

其他资源

- [VDSM hook](#)
- 在 RHEL 文档中 [创建嵌套虚拟机](#)。

2.5.5.4. 将主机移到维护模式

许多常见的维护任务（包括网络配置和部署软件更新）都需要将主机置于维护模式。在可能导致 **VDSM** 停止正常工作的事件（如重启或网络或存储问题）之前，主机应置于维护模式。

当主机被置于维护模式时，**Red Hat Virtualization Manager** 会尝试将所有正在运行的虚拟机都迁移到备用主机。实时迁移应用标准先决条件，特别是集群中必须至少有一个活动主机，且具备相应的容量才可运行迁移的虚拟机。



注意

固定在主机上且无法迁移的虚拟机将被关闭。您可以通过在主机详情视图中的 **Virtual Machines** 选项卡中点 **Pinned to Host** 来检查哪些虚拟机被固定到主机。

将主机置于维护模式

1. 单击 **Compute** → **Hosts**，再选择所需的主机。
2. 单击 **Management** → **Maintenance**。这将打开 **Maintenance Host (s)** 确认窗口。
3. (可选) 输入将主机置于维护模式的 **Reason**，该模式将显示在日志中以及主机再次激活时。然后点 **OK**



注意

只有在集群设置中启用时，才会显示主机维护 **Reason** 字段。如需更多信息，请参阅[集群常规设置说明](#)。

4. (可选) 为支持 **Gluster** 的主机选择所需选项。

选择 **Ignore Gluster Quorum and Self-Heal Validations** 选项以避免默认检查。默认情况下，管理器会检查当主机进入维护模式时是否不会丢失 **Gluster** 仲裁。管理器还通过将主机移至维护模式，检查是否有可影响的自我修复活动。如果 **Gluster** 仲裁将丢失，或者有会受到影响的自我修复活动，则管理器会阻止主机进入维护模式。只有当没有将主机置于维护模式时使用这个选项。

选择 **Stop Gluster Service** 选项，以停止所有 **Gluster** 服务，同时将主机移入维护模式。



注意

只有所选主机支持 **Gluster** 时，这些字段才会出现在主机维护窗口中。如需更多信息，请参阅[替换主 Gluster Storage 节点以维护 Red Hat Hyperconverged Infrastructure](#)。

5. 单击 **OK** 以启动维护模式。

所有正在运行的虚拟机都迁移到其他主机上。如果主机是存储池管理程序 (SPM)，则 SPM 角色将迁移到其他主机。主机的 **Status** 字段更改为 **Preparing for Maintenance**，并在操作成功完成时最终变为 **Maintenance**。当主机处于维护模式时，VDSM 不会停止。



注意

如果有任何虚拟机上的迁移失败，请单击主机上的 **Management** → **Activate** 停止操作进入维护模式，然后单击虚拟机上的 **Cancel Migration** 来停止迁移。

2.5.5.5. 从维护模式激活主机

必须先激活已置于维护模式或最近添加到环境中的主机。如果主机未就绪，激活可能会失败；确保在尝试激活主机前完成所有任务。

流程

1. 单击 **Compute** → **Hosts**，再选择 主机。
2. 点 **Management** → **Activate**。

主机状态会更改为 **Unassigned**，然后在操作完成时最后 启动。虚拟机现在可以在主机上运行。当主机被置于维护模式时，从主机迁移的虚拟机在激活后不会自动迁移到主机，但可以手动迁移。如果主机在进入维护模式之前是存储池管理器 (SPM)，则当主机激活时 SPM 角色不会自动返回。

2.5.5.5.1. 配置主机防火墙规则

您可以使用 **Ansible** 配置主机防火墙规则，使其具有持久性。集群必须配置为使用 **firewalld**。



注意

不支持更改 **firewalld** 区域。

为主机配置防火墙规则

1. 在 Manager 计算机上，编辑 `ovirt-host-deploy-post-tasks.yml.example` 来添加自定义防火墙端口：

```
# vi /etc/ovirt-engine/ansible/ovirt-host-deploy-post-tasks.yml.example
---
#
# Any additional tasks required to be executing during host deploy process can
# be added below
#
- name: Enable additional port on firewalld
  firewalld:
    port: "12345/tcp"
    permanent: yes
    immediate: yes
    state: enabled
```

2. 将文件保存为 `ovirt-host-deploy-post-tasks.yml`。

使用更新的防火墙规则配置新的或重新安装的主机。

现有的主机需要通过点 **Installation** → **Reinstall** 并选择 **Automatically configure host firewall** 来重新安装。

2.5.5.5.2. 删除主机

有时需要从 Red Hat Virtualization 环境中删除主机，比如重新安装主机时。

流程

1. 单击 **Compute** → **Hosts**，再选择 主机。
2. 单击 **Management** → **Maintenance**。
3. 主机处于维护模式后，单击 **Remove**。**Remove Host (s)** 确认窗口将打开。
4. 如果主机属于 Red Hat Gluster Storage 集群的一部分，并选择 **Force Remove** 复选框，并且在其上有卷 **brick**，或者主机是否不响应。

5. 点击 **OK**。

2.5.5.5.3. 更新次版本之间的主机

您可以更新**集群中的所有主机**，或**更新单个主机**。

2.5.5.5.3.1. 更新集群中的所有主机

您可以更新集群中的所有主机，而不是逐一更新主机。这在升级到 Red Hat Virtualization 的新版本时特别有用。如需有关用于自动化更新的 Ansible 角色的更多信息，请参阅 [oVirt Cluster Upgrade](#)。

一次更新一个集群。

限制

- 在 RHVH 上，更新仅保留 /etc 和 /var 目录中的修改内容。更新期间会覆盖其他路径中的修改数据。
- 如果启用了迁移，则虚拟机将自动迁移到集群中的另一主机上。
- 在自托管引擎环境中，管理器虚拟机只能在同一集群中自托管引擎节点之间迁移。它不能迁移到标准主机。
- 集群必须有足够的内存供其主机执行维护。否则，虚拟机迁移将挂起且失败。您可以通过在更新主机前关闭部分或所有虚拟机来减少主机更新的内存使用。
- 您无法将固定的虚拟机（如使用 vGPU 的虚拟机）迁移到另一台主机。固定虚拟机会在更新过程中关闭，除非您选择跳过该主机。


流程

1. 在管理门户中，点 **Compute** → **Clusters** 并选择集群。Upgrade status 列显示集群中任何主机的升级是否可用。

2. 单击 **Upgrade**。
3. 选择要更新的主机，然后单击 **Next**。
4. 配置选项：
 - **Stop Pinned VMs** 会关闭固定到集群中主机的任何虚拟机，这个选项被默认选择。您可以清除此复选框以跳过更新这些主机，从而使固定虚拟机保持运行，例如当固定虚拟机运行重要服务或进程时，您不希望它在更新过程中在未知时间关闭。
 - **Upgrade Timeout (Minutes)** 设置在集群升级失败并显示超时前等待各个主机更新的时间。默认值为 60。您可以为可能不足 60 分钟的大型集群增加它，或者为主机快速更新的小型集群减少它。
 - **Check Upgrade** 会在运行升级过程前，检查每个主机是否有可用的更新。默认情况下不选择它，但如果您需要确保包括最新的更新，例如当您配置了 **Manager** 以检查主机更新少于默认值时，您可以选择它。
 - **Reboot After Upgrade** 会在更新后重新启动，这会默认选择。如果您确定没有需要主机重新引导的待定更新，您可以清除此复选框来加快进程。
 - 在更新过程中，使用 **Maintenance Policy** 将集群的调度策略设置为 [cluster_maintenance](#)。默认情况下会选择它，因此活动有限，除非为高可用，虚拟机不会启动。如果您有一个自定义调度策略要在更新过程中一直使用，但这可能会产生未知的后果，您可以清除此复选框。在禁用这个选项前，请确保您的自定义策略与集群升级活动兼容。
5. 点 **Next**。
6. 检查受影响的主机和虚拟机的摘要。
7. 单击 **Upgrade**。
8. 集群升级状态屏幕会显示进度条，显示完成的情况，以及升级过程中的步骤列表。您可以

点击 **Go to Event Log** 打开升级的日志条目。关闭此屏幕不会中断升级过程。

您可以跟踪主机更新的进度：

- 在 **Compute** → **Clusters** 视图中，**Upgrade Status** 列会显示一个进度条，显示完成的百分比。
- 在 **Compute** → **Hosts** 视图中
- 在 **Notification Drawer** 的 **Events** 部分()。

您可以通过 **Compute** → **Virtual Machines** 视图中的 **Status** 栏跟踪各个虚拟机的迁移进度。在大型环境中，您可能需要过滤结果以显示一组特定的虚拟机。

2.5.5.5.3.2. 更新单个主机

使用主机升级管理器直接从管理门户更新各个主机。



注意

升级管理器仅检查状态为 **Up** 或 **Non-operational**，但不是 **Maintenance** 的主机。

限制

- 在 RHVH 上，更新仅保留 **/etc** 和 **/var** 目录中的修改内容。更新期间会覆盖其他路径中的修改数据。
- 如果启用了迁移，则虚拟机将自动迁移到集群中的另一主机上。在主机使用量相对较低时更新主机。
- 在自托管引擎环境中，管理器虚拟机只能在同一集群中自托管引擎节点之间迁移。它不能迁移到标准主机。

- 集群必须有足够的内存供其主机执行维护。否则，虚拟机迁移将挂起且失败。您可以通过在更新主机前关闭部分或所有虚拟机来减少主机更新的内存使用。
- 您无法将固定的虚拟机（如使用 vGPU 的虚拟机）迁移到另一台主机。在更新主机之前，必须关闭固定虚拟机。

流程

1.

确保启用了正确的存储库。要查看当前启用的存储库列表，请运行 `dnf repolist`。

-

对于 Red Hat Virtualization 主机：

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

-

对于 Red Hat Enterprise Linux 主机：

```
# subscription-manager repos \
  --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=advanced-virt-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms

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

2.

在管理门户中，点 **Compute** → **Hosts** 并选择要更新的主机。

3.

点 **Installation** → **Check for Upgrade** 并点 **OK**。

打开 Notification Drawer (



)并展开 **Events** 部分来查看结果。

4.

如果有可用更新，点 **Installation** → **Upgrade**。

5.

点 **OK** 来更新主机。运行的虚拟机会根据其迁移策略迁移。如果对任何虚拟机禁用迁移，则会提示您将其关闭。

主机详情会在 **Compute** → **Hosts** 中更新，其状态会经历以下阶段：

Maintenance > Installing > Reboot > Up



注意

如果更新失败，主机的状态将变为 **Install Failed**。在 **Install Failed Installation** → **Upgrade**。

对 **Red Hat Virtualization** 环境中的每一主机重复此步骤。



注意

您应该从管理门户更新主机。但是，您可以使用 `dnf upgrade` 来更新主机。

2.5.5.5.3.3. 手动更新主机

小心

此信息适用于需要手动更新主机的高级系统管理员。红帽不支持此方法。本节中描述的程序并没有完全包括重要的步骤，如证书续订。假设对其已有了解。红帽支持使用管理门户更新主机。详情请参阅 *Administration Guide* 中的 [Updating individual hosts](#) 或 [Updating all hosts in a cluster](#)。

您可以使用 `dnf` 命令更新您的主机。定期更新您的系统以确保及时应用安全和漏洞修复。

限制

- 在 RHVH 上，更新仅保留 `/etc` 和 `/var` 目录中的修改内容。更新期间会覆盖其他路径中的修改数据。
- 如果启用了迁移，则虚拟机将自动迁移到集群中的另一主机上。在主机使用量相对较低时更新主机。
-

在自托管引擎环境中，管理器虚拟机只能在同一集群中自托管引擎节点之间迁移。它不能迁移到标准主机。

- 集群必须有足够的内存供其主机执行维护。否则，虚拟机迁移将挂起且失败。您可以通过在更新主机前关闭部分或所有虚拟机来减少主机更新的内存使用。
- 您无法将固定的虚拟机（如使用 vGPU 的虚拟机）迁移到另一台主机。在更新主机之前，必须关闭固定虚拟机。

流程

1. 确保启用了正确的存储库。您可以通过运行 `dnf repolist` 来检查当前启用了哪些存储库。

- 对于 Red Hat Virtualization 主机：

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

- 对于 Red Hat Enterprise Linux 主机：

```
# subscription-manager repos \
  --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=advanced-virt-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms

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

2. 在管理门户中，点 **Compute** → **Hosts** 并选择要更新的主机。

3. 点 **Management** → **Maintenance** 和 **OK**。

4. 对于 Red Hat Enterprise Linux 主机：

- a. 确定 Red Hat Enterprise Linux 的当前版本：

```
# cat /etc/redhat-release
```

-
- b. 检查哪个版本的 `redhat-release` 软件包可用：

```
# dnf --refresh info --available redhat-release
```

此命令显示任何可用的更新。例如，当从 Red Hat Enterprise Linux 8.2.z 升级到 8.3，比较软件包版本和当前安装的版本：

```
Available Packages
Name      : redhat-release
Version   : 8.3
Release   : 1.0.el8
...
```

小心

Red Hat Enterprise Linux Advanced Virtualization 模块通常比 Red Hat Enterprise Linux y-stream 晚发布。如果没有新的 Advanced Virtualization 模块可用，或者有启用它的错误，在此停止并取消升级。否则，您将面临损坏主机的风险。

- c. 如果 Red Hat Enterprise Linux 8.3 或更高版本有 Advanced Virtualization 流，请重置 `virt` 模块：

```
# dnf module reset virt
```



注意

如果在 Advanced Virtualization 流中已启用此模块，则不需要这一步骤，但它不会造成负面影响。

您可以输入以下内容来查看流的值：

```
# dnf module list virt
```

- d. 使用以下命令在高级虚拟化流中启用 `virt` 模块：

- **RHV 4.4.2 :**

```
# dnf module enable virt:8.2
```

-

RHV 4.4.3 到 4.4.5 :

```
# dnf module enable virt:8.3
```

-

对于 RHV 4.4.6 到 4.4.10 :

```
# dnf module enable virt:av
```

-

对于 RHV 4.4 及更新的版本 :

```
# dnf module enable virt:rhel
```



注意

从 RHEL 8.6 开始，高级虚拟化软件包将使用标准 `virt:rhel` 模块。对于 RHEL 8.4 和 8.5，只使用一个高级虚拟化流，`rhel:av`。

5.

启用 `nodejs` 模块的版本 14:

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

6.

更新主机 :

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

7.

重新启动主机，以确保正确应用所有更新。



注意

检查基于 `img` 的日志，以查看是否有其他软件包更新针对 Red Hat Virtualization 主机失败。如果在更新后成功重新安装某些软件包，请检查 `/var/imagbased/perted-rpms` 中是否列出了软件包。添加任何缺少的软件包，然后运行 `rpm -Uvh /var/imagbased/persisted-rpms/*`。

对 Red Hat Virtualization 环境中的每一主机重复此过程。

2.5.5.5.4. 重新安装主机

从管理门户重新安装 Red Hat Virtualization 主机(RHVH)和 Red Hat Enterprise Linux 主机。该流程包括停止和重启主机。



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。

前提条件

- 如果集群启用了迁移，虚拟机可以自动迁移到集群中的另一台主机。因此，在主机使用量相对较低时，重新安装主机。
- 确保集群有足够的内存来执行维护。如果集群缺少内存，迁移虚拟机将挂起，然后失败。要减少内存用量，请在将主机移至维护之前关闭部分或所有虚拟机。
- 在执行重新安装前，请确保集群包含多个主机。不要尝试同时重新安装所有主机。个主机必须保持可用才能执行存储池管理程序(SPM)任务。

流程

1. 单击 **Compute** → **Hosts**，再选择 主机。
2. 点 **Management** → **Maintenance** 和 **OK**。
3. 点 **Installation** → **Reinstall**。这将打开 **Install Host** 窗口。

4.

单击**确定**以重新安装主机。

重新安装主机并将其状态返回到**启动**后，您可以将虚拟机迁移到主机。



重要

将 Red Hat Virtualization Host 注册到 Red Hat Virtualization Manager 并重新安装它后，管理门户可能会错误地将其状态显示为 **Install Failed**。单击 **Management** → **Activate**，主机将更改为 **Up** 状态并可供使用。

2.5.5.6. 查看主机勘误


主机已配置为从 Red Hat Satellite 服务器接收勘误信息后，可以查看每个主机的勘误信息。有关将主机配置为接收勘误信息的更多信息，请参阅 [为主机配置 Satellite 勘误管理](#)

流程

1. 单击 **Compute** → **Hosts**。
2. 单击主机的名称。这会打开详情视图。
3. 点 **Errata** 选项卡。

2.5.5.7. 查看主机的 Health 状态

除了其常规状态外，主机还具有外部健康状态。外部健康状态由插件或外部系统报告，或者由管理员设置，并出现在主机名称左侧的以下图标之一：

- 确定：无图标
- info：

-

警告：



•

错误：



•

失败：



要查看主机健康状况的更多详情，请点主机的名称。这会打开详情视图，然后点 **Events** 选项卡。

也可以使用 **REST API** 查看主机的健康状况。主机上的 **GET** 请求将包含 `external_status` 元素，其中包含健康状况。

您可以通过 **事件** 集合在 **REST API** 中设置主机健康状况。如需更多信息，请参阅 *REST API 指南* 中的 [添加事件](#)。

2.5.5.8. 查看主机设备

您可以在详情视图中的 **Host Devices** 选项卡中查看每个主机的主机设备。如果为直接设备分配配置了主机，则这些设备可以直接附加到虚拟机，以提高性能。

如需有关直接设备分配的硬件要求的更多信息，请参阅 *Hardware Considerations for Implementing SR-IOV* 中的 [Additional Hardware Considerations for Using Device Assignment](#)。

有关配置主机以进行直接设备分配的更多信息，请参阅 [PCI Passthrough 主机任务配置主机](#)。

有关将主机设备附加到虚拟机的更多信息，请参阅 *虚拟机管理指南* 中的 [主机设备](#)。

流程

1. 单击 **Compute** → **Hosts**。
2. 单击主机的名称。这会打开详情视图。
3. 单击 **主机设备** 选项卡。

此选项卡列出了主机设备的详细信息，包括设备是否附加到虚拟机，并且当前由该虚拟机使用。

2.5.5.9. 从管理门户访问 Cockpit

Cockpit 默认在 Red Hat Virtualization 主机上(RHVM)和 Red Hat Enterprise Linux 主机上可用。您可以通过在浏览器中输入地址或通过管理门户来访问 **Cockpit Web** 界面。

流程

1. 在管理门户中，单击 **Compute** → **Hosts** 并选择主机。
2. 单击 **Host Console**。

Cockpit 登录页面将在新的浏览器窗口中打开。

2.5.5.9.1. 设置传统 SPICE 密码

SPICE 控制台默认使用 **FIPS** 兼容加密和密码字符串。默认的 **SPICE** 密码字符串为：
kECDHE+FIPS:kDHE+FIPS:kRSA+FIPS:!eNULL:!aNULL:!aNULL

此字符串通常已足够。但是，如果您的虚拟机具有较旧的操作系统或 **SPICE** 客户端，其中一个或另一个不支持 **FIPS** 兼容的加密，则必须使用更弱的密码字符串。否则，如果您在现有集群中安装新集群或新主机并尝试连接到该虚拟机，则可能会出现连接安全错误。

您可以使用 **Ansible playbook** 更改密码字符串。

更改密码字符串

1. 在 Manager 计算机上，在 `/usr/share/ovirt-engine/playbooks` 目录中创建文件。例如：

```
# vim /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

2. 在文件中输入以下内容并保存它：

```
name: oVirt - setup weaker SPICE encryption for old clients
hosts: hostname
vars:
  host_deploy_spice_cipher_string: 'DEFAULT:-RC4:-3DES:-DES'
roles:
  - ovirt-host-deploy-spice-encryption
```

3. 运行您刚才创建的文件：

```
# ansible-playbook -I hostname /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

或者，您可以使用带有变量 `host_deploy_spice_cipher_string` 的 `--extra-vars` 选项的 Ansible `playbook ovirt-host-deploy` 重新配置主机：

```
# ansible-playbook -I hostname \
  --extra-vars host_deploy_spice_cipher_string="DEFAULT:-RC4:-3DES:-DES" \
  /usr/share/ovirt-engine/playbooks/ovirt-host-deploy.yml
```

2.5.5.10. 配置主机电源管理设置

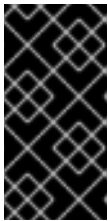
配置主机电源管理设备设置，以从管理门户执行主机生命周期操作（停止、启动、重新启动）。

您必须配置主机电源管理，以便使用主机高可用性和虚拟机高可用性。有关电源管理设备的更多信息，请参阅[技术参考中的电源管理](#)。

流程

1. 单击 **Compute** → **Hosts** 并选择一个主机。

2. 单击 **Management** → **Maintenance**，然后单击 **OK** 进行确认。
3. 当主机处于维护模式时，单击 **Edit**。
4. 点 **Power Management** 选项卡。
5. 选中 **Enable Power Management** 复选框来启用字段。
6. 选择 **Kdump 集成** 复选框以防止在执行内核崩溃转储时隔离主机。

**重要**

如果在现有主机上启用或禁用 **Kdump 集成**，您必须[重新安装主机](#)以便配置 **kdump**。

7. (可选) 如果您不希望主机的电源管理由主机的集群的调度策略控制，请选择 **Disable policy control of power management** 复选框。
8. 单击加号(+)按钮，以添加新的电源管理设备。这会打开 **Edit fence agent** 窗口。
9. 在相应的字段中，输入电源管理设备的用户名和密码。
10. 从下拉列表中选择电源管理设备类型。
11. 在 **Address** 字段中输入 IP 地址。
12. 输入电源管理设备用来与主机通信的 **SSH** 端口号。
13. 输入 **Slot** 编号，用于识别电源管理设备的刀片式。

14. 输入电源管理设备的 **Options**。使用以逗号分隔的 **'key=value'** 条目列表。
 - 如果可以使用 IPv4 和 IPv6 IP 地址（默认），将 **Options** 字段留空。
 - 如果只能使用 IPv4 IP 地址，输入 **inet4_only=1**。
 - 如果只能使用 IPv6 IP 地址，输入 **inet6_only=1**。
15. 选中 **Secure** 复选框，以启用电源管理设备安全地连接到主机。
16. 单击 **Test** 以确保设置正确。测试 **Succeeded**，在成功验证后，**Host Status** 为：时会显示。
17. 单击 **OK** 关闭 **Edit fence agent** 窗口。
18. 在电源管理选项卡中，选择展开高级参数，并使用"上移"按钮指定管理器将搜索主机的集群和 **dc**（数据中心）用于隔离代理的顺序。
19. 单击 **OK**。

**注意**

- 对于 IPv6，Red Hat Virtualization 仅支持静态寻址。
- 不支持双栈 IPv4 和 IPv6 地址。

现在，管理门户中启用了 **Management** → **Power Management** 下拉菜单。

2.5.5.11. 配置主机存储池管理程序设置

存储池管理程序 (SPM) 是针对数据中心中的一个主机的管理角色，用于维护对存储域的访问控制。

SPM 必须始终可用，如果 SPM 主机不可用，则 SPM 角色将分配给其他主机。由于 SPM 角色使用部分主机的可用资源，因此优先选择可以负担资源的主机非常重要。

主机的存储池管理器(SPM)优先级设置会改变被分配 SPM 角色的主机的可能性：在主机具有高 SPM 优先级的主机前，将被分配 SPM 角色。

流程

1. 单击 **Compute** → **Hosts**。
2. 单击 **Edit**。
3. 单击 **SPM** 选项卡。
4. 使用单选按钮为主机选择适当的 **SPM** 优先级。
5. 单击 **OK**。

2.5.5.11.1. 将自托管引擎主机迁移到其他集群

您不能将配置为自托管引擎主机的主机迁移到运行自托管引擎虚拟机所在的数据中心或集群。所有自托管引擎主机必须位于同一数据中心和集群中。

您需要通过从主机取消部署自托管引擎配置来禁用主机作为自托管引擎主机。

流程

1. 单击 **Compute** → **Hosts**，再选择 **主机**。
2. 单击 **Management** → **Maintenance**。主机的状态更改为 **Maintenance**。
3. 在 **Reinstall** 下，选择 **Hosted Engine UNDEPLOY**。

4. 点 **Reinstall**。

提示

或者，也可以使用 REST API `undeploy_hosted_engine` 参数。

5. 点 **Edit**。
6. 选择目标数据中心和集群。
7. 点击 **OK**。
8. 点 **Management** → **Activate**。

其他资源

- [将主机移到维护模式](#)
- [从维护模式激活主机](#)

2.5.6. New Host 和 Edit Host Windows 中的设置和控件的说明


2.5.6.1. 主机常规设置说明

这些设置适用于编辑主机详情或添加新的 Red Hat Enterprise Linux 主机和 Satellite 主机提供程序主机。

General 设置表包含 **New Host** 或 **Edit Host** 窗口的常规选项卡上所需的信息。

表 2.20. 常规设置

字段名称	Description
主机集群	主机所属的集群和数据中心。
使用 Foreman/Satellite	<p>选择或清除此复选框，以查看或隐藏用于添加由 Satellite 主机提供程序提供的主机的选项。以下选项也可用：</p> <p>发现的主机</p> <ul style="list-style-type: none"> ● 发现的主机 - 填充引擎所发现的卫星主机名称的下拉列表。 ● 主机组 -A 可用主机组的下拉列表。 ● 计算资源 - 提供计算资源的虚拟机监控程序下拉列表。 <p>置备的主机</p> <ul style="list-style-type: none"> ● Provider Hosts - 使用所选外部提供者提供的主机名称填充的下拉列表。此列表中的条目按照提供程序搜索过滤器中输入的任何搜索查询过滤。 ● Provider search filter - 允许您搜索所选外部提供者提供的主机的文本字段。这个选项特定于供应商; 请参阅供应商文档来获取有关特定供应商的搜索查询的详情。将此字段留空以查看所有可用的主机。
Name	主机的名称。此文本字段的限制为 40 个字符，且必须是唯一的名称，其中含有大写字母和小写字母、数字、连字符和下划线的任意组合。
注释	用于添加与主机相关的纯文本可读注释的字段。
Hostname	主机的 IP 地址或可解析的主机名。如果使用可解析的主机名，您必须确保解析主机名的所有地址都解析为与主机的管理网络匹配的 IP 地址、IPv4 和 IPv6。
密码	主机的 root 用户的密码。在添加主机时设置密码。之后无法编辑密码。
安装后激活主机	<p>选择这个复选框以在成功安装后激活主机。这默认是启用的，且需要成功激活管理程序。</p> <p>成功安装后，您可以清除此复选框，将主机状态切换为维护。这样，管理员可以对虚拟机监控程序执行其他配置任务。</p>

字段名称	Description
安装后重启主机	<p>选中此复选框以在主机安装后重新启动。默认启用。</p> <div style="display: flex; align-items: flex-start;">  <div> <p>注意</p> <p>更改主机的内核命令行参数，或者更改集群的防火墙类型，还需要重新引导主机。</p> </div> </div>
SSH 公钥	<p>将文本框中的内容复制到主机上的 <code>/root/.ssh/authorized_hosts</code> 文件中，以使用 Manager 的 SSH 密钥，而不使用密码来与主机进行身份验证。</p>
自动配置主机防火墙	<p>在添加新主机时，管理器可在主机的防火墙上打开所需的端口。默认启用。这是一个 高级参数。</p>
SSH 指纹	<p>您可以 <code>fetch</code> 主机的 SSH 指纹，并将其与预期主机返回的指纹进行比较，确保它们匹配。这是一个 高级参数。</p>

2.5.6.2. 主机电源管理设置说明

Power Management 设置表包含新建主机或编辑主机窗口的电源管理选项卡上所需的信息。如果主机有一个受支持的电源管理卡，您可以配置电源管理卡。

表 2.21. 电源管理设置

字段名称	Description
启用电源管理	<p>启用主机上的电源管理。选中此复选框，以启用 Power Management 选项卡中的其余字段。</p>
kdump 集成	<p>在执行内核崩溃转储时防止主机隔离，以便崩溃转储不会中断。在 Red Hat Enterprise Linux 7.1 及更新的版本中，kdump 会被默认可用。如果主机上的 kdump 可用，但其配置无效(kdump 服务无法启动)，启用 Kdump 集成 会导致主机（重新）安装失败。如果在现有主机上启用或禁用 Kdump 集成，则必须 重新安装主机。</p>
禁用电源管理的策略控制	<p>电源管理由主机的集群的调度策略控制。如果启用了电源管理并且达到定义的低利用率值，则管理器将关闭主机机器，并在负载平衡需要或集群中没有足够的可用主机时再次重新启动。选择这个复选框以禁用策略控制。</p>

字段名称	Description
按不同顺序排列代理	<p>列出主机的隔离代理。隔离代理可以是连续的、并行或两者的组合。</p> <ul style="list-style-type: none"> ● 如果按顺序使用隔离代理，则将使用主代理来停止或启动主机，如果失败，则使用二级代理。 ● 如果同时使用隔离代理，则两个隔离代理都必须响应停止主机的 Stop 命令；如果一个代理响应 Start 命令，则主机将启动。 <p>默认情况下，隔离代理是连续的。使用 up 和 down 按钮更改使用隔离代理的顺序。</p> <p>要使两个隔离代理并发并发，请从其他隔离代理旁的 Concurrent with 下拉列表选择一个隔离代理。额外的隔离代理可以添加到并发隔离代理组中，方法是从附加隔离代理旁的 Concurrent with 下拉列表中选择组。</p>
添加隔离代理	<p>点击 + 按钮添加新隔离代理。这会打开 Edit fence agent 窗口。有关此窗口中字段的更多信息，请查看下表。</p>
电源管理代理首选项	<p>默认情况下，指定管理器将在与主机相同的集群中搜索隔离代理，如果没有找到隔离代理，管理器将在同一 dc（数据中心）中搜索。使用上下和下移按钮来更改使用这些资源的顺序。此字段位于 高级参数 下。</p>

下表包含 **Edit fence agent** 窗口中所需的信息。

表 2.22. 编辑隔离代理 设置

字段名称	Description
地址	访问主机的电源管理设备的地址。可解析的主机名或 IP 地址。
用户名	用于访问电源管理设备的用户帐户。您可以在该设备中设置用户，或使用默认用户。
密码	访问电源管理设备的用户的密码。

字段名称	Description
类型	<p>主机上的电源管理设备类型。选择以下任意一项：</p> <ul style="list-style-type: none"> ● APC - APC MasterSwitch 网络电源开关。不适用于 APC 5.x 电源开关设备。 ● apc_snmp - 与 APC 5.x 电源开关设备一起使用。 ● BladeCenter - IBM Bladecenter Remote Supervisor Adapter。 ● cisco_ucs - Cisco Unified Computing System。 ● drac5 - Dell Remote Access Controller for Dell computers。 ● drac7 - Dell Remote Access Controller for Dell computers。 ● eps - ePowerSwitch 8M+ 网络电源开关。 ● hpblade - HP BladeSystem。 ● ilo, ilo2, ilo3, ilo4 - HP Integrated Lights-Out。 ● ipmilan - Intelligent Platform Management Interface and Sun Integrated Lights Out Management devices。 ● RSA - IBM Remote Supervisor Adapter。 ● rsb - Fujitsu-Siemens RSB 管理界面。 ● WTI - WTI 网络电源交换机。 <p>有关电源管理设备的更多信息，请参阅 技术参考中的电源管理。</p>
端口	电源管理设备用来与主机通信的端口号。
插槽	用于识别电源管理设备的刀片数。
Service Profile	用于识别电源管理设备的刀片式服务配置文件名称。当设备类型为 cisco_ucs 时，此字段会出现而不是 Slot 。
选项	<p>电源管理设备特定选项。输入这些内容作为 'key=value'。有关可用选项，请参阅主机电源管理设备的文档。</p> <p>对于 Red Hat Enterprise Linux 7 主机，如果您使用 cisco_ucs 作为电源管理设备，您还需要将 ssl_insecure=1 附加到 Options 字段中。</p>

字段名称	Description
安全	选中此复选框，以允许电源管理设备安全地连接到主机。这可以通过 ssh、ssl 或其他验证协议完成，具体取决于电源管理代理。

2.5.6.3. SPM 优先级设置说明

SPM 设置表详述了新建主机或编辑主机窗口的 SPM 选项卡上所需的信息。

表 2.23. SPM 设置

字段名称	Description
SPM 优先级	定义主机将被授予存储池管理程序 (SPM) 角色的可能性。选项包括 Low, Normal, 和 High 优先级。低优先级意味着被分配 SPM 角色的主机的可能性较小，高优先级意味着会增加的可能性。默认设置为 Normal。

2.5.6.4. 主机控制台设置说明

Console 设置表详细说明了 New Host 或 Edit Host 窗口的 Console 选项卡上所需的信息。

表 2.24. 控制台设置

字段名称	Description
覆盖显示地址	选中此复选框来覆盖主机的显示地址。当主机由内部 IP 定义且位于 NAT 防火墙后面时，此功能很有用。当用户从内部网络外连接到虚拟机时，而不是返回运行虚拟机的主机的专用地址时，虚拟机会返回公共 IP 或 FQDN（在外部网络中解析到公共 IP）。
显示地址	此处指定的显示地址将用于此主机上运行的所有虚拟机。地址必须采用完全限定域名或 IP 的格式。
vGPU 放置	指定 vGPU 的首选放置： <ul style="list-style-type: none"> ● 整合：如果您想要在可用物理卡中运行更多 vGPU，则选择此选项。 ● 分隔：如果您更喜欢在单独的物理卡中运行每个 vGPU，则使用这个选项。

2.5.6.5. 网络供应商设置介绍

Network Provider 设置表详细介绍了 **New Host** 或 **Edit Host** 窗口的 **Network Provider** 选项卡所需的信息。

表 2.25. Network Provider 设置

字段名称	Description
外部网络提供程序	如果您添加了外部网络供应商，并且希望该主机的网络由外部网络供应商调配，请从列表中进行选择。

2.5.6.6. 内核设置说明

内核设置表详细介绍了 **New Host** 或 **Edit Host** 窗口中的内核选项卡上需要的信息。常见内核引导参数选项被列为复选框，以便您可以轻松选择它们。

对于更复杂的更改，请使用 **内核命令行** 旁边的免费文本条目字段添加到所需的任何其他参数中。如果更改任何内核命令行参数，则必须 [重新安装主机](#)。



重要

如果主机附加到 **Manager**，则必须将主机置于维护模式，然后才能进行更改。进行更改后，[重新安装主机](#) 以应用更改。

表 2.26. 内核 设置

字段名称	Description
hostdev Passthrough 和 SR-IOV	在内核中启用 IOMMU 标志，以便虚拟机可以使用主机设备，就像将其直接附加到虚拟机一样。主机硬件和固件还必须支持 IOMMU。硬件上必须启用虚拟化扩展和 IOMMU 扩展。请参阅 PCI 传递配置主机 。IBM POWER8 默认启用 IOMMU。
嵌套虚拟化	启用 vmx 或 svm 标志，以便虚拟机可在虚拟机中运行。这个选项是一个技术预览功能：它只用于评估目的。它不可用于生产环境。要使用这个设置，您必须在主机上安装 vdsms-hook-nestedvt hook。详情请参阅 启用所有虚拟机的嵌套虚拟化 和 为单独虚拟机启用嵌套虚拟化

字段名称	Description
不安全的中断	如果启用了 IOMMU，但 passthrough 会失败，因为硬件不支持中断重新映射，您可以考虑启用这个选项。请注意，只有在主机上的虚拟机被信任时，您应该只启用这个选项，但该选项可能会使主机公开到虚拟机的 MSI 攻击。这个选项仅用于在将未认证硬件用于评估时用作临时解决方案。
PCI 预分配	如果您的 SR-IOV NIC 无法因为内存问题而分配虚拟功能，请考虑启用这个选项。主机硬件和固件还必须支持 PCI 实际位置。这个选项仅用于在将未认证硬件用于评估时用作临时解决方案。
将 Nouveau 列入黑名单	阻止 nouveau 驱动程序。nouveau 是 NVIDIA GPU 的社区驱动程序，它与厂商附加的驱动程序冲突。当供应商驱动程序优先考虑时，nouveau 驱动程序应该会被阻止。
SMT Disabled	禁用 Simultaneous Multi Threading (SMT)。禁用 SMT 可缓解安全漏洞（如 L1TF 或 MDS）对系统的影响。
FIPS 模式	启用 FIPS 模式。详情请参阅 启用 FIPS 。
内核命令行	此字段允许您将更多内核参数附加到默认参数。



注意

如果内核引导参数灰显，则单击 **重置按钮**，且可以使用 **选项**。

2.5.6.7. 托管引擎设置说明

托管引擎设置表详细介绍了新建主机或编辑主机窗口的托管引擎选项卡所需的信息。

表 2.27. 托管引擎设置

字段名称	Description
------	-------------

字段名称	Description
选择托管引擎部署操作	<p>有三个选项可用：</p> <ul style="list-style-type: none"> ● none - 不需要操作。 ● deploy - 选择此选项以将主机部署为自托管引擎节点。 ● 取消部署 - 对于自托管引擎节点，您可以选择此选项来取消部署主机并移除与自托管引擎相关的配置。

2.5.7. 主机弹性

2.5.7.1. 主机高可用性

Red Hat Virtualization Manager 使用隔离来保持集群中的主机响应。不响应的主机 与非 操作主机不同。非 **Operational** 主机可由 **Manager** 进行通信，但具有不正确的配置，例如缺少逻辑网络。不响应的主机 不能与管理器通信。

隔离可让集群响应意外的主机故障，并强制进行节能、负载均衡和虚拟机可用性策略。您应该为主机的电源管理设备配置隔离参数，并从时间测试其正确性。在隔离操作中，重启后不响应的主机，如果主机没有在指定时间内返回活动状态，则仍然保持不响应的等待的手动干预和故障排除。



注意

要自动检查隔离参数，您可以配置 **PMHealthCheckEnabled**（默认为 **false**）和 **PMHealthCheckIntervallnSec**（默认为 **3600 sec**）**engine-config** 选项。

当设置为 **true** 时，**PackpmHealthCheckEnabled** 会按照 **PMHealthCheckIntervallnSec** 指定的时间间隔检查所有主机代理，并在检测到问题时引发警告。有关配置 **engine-config** 选项的更多信息，请参阅 **engine-config** 命令语法。

虚拟机管理器可通过 **Red Hat Virtualization Manager** 在代理主机、代理主机或管理门户中手动执行。在不响应的主机上运行的所有虚拟机均已停止，并且高可用性虚拟机在不同的主机上启动。电源管理操作至少需要两台主机。

管理器启动后，它会自动尝试隔离在静默时间（默认为 5 分钟）后启用了电源管理的不响应的主机。可以通过更新 **DisableFenceAtStartupInSec engine-config** 选项来配置静默时间。



注意

DisableFenceAtStartupInSec engine-config 选项有助于防止管理器在启动时试图隔离主机的场景。这在数据中心中断后发生，因为主机的引导过程通常比 Manager 引导过程长。

可以使用电源管理参数自动隔离主机主机，或者右键点主机并使用菜单上的选项来手动隔离。



重要

如果主机运行具有高可用性的虚拟机，则必须启用和配置电源管理。

2.5.7.2. Red Hat Virtualization 中的代理电源管理

Red Hat Virtualization Manager 不会直接与隔离代理通信。相反，经理使用代理向主机电源管理设备发送电源管理命令。管理器使用 VDSM 执行电源管理设备操作，因此环境中的另一台主机用作隔离代理。

您可以选择：

- 任何与需要隔离的主机相同的集群中的主机。
- 任何与需要隔离的主机在同一数据中心中的主机。

可行的隔离代理主机的状态为 **UP** 或 **Maintenance**。

2.5.7.3. 在主机上设置隔离参数

主机隔离的参数使用 **New Host** 或 **Edit Host** 窗口中的 **Power Management** 字段进行设置。电源管理系统能够使用其他接口（如远程访问卡(RAC)）隔离问题的主机。

所有电源管理操作都是使用代理主机完成的，而不是由 Red Hat Virtualization Manager 直接使用。电源管理操作至少需要两台主机。

流程

1. 单击 **Compute** → **Hosts**，再选择 **主机**。
2. 点 **Edit**。
3. 点 **Power Management** 选项卡。
4. 选中 **Enable Power Management** 复选框来启用字段。
5. 选择 **Kdump 集成** 复选框以防止在执行内核崩溃转储时隔离主机。

**重要**

如果在现有主机上启用或禁用 **Kdump 集成**，则必须[重新安装主机](#)。

6. (可选) 如果您不希望主机的电源管理由主机的集群的调度策略控制，请选择 **Disable policy control of of power management** 复选框。
7. 点击 **+** 按钮添加新的电源管理设备。这会打开 **Edit fence agent** 窗口。
8. 输入电源管理设备的地址、用户名和密码。
9. 从下拉列表中选择电源管理 设备类型。
10. 输入电源管理设备用来与主机通信的 **SSH** 端口号。
11. 输入 **Slot** 编号，用于识别电源管理设备的刀片式。
12. 输入电源管理设备的 **Options**。使用以逗号分隔的 **'key=value'** 条目列表。
- 13.

13. 选中 **Secure** 复选框，以启用电源管理设备安全地连接到主机。

14. 点击 **Test** 按钮，以确保设置正确。测试 **Succeeded**，在成功验证后，**Host Status** 为：时会显示。



警告

电源管理参数(**userid**、**password**、选项等)仅在设置期间和之后手动进行测试。如果您选择忽略有关不正确的参数的警报，或者在没有相应更改 **Red Hat Virtualization Manager** 的情况下在电源管理硬件上更改参数，那么在大多数需要时，隔离可能会失败。

15. 点击 **OK** 关闭 **Edit fence agent** 窗口。

16. 在电源管理选项卡中，选择展开高级参数，并使用"上移"按钮指定管理器将搜索主机的集群和 **dc**（数据中心）用于隔离代理的顺序。

17. 点击 **OK**。

您返回到主机列表。请注意，主机名旁边的感叹号现已消失，表示电源管理已经配置成功。

2.5.7.4. fence_kdump 高级配置

kdump

点主机的名称在详情视图中的 **General** 选项卡中查看 **kdump** 服务的状态：

- 启用: **kdump** 已被正确配置，**kdump** 服务正在运行。

- 禁用 : kdump 服务没有运行 (在这种情况下, kdump 集成无法正常工作)。
- 未知 : 只适用于之前 VDSM 版本的主机没有报告 kdump 状态。

有关安装和使用 kdump 的更多信息, 请参阅 [Red Hat Enterprise Linux 7 Kernel Crash Dump Guide](#)。

fence_kdump

在 New Host 或 Edit Host 窗口的 Power Management 选项卡中启用 Kdump 集成配置标准 fence_kdump 设置。如果环境的网络配置很简单, 且 Manager 的 FQDN 可以在所有主机上可解析, 则默认的 fence_kdump 设置就可以使用。

但是, 有些情况下, 需要高级配置 fence_kdump。更复杂的网络的环境可能需要手动更改 Manager、fence_kdump 侦听程序或两者的配置。例如, 如果 Manager 的 FQDN 无法在所有启用了 Kdump 集成的主机上解析, 您可以使用 engine-config 设置正确的主机名或 IP 地址 :

```
engine-config -s FenceKdumpDestinationAddress=A.B.C.D
```

以下示例用例中可能还需要配置更改 :

- 管理器有两个 NIC, 其中其中一个面向公众的, 第二个是 fence_kdump 消息的首选目的地。
- 您需要在不同的 IP 或端口上执行 fence_kdump 侦听器。
- 您需要为 fence_kdump 通知消息设置自定义间隔, 以防止可能的数据包丢失。

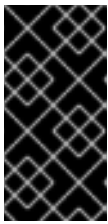
仅为高级用户推荐自定义的 fence_kdump 检测设置, 因为只有在更复杂的网络设置中才需要更改默认配置。

2.5.7.5. fence_kdump 侦听器配置

编辑 `fence_kdump` 侦听器的配置。这只在默认配置不够时才需要。

流程

1. 在 `/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/` 中创建一个新文件（例如 `my-fence-kdump.conf`）。
2. 使用语法 `OPTION=值` 输入您的自定义，并保存文件。



重要

编辑的值也需要在 `engine-config` 中改变，如在 [Manager](#) 中配置 `fence-kdump` 的 `fence_kdump Listener Configuration Options` 列表所述。

3. 重启 `fence_kdump` 侦听器：

```
# systemctl restart ovirt-fence-kdump-listener.service
```

如果需要，可以自定义以下选项：

表 2.28. `fence_kdump` Listener 配置选项

变量	Description	默认	备注
<code>LISTENER_ADDRESS</code>	定义要接收 <code>fence_kdump</code> 消息的 IP 地址。	0.0.0.0	如果更改了此参数的值，它必须与 <code>engine-config</code> 中的 <code>FenceKdumpDestinationAddress</code> 的值匹配。
<code>LISTENER_PORT</code>	定义要接收 <code>fence_kdump</code> 消息的端口。	7410	如果更改了此参数的值，它必须与 <code>engine-config</code> 中的 <code>FenceKdumpDestinationPort</code> 的值匹配。

变量	Description	默认	备注
HEARTBEAT_INTERVAL	定义监听器的心跳更新间隔（以秒为单位）。	30	如果更改了此参数的值，它的大小必须小于 engine-config 中的 FenceKdumpListenerTimeout 的值。
SESSION_SYNC_INTERVAL	定义将监听器的主机 kdump 会话同步到数据库的时间间隔（以秒为单位）。	5	如果更改了此参数的值，它的大小必须小于 engine-config 中的 KdumpStartedTimeout 的值。
REOPEN_DB_CONNECTION_INTERVAL	定义重新打开之前不可用的数据库连接的时间间隔（以秒为单位）。	30	-
KDUMP_FINISHED_TIMEOUT	定义主机 kdump 流标记为 FINISHED 的主机最后一次收到的消息后的最大超时时间（以秒为单位）。	60	如果更改了此参数的值，它的大小必须加倍于 engine-config 中的 FenceKdumpMessageInterval 的值。

2.5.7.6. 在 Manager 上配置 fence_kdump

编辑 Manager 的 kdump 配置。这只在默认配置不够时才需要。可使用以下方法找到当前的配置值：

```
# engine-config -g OPTION
```

流程

1. 使用 **engine-config** 命令编辑 kdump 的配置：

```
# engine-config -s OPTION=value
```



重要

还必须在 **fence_kdump** 侦听器配置文件中更改编辑的值，如 **Kdump Configuration Options** 表中所述。请参阅 [fence_kdump 侦听器配置](#)。

2. 重启 **ovirt-engine** 服务：

```
# systemctl restart ovirt-engine.service
```

3.

如果需要，重新安装启用了 **Kdump 集成** 的所有主机（请参阅下表）。

可使用 **engine-config** 配置以下选项：

表 2.29. kdump 配置选项

变量	Description	默认	备注
FenceKdumpDestinationAddress	定义要向发送 fence_kdump 消息的主机名或 IP 地址。如果为空，则使用 Manager 的 FQDN。	空字符串（使用 Manager FQDN）	如果更改了此参数的值，它必须与 fence_kdump 侦听器配置文件中的 LISTENER_ADDRESS 的值匹配，且所有启用了 Kdump 集成 的所有主机都需要被重新安装。
FenceKdumpDestinationPort	定义将 fence_kdump 消息发送到的端口。	7410	如果更改了此参数的值，它必须与 fence_kdump 侦听器配置文件中的 LISTENER_PORT 值匹配，并且必须重新安装启用了 Kdump 集成 的所有主机。
FenceKdumpMessageInterval	定义 fence_kdump 发送的消息之间的间隔（以秒为单位）。	5	如果更改了此参数的值，则必须小于 fence_kdump 侦听器配置文件中的 KDUMP_FINISHED_TIMEOUT 的值的一半，且必须重新安装启用了 Kdump 集成 的所有主机。
FenceKdumpListenerTimeout	定义最后心跳后的最大超时时间（以秒为单位），以考虑 fence_kdump 侦听器程序处于活动状态。	90	如果更改了此参数的值，它的大小必须加倍于 fence_kdump 侦听器配置文件中的 HEARTBEAT_INTERVAL 的值。

变量	Description	默认	备注
KdumpStartedTimeout	定义在收到 kdumping 主机的第一个信息（检测主机 kdump 流已启动）前等待的最大超时时间（以秒为单位）。	30	如果更改了此参数的值，它的大小必须是 fence_kdump 侦听器配置文件中的 SESSION_SYNC_INTERVAL 的值和 FenceKdumpMessageInterval 的两倍或更大。

2.5.7.7. 软隔离主机

由于意外问题，主机有时可能会变得不响应，但 VDSM 无法响应请求，但依赖于 VDSM 的虚拟机仍保持有效并可访问。在这些情况下，重新启动 VDSM 将返回到响应状态并解决这个问题。

"SSH Soft 隔离"是一个进程，管理器尝试在不响应的主机上通过 SSH 重新启动 VDSM。如果管理器无法通过 SSH 重新启动 VDSM，则隔离的责任将在配置了外部隔离代理时进入外部隔离代理。

通过 SSH 进行软隔离的工作方式如下：必须在主机上配置和启用隔离，并且数据中心必须存在有效的代理主机（第二个主机，处于 UP 状态）。当 Manager 和主机间的连接超时，会出现以下情况：

1. 在第一个网络失败时，主机的状态将变为"连接"。
2. 然后，管理器尝试询问 VDSM 以获得其状态，或者等待主机上负载确定的时间间隔。用于确定间隔长度的公式由配置值 `TimeoutToResetVdsInSeconds` 配置（默认为 60 秒）+ `[DelayResetPerVmInSeconds`（默认为 0.5 秒）]*（在主机上运行虚拟机的数量）+ `[DelayResetForSpmlnSeconds`（默认为 20 秒）]*（如果主机为 SPM）运行。为了给 VDSM 给予响应的最大时间，经理可选择上述两个选项的更长时间（三个尝试检索 VDSM 的状态或以上公式决定的间隔）。
3. 如果主机没有响应该间隔经过的，则 `vdsmd restart` 将通过 SSH 执行。
4. 如果 `vdsmd` 重启在主机和 Manager 之间重新建立连接时无法成功，则主机的状态会变为 `Non Responsive`，如果配置了电源管理，则隔离将移交给外部隔离代理。



注意

通过 **SSH** 进行软隔离可以在没有配置电源管理的主机上执行。这与“隔离”不同，只能在配置了电源管理的主机上执行。

2.5.7.8. 使用主机电源管理功能

为主机配置了电源管理后，您可以从管理门户界面访问多个选项。虽然每个电源管理设备都有自己的可定制选项，但它们都支持启动、停止和重新启动主机的基本选项。

流程

1.

单击 **Compute** → **Hosts**，再选择 **主机**。

2.

点 **Management** 下拉菜单并选择以下 **Power Management** 选项之一：



重新启动：此选项将停止主机并等待主机的状态更改为 **Down**。当代理确认主机已停机时，高可用性虚拟机会在集群中的另一主机上重新启动。然后代理重启这个主机。当主机准备好使用状态时，其状态显示为 **Up**。



启动：此选项启动主机，并允许它加入群集。当它准备就绪后，其状态显示为 **Up**。



停止：此选项关闭主机。在使用此选项前，请确保主机上运行的虚拟机已迁移到集群中的其他主机。否则，虚拟机将崩溃，并且只有高可用性虚拟机将在另一主机上重新启动。当主机停止后，其状态显示为 **Non-Operational**。



注意

如果没有启用 **Power Management**，您可以通过选择它来重启或停止主机，点 **Management** 下拉菜单，然后选择 **SSH Management** 选项、**Restart** 或 **Stop**。



重要

当主机上定义了两个隔离代理时，可以同步或按顺序使用它们。对于并行代理，两个代理都必须响应 **Stop** 命令，使主机被停止；当一个代理响应 **Start** 命令时，主机将启动。对于后续代理，要启动或停止主机，首先使用主代理；如果失败，则使用二级代理。

3.

点击 **OK**。

其他资源



[配置 ACPI 以用于集成的隔离设备](#)

2.5.7.9. 手动隔离或隔离不响应的主机

如果主机无法预测到不响应状态，例如因为硬件故障，这可能会显著影响环境的性能。如果您没有电源管理设备，或者配置不正确，则可以手动重启主机。



警告

不要选择 **Confirm 'Host been Rebooted'**，除非您已手动重启主机。在主机仍然运行时使用这个选项可能会导致虚拟机镜像崩溃。

流程


1.

在管理门户中，单击 **Compute** → **Hosts**，并确认主机的状态为 **Nonsponsive**。

2.

手动重启主机。这可能意味着，物理输入实验并重启主机。

3.

在管理门户中，选择主机并点 **More Actions** (
)，然后点 **Confirm 'Host is Rebooted'**。

4. 选择 **Approve Operation** 复选框，再单击 **OK**。
5. 如果您的主机需要非常长的时间引导，您可以设置 **ServerRebootTimeout** 来指定在等待了多少秒之后将主机看做为 **Non Responsive**：

```
# engine-config --set ServerRebootTimeout=integer
```

2.6. 存储

2.6.1. 关于 Red Hat Virtualization 存储

Red Hat Virtualization 将集中式存储系统用于虚拟磁盘、ISO 文件和快照。可使用以下方法实现存储网络：

- 网络文件系统 (NFS)
- 其他 POSIX 兼容文件系统
- Internet Small Computer System Interface (iSCSI)
- 直接连接到虚拟化主机的本地存储
- 光纤通道协议 (FCP)
- 并行 NFS (pNFS)

设置存储是新数据中心的先决条件，因为除非附加并激活存储域，否则无法初始化数据中心。

作为 Red Hat Virtualization 系统管理员，您可以为虚拟化企业创建、配置、附加和维护存储。您必须熟悉存储类型及其使用。请阅读您的存储阵列指南，并查看 [Red Hat Enterprise Linux 管理存储设备](#) 以了解有关概念、协议、要求和常规存储使用的更多信息。

要添加存储域，您必须能够成功访问管理门户，且至少有一个主机已连接状态为 Up。

Red Hat Virtualization 有三种存储域类型：

- **数据域：** 一个数据域在数据中心中保存所有虚拟机和模板的虚拟硬盘和 OVF 文件。另外，虚拟机的快照也存储在数据域中。

数据域无法在数据中心之间共享。可向同一数据中心添加多个类型的数据域(iSCSI、NFS、FC、POSIX 和 Gluster)，它们都是共享的，而不是本地域。

您必须将数据域附加到数据中心，然后才能将其他类型的域附加到数据中心。

- **ISO 域：** ISO 域存储用于为虚拟机安装和引导操作系统和应用程序的 ISO 文件（或逻辑 CD）。ISO 域删除数据中心对物理介质的需求。ISO 域可以在不同的数据中心之间共享。ISO 域只能基于 NFS。只能将一个 ISO 域添加到数据中心。

- **导出域：** 导出域是用于在数据中心和 Red Hat Virtualization 环境之间复制和移动镜像的临时存储存储库。导出域可用于备份虚拟机。导出域可以在数据中心之间移动，但一次只能在一个数据中心内处于活动状态。导出域只能基于 NFS。只能将一个导出域添加到数据中心。



注意

导出存储域已弃用。存储数据域可以从数据中心取消附加，并导入到同一环境中或不同环境中的其他数据中心。然后，可以将虚拟机、浮动虚拟磁盘和模板从导入的存储域上传到所连接的数据中心。有关 [导入存储域的信息](#)，请参阅导入现有存储域。



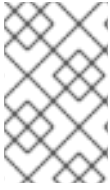
重要

您确定数据中心的存储需求后，只在为 Red Hat Virtualization 环境配置并附加存储。

2.6.2. 了解存储域

存储域是一组具有通用存储接口的镜像集合。存储域包含模板和虚拟机（包括快照）或 ISO 文件的完整映像。存储域可以由块设备(SAN - iSCSI 或 FCP)或文件系统(NAS - NFS、GlusterFS 或其他 POSIX 兼容文件系统)组成。

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



注意

GlusterFS 存储已弃用，并将在以后的发行版本中删除。

在 NFS 上，所有虚拟磁盘、模板和快照都是文件。

在 SAN (iSCSI/FCP)上，每个虚拟磁盘、模板或快照都是逻辑卷。块设备聚合到名为卷组的逻辑实体中，然后由 LVM（逻辑卷管理器）划分为逻辑卷，用作虚拟硬盘。有关 LVM 的详情，请参阅 [Red Hat Enterprise Linux 配置和管理逻辑卷](#)。

虚拟磁盘可以采用两种格式之一，即 QCOW2 或 raw。存储的类型可以是稀疏或预分配。快照始终是稀疏的，但可以为任何格式的磁盘获取快照。

共享相同存储域的虚拟机可以在属于同一集群的主机之间迁移。

2.6.3. 准备和添加 NFS 存储

2.6.3.1. 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。

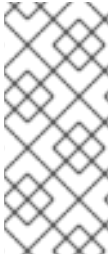
```
# vi /etc/exports  
# cat /etc/exports  
/storage *(rw)
```

5. 重启以下服务：

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

- 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。

2.6.3.2. 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

- 在管理门户中，点 **Storage** → **Domains**。
- 点 **New Domain**。
- 输入存储域的名称。
- 接受 **Data Center**, **Domain Function**, **Storage Type**, **Format**, 和 **Host** 列表的默认值。
- 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 **OK**。

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。

2.6.3.3. 增加 NFS 存储

要增加 NFS 存储量，您可以创建新的存储域并将其添加到现有数据中心，或者增加 NFS 服务器上的可用空间。有关前者选项，请参阅添加 [NFS 存储](#)。下面的步骤解释了如何增加现有 NFS 服务器中的可用空间。

流程

1. 点 **Storage → Domains**。
2. 点 **NFS 存储域的名称**。这会打开详情视图。
3. 单击 **数据中心** 选项卡，然后单击 **维护**，以将存储域置于维护模式。这会卸载现有的共享，并使它能够调整存储域的大小。
4. 在 **NFS 服务器** 中，重新定义存储大小。有关 Red Hat Enterprise Linux 6 系统，请查看

[Red Hat Enterprise Linux 6 存储管理指南](#)。有关 Red Hat Enterprise Linux 7 系统，请查看 [Red Hat Enterprise Linux 7 存储管理指南](#)。对于 Red Hat Enterprise Linux 8 系统，请参阅 [调整分区](#)。

5.

在详情视图中，单击 **Data Center** 选项卡，然后单击 **Activate** 以挂载存储域。

2.6.4. 准备和添加本地存储

使用虚拟机主机上物理安装的存储设备的虚拟机磁盘称为本地存储设备。

存储设备必须是存储域的一部分。本地存储的存储域类型称为本地存储域。

配置主机来自动使用本地存储，并将主机添加到新本地存储域、新的本地存储域、数据中心和集群，从而无法添加其他主机。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。

2.6.4.1. 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** 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 `vdsm` 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
```

2.6.4.2. 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、本地群集和本地存储域中。

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 OK。

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。

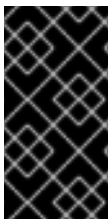
2.6.5. 准备和添加兼容 POSIX 的文件系统存储

2.6.5.1. 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。

2.6.5.2. 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 OK。**

2.6.6. 准备和添加块存储

2.6.6.1. 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。



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：

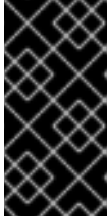
```
# cat /etc/multipath/conf.d/host.conf
multipaths {
  multipath {
    wwid boot_LUN_wwid
    no_path_retry queue
  }
}
```

2.6.6.2. 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 **OK**。

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](#)。

2.6.6.3. 配置 iSCSI 多路径

iSCSI 多路径可让您创建和管理逻辑网络和 iSCSI 存储连接组。主机和 iSCSI 存储之间的多个网络路径可防止主机故障出现。

管理器使用分配给 iSCSI 绑定中逻辑网络的 NIC 或 VLAN 将集群中的每个主机连接到每个目标。

您可以使用多个目标和逻辑网络创建 iSCSI 绑定以实现冗余。

前提条件

- 一个或多个 [iSCSI 目标](#)
- 一个或多个满足以下要求的 [逻辑网络](#)：
 - 未定义为 [Required](#) 或 [VM Network](#)

- **分配给主机接口**
- 在相同的 VLAN 和子网络中**分配一个静态 IP 地址**，如 iSCSI 绑定中的其他裸机网络



注意

自托管引擎部署不支持多路径。

流程

1. 单击 **Compute** → **Data Centers**。
2. 点数据中心名称。这会打开详情视图。
3. 在 **iSCSI 多路径** 选项卡中，点 **Add**。
4. 在 **Add iSCSI Bond** 窗口中，输入名称和描述。
5. 从逻辑网络选择 **逻辑网络**，再从 **Storage Targets** 中选择存储域。您必须选择到同一目标的所有路径。
6. 单击 **OK**。

数据中心中的主机通过 iSCSI 绑定中的逻辑网络连接到 iSCSI 目标。

2.6.6.4. 将逻辑网络迁移到 iSCSI 绑定

如果您的逻辑网络是为 iSCSI 流量创建并在现有 **网络绑定** 之上配置的逻辑网络，您可以在不中断或停机的情况下将其迁移到同一子网上的 iSCSI 绑定。

流程

1.
修改当前的逻辑网络，使其不是必需的：
 - a.
单击 **Compute** → **Clusters**。
 - b.
点集群名称。这会打开详情视图。
 - c.
在 **Logical Networks** 选项卡中，选择当前的逻辑网络(net-1)，再点 **Manage Networks**。
 - d.
清除 **Require** 复选框，然后单击 **OK**。

2.
创建一个不是 **Required** 和 **VM network** 的新的逻辑网络：
 - a.
点 **Add Network**。此时将打开 **New Logical Network** 窗口。
 - b.
在 **General** 选项卡中，输入名称 (net-2) 并清除 **VM network** 复选框。
 - c.
在 **Cluster** 选项卡中，清除 **Require** 复选框，然后点 **OK**。

3.
删除当前的网络绑定并重新分配逻辑网络：
 - a.
单击 **Compute** → **Hosts**。
 - b.
点主机名。这会打开详情视图。
 - c.
在 **Network Interfaces** 选项卡中，单击 **Setup Host Networks**。
 - d.
将 net-1 拖到右侧，以取消分配它。

- e. 将当前绑定拖到右侧以移除它。
 - f. 将 net-1 和 net-2 拖到左侧，将它们分配到物理接口。
 - g. 单击 net-2 的铅笔图标。此时将打开 Edit Network 窗口。
 - h. 在 IPV4 选项卡中，选择 Static。
 - i. 输入子网的 IP 和 Netmask/Routing Prefix，点 OK。
4. 创建 iSCSI 绑定：
- a. 单击 Compute → Data Centers。
 - b. 点数据中心名称。这会打开详情视图。
 - c. 在 iSCSI 多路径 选项卡中，点 Add。
 - d. 在 Add iSCSI Bond 窗口中，输入 Name，选择网络、net-1 和 net-2，然后点确定。

您的数据中心有一个 iSCSI 绑定，其中包含旧的和新的逻辑网络。

2.6.6.5. 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。

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
  }
}
```

2.6.6.6. 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 **OK**。

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。

2.6.6.7. 增加 iSCSI 或 FCP 存储

提高 iSCSI 或 FCP 存储大小有几种方法：

- 将现有 LUN 添加到当前存储域中。
- 使用新 LUN 创建新存储域并将其添加到现有数据中心。请参阅添加 [iSCSI 存储](#)。
- 通过重新定义底层 LUN 的大小扩展存储域。

有关配置或重新定义 FCP 存储大小的详情，请参考为 [Red Hat Enterprise Linux 8 管理存储设备](#) 中的 [使用光纤通道设备](#)。

以下流程解释了如何通过向现有存储域添加新的 LUN 来扩展存储区域网络 (SAN) 存储。

前提条件

- 存储域的状态必须是 **UP**。
- LUN 必须可以被状态为 **UP** 的所有主机访问，否则操作将失败，并且 LUN 不会添加到域中。但是，主机本身不会受到影响。如果新添加的主机或结束维护的主机或处于一个处于 **Non**

Operational 状态的主机无法访问 LUN，则主机的状态将变为 **Non Operational**。

增加现有 iSCSI 或 FCP 存储域

1. 点 **Storage** → **Domains** 并选择 **iSCSI** 或 **FCP** 域。
2. 单击 **Manage Domain**。
3. 点 **Targets** → **LUNs**，点 **Discover Targets** 展开按钮。
4. 输入存储服务器的连接信息，然后点 **Discover** 以启动连接。
5. 点 **LUNs** → **Targets**，选择新可用 LUN 的复选框。
6. 点 **OK**，将 LUN 添加到所选存储域。

这将根据添加的 LUN 的大小增加存储域。

当调整底层 LUN 来扩展存储域时，还必须在管理门户中刷新 LUN。

刷新 LUN 大小

1. 点 **Storage** → **Domains** 并选择 **iSCSI** 或 **FCP** 域。
2. 单击 **Manage Domain**。
3. 点 **LUNs** → **Targets**。

4. 在 **Additional Size** 列中，点 LUN 的 **Add Additional_Storage_Size** 按钮进行刷新。
5. 点 **OK** 刷新 LUN 以指示新的存储大小。

2.6.6.8. 重新使用 LUN

LUN 无法重复使用，因为 可以创建存储域或虚拟磁盘。如果您尝试重复使用 LUN，管理门户会显示以下出错信息：

```
Physical device initialization failed. Please check that the device is empty and accessible by the host.
```

自托管引擎在安装过程中显示以下错误：

```
[ ERROR ] Error creating Volume Group: Failed to initialize physical device: ("
[u'/dev/mapper/00000000000000000000000000000000']")
[ ERROR ] Failed to execute stage 'Misc configuration': Failed to initialize physical device: ("
[u'/dev/mapper/00000000000000000000000000000000']")
```

在 LUN 可以重复使用前，必须清除旧的分区表。



流程

您必须在正确的 LUN 上运行此步骤，以便不会意外破坏数据。

1. 删除 `< LUN_ID >` 中的分区映射：


```
kpartx -dv /dev/mapper/<LUN_ID>
```
2. 在 `< LUN_ID >` 中擦除 `filesystem` 或 `raid` 签名：


```
wipefs -a /dev/mapper/<LUN_ID>
```
3. 告知操作系统，关于 `< LUN_ID >` 上的分区表更改：

partprobe

2.6.6.9. 删除过时的 LUN

当删除存储域时，已过时的 LUN 链接可能会保留在存储服务器上。这可能导致多路径扫描速度、分散日志文件和 LUN ID 冲突。

Red Hat Virtualization 不会管理 iSCSI 服务器，因此当删除存储域时无法自动删除 LUN。管理员可以使用 `remove_stale_lun.yml` Ansible 角色手动删除过时的 LUN 链接。此角色从属于给定数据中心的所有主机中删除过时的 LUN 链接。有关此角色及其变量的更多信息，请参阅 [oVirt Ansible 集中的 Remove Stale LUN 角色](#)。



注意

假设您在从引擎机器中运行 `remove_stale_lun.yml`，因为所有主机上已经添加 `engine ssh` 密钥。如果 `playbook` 没有在引擎计算机上运行，则必须将用户的 SSH 密钥添加到属于数据中心的所有主机中，或者用户必须提供适当的清单文件。

流程

1. 点 **Storage** → **Domains**。
2. 点存储域的名称。这会打开详情视图。
3. 点 **Data Center** 选项卡。
4. 单击 **Maintenance**，然后单击 **OK**。
5. 单击 **Detach**，然后单击 **确定**。
6. 单击 **Remove**。
7. 点 **OK** 以将存储域从源环境中删除。

8. 从存储服务器中删除 LUN。
9. 使用 Ansible 从主机中删除过时的 LUN :

```
# ansible-playbook --extra-vars "lun=<LUN>"
/usr/share/ansible/collections/ansible_collections/ovirt/ovirt/roles/remove_stale_lun/examples/remove_stale_lun.yml
```

在上述步骤中，LUN 是从存储服务器中删除的 LUN。



注意

如果您使用 Ansible 从主机中删除过时的 LUN，而无需首先从存储服务器删除 LUN，则当 VDSM 执行 iSCSI 重新扫描时，已过时的 LUN 将重新显示主机上。

2.6.6.10. 创建 LVM 过滤器

LVM 过滤器是一个可以在 `/etc/lvm/lvm.conf` 中设置的功能，可接受基于 regex 查询的卷列表中的设备或拒绝设备。例如，要忽略 `/dev/cdrom`，您可以使用 `filter=["r!^/dev/cdrom$"]`，或将以下参数添加到 `lvm` 命令中：`lvs --config 'devices{filter=["r|cdrom"]}'`。

这为防止主机扫描和激活主机不需要的逻辑卷提供了简单的方法。特别是，解决方案解决了 RHV 管理的共享存储上的逻辑卷，以及由 RHV 原始卷中的客户机创建的逻辑卷。需要这个解决方案，因为扫描和激活其他逻辑卷可能会导致数据崩溃、缓慢引导或其他问题。

解决方案是在每台主机上配置 LVM 过滤器，它允许主机上的 LVM 仅扫描主机所需的逻辑卷。

您可以使用命令 `vdsm-tool config-lvm-filter` 分析当前的 LVM 配置，并决定是否需要配置过滤器。

如果尚未配置 LVM 过滤器，该命令会为主机生成 LVM 过滤选项，并在 LVM 配置中添加选项。

场景 1：未配置的主机

在还没有配置的主机上，当用户确认操作后，命令会自动配置 LVM：

```
# vdsm-tool config-lvm-filter
```

```
Analyzing host...
```

```
Found these mounted logical volumes on this host:
```

```
logical volume: /dev/mapper/vg0-lv_home
```

```
mountpoint:    /home
```

```
devices:       /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_root
```

```
mountpoint:    /
```

```
devices:       /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_swap
```

```
mountpoint:    [SWAP]
```

```
devices:       /dev/vda2
```

```
This is the recommended LVM filter for this host:
```

```
filter = [ "a|^/dev/vda2$", "r|.*)" ]
```

This filter will allow LVM to access the local devices used by the hypervisor, but not shared storage owned by VDSM. If you add a new device to the volume group, you will need to edit the filter manually.

```
Configure LVM filter? [yes,NO] ? [NO/yes] yes
```

```
Configuration completed successfully!
```

```
Please reboot to verify the LVM configuration.
```

场景 2：配置的主机

如果已经配置主机，命令只告知用户已经配置 LVM 过滤器：

```
# vdsm-tool config-lvm-filter
```

```
Analyzing host...
```

```
LVM filter is already configured for Vdsm
```

场景 3：需要手动配置

如果主机配置与 VDSM 所需的配置不匹配，则需要手动配置 LVM 过滤器：

```
# vdsm-tool config-lvm-filter
```

Analyzing host...

Found these mounted logical volumes on this host:

```
logical volume: /dev/mapper/vg0-lv_home
mountpoint:    /home
devices:      /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_root
mountpoint:    /
devices:      /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_swap
mountpoint:    [SWAP]
devices:      /dev/vda2
```

This is the recommended LVM filter for this host:

```
filter = [ "a|^/dev/vda2$|", "r|.*)" ]
```

This filter will allow LVM to access the local devices used by the hypervisor, but not shared storage owned by VDSM. If you add a new device to the volume group, you will need to edit the filter manually.

This is the current LVM filter:

```
filter = [ "a|^/dev/vda2$|", "a|^/dev/vdb1$|", "r|.*)" ]
```

WARNING: The current LVM filter does not match the recommended filter, Vdsm cannot configure the filter automatically.

Please edit `/etc/lvm/lvm.conf` and set the 'filter' option in the 'devices' section to the recommended value.

It is recommended to reboot after changing LVM filter.

2.6.7. 准备和添加红帽 Gluster 存储

2.6.7.1. 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](#)。

2.6.7.2. 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](#)。

2.6.8. 导入现有存储域

2.6.8.1. 导入现有存储域概述

除了添加新的存储域（不包含数据）外, 您还可以导入现有存储域并访问其包含的数据。通过导入存储域, 您可以在 Manager 数据库中故障时恢复数据, 并将数据从一个数据中心或环境迁移到另一个数据中心。

以下是导入每个存储域类型的概述：

Data

通过导入现有数据存储域, 您可以访问数据存储域包含的所有虚拟机和模板。导入存储域后, 您必须手动将虚拟机、浮动磁盘镜像和模板导入目标数据中心。导入数据存储域包含的虚拟机和模板的过程与导出存储域类似的过程。但是, 因为数据存储域包含给定数据中心中的所有虚拟机和模板, 因此建议在数据中心或环境之间进行虚拟机恢复或大规模迁移虚拟机。



重要

您可以导入附加到数据中心的现有数据存储域, 并具有正确的支持的兼容性级别。如需更多信息, 请参阅[从较旧的 RHV 版本导入存储域和虚拟机的相关支持性和限制](#)。

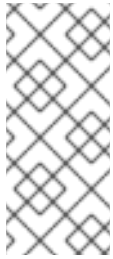
ISO

导入现有的 ISO 存储域可让您访问 ISO 存储域包含的所有 ISO 文件和虚拟磁盘组。导入存储域才能访问这些资源后不需要额外的操作；您可以根据需要将它们附加到虚拟机。

Export

通过导入现有的导出存储域, 您可以访问导出存储域包含的所有虚拟机映像和模板。因为导出域是为导出和导入虚拟机映像和模板而设计的, 建议在环境或环境之间迁移少量虚拟机和模板的方法。

有关在导出存储域中导出和导入虚拟机和模板的信息，请参阅[虚拟机管理指南](#)中的[导出和导入虚拟机和模板](#)。



注意

导出存储域已弃用。存储数据域可以从数据中心取消附加，并导入到同一环境中或不同环境中的其他数据中心。然后，可以将虚拟机、浮动虚拟磁盘和模板从导入的存储域上传到所连接的数据中心。



警告

将存储域附加到目标 Data-Center 时，它可能会升级到较新的存储域格式，且可能无法重新连接到源 Data-Center。这会破坏使用 Data-Domain 作为导出域的替代。

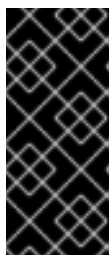
2.6.8.2. 导入存储域

导入之前附加到同一环境或不同环境中的数据中心的存储域。此流程假设存储域不再附加到任何环境中的任何数据中心，以避免数据崩溃。要导入并附加现有数据存储域到数据中心，必须初始化目标数据中心。

流程

1. 点 **Storage** → **Domains**。
2. 单击 **Import Domain**。
3. 选择您要导入存储域的数据中心。
4. 输入存储域的名称。
5. 从下拉列表中选择 **Domain Function** 和 **Storage Type**。

6. 从主机下拉列表中选择主机。

**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. 输入存储域的详细信息。

**注意**

根据您在 Domain Function 和 Storage Type 列表中选择值，用于指定存储域详情的字段。这些字段与可用于添加新的存储域的用户相同。

8. 在将存储域附加到所选数据中心后，选择 **Activate Domain in Data Center** 复选框，以激活该存储域。
9. 点击 **OK**。

现在，您可以将虚拟机和模板从存储域导入到数据中心。

**警告**

将存储域附加到目标 Data-Center 时，它可能会升级到较新的存储域格式，且可能无法重新连接到源 Data-Center。这会破坏使用 Data-Domain 作为导出域的替代。

相关信息

[从数据域中导入虚拟机](#)

从导入的 Data Storage Domains 导入模板

2.6.8.3. 在 Same 环境中数据中心之间迁移存储域

将存储域从一个数据中心迁移到同一 Red Hat Virtualization 环境中的另一个数据中心，以允许目标数据中心访问存储域中包含的数据。这个过程涉及将存储域从一个数据中心分离，并将其附加到不同的数据中心。



警告

将数据存储域迁移到具有比原始数据中心更高的兼容性等级的数据中心升级存储域的存储格式版本。

如果由于任何原因（如将虚拟机迁移到新数据中心）将存储域重新移至原始数据中心，请注意更高版本可防止将数据存储域重新连接到原始数据中心。

管理门户提示您确认您想要更新存储域格式，例如从 V3 更新至 V5。它还警告，您将无法将其重新附加到具有较低数据中心级别的旧数据中心。

要临时解决这个问题，您可以创建一个与源数据中心相同的兼容版本的目标数据中心。当您不再需要维护较低兼容性版本时，可以提高目标数据中心的兼容性版本。

详情请参阅 [从较旧的 RHV 版本导入存储域和虚拟机的相关支持性和限制](#)。

流程

1. 关闭在所需存储域上运行的所有虚拟机。
2. 点 **Storage** → **Domains**。
3. 点存储域的名称。这会打开详情视图。

4. 点 **Data Center** 选项卡。
5. 单击 **Maintenance**，然后单击 **OK**。
6. 单击 **Detach**，然后单击确定。
7. 点 **Attach**。
8. 选择目标数据中心，然后单击确定。

存储域连接到目标数据中心，并自动激活。现在，您可以将虚拟机和模板从存储域导入到目标数据中心。

2.6.8.4. 在不同环境中在数据中心间迁移存储域

将存储域从一个 Red Hat Virtualization 环境迁移到另一个环境，以允许目标环境访问存储域中包含的数据。这个过程涉及从一个 Red Hat Virtualization 环境中删除存储域，并将其导入到不同的环境中。要将现有数据存储域导入并附加到 Red Hat Virtualization 数据中心，存储域的源数据中心必须具有正确的兼容性级别。



警告

将数据存储域迁移到具有比原始数据中心更高的兼容性等级的数据中心升级存储域的存储格式版本。

如果由于任何原因（如将虚拟机迁移到新数据中心）将存储域重新移至原始数据中心，请注意更高版本可防止将数据存储域重新连接到原始数据中心。

管理门户提示您确认您想要更新存储域格式，例如从 V3 更新至 V5。它还警告，您将无法将其重新附加到具有较低数据中心级别的旧数据中心。

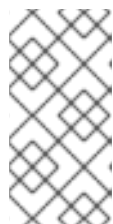
要临时解决这个问题，您可以创建一个与源数据中心相同的兼容版本的目标数据中心。当您不再需要维护较低兼容性版本时，可以提高目标数据中心的兼容性版本。

详情请参阅 [从较旧的 RHV 版本导入存储域和虚拟机的相关支持性和限制](#)。

流程

1. 登录源环境的管理门户。
2. 关闭在所需存储域上运行的所有虚拟机。
3. 点 **Storage** → **Domains**。
4. 点存储域的名称。这会打开详情视图。
5. 点 **Data Center** 选项卡。
6. 单击 **Maintenance**，然后单击 **OK**。
7. 单击 **Detach**，然后单击确定。
8. 单击 **Remove**。
9. 在 **Remove Storage (s)** 窗口中，确保 **Format Domain, i.e. Storage Content will be lost!** 复选框没有被选择。此步骤在存储域中保留数据，以备以后使用。
10. 点 **OK** 以将存储域从源环境中删除。
11. 登录目标环境的管理门户。

12. 点 **Storage** → **Domains**。
13. 单击 **Import Domain**。
14. 从 **Data Center** 下拉列表中选择目标数据中心。
15. 输入存储域的名称。
16. 从适当的下拉列表中，选择 **Domain Function** 和 **Storage Type**。
17. 从主机下拉列表选择一个主机。
18. 输入存储域的详细信息。

**注意**

根据您在 **Storage Type** 下拉列表中选择的值，用于指定存储域详情的字段。这些字段与可用于添加新的存储域的用户相同。

19. 选择 **Activate Domain in Data Center** 复选框，以在连接该存储域时自动激活。
20. 单击 **OK**。

存储域连接到新 **Red Hat Virtualization** 环境中的目标数据中心，并自动激活。现在，您可以将虚拟机和模板从导入存储域导入到目标数据中心。

**警告**

将存储域附加到目标 Data-Center 时，它可能会升级到较新的存储域格式，且可能无法重新连接到源 Data-Center。这会破坏使用 Data-Domain 作为导出域的替代。

2.6.8.5. 从导入的 Data Storage Domains 导入模板

从您导入 Red Hat Virtualization 环境中的数据存储域中导入模板。此流程假设导入的数据存储域已附加到数据中心，并已激活。

流程

1. 点 **Storage** → **Domains**。
2. 单击导入的存储域的名称。这会打开详情视图。
3. 点 **Template Import** 选项卡。
4. 选择要导入的一个或多个模板。
5. 点 **Import**。
6. 对于 **Import Templates (s)** 窗口中的每个模板，请确保 **Cluster** 列表中选择了正确的目标集群。
7. 将外部虚拟机 vNIC 配置集映射到目标集群中存在的配置集：
 - a. 点击 **vNic Profiles Mapping**。

- b. 从 **Target vNic Profile** 下拉列表中选择要使用的 **vNIC 配置集**。
 - c. 如果在 **Import Templates** 窗口中选择了多个目标集群，请在 **Target Cluster** 下拉列表中选择每个目标集群，并确保映射正确。
 - d. 点击 **OK**。
8. 点击 **OK**。

导入的模板将不再显示在模板导入选项卡下的列表中。

2.6.9. 存储任务

2.6.9.1. 将镜像上传到数据存储域

您可以将虚拟磁盘镜像和 ISO 镜像上传到管理门户中的数据存储域，或使用 REST API 上传。



注意

要使用 REST API 上传镜像，请参阅 *REST API 指南* 中的 [IMAGETRANSFERS](#) 和 [IMAGETRANSFER](#)。

兼容 QEMU 的虚拟磁盘可以附加到虚拟机。虚拟磁盘类型必须是 QCOW2 或 raw。从 QCOW2 虚拟磁盘创建的磁盘无法共享，QCOW2 虚拟磁盘文件不得具有备份文件。

ISO 映像可以作为 CDROM 连接到虚拟机或用于启动虚拟机。

前提条件

上传功能使用 HTML 5 API，这需要您的环境包含以下内容：

- 证书颁发机构（导入到用于访问管理门户的网页浏览器中）。

要导入证书颁发机构，访问 https://engine_address/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA 并启用所有信任设置。请参阅有关在 [Firefox](#)、[Internet Explorer](#) 或 [Google Chrome](#) 中安装证书颁发机构的说明。

- 支持 HTML 5 的浏览器，如 Firefox 35、Internet Explorer 10、Chrome 13 或更高版本。

流程

1. 点 **Storage** → **Disks**。
2. 从 **Upload** 菜单中选择 **Start**。
3. 单击 **Choose File**，再选择要上传的镜像。
4. 填写 **Disk Options** 字段。有关 [相关字段的描述](#)，请参阅 [New Virtual Disk Window](#) 中的 [Settings](#) 的说明。
5. 单击 **OK**。

进度条显示上传的状态。您可以从 **Upload** 菜单中暂停、取消或恢复上传。

提示

如果上传超时并显示消息的 **Reason: timeout**，因为要传输不活跃，请增加超时值并重启 **ovirt-engine** 服务：

```
# engine-config -s TransferImageClientInactivityTimeoutInSeconds=6000
# systemctl restart ovirt-engine
```

2.6.9.2. 将 VirtIO 镜像文件上传到存储域

virtio-win_version.iso 镜像包含以下用于 Windows 虚拟机以提高性能和可用性：

- **virtio** 驱动程序

- 客户机代理的安装程序
- 驱动程序的安装程序

要安装并上传 `virtio-win_version.iso` 的最新版本：

1. 在 Manager 机器上安装镜像文件：

```
# dnf -y install virtio-win
```

在 Manager 机器上安装后，镜像文件为 `/usr/share/virtio-win/virtio-win_version.iso`

2. 将镜像文件上传到在安装过程中没有在本地创建的数据存储域中。如需更多信息，请参阅管理指南中的[将镜像上传到数据存储域](#)。
3. 将镜像文件附加到虚拟机。

虚拟机现在可以使用 `virtio` 驱动程序和代理。

有关将镜像文件附加到虚拟机的详情，请参考[虚拟机管理指南](#)中的[在 Windows 上安装客户机代理、工具和驱动程序](#)。

2.6.9.3. 将镜像上传到 ISO 域



注意

ISO 域是已弃用的存储域类型。Red Hat Virtualization 4.4 中删除了 ISO Uploader 工具 `ovirt-iso-uploader`。您应该使用管理门户或使用 REST API 将 ISO 镜像上传到数据域。详情请参阅[将镜像上传到数据存储域](#)。

虽然 ISO 域已弃用，但此处仍提供此信息以便您需要使用 ISO 域。

要将 ISO 镜像上传到 ISO 存储域，以便从 Manager 内部提供它，请按照以下步骤操作。

流程

1. 以 root 身份登录属于您的 ISO 存储域所在的数据中心的主机。

2. 获取 /rhev/data-center 的目录树：

```
# tree /rhev/data-center
.
|-- 80dfacc7-52dd-4d75-ab82-4f9b8423dc8b
| |-- 76d1ecba-b61d-45a4-8eb5-89ab710a6275 → /rhev/data-
center/mnt/10.10.10.10:_rhevnfssd/76d1ecba-b61d-45a4-8eb5-89ab710a6275
| |-- b835cd1c-111c-468d-ba70-fec5346af227 → /rhev/data-
center/mnt/10.10.10.10:_rhevisosd/b835cd1c-111c-468d-ba70-fec5346af227
| |-- mastersd → 76d1ecba-b61d-45a4-8eb5-89ab710a6275
| |-- tasks → mastersd/master/tasks
| `-- vms → mastersd/master/vms
|-- hsm-tasks
`-- mnt
    |-- 10.10.10.10:_rhevisosd
    | |-- b835cd1c-111c-468d-ba70-fec5346af227
    | | |-- dom_md
    | | | |-- ids
    | | | |-- inbox
    | | | |-- leases
    | | | |-- metadata
    | | | `-- outbox
    | | `-- images
    | | `-- 11111111-1111-1111-1111-111111111111
    | `-- lost+found [error opening dir]
```

(output trimmed)

3. 将镜像安全地从源位置复制到完全路径 11111111-1111-1111-1111-111111111111:

```
# scp root@isosource:/isos/example.iso /rhev/data-
center/mnt/10.96.4.50:_rhevisosd/b835cd1c-111c-468d-ba70-
fec5346af227/images/11111111-1111-1111-1111-111111111111
```

4. 新复制的 ISO 镜像的文件权限应为 36:36 (vdsm:kvm)。如果没有，请将 ISO 文件的用户和组所有权更改为 36:36 (vdsm 的用户和组)：

```
# cd /rhev/data-center/mnt/10.96.4.50:_rhevisosd/b835cd1c-111c-468d-ba70-  
fec5346af227/images/11111111-1111-1111-1111-111111111111  
# chown 36.36 example.iso
```

ISO 镜像现在应在数据中心的 ISO 域中可用。

2.6.9.4. 将存储域移到维护模式

存储域必须处于维护模式，然后才能被分离和删除。这要求将另一个数据域重新设计为 **master** 数据域。



重要

如果虚拟机在存储域上具有租用，则无法将存储域进入维护模式。需要关闭虚拟机，或者需要首先删除或移动到其他存储域中。有关虚拟机租期的信息，请参阅 [虚拟机管理指南](#)。

通过添加更多 LUN 扩展 iSCSI 域，只能在域活跃时完成。

流程

1. 关闭在存储域上运行的所有虚拟机。
2. 点 **Storage** → **Domains**。
3. 点存储域的名称。这会打开详情视图。
4. 点 **Data Center** 选项卡。
5. 点 **Maintenance**。

**注意**

Ignore OVF 更新失败复选框允许存储域进入维护模式，即使 OVF 更新失败。

6.

点击 **OK**。

存储域将被停用，并在结果列表中具有不活动状态。现在，您可以编辑、分离、删除或重新激活数据中心中不活跃的存储域。

**注意**

您还可以在与其关联的数据中心的详情视图使用 **Storage** 选项卡激活、分离和将域置于维护模式。

2.6.9.5. 编辑存储域

您可以通过管理门户编辑存储域参数。根据存储域的状态，可以是 **active** 或 **inactive**，不同的字段可用于编辑。**Data Center**, **Domain Function**, **Storage Type**, 和 **Format** 等项不能改变。

•

Active : 当存储域处于活跃状态时，可以编辑 **Name**, **Description**, **Comment**, **Warning Low Space Indicator (%)**, **Critical Space Action Blocker (GB)**, **Wipe After Delete**, 和 **Discard After Delete** 字段。只有存储域处于活动状态时才能编辑 **Name** 字段。还可以在存储域不活跃时编辑所有其他字段。

•

Inactive : 当存储域处于维护模式或未附加模式时（处于不活动状态）您可以编辑 **Name**, **Data Center**, **Domain Function**, **Storage Type**, 和 **Format** 之外的所有字段。存储域必须不活跃才能编辑存储连接、挂载选项和其他高级参数。这只支持 **NFS**、**POSIX** 和 **Local** 存储类型。

**注意**

无法通过管理门户编辑 **iSCSI** 存储连接，但可以通过 **REST API** 编辑。请参阅 *REST API 指南* 中的 [更新存储连接](#)。

编辑 Active Storage Domain*

1.

单击 **Storage** → **Domains** 并选择一个存储域。

2. 单击 **Manage Domain**。
3. 根据需要编辑可用的字段。
4. 单击 **OK**。

编辑不活跃存储域

1. 点 **Storage → Domains**。
2. 如果存储域处于活跃状态，请将其移到维护模式：
 - a. 点存储域的名称。这会打开详情视图。
 - b. 点 **Data Center** 选项卡。
 - c. 点 **Maintenance**。
 - d. 单击 **OK**。
3. 单击 **Manage Domain**。
4. 根据需要编辑存储路径和其他详情。新的连接详情必须与原始连接的存储类型相同。
5. 单击 **OK**。
6. 激活存储域：
 - a. 点存储域的名称。这会打开详情视图。

- b. 点 **Data Center** 选项卡。
- c. 点 **Activate**。

2.6.9.6. 更新 OVF

默认情况下，M OVF 每 60 分钟更新一次。但是，如果您导入了重要的虚拟机或进行关键更新，您可以手动更新 OVF。

流程

1. 点 **Storage** → **Domains**。
2. 选择存储域并点 **More Actions** ()，然后点 **Update OVFs**。

OVF 已更新，并显示在 Events 中。

2.6.9.7. 从维护模式激活存储域

如果您要更改数据中心的存储，则必须将存储域置于维护模式。激活存储域以恢复使用该存储域。

1. 点 **Storage** → **Domains**。
2. 点不活跃存储域的名称。这会打开详情视图。
3. 点 **Data Centers** 选项卡。
4. 点 **Activate**。



重要

如果您在激活数据域之前尝试激活 ISO 域，则会显示错误消息，并且域未激活。

2.6.9.8. 将存储域从数据中心分离

将存储域从一个数据中心分离，将其迁移到另一个数据中心。

流程

1. 点 **Storage → Domains**。
2. 点存储域的名称。这会打开详情视图。
3. 点 **Data Center** 选项卡。
4. 点 **Maintenance**。
5. 单击 **OK** 以启动维护模式。
6. 单击 **Detach**。
7. 单击 **OK** 以分离存储域。

存储域已从数据中心分离，准备好连接到另一个数据中心。

2.6.9.9. 将存储域附加到数据中心

将存储域连接到数据中心。

流程

1. 点 **Storage** → **Domains**。
2. 点存储域的名称。这会打开详情视图。
3. 点 **Data Center** 选项卡。
4. 点 **Attach**。
5. 选择相应的数据中心。
6. 点击 **OK**。

存储域连接到数据中心，并自动激活。

2.6.9.10. 删除存储域

在您的数据中心中有一个要从虚拟环境中删除的存储域。

流程

1. 点 **Storage** → **Domains**。
2. 将存储域移到维护模式并分离它：
 - a. 点存储域的名称。这会打开详情视图。
 - b. 点 **Data Center** 选项卡。
 - c. 单击 **Maintenance**，然后单击 **OK**。


- d. 单击 **Detach**，然后单击**确定**。
3. 单击 **Remove**。
4. (可选) 选择 **格式化域**，即存储内容将丢失！复选框可清除域的内容。
5. 单击 **OK**。

存储域已从环境中永久移除。

2.6.9.11. 销毁存储域

存储域遇到错误可能无法通过正常流程删除。销毁存储域以强制从虚拟环境中删除存储域。

流程

1. 点 **Storage → Domains**。
2. 选择存储域并点 **More Actions** (), 然后点 **Destroy**。
3. 选择 **Approve operation** 复选框。
4. 单击 **OK**。

2.6.9.12. 创建磁盘配置集

磁盘配置文件定义存储域中虚拟磁盘的最大吞吐量以及最大输入和输出操作级别。磁盘配置文件基于数据中心中定义的存储配置文件创建，必须手动分配到单独的虚拟磁盘，才能使配置文件生效。

此流程假设您已在存储域所属数据中心下定义了一个或多个服务条目存储质量。

流程

1. 点 **Storage** → **Domains**。
2. 点数据存储域的名称。这会打开详情视图。
3. 点 **Disk Profiles** 选项卡。
4. 单击 **New**。
5. 为磁盘配置文件输入 **Name** 和 **Description**。
6. 从 **QoS** 列表中选择要应用到磁盘配置集的服务质量。
7. 点击 **OK**。

2.6.9.13. 删除磁盘配置集

从 Red Hat Virtualization 环境中删除现有磁盘配置集。

流程

1. 点 **Storage** → **Domains**。
2. 点数据存储域的名称。这会打开详情视图。
3. 点 **Disk Profiles** 选项卡。
4. 选择要删除的磁盘配置文件。

5. 单击 **Remove**。
6. 单击 **OK**。

如果磁盘配置集分配给任何虚拟磁盘，则会从这些虚拟磁盘中移除该磁盘。

2.6.9.14. 查看存储域的 Health 状态

除了常规的 **Status** 外，存储域还具有外部健康状态。外部健康状态由插件或外部系统报告，或者由管理员设置，并出现在存储域名称左侧的以下图标之一：

- 确定：无图标
- info：

- 警告：

- 错误：

- 失败：


要查看有关存储域健康状态的详情，请单击存储域的名称。这会打开详情视图，然后点 **Events** 选项卡。

也可以使用 **REST API** 查看存储域的健康状况。存储域上的 **GET** 请求将包含 **external_status** 元素，其中包含健康状态。

您可以通过 [事件集合](#) 在 REST API 中设置存储域的健康状况。如需更多信息，请参阅 [REST API 指南](#) 中的 [添加事件](#)。

2.6.9.15. 在为存储域删除后设置 Discard

选择了 **Discard After Delete** 复选框后，会在逻辑卷上调用 `blkdiscard` 命令，并在删除时对底层存储进行通知，通知块可用。存储阵列可以使用空闲的空间并在请求时分配。删除后丢弃 仅适用于块存储。对于文件存储，这个标志不适用于 Red Hat Virtualization Manager，例如 NFS。

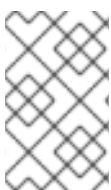
限制：

- 在块存储域（如 iSCSI 或光纤通道）中丢弃 删除 功能才可用。
- 底层存储必须支持 Discard。

在创建块存储域或编辑块存储域时，可以在 [删除后丢弃](#)。请参阅 [准备和添加块存储](#) 和 [编辑存储域](#)。

2.6.9.16. 在有超过 250 个主机的环境中启用 4K 支持

默认情况下，GlusterFS 域和本地存储域支持 Red Hat Virtualization 环境中有最多 250 个主机的 4K 块大小。4k 块大小可以提供更好的性能，特别是在使用大型文件时，在使用需要 4K 兼容性的工具时（如 VDO）也需要这样做。



注意

GlusterFS 存储已弃用，并将在以后的发行版本中删除。

当主机数量上限为 250 时，Sanlock 分配的锁定空间区域为 1 MB。当您在使用 4K 存储时增加主机的最大数量时，锁定空间区会较大。例如，在使用 2000 个主机时，锁定空间区域可能会大为 8 MB。

您可以通过设置 engine 配置参数 `MaxNumberOfHostsInStoragePool` 在有超过 250 个主机的环境中启用 4K 块支持。

流程

1. 在 Manager 机器上启用所需的最大主机数：

```
# engine-config -s MaxNumberOfHostsInStoragePool=NUMBER_OF_HOSTS
```

2. 重启 JBoss 应用服务器：

```
# service jboss-as restart
```

例如，如果您有一个具有 300 个主机的集群，请输入：

```
# engine-config -s MaxNumberOfHostsInStoragePool=300
# service jboss-as restart
```

验证

查看 Manager 中的 MaxNumberOfHostsInStoragePool 参数的值：

```
# engine-config --get=MaxNumberOfHostsInStoragePool
MaxNumberOfHostsInStoragePool: 250 version: general
```

2.6.9.17. 禁用 4K 支持

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



注意

GlusterFS 存储已弃用，并将在以后的发行版本中删除。

您可以禁用 4K 块支持。

流程

1. 确定启用了 4K 块支持。

```
$ vdsm-client Host getCapabilities
...
```

```
{
  "GLUSTERFS" : [
    0,
    512,
    4096,
  ]
  ...
}
```

2.

编辑 `/etc/vdsm/vdsm.conf.d/gluster.conf` 并将 `enable_4k_storage` 设置为 `false`。例如：

```
$ vi /etc/vdsm/vdsm.conf.d/gluster.conf

[gluster]
# Use to disable 4k support
# if needed.
enable_4k_storage = false
```

2.6.9.18. 监控存储域中的可用空间

您可以监控存储域中的可用空间，并创建一个警报来警告您何时存储域接近容量。您还可以定义在域关闭时指出域的关键阈值。

使用 **Virtual Data Optimizer (VDO)**和精简池支持，您可能会看到比物理可用的更多可用空间。对于 VDO 此行为，但 **Manager** 无法预测您实际写入的数据量。**Warning Low Confirmed Space Indicator** 参数会在域接近物理空间容量时通知您，显示已确认空间的大小。已确认空间指的是可用于写入数据的实际空间。

流程

1. 在管理门户中，点 **Storage** → **Storage Domain**，再点存储域的名称。
2. 单击 **Manage Domain**。此时会打开 **Manage Domains** 对话框。
3. 展开 **Advanced Parameters**。
4. 对于 **Warning 低 Space Indicator (%)** 输入百分比值。当存储域中的可用空间达到这个值时，您该域的 **Manager** 警报已接近容量。
5. 对于 **关键空间操作块(GB)**，以 **GB** 为单位输入一个值。当存储域中的可用空间达到这个值时，管理器将关闭。

6. 对于 **Warning 低确认空间分配器(%)** 的百分比值。当存储域中的可用空间达到这个值时，**Manager** 会提醒您写入数据的实际空间已接近容量。

2.7. 池

2.7.1. 虚拟机池简介

虚拟机池是一组虚拟机，这些虚拟机都是同一模板的克隆，可由给定组中的任何用户按需使用。借助虚拟机池，管理员可以为用户快速配置一组常规虚拟机。

用户可以通过从池中获取虚拟机来访问虚拟机。当用户从池中获取虚拟机时，会为它们提供池中的任何一个虚拟机（如果有的话）。该虚拟机的操作系统和配置与池所基于的模板相同，但用户每次获取虚拟机时都可能无法收到与池相同的成员。用户还可以从同一虚拟机池中获取多个虚拟机，具体取决于该池的配置。

默认情况下，虚拟机池是无状态的，这意味着虚拟机数据和配置更改在重新引导后不会保留。但是，可以将池配置为有状态，从而允许上一个用户所做的更改保留。但是，如果用户为从虚拟机池中获取的虚拟机配置了控制台选项，则这些选项将设置为该虚拟机池针对该用户的默认设置。



注意

从管理门户访问时，从池中获取的虚拟机不无状态。这是因为管理员需要能够在必要时将更改写入到磁盘。

在原则上，池中的虚拟机会在用户获取时启动，并在用户完成时关闭。但是，虚拟机池也可以包含预先启动的虚拟机。预先启动的虚拟机会一直处于 **up** 状态，并保持闲置状态，直到被用户获取为止。这样，用户可以立即开始使用此类虚拟机，但由于闲置，这些虚拟机也会消耗系统资源，而这些虚拟机也会消耗系统资源。

2.7.2. 创建虚拟机池

您可以根据通用模板创建包含多个虚拟机的虚拟机池。有关密封虚拟机并创建模板的信息，请参阅 *虚拟机管理指南* 中的 [模板](#)。

sysprep 文件配置选项用于 Windows 虚拟机

根据您的要求，可以使用几个 `sysprep` 文件配置选项。

如果您的池不需要加入一个域，您可以使用默认的 `sysprep` 文件，位于 `/usr/share/ovirt-engine/conf/sysprep/`。

如果您的池需要加入域，您可以为每个 Windows 操作系统创建一个自定义 `sysprep`：

1. 将每个操作系统的相关部分从 `/usr/share/ovirt-engine/conf/osinfo-defaults.properties` 复制到新文件，并将它保存为 `99-defaults.properties`。
2. 在 `99-defaults.properties` 中，指定 Windows 产品激活码以及新自定义 `sysprep` 文件的路径：

```
os.operating_system.productKey.value=Windows_product_activation_key ...
os.operating_system.sysprepPath.value =
${ENGINE_USR}/conf/sysprep/sysprep.operating_system
```

3. 创建一个新的 `sysprep` 文件，指定域、域密码和域管理员：

```
<Credentials>
  <Domain>__AD_Domain__</Domain>
  <Password>__Domain_Password__</Password>
  <Username>__Domain_Administrator__</Username>
</Credentials>
```

如果您需要为 Windows 虚拟机的不同池配置不同的 `sysprep` 设置，您可以在管理门户中创建自定义 `sysprep` 文件（请参阅以下 [创建虚拟机池](#)）。如需更多信息，请参阅 [虚拟机指南](#) 中的 [使用 Sysprep 自动配置虚拟机](#)。

流程

1. 点 **Compute** → **Pools**。
2. 单击 **New**。

3. 从下拉列表中选择 **Cluster**。
4. 从下拉菜单中选择一个 **Template** 和 **version**。模板提供了池中所有虚拟机的标准设置。
5. 从下拉列表中选择 **Operating System**。
6. 使用 **Optimized for** 针对 **Desktop** 或 **Server** 对虚拟机进行优化。



注意

不建议对池进行 **高性能** 优化，因为高性能虚拟机被固定到单个主机和拥塞资源。包含具有这种配置的虚拟机的池不佳。

7. 输入 **Name** 和（可选）**描述**和**注释**。

池的 **Name** 应用于池中每个虚拟机，带有数字后缀。您可以使用 **?** 作为占位符自定义虚拟机的数量。

例 2.1. 池名称和虚拟机编号示例

- **pool: MyPool**

虚拟机 : MyPool-1, MyPool-2, ... MyPool-10
- **Pool: MyPool-???**

虚拟机 : MyPool-001, MyPool-002, ... MyPool-010

8. 为池输入**虚拟机数量**。
9. 在 **Prestarted** 字段中输入要预先启动的**虚拟机数量**。

10. 选择允许单个用户在会话中运行的最大 VM 数量。最小值为 1。
11. 选择 **Delete Protection** 复选框来启用删除保护。
12. 如果您要创建非 Windows 虚拟机池，或者如果您使用默认的 `sysprep`，请跳过这一步。如果您要为 Windows 虚拟机池创建自定义 `sysprep` 文件：
 - a. 点 **Show Advanced Options** 按钮。
 - b. 单击 **Initial Run** 选项卡，再选中 **Use Cloud-Init/Sysprep** 复选框。
 - c. 点 **Authentication** 箭头，输入 **User Name** 或 **Password**，或选择 **Use already configured password**。



注意

此用户名是本地管理员的名称。您可以在 **Authentication** 部分或自定义 `sysprep` 文件中从此处更改其值(用户)。

- d. 单击 **Custom Script** 箭头，并将默认 `sysprep` 文件的内容（位于 `/usr/share/ovirt-engine/conf/sysprep/`）粘贴到文本框中。
- e. 您可以修改 `sysprep` 文件的以下值：
 -

密钥.如果您不想使用预定义的 Windows 激活密钥，请将 `<![CDATA[$ProductKey$]>` 替换为有效的产品键：

```
<ProductKey>
  <Key><![CDATA[$ProductKey$]></Key>
</ProductKey>
```

例 2.2. Windows 产品密钥示例

```
<ProductKey>
  <Key>0000-000-000-000</Key>
</ProductKey>
```

- Windows 虚拟机要加入的 Domain, 域的 Password, 以及域管理员的 Username :

```
<Credentials>
  <Domain>__AD_Domain__</Domain>
  <Password>__Domain_Password__</Password>
  <Username>__Domain_Administrator__</Username>
</Credentials>
```

例 2.3. 域凭证示例

```
<Credentials>
  <Domain>addomain.local</Domain>
  <Password>12345678</Password>
  <Username>Sarah_Smith</Username>
</Credentials>
```



注意

需要 Domain、Password 和 Username 来加入该域。Key 用于激活。您无需同时需要两者。

在 Initial Run 选项卡中无法修改域和凭证。

- 本地管理员 FullName:

```
<UserData>
...
  <FullName>__Local_Administrator__</FullName>
...
</UserData>
```

- 本地管理员的 DisplayName 和 Name :

```
<LocalAccounts>
  <LocalAccount wcm:action="add">
```

```
<Password>
  <Value><![CDATA[$AdminPassword$]]></Value>
  <PlainText>true</PlainText>
</Password>
<DisplayName>__Local_Administrator__</DisplayName>
<Group>administrators</Group>
<Name>__Local_Administrator__</Name>
</LocalAccount>
</LocalAccounts>
```

可在 Initial Run 选项卡中填写 sysprep 文件中的其余变量。

13.

可选。设置池类型：

a.

点 Type 标签页并选择 Pool Type：

- 手动 - 管理员负责将虚拟机明确返回到池。
- 自动 - 虚拟机自动返回到虚拟机池。

b.

选中 **Stateful Pool** 复选框，以确保虚拟机以有状态模式启动。这样可确保上一个用户所做的更改将保留在虚拟机上。

c.

点击 **OK**。

14.

可选。覆盖 SPICE 代理：

a.

在控制台选项卡中，选中覆盖 SPICE 代理复选框。

b.

在 **Overridden SPICE 代理地址** 字段中，指定 SPICE 代理的地址来覆盖全局 SPICE 代理。

c.

点击 **OK**。

15.

对于 Windows 虚拟机池，点 **Compute** → **Virtual Machines**，然后点 **Run** → **Run Once**。

注意

如果虚拟机没有启动，并在 `%WINDIR%\panther\UnattendGC\setupact.log` 中存在 `Info [windeploy.exe] Found no unattend file`，将 `UnattendFile` 键添加到用于创建池模板的 Windows 虚拟机的 registry 中：

1. 检查 Windows 虚拟机是否具有带有 unattend 文件附加的辅助 CD-ROM 设备，例如 `A:\Unattend.xml`。
2. 选择虚拟机，然后点 **Run** → **Run once**。
3. 在 **Boot Options** 下，选中 **Attach Windows guest 工具 CD**。
4. 点 **Start**，点 **Run**，在 **Open** 文本框中键入 `regedit`，然后点 **OK**。
5. 在左侧窗格中，前往 **HKEY_LOCAL_MACHINE** → **SYSTEM** → **设置**。
6. 右键单击右侧窗格并选择 **New** → **String Value**。
7. 输入 `UnattendFile` 作为密钥名称。
8. 双击新密钥并输入 unattend 文件名和路径，例如 `A:\Unattend.xml` 作为密钥值。
9. 保存 registry，密封 Windows 虚拟机，并创建一个新模板。详情请参阅 [虚拟机管理指南](#) 中的 [模板](#)。

您已创建并配置了指定数量的相同虚拟机的虚拟机池。您可以在 **Compute** → **Virtual Machines** 中查看这些虚拟机，或者通过点击池的名称打开其详情视图；池中的虚拟机通过其图标与独立的虚拟机区分开。

2.7.3. 新池和编辑池 Windows 中的设置和控制的说明

2.7.3.1. 新池和编辑池常规设置说明

下表详述了新建池和编辑池窗口的常规选项卡上特定于虚拟机池的必需信息。所有其他设置与新建虚拟机窗口中的设置相同。

表 2.30. 常规设置

字段名称	Description
模板	虚拟机池所基于的模板和模板子版本。如果您基于模板的 latest 子版本创建池，则池中的所有虚拟机都将自动接收最新的模板版本。有关为虚拟机配置模板的更多信息，请参阅 <i>Virtual Machine Management Guide</i> 中的 Virtual Machine General Settings Explained 和 Explanation of Settings in the New Template and Edit Template Windows 。
Description	虚拟机池有意义的描述。
注释	用于添加有关虚拟机池的纯文本可读注释的字段。
预启动的虚拟机	允许您指定虚拟机池中启动的虚拟机数量，在用户执行之前启动并保持该状态供用户获取。此字段的值必须介于 0 到虚拟机池中虚拟机总数之间。
Number of VMs/Increase number of VMs in pool by	允许您指定在虚拟机池中创建和提供的虚拟机数量。在编辑窗口中，您可以通过指定数量在虚拟机池中增加虚拟机数量。默认情况下，您可以在池中创建的虚拟机最大数量是 1000。可以使用 engine-config 命令的 MaxVmsInPool 键来配置此值。
每个用户的最大虚拟机数	允许您指定单个用户一次可以从虚拟机池中获取的最大虚拟机数量。此字段的值必须介于 1 到 32,767 之间。
删除保护	允许您阻止池中的虚拟机被删除。
Sealed	确保从模板中置备的虚拟机中不会复制特定于机器的设置。有关密封流程的更多信息，请参阅 为作为模板部署封装 Windows 虚拟机

2.7.3.2. 新池和编辑池类型设置说明

下表详述了新建池和编辑池窗口的"类型"选项卡上需要的信息。

表 2.31. 类型设置

字段名称	Description
池类型	<p>此下拉菜单允许您指定虚拟机池的类型。可用的选项如下：</p> <ul style="list-style-type: none"> ● 自动：在用户使用完从虚拟机池中获取的虚拟机后，该虚拟机会自动返回到虚拟机池。 ● 手动：在用户使用完从虚拟机池中获取的虚拟机后，该虚拟机仅在管理员手动返回虚拟机时返回到虚拟机池。
有状态池	指定虚拟机传递到其他用户时是否保留池中的虚拟机状态。这意味着之前用户所做的更改将保留在虚拟机上。

2.7.3.3. 新池和编辑池控制台设置说明

下表详述了新建池或编辑池窗口的控制台选项卡上特定于虚拟机池所需的信息。所有其他设置与新建虚拟机和编辑虚拟机窗口中的设置相同。

表 2.32. 控制台设置

字段名称	Description
覆盖 SPICE 代理	选中此复选框可覆盖全局配置中定义的 SPICE 代理。当用户（例如，通过虚拟机门户进行连接）位于主机所在的网络之外时，此功能很有用。
覆盖的 SPICE 代理地址	<p>SPICE 客户端连接到虚拟机时使用的代理。此代理覆盖为 Red Hat Virtualization 环境定义的全局 SPICE 代理，以及为虚拟机池所属集群定义的 SPICE 代理（如果有）。地址必须采用以下格式：</p> <pre>protocol://host:port</pre>


2.7.3.4. 虚拟机池主机设置说明

下表详述了新建池和编辑池窗口的主机选项卡上可用的选项。

表 2.33. 虚拟机池：主机设置

字段名称	子元素	Description
------	-----	-------------

字段名称	子元素	Description
开始运行于		<p>定义要在其上运行虚拟机的首选主机。选择：</p> <ul style="list-style-type: none"> ● 集群中的任何主机 - 虚拟机可以在集群中的任何可用主机上启动并运行。 ● 特定主机 - 虚拟机将在集群的特定主机上运行。但是，管理器或管理员可以根据虚拟机的迁移和高可用性设置，将虚拟机迁移到集群中的不同主机上。从可用的主机列表中选择特定的主机或主机组。
CPU 选项	透传主机 CPU	选择后，允许虚拟机使用主机的 CPU 标志。选择后， Migration Options 被设置为 只允许手动迁移 。
	仅迁移到具有相同 TSC 频率的主机	选择后，此虚拟机只能迁移到具有相同 TSC 频率的主机。此选项仅对高性能虚拟机有效。
迁移选项	迁移模式	<p>定义运行和迁移虚拟机的选项。如果不在此处使用选项，则虚拟机将根据集群的策略运行或迁移。</p> <ul style="list-style-type: none"> ● 允许手动和自动迁移 - 虚拟机可根据环境状态自动从一个主机迁移到另一个主机，或者由管理员手动迁移。 ● 仅允许手动迁移 - 虚拟机只能由管理员手动从一个主机迁移到另一个主机。 ● 不允许迁移 - 虚拟机无法自动或手动迁移。
	迁移策略	<p>定义迁移聚合策略。如果复选框未选中，主机将确定该策略。</p> <ul style="list-style-type: none"> ● 集群默认（最小停机时间） - vdsm.conf 中的覆盖仍会被应用。客户机代理 hook 机制已被禁用。 ● 最小停机时间 - 允许虚拟机在典型情况下迁移。虚拟机不应遇到任何显著的停机时间。如果虚拟机迁移长时间后（依赖于

字段名称	子元素	Description
		<p>QEMU 迭代，且最多为 300 毫秒)，迁移将中止。客户机代理 hook 机制已启用。</p> <ul style="list-style-type: none"> ● 后复制迁移 - 使用后复制迁移时，将暂停源主机上的迁移虚拟机 vCPU，仅传输最小内存页面，激活目标主机上的虚拟机 vCPU，并在虚拟机运行目标时传输其余内存页面。 后复制策略首先尝试预复制，以验证是否可能发生聚合。如果虚拟机迁移在很长时间后没有聚合，迁移会切换到后复制。 <p>这可显著减少迁移的虚拟机停机时间，还可以确保无论源虚拟机的内存页面变化速度如何快。对于迁移大量连续使用的虚拟机来说，这是最佳选择，无法使用标准预复制迁移进行迁移。</p> <p>此策略的缺点在于，在复制后阶段，虚拟机可能会显著下降，因为主机之间缺少内存部分传输。</p> <div data-bbox="1139 1137 1430 2128" style="background-color: #fff9c4; padding: 10px; border: 1px solid #ccc;"> <div style="display: flex; align-items: center; gap: 10px;">  <div style="text-align: right;"> <p>警告</p> <p>如果在完成后复制进程前网络连接中断，管理器将暂停，然</p> </div> </div> </div>

字段名称	子元素	Description
		<p data-bbox="1321 107 1362 1518">后终止正在运行的虚拟机。如果虚拟机可用性至关重要，或者迁移网络不稳定，请不要使用复制后迁移。</p> <ul data-bbox="1098 1659 1428 1966" style="list-style-type: none">● 如果需要，暂停工作负载 - 允许虚拟机在大多数情况下迁移，包括在虚拟机运行繁重工作负载时。因此，虚拟机所经历的停机时间可能比使用其他设置造成的显著停机时间更多。迁移可能仍然针对极端工作负载中止。客户机代理 hook 机制已启用。

字段名称	子元素	Description
	启用迁移加密	<p>允许在迁移过程中对虚拟机进行加密。</p> <ul style="list-style-type: none"> ● 集群默认 ● 加密 ● 不加密
	并行迁移	<p>允许您指定是否使用多少并行迁移连接。</p> <ul style="list-style-type: none"> ● 集群默认：并行迁移连接由集群默认决定。 ● 禁用：虚拟机使用单一的非并行连接迁移。 ● auto：自动决定并行连接数量。此设置可能会自动禁用并行连接。 ● auto Parallel：自动确定并行连接数量。 ● Custom：允许您指定首选并行连接数，实际数量可能较低。
	VM 迁移连接数	<p>此设置仅在选择 Custom 时可用。自定义并行迁移的首选数量，2 到 255 之间。</p>
配置 NUMA	NUMA 节点数	<p>主机上可以分配给虚拟机的虚拟 NUMA 节点数。</p>

字段名称	子元素	Description
	NUMA 固定	<p>打开 NUMA Topology 窗口。此窗口显示主机的总 CPU、内存和 NUMA 节点，以及虚拟机的虚拟 NUMA 节点。您可以通过单击每个 vNUMA 并将每个 vNUMA 拖到左侧的 NUMA 节点，手动固定虚拟 NUMA 节点以托管 NUMA 节点。</p> <p>您还可以为内存分配设置 Tune 模式：</p> <p>严格 - 如果无法在目标节点上分配内存，则内存分配将失败。</p> <p>首选 - 内存从单一首选节点分配。如果没有足够的内存可用，可以从其他节点分配内存。</p> <p>interleave - 内存以轮循算法跨节点分配。</p> <p>如果您定义 NUMA 固定，Migration Options 被设置为只允许手动迁移。</p>

2.7.3.5. 新池和编辑池资源分配设置说明

下表详述了新建池和编辑池窗口的资源分配选项卡所需的信息，它们特定于虚拟机池。所有其他设置与新建虚拟机窗口中的设置相同。如需更多信息，请参阅[虚拟机管理指南](#)中的[虚拟机资源分配设置说明](#)。

表 2.34. 资源分配设置

字段名称	子元素	Description
磁盘分配	自动选择目标	选中此复选框，自动选择具有最多可用空间的存储域。 Target 和 Disk Profile 字段被禁用。
	格式	此字段是只读的，始终显示 QCOW2 。

2.7.3.6. 编辑虚拟机池

创建虚拟机池后，可以编辑其属性。编辑虚拟机池时可用的属性与创建新虚拟机池时可用的属性相同，不同之处在于，**Number of VMs** 属性被 **Increase number of VMs in pool by** 替换。



注意

编辑虚拟机池时，引入的更改仅会影响到新虚拟机。在引入变化时已存在的虚拟机仍不受影响。

流程

1. 点 **Compute** → **Pools** 并选择虚拟机池。
2. 点 **Edit**。
3. 编辑虚拟机池的属性。
4. 点 **确定**。

2.7.3.7. 预启动池中的虚拟机

虚拟机池中的虚拟机默认是关机。当用户从池中请求虚拟机时，会开启虚拟机并分配给该用户。相反，预先启动的虚拟机已在运行并等待分配给用户，减少用户必须等待的时间，然后才能访问虚拟机。当预先启动的虚拟机关闭时，它会返回到池并恢复到其原始状态。预先启动的虚拟机的最大数量是池中虚拟机的数量。

预先启动的虚拟机适合那些用户需要立即访问虚拟机（不特别分配给他们的虚拟机）的环境。只有自动池可以预先启动的虚拟机。

流程

1. 点 **Compute** → **Pools** 并选择虚拟机池。
2. 点 **Edit**。
3. 在 **Prestarted VMs** 字段中输入要预先启动的虚拟机数量。
4. 点 **Type** 标签页。确保 **Pool Type** 设置为 **Automatic**。

5. 点击 **OK**。

2.7.3.8. 将虚拟机添加到虚拟机池

如果您要求虚拟机数量超过最初在虚拟机池中调配的虚拟机，请将更多虚拟机添加到池中。

流程

1. 点 **Compute** → **Pools** 并选择虚拟机池。
2. 点 **Edit**。
3. 在池 **by** 字段中，在增加虚拟机数量后 输入附加虚拟机的数量。
4. 点击 **OK**。

2.7.3.9. 从虚拟机池中分离虚拟机

您可以从虚拟机池中分离虚拟机。分离虚拟机会将其从池中移除，从而成为独立的虚拟机。

流程

1. 点 **Compute** → **Pools**。
2. 点池的名称。这会打开详情视图。
3. 点 **Virtual Machines** 选项卡列出池中的虚拟机。
4. 确保虚拟机的状态为 **Down** ；您无法分离正在运行的虚拟机。
5. 选择一个或多个虚拟机并点击 **Detach**。

6. 点击 **OK**。



注意

虚拟机仍存在于环境中，并可从 **Compute → Virtual Machines** 查看和访问。请注意，图标会更改以表示分离的虚拟机是独立的虚拟机。

2.7.3.10. 删除虚拟机池

您可以从数据中心的删除虚拟机池。您必须先删除或分离池中的所有虚拟机。从池中分离虚拟机会将它们保留为独立的虚拟机。

流程

1. 点 **Compute → Pools** 并选择虚拟机池。
2. 单击 **Remove**。
3. 点击 **OK**。

2.8. 虚拟磁盘

2.8.1. 了解虚拟机存储

Red Hat Virtualization 支持三种存储类型：NFS、iSCSI 和 FCP。

在每个类型中，称为存储池管理器(SPM)的主机管理主机和存储之间的访问。SPM 主机是唯一在存储池中拥有完全访问权限的节点；SPM 可以修改存储域元数据和池的元数据。所有其他主机只能访问虚拟机硬盘镜像数据。

默认情况下，在 NFS、本地或远程 POSIX 兼容数据中心的 SPM 将使用精简配置的格式在文件系统中作为文件创建虚拟磁盘。

在 iSCSI 和其他基于块的数据中心中，SPM 会在提供的逻辑单元号(LUN)之上创建一个卷组，并使逻辑卷用作虚拟磁盘。默认情况下，基于块的存储上的虚拟磁盘是预分配的。

如果虚拟磁盘预先分配，则会创建以 GB 为单位指定大小的逻辑卷。可以使用 `kpartx`、`vgscan`、`vgscan`、`vgchange` 或 `mount` 将虚拟机挂载到 Red Hat Enterprise Linux 服务器上，以调查虚拟机的进程或问题。

如果虚拟磁盘被精简配置，则会创建一个 1 GB 逻辑卷。该逻辑卷由运行虚拟机的主机持续监控。使用量接近一个阈值时，主机会通知 SPM，SPM 会将逻辑卷扩展为 1 GB。主机负责在逻辑卷扩展后恢复虚拟机。如果虚拟机进入暂停状态，这表示 SPM 无法随时间扩展磁盘。如果 SPM 太忙或者没有足够的存储空间，会出现这种情况。

预分配（原始）格式的虚拟磁盘比精简配置(QCOW2)格式的虚拟磁盘要快得多。创建虚拟磁盘需要较少的时间。精简配置格式适用于非 I/O 密集型虚拟机。对于具有高 I/O 写入的虚拟机，建议预分配格式。如果虚拟机每四秒写入超过 1 GB，请尽可能使用预分配的磁盘。

2.8.2. 了解虚拟磁盘

Red Hat Virtualization 有 Preallocated (thick provisioned) 和 Sparse (thin provisioned) 存储选择。

- 预分配

预分配的虚拟磁盘会分配虚拟机前需要的所有存储。例如，为虚拟机的数据分区创建的 20 GB 预分配逻辑卷将在创建后立即占用 20 GB 存储空间。

- 稀疏

稀疏分配允许管理员定义分配给虚拟机的总存储，但只有在需要时才会分配存储。

例如，在首次创建时，一个 20 GB 的精简置备的逻辑卷会占用 0 GB 存储空间。安装操作系统时，可能需要安装的文件的大小，并将继续随着数据增长到最多 20 GB 大小而增加。

您可以在 **Storage** → **Disks** 中查看虚拟磁盘的 ID。ID 用于识别虚拟磁盘，因为它的设备名称（例如 `/dev/vda0`）可能会更改，从而导致磁盘崩溃。您还可以查看 `/dev/disk/by-id` 中的虚拟磁盘 ID。

您可以在存储域、虚拟机和模板的详情视图中的 **Storage** → **Disks** 和 **Disks** 选项卡查看磁盘的虚拟大小。**Virtual Size** 是虚拟机可以使用的磁盘空间总量。在创建或编辑虚拟磁盘时，它是您在 **Size (GB)** 字

段中输入的数字。

您可以在存储域和模板的详情视图中的 **Disks** 选项卡中查看磁盘实际大小。这是目前已分配给虚拟机的磁盘空间量。预分配磁盘显示的虚拟大小和实际大小的值相同。稀疏磁盘可能会显示不同的值，具体取决于分配的磁盘空间量。

下表介绍了存储类型和格式的可能组合。

表 2.35. 允许的存储组合

存储	格式	类型	备注
NFS	Raw	预分配	此文件的初始大小等于为虚拟磁盘定义的存储大小，并且没有格式设置。
NFS	Raw	稀疏	此文件的初始大小接近零，并且没有格式设置。
NFS	QCOW2	稀疏	此文件的初始大小接近零，并且具有 QCOW2 格式。随后的层将是 QCOW2 格式。
SAN	Raw	预分配	具有初始大小等于为虚拟磁盘定义的存储大小的块设备，并且没有格式设置。
SAN	QCOW2	稀疏	具有初始大小小于为虚拟磁盘定义的大小（目前为 1GB）的块设备，并且具有根据需要分配的 QCOW2 格式（目前为 1GB 增量）。

2.8.3. 在删除后将设置为 Wipe Virtual Disks

当虚拟磁盘被删除后，`wipe_after_delete` 标记（在管理门户中为 **Wipe After Delete** 复选框）将把使用的数据替换为零。如果设为 `false`（这是默认设置），删除磁盘将打开这些块以供重复使用，但不会擦除数据。因此，这个数据可以被恢复，因为块没有返回到零。

`wipe_after_delete` 标志仅适用于块存储。在文件存储（例如 NFS）上，选项不会进行任何操作，因为文件系统会确保不存在数据。

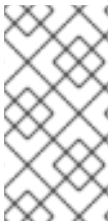
为虚拟磁盘启用 `wipe_after_delete` 更为安全，如果虚拟磁盘包含任何敏感数据，则建议使用。这是一个更密集的操作，用户会在性能方面造成性能下降，延长了删除时间。



注意

删除功能后擦除功能与安全删除不同，且不能保证从存储中删除数据，只是在同一存储中创建的新磁盘不会从旧磁盘中公开数据。

在设置过程中（请参阅 [配置 Red Hat Virtualization Manager](#)）或者使用 `engine-config` 工具在 [Red Hat Virtualization Manager](#) 上使用 `engine-config` 工具，将 `default_after_delete` 标志默认更改为 `true`。重启 `ovirt-engine` 服务以使设置更改生效。



注意

更改 `wipe_after_delete` 标志的默认设置不会影响已存在的磁盘的 `Wipe After Delete` 属性。

使用引擎配置工具将 `SANWipeAfterDelete` 设置为 `True`

1. 使用 `--set` 操作运行 `engine-config` 工具：

```
# engine-config --set SANWipeAfterDelete=true
```

2. 重启 `ovirt-engine` 服务以使更改生效：

```
# systemctl restart ovirt-engine.service
```

可以检查位于主机上的 `/var/log/vdsm.log` 文件，以确认虚拟磁盘已成功擦除并删除。

对于成功擦除，日志文件将包含条目，`storage_domain_id/volume_id` 为零，将被删除。例如：

```
a9cb0625-d5dc-49ab-8ad1-72722e82b0bf/a49351a7-15d8-4932-8d67-512a369f9d61 was zeroed and will be deleted
```

对于成功删除，日志文件将包含条目，使用 `VG:storage_domain_id LVs: list_of_volume_ids, img: image_id`。例如：

```
finished with VG:a9cb0625-d5dc-49ab-8ad1-72722e82b0bf LVs: {'a49351a7-15d8-4932-8d67-512a369f9d61': lmgPar(imgs=['11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d'], parent='00000000-0000-0000-0000-000000000000')}, img: 11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d
```

成功擦除后会显示一个日志消息 `zeroing storage_domain_id/volume_id` 失败。Zero and remove this volume manually, 未成功删除会显示 `Remove failed for some of VG: storage_domain_id zeroed volumes: list_of_volume_ids`。

2.8.4. Red Hat Virtualization 中的可共享磁盘

有些应用程序需要在服务器之间共享存储。Red Hat Virtualization 允许您将虚拟机硬盘标记为可共享，并将这些磁盘附加到虚拟机。这样，一个虚拟磁盘可以被多个集群感知客户机使用。

在每次情况下都不会使用共享磁盘。对于群集数据库服务器和其他高可用服务等应用程序，共享磁盘合适。将共享磁盘附加到多个不感知集群的客户端可能会导致数据崩溃，因为它们对磁盘的读取和写入不协调。

您不能对共享磁盘执行快照。拍摄快照的虚拟磁盘不能标记为可共享。

您可以在创建磁盘时或者稍后编辑磁盘时标记磁盘共享。



重要

只有 RAW 格式磁盘才能进行共享。

2.8.5. 在 Red Hat Virtualization 中只读磁盘

有些应用程序要求管理员通过只读权限共享数据。您可以在虚拟机的详情视图中通过 **Disks** 选项卡创建或编辑虚拟机时，您可以进行此操作，并选择 **Read Only** 复选框。这样，一个磁盘可由多个集群感知客户机读取，而管理员则维护编写特权。

在虚拟机运行时，您无法更改磁盘的只读状态。



重要

挂载文件系统需要读写访问权限。对于包括如文件系统 (EXT3, EXT4, 或 XFS) 的虚拟磁盘, 不适合使用 **Read Only** 选项。

2.8.6. 虚拟磁盘任务

2.8.6.1. 创建虚拟磁盘

镜像 磁盘创建完全由 **Manager** 管理。直接 LUN 磁盘需要外部准备的目标已存在。

您可以创建附加到特定虚拟机的虚拟磁盘。在创建附加的虚拟磁盘时提供了额外的选项, 具体如 [新建虚拟磁盘窗口中的 Settings](#) 所述。

创建附加到虚拟机的虚拟磁盘

1. 单击 **Compute** → **Virtual Machines**。
2. 点虚拟机的名称。这会打开详情视图。
3. 点 **Disks** 选项卡。
4. 单击 **New**。
5. 单击相应的按钮, 以指定虚拟磁盘是镜像还是直接 LUN 磁盘。
6. 选择虚拟磁盘所需的选项。选项根据所选的磁盘类型进行更改。有关 [每个磁盘类型的每个选项的详情](#), 请参阅 [New Virtual Disk Window](#) 中的设置说明。
7. 单击 **OK**。

您还可以创建不属于任何虚拟机的浮动虚拟磁盘。您可以将此磁盘附加到单个虚拟机, 或者在磁盘共享的情况下将其附加到多个虚拟机。创建虚拟磁盘时某些选项不可用, 如 [New Virtual Disk Window](#) 中

的 Settings 所述。

创建浮动虚拟磁盘

1. 单击 **Storage** → **Disks**。
2. 单击 **New**。
3. 单击相应的按钮，以指定虚拟磁盘是镜像还是直接 LUN 磁盘。
4. 选择虚拟磁盘所需的选项。选项根据所选的磁盘类型进行更改。有关 [每个磁盘类型的每个选项的详情](#)，请参阅 [New Virtual Disk Window](#) 中的设置说明。
5. 单击 **OK**。

2.8.6.2. New Virtual Disk 窗口中的设置信息

由于用于创建浮动和附加的虚拟磁盘的新虚拟磁盘窗口非常相似，因此在单一部分中描述其设置。

表 2.36. 新虚拟磁盘和编辑虚拟磁盘设置：镜像

字段名称	Description
Size(GB)	以 GB 为单位的新虚拟磁盘大小。
Alias	虚拟磁盘的名称，限制为 40 个字符。
Description	虚拟磁盘的描述。建议使用此字段，但不强制设置。
Interface	<p>此字段仅在创建附加的磁盘时显示。</p> <p>磁盘向虚拟机呈现的虚拟接口。VirtIO 速度更快，但需要驱动程序。Red Hat Enterprise Linux 5 及更高版本包括这些驱动程序。Windows 不包括以下驱动程序，但您可以从 virtio-win ISO 镜像安装它们。IDE 和 SATA 设备不需要特殊驱动程序。</p> <p>在停止磁盘所附加的所有虚拟机后，可以更新接口类型。</p>

字段名称	Description
数据中心	<p>此字段仅在创建浮动磁盘时显示。</p> <p>提供虚拟磁盘的数据中心。</p>
存储域	<p>存储虚拟磁盘的存储域。下拉列表显示给定数据中心中所有可用的存储域，还显示存储域中的总空间和当前可用空间。</p>
分配策略	<p>新虚拟磁盘的调配策略。</p> <ul style="list-style-type: none"> ● 在创建虚拟磁盘时，预分配 存储域中磁盘的整个大小。虚拟大小和预分配磁盘的实际大小相同。与精简调配的虚拟磁盘相比，预分配的虚拟磁盘需要更长的时间，但读取和写入性能更佳。建议为服务器和其他 I/O 密集型虚拟机预分配的虚拟磁盘。如果虚拟机每四秒写入超过 1 GB，请尽可能使用预分配的磁盘。 ● 精简资源调配 会在创建虚拟磁盘时分配 1 GB，并为磁盘可增长的大小设置最大限制。磁盘的虚拟大小是最大限制；磁盘的实际大小是到目前为止已分配的空间。精简置备的磁盘比预分配的磁盘创建更快，并允许存储过量使用。建议桌面使用精简配置虚拟磁盘。
磁盘配置文件	<p>分配给虚拟磁盘的磁盘配置文件。磁盘配置文件定义存储域中虚拟磁盘的最大吞吐量以及最大输入和输出操作级别。磁盘配置文件根据为数据中心创建的服务条目的存储质量在存储域级别定义。</p>
激活磁盘	<p>此字段仅在创建附加的磁盘时显示。</p> <p>创建后立即激活虚拟磁盘。</p>
删除后擦除	<p>允许您启用增强的安全性，从而在删除虚拟磁盘时删除敏感资料。</p>
可引导	<p>此字段仅在创建附加的磁盘时显示。</p> <p>允许您在虚拟磁盘中启用可引导标记。</p>
可共享	<p>允许您一次将虚拟磁盘附加到多个虚拟机。</p>
read-Only	<p>此字段仅在创建附加的磁盘时显示。</p> <p>允许您将磁盘设置为只读。同一磁盘可以以只读方式附加到一个虚拟机，并且可以重新写入到另一台虚拟机。</p>

字段名称	Description
启用增量备份	在虚拟磁盘上启用增量备份。增量备份需要以 QCOW2 格式而非 RAW 格式格式化磁盘。请参阅 增加备份和恢复 。
启用 Discard	此字段仅在创建附加的磁盘时显示。 允许您在虚拟机启动时缩小精简置备的磁盘。对于块存储，底层存储设备必须支持丢弃调用，选项不能用于 Wipe After Delete，除非底层存储支持 discard_zeroes_data 属性。对于文件存储，底层文件系统和块设备必须支持丢弃调用。如果满足所有要求，QEMU 将 guest 虚拟机发出的 SCSI UNMAP 命令传递给底层存储，以释放未使用的空间。

Direct LUN 设置可以在 **Targets > LUNs** 或 **LUNs > Targets** 中显示。目标 > LUN 根据发现它们的主机对可用 LUN 进行排序，而 LUNs > Targets 则显示 LUN 的单一列表。

填写 **Discover Targets** 部分中的字段，然后单击 **Discover** 来发现目标服务器。然后，您可以单击 **Login All** 按钮列出目标服务器上的可用 LUN，并使用每个 LUN 旁边的单选按钮，选择要添加的 LUN。

将 LUN 直接用作虚拟机硬盘映像可删除虚拟机及其数据之间的抽象层。

在将直接 LUN 用作虚拟机硬盘镜像时，您必须考虑以下事项：

- 不支持直接 LUN 硬盘镜像的实时迁移。
- 直接 LUN 磁盘不包括在虚拟机导出中。
- 直接 LUN 磁盘不包含在虚拟机快照中。

表 2.37. 新虚拟磁盘和编辑虚拟磁盘设置：Direct LUN

字段名称	Description
Alias	虚拟磁盘的名称，限制为 40 个字符。

字段名称	Description
Description	<p>虚拟磁盘的描述。建议使用此字段，但不强制设置。默认情况下，LUN ID 的最后 4 个字符被插入到字段中。</p> <p>可以使用 engine-config 命令将 PopulateDirectLUNDiskDescriptionWithLUNID 配置键设置为适当的值来配置默认行为。对于要使用的完整 LUN ID，可将配置密钥设置为 -1，对于忽略这个功能，可以将其设置为 0。正整数使用相应 LUN ID 的字符数填充描述信息。</p>
Interface	<p>此字段仅在创建附加的磁盘时显示。</p> <p>磁盘向虚拟机呈现的虚拟接口。VirtIO 速度更快，但需要驱动程序。Red Hat Enterprise Linux 5 及更高版本包括这些驱动程序。Windows 不包括这些驱动程序，但可以从 virtio-win ISO 安装它们。IDE 和 SATA 设备不需要特殊驱动程序。</p> <p>在停止磁盘所附加的所有虚拟机后，可以更新接口类型。</p>
数据中心	<p>此字段仅在创建浮动磁盘时显示。</p> <p>提供虚拟磁盘的数据中心。</p>
主机	<p>挂载 LUN 的主机。您可以在数据中心中选择任何主机。</p>
存储类型	<p>要添加的外部 LUN 的类型。您可以从 iSCSI 或光纤通道 中进行选择。</p>
发现目标	<p>当您使用 iSCSI 外部 LUN 时，可以扩展此部分，并选择 Targets > LUNs。</p> <p>地址 - 目标服务器的主机名或 IP 地址。</p> <p>port - 用于尝试连接到目标服务器的端口。默认端口为 3260。</p> <p>用户身份验证 - iSCSI 服务器需要用户身份验证。使用 iSCSI 外部 LUN 时，可以看到 User Authentication 字段。</p> <p>CHAP 用户名 - 有权登录到 LUN 的用户的用户名。选择了 User Authentication 复选框时，可以访问此字段。</p> <p>CHAP 密码 - 有权登录到 LUN 的用户密码。选择了 User Authentication 复选框时，可以访问此字段。</p>

字段名称	Description
激活磁盘	<p>此字段仅在创建附加的磁盘时显示。</p> <p>创建后立即激活虚拟磁盘。</p>
可引导	<p>此字段仅在创建附加的磁盘时显示。</p> <p>允许您在虚拟磁盘中启用可引导标记。</p>
可共享	<p>允许您一次将虚拟磁盘附加到多个虚拟机。</p>
read-Only	<p>此字段仅在创建附加的磁盘时显示。</p> <p>允许您将磁盘设置为只读。同一磁盘可以以只读方式附加到一个虚拟机，并且可以重新写入到另一台虚拟机。</p>
启用 Discard	<p>此字段仅在创建附加的磁盘时显示。</p> <p>允许您在虚拟机启动时缩小精简置备的磁盘。启用此选项后，QEMU 将发出自客户机虚拟机的 SCSI UNMAP 命令传递到底层存储，以释放未使用的空间。</p>
启用 SCSI 透传	<p>此字段仅在创建附加的磁盘时显示。</p> <p>当接口设置为 VirtIO-SCSI 时可用。选择此复选框可启用物理 SCSI 设备的透传到虚拟磁盘。启用 SCSI 透传的 VirtIO-SCSI 接口自动包含 SCSI 丢弃支持。选择这个复选框时不支持 read -Only。</p> <p>如果没有选择此复选框，虚拟磁盘将使用仿真 SCSI 设备。在模拟 VirtIO -SCSI 磁盘上支持只读只读。</p>
允许 Privileged SCSI I/O	<p>此字段仅在创建附加的磁盘时显示。</p> <p>选择了 Enable SCSI Pass-Through 复选框时可用。选择此复选框可启用未过滤的 SCSI Generic I/O(SG_IO)访问，从而允许磁盘上具有特权 SG_IO 命令。这是持久保留所必需的。</p>
使用 SCSI 保留	<p>此字段仅在创建附加的磁盘时显示。</p> <p>当选择了 Enable SCSI Pass-Through 和 Allow Privileged SCSI I/O 复选框时可用。选择此复选框可禁用使用此磁盘的任何虚拟机的迁移，以防止使用 SCSI 保留的虚拟机丢失对磁盘的访问。</p>



重要

挂载文件系统需要读写访问权限。对于包括如文件系统（EXT3, EXT4, 或 XFS）的虚拟磁盘，不适用于使用 **Read-Only** 选项。

2.8.6.3. 实时迁移概述

在连接的虚拟机运行时，虚拟磁盘可以从一个存储域迁移到另一个存储域。这称为实时存储迁移。当迁移连接到正在运行的虚拟机的磁盘时，源存储域中将创建磁盘映像链的快照，并且整个映像链复制到目标存储域中。因此，请确保源存储域和目标存储域中有足够的存储空间来托管磁盘镜像链和快照。每次实时迁移时都会创建一个新的快照，即使迁移失败。

在使用实时存储迁移时请考虑以下几点：

- 您可以一次实时迁移多个磁盘。
- 同一虚拟机的多个磁盘可以驻留在多个存储域上，但每个磁盘的镜像链必须位于单一存储域中。
- 您可以在同一数据中心内的两个存储域之间实时迁移磁盘。
- 您无法实时迁移直接 LUN 硬盘镜像，或者标记为可共享的磁盘。

2.8.6.4. 移动虚拟磁盘

将附加到虚拟机的虚拟磁盘或作为浮动虚拟磁盘从一个存储域移动到另一个存储域。您可以移动附加到正在运行的虚拟机的虚拟磁盘，这称为实时存储迁移。或者，在继续操作前关闭虚拟机。

移动磁盘时请考虑以下几点：

- 您可以同时移动多个磁盘。
- 您可以在同一数据中心中的任何两个存储域之间移动磁盘。

- 如果虚拟磁盘附加到基于模板创建的虚拟机并使用精简配置存储分配选项，您必须将虚拟机磁盘复制到与虚拟磁盘相同的存储域上。

流程

1. 点 **Storage** → **Disks** 并选择要移动的一个或多个虚拟磁盘。
2. 单击 **Move**。
3. 从 **Target** 列表中，选择将移动虚拟磁盘到的存储域。
4. 在 **Disk Profile** 列表中，为磁盘选择一个配置集（如果适用）。
5. 单击 **OK**。

虚拟磁盘将移到目标存储域中。在移动过程中，**Status** 列会显示 **锁定**，进度条表示移动操作的进度。

2.8.6.5. 更改磁盘接口类型

用户可以在磁盘创建后更改磁盘接口类型。这可让您将现有磁盘附加到需要不同接口类型的虚拟机。例如，可以将使用 **VirtIO** 接口的磁盘附加到需要 **VirtIO-SCSI** 或 **IDE** 接口的虚拟机中。这为备份和恢复目的提供了迁移磁盘的灵活性。还可以为每个虚拟机更新可共享磁盘的磁盘接口。这意味着，使用共享磁盘的每个虚拟机都可以使用不同的接口类型。

要更新磁盘接口类型，必须首先停止使用磁盘的所有虚拟机。

更改磁盘接口类型*

1. 点 **Compute** → **Virtual Machines** 并停止适当的虚拟机。
2. 点虚拟机的名称。这会打开详情视图。

3. 点 **Disks** 标签页并选择**磁盘**。
4. 点 **Edit**。
5. 从 **Interface** 列表中，选择新接口类型，再单击 **OK**。

您可以将磁盘附加到需要不同接口类型的不同虚拟机。

使用不同的接口类型将磁盘附加到不同的虚拟机

1. 点 **Compute** → **Virtual Machines** 并停止适当的虚拟机。
2. 点虚拟机的名称。这会打开详情视图。
3. 点 **Disks** 标签页并选择**磁盘**。
4. 单击 **Remove**，然后单击**确定**。
5. 返回到 **Virtual Machines**，然后单击**磁盘要附加到的新虚拟机的名称**。
6. 点 **Disks** 选项卡，然后点 **Attach**。
7. 在 **Attach Virtual Disks** 窗口中选择**磁盘**，然后从接口下拉菜单中选择适当的 **接口**。
8. 单击 **OK**。

2.8.6.6. 复制虚拟磁盘

您可以将虚拟磁盘从一个存储域复制到另一个存储域。复制的磁盘可附加到虚拟机。

流程

1. 点 **Storage** → **Disks** 并选择**虚拟磁盘**。
2. 点 **Copy**。
3. (可选) 在 **Alias** 字段中输入新名称。
4. 从 **Target** 列表中, 选择要复制虚拟磁盘的存储域。
5. 在 **Disk Profile** 列表中, 为磁盘选择一个配置集 (如果适用)。
6. 点击 **OK**。

在复制时, 虚拟磁盘的状态为 **Locked**。

2.8.6.7. 提高磁盘性能

在管理门户中, 在虚拟机的 **资源分配** 标签页中, 会检查默认的 **I/O Threads** 设置 (启用), 且线程数量为 1。


假设虚拟机具有多个含有 **VirtIO** 控制器的磁盘, 其工作负载则利用了这些控制器。在这种情况下, 您可以通过增加 **I/O** 线程数量来提高性能。

但是, 也考虑增加 **I/O** 线程数量会降低虚拟机的线程池。如果您的工作负载不使用 **VirtIO** 控制器以及分配给它们的线程, 增加 **I/O** 线程数量可能会降低整体性能。

要找到线程的最佳数量, 请在调整线程数量前后对运行工作负载的虚拟机性能进行基准测试。

流程

1. 在 **Compute** → **Virtual Machines** 上, 关闭虚拟机。

2. 点虚拟机的名称。
3. 在详细信息窗格中，点 **Vm Devices** 选项卡。
4. 计算其 **Type** 为 **virtio** 或 **virtio-scsi** 的控制器数量。
5. 点 **Edit**。
6. 在 **Edit Virtual Machine** 窗口中，单击 **Resource Allocation** 选项卡。
7. 确认选中了 **I/O 线程已启用**（启用）。
8. 在启用 **I/O Threads** 右侧，增大线程数量，但不超过类型为 **virtio** 或 **virtio-scsi** 的控制器数量。
9. 点击 **OK**。
10. 在详细信息窗格中，点 **Disks** 选项卡。
11. 对于每个磁盘，使用 **More Actions** () 来取消激活和激活磁盘。此操作会将磁盘重新 **map** 到控制器。
12. 点 **Run** 启动虚拟机。

验证步骤

- 要查看哪些控制器具有 **I/O** 线程，请点击详情窗格中的 **Vm Devices**，并在 **Spec Params** 列中查找 **ioThreadid=**。
- 要查看磁盘到控制器的映射，请登录到主机机器并输入以下命令：

```
# virsh -r dumpxml virtual_machine_name
```

其他资源

- [配置高性能虚拟机、模板和池](#)
- [虚拟机资源分配设置说明](#)

2.8.6.8. 将镜像上传到数据存储域

您可以将虚拟磁盘镜像和 ISO 镜像上传到管理门户中的数据存储域，或使用 REST API 上传。[详情请参阅将镜像上传到数据存储域。](#)

2.8.6.9. 从导入的存储域导入磁盘镜像

从导入的存储域导入浮动虚拟磁盘。



注意

只有 QEMU 兼容磁盘才能导入到 Manager 中。

流程

1. 点 **Storage → Domains**。
2. 点导入的存储域的名称。这会打开详情视图。
3. 点 **Disk Import** 标签页。
4. 选择一个或多个磁盘并点击 **Import**。
5. 为每个磁盘选择适当的 **Disk Profile**。

6.

点击 **OK**。

2.8.6.10. 从导入的存储域导入未注册的磁盘镜像

从存储域导入浮动虚拟磁盘。在 Red Hat Virtualization 环境外创建的浮动磁盘不会向 Manager 注册。扫描存储域，以识别要导入的未注册浮动磁盘。



注意

只有 QEMU 兼容磁盘才能导入到 Manager 中。

流程

1.

点 **Storage** → **Domains**。

2.

点存储域的名称。这会打开详情视图。

3.

点 **More Actions** (



)，然后点 **Scan Disks**，以便 Manager 可以识别未注册的磁盘。

4.

点 **Disk Import** 标签页。

5.

选择一个或多个磁盘镜像并单击 **Import**。

6.

为每个磁盘选择适当的 **Disk Profile**。

7.

点击 **OK**。

2.8.6.11. 从 OpenStack Image Service 导入虚拟磁盘

如果 OpenStack 镜像服务作为外部提供程序添加到管理器中，则由 OpenStack Image Service 管理的虚拟磁盘可以导入到 Red Hat Virtualization Manager 中。

1. 点 **Storage** → **Domains**。
2. 单击 **OpenStack Image Service** 域的名称。这会打开详情视图。
3. 点 **Images** 选项卡并选择一个镜像。
4. 点 **Import**。
5. 选择将导入映像 的数据中心。
6. 从 **Domain Name** 下拉列表中，选择要在其中存储映像的存储域。
7. (可选) 从 **Quota** 下拉列表中选择应用到镜像的配额。
8. 点击 **OK**。

磁盘现在可以附加到虚拟机。

2.8.6.12. 将虚拟磁盘导出到 OpenStack 镜像服务

虚拟磁盘可以导出到作为外部提供程序添加到 Manager 的 OpenStack Image Service 中。



重要

只有在没有多个卷时，才能导出虚拟磁盘，且不会被精简调配，且没有任何快照。

1. 点 **Storage** → **Disks** 并选择要导出的磁盘。
2. 点 **More Actions** (
 - ⋮

), 然后点 **Export**。

3. 从 **Domain Name** 下拉列表中, 选择将磁盘导出到的 **OpenStack Image Service**。
4. 在 **Quota** 下拉列表中, 为磁盘选择配额 (如果要应用配额)。
5. 点击 **OK**。

2.8.6.13. 重新声明虚拟磁盘空间

使用精简置备的虚拟磁盘不会在从它们中删除文件后自动缩小。例如, 如果实际磁盘大小为 100GB, 并且您删除 50GB 的文件, 分配的磁盘大小为 100GB, 剩余的 50GB 不会被主机返回, 因此不能被其他虚拟机使用。可以通过对虚拟机磁盘执行 **sparsify** 操作来回收未使用的磁盘空间。这会可用空间从磁盘镜像传输到主机。您可以并行解析多个虚拟磁盘。


在克隆虚拟机、基于虚拟机创建模板或清理存储域的磁盘空间之前, 请执行该操作。

限制

- NFS 存储域必须使用 NFS 版本 4.2 或更高版本。
- 您无法对使用直接 LUN 的磁盘进行解析。
- 您无法对使用预分配策略的磁盘进行解析。如果要从模板创建虚拟机, 则必须从 **Storage Allocation** 字段中选择 **Thin**, 或者选择 **Clone**, 确保模板基于具有精简配置的虚拟机。
- 您只能对活跃快照进行拍摄。

Sparsifying a Disk

1. 点 **Compute** → **Virtual Machines** 并关闭所需的虚拟机。

2. 点虚拟机的名称。这会打开详情视图。
3. 点 Disks 选项卡。确保磁盘的状态为 OK。
4. 点 More Actions (), 然后点 Sparsify。
5. 点击 OK。

在 sparsify 操作期间, sparsify 事件出现在 Events 选项卡中, 磁盘的状态变为 Locked。操作完成后, 在 Events 选项卡中会显示 Sparsified 成功事件, 磁盘的状态会显示为 OK。未使用的磁盘空间已返回到主机, 并可供其他虚拟机使用。

2.9. 外部供应商

2.9.1. Red Hat Virtualization 中的外部提供程序简介

除了由 Red Hat Virtualization Manager 本身管理的资源外, 红帽虚拟化还可以利用由外部来源管理的资源。这些资源(称为外部提供商)的提供程序可以提供诸如虚拟化主机、虚拟机镜像和网络等资源。

Red Hat Virtualization 目前支持以下外部供应商:

Red Hat Satellite for Host Provisioning

卫星是管理物理和虚拟主机生命周期的所有方面的工具。在 Red Hat Virtualization 中, 由 Satellite 管理的主机可以添加到并用作虚拟化主机的 Red Hat Virtualization Manager。将卫星实例添加到管理器后, 可以通过在添加新主机时搜索卫星实例上的可用主机来添加由卫星实例管理的主机。有关使用 Red Hat Satellite 安装 Red Hat Satellite 和管理主机的更多信息, 请参阅 [Red Hat Satellite 快速入门指南](#) 和 [Red Hat Satellite 管理主机](#)。

KubeVirt/OpenShift Virtualization

OpenShift Virtualization (以前称为容器原生虚拟化或 "CNV") 可让您将虚拟机(VM)引入容器化 workflow, 以便您可以使用容器和无服务器来开发、管理和部署虚拟机。在 RHV Manager 中, 添加此提供程序是使用 OpenShift Virtualization 的要求之一。详情请参阅 [添加 KubeVirt/OpenShift Virtualization 作为外部供应商](#)。

用于镜像管理的 OpenStack Image Service (Glance)

OpenStack Image Service 提供虚拟机镜像的目录。在 Red Hat Virtualization 中，您可以将这些镜像导入到 Red Hat Virtualization Manager 中，并用作浮动磁盘或附加到虚拟机，并转换为模板。将 OpenStack Image Service 添加到 Manager 后，它显示为未附加到任何数据中心的存储域。Red Hat Virtualization 环境中的虚拟磁盘也可以作为虚拟磁盘导出到 OpenStack Image Service 中。



注意

对 OpenStack Glance 的支持现已弃用。这个功能将在以后的版本中删除。

VMware for Virtual Machine Provisioning

在 VMware 中创建的虚拟机可以使用 V2V (virt-v2v) 转换并导入到 Red Hat Virtualization 环境中。将 VMware 供应商添加到 Manager 后，您可以导入它提供的虚拟机。V2V 转换是在指定代理主机上执行，作为导入操作的一部分。

用于虚拟机置备的 RHEL 5 Xen

在 RHEL 5 Xen 中创建的虚拟机可以使用 V2V (virt-v2v) 转换并导入到 Red Hat Virtualization 环境中。将 RHEL 5 Xen 主机添加到 Manager 后，您可以导入它所提供的虚拟机。V2V 转换是在指定代理主机上执行，作为导入操作的一部分。

虚拟机置备的 KVM

在 KVM 中创建的虚拟机可导入到 Red Hat Virtualization 环境中。将 KVM 主机添加到 Manager 后，您可以导入它提供的虚拟机。

Open Virtual Network (OVN) for Network Provisioning

Open Virtual Network (OVN) 是一个 Open vSwitch (OVS) 扩展，提供软件定义型网络。将 OVN 添加到 Manager 后，您可以导入现有的 OVN 网络，并从 Manager 创建新 OVN 网络。您还可以使用 engine-setup 在 Manager 上自动安装 OVN。

2.9.2. 添加外部供应商

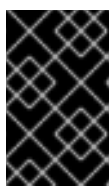
2.9.2.1. 为主机调配添加 Red Hat Satellite 实例

添加用于主机调配的 Satellite 实例到 Red Hat Virtualization Manager。Red Hat Virtualization 4.2 支持 Red Hat Satellite 6.1。

流程

1. 单击 **Administration** → **Providers**。

2. 点 **Add**。
3. 输入名称和描述。
4. 从 **Type** 下拉列表中，选择 **Foreman/Satellite**。
5. 在 **Provider URL** 文本字段中输入安装 **Satellite** 实例的机器的 **URL** 或全限定域名。您不需要指定端口号。



重要

IP 地址不能用于添加卫星实例。

6. 选中 **Requires Authentication** 复选框。
7. 输入卫星实例的"用户名"和"密码"。您必须使用与用于登录 **Satellite** 调配门户相同的用户名和密码。
8. 测试凭证：
 - a. 单击 **Test**，以测试您是否可以使用提供的凭据通过卫星实例成功进行身份验证。
 - b. 如果 **Satellite** 实例使用 **SSL**，则会打开 **Import provider certificate** 窗口；点 **OK** 以导入 **Satellite** 实例提供的证书，确保 **Manager** 可以与实例通信。
9. 点击 **OK**。

2.9.2.2. 为镜像管理添加 OpenStack Image (Glance)实例

**注意**

对 **OpenStack Glance** 的支持现已弃用。这个功能将在以后的版本中删除。

为 **Red Hat Virtualization Manager** 添加用于镜像管理的 **OpenStack Image (Glance)**实例。

流程

1. 单击 **Administration** → **Providers**。
2. 点 **Add**，然后在 **General Settings** 选项卡中输入详情。有关这些字段的更多信息，[请参阅添加 Provider General Settings Explained](#)。
3. 输入名称和描述。
4. 从 **Type** 下拉列表中选择 **OpenStack Image**。
5. 在 **Provider URL** 文本字段中输入安装 **OpenStack Image** 实例的机器的 **URL** 或全限定域名。
6. (可选) 选择 **Requires Authentication** 复选框，然后为 **Keystone** 中注册的 **OpenStack Image** 实例用户输入 **Username** 和 **Password**。您还必须通过定义协议（必须是 **HTTP**）、**Hostname** 和 **API** 端口来定义 **Keystone** 服务器的身份验证 **URL**。

输入 **OpenStack Image** 实例的租户。
7. 测试凭证：
 - a. 单击 **Test**，以测试您是否可以使用提供的凭据通过 **OpenStack Image** 实例成功进行身份验证。
 - b. 如果 **OpenStack Image** 实例使用 **SSL**，则打开 **Import provider certificate** 窗口。单击 **OK**，以导入 **OpenStack Image** 实例提供的证书，以确保管理器能够与实例通信。

8. 点击 OK。

2.9.2.3. 将 KubeVirt/Openshift 虚拟化添加为外部供应商

要在 OpenShift Container Platform 上的容器中运行虚拟机，您需要将 OpenShift 添加为 Red Hat Virtualization 中的外部供应商。



注意

这个功能被称为 *OpenShift Virtualization*。

前提条件

- 在 OpenShift Container Platform 中，为 OpenShift Virtualization 配置集群。

流程

1. 在 RHV 管理门户中，前往 Administration → Providers，再单击 New。
2. 在 Add Provider 中，将 Type 设置为 KubeVirt/Openshift Virtualization。
3. 输入所需的提供程序 URL 和 Token。
4. 可选：输入高级参数的值，如证书颁发机构、Prometheus URL 和 Prometheus 证书颁发机构。
5. 单击 Test 以验证与新提供程序的连接。
6. 单击 OK 以完成添加新提供程序。

验证步骤

1. 在 RHV 管理门户中，点 Compute → Clusters。

2. 点您刚才创建的新集群的名称。这个集群名称 `kubevirt` 例如，基于供应商的名称。此操作会打开集群详情视图。
3. 点 **Hosts** 标签页，验证 **OpenShift Container Platform worker** 节点的状态是否为 `up`。

**注意**

`control plane` 节点的状态是 `down`，即使它们正在运行，因为它们无法托管虚拟机。

4. 使用 **Compute** → **Virtual Machines** 将虚拟机部署到新集群中。
5. 在 **OpenShift Container Platform web** 控制台中，在 **Administrator** 视角中使用 **Workloads** → **Virtual Machines** 查看您部署的虚拟机。

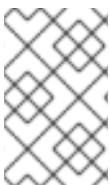
其他资源

- [关于 OpenShift virtualization](#)
- [添加 Provider General Settings Explained](#)

2.9.2.4. 将 VMware 实例添加为虚拟机提供程序

添加 **VMware vCenter** 实例，以便将虚拟机从 **VMware** 导入到 **Red Hat Virtualization Manager**。

Red Hat Virtualization 使用 **V2V** 将 **VMware** 虚拟机转换为正确的格式，然后再导入它们。`virt-v2v` 软件包必须安装到至少一个主机上。默认情况下，`virt-v2v` 软件包在 **Red Hat Virtualization** 主机 (**RHVH**) 上可用，并在 **Red Hat Enterprise Linux** 主机上作为 **VDSM** 的依赖性安装在 **Red Hat Virtualization** 环境中。**Red Hat Enterprise Linux** 主机必须是 **Red Hat Enterprise Linux 7.2** 或更高版本。

**注意**

`virt-v2v` 软件包在 **ppc64le** 架构中不可用，这些主机无法用作代理主机。

流程

1. 单击 **Administration** → **Providers**。
2. 点 **Add**。
3. 输入名称和描述。
4. 从 **Type** 下拉列表中选择 **VMware**。
5. 选择要导入 **VMware** 虚拟机的数据中心，或者选择任何数据中心以便在单个导入操作期间指定目标数据中心。
6. 在 **vCenter** 字段中输入 **VMware vCenter** 实例的 IP 地址或完全限定域名。
7. 在 **ESXi** 字段中输入要从中导入虚拟机的主机的 IP 地址或全限定域名。
8. 在 **Data Center** 字段中输入指定 **ESXi** 主机所在的数据中心的名称。
9. 如果您在 **ESXi** 主机和 **Manager** 之间交换了 **SSL** 证书，请保留 **Verify server** 的 **SSL** 证书复选框来验证 **ESXi** 主机的证书。如果没有，请清除复选框。
10. 在已安装 **virt-v2v** 的选定数据中心中选择一个主机，以便在虚拟机导入操作期间充当 **Proxy** 主机。此主机还必须能够连接到 **VMware vCenter** 外部供应商的网络。如果您选择了上述任何数据中心，则无法在此处选择主机，而是在单独导入操作期间指定主机。
11. 为 **VMware vCenter** 实例输入 **Username** 和 **Password**。用户必须有权访问包含虚拟机的 **VMware** 数据中心和 **ESXi** 主机。
12. 测试凭证：

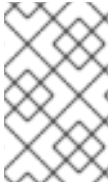
- a. 点 **Test** 来测试您可以使用提供的凭证与 **VMware vCenter** 实例成功进行身份验证。
 - b. 如果 **VMware vCenter** 实例使用 **SSL**，则打开 **Import provider certificate** 窗口；点 **OK** 导入 **VMware vCenter** 实例提供的证书，以确保管理器可以与实例通信。
13. 点击 **OK**。

要从 **VMware** 外部提供程序导入虚拟机，请参阅 *虚拟机管理指南* 中的 [从 VMware 提供程序导入虚拟机](#)。

2.9.2.5. 将 RHEL 5 Xen 主机添加为虚拟机提供程序

添加 **RHEL 5 Xen** 主机，以将虚拟机从 **Xen** 导入到 **Red Hat Virtualization**。

Red Hat Virtualization 使用 **V2V** 将 **RHEL 5 Xen** 虚拟机转换为正确的格式，然后再导入它们。**virt-v2v** 软件包必须安装到至少一个主机上。默认情况下，**virt-v2v** 软件包在 **Red Hat Virtualization** 主机（**RHVH**）上可用，并在 **Red Hat Enterprise Linux** 主机上作为 **VDSM** 的依赖性安装在 **Red Hat Virtualization** 环境中。**Red Hat Enterprise Linux** 主机必须是 **Red Hat Enterprise Linux 7.2** 或更高版本。



注意

virt-v2v 软件包在 **ppc64le** 架构中不可用，这些主机无法用作代理主机。

流程

1. 启用代理主机和 **RHEL 5 Xen** 主机之间的公钥身份验证：
 - a. 登录代理主机，并为 **vdsm** 用户生成 **SSH** 密钥。


```
# sudo -u vsdm ssh-keygen
```
 - b. 将 **vdsm** 用户的公钥复制到 **RHEL 5 Xen** 主机。代理主机的 **known_hosts** 文件也会更新，使其包含 **RHEL 5 Xen** 主机的主机密钥。


```
# sudo -u vsdm ssh-copy-id root@xenhost.example.com
```

-
- c. 登录 RHEL 5 Xen 主机，以验证登录是否正常工作。

```
# sudo -u vdsm ssh root@xenhost.example.com
```

2. 单击 **Administration** → **Providers**。
3. 点 **Add**。
4. 输入名称和描述。
5. 从 **Type** 下拉列表中选择 **XEN**。
6. 选择要导入 Xen 虚拟机的数据中心，或者选择任何数据中心以在单个导入操作期间指定目标数据中心。
7. 在 **URI** 字段中输入 RHEL 5 Xen 主机的 **URI**。
8. 在已安装 **virt-v2v** 的选定数据中心中选择一个主机，以便在虚拟机导入操作期间充当 **Proxy** 主机。该主机还必须能够连接到 RHEL 5 Xen 外部提供程序的 **网络**。如果您选择了上述任何 **数据中心**，则无法在此处选择主机，而是在单独导入操作期间指定主机。
9. 单击 **Test** 以测试您是否可以通过 RHEL 5 Xen 主机成功进行身份验证。
10. 单击 **OK**。

要从 RHEL 5 Xen 外部提供程序导入虚拟机，请参阅 [虚拟机管理指南](#) 中的 [从 RHEL 5 Xen 主机导入虚拟机](#)。

2.9.2.6. 将 KVM 主机添加为虚拟机提供程序

添加 KVM 主机从 KVM 导入虚拟机到 Red Hat Virtualization Manager。

流程

1. 启用代理主机和 KVM 主机之间的公钥身份验证：

- a. 登录代理主机，并为 `vdsm` 用户生成 SSH 密钥。

```
# sudo -u vdsmd ssh-keygen
```

- b. 将 `vdsmd` 用户的公钥复制到 KVM 主机。代理主机的 `known_hosts` 文件也会更新，以包含 KVM 主机的主机密钥。

```
# sudo -u vdsmd ssh-copy-id root@kvmhost.example.com
```

- c. 登录 KVM 主机，以验证登录是否正常工作。

```
# sudo -u vdsmd ssh root@kvmhost.example.com
```

2. 单击 **Administration** → **Providers**。

3. 点 **Add**。

4. 输入名称和描述。

5. 从 **Type** 下拉列表中选择 **KVM**。

6. 选择要导入 KVM 虚拟机的数据中心，或者选择任何数据中心以在单个导入操作期间指定目标数据中心。

7. 在 **URI** 字段中输入 KVM 主机的 URI。

```
qemu+ssh://root@host.example.com/system
```

8. 选择所选数据中心中的主机，在虚拟机导入操作期间用作 **Proxy Host**。此主机还必须能够连接到 KVM 外部提供程序的程序。如果您在上面的 **数据中心** 字段中选择了任何数据中心，则无

法在此处选择主机。该字段已问候并显示 Data Center 中的任何主机。反之，您可以在独立导入操作中指定主机。

9. (可选) 选中 **Requires Authentication** 复选框，再输入 KVM 主机的用户名和密码。用户必须具有虚拟机所在的 KVM 主机的访问权限。
10. 单击 **Test** 以测试您是否可以使用提供的凭证与 KVM 主机成功进行身份验证。
11. 单击 **OK**。

要从 KVM 外部提供商导入虚拟机，请参阅 *虚拟机管理指南* 中的 [从 KVM 主机导入虚拟机](#)。

2.9.2.7. 添加 Open Virtual Network (OVN) 作为外部网络提供程序

您可以使用 Open Virtual Network (OVN) 创建覆盖虚拟网络，以便在虚拟机之间进行通信而无需添加 VLAN 或更改基础架构。OVN 是 Open vSwitch (OVS) 的扩展，可为虚拟 L2 和 L3 覆盖提供原生支持。

您还可以将 OVN 网络连接到原生 Red Hat Virtualization 网络。如需更多信息，请参阅 [将 OVN 网络连接到物理网络](#)。这个功能仅作为技术预览提供。

ovirt-provider-ovn 公开 OpenStack 网络 REST API。您可以使用此 API 创建网络、子网、端口和路由器。详情请参阅 [OpenStack Networking API v2.0](#)。

如需了解更多详细信息，请参阅 [Open vSwitch 文档](#) 和 [Open vSwitch Manpages](#)。

2.9.2.7.1. 安装新的 OVN 网络提供程序

使用 engine-setup 安装 OVN 执行以下步骤：

- 在 Manager 机器上设置 OVN 中央服务器。
- 将 OVN 添加至红帽虚拟化作为外部网络提供程序。

- 在 **Default** 集群中，将 **Default Network Provider** 设置为 **ovirt-provider-ovn**。

重要

- 安装 **OVN** 只会更改 **Default** 集群上的 **Default Network Provider** 设置，而不是在其他集群中。
- 更改默认网络提供程序设置不会更新该集群中的主机以使用默认网络提供程序。
- 对于要使用的主机和虚拟机，请执行本主题末尾的“下一步步骤”中所述的添加任务。

流程

1.

可选：如果您使用带有 **engine-setup** 的预配置应答文件，请添加以下条目来安装 **OVN**：

```
OVESETUP_OVN/ovirtProviderOvn=bool:True
```

2.

在 **Manager** 计算机上运行 **engine-setup**。

3.

如果不使用预先配置的应答文件，则当 **engine-setup** 要求时回答是：

```
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]:
```

4.

回答以下问题：

```
Use default credentials (admin@internal) for ovirt-provider-ovn (Yes, No) [Yes]?:
```

如果为 **Yes**，**engine-setup** 将使用之前在设置过程中指定的默认引擎用户和密码。这个选项仅在新安装过程中可用。

oVirt OVN provider user[admin]:
oVirt OVN provider password[empty]:

您可以使用默认值或指定 oVirt OVN provider 用户和密码。



注意

要稍后更改身份验证方法，您可以编辑 `/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` 文件，或创建一个新的 `/etc/ovirt-provider-ovn/conf.d/20_engine_setup.conf` 文件。重启 `ovirt-provider-ovn` 服务以使更改生效。如需有关 OVN 身份验证的更多信息，请参阅 [OVN 的 oVirt 外部网络供应商](#)。

后续步骤

在创建使用新安装的 OVN 网络的虚拟机前，请完成这些附加步骤：

1. [将一个网络添加到 Default 集群](#)。
 - a. 在执行此操作时，选择 **Create on external provider** 复选框。这会基于 `ovirt-provider-ovn` 创建一个网络。
 - b. 可选：要将 [OVN 网络连接到物理网络](#)，请选择 **连接到物理网络** 复选框，并指定要使用的 Red Hat Virtualization 网络。
 - c. 可选：确定网络是否应使用安全组并从 **Security Groups** 下拉菜单中选择一个。有关可用选项的详情，请查看 [逻辑网络常规设置说明](#)。
2. [在 Default 集群上添加主机或重新安装主机](#)，以便它们使用集群的新默认网络提供程序、`ovirt-provider-ovn`。
3. 可选：编辑非默认集群，将 **Default Network Provider** 设置为 `ovirt-provider-ovn`。
 - a. 可选：在每个非默认集群上重新安装主机，以便它们使用集群的新默认网络提供程序、`ovirt-provider-ovn`。

其他资源

- 要将主机配置为使用现有的非默认网络，请参阅为 [OVN 隧道网络配置主机](#)。

2.9.2.7.2. 在单主机上更新 OVN Tunnel Network

您可以使用 `vdsm-tool` 更新单一主机上的 OVN 隧道网络：

```
# vsdm-tool ovn-config OVN_Central_IP Tunneling_IP_or_Network_Name Host_FQDN
```



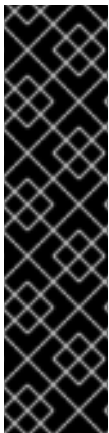
注意

`Host_FQDN` 必须与此主机的引擎中指定的 FQDN 匹配。

例 2.4. 使用 `vdsm-tool` 更新主机

```
# vsdm-tool ovn-config 192.168.0.1 MyNetwork MyFQDN
```

2.9.2.7.3. 将 OVN 网络连接到物理网络

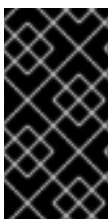


重要

此功能依赖于 Open vSwitch 支持，它只在 Red Hat Virtualization 中作为技术预览提供。红帽产品服务级别协议 (SLA) 不支持技术预览功能，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。

如需有关红帽技术预览功能支持范围的更多信息，请参阅 [技术预览功能支持范围](#)。

您可以创建一个外部提供者网络，覆盖一个原生 Red Hat Virtualization 网络，以便每个虚拟机都出现在共享同一子网上。



重要

如果您为 OVN 网络创建了一个子网，则使用该网络的虚拟机将从那里接收 IP 地址。如果您希望物理网络分配 IP 地址，请不要为 OVN 网络创建一个子网。

前提条件

- 集群必须将 OVS 选择为 **Switch Type**。添加到此集群的主机不得配置任何已存在的 Red Hat Virtualization 网络，如 ovirtmgmt 网桥。
- 物理网络必须在主机上可用。您可以根据需要设置集群所需的物理网络（在 **Manage Networks** 窗口中，或者 **New Logical Network** 窗口的 **Cluster** 选项卡）。

流程

1. 单击 **Compute** → **Clusters**。
2. 点集群名称。这会打开详情视图。
3. 单击逻辑网络选项卡，再单击添加网络。
4. 为网络输入 **Name**。
5. 选择 **Create on external provider** 复选框。默认选择 **ovirt-provider-ovn**。
6. 如果尚未选中，请选择"连接到物理网络"复选框。
7. 选择要将新网络连接到的物理网络：
 - 单击 **Data Center Network** 单选按钮，再从下拉列表中选择物理网络。这是推荐的选项。
 - 单击"自定义"单选按钮，并输入物理网络的名称。如果物理网络启用了 VLAN 标记，还必须选择 **Enable VLAN tagging** 复选框，并输入物理网络的 VLAN 标签。



重要

物理网络的名称不能超过 15 个字符，或者包含特殊字符。

8. 点击 OK。

```
////Removing for BZ2006228
include::topics/Adding_an_External_Network_Provider.adoc[leveloffset=+2]
```

2.9.2.8. 添加 Provider General Settings Explained

通过 Add Provider 窗口中的 General 选项卡，您可以注册外部供应商的核心详情。

表 2.38. 添加 Provider: 常规设置

设置	解释
Name	在 Manager 中代表供应商的名称。
Description	提供商的纯文本可读描述。
类型	<p>外部供应商的类型。更改此设置可更改用于配置提供程序的可用字段。</p> <p>外部网络提供程序</p> <ul style="list-style-type: none"> ● 网络插件：确定主机上将使用哪些驱动程序实施来处理 NIC 操作。如果将带有 oVirt Network Provider for OVN 插件的外部网络提供程序添加为集群的默认网络提供程序，这也决定了将哪些驱动程序安装到添加到集群的主机上。 ● 自动同步：允许您指定供应商是否会自动与现有网络同步。 ● 提供者 URL：托管外部网络提供程序的机器的 URL 或完全限定域名。您必须将外部网络提供程序的端口号添加到 URL 或完全限定域名的末尾。默认情况下，此端口号为 9696。 ● 只读：允许您指定外部网络供应商是否可以从管理门户中修改。 ● 需要 Authentication：允许您指定是否需要身份验证才能访问外部网络供应商。 ● 用户名：用于连接外部网络提供程序的用户名。如果使用 Active Directory 进行身份验证，用户名的格式为

设置	解释 <i>username@domain@auth_profile</i> 而不是默认的 <i>username@domain</i> 。
	<ul style="list-style-type: none"> ● Password : 上面用户名要进行身份验证的密码。 ● 协议 : 用于与 Keystone 服务器通信的协议。默认值为 HTTPS。 ● 主机名 : Keystone 服务器的 IP 地址或主机名。 ● API 端口 : Keystone 服务器的 API 端口号。 ● API 版本 : Keystone 服务器的版本。该值为 v2.0, 字段被禁用。 ● 租户名称 : 可选。外部网络提供程序所属的租户的名称。 <p>Foreman/Satellite</p> <ul style="list-style-type: none"> ● 提供程序 URL : 托管卫星实例的计算机的 URL 或完全限定域名。您不需要在 URL 或完全限定域名末尾添加端口号。 ● 需要 Authentication : 允许您指定供应商是否需要身份验证。选择 Foreman/Satellite 时, 身份验证是必须的身份验证。 ● 用户名 : 用于连接卫星实例的用户名。此用户名必须是用于登录 Satellite 实例上的调配门户的用户名。 ● Password : 上面用户名要进行身份验证的密码。此密码必须是用于登录卫星实例上调配门户的密码。 <p>KubeVirt/OpenShift Virtualization</p> <ul style="list-style-type: none"> ● Provider URL : OpenShift Container Platform API 的 URL 或完全限定域名和端口号。默认情况下, 这个端口号为 6443。 ● 令牌 用于向 API 验证此连接的 OAuth 访问令牌。 ● 证书颁发机构(CA)证书, 以在发出 https 请求时被信任。 ● Prometheus URL 用于 OpenShift 集群的 prometheus 服务的 URL。如果没有提供这个 URL, 则软件将尝试自动检测这个 URL。 ● Prometheus 证书颁发机构(prometheus)的 X509 证书。如果没有指定此 CA, 则供应商使用 KubeVirt CA。 <p>OpenStack Image</p> <ul style="list-style-type: none"> ● 提供程序 URL : 托管 OpenStack 镜像服务的计算机的 URL 或全限定域名。您必须将 OpenStack 镜像服务的端口号添加到 URL 或完全限定域名的末尾。默认情况下, 这个端口号为 9292。

设置	解释
	<ul style="list-style-type: none"> ● 需要 Authentication : 允许您指定是否需要身份验证才能访问 OpenStack 镜像服务。 ● 用户名 : 用于连接 Keystone 服务器的用户名。此用户名必须是 OpenStack 镜像服务所属的 Keystone 实例中注册的 OpenStack 镜像服务的用户名。 ● Password : 上面用户名要进行身份验证的密码。此密码必须是 OpenStack 镜像服务所属 Keystone 实例中注册的 OpenStack 镜像服务的密码。 ● 协议 : 用于与 Keystone 服务器通信的协议。这必须设置为 HTTP。 ● 主机名 : Keystone 服务器的 IP 地址或主机名。 ● API 端口 : Keystone 服务器的 API 端口号。 ● API 版本 : Keystone 服务的版本。该值为 v2.0, 字段被禁用。 ● 租户名称 : OpenStack 镜像服务所属的 OpenStack 租户的名称。 <p>OpenStack Volume</p> <ul style="list-style-type: none"> ● 数据中心 : 将附加到 OpenStack 卷存储卷的数据中心。 ● 提供程序 URL : 托管 OpenStack 卷实例的计算机的 URL 或完全限定域名。您必须将 OpenStack 卷实例的端口号添加到 URL 或完全限定域名的末尾。默认情况下, 此端口号为 8776。 ● 需要 Authentication : 允许您指定是否需要身份验证才能访问 OpenStack 卷服务。 ● 用户名 : 用于连接 Keystone 服务器的用户名。此用户名必须是在 OpenStack 卷实例所属的 Keystone 实例中注册的 OpenStack 卷的用户名。 ● Password : 上面用户名要进行身份验证的密码。此密码必须是在 OpenStack 卷实例所属的 Keystone 实例中注册的 OpenStack 卷的密码。 ● 协议 : 用于与 Keystone 服务器通信的协议。这必须设置为 HTTP。 ● 主机名 : Keystone 服务器的 IP 地址或主机名。 ● API 端口 : Keystone 服务器的 API 端口号。 ● API 版本 : Keystone 服务器的版本。该值为 v2.0, 字段被禁用。 ● 租户名称 : OpenStack 卷实例所属的 OpenStack 租户的名称。

设置	VMware 解释
	<ul style="list-style-type: none"> ● 数据中心：指定将要导入 VMware 虚拟机的数据中心，或者选择任何数据中心以在单个导入操作期间指定目标数据中心（使用虚拟机选项卡中的 Import 功能）。 ● vCenter：VMware vCenter 实例的 IP 地址或完全限定域名。 ● ESXi：导入虚拟机的主机的 IP 地址或完全限定域名。 ● 数据中心：指定 ESXi 主机所在的数据中心的名称。 ● Cluster：指定 ESXi 主机所在的集群名称。 ● 验证服务器的 SSL 证书：指定连接时是否会验证 ESXi 主机的证书。 ● 代理主机：在所选数据中心中选择安装 virt-v2v 的主机，以便在虚拟机导入操作期间用作主机。此主机还必须能够连接到 VMware vCenter 外部供应商的网络。如果选择了任何数据中心，您不能在这里选择主机，而是可在单个导入操作中指定主机（使用虚拟机选项卡中的 Import 功能）。 ● 用户名：用于连接 VMware vCenter 实例的用户名。用户必须有权访问包含虚拟机的 VMware 数据中心和 ESXi 主机。 ● Password：上面用户名要进行身份验证的密码。 <p>RHEL 5 Xen</p> <ul style="list-style-type: none"> ● 数据中心：指定将要导入 Xen 虚拟机的数据中心，或者选择任何数据中心以便在单个导入操作期间指定目标数据中心（在虚拟机选项卡中使用 Import 功能）。 ● URI：RHEL 5 Xen 主机的 URI。 ● 代理主机：在所选数据中心中选择安装 virt-v2v 的主机，以便在虚拟机导入操作期间用作主机。该主机还必须能够连接到 RHEL 5 Xen 外部提供程序的网路。如果您选择了任何数据中心，则不能在这里选择主机，而是可在单个导入操作中指定主机（使用虚拟机选项卡中的 Import 功能）。 <p>KVM</p> <ul style="list-style-type: none"> ● 数据中心：指定将导入 KVM 虚拟机的数据中心，或者选择任何数据中心以便在单个导入操作期间指定目标数据中心（在虚拟机选项卡中使用 Import 功能）。 ● URI：KVM 主机的 URI。 ● 代理主机：在所选数据中心中选择一个主机，在虚拟机导入操作期间用作主机。此主机还必须能够连接到 KVM 外部提供程序的网

设置	解释
	<p>络。如果您选择了任何数据中心，则不能在这里选择主机，而是可在单个导入操作中指定主机（使用虚拟机选项卡中的 Import 功能）。</p> <ul style="list-style-type: none"> ● 需要身份验证：允许您指定是否需要身份验证才能访问 KVM 主机。 ● 用户名：用于连接 KVM 主机的用户名。 ● Password：上面用户名要进行身份验证的密码。
测试	允许用户测试指定的凭证。此按钮可供所有提供程序类型使用。

2.9.3. 编辑外部供应商

流程

1. 单击 **Administration** → **Providers**，再选择要编辑的外部提供程序。
2. 点 **Edit**。
3. 将提供程序的当前值更改为首选值。
4. 单击 **OK**。

2.9.4. 删除外部供应商

流程

1. 单击 **Administration** → **Providers**，再选择要删除的外部提供程序。
2. 单击 **Remove**。
3. 单击 **OK**。

第 3 章 管理环境

3.1. 管理自托管引擎

3.1.1. 维护自托管引擎

3.1.1.1. 自托管引擎维护模式解释

通过维护模式，您可以启动、停止和修改 Manager 虚拟机，而不影响高可用性代理，以及重启和修改环境中的自托管引擎节点，而无需与 Manager 干扰。

有三种维护模式：

- **全局** - 集群中的所有高可用性代理都禁止监控 Manager 虚拟机的状态。对于需要停止 ovirt-engine 服务的任何设置或升级操作，必须应用全局维护模式，比如升级到更新的 Red Hat Virtualization 版本。
- **local** - 发布命令的节点上的高可用性代理在监控 Manager 虚拟机的状态被禁用。在处于本地维护模式时，该节点无法托管管理器虚拟机；如果托管了 Manager 虚拟机，则管理器将迁移到另一节点，提供有一个可用的节点。在对自托管引擎节点应用系统更改或更新时，建议使用本地维护模式。
- **none** - 禁用维护模式，确保高可用性代理正在运行。

3.1.1.2. 设置本地维护模式

启用本地维护模式可在单个自托管引擎节点上停止高可用性代理。

从管理门户设置本地维护模式

1. 将自托管引擎节点设置为本地维护模式：
 - a. 在管理门户中，单击 **Compute** → **Hosts** 并选择自托管引擎节点。
 - b. 单击 **Management** → **Maintenance** 和 **OK**。该节点会自动触发本地维护模式。

2. 完成任何维护任务后，禁用维护模式：
 - a. 在管理门户中，单击 **Compute** → **Hosts** 并选择自托管引擎节点。
 - b. 点 **Management** → **Activate**。

通过命令行设置本地维护模式

1. 登录到自托管引擎节点并将其设置为本地维护模式：

```
# hosted-engine --set-maintenance --mode=local
```

2. 完成任何维护任务后，禁用维护模式：



```
# hosted-engine --set-maintenance --mode=none
```

3.1.1.3. 设置全局维护模式

启用全局维护模式可在集群中的所有自托管引擎节点上停止高可用性代理。

从管理门户设置全局维护模式

1. 将所有自托管引擎节点设置为全局维护模式：
 - a. 在管理门户中，单击 **Compute** → **Hosts** 并选择任何自托管引擎节点。
 - b. 点 **More Actions** (
⋮
)，然后点 **Enable Global HA Maintenance**。
2. 完成任何维护任务后，禁用维护模式：
 - a. 在管理门户中，单击 **Compute** → **Hosts** 并选择任何自托管引擎节点。

- b.  点 More Actions (), 然后点 Disable Global HA Maintenance。

从命令行设置全局维护模式

1. 登录到任何自托管引擎节点并将其设置为全局维护模式：

```
# hosted-engine --set-maintenance --mode=global
```

2. 完成任何维护任务后，禁用维护模式：

```
# hosted-engine --set-maintenance --mode=none
```

3.1.2. 管理 Manager 虚拟机

`hosted-engine` 实用程序提供了多个命令来帮助管理 Manager 虚拟机。您可以在任何自托管引擎节点上运行 `hosted-engine`。要查看所有可用命令，请运行 `hosted-engine --help`。有关特定命令的附加信息，请运行 `hosted-engine --命令 --help`。

3.1.2.1. 更新自托管引擎配置

若要更新自托管引擎配置，请使用 `hosted-engine --set-shared-config` 命令。此命令会在初始部署后，更新共享存储域中的自托管引擎配置。

要查看当前的配置值，请使用 `hosted-engine --get-shared-config` 命令。

要查看所有可用配置密钥及其对应类型的列表，请输入以下命令：

```
# hosted-engine --set-shared-config key --type=type --help
```

其中 `type` 是以下之一：

<code>he_local</code>	在本地主机上 <code>/etc/ovirt-hosted-engine/hosted-engine.conf</code> 的本地实例中设置值，以便只有该主机使用新值。要启用新值，请重启 <code>ovirt-ha-agent</code> 和 <code>ovirt-ha-broker</code> 服务。
-----------------------	--

he_shared	在共享存储上的 <code>/etc/ovirt-hosted-engine.conf</code> 中设置值，以便在配置更改后部署的所有主机。要在主机上启用新值，请重新部署该主机。
ha	在本地存储的 <code>/var/lib/ovirt-hosted-engine-ha/ha.conf</code> 中设置值。新设置立即生效。
broker	在本地存储的 <code>/var/lib/ovirt-hosted-engine-ha/broker.conf</code> 中设置值。重启 <code>ovirt-ha-broker</code> 服务以启用新设置。

3.1.2.2. 配置电子邮件通知

您可以使用 **SMTP** 在自托管引擎节点上发生任何 **HA** 状态配置电子邮件通知。可更新的密钥包括：`smtp-server`、`smtp-port`、`source-email`、`destination-emails` 和 `state_transition`。

配置电子邮件通知：

1.

在自托管引擎节点上，将 `smtp-server` 密钥设置为所需的 **SMTP** 服务器地址：

```
# hosted-engine --set-shared-config smtp-server smtp.example.com --type=broker
```



注意

要验证自托管引擎配置文件是否已更新，请运行：

```
# hosted-engine --get-shared-config smtp-server --type=broker
broker : smtp.example.com, type : broker
```

2.

检查是否已配置默认 **SMTP** 端口（端口 25）：

```
# hosted-engine --get-shared-config smtp-port --type=broker
broker : 25, type : broker
```

3.

指定您希望 **SMTP** 服务器用于发送电子邮件通知的电子邮件地址。只能指定一个地址。

```
# hosted-engine --set-shared-config source-email source@example.com --type=broker
```

4.

指定接收电子邮件通知的目标电子邮件地址。要指定多个电子邮件地址，使用逗号分隔每个地址。

```
# hosted-engine --set-shared-config destination-emails  
destination1@example.com,destination2@example.com --type=broker
```

要验证是否已为您的自托管引擎环境正确配置了 SMTP，请更改自托管引擎节点上的 HA 状态，并检查电子邮件通知是否已发送。例如，您可以通过将 HA 代理置于维护模式来更改 HA 状态。如需更多信息，请参阅[维护自托管引擎](#)。

3.1.3. 在附加主机上为自托管引擎配置 Memory Slots 保留

如果 Manager 虚拟机关闭或需要迁移，则必须在自托管引擎节点上有足够的内存供 Manager 虚拟机重新启动或迁移到该虚拟机。可以使用调度策略在多个自托管引擎节点上保留此内存。在启动或迁移任何虚拟机之前，调度策略会检查足够的内存来启动 Manager 虚拟机是否保留在指定数量上。如需有关调度策略的更多信息，请参阅[管理指南](#)中的[创建调度策略](#)。

要在 Red Hat Virtualization Manager 中添加更多的自托管引擎节点，请参阅[将自托管引擎节点添加到 Manager](#) 中。

在附加主机上为自托管引擎配置 Memory Slots 保留

1. 点 **Compute** → **Clusters** 并选择包含自托管引擎节点的集群。
2. 点 **Edit**。
3. 单击 **Scheduling Policy** 选项卡。
4. 单击 **+**，然后选择 **HeSparesCount**。
5. 输入可保留足够可用内存的额外自托管引擎节点数量，以启动 **Manager** 虚拟机。
6. 单击 **OK**。

3.1.4. 在 Red Hat Virtualization Manager 中添加自托管引擎节点

添加自托管引擎节点的方式与标准主机相同，另外一步用于将主机部署为自托管引擎节点。可自动检

测共享存储域，并在需要时将节点用作故障转移主机来托管管理器虚拟机。您还可以将标准主机附加到自托管引擎环境中，但不能托管管理器虚拟机。至少有两个自托管引擎节点，以确保 Manager 虚拟机高度可用。您还可以使用 REST API 添加其他主机。请参阅 [REST API 指南中的主机](#)。

前提条件

- 所有自托管引擎节点必须位于同一群集中。
- 如果您要重复使用自托管引擎节点，请删除其现有的自托管引擎配置。请参阅[从自托管引擎环境中删除主机](#)。

流程

1. 在管理门户中，点 **Compute** → **Hosts**。
2. 点 **New**。

有关其他主机设置的详情，请参考 [管理指南中的新主机](#)和[编辑主机 Windows 中的设置和控制说明](#)。
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）配置电源管理，其中主机具有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](#)。

7. 点托管引擎选项卡。
8. 选择 **Deploy**。
9. 点击 **OK**。

3.1.5. 将现有主机重新安装为自托管引擎节点

您可以将自托管引擎环境中的现有标准主机转换为能够托管 **Manager** 虚拟机的自托管引擎节点。



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. 单击 **Compute** → **Hosts**，再选择 **主机**。
2. 点 **Management** → **Maintenance** 和 **OK**。
3. 点 **Installation** → **Reinstall**。
4. 单击 **Hosted Engine** 选项卡，再从下拉菜单中选择 **DEPLOY**。
5. 点击 **确定**。

主机通过自托管引擎配置重新安装，并使用管理门户中的 **crown** 图标标记。

3.1.6. 在救援模式中引导 Manager 虚拟机

这部分论述了如何在 Manager 虚拟机启动时将 Manager 虚拟机引导至救援模式。如需更多信息，请参阅 *Red Hat Enterprise Linux 系统管理员指南* 中的 [引导至救援模式](#)。

1. 连接到其中一个 hosted-engine 节点：

```
$ ssh root@host_address
```

2. 将自托管引擎设置为全局维护模式：

```
# hosted-engine --set-maintenance --mode=global
```

3. 检查 Manager 虚拟机是否正在运行实例：

```
# hosted-engine --vm-status
```

如果 Manager 虚拟机实例正在运行，连接到其主机：

```
# ssh root@host_address
```

4. 关闭虚拟机：

```
# hosted-engine --vm-shutdown
```



注意

如果虚拟机没有关闭，请执行以下命令：

```
# hosted-engine --vm-poweroff
```

5. 以暂停模式启动 Manager 虚拟机：

```
hosted-engine --vm-start-paused
```

6. 设置临时 VNC 密码：

```
hosted-engine --add-console-password
```

命令输出所需的信息，您需要使用 VNC 登录到 Manager 虚拟机。

7. 使用 VNC 登录到 Manager 虚拟机。Manager 虚拟机仍暂停，因此它似乎为 frozen。

8. 使用以下命令恢复 Manager 虚拟机：



警告

运行以下命令后会显示引导装载程序菜单。在引导装载程序进行正常引导过程前，您需要进入救援模式。继续此命令之前，阅读有关进入救援模式的下一步。

```
# /usr/bin/virsh -c qemu:///system?authfile=/etc/ovirt-hosted-engine/virsh_auth.conf  
resume HostedEngine
```

9. 在救援模式下引导 Manager 虚拟机。

10. 禁用全局维护模式

```
# hosted-engine --set-maintenance --mode=none
```

现在，您可以在 Manager 虚拟机上运行 rescue 任务。

3.1.7. 从自托管引擎环境中删除主机

要从环境中删除自托管引擎节点，请将节点置于维护模式，取消部署该节点，并选择性地将其删除。在 HA 服务停止后，可以将该节点作为常规主机进行管理，并且删除了自托管引擎配置文件。

流程

1. 在管理门户中，单击 **Compute** → **Hosts** 并选择自托管引擎节点。
2. 点 **Management** → **Maintenance** 和 **OK**。
3. 点 **Installation** → **Reinstall**。
4. 点 **Hosted Engine** 选项卡，从下拉菜单中选择 **UNDEPLOY**。此操作将停止 **ovirt-ha-agent** 和 **ovirt-ha-broker** 服务，并删除自托管引擎配置文件。
5. 点击 **OK**。
6. (可选) 点击 **Remove**。此时将打开 **Remove Host (s)** 确认窗口。
7. 点击 **OK**。

3.1.8. 更新自托管引擎

要将自托管引擎从当前版本更新到最新版本，您必须将环境置于全局维护模式，然后按照标准流程在次版本间更新。

启用全局维护模式

您必须将自托管引擎环境置于全局维护模式，然后才能在 **Manager** 虚拟机上执行任何设置或升级任务。

流程

1. 登录到自托管引擎节点并启用全局维护模式：

```
# hosted-engine --set-maintenance --mode=global
```
2. 在继续前确认环境处于全局维护模式：


```
# hosted-engine --vm-status
```

您应该会看到指示集群处于全局维护模式的消息。

更新 Red Hat Virtualization Manager

流程

1. 在 Manager 机器中检查更新的软件包是否可用：

```
# engine-upgrade-check
```

2. 更新设置软件包：

```
# yum update ovirt-*setup* rh-*vm-setup-plugins
```

3. 使用 `engine-setup` 脚本更新 Red Hat Virtualization Manager。`engine-setup` 脚本会提示您显示一些配置问题，然后停止 `ovirt-engine` 服务，下载并安装更新的软件包，备份和更新数据库，执行安装后配置，以及启动 `ovirt-engine` 服务。

```
# engine-setup
```

当脚本成功完成时，会显示以下信息：

```
Execution of setup completed successfully
```



注意

Red Hat Virtualization Manager 安装过程中也会使用 `engine-setup` 脚本，并存储提供的配置值。在更新过程中，在预览配置时会显示存储的值，如果安装后使用 `engine-config` 更新配置，则可能不会更新。例如，如果在安装后使用 `engine-config` 将 `SANWipeAfterDelete` 更新为 `true`，`engine-setup` 会在配置预览中输出 "Default SAN wipe after delete: False"。但是 `engine-setup` 不会覆盖更新的值。



重要

更新过程可能需要一些时间。在进程完成之前，请勿停止该进程。

4. 更新基本操作系统以及在 **Manager** 中安装的任何可选软件包：

```
# yum update --nobest
```

重要

如果您在更新过程中遇到必要的 **Ansible** 软件包冲突，请参阅在 [RHV 管理器上无法执行 yum update \(ansible 冲突\)](#)。

重要

如果更新了任何内核软件包：

1. 禁用全局维护模式
2. 重启计算机以完成更新。

相关信息

禁用全局维护模式

禁用全局维护模式

流程

1. 登录 **Manager** 虚拟机，并将它关闭。
2. 登录到自托管引擎节点之一并禁用全局维护模式：

```
# hosted-engine --set-maintenance --mode=none
```

当您退出全局维护模式时，**ovirt-ha-agent** 会启动 **Manager** 虚拟机，然后 **Manager** 会自动启动。管理器最多可能需要十分钟才能启动。

3. 确认环境正在运行：

```
# hosted-engine --vm-status
```

列出的信息包括引擎状态。引擎状态的值应该是：

```
{"health": "good", "vm": "up", "detail": "Up"}
```



注意

当虚拟机仍在引导且管理器尚未启动时，引擎状态为：

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

如果发生这种情况，请等待几分钟后重试。

3.1.9. 在自托管引擎中更改 Manager 的 FQDN

您可以使用 `ovirt-engine-rename` 命令更新 Manager 的完全限定域名(FQDN)的记录。

详情请查看使用 [Ovirt Engine Rename 工具重新创建管理器](#)。

3.2. 备份和迁移

3.2.1. 备份和恢复 Red Hat Virtualization Manager

3.2.1.1. 备份 Red Hat Virtualization Manager - 概述

使用 `engine-backup` 工具对 Red Hat Virtualization Manager 进行定期备份。工具会将引擎数据库和配置文件备份到一个文件中，并可在不中断 `ovirt-engine` 服务的情况下运行。

3.2.1.2. `engine-backup` 命令的语法

`engine-backup` 命令以两种基本模式之一工作：

```
# engine-backup --mode=backup
```

```
# engine-backup --mode=restore
```

这两个模式由一组选项进一步扩展，允许您指定 **engine** 数据库的备份范围和不同凭证。运行 **engine-backup --help** 以获得选项及其功能的完整列表。

基本选项

--mode

指定命令是否执行备份操作还是恢复操作。可用的选项有：**backup**（默认）、**恢复**，并**验证**。您必须为 **验证** 或 **恢复操作** 定义 **mode** 选项。

--file

指定保存到备份模式的文件的路径和名称（例如 *file_name.backup*），并在恢复模式中作为备份数据读取。该路径默认定义为 */var/lib/ovirt-engine-backup/*。

--log

指定写入备份或恢复操作的文件的路径和名称（例如：*log_file_name*）。该路径默认定义为 */var/log/ovirt-engine-backup/*。

--scope

指定 **backup** 或 **restore** 操作的范围。有四个选项：**all**，用于备份或恢复所有数据库和配置数据（默认设置）；**文件**，仅备份或恢复系统上的文件；**db**，仅备份或恢复管理器数据库；以及 **dwhdb**，仅备份或恢复数据仓库数据库。

在同一个 **engine-backup** 命令中可以多次指定 **--scope** 选项。

Manager 数据库选项

仅当在 **restore** 模式中使用 **engine-backup** 命令时，以下选项才可用。以下选项语法适用于恢复管理器数据库。同一选项可用于恢复数据仓库数据库。如需数据仓库选项语法，请参阅 **engine-backup --help**。

--provision-db

创建供要恢复到的 Manager 数据库备份的 PostgreSQL 数据库。当在远程主机上恢复备份或全新安装时，需要这个选项，如果没有配置 PostgreSQL 数据库。当在恢复模式中使用此选项时，默认添加 **--restore-permissions** 选项。

--provision-all-databases

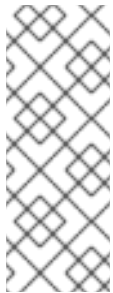
为存档中包含的所有内存转储创建数据库。启用后，这是默认设置。

--change-db-credentials

允许您指定备用凭证，以便使用备份本身中存储的凭据来恢复 **Manager** 数据库。有关这个选项所需的附加参数，请参阅 **engine-backup --help**。

--restore-permissions 或 **--no-restore-permissions**

恢复或不会恢复数据库用户权限。恢复备份时需要其中一个选项。当在恢复模式中使用 **--provision 598** 选项时，默认应用 **--restore-permissions**。



注意

如果备份包含额外的数据库用户，请使用 **--restore-permissions** 和 **--provision-db**（或 **--provision-dwh-db**）选项恢复备份，则创建具有随机密码的额外用户。如果额外用户需要访问恢复的系统，则必须手动更改这些密码。请参阅 [如何在从备份中恢复 Red Hat Virtualization 后向额外数据库用户授予访问权限](#)。

3.2.1.3. 使用 **engine-backup** 命令创建备份

在 **Manager** 处于活跃状态时，您可以使用 **engine-backup** 命令备份 Red Hat Virtualization **Manager**。在 **--scope** 选项中附加以下值之一以指定您要备份的内容：

all

管理器上所有数据库和配置文件的完整备份。这是 **--scope** 选项的默认设置。

files

仅备份系统中的文件

db

仅 **Manager** 数据库的备份

dwhdb

仅 **Data Warehouse** 数据库的备份

cinderlibdb

仅备份 Cinderlib 数据库

grafanadb

仅 Grafana 数据库的备份

您可以多次指定 `--scope` 选项。

您还可以配置 `engine-backup` 命令来备份其他文件。它恢复了它备份的所有信息。



重要

要将数据库恢复到 Red Hat Virtualization Manager 的全新安装，只需要一个数据库备份是不够的。管理器还需要访问配置文件。如果指定除了 `所有` 之外的范围，还必须包含 `--scope=files` 或备份文件系统。

有关 `engine-backup` 命令的完整说明，在 Manager 机器上输入 `engine-backup --help`。

流程

1. 登录到 Manager 机器。
2. 创建备份：

```
# engine-backup
```

默认情况下不应用以下设置：

```
--scope=all
```

```
--mode=backup
```

该命令在 `/var/lib/ovirt-engine-backup/file_name.backup` 中生成备份，以及 `/var/log/ovirt-engine-backup/log_file_name` 中的日志文件。

使用 `file_name.tar` 恢复环境。

以下示例演示了几个不同的备份场景。

例 3.1. 完整备份

```
# engine-backup
```

例 3.2. Manager 数据库备份

```
# engine-backup --scope=files --scope=db
```

例 3.3. Data Warehouse 数据库备份

```
# engine-backup --scope=files --scope=dwhdb
```

例 3.4. 在备份中添加特定文件

1.

创建一个目录来存储 `engine-backup` 命令的配置自定义：

```
# mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d
```

2.

在新目录中创建一个名为 `ntp-chrony.sh` 的文本文件，其内容如下：

```
BACKUP_PATHS="${BACKUP_PATHS}  
/etc/chrony.conf  
/etc/ntp.conf  
/etc/ovirt-engine-backup"
```

3.

运行 `engine-backup` 命令时，请使用 `--scope=files`。备份和恢复包括 `/etc/chrony.conf`、`/etc/ntp.conf` 和 `/etc/ovirt-engine-backup`。

3.2.1.4. 使用 `engine-backup` 命令恢复备份

使用 `engine-backup` 命令恢复备份涉及更多步骤，而不是根据恢复的目的来创建备份。例如，`engine-backup` 命令可用于将备份恢复到 Red Hat Virtualization 的全新安装、现有 Red Hat Virtualization 安装之上，以及使用本地或远程数据库。



重要

用于恢复备份的 Red Hat Virtualization Manager（如 4.4.8）的版本必须早于或等于用于创建备份的 Red Hat Virtualization Manager 版本（如 4.4.7）。从 Red Hat Virtualization 4.4.7 开始，这个策略被 `engine-backup` 命令强制使用。要查看备份文件中所含的 Red Hat Virtualization 版本，请解压缩备份文件并在解压缩文件的根目录中的 `version` 文件中读取值。

3.2.1.5. 将备份恢复到刷新安装

`engine-backup` 命令可用于将备份恢复到 Red Hat Virtualization Manager 的全新安装。以下流程必须在安装基础操作系统以及安装了 Red Hat Virtualization Manager 所需的软件包的机器上执行，但尚未运行 `engine-setup` 命令。此流程假定可以从要恢复备份的机器中访问备份文件或文件。

流程

1. 登录到 Manager 机器。如果您要将引擎数据库恢复到远程主机，您将需要登录 并对该主机执行相关的操作。同样，如果也将数据仓库恢复到远程主机，您将需要登录到该主机上的相关操作。

2. 恢复完整备份或仅数据库备份。



恢复完整备份：

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db
```

当在恢复 模式中使用 `--provision 598` 选项时，默认应用 `--restore-permissions`。

如果 Data Warehouse 也作为完整备份的一部分恢复，请置备额外的数据库：

```
engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db --provision-dwh-db
```


- 通过恢复配置文件和数据库备份来恢复仅数据库备份：

```
# engine-backup --mode=restore --scope=files --scope=db --file=file_name --
log=log_file_name --provision-db
```

上例恢复 Manager 数据库的备份。

```
# engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --
log=log_file_name --provision-dwh-db
```

上面的示例恢复数据仓库数据库的备份。

如果成功，则会显示以下输出：

```
You should now run engine-setup.
Done.
```

3. 运行以下命令并按照提示配置恢复的 Manager:

```
# engine-setup
```

Red Hat Virtualization Manager 已恢复到备份中保留的版本。要更改新 Red Hat Virtualization 系统的完全限定域名，请参阅 [oVirt Engine Rename Tool](#)。

3.2.1.6. 恢复备份以覆盖现有安装

`engine-backup` 命令可以将备份恢复到已安装并设置了 Red Hat Virtualization Manager 的机器。当您进行环境备份后，在该环境中执行更改，然后希望通过从备份中恢复环境来撤销更改，这将非常有用。

因为备份进行了备份，如添加或删除主机后对环境所做的更改将不会出现在恢复的环境中。您必须恢复这些更改。

流程

1. 登录到 Manager 机器。

2. 删除配置文件并清理与 **Manager** 关联的数据库：

```
# engine-cleanup
```

engine-cleanup 命令只清理 **Manager** 数据库；它不会丢弃数据库或删除拥有该数据库的用户。

3. 恢复完整备份或仅数据库备份。您不需要创建新数据库或指定数据库凭据，因为用户和数据库已经存在。

- 恢复完整备份：

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --restore-permissions
```

- 通过恢复配置文件和数据库备份来恢复仅数据库备份：

```
# engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=file_name --log=log_file_name --restore-permissions
```



注意

要只恢复 **Manager** 数据库（例如，如果 **Data Warehouse** 数据库位于另一台机器上），您可以省略 `--scope=dwhdb` 参数。

如果成功，则会显示以下输出：

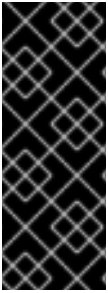
```
You should now run engine-setup.  
Done.
```

4. 重新配置管理器：

```
# engine-setup
```

3.2.1.7. 使用不同凭证恢复备份

engine-backup 命令可以将备份恢复到已安装并设置了 Red Hat Virtualization Manager 的机器，但备份中数据库的凭证与要恢复备份的机器中的数据库不同。当您进行安装备份并希望从备份恢复到不同系统时，这非常有用。



重要

当恢复备份以覆盖现有安装时，您必须运行 **engine-cleanup** 命令来清理现有安装，然后才能使用 **engine-backup** 命令。**engine-cleanup** 命令只清理 **engine** 数据库，不会丢弃数据库或删除拥有该数据库的用户。因此，您不需要创建新数据库或指定数据库凭证。但是，如果引擎数据库所有者的凭据未知，则必须在恢复备份前更改它们。

流程

1. 登录到 Red Hat Virtualization Manager 机器。
2. 运行以下命令并按照提示删除管理器的配置文件并清理管理器的数据库：

```
# engine-cleanup
```

3. 如果该用户的凭据未知，则更改引擎数据库所有者的密码：

- a. 输入 **postgresql** 命令行：

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

- b. 更改拥有引擎数据库的用户的密码：

```
postgres=# alter role user_name encrypted password 'new_password';
```

如果需要，为拥有 **ovirt_engine_history** 数据库的用户重复此操作。

4. 使用 **--change-db-credentials** 参数恢复完整备份或仅数据库备份，以传递新数据库的凭证。数据库的 **database_location** 于管理器本地，是 **localhost**。



注意

以下示例在不指定密码的情况下为每个数据库使用 `--*password` 选项，该选项会提示输入每个数据库的密码。另外，您还可以为每个数据库使用 `--*passfile=password_file` 选项，安全地将密码传递给 `engine-backup` 工具，而无需交互式提示。

- 恢复完整备份：

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --no-restore-permissions
```

如果 Data Warehouse 也作为完整备份的一部分恢复，包括修订额外数据库的凭证：

```
engine-backup --mode=restore --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --change-dwh-db-credentials --dwh-db-host=database_location --dwh-db-name=database_name --dwh-db-user=ovirt_engine_history --dwh-db-password --no-restore-permissions
```

- 通过恢复配置文件和数据库备份来恢复仅数据库备份：

```
# engine-backup --mode=restore --scope=files --scope=db --file=file_name --log=log_file_name --change-db-credentials --db-host=database_location --db-name=database_name --db-user=engine --db-password --no-restore-permissions
```

上例恢复 Manager 数据库的备份。

```
# engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --log=log_file_name --change-dwh-db-credentials --dwh-db-host=database_location --dwh-db-name=database_name --dwh-db-user=ovirt_engine_history --dwh-db-password --no-restore-permissions
```

上面的示例恢复数据仓库数据库的备份。

如果成功，则会显示以下输出：

```
You should now run engine-setup.
Done.
```

5. 运行以下命令并按照提示重新配置防火墙并确保正确配置了 `ovirt-engine` 服务：

```
# engine-setup
```

3.2.1.8. 备份和恢复自托管引擎

您可以备份自托管引擎，并在新的自托管环境中恢复它。对于诸如将环境迁移到具有不同存储类型的新自托管引擎存储域等任务使用这个步骤。

当您在部署期间指定备份文件时，备份会在新的 `Manager` 虚拟机上恢复，并带有新的自托管引擎存储域。旧的 `Manager` 被移除，旧的自托管引擎存储域被重命名，您可以在确认新环境正常工作后手动删除。强烈建议在新的主机上部署；如果在备份环境中存在用于部署的主机，它将从恢复的数据库中删除，以避免新环境中的冲突。如果部署到新主机上，则必须为主机分配唯一名称。重新利用备份中包含的现有主机的名称可能会导致新环境中的冲突。

备份和恢复操作涉及以下密钥操作：

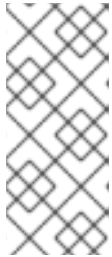
1. 使用 `engine-backup` 工具备份原始管理器。
2. 部署新的自托管引擎并恢复备份。
3. 在新 `Manager` 虚拟机上启用 `Manager` 存储库。
4. 重新安装自托管引擎节点以更新其配置。
5. 删除旧的自托管引擎存储域。

这个过程假设您可以访问，并可更改原始 `Manager`。

前提条件

- 为 `Manager` 和主机准备的完全限定域名。正向和反向查找记录必须在 `DNS` 中设置。新管理器必须与原始 `Manager` 具有相同的完全限定域名。

- 原始管理器必须更新至最新的次版本。用于恢复备份的 Red Hat Virtualization Manager (如 4.4.8) 的版本必须早于或等于用于创建备份的 Red Hat Virtualization Manager 版本 (如 4.4.7)。从 Red Hat Virtualization 4.4.7 开始, 这个策略被 `engine-backup` 命令强制使用。请参阅 [升级指南](#) 中的 [更新 Red Hat Virtualization Manager](#)。



注意

如果您需要恢复备份, 但没有新的设备, 恢复过程将暂停, 您可以通过 SSH 登录临时管理器机器, 根据需要注册、注册、订阅或配置频道, 然后在恢复过程恢复过程前升级 Manager 软件包。

- 数据中心兼容性级别必须设置为最新版本, 以确保与更新的存储版本兼容。
- 环境中必须至少有一个常规主机。此主机 (以及任何其他常规主机) 将保持活动状态, 以托管 SPM 角色和任何正在运行的虚拟机。如果常规主机尚不是 SPM, 请在创建备份之前移动 SPM 角色, 方法是选择常规主机并单击 **Management** → **Select as SPM**。

如果没有可用的常规主机, 可以通过两种方式来添加:

- 从节点中删除自托管引擎配置 (但不从环境中删除该节点)。请参阅 [从自托管引擎环境中删除主机](#)。
- 添加新的常规主机。请参阅 [将标准主机添加到 Manager 主机任务](#)。

3.2.1.8.1. 备份原始管理器

使用 `engine-backup` 命令备份原始管理器, 并将备份文件复制到单独的位置, 以便可在进程的任意时间点上访问该文件。

有关 `engine-backup --mode=backup` 选项的更多信息, 请参阅 [管理指南](#) 中的 [备份和恢复 Red Hat Virtualization Manager](#)。

流程

1. 登录到一个自托管引擎节点, 并将环境移到全局维护模式:

```
# hosted-engine --set-maintenance --mode=global
```

2.

登录到原始 Manager 并停止 ovirt-engine 服务：

```
# systemctl stop ovirt-engine
# systemctl disable ovirt-engine
```



注意

虽然禁止运行原始管理器，但建议不要对环境进行更改，因为它在创建备份后不会对环境进行任何更改。此外，它还会阻止原始管理器和新管理器同时管理现有资源。

3.

运行 `engine-backup` 命令，指定要创建的备份文件的名称，以及要存储备份日志的日志文件名称：

```
# engine-backup --mode=backup --file=file_name --log=log_file_name
```

4.

将文件复制到外部服务器。在以下示例中，`storage.example.com` 是网络存储服务器的完全限定域名，它将存储备份直到需要，`/backup/` 是任何指定的文件夹或路径。

```
# scp -p file_name log_file_name storage.example.com:/backup/
```

5.

如果您不要求 Manager 机器用于其他目的，请从 Red Hat Subscription Manager 中取消注册它：

```
# subscription-manager unregister
```

6.

登录到其中一个自托管引擎节点并关闭原始 Manager 虚拟机：

```
# hosted-engine --vm-shutdown
```

备份管理器后，部署新的自托管引擎并在新虚拟机上恢复备份。

3.2.1.8.2. 在新的自托管引擎中恢复备份

在新主机上运行 `hosted-engine` 脚本，并使用 `--restore-from-file=path/to/file_name` 选项在部署期

间恢复 Manager 备份。

重要

如果您使用 iSCSI 存储，且您的 iSCSI 目标根据启动器的 ACL 过滤连接，则部署可能会失败，并显示 `STORAGE_DOMAIN_UNREACHABLE` 错误。要防止这种情况，您必须在开始自托管引擎部署前更新 iSCSI 配置：

- 如果要在现有主机上重新部署，您必须更新 `/etc/iscsi/initiatorname.iscsi` 中的主机的 iSCSI 启动器设置。initiator IQN 必须与之前在 iSCSI 目标中映射的相同，或者更新至一个新的 IQN（如果适用）。
- 如果要在全新的主机上部署，您必须更新 iSCSI 目标配置以接受来自该主机的连接。

请注意，IQN 可以在主机端（iSCSI 启动器）或存储侧（iSCSI 目标）上更新。

流程

1. 将备份文件复制到新主机。在以下示例中，`host.example.com` 是主机的 FQDN，`/backup/` 是任何指定的文件夹或路径。

```
# scp -p file_name host.example.com:/backup/
```

2. 登录新主机。

3. 如果在 Red Hat Virtualization Host 上部署，则 `ovirt-hosted-engine-setup` 已安装，因此可以跳过这一步。如果要在 Red Hat Enterprise Linux 上部署，请安装 `ovirt-hosted-engine-setup` 软件包：

```
# dnf install ovirt-hosted-engine-setup
```

4. 使用 `tmux` 窗口管理器运行脚本，以避免在出现网络或终端中断时丢失会话。

安装并运行 `tmux`：


```
# dnf -y install tmux
# tmux
```

5. 运行 `hosted-engine` 脚本，指定到备份文件的路径：

```
# hosted-engine --deploy --restore-from-file=backup/file_name
```

要随时转义脚本，请使用 `CTRL+D` 中止部署。

6. 选择 **Yes** 以开始部署。

7. 配置网络。脚本会检测可能的 `NIC`，以用作环境的管理网桥。

8. 如果要使用自定义设备进行虚拟机安装，请输入 `OVA` 存档的路径。否则，将此字段留空，以使用 `RHV-M Appliance`。

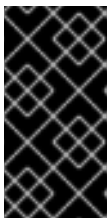
9. 输入 `Manager` 的 `root` 密码。

10. 输入可让您以 `root` 用户身份登录 `Manager` 的 `SSH` 公钥，并指定是否为 `root` 用户启用 `SSH` 访问。

11. 输入虚拟机的 `CPU` 和内存配置。

12. 输入 `Manager` 虚拟机的 `MAC` 地址，或接受随机生成的地址。如果要通过 `DHCP` 为 `Manager` 虚拟机提供 `IP` 地址，请确保此 `MAC` 地址具有有效的 `DHCP` 保留。部署脚本将不会为您配置 `DHCP` 服务器。

13. 输入虚拟机的网络详情。如果指定了 `Static`，请输入 `Manager` 的 `IP` 地址。



重要

静态 `IP` 地址必须属于与主机相同的子网。例如，如果主机在 `10.1.1.0/24` 中，则管理器虚拟机的 `IP` 必须位于同一子网范围 (`10.1.1.1-254/24`) 中。

14.

指定是否将 **Manager 虚拟机** 和基础主机的条目添加到虚拟机的 `/etc/hosts` 文件中。您必须确保主机名可以被解析。

15.

提供 **SMTP 服务器** 的名称和 **TCP 端口号**、用于发送电子邮件通知的电子邮件地址，以及用于接收这些通知的电子邮件地址列表：

16.

输入 `admin@internal` 用户的密码来访问管理门户。

该脚本将创建虚拟机。如果需要安装 **RHV-M** 设备，这可能需要一些时间。

注意

如果主机无法正常工作，因为缺少所需的网络或类似问题，部署会暂停并显示以下消息：

```
[ INFO ] You can now connect to https://<host name>:6900/ovirt-engine/ and
check the status of this host and eventually remediate it, please continue only
when the host is listed as 'up'
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks]
[ INFO ] ok: [localhost]
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary lock file]
[ INFO ] changed: [localhost]
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution until
/tmp/ansible.<random>_he_setup_lock is removed, delete it once ready to
proceed]
```

暂停进程允许您：

- 使用提供的 **URL** 连接到管理门户。
- 评估该情况，了解主机无法正常运行的原因，并进行修改。例如，如果此部署从备份中恢复，且主机集群包含的备份包含主机集群所需的网络，则配置网络，将相关主机 **NIC** 附加到这些网络。
- 一旦一切正常，主机状态为 **Up**，删除上述消息中显示的锁定文件。部署将继续。

17.

选择要使用的存储类型：

- 对于 NFS，请输入版本、完整地址和到存储的路径以及所有挂载选项。



警告

不要为新存储域使用旧的自托管引擎存储域挂载点，因为您面临丢失虚拟机数据的风险。

- 对于 iSCSI，请输入门户详情并从自动检测的列表中选择目标和 LUN。您只能在部署期间选择一个 iSCSI 目标，但支持多路径连接同一门户组的所有门户。



注意

要指定多个 iSCSI 目标，您必须先启用多路径，然后才能部署自托管引擎。详情请查看 [Red Hat Enterprise Linux DM 多路径](#)。另外，还有一个[多路径帮助程序工具](#)，它生成脚本来安装和配置使用不同选项的多路径。

- 对于 Gluster 存储，请输入到存储的完整地址和路径，以及任何挂载选项。



警告

不要为新存储域使用旧的自托管引擎存储域挂载点，因为您面临丢失虚拟机数据的风险。

**重要**

仅支持副本 1 和副本 3 Gluster 存储。确保您按如下方式配置卷：

```
gluster volume set VOLUME_NAME group virt
gluster volume set VOLUME_NAME performance.strict-o-direct on
gluster volume set VOLUME_NAME network.remote-dio off
gluster volume set VOLUME_NAME storage.owner-uid 36
gluster volume set VOLUME_NAME storage.owner-gid 36
gluster volume set VOLUME_NAME network.ping-timeout 30
```

- 对于光纤通道，从自动检测的列表中选择 LUN。必须配置并连接主机总线适配器，而且 LUN 不得包含任何现有数据。要重复使用现有 LUN，请参阅 [管理指南中的重新使用 LUN](#)。

18.

输入 Manager 磁盘大小。

该脚本会继续，直到部署完成。

19.

部署过程会更改管理器的 SSH 密钥。要允许客户端机器在没有 SSH 错误的情况下访问新管理器，请在访问原始管理器的任何客户端机器上从 `.ssh/known_hosts` 文件中删除原始 Manager 条目。

部署完成后，登录新的 Manager 虚拟机并启用所需的存储库。

3.2.1.8.3. 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**

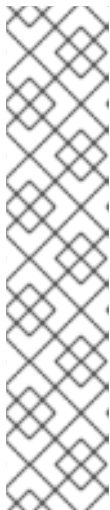
如果您使用 IPv6 网络，请使用 IPv6 转换机制来访问 Content Delivery Network 和 subscription Manager。

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
```

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](#)

现在，管理器及其资源在新的自托管环境中运行。自托管引擎节点必须在 **Manager** 中重新安装，以更新其自托管引擎配置。标准主机不会受到影响。为每个自托管引擎节点执行以下步骤。

3.2.1.8.4. 重新安装主机

从管理门户重新安装 Red Hat Virtualization 主机(RHVM)和 Red Hat Enterprise Linux 主机。该流

程包括停止和重启主机。



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。

前提条件

- 如果集群启用了迁移，虚拟机可以自动迁移到集群中的另一台主机。因此，在主机使用量相对较低时，重新安装主机。
- 确保集群有足够的内存来执行维护。如果集群缺少内存，迁移虚拟机将挂起，然后失败。要减少内存用量，请在将主机移至维护之前关闭部分或所有虚拟机。
- 在执行重新安装前，请确保集群包含多个主机。不要尝试同时重新安装所有主机。个主机必须保持可用才能执行存储池管理程序(SPM)任务。

流程

1. 单击 **Compute** → **Hosts**，再选择 主机。
2. 点 **Management** → **Maintenance** 和 **OK**。
3. 点 **Installation** → **Reinstall**。这将打开 **Install Host** 窗口。
4. 单击 **Hosted Engine** 选项卡，再从下拉菜单中选择 **DEPLOY**。
5. 单击 **确定** 以 重新安装主机。

重新安装主机并将其状态返回到 **启动** 后，您可以将虚拟机迁移到主机。



重要

将 Red Hat Virtualization Host 注册到 Red Hat Virtualization Manager 并重新安装它后，管理门户可能会错误地将其状态显示为 **Install Failed**。单击 **Management** → **Activate**，主机将更改为 **Up** 状态并可供使用。

在重新安装自托管引擎节点后，您可以通过在其中一个节点上运行以下命令来检查新环境的状态：

```
# hosted-engine --vm-status
```

在恢复过程中，旧的自托管引擎存储域被重命名为，在恢复错误时不会从新环境中删除。确认环境正常运行后，您可以删除旧的自托管引擎存储域。

3.2.1.8.5. 删除存储域

在您的数据中心中有一个要从虚拟环境中删除的存储域。

流程

1. 单击 **Storage** → **Domains**。
2. 将存储域移到维护模式并分离它：
 - a. 单击存储域的名称。这会打开详情视图。
 - b. 单击 **Data Center** 选项卡。
 - c. 单击 **Maintenance**，然后单击 **OK**。
 - d. 单击 **Detach**，然后单击 **确定**。

3. 单击 **Remove**。
4. (可选) 选择 **格式化域**，即存储内容将丢失！复选框可清除域的内容。
5. 单击 **OK**。

存储域已从环境中永久移除。

3.2.1.9. 从现有的备份中恢复自托管引擎

如果由于无法修复的问题而出现自托管引擎不可用，您可以在新的自托管环境中使用在问题开始前的备份将其恢复（如果可用）。

当您在部署期间指定备份文件时，备份会在新的 **Manager** 虚拟机上恢复，并带有新的自托管引擎存储域。旧的 **Manager** 被移除，旧的自托管引擎存储域被重命名，您可以在确认新环境正常工作后手动删除。强烈建议在新的主机上部署；如果在备份环境中存在用于部署的主机，它将从恢复的数据库中删除，以避免新环境中的冲突。如果部署到新主机上，则必须为主机分配唯一名称。重新利用备份中包含的现有主机的名称可能会导致新环境中的冲突。

恢复自托管引擎涉及以下关键操作：

1. 部署新的自托管引擎并恢复备份。
2. 在新 **Manager** 虚拟机上启用 **Manager** 存储库。
3. 重新安装自托管引擎节点以更新其配置。
4. 删除旧的自托管引擎存储域。

此流程假设您无法访问原始管理器，并且新主机可以访问备份文件。

前提条件

- 为 **Manager** 和主机准备的完全限定域名。正向和反向查找记录必须在 **DNS** 中设置。新管理器必须与原始 **Manager** 具有相同的完全限定域名。

3.2.1.9.1. 在新的自托管引擎中恢复备份

在新主机上运行 `hosted-engine` 脚本，并使用 `--restore-from-file=path/to/file_name` 选项在部署期间恢复 **Manager** 备份。

重要

如果您使用 **iSCSI** 存储，且您的 **iSCSI** 目标根据启动器的 **ACL** 过滤连接，则部署可能会失败，并显示 `STORAGE_DOMAIN_UNREACHABLE` 错误。要防止这种情况，您必须在开始自托管引擎部署前更新 **iSCSI** 配置：

- 如果要在现有主机上重新部署，您必须更新 `/etc/iscsi/initiatorname.iscsi` 中的主机的 **iSCSI** 启动器设置。initiator IQN 必须与之前在 **iSCSI** 目标中映射的相同，或者更新至一个新的 IQN（如果适用）。
- 如果要在全新的主机上部署，您必须更新 **iSCSI** 目标配置以接受来自该主机的连接。

请注意，IQN 可以在主机端（**iSCSI** 启动器）或存储侧（**iSCSI** 目标）上更新。

流程

1. 将备份文件复制到新主机。在以下示例中，`host.example.com` 是主机的 FQDN，`/backup/` 是任何指定的文件夹或路径。

```
# scp -p file_name host.example.com:/backup/
```

2. 登录新主机。

3. 如果在 **Red Hat Virtualization Host** 上部署，则 `ovirt-hosted-engine-setup` 已安装，因此可以跳过这一步。如果要在 **Red Hat Enterprise Linux** 上部署，请安装 `ovirt-hosted-engine-setup` 软件包：

```
# dnf install ovirt-hosted-engine-setup
```

4. 使用 **tmux** 窗口管理器运行脚本，以避免在出现网络或终端中断时丢失会话。

安装并运行 **tmux** ：

```
# dnf -y install tmux
# tmux
```

5. 运行 **hosted-engine** 脚本，指定到备份文件的路径：

```
# hosted-engine --deploy --restore-from-file=backup/file_name
```

要随时转义脚本，请使用 **CTRL+D** 中止部署。

6. 选择 **Yes** 以开始部署。

7. 配置网络。脚本会检测可能的 **NIC**，以用作环境的管理网桥。

8. 如果要使用自定义设备进行虚拟机安装，请输入 **OVA** 存档的路径。否则，将此字段留空，以使用 **RHV-M Appliance**。

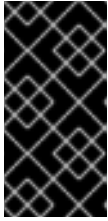
9. 输入 **Manager** 的 **root** 密码。

10. 输入可让您以 **root** 用户身份登录 **Manager** 的 **SSH** 公钥，并指定是否为 **root** 用户启用 **SSH** 访问。

11. 输入虚拟机的 **CPU** 和内存配置。

12. 输入 **Manager** 虚拟机的 **MAC** 地址，或接受随机生成的地址。如果要通过 **DHCP** 为 **Manager** 虚拟机提供 **IP** 地址，请确保此 **MAC** 地址具有有效的 **DHCP** 保留。部署脚本将不会为您配置 **DHCP** 服务器。

13. 输入虚拟机的网络详情。如果指定了 **Static**，请输入 **Manager** 的 **IP** 地址。

**重要**

静态 IP 地址必须属于与主机相同的子网。例如，如果主机在 10.1.1.0/24 中，则管理器虚拟机的 IP 必须位于同一子网范围 (10.1.1.1-254/24) 中。

14. **指定是否将 Manager 虚拟机和基础主机的条目添加到虚拟机的 /etc/hosts 文件中。您必须确保主机名可以被解析。**

15. **提供 SMTP 服务器的名称和 TCP 端口号、用于发送电子邮件通知的电子邮件地址，以及用于接收这些通知的电子邮件地址列表：**

16. **输入 admin@internal 用户的密码来访问管理门户。**

该脚本将创建虚拟机。如果需要安装 RHV-M 设备，这可能需要一些时间。

注意

如果主机无法正常工作，因为缺少所需的网络或类似问题，部署会暂停并显示以下消息：

```
[ INFO ] You can now connect to https://<host name>:6900/ovirt-engine/ and
check the status of this host and eventually remediate it, please continue only
when the host is listed as 'up'
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks]
[ INFO ] ok: [localhost]
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary lock file]
[ INFO ] changed: [localhost]
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution until
/tmp/ansible.<random>_he_setup_lock is removed, delete it once ready to
proceed]
```

暂停进程允许您：

- 使用提供的 URL 连接到管理门户。
- 评估该情况，了解主机无法正常运行的原因，并进行修改。例如，如果此部署从备份中恢复，且主机集群包含的备份包含主机集群所需的网络，则配置网络，将相关主机 NIC 附加到这些网络。
- 一旦一切正常，主机状态为 *Up*，删除上述消息中显示的锁定文件。部署将继续。

17.

选择要使用的存储类型：

- 对于 NFS，请输入版本、完整地址和到存储的路径以及所有挂载选项。

**警告**

不要为新存储域使用旧的自托管引擎存储域挂载点，因为您面临丢失虚拟机数据的风险。

- 对于 iSCSI，请输入门户详情并从自动检测的列表中选择目标和 LUN。您只能在部署期间选择一个 iSCSI 目标，但支持多路径连接同一门户组的所有门户。



注意

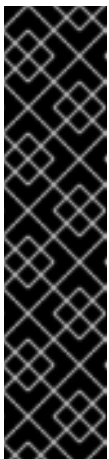
要指定多个 iSCSI 目标，您必须先启用多路径，然后才能部署自托管引擎。详情请查看 [Red Hat Enterprise Linux DM 多路径](#)。另外，还有一个[多路径帮助程序工具](#)，它生成脚本来安装和配置使用不同选项的多路径。

- 对于 Gluster 存储，请输入到存储的完整地址和路径，以及任何挂载选项。



警告

不要为新存储域使用旧的自托管引擎存储域挂载点，因为您面临丢失虚拟机数据的风险。



重要

仅支持副本 1 和副本 3 Gluster 存储。确保您按如下方式配置卷：

```
gluster volume set VOLUME_NAME group virt
gluster volume set VOLUME_NAME performance.strict-o-direct on
gluster volume set VOLUME_NAME network.remote-dio off
gluster volume set VOLUME_NAME storage.owner-uid 36
gluster volume set VOLUME_NAME storage.owner-gid 36
gluster volume set VOLUME_NAME network.ping-timeout 30
```

- 对于光纤通道，从自动检测的列表中选择 LUN。必须配置并连接主机总线适配器，而且 LUN 不得包含任何现有数据。要重复使用现有 LUN，请参阅[管理指南中的重新使用 LUN](#)。

18. 输入 Manager 磁盘大小。

该脚本会继续，直到部署完成。

19.

部署过程会更改管理器的 SSH 密钥。要允许客户端机器在没有 SSH 错误的情况下访问新管理器，请在访问原始管理器的任何客户端机器上从 `.ssh/known_hosts` 文件中删除原始 Manager 条目。

部署完成后，登录新的 Manager 虚拟机并启用所需的存储库。

3.2.1.9.2. 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
```

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](#)

现在，管理器及其资源在新的自托管环境中运行。自托管引擎节点必须在 **Manager** 中重新安装，以更新其自托管引擎配置。标准主机不会受到影响。为每个自托管引擎节点执行以下步骤。

3.2.1.9.3. 重新安装主机

从管理门户重新安装 Red Hat Virtualization 主机(RHVH)和 Red Hat Enterprise Linux 主机。该流程包括停止和重启主机。



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。

前提条件

-

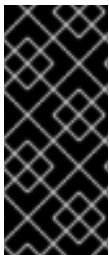
如果集群启用了迁移，虚拟机可以自动迁移到集群中的另一台主机。因此，在主机使用量相对较低时，重新安装主机。

- 确保集群有足够的内存来执行维护。如果集群缺少内存，迁移虚拟机将挂起，然后失败。要减少内存用量，请在将主机移至维护之前关闭部分或所有虚拟机。
- 在执行重新安装前，请确保集群包含多个主机。不要尝试同时重新安装所有主机。个主机必须保持可用才能执行存储池管理程序(SPM)任务。

流程

1. 单击 **Compute** → **Hosts**，再选择 主机。
2. 单击 **Management** → **Maintenance** 和 **OK**。
3. 单击 **Installation** → **Reinstall**。这将打开 **Install Host** 窗口。
4. 单击 **Hosted Engine** 选项卡，再从下拉菜单中选择 **DEPLOY**。
5. 单击 **确定** 以重新安装主机。

重新安装主机并将其状态返回到 **启动** 后，您可以将虚拟机迁移到主机。



重要

将 Red Hat Virtualization Host 注册到 Red Hat Virtualization Manager 并重新安装它后，管理门户可能会错误地将其状态显示为 **Install Failed**。单击 **Management** → **Activate**，主机将更改为 **Up** 状态并可供使用。

在重新安装自托管引擎节点后，您可以通过在其中一个节点上运行以下命令来检查新环境的状态：

```
# hosted-engine --vm-status
```

在恢复过程中，旧的自托管引擎存储域被重命名为，在恢复错误时不会从新环境中删除。确认环境正常运行后，您可以删除旧的自托管引擎存储域。

3.2.1.9.4. 删除存储域

在您的数据中心中有一个要从虚拟环境中删除的存储域。

流程

1. 点 **Storage** → **Domains**。
2. 将存储域移到维护模式并分离它：
 - a. 点存储域的名称。这会打开详情视图。
 - b. 点 **Data Center** 选项卡。
 - c. 单击 **Maintenance**，然后单击 **OK**。
 - d. 单击 **Detach**，然后单击确定。
3. 单击 **Remove**。
4. (可选) 选择 **格式化域**，即存储内容将丢失！复选框可清除域的内容。
5. 单击 **OK**。

存储域已从环境中永久移除。

3.2.1.10. 从现有的备份覆盖自托管引擎

如果自托管引擎可以访问，但遇到数据库崩溃等问题，或者难以回滚的配置错误，您可以使用在问题

开始前的备份恢复到之前的状态。

恢复自托管引擎之前的状态涉及以下步骤：

1. 将环境置于全局维护模式。
2. 在 **Manager** 虚拟机上恢复备份。
3. 禁用全局维护模式。

有关 `engine-backup --mode=restore` 选项的更多信息，请参阅 [备份和恢复管理器](#)。

3.2.1.10.1. 启用全局维护模式

您必须将自托管引擎环境置于全局维护模式，然后才能在 **Manager** 虚拟机上执行任何设置或升级任务。

流程

1. 登录到自托管引擎节点并启用全局维护模式：

```
# hosted-engine --set-maintenance --mode=global
```

2. 在继续前确认环境处于全局维护模式：

```
# hosted-engine --vm-status
```

您应该会看到指示集群处于全局维护模式的消息。

3.2.1.10.2. 恢复备份以覆盖现有安装

`engine-backup` 命令可以将备份恢复到已安装并设置了 Red Hat Virtualization Manager 的机器。当您进行环境备份后，在该环境中执行更改，然后希望通过从备份中恢复环境来撤销更改，这将非常有用。

因为备份进行了备份，如添加或删除主机后对环境所做的更改将不会出现在恢复的环境中。您必须恢复这些更改。

流程

1. 登录到 Manager 机器。
2. 删除配置文件并清理与 Manager 关联的数据库：

```
# engine-cleanup
```

`engine-cleanup` 命令只清理 Manager 数据库；它不会丢弃数据库或删除拥有该数据库的用户。

3. 恢复完整备份或仅数据库备份。您不需要创建新数据库或指定数据库凭据，因为用户和数据库已经存在。

- 恢复完整备份：

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --restore-permissions
```

- 通过恢复配置文件和数据库备份来恢复仅数据库备份：

```
# engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=file_name --log=log_file_name --restore-permissions
```



注意

要只恢复 Manager 数据库（例如，如果 Data Warehouse 数据库位于另一台机器上），您可以省略 `--scope=dwhdb` 参数。

如果成功，则会显示以下输出：

```
You should now run engine-setup.  
Done.
```

4. **重新配置管理器：**

```
# engine-setup
```

3.2.1.10.3. 禁用全局维护模式

流程

1. **登录 Manager 虚拟机，并将它关闭。**
2. **登录到自托管引擎节点之一并禁用全局维护模式：**

```
# hosted-engine --set-maintenance --mode=none
```

当您退出全局维护模式时，`ovirt-ha-agent` 会启动 **Manager 虚拟机**，然后 **Manager** 会自动启动。管理器最多可能需要十分钟才能启动。

3. **确认环境正在运行：**

```
# hosted-engine --vm-status
```

列出的信息包括引擎状态。引擎状态的值应该是：

```
{"health": "good", "vm": "up", "detail": "Up"}
```

注意

当虚拟机仍在引导且管理器尚未启动时，引擎状态为：

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

如果发生这种情况，请等待几分钟后重试。

当环境再次运行时，您可以启动任何停止的虚拟机，并检查环境中的资源是否如期执行。

3.2.2. 将数据仓库迁移到 9 月的机器

本节论述了如何将数据仓库数据库和服务从 Red Hat Virtualization Manager 机器迁移到单独的机器。在单独的计算机上托管数据仓库服务可减少每台计算机的负载，并避免与其他进程共享 CPU 和内存资源导致的潜在冲突。



注意

红帽只支持安装数据仓库数据库、数据仓库服务和 Grafana，它们都与彼此相同，尽管您可以在独立的机器上分别安装这些组件。

您有以下迁移选项：

- 您可以从管理器计算机迁移数据仓库服务，并将其与现有数据仓库数据库 (ovirt_engine_history) 连接。
- 您可以从 Manager 机器迁移数据仓库数据库，然后迁移数据仓库服务。

3.2.2.1. 将数据仓库数据库迁移到独立机器

在迁移数据仓库服务之前，迁移数据仓库数据库 (ovirt_engine_history)。使用 engine-backup 创建数据库备份，并在新数据库计算机上恢复它。有关 engine-backup 的更多信息，请运行 engine-backup --help。



注意

红帽只支持安装数据仓库数据库、数据仓库服务和 Grafana，它们都与彼此相同，尽管您可以在独立的机器上分别安装这些组件。

新数据库服务器必须安装了 Red Hat Enterprise Linux 8。

在新数据库服务器上启用所需的存储库。

3.2.2.1.1. 启用 Red Hat Virtualization Manager 存储库

您需要使用 Red Hat Subscription Manager 登录并注册数据仓库，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

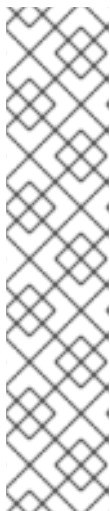
如果您使用 IPv6 网络，请使用 IPv6 转换机制来访问 Content Delivery Network 和 subscription Manager。

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
```

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](#)

3.2.2.1.2. 将数据仓库数据库迁移到独立机器

流程

1. 在 Manager 中创建数据仓库数据库和配置文件的备份：

```
# engine-backup --mode=backup --scope=grafanadb --scope=dwhdb --scope=files --  
file=file_name --log=log_file_name
```

2. 将备份文件从 Manager 复制到新机器：

```
# scp /tmp/file_name root@new.dwh.server.com:/tmp
```

3. 在新机器上安装 engine-backup：

```
# dnf install ovirt-engine-tools-backup
```

4. 安装 PostgreSQL 服务器软件包：

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

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

```
# su - postgres -c 'initdb'  
# systemctl enable postgresql  
# systemctl start postgresql
```

6. 在新计算机上恢复数据仓库数据库。*file_name* 是从 Manager 复制的备份文件。

```
# engine-backup --mode=restore --scope=files --scope=grafanadb --scope=dwhdb --  
file=file_name --log=log_file_name --provision-dwh-db
```

当在恢复模式中使用 `--provision 598` 选项时，默认应用 `--restore-permissions`。

数据仓库数据库现在托管在与管理器托管的独立计算机上。成功恢复数据仓库数据库后，提示您运行 `engine-setup` 命令。在运行此命令之前，请先迁移数据仓库服务。

3.2.2.2. 将数据仓库服务迁移到独立机器

您可以将 Red Hat Virtualization Manager 上安装并配置的数据仓库服务迁移到单独的机器。在单独的计算机上托管数据仓库服务有助于减少管理器计算机上的负载。

请注意，这个过程仅迁移数据仓库服务。

要在迁移数据仓库服务前迁移数据仓库数据库(ovirt_engine_history)，请参阅 [迁移数据仓库数据库到 9 月 9 日](#)。



注意

红帽只支持安装数据仓库数据库、数据仓库服务和 Grafana，它们都与彼此相同，尽管您可以在独立的机器上分别安装这些组件。

前提条件

- 您必须在同一台机器上安装并配置了管理器和数据仓库。
- 要设置新的数据仓库机器，您必须有以下内容：
 - Manager 的 `/etc/ovirt-engine/engine.conf.d/10-setup-database.conf` 文件中的密码。
 - 允许从数据仓库计算机访问 Manager 数据库计算机的 TCP 端口 5432。
 - 数据仓库数据库中的 `/etc/ovirt-engine-dwh/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf` 文件中的用户名和密码。

如果您使用将 [Data Warehouse Database 中的步骤迁移到 9 月 9 日机器](#) 中所述迁移了 `ovirt_engine_history` 数据库，则备份包括该机器上的数据库设置中定义的这些凭证。

安装此场景需要四个步骤：

1. 设置新的数据仓库机器
2. 在管理器机器上停止数据仓库服务
3. 配置新的数据仓库
4. 在 Manager 计算机上禁用数据仓库软件包

3.2.2.2.1. 设置新的数据仓库机器

启用 Red Hat Virtualization 软件仓库并在 Red Hat Enterprise Linux 8 机器上安装数据仓库设置软件包：

1. 启用所需的软件仓库：
 - a. 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
```

- b. 查找 Red Hat Virtualization Manager 订阅池并记录池 ID：

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

- c. 使用池 ID 将订阅附加到系统：

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

- d. 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
```

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

2. 启用 `pki-deps` 模块。

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

3. 确保当前安装的所有软件包都为最新版本：

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

4. 安装 `ovirt-engine-dwh-setup` 软件包：

```
# dnf install ovirt-engine-dwh-setup
```

3.2.2.2.2. 在 Manager 机器上停止数据仓库服务

流程

1. 停止数据仓库服务：

```
# systemctl stop ovirt-engine-dwhd.service
```

2. 如果数据库托管在远程计算机上，您必须通过编辑 `postgres.conf` 文件来手动授予访问权限。编辑 `/var/lib/pgsql/data/postgresql.conf` 文件并修改 `listen_addresses` 行，使其与以下内容匹配：

```
listen_addresses = '*'
```

如果该行不存在或已被注释掉，请手动添加。

如果数据库托管在 Manager 机器上，且是在 Red Hat Virtualization Manager 完全设置过程中配置的，则默认授予访问权限。

3. 重启 `postgresql` 服务：

-

```
# systemctl restart postgresql
```

3.2.2.2.3. 配置新的数据仓库（Data Warehouse 机器）

本节中显示的选项或设置顺序可能因您的环境而异。

1.

如果您要同时将 `ovirt_engine_history` 数据库和数据仓库服务迁移到同一个计算机上，请运行以下命令，否则继续下一步。

```
# sed -i '/^ENGINE_DB_/d' \
    /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf

# sed -i \
    -e 's;^\(OVESETUP_ENGINE_CORE/enable=bool\):True;\1:False;' \
    -e '/^OVESETUP_CONFIG/fqdn/d' \
    /etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

2.

删除 `apache/grafana` PKI 文件，以便 `engine-setup` 使用正确值重新生成这些文件：

```
# rm -f \
    /etc/pki/ovirt-engine/certs/apache.cer \
    /etc/pki/ovirt-engine/certs/apache-grafana.cer \
    /etc/pki/ovirt-engine/keys/apache.key.nopass \
    /etc/pki/ovirt-engine/keys/apache-grafana.key.nopass \
    /etc/pki/ovirt-engine/apache-ca.pem \
    /etc/pki/ovirt-engine/apache-grafana-ca.pem
```

3.

运行 `engine-setup` 命令，开始在机器上配置数据仓库：

```
# engine-setup
```

4.

按 `Enter` 接受自动检测到的主机名，或者输入替代主机名并按 `Enter`：

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

5.

按 `Enter` 键自动配置防火墙，或者键入 `No` 并按 `Enter` 来维护现有设置：

```
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。

6.

为 Manager 输入完全限定域名和密码。按 Enter 键接受其他字段中的默认值：

```
Host fully qualified DNS name of the engine server []: engine-fqdn
Setup needs to do some actions on the remote engine server. Either automatically,
using ssh as root to access it, or you will be prompted to manually perform each such
action.
Please choose one of the following:
1 - Access remote engine server using ssh as root
2 - Perform each action manually, use files to copy content around
(1, 2) [1]:
ssh port on remote engine server [22]:
root password on remote engine server engine-fqdn: password
```

7.

输入 Manager 数据库计算机的 FQDN 和密码。按 Enter 键接受其他字段中的默认值：

```
Engine database host []: manager-db-fqdn
Engine database port [5432]:
Engine database secured connection (Yes, No) [No]:
Engine database name [engine]:
Engine database user [engine]:
Engine database password: password
```

8.

确认安装设置：

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

数据仓库服务现在在远程计算机上配置。继续在管理器计算机上禁用数据仓库服务。

3.2.2.2.4. 在 Manager 机器上禁用数据仓库服务

前提条件

- Manager 机器上的 Grafana 服务被禁用：

```
# systemctl disable --now grafana-server.service
```

流程

1. 在 Manager 机器中重启 Manager :

```
# service ovirt-engine restart
```

2. 运行以下命令修改文件 `/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf`，并将选项设置为 `False`：

```
# sed -i \  
-e 's;^\(OVESETUP_DWH_CORE/enable=bool\):True;\1:False;' \  
-e 's;^\(OVESETUP_DWH_CONFIG/remoteEngineConfigured=bool\):True;\1:False;' \  
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf  
  
# sed -i \  
-e 's;^\(OVESETUP_GRAFANA_CORE/enable=bool\):True;\1:False;' \  
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

3. 禁用数据仓库服务：

```
# systemctl disable ovirt-engine-dwhd.service
```

4. 删除数据仓库文件：

```
# rm -f /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/*.conf /var/lib/ovirt-engine-dwh/backups/*
```

数据仓库服务现在托管在管理器之外的独立机器上。

3.2.3. 使用备份存储域备份和恢复虚拟机

3.2.3.1. 备份存储域解释

备份存储域是一个可用于存储和迁移虚拟机和虚拟机模板，用于备份和恢复用于灾难恢复、迁移或任何其他备份/恢复模式。备份域不同于非备份域，使备份域上的所有虚拟机都处于关机状态。虚拟机不能在备份域中运行。

您可以将任何数据存储域设置为备份域。您可以选择或在 **Manage Domain** 对话框中选择或取消选择复选框来禁用此设置。您只能在该存储域上的所有虚拟机停止后启用此设置。

您无法启动存储在备份域中的虚拟机。Manager 会阻止这个操作以及可能会使备份造成任何其他操作。但是，如果虚拟机磁盘不属于备份域，您可以基于存储在备份域上的模板运行虚拟机。

与其他类型的存储域一样，您可以将备份域附加到数据中心或从数据中心进行分离。因此，除了存储备份外，您还可以使用备份域在数据中心之间迁移虚拟机。

优点

下面列出了一些使用备份域而不是导出域的原因：

- 您可以在数据中心中有多个备份存储域，而不是只有一个导出域。
- 您可以指定一个备份存储域，以用于备份和灾难恢复。
- 您可以将虚拟机、模板或快照的备份传输到备份存储域
- 迁移大量虚拟机、模板或 OVF 文件比导出域要快得多。
- 备份域使用磁盘空间比导出域更有效。
- 备份域支持文件存储(NFS、Gluster)和块存储（光纤通道和 iSCSI）。这与导出域不同，它只支持文件存储。
- 您可以动态启用和禁用存储域的备份设置，考虑限制。

限制

- `_backup` 域中的任何虚拟机或模板都必须在同一域中拥有其所有磁盘。
- 必须先关闭存储域上的所有虚拟机，然后才能将它设置为备份域。
- 您无法运行存储在备份域中的虚拟机，因为这样做可能会操控磁盘的数据。

- 备份域不能是内存卷的目标，因为内存卷只支持活跃虚拟机。
- 您不能在备份域中预览虚拟机。
- 无法将虚拟机实时迁移到备份域。
- 您不能将备份域设置为主域。
- 您不能将自托管引擎的域设置为备份域。
- 不要使用默认存储域作为备份域。

3.2.3.2. 将数据存储域设置为备份域

前提条件

- 属于存储域上虚拟机或模板的所有磁盘都必须位于同一域中。
- 域上的所有虚拟机都必须关机。

流程

1. 在管理门户中，选择 **Storage** → **Domains**。
2. 创建新的存储域或选择现有存储域，然后单击 **管理域**。此时会打开 **Manage Domains** 对话框。
3. 在高级参数下，选中备份复选框。

现在，域是备份域。

3.2.3.3. 使用备份域备份或恢复虚拟机或快照

您可以备份已关闭的虚拟机或快照。然后，您可以将备份保存到同一数据中心，并根据需要恢复备份，或者将其迁移到另一个数据中心。

步骤：备份虚拟机

1. 创建备份域。请参阅 [将存储域设置为备份域备份域](#)。
2. 根据您要备份的虚拟机创建新虚拟机：
 - 要备份快照，首先从快照创建虚拟机。请参阅[虚拟机管理指南中的从快照创建虚拟机](#)。
 - 要备份虚拟机，请先克隆虚拟机。请参阅[虚拟机管理指南中的克隆虚拟机](#)。在继续操作前，请确保克隆已关闭。
3. 将新虚拟机导出到备份域。请参阅[虚拟机管理指南中的将虚拟机导出到数据域](#)。

步骤：恢复虚拟机

1. 确保存储虚拟机备份的备份存储域已附加到数据中心。
2. 从备份域导入虚拟机。请参阅[从数据域中导入虚拟机](#)。

相关信息

- [导入存储域](#)
- [在同一环境中的数据中心间迁移存储域](#)
- [在不同环境中的数据中心间迁移存储域](#)

3.2.4. 使用备份和恢复 API 备份和恢复虚拟机

3.2.4.1. 备份和恢复 API

备份和恢复 API 是功能的集合，允许您执行完整或文件级备份和恢复虚拟机。API 结合了 Red Hat Virtualization 的多个组件，如实时快照和 REST API，用于创建和操作临时卷，这些卷可以连接到包含独立软件供应商提供的备份软件的虚拟机。

有关支持的第三方备份供应商，请参阅 [Red Hat Virtualization 生态系统](#)。

3.2.4.2. 备份虚拟机

使用备份和恢复 API 来备份虚拟机。此流程假设您有两个虚拟机：要备份的虚拟机，以及在其中安装管理备份的软件的虚拟机。

流程

1. 使用 REST API，创建要备份的虚拟机的快照：

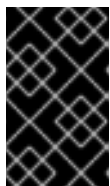
```
POST /api/vms/{vm:id}/snapshots/ HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

```
<snapshot>
  <description>BACKUP</description>
</snapshot>
```



注意

- 在这里，将 `{vm:id}` 替换为您要生成快照的虚拟机 ID。这个 ID 位于 Administration Portal 和 VM Portal 的 New Virtual Machine 和 Edit Virtual Machine 窗口的 General 选项卡中。
- 对虚拟机执行快照将其当前配置数据存储快照下 初始化 中的配置属性的 data 属性中。



重要

您不能对标记为共享的磁盘或基于直接 LUN 磁盘执行快照。

2.

从快照下的 data 属性中检索虚拟机的配置数据：

```
GET /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1
All-Content: true
Accept: application/xml
Content-type: application/xml
```



注意

- 此处，将 `{vm:id}` 替换为之前生成快照的虚拟机 ID。将 `{snapshot:id}` 替换为快照 ID。
- 添加 `All-Content: true` 标头以在响应中检索额外的 OVF 数据。XML 响应中的 OVF 数据位于 VM 配置元素中 `<initialization><configuration>` 中。之后，您将使用这些数据来恢复虚拟机。

3.

获取快照 ID：

```
GET /api/vms/{vm:id}/snapshots/ HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

4.

确定快照的磁盘 ID：

```
GET /api/vms/{vm:id}/snapshots/{snapshot:id}/disks HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

5.

将快照作为活跃磁盘附加到虚拟机，并具有正确的接口类型（例如，`virtio_scsi`）：

```
POST /api/vms/{vm:id}/diskattachments/ HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

```
<disk_attachment>
<active>true</active>
<interface>_virtio_scsi_</interface>
<disk id="{disk:id}">
<snapshot id="{snapshot:id}"/>
</disk>
</disk_attachment>
```



注意

在这里，将 `{vm:id}` 替换为 备份虚拟机的 ID，而不是您之前生成快照的虚拟机。将 `{disk:id}` 替换为磁盘 ID。将 `{snapshot:id}` 替换为快照 ID。

6. 使用备份虚拟机上的备份软件备份快照磁盘上的数据。
7. 从备份虚拟机中删除快照磁盘附件：

```
DELETE /api/vms/{vm:id}/diskattachments/{snapshot:id} HTTP/1.1
Accept: application/xml
Content-type: application/xml
```



注意

在这里，将 `{vm:id}` 替换为 备份虚拟机的 ID，而不是您之前生成快照的虚拟机。将 `{snapshot:id}` 替换为快照 ID。

8. 另外，还可删除快照：

```
DELETE /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1
Accept: application/xml
Content-type: application/xml
```



注意

此处，将 `{vm:id}` 替换为之前生成快照的虚拟机 ID。将 `{snapshot:id}` 替换为快照 ID。

您已在使用在单独虚拟机上安装的备份软件，在固定时间点备份虚拟机状态。

3.2.4.3. 恢复虚拟机

恢复使用备份和恢复 API 备份的虚拟机。此流程假设您已安装了备份虚拟机，用来管理之前备份的软件。

流程

1. 在管理门户中，创建一个浮动磁盘来恢复备份。有关如何创建 [浮动磁盘](#) 的详情，请参阅 [创建虚拟磁盘](#)。

2. 将磁盘附加到备份虚拟机：

```
POST /api/vms/{vm:id}/disks/ HTTP/1.1
```

```
Accept: application/xml
```

```
Content-type: application/xml
```

```
<disk id="{disk:id}">
```

```
</disk>
```



注意

此处，将 {vm:id} 替换为此 *backup* 虚拟机的 ID，而不是您之前创建的快照的虚拟机。将 {disk:id} 替换为备份虚拟机时所使用的磁盘 ID。

3. 使用备份软件将备份恢复到磁盘。

4. 从备份虚拟机中分离磁盘：

```
DELETE /api/vms/{vm:id}/disks/{disk:id} HTTP/1.1
```

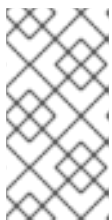
```
Accept: application/xml
```

```
Content-type: application/xml
```

```
<action>
```

```
  <detach>>true</detach>
```

```
</action>
```



注意

此处，将 {vm:id} 替换为此 *backup* 虚拟机的 ID，而不是您之前创建的快照的虚拟机。将 {disk:id} 替换为磁盘 ID。

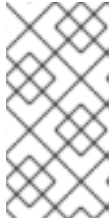
5. 使用正在恢复的虚拟机的配置数据创建新虚拟机：

```
POST /api/vms/ HTTP/1.1
```

```
Accept: application/xml
```

Content-type: application/xml

```
<vm>
  <cluster>
    <name>cluster_name</name>
  </cluster>
  <name>_NAME_</name>
  <initialization>
  <configuration>
  <data>
  <!-- omitting long ovf data -->
  </data>
  <type>ovf</type>
  </configuration>
  </initialization>
  ...
</vm>
```



注意

要在创建虚拟机时覆盖 ovf 中的任何值，请在 `initialization` 元素 *之前或之后* 重新定义该元素。不在初始化元素内。

6.

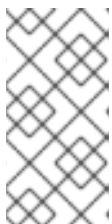
将磁盘附加到虚拟机：

POST /api/vms/{vm:id}/disks/ HTTP/1.1

Accept: application/xml

Content-type: application/xml

```
<disk id="{disk:id}">
</disk>
```



注意

此处，将 `{vm:id}` 替换为新虚拟机的 ID，而不是您之前创建的快照的虚拟机。将 `{disk:id}` 替换为磁盘 ID。

您已使用使用备份和恢复 API 创建的备份恢复虚拟机。

3.2.5. 使用增加备份和恢复 API 备份和恢复虚拟机

3.2.5.1. 增量备份和恢复 API

Red Hat Virtualization 提供了一个增量备份 API，可用于完整备份 QCOW2 或 RAW 虚拟磁盘，或

者 QCOW 2 虚拟磁盘的增量备份，而无需任何临时快照。数据以 RAW 格式备份，无论正在备份的虚拟磁盘是 QCOW2 或 RAW。您可以恢复 RAW 客户机数据以及 RAW 或 QCOW2 磁盘。增量备份 API 是 RHV REST API 的一部分。您可以备份正在运行或非运行的虚拟机。

作为开发人员，您可以使用 API 来开发备份应用程序。

功能

备份比使用备份和恢复 API 更简单、更强大。Incremental Backup API 改进了与备份应用程序集成，并提供新的支持来备份和恢复 RAW 客户机数据，而不考虑底层磁盘格式。

如果无效的位图导致备份失败，您可以在备份链中删除特定的检查点。您不需要运行完整备份。

限制：

- 只有 QCOW2 格式的磁盘才可以递增，而不是 RAW 格式磁盘。备份过程以 RAW 格式保存备份的数据。
- 只有以 RAW 格式备份的数据才能恢复。
- 增量恢复不支持在备份时存在快照恢复，而增量恢复只恢复数据，而不是在备份时存在卷或镜像的结构。这个限制对于其他系统的备份解决方案很常见。
- 与备份解决方案通常一样，增量恢复只恢复快照中的数据，而不是在备份时存在时卷或镜像的结构。
- 一个未彻底的关闭（无论原因）可能会对磁盘上的位映射无效，这会导致整个备份链无效。使用无效的位映射恢复增量备份会导致虚拟机数据被破坏。

除了启动备份外，无法检测无效的位映射。如果磁盘包含无效的位映射，则操作会失败。

下表描述了支持增量备份的磁盘配置。



注意

使用管理门户创建磁盘时，您将设置存储类型、置备类型，以及增量备份是启用还是禁用。根据这些设置，Manager 会决定虚拟磁盘格式。

表 3.1. 增量备份支持的磁盘配置

存储类型	置备类型	当增量备份为...	虚拟磁盘格式是...
block	thin	enabled	qcow2
block	预分配	enabled	qcow2 (preallocated)
file	thin	enabled	qcow2
file	预分配	enabled	qcow2 (preallocated)
block	thin	disabled	qcow2
block	预分配	disabled	raw (preallocated)
file	thin	disabled	原始 (稀疏)
file	预分配	disabled	raw (preallocated)
network	<i>Not applicable</i>	disabled	raw
LUN	<i>Not applicable</i>	disabled	raw

3.2.5.1.1. 增量备份流

使用 Incremental Backup API 的备份应用程序必须遵循此序列备份已启用的虚拟机磁盘进行增量备份：

1. 备份应用使用 REST API 查找应包含在备份中的虚拟机磁盘。只包括 QCOW2 格式的磁盘。
2. 备份应用启动完整备份或增量备份。API 调用指定虚拟机 ID、可选先前检查点 ID 以及要备份的磁盘列表。如果 API 调用没有指定之前的检查点 ID，则完整备份将开始，其中包含指定磁盘中的所有数据（基于每个磁盘的当前状态）。

3. 该引擎会准备要备份的虚拟机。虚拟机可以在备份过程中继续运行。
4. 备份应用程序轮询备份状态引擎，直到引擎报告备份已准备好开始。
5. 当备份准备好开始时，备份应用程序会为备份中包含的每个磁盘创建一个镜像传输对象。
6. 备份应用程序从 `ovirt-imageio` 获取更改的块列表，用于每个镜像传输。如果更改列表不可用，备份应用程序会出错。
7. 备份应用程序从 `ovirt-imageio` 下载经过 RAW 格式的块，并将它们存储在备份介质中。如果更改的块列表不可用，备份应用程序可能会回退来复制整个磁盘。
8. 备份应用程序完成所有镜像传输。
9. 备份应用程序使用 REST API 完成备份。

3.2.5.1.2. 增量恢复流

使用 Incremental Backup API 的备份应用程序必须遵循此序列来恢复已备份的虚拟机磁盘：

1. 用户使用备份应用程序根据可用备份选择恢复点。
2. 备份应用程序会创建一个新磁盘，或使用现有磁盘保存恢复的数据的快照。
3. 备份应用程序为每个磁盘启动上传镜像传输，其格式为原始。这会在将 RAW 数据上传到 QCOW2 磁盘时启用格式转换。
4. 备份应用程序使用 API 将此恢复中包含的数据传输到 `imageio`。
5. 备份应用程序完成镜像传输。

3.2.5.1.3. 增量备份和恢复 API 任务

[Red Hat Virtualization REST API 指南](#)中记录了 [Incremental Backup and Restore API](#)。备份和恢复流程需要以下操作：

- 在新的或现有虚拟磁盘中启用增量备份：
 - [使用管理门户的新磁盘](#)
 - [使用管理门户的现有磁盘](#)
 - [使用 API 调用的新或现有磁盘](#)
- [查找为增量备份启用的磁盘](#)
- [启动完整备份](#)
- [启动增量备份](#)
- [备份最终大小](#)
- [获取有关备份的信息](#)
- [在备份中获取有关磁盘的信息](#)
- [列出虚拟机的所有检查点](#)
- [列出特定虚拟机检查点的信息](#)

- [删除特定虚拟机的检查点](#)
- [下载镜像转让对象来归档备份](#)
- [上传镜像转让对象以恢复备份](#)
- [列出已更改的块](#)
- [下载和上传更改的块](#)

3.2.5.1.4. 在新虚拟磁盘中启用增量备份

为虚拟磁盘启用增量备份，将其标记为增量备份中。添加磁盘时，您可以使用 REST API 或管理门户为每个磁盘启用增量备份。您可以使用完整备份备份备份或者与之前相同的方式，备份未启用的现有磁盘。



注意

Manager 不需要启用磁盘，使其包含在增量备份中，但您可以启用它来跟踪启用了哪些磁盘。

由于增量备份需要采用 QCOW2 格式化磁盘，因此请使用 QCOW2 格式，而非 RAW 格式。

流程

1. [添加新的虚拟磁盘](#)。如需更多信息，[请参阅创建虚拟磁盘](#)。
2. 在配置磁盘时，选中 **Enable Incremental Backup** 复选框。

其他资源

- [使用 API 为磁盘启用增量备份](#)。

3.2.5.1.5. 在现有 RAW 虚拟磁盘中启用增量备份

因为采用 RAW 格式的磁盘不支持增量备份，所以任何 RAW 格式磁盘之上的 QCOW2 格式层必须存在，才能使用增量备份。创建快照会从创建快照的时间点，生成 QCOW2 层，并在快照中包含的所有磁盘上实现增量备份。



警告

如果磁盘的基本层使用 RAW 格式，请删除最后一个快照，并将顶级 QCOW2 层合并到基础层，将磁盘转换为 RAW 格式，从而在设置了增量备份时禁用增量备份。要重新启用增量备份，您可以创建一个新快照，包括这个磁盘。

流程

1. 在管理门户中，点 **Compute** → **Virtual Machines**。
2. 选择虚拟机并点击 **Disks** 选项卡。
3. 单击 **编辑** 按钮。这会打开 **Edit Disk** 对话框。
4. 选中“启用增量备份”复选框。

其他资源

- [使用 API 为磁盘启用增量备份](#)

3.2.5.1.6. 启用增量备份

您可以使用 REST API 请求为虚拟机的磁盘启用增量备份。

流程

- 为新磁盘启用增量备份。例如，对于 ID 为 123 的虚拟机上的新磁盘，请发送此请求：

POST /ovirt-engine/api/vms/123/diskattachments

请求正文应包含 `backup` 设置为 `incremental`，作为 `磁盘` 对象的一部分，如下所示：

```

<disk_attachment>
  ...
  <disk>
    ...
    <backup>incremental</backup>
    ...
  </disk>
</disk_attachment>

```

响应是：

```

<disk_attachment>
  ...
  <disk href="/ovirt-engine/api/disks/456" id="456"/>
  ...
</disk_attachment>

```

其他资源

- [RHV 的 REST API 指南中的 DiskBackup enum](#)

3.2.5.1.7. 查找为增量备份启用的磁盘

对于指定的虚拟机，您可以列出为增量备份启用的磁盘，并根据备份属性过滤。

流程

1. 列出附加到虚拟机的磁盘。例如，对于 ID 为 123 的虚拟机，请发送此请求：

GET /ovirt-engine/api/vms/123/diskattachments

响应包含所有 `disk_attachment` 对象，每个对象包括一个或多个磁盘对象。例如：

```

<disk_attachments>
  <disk_attachment>
    ...
    <disk href="/ovirt-engine/api/disks/456" id="456"/>

```

```

...
</disk_attachment>
...
</disk_attachments>

```

2.

使用 `disk` 服务查看上一步中的磁盘属性。例如，对于 ID 为 456 的磁盘，请发送此请求：

```
GET /ovirt-engine/api/disks/456
```

响应包括磁盘的所有属性。备份 被设置为 `none` 或 `incremental`。例如：

```

<disk href="/ovirt-engine/api/disks/456" id="456">
...
  <backup>incremental</backup>
...
</disk>

```

其他资源

- [Disk struct 的 backup 属性](#)
- [DiskBackup enum](#)

3.2.5.1.8. 启动完整备份

在进行完整备份后，您可以使用生成的检查点 ID 作为下一个增量备份中的起点。

在对正在运行的虚拟机进行备份时，该过程会在与正在备份的磁盘相同的存储域中创建全新磁盘。备份过程会创建此磁盘，使新数据在备份期间写入到正在运行的虚拟机中。您可以在备份过程中在管理门户中看到这一全新磁盘。在备份完成后，它将自动删除。

启动完整备份需要请求调用正文，并包含响应。

流程

1.

发送指定虚拟机的请求进行备份。例如，指定 ID 为 123 的虚拟机，如下所示：

```
POST /ovirt-engine/api/vms/123/backups
```


2.

在请求正文中，指定要备份的磁盘。例如，要启动 ID 为 456 的磁盘的完整备份，请发送以下请求正文：

```
<backup>
  <disks>
    <disk id="456" />
    ...
  </disks>
</backup>
```

响应正文应类似于如下：

```
<backup id="789">
  <disks>
    <disk id="456" />
    ...
  </disks>
  <status>initializing</status>
  <creation_date>
</backup>
```

响应包括以下内容：

- 备份 ID
- 备份的状态，表示备份正在初始化。

3.

轮询备份，直到状态就绪。响应包括 `to_checkpoint_id`。请注意此 ID，并在下一次增量备份中使用它进行 `from_checkpoint_id`。

其他资源

- [RHV 的 REST API 指南中的 VmBackups 服务的 add 方法](#)

3.2.5.1.9. 启动增量备份

完成给定虚拟磁盘的完整备份后，磁盘后续增量备份仅包含自上次备份之后的更改。使用最新备份中的 `to_checkpoint_id` 值作为请求正文中 `from_checkpoint_id` 的值。

在对正在运行的虚拟机进行备份时，该过程会在与正在备份的磁盘相同的存储域中创建全新磁盘。备份过程会创建此磁盘，使新数据在备份期间写入到正在运行的虚拟机中。您可以在备份过程中在管理门户中看到这一全新磁盘。在备份完成后，它将自动删除。

启动增量备份或混合备份需要使用正文进行请求调用，并包含响应。

流程

1. 发送指定虚拟机的请求进行备份。例如，指定 ID 为 123 的虚拟机，如下所示：

```
POST /ovirt-engine/api/vms/123/backups
```

2. 在请求正文中，指定要备份的磁盘。例如，要启动 ID 为 456 的磁盘的增量备份，请发送以下请求正文：

```
<backup>
  <from_checkpoint_id>previous-checkpoint-uuid</from_checkpoint_id>
  <disks>
    <disk id="456" />
    ...
  </disks>
</backup>
```

注意

在请求正文中，如果您包含之前检查点中不包含的磁盘，则请求也会运行此磁盘的完整备份。例如，ID 为 789 的磁盘还没有备份。要在上述请求正文中添加 789 的完整备份，请发送请求正文，如下所示：

```
<backup>
  <from_checkpoint_id>previous-checkpoint-
  uuid</from_checkpoint_id>
  <disks>
    <disk id="456" />
    <disk id="789" />
    ...
  </disks>
</backup>
```

响应正文应类似于如下：

```

<backup id="101112">
<from_checkpoint_id>previous-checkpoint-uuid</from_checkpoint_id>
<to_checkpoint_id>new-checkpoint-uuid</to_checkpoint_id>
  <disks>
    <disk id="456" />
    <disk id="789" />
    ...
  </disks>
  <status>initializing</status>
  <creation_date>
</backup>

```

响应包括以下内容：

- 备份 ID。
 - 备份中包含的任何磁盘的 ID。
 - 表示备份正在初始化的状态。
3. 轮询备份，直到状态就绪。响应包括 `to_checkpoint_id`。请注意此 ID，并在下一次增量备份中使用它进行 `from_checkpoint_id`。

其他资源

- [RHV 的 REST API 指南中的 VmBackups 服务的 add 方法。](#)

3.2.5.1.10. 获取有关备份的信息

您可以获取有关可用于启动新增量备份的备份的信息。

`VmBackups` 服务的列表方法返回以下有关备份的信息：

- 备份的每个磁盘的 ID。

- 备份的开头和端点的 ID。
- 备份磁盘镜像的 ID，用于备份中包含的每个磁盘。
- 备份的状态。
- 创建备份的日期。

当 `<status>` 的值就绪时，响应包括 `<to_checkpoint_id>`，它应用作下一个增量备份中的 `<from_checkpoint_id>`，您可以开始下载磁盘来备份虚拟机存储。

流程

- 要获取一个带有 ID 为 123 的虚拟机的 ID 为 456 的备份的信息，请发送如下请求：

```
GET /ovirt-engine/api/vms/456/backups/123
```

响应包括 ID 为 456 的备份，`<from_checkpoint_id>` 999 和 `<to_checkpoint_id>` 666。备份中包含的磁盘在 `<link>` 元素中引用。

```
<backup id="456">
  <from_checkpoint_id>999</from_checkpoint_id>
  <to_checkpoint_id>666</to_checkpoint_id>
  <link href="/ovirt-engine/api/vms/456/backups/123/disks" rel="disks"/>
  <status>ready</status>
  <creation_date>
</backup>
```

其他资源

- [列出 VmBackups 服务的方法](#)

3.2.5.1.11. 在备份中获取有关磁盘的信息

您可以获取有关作为备份一部分的磁盘的信息，包括备份中每个磁盘的备份模式，这有助于确定用于下载备份的模式。

`VmBackupDisks` 服务 列表 方法返回以下有关备份的信息：

- 备份的每个磁盘的 ID 和名称。
- 备份磁盘镜像的 ID，用于备份中包含的每个磁盘。
- 磁盘格式。
- 磁盘支持的备份行为。
- 对磁盘进行的备份类型（完整/递增）。

流程

- 要获取一个带有 ID 为 123 的虚拟机的 ID 为 456 的备份的信息，请发送如下请求：

```
GET /ovirt-engine/api/vms/456/backups/123/disks
```

响应包括 ID 为 789 的磁盘，磁盘镜像的 ID 为 555。

```
<disks>
  <disk id="789">
    <name>vm1_Disk1</name>
    <actual_size>671744</actual_size>
    <backup>incremental</backup>
    <backup_mode>full</backup_mode>
    <format>cow</format>
    <image_id>555</image_id>
    <qcow_version>qcow2_v3</qcow_version>
    <status>locked</status>
    <storage_type>image</storage_type>
    <total_size>0</total_size>
  </disk>
</disks>
```

其他资源

- [列出 VmBackupDisks 服务的方法](#)

3.2.5.1.12. 备份最终大小

备份最终结束备份，解锁资源，并执行清理。使用 [完成的备份服务方法](#)

流程

- 要在 ID 为 123 的虚拟机上完成 ID 为 456 的磁盘备份，请发送请求，如下所示：

```
POST /vms/123/backups/456/finalize
```

其他资源

- 在 [REST API 指南](#)中完成 [POST](#)。

3.2.5.1.13. 为增量备份创建镜像传输对象

当备份准备好下载时，备份应用应 [创建镜像transfer](#) 对象，该对象为增量备份启动传输。

创建镜像转让对象需要带有正文的请求调用。

流程

1. 发送请求，如下所示：

```
POST /ovirt-engine/api/imagetransfers
```

2. 在请求正文中，指定以下参数：

- 磁盘 ID。
- 备份 ID。

- 磁盘的方向设置为 **download**。
- 磁盘设置为 **raw** 的格式。

例如，要传输磁盘 ID 为 123 且备份 ID 为 456 的磁盘的备份，请发送以下请求正文：

```
<image_transfer>
  <disk id="123"/>
  <backup id="456"/>
  <direction>download</direction>
  <format>raw</format>
</image_transfer>
```

其他资源

- RHV 的 *REST API 指南* 中的 [创建一个 imagetransfer 对象的 add 方法](#)。

3.2.5.1.14. 创建用于增量恢复的镜像传输对象

要启用使用增量备份 API 备份的原始数据到 QCOW2 格式磁盘，备份应用程序应创建镜像transfer 对象。

当传输格式为 raw 且底层磁盘格式是 QCOW2 时，在写入存储时，上传的数据会在 fly to QCOW2 格式中转换。不支持将数据从 QCOW2 磁盘上传到 RAW 磁盘。

创建镜像转让对象需要带有正文的请求调用。

流程

1. 发送请求，如下所示：

```
POST /ovirt-engine/api/imagetransfers
```

2. 在请求正文中，指定以下参数：

- 磁盘 ID 或快照 ID。
- 磁盘集的方向，以上传。
- 磁盘设置为 raw 的格式。

例如，要传输磁盘 ID 为 123 的磁盘备份，请发送以下请求正文：

```
<image_transfer>
  <disk id="123"/>
  <direction>upload</direction>
  <format>raw</format>
</image_transfer>
```

其他资源

- RHV 的 *REST API 指南* 中的 [创建一个 imagetransfer 对象的 add 方法](#)。

3.2.5.1.15. 列出虚拟机的检查点

您可以通过发送请求调用来列出虚拟机的所有检查点，包括每个检查点的信息。

流程

- 发送指定虚拟机的请求。例如，指定 ID 为 123 的虚拟机，如下所示：

```
GET /vms/123/checkpoints/
```

响应包括所有虚拟机的检查点。每个检查点包含以下信息：

- 检查点的磁盘。
- 父检查点的 ID。

- 检查点的创建日期。
- 所属的虚拟机。

例如：

```
<parent_id>, <creation_date> and the virtual machine it belongs to <vm>:
<checkpoints>
  <checkpoint id="456">
    <link href="/ovirt-engine/api/vms/vm-uuid/checkpoints/456/disks" rel="disks"/>
    <parent_id>parent-checkpoint-uuid</parent_id>
    <creation_date>xxx</creation_date>
    <vm href="/ovirt-engine/api/vms/123" id="123"/>
  </checkpoint>
</checkpoints>
```

其他资源

- [RHV 的 REST API 指南](#) 中的 [列出虚拟机检查点的 list 方法](#)。

3.2.5.1.16. 列出虚拟机的特定检查点

您可以通过发送请求调用来列出虚拟机的特定检查点的信息。

流程

- 发送指定虚拟机的请求。例如，指定 ID 为 123 的虚拟机，以及检查点 ID 456，如下所示：

```
GET /vms/123/checkpoints/456
```

响应包括检查点的以下信息：

- 检查点的磁盘。
- 父检查点的 ID。

- 检查点的创建日期。
- 所属的虚拟机。

例如：

```
<checkpoint id="456">
  <link href="/ovirt-engine/api/vms/vm-uuid/checkpoints/456/disks" rel="disks"/>
  <parent_id>parent-checkpoint-uuid</parent_id>
  <creation_date>xxx</creation_date>
  <vm href="/ovirt-engine/api/vms/123" id="123"/>
</checkpoint>
```

其他资源

- [RHV 的 REST API 指南](#) 中的 [列出虚拟机检查点的 list 方法](#)。

3.2.5.1.17. 删除检查点

您可以通过发送 **DELETE** 请求来删除虚拟机的检查点。您可以删除虚拟机上的检查点，不论它是否正在运行。

流程

- 发送指定虚拟机和检查点的请求。例如，指定 ID 为 123 的虚拟机，以及 ID 为 456 的检查点，如下所示：

```
DELETE /vms/123/checkpoints/456/
```

其他资源

- [删除 VmCheckpoint 的方法](#)

3.2.5.1.18. 使用 imageio API 来传输备份数据

镜像传输 API 会启动和停止镜像转让。结果是一个转让 URL。

您可以使用 `imageio API` 实际传输来自转让 `URL` 的数据。

有关使用 `imageio API` 的完整信息，请参阅 [ovirt-imageio Images API 引用](#)。

表 3.2. 增量备份和恢复中使用的 `imageio Image API` 方法

API 请求	Description	Imageio Image API 参考部分
OPTIONS /images/{ticket-id} HTTP/1.1	获取服务器选项，找出服务器支持的功能。	请参阅 <i>OPTIONS</i>
GET /images/{ticket-id}/extents	获取磁盘镜像内容和分配的信息，或者有关增量备份期间更改的块的信息。这些信息被称为 <i>扩展</i> 信息。	请参阅 <i>EXTENTS</i>
GET /images/{ticket-id}/extent?context=dirty	进行镜像传输的程序需要下载备份中的更改。这些更改称为脏扩展。要下载更改，请发送类似以下请求：	请参阅 <i>EXTENTS</i> → <i>Examples</i> → <i>Request dirty extents</i>
PUT /images/{ticket-id}	备份应用程序会创建一个新磁盘，或使用现有磁盘保存恢复的数据的快照。	请参阅 <i>PUT</i>

其他资源

Red Hat Virtualization Python SDK 包括一些可用于开始进行传输备份的实施示例：

- [ovirt-imageio Images API 参考](#)
- [创建磁盘](#)
- [Calling `imagetransfer.create_transfer\(\)`](#)
- [简化创建转让的帮助](#)
- [使用 Red Hat Virtualization Python SDK](#)

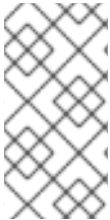
3.3. 使用 RED HAT SATELLITE 设置勘误查看

在管理门户中，您可以配置 Red Hat Virtualization 以查看 Red Hat Virtualization Manager 中的 Red Hat Satellite 中的勘误。将主机、虚拟机和管理器与 Red Hat Satellite 供应商相关联后，您可以收到有关可用勘误表的更新及其重要性，并决定何时应用它们。有关 Red Hat Satellite 的更多信息，请参阅 [Red Hat Satellite 文档](#)。

Red Hat Virtualization 4.4 支持使用 Red Hat Satellite 6.6 查看勘误。

前提条件

- **Satellite 服务器必须添加为外部提供程序。**
- **管理器、主机和虚拟机都必须通过对应的 FQDN 在卫星服务器中注册。这样可确保外部内容主机 ID 无需在 Red Hat Virtualization 中维护。**
- **管理 Manager、主机和虚拟机的 Satellite 帐户必须具有管理员权限和默认的机构集。**



注意

Katello 代理已弃用，并将在以后的 Satellite 版本中删除。迁移进程以使用远程执行功能远程更新客户端。

配置 Red Hat Virtualization 勘误

要将 Manager、主机和虚拟机与 Red Hat Satellite 供应商关联，请完成以下步骤：

1. **将所需的卫星服务器作为外部提供者添加到 Manager 中。**
2. **配置所需的主机以显示可用的勘误表。**
3. **配置所需的虚拟机，以显示可用的勘误表。**

查看 Red Hat Virtualization Manager 勘误

1. 点 **Administration** → **Errata**。
2. 选中 **Security**、**Bugs** 或 **Enhancements** 复选框，以仅查看这些勘误表类型。

其他资源

- [为主机配置 Satellite 勘误管理](#)
- [Red Hat Enterprise Linux 虚拟机的虚拟机管理指南中，在 Linux 上安装客户机代理、工具和驱动程序。](#)
- [Windows 虚拟机的虚拟机管理指南中，在 Windows 上安装客户机代理、工具和驱动程序。](#)
- [查看主机勘误](#)
- 有关更多信息，[在虚拟机管理指南中配置卫星勘误表查看虚拟机。](#)
- [虚拟机管理指南中的查看虚拟机的 Red Hat Satellite 勘误。](#)

3.4. 在证书过期前续订证书

在早于版本 4.4 SP1 的 Red Hat Virtualization 中，所有证书都遵循 398 天生命周期。从 Red Hat Virtualization 版本 4.4 SP1 开始，虚拟机监控程序和 Manager 之间的自签名内部证书遵循 5 年生命周期。Web 浏览器可见的证书仍遵循标准的 398 天生命周期，并且必须每年续订一次。



警告

不要让证书过期。如果它们到期，则主机和经理停止响应，恢复是一个容易出错且耗时的过程。

流程

1.

更新主机证书：

a.

在管理门户中，点 **Compute** → **Hosts**。

b.

单击 **Management** → **Maintenance**，然后单击 **OK**。虚拟机应自动从主机中迁移。如果固定或无法迁移，则必须关闭它们。

c.

当主机处于维护模式且此主机上不存在更多虚拟机时，请单击 **Installation** → **Enroll Certificate**。

d.

注册完成后，单击 **管理** → **激活**。

2.

更新 Manager 证书：

a.

仅自托管引擎：登录主机并将其置于全局维护模式。

```
# hosted-engine --set-maintenance --mode=global
```

b.

自托管引擎和单机管理器：登录 **Manager** 并运行 **engine-setup**。

```
# engine-setup --offline
```

engine-setup 脚本会提示您配置问题。根据情况回答问题，或使用回答文件。

c.

在以下 **engine-setup** 提示后输入 **Yes**：

```
Renew certificates? (Yes, No) [Yes]:
```

d.

仅自托管引擎：登录主机并禁用全局维护模式：

```
# hosted-engine --set-maintenance --mode=none
```

其他资源

- [如果过期，如何手动续订 RHV 主机 SSL 证书？](#)

3.5. 使用 ANSIBLE 自动化配置任务

Ansible 是一个自动化工具，用于配置系统、部署软件和执行滚动更新。**Red Hat Virtualization** 包括了一个有限的 **Ansible** 版本，可自动执行 **RHV** 安装后的任务，如数据中心设置和配置、管理用户和虚拟机操作。

与 **REST API** 和 **SDK** 相比，**Ansible** 提供了更简单的方法自动化 **Red Hat Virtualization** 配置，并可与其他 **Ansible** 模块集成。有关 **Red Hat Virtualization** 可用 **Ansible** 模块的更多信息，请参阅 **Red Hat Ansible Automation Hub** 文档中的 [oVirt Ansible Collection](#)。



注意

Ansible Tower 是通过 **Web** 界面和 **Ansible** 的 **REST API** 访问的图形化启用了框架。如果您想要对 **Ansible Tower** 的支持，则必须具有 **Ansible Tower** 许可证，它不属于 **Red Hat Virtualization** 订阅。

有关使用 [Ansible](#) 的替代安装说明，请参阅 [Ansible](#) 文档。

3.5.1. oVirt Ansible Collection

oVirt Ansible Collection 提供了用于管理 **Red Hat Virtualization** 基础架构的各个部分的模块、角色和插件。模块用于 **Ansible** 和 **Red Hat Virtualization Manager** 之间的通信。**Ansible** 角色提供了一种方法来模块化 **Ansible** 代码，可将大型 **playbook** 划分为可被其他用户共享的较小可重复使用的文件。有关 **oVirt Ansible Collection** 的更多信息，请参阅 [Automation Hub](#) 文档。

3.5.1.1. 从 RPM 软件包安装 oVirt Ansible Collection

您可以从 **Red Hat Virtualization Manager** 仓库安装 **oVirt Ansible Collection for Red Hat Virtualization**。

前提条件

要安装 **oVirt Ansible Collection**，您必须订阅以下订阅频道之一：

- 使用 Red Hat Virtualization 订阅 - rhv-4.4-manager-for-rhel-8-x86_64-rpms
- 使用任何 Red Hat Enterprise Linux 订阅 - rhv-4-tools-for-rhel-8-x86_64-rpms

流程

1. 运行以下命令，在 Manager 机器上安装 oVirt Ansible Collection ：

```
# dnf install ovirt-ansible-collection
```

2. 默认情况下，集合会被安装到：

```
/usr/share/ansible/collections/ansible_collections/redhat/rhv.
```

ovirt-ansible-collection 软件包的结构如下：

```
/usr/share/ansible/collections/ansible_collections/redhat/rhv/usr/share/doc/ovirt-ansible-collection/
```

3.5.1.2. 从 Automation Hub 安装 oVirt Ansible Collection

Automation Hub 是一个新的位置，可用于安装 oVirt Ansible Collection。要配置环境，请按照 [oVirt Ansible Collection 文档](#) 中的说明操作。

流程

1. 安装集合

```
# ansible-galaxy collection install redhat.rhv
```

2. Automation Hub 目前没有安装 RPM 依赖项。请确定您在执行 `playbook` 的主机上有这些软件包：

- `python3-ovirt-engine-sdk4`

- `python3-netaddr`
- `python3-jmespath`
- `python3-passlib`

3.5.1.3. 使用 oVirt Ansible Collection 配置 Red Hat Virtualization

以下流程指导您创建并运行使用 oVirt Ansible Collection 配置 Red Hat Virtualization 的 `playbook`。本例使用 Ansible 连接到本地计算机上的 Manager 并创建一个新的数据中心。

前提条件

- 确保在运行 `playbook` 的机器上安装了 Python SDK。

流程

1. 创建 `playbook`。

```
- name: RHV infrastructure
  hosts: localhost
  connection: local
  gather_facts: false

  vars_files:
    # Contains variables to connect to the Manager
    - engine_vars.yml
    # Contains encrypted engine_password variable using ansible-vault
    - passwords.yml

  pre_tasks:
    # The use of redhat.rhv before ovirt_auth is to check if oVirt Ansible Collection is correctly
    loaded
    - name: Login to RHV
      redhat.rhv.ovirt_auth:
        hostname: "{{ engine_fqdn }}"
        username: "{{ engine_user }}"
        password: "{{ engine_password }}"
        ca_file: "{{ engine_cafile | default(omit) }}"
        insecure: "{{ engine_insecure | default(true) }}"
      tags:
        - always
```

```
vars:
  data_center_name: mydatacenter
  data_center_description: mydatacenter
  data_center_local: false
  compatibility_version: 4.4

roles:
  - infra
collections:
  - redhat.rhv
post_tasks:
  - name: Logout from RHV
    ovirt_auth:
      state: absent
      ovirt_auth: "{{ ovirt_auth }}"
tags:
  - always
```

您已成功使用 oVirt Ansible Collection 的 `infra` Ansible 角色来创建名为 `mydatacenter` 的数据中心。

3.6. 用户和角色

3.6.1. 用户简介

在 Red Hat Virtualization 中，有两种类型的用户域：本地域和外部域。在 Manager 安装过程中，会创建一个称为 `内部域` 的默认本地域，默认的用户 `admin`。

您可以使用 `ovirt-aaa-jdbc-tool` 在 `internal` 域中创建其他用户。在本地域中创建的用户帐户称为本地用户。您还可以将外部目录服务器（如 Red Hat Directory、Active Directory、OpenLDAP 和许多其他支持选项）附加到 Red Hat Virtualization 环境中，并将其用作外部域。在外部域中创建的用户帐户称为目录用户。

本地用户和目录用户都需要通过管理门户分配适当的角色和权限，然后才能在环境中正常工作。用户角色主要有两种：最终用户和管理员。最终用户角色使用和管理虚拟机门户中的虚拟资源。管理员角色使用管理门户维护系统基础架构。可以为虚拟机和主机等独立资源为用户分配角色，或者分配到集群和数据中心的某一对象层次结构。

3.6.2. Directory 服务器介绍

在安装过程中，Red Hat Virtualization Manager 在 `internal` 域中创建一个 `admin` 用户。用户也称为 `admin@internal`。此帐户供初始配置环境和故障排除时使用。附加外部目录服务器后，添加目录用户，并为他们分配适当的角色和权限，则可以禁用 `admin@internal` 用户（如果需要）。

- **389ds**
- **389ds RFC-2307 Schema**
- **Active Directory**
- **IBM Security Directory Server**
- **IBM Security Directory Server RFC-2307 Schema**
- **FreeIPA**
- **iDM**
- **Novell eDirectory RFC-2307 Schema**
- **OpenLDAP RFC-2307 Schema**
- **OpenLDAP 标准架构**
- **Oracle Unified Directory RFC-2307 Schema**
- **RFC-2307 Schema (Generic)**
- **Red Hat Directory Server (RHDS)**
- **Red Hat Directory Server (RHDS) RFC-2307 Schema**

iPlanet

重要

无法在同一系统中安装 Red Hat Virtualization Manager (rhevm)和 IdM (ipa-server)。IdM 与 Red Hat Virtualization Manager 所需的 mod_ssl 软件包不兼容。

重要

如果您要将 Active Directory 用作目录服务器，并且您希望在创建模板和虚拟机时使用 sysprep，那么 Red Hat Virtualization 管理用户必须委托给域：

- 将计算机加入到域中
- 修改组成员资格

有关在 Active Directory 中 [创建用户帐户](#)的详情，请参考[创建新用户帐户](#)。

有关 Active Directory 中委托控制的详情，请参考 [机构单元的控制](#)。

3.6.3. 配置外部 LDAP 供应商

3.6.3.1. 配置外部 LDAP 提供程序（活动设置）

注意

ovirt-engine-extension-aaa-ldap 已被弃用。对于新安装，请使用 Red Hat Single Sign On。如需更多信息，请参阅《[管理指南](#)》中的 [安装和配置 Red Hat Single Sign On](#)。

ovirt-engine-extension-aaa-ldap 扩展允许用户轻松自定义其外部目录设置。ovirt-engine-extension-aaa-ldap 扩展支持许多不同的 LDAP 服务器类型，还提供了交互式设置脚本，以帮助您设置大多数 LDAP 类型。

如果交互式设置脚本中没有列出 LDAP 服务器类型，或者您希望进行更多自定义，您可以手动编辑配

置文件。如需更多信息，请参阅[配置外部 LDAP 供应商](#)。

有关 Active Directory 示例，请参阅 [附加 Active Directory](#)。

前提条件

- 您必须知道 DNS 或 LDAP 服务器的域名。
- 要在 LDAP 服务器和 Manager 间设置安全连接，请确保已准备好 PEM 编码的 CA 证书。
- 至少有一组帐户名称和密码已准备好对 LDAP 服务器执行搜索和登录查询。

流程

1. 在 Red Hat Virtualization Manager 中，安装 LDAP 扩展软件包：

```
# dnf install ovirt-engine-extension-aaa-ldap-setup
```

2. 运行 `ovirt-engine-extension-aaa-ldap-setup` 来启动交互式设置：

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. 输入对应数字来选择 LDAP 类型。如果您不确定 LDAP 服务器是哪个 schema，请选择您的 LDAP 服务器类型的标准模式。对于 Active Directory，请按照 [Attaching an Active Directory](#) 中的步骤进行操作。

```
Available LDAP implementations:
```

```
1 - 389ds
2 - 389ds RFC-2307 Schema
3 - Active Directory
4 - IBM Security Directory Server
5 - IBM Security Directory Server RFC-2307 Schema
6 - IPA
7 - Novell eDirectory RFC-2307 Schema
8 - OpenLDAP RFC-2307 Schema
9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
11 - RFC-2307 Schema (Generic)
12 - RHDS
```

13 - RHDS RFC-2307 Schema

14 - iPlanet

Please select:

4.

按 Enter 接受默认值，并为 LDAP 服务器名称配置域名：

It is highly recommended to use DNS resolution for LDAP server.

If for some reason you intend to use hosts or plain address disable DNS usage.

Use DNS (Yes, No) [Yes]:

5.

选择 DNS 策略方法：

•

对于选项 1，使用 `/etc/resolv.conf` 中列出的 DNS 服务器来解决 IP 地址。检查 `/etc/resolv.conf` 文件是否已使用正确的 DNS 服务器更新。

•

对于选项 2，请输入完全限定域名(FQDN)或 LDAP 服务器的 IP 地址。您可以使用 `dig` 命令和 SRV 记录来查找域名。SRV 记录采用以下格式：

```
_service._protocol.domain_name
```

示例：`dig _ldap._tcp.redhat.com SRV.`

•

对于选项 3，请输入以空格分隔的 LDAP 服务器列表。使用服务器的 FQDN 或 IP 地址。此策略在 LDAP 服务器之间提供负载均衡。根据循环算法，查询在所有 LDAP 服务器中分发。

•

对于选项 4，请输入以空格分隔的 LDAP 服务器列表。使用服务器的 FQDN 或 IP 地址。此策略定义了第一个 LDAP 服务器作为响应查询的默认 LDAP 服务器。如果第一个服务器不可用，则查询将进入列表中的下一个 LDAP 服务器。

1 - Single server

2 - DNS domain LDAP SRV record

3 - Round-robin between multiple hosts

4 - Failover between multiple hosts

Please select:

6.

选择 LDAP 服务器支持的安全连接方法，并指定获取 PEM 编码的 CA 证书的方法：

- 文件 允许您提供证书的完整路径。
- URL 允许您指定证书的 URL。
- 内联 允许您在终端中粘贴证书的内容。
- 系统 允许您指定所有 CA 文件的默认位置。
- 不安全的 跳过证书验证，但连接仍然使用 TLS 加密。

NOTE:

It is highly recommended to use secure protocol to access the LDAP server. Protocol startTLS is the standard recommended method to do so. Only in cases in which the startTLS is not supported, fallback to non standard ldaps protocol. Use plain for test environments only. Please select protocol to use (startTLS, ldaps, plain) [startTLS]: *startTLS* Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure): Please enter the password:

**注意**

LDAPS 代表覆盖安全套接字链接的轻量级目录访问协议。对于 **SSL** 连接，请选择 **ldaps** 选项。

7. 输入搜索用户可分辨名称(DN)。用户必须具有权限才能浏览目录服务器上的所有用户和组。搜索用户必须在 LDAP 注解中指定。如果允许匿名搜索，请按 Enter 键，无需输入。

Enter search user DN (for example uid=username,dc=example,dc=com or leave empty for anonymous): uid=user1,ou=Users,ou=department-1,dc=example,dc=com
Enter search user password:

8. 输入基本 DN :

Please enter base DN (dc=redhat,dc=com) [dc=redhat,dc=com]: *ou=department-1,dc=redhat,dc=com*

9.

如果您想要为虚拟机配置单点登录，请选择“是”。请注意，这个功能不能用于管理门户功能的单点登录。该脚本提醒您配置集名称必须与域名匹配。在虚拟机管理指南中，您仍需要遵循[为虚拟机配置单点登录](#)的说明。

Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]:

10.

指定配置集名称。配置集名称对登录页面上的用户可见。这个示例使用 `redhat.com`。



注意

要在域配置后重命名配置集，编辑 `/etc/ovirt-engine/extensions.d/redhat.com-authn.properties` 文件中的 `ovirt.engine.aaa.authn.profile.name` 属性。重启 `ovirt-engine` 服务以使更改生效。

Please specify profile name that will be visible to users: `redhat.com`

图 3.1. 管理门户登录页面



注意

首次登录时，用户必须从下拉菜单中选择配置集。这些信息存储在浏览器 Cookie 中，并在用户下一次登录时预选择。

11.

测试登录功能，以确保您的 LDAP 服务器已正确地连接到您的 Red Hat Virtualization 环

境。对于登录查询，请输入您的用户名和密码：

NOTE:

It is highly recommended to test drive the configuration before applying it into engine. Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login sequence.

Please provide credentials to test login flow:

Enter user name:

Enter user password:

[INFO] Executing login sequence...

...

[INFO] Login sequence executed successfully

12.

检查用户详情是否正确。如果用户详情不正确，请选择 **Abort**：

Please make sure that user details are correct and group membership meets expectations (search for PrincipalRecord and GroupRecord titles).

Abort if output is incorrect.

Select test sequence to execute (Done, Abort, Login, Search) [Abort]:

13.

建议手动测试搜索功能。对于搜索查询，请为用户帐户选择 **Principal**，或者为组帐户选择 **Group**。如果您希望返回用户帐户的组信息，对于 **Resolve Groups** 选择 **Yes**。会创建三个配置文件，并显示在屏幕输出中。

Select test sequence to execute (Done, Abort, Login, Search) [Search]: *Search*

Select entity to search (Principal, Group) [Principal]:

Term to search, trailing '*' is allowed: *testuser1*

Resolve Groups (Yes, No) [No]:

14.

选择 **Done** 以完成设置：

Select test sequence to execute (Done, Abort, Login, Search) [Abort]: *Done*

[INFO] Stage: Transaction setup

[INFO] Stage: Misc configuration

[INFO] Stage: Package installation

[INFO] Stage: Misc configuration

[INFO] Stage: Transaction commit

[INFO] Stage: Closing up

CONFIGURATION SUMMARY

Profile name is: *redhat.com*

The following files were created:

/etc/ovirt-engine/aaa/redhat.com.properties

/etc/ovirt-engine/extensions.d/redhat.com.properties

/etc/ovirt-engine/extensions.d/redhat.com-authn.properties

[INFO] Stage: Clean up

Log file is available at */tmp/ovirt-engine-extension-aaa-ldap-setup-20171004101225-*

```
mmneib.log:
[ INFO ] Stage: Pre-termination
[ INFO ] Stage: Termination
```

15.

重新启动 `ovirt-engine` 服务。您所创建的配置集现在包括在管理门户和虚拟机门户中。要在 LDAP 服务器上分配适当的角色和权限，如要登录虚拟机门户，请参阅 [Manager User Tasks](#)。

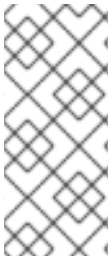
```
# systemctl restart ovirt-engine.service
```



注意

如需更多信息，请参阅 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-version` 中的 LDAP 身份验证和授权扩展 README 文件。

3.6.3.2. 附加 Active Directory



注意

`ovirt-engine-extension-aaa-ldap` 已被弃用。对于新安装，请使用 Red Hat Single Sign On。如需更多信息，请参阅《管理指南》中的 [安装和配置 Red Hat Single Sign-On](#)。

前提条件

- 您需要知道 Active Directory 林名称。林名称也称为根域名。



注意

`/usr/share/ovirt-engine-extension-aaa-ldap-setup` 工具中提供了最常见的 Active Directory 配置示例，它不能使用 `ovirt-engine-extension-aaa-ldap/examples/README.md` 提供。

- 您需要将可解析 Active Directory 林名称的 DNS 服务器添加到 Manager 上的 `/etc/resolv.conf` 文件，或者记下 Active Directory DNS 服务器，并在交互式设置脚本提示时输入它们。
- 要在 LDAP 服务器和 Manager 间设置安全连接，请确保已准备了 PEM 编码的 CA 证书。如需更多信息，请参阅在 [Manager 和 LDAP 服务器间设置 SSL 或 TLS 连接](#)。

- 除非支持匿名搜索，否则具有可浏览所有用户和组权限的用户必须可用于 **Active Directory**，才能用作搜索用户。请注意搜索用户的可识别名称(DN)。不要将管理员用户用于 **Active Directory**。
- 您必须至少有一个帐户名称和密码已就绪，才能对 **Active Directory** 执行搜索和登录查询。
- 如果您的 **Active Directory** 部署跨越多个域，请注意 `/usr/share/ovirt-engine-extension-aaa-ldap/profiles/ad.properties` 文件中所描述的限制。

流程

1. 在 Red Hat Virtualization Manager 中，安装 LDAP 扩展软件包：

```
# dnf install ovirt-engine-extension-aaa-ldap-setup
```

2. 运行 `ovirt-engine-extension-aaa-ldap-setup` 来启动交互式设置：

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. 输入对应数字来选择 LDAP 类型。此步骤后 LDAP 相关问题对于不同的 LDAP 类型是不同的。

```
Available LDAP implementations:
1 - 389ds
2 - 389ds RFC-2307 Schema
3 - Active Directory
4 - IBM Security Directory Server
5 - IBM Security Directory Server RFC-2307 Schema
6 - IPA
7 - Novell eDirectory RFC-2307 Schema
8 - OpenLDAP RFC-2307 Schema
9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
11 - RFC-2307 Schema (Generic)
12 - RHDS
13 - RHDS RFC-2307 Schema
14 - iPlanet
Please select: 3
```

4. 输入 **Active Directory** 林名称。如果 Manager 的 DNS 无法解析林名称，该脚本会提示您输入一个空格分隔的 **Active Directory** DNS 服务器名称列表。

```
Please enter Active Directory Forest name: ad-example.redhat.com
[ INFO ] Resolving Global Catalog SRV record for ad-example.redhat.com
[ INFO ] Resolving LDAP SRV record for ad-example.redhat.com
```

5.

选择 LDAP 服务器支持的安全连接方法，并指定获取 PEM 编码的 CA 证书的方法。file 选项允许您提供证书的完整路径。URL 选项允许您指定证书的 URL。使用 inline 选项，将证书的内容粘贴到终端中。system 选项允许您指定所有 CA 文件的位置。insecure 选项允许您在不安全模式中使用 startTLS。

NOTE:

It is highly recommended to use secure protocol to access the LDAP server.

Protocol startTLS is the standard recommended method to do so.

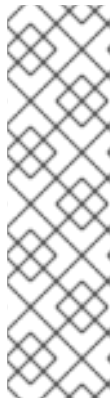
Only in cases in which the startTLS is not supported, fallback to non standard ldaps protocol.

Use plain for test environments only.

Please select protocol to use (startTLS, ldaps, plain) [startTLS]: *startTLS*

Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure): *File*

Please enter the password:

**注意**

LDAPS 代表覆盖安全套接字链接的轻量级目录访问协议。对于 SSL 连接，请选择 ldaps 选项。

有关创建 PEM 编码的 CA 证书的更多信息，请参阅在 [Manager](#) 和 [LDAP 服务器](#) 间设置 [SSL 或 TLS 连接](#)。

6.

输入搜索用户可分辨名称(DN)。用户必须具有权限才能浏览目录服务器上的所有用户和组。搜索用户必须是 LDAP 注解。如果允许匿名搜索，请按 Enter 键，无需输入。

```
Enter search user DN (empty for anonymous):
cn=user1,ou=Users,dc=test,dc=redhat,dc=com
Enter search user password:
```

7.

指定是否为虚拟机使用单点登录。此功能默认是启用的，但如果启用了管理门户的单点登录，则无法使用。该脚本提醒您配置集名称必须与域名匹配。在虚拟机管理指南中，您仍需要遵循 [为虚拟机配置单点登录](#) 的说明。

```
Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]:
```

8.

指定配置集名称。配置集名称对登录页面上的用户可见。这个示例使用 `redhat.com`。

Please specify profile name that will be visible to users:`redhat.com`

图 3.2. 管理门户登录页面



注意

第一次登录时，用户需要从下拉列表中选择所需的配置集。然后，信息会存储在浏览器 **Cookie** 中，并在用户下一次登录时预选择。

9.

测试搜索和登录功能，以确保您的 **LDAP** 服务器已正确地连接到您的 **Red Hat Virtualization** 环境。对于登录查询，请输入帐户名称和密码。对于搜索查询，为用户帐户选择 **Principal**，然后选择 **Group for group for group**。如果您希望返回用户帐户的组帐户信息，对于 **Resolve Groups** 选择 **Yes**。选择 **Done** 以完成设置。会创建三个配置文件，并显示在屏幕输出中。

NOTE:

It is highly recommended to test drive the configuration before applying it into engine. Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login sequence.

Select test sequence to execute (Done, Abort, Login, Search) [Abort]: Login

Enter search user name: `testuser1`

Enter search user password:

[INFO] Executing login sequence...

...

Select test sequence to execute (Done, Abort, Login, Search) [Abort]: Search

Select entity to search (Principal, Group) [Principal]:

Term to search, trailing '*' is allowed: `testuser1`

Resolve Groups (Yes, No) [No]:

```

[ INFO ] Executing login sequence...
...
Select test sequence to execute (Done, Abort, Login, Search) [Abort]: Done
[ INFO ] Stage: Transaction setup
[ INFO ] Stage: Misc configuration
[ INFO ] Stage: Package installation
[ INFO ] Stage: Misc configuration
[ INFO ] Stage: Transaction commit
[ INFO ] Stage: Closing up
    CONFIGURATION SUMMARY
    Profile name is: redhat.com
    The following files were created:
        /etc/ovirt-engine/aaa/redhat.com.properties
        /etc/ovirt-engine/extensions.d/redhat.com-authz.properties
        /etc/ovirt-engine/extensions.d/redhat.com-authn.properties
[ INFO ] Stage: Clean up
    Log file is available at /tmp/ovirt-engine-extension-aaa-ldap-setup-20160114064955-
    1yar9i.log:
[ INFO ] Stage: Pre-termination
[ INFO ] Stage: Termination

```

10.

您所创建的配置集现在包括在管理门户和虚拟机门户中。要在 LDAP 服务器上分配适当的角色和权限，如要登录虚拟机门户，请参阅 [Manager User Tasks](#)。



注意

如需更多信息，请参阅 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-version` 中的 LDAP 身份验证和授权扩展 README 文件。

3.6.3.3. 配置外部 LDAP 提供程序(Manual Method)



注意

`ovirt-engine-extension-aaa-ldap` 已被弃用。对于新安装，请使用 Red Hat Single Sign On。如需更多信息，请参阅《管理指南》中的 [安装和配置 Red Hat Single Sign On](#)。

`ovirt-engine-extension-aaa-ldap` 扩展使用 LDAP 协议访问目录服务器并可完全自定义。除非您要启用对虚拟机门户的单点登录或管理门户功能，否则不需要 Kerberos 身份验证。

如果上一节中的交互式设置方法没有涵盖您的用例，您可以手动修改配置文件以附加 LDAP 服务器。以下流程使用通用详情。具体值取决于您的设置。

流程

1. 在 Red Hat Virtualization Manager 中，安装 LDAP 扩展软件包：

```
# dnf install ovirt-engine-extension-aaa-ldap
```

2. 将 LDAP 配置模板文件复制到 `/etc/ovirt-engine` 目录中。模板文件可用于活动目录(ad)和其他目录类型(简单)。这个示例使用简单的配置模板。

```
# cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple/. /etc/ovirt-engine
```

3. 重命名配置文件，以匹配您希望对管理门户和虚拟机门户中用户可见的配置集名称：

```
# mv /etc/ovirt-engine/aaa/profile1.properties /etc/ovirt-engine/aaa/example.properties
# mv /etc/ovirt-engine/extensions.d/profile1-authn.properties /etc/ovirt-engine/extensions.d/example-authn.properties
# mv /etc/ovirt-engine/extensions.d/profile1-authz.properties /etc/ovirt-engine/extensions.d/example-authz.properties
```

4. 通过取消注释 LDAP 服务器类型并更新域和密码字段来编辑 LDAP 属性配置文件：

```
# vi /etc/ovirt-engine/aaa/example.properties
```

例 3.5. 示例配置集：LDAP server 部分

```
# Select one
#
include = <openldap.properties>
#include = <389ds.properties>
#include = <rhds.properties>
#include = <ipa.properties>
#include = <iplanet.properties>
#include = <rfc2307-389ds.properties>
#include = <rfc2307-rhds.properties>
#include = <rfc2307-openldap.properties>
#include = <rfc2307-edir.properties>
#include = <rfc2307-generic.properties>

# Server
#
vars.server = ldap1.company.com

# Search user and its password.
#
vars.user = uid=search,cn=users,cn=accounts,dc=company,dc=com
vars.password = 123456
```

```
pool.default.serverset.single.server = ${global:vars.server}
pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}
```

要使用 TLS 或 SSL 协议与 LDAP 服务器交互，请获取 LDAP 服务器的 root CA 证书，并使用它来创建公共密钥存储文件。取消注释以下行，并指定 public 密钥存储文件的完整路径，以及用于访问该文件的密码。



注意

有关创建公共密钥存储文件的更多信息，请参阅在 [Manager 和 LDAP 服务器之间设置 SSL 或 TLS 连接](#)。

例 3.6. profile: keystore 部分示例

```
# Create keystore, import certificate chain and uncomment
# if using tls.
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = /full/path/to/myrootca.jks
pool.default.ssl.truststore.password = password
```

5.

检查身份验证配置文件。该配置集在管理门户中对用户可见，并且虚拟机门户登录页面由 `ovirt.engine.aaa.authn.profile.name` 定义。配置配置文件位置必须与 LDAP 配置文件位置匹配。所有字段都可保留为默认值。

```
# vi /etc/ovirt-engine/extensions.d/example-authn.properties
```

例 3.7. 身份验证配置文件示例

```
ovirt.engine.extension.name = example-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa ldap.AuthnExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = example
ovirt.engine.aaa.authn.authz.plugin = example-authz
config.profile.file.1 = ../aaa/example.properties
```

6.

检查授权配置文件。配置配置文件位置必须与 LDAP 配置文件位置匹配。所有字段都可保留为默认值。


```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

例 3.8. 授权配置文件示例

```
ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.ldap.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties
```

7.

确保配置集的所有权和权限是适当的：

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
# chmod 600 /etc/ovirt-engine/aaa/example.properties
```

8.

重启引擎服务：

```
# systemctl restart ovirt-engine.service
```

9.

您所创建的示例配置集现在包括在管理门户和虚拟机门户中。要为 LDAP 服务器上的用户帐户提供适当的权限，例如，要登录到虚拟机门户，请参阅 [Manager User Tasks](#)。



注意

如需更多信息，请参阅 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-version` 中的 LDAP 身份验证和授权扩展 README 文件。

3.6.3.4. 删除外部 LDAP 供应商

此流程演示了如何删除外部配置的 LDAP 供应商及其用户。

流程

1.

删除 LDAP 供应商配置文件，替换默认名称 `profile1`：

```
# rm /etc/ovirt-engine/extensions.d/profile1-authn.properties
# rm /etc/ovirt-engine/extensions.d/profile1-authz.properties
# rm /etc/ovirt-engine/aaa/profile1.properties
```

2.

重启 `ovirt-engine` 服务：

```
# systemctl restart ovirt-engine
```

3.

在管理门户中，在 **Users** 资源选项卡中，选择此提供程序的用户(授权 提供程序是 `profile1-authz`)，然后单击 **Remove**。

3.6.4. 为单点登录配置 LDAP 和 Kerberos

单点登录允许用户在不重新输入密码的情况下登录到虚拟机门户或管理门户。从 Kerberos 服务器获取身份验证凭据。要将单点登录配置为管理门户和虚拟机门户，您需要配置两个扩展：`ovirt-engine-extension-aaa-misc` 和 `ovirt-engine-extension-aaa-ldap`；和两个 Apache 模块：`mod_auth_gssapi` 和 `mod_session`。您可以配置不涉及 Kerberos 的单点登录，但这超出了本文档的范围。



注意

如果启用了虚拟机门户的单点登录，则无法对虚拟机的单点登录。启用虚拟机门户的单点登录后，虚拟机门户不需要接受密码，因此您就无法将密码委派至虚拟机。

本例假定以下几项：

- 现有密钥分发中心(KDC)服务器使用 MIT 版本的 Kerberos 5。
- 您有 KDC 服务器的管理权限。
- Kerberos 客户端安装在 Red Hat Virtualization Manager 和用户机器上。
- `kadmin` 工具用于创建 Kerberos 服务主体和 `keytab` 文件。

这个过程涉及以下组件：

- 在 KDC 服务器中
 - 在 Red Hat Virtualization Manager 上为 Apache 服务创建服务主体和 keytab 文件。
- On the Red Hat Virtualization Manager
 - 安装身份验证和授权扩展软件包和 Apache Kerberos 身份验证模块。
 - 配置扩展文件。

3.6.4.1. 为 Apache 服务配置 Kerberos

1. 在 KDC 服务器中，使用 `kadmin` 实用程序在 Red Hat Virtualization Manager 中为 Apache 服务创建服务主体。服务主体是 Apache 服务的 KDC 的引用 ID。

```
# kadmin
kadmin> addprinc -randkey HTTP/fqdn-of-rhevm@REALM.COM
```

2. 为 Apache 服务生成 keytab 文件。keytab 文件存储共享 secret 密钥。



注意

`engine-backup` 命令在备份和恢复时包括文件 `/etc/httpd/http.keytab`。如果您在 keytab 文件中使用不同的名称，请确保备份和恢复它。

```
kadmin> ktadd -k /tmp/http.keytab HTTP/fqdn-of-rhevm@REALM.COM
kadmin> quit
```

3. 将 keytab 文件从 KDC 服务器复制到 Red Hat Virtualization Manager:

```
# scp /tmp/http.keytab root@rhevm.example.com:/etc/httpd
```

== 将单点登录配置为虚拟机门户或管理门户

4. 在 Red Hat Virtualization Manager 中，确保 keytab 的所有权和权限是适当的：

```
# chown apache /etc/httpd/http.keytab
# chmod 400 /etc/httpd/http.keytab
```

5. 安装身份验证扩展软件包、LDAP 扩展软件包以及 mod_auth_gssapi 和 mod_session Apache 模块：

```
# dnf install ovirt-engine-extension-aaa-misc ovirt-engine-extension-aaa-ldap
mod_auth_gssapi mod_session
```



注意

ovirt-engine-extension-aaa-ldap 已被弃用。对于新安装，请使用 Red Hat Single Sign On。如需更多信息，请参阅《管理指南》中的 [安装和配置 Red Hat Single Sign-On](#)。

6. 将 SSO 配置模板文件复制到 /etc/ovirt-engine 目录中。模板文件可用于 Active Directory (ad-ssso) 和其他目录类型 (simple-ssso)。本例使用简单的 SSO 配置模板。

```
# cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple-ssso/. /etc/ovirt-engine
```

7. 将 ovirt-ssso.conf 移到 Apache 配置目录中。



注意

engine-backup 命令在备份和恢复时包含文件 /etc/httpd/conf.d/ovirt-ssso.conf。如果您对此文件使用不同的名称，请确保备份和恢复它。

```
# mv /etc/ovirt-engine/aaa/ovirt-ssso.conf /etc/httpd/conf.d
```

8. 检查验证方法文件。您不需要编辑此文件，因为域会自动从 keytab 文件中获取。

```
# vi /etc/httpd/conf.d/ovirt-ssso.conf
```

例 3.9. 身份验证方法文件示例

```

<LocationMatch ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/token-http-
auth)|^/ovirt-engine/api>
  <If "req('Authorization') !~ /^(Bearer|Basic)/i">
    RewriteEngine on
    RewriteCond %{LA-U:REMOTE_USER} ^(.*)$
    RewriteRule ^(.*)$ - [L,NS,P,E=REMOTE_USER:%1]
    RequestHeader set X-Remote-User %{REMOTE_USER}s

    AuthType GSSAPI
    AuthName "Kerberos Login"

    # Modify to match installation
    GssapiCredStore keytab:/etc/httpd/http.keytab
    GssapiUseSessions On
    Session On
    SessionCookieName ovirt_gssapi_session path=/private;httponly;secure;

    Require valid-user
    ErrorDocument 401 "<html><meta http-equiv='refresh' content='0'; url=/ovirt-
engine/sso/login-unauthorized"/><body><a href="/ovirt-engine/sso/login-
unauthorized">Here</a></body></html>"
  </If>
</LocationMatch>

```

9.

重命名配置文件，以匹配您希望对管理门户和虚拟机门户中用户可见的配置集名称：

```
# mv /etc/ovirt-engine/aaa/profile1.properties /etc/ovirt-engine/aaa/example.properties
```

```
# mv /etc/ovirt-engine/extensions.d/profile1-http-authn.properties /etc/ovirt-
engine/extensions.d/example-http-authn.properties
```

```
# mv /etc/ovirt-engine/extensions.d/profile1-http-mapping.properties /etc/ovirt-
engine/extensions.d/example-http-mapping.properties
```

```
# mv /etc/ovirt-engine/extensions.d/profile1-authz.properties /etc/ovirt-
engine/extensions.d/example-authz.properties
```

10.

通过取消注释 LDAP 服务器类型并更新域和密码字段来编辑 LDAP 属性配置文件：

```
# vi /etc/ovirt-engine/aaa/example.properties
```

例 3.10. 示例配置集：LDAP server 部分

```

# Select one
include = <openldap.properties>
#include = <389ds.properties>
#include = <rhds.properties>
#include = <ipa.properties>

```

```

#include = <iplanet.properties>
#include = <rfc2307-389ds.properties>
#include = <rfc2307-rhds.properties>
#include = <rfc2307-openldap.properties>
#include = <rfc2307-edir.properties>
#include = <rfc2307-generic.properties>

# Server
#
vars.server = ldap1.company.com

# Search user and its password.
#
vars.user = uid=search,cn=users,cn=accounts,dc=company,dc=com
vars.password = 123456

pool.default.serverset.single.server = ${global:vars.server}
pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}

```

要使用 TLS 或 SSL 协议与 LDAP 服务器交互，请获取 LDAP 服务器的 root CA 证书，并使用它来创建公共密钥存储文件。取消注释以下行，并指定 public 密钥存储文件的完整路径，以及用于访问该文件的密码。



注意

有关创建公共密钥存储文件的更多信息，请参阅在 [Manager](#) 和 [LDAP 服务器](#) 之间设置 [SSL 或 TLS 连接](#)。

例 3.11. profile: keystore 部分示例

```

# Create keystore, import certificate chain and uncomment
# if using ssl/tls.
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = /full/path/to/myrootca.jks
pool.default.ssl.truststore.password = password

```

11.

检查身份验证配置文件。该配置集在管理门户中对用户可见，并且虚拟机门户登录页面由 `ovirt.engine.aaa.authn.profile.name` 定义。配置配置文件位置必须与 LDAP 配置文件位置匹配。所有字段都可保留为默认值。

```
# vi /etc/ovirt-engine/extensions.d/example-http-authn.properties
```

例 3.12. 身份验证配置文件示例

```
ovirt.engine.extension.name = example-http-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthnExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = example-http
ovirt.engine.aaa.authn.authz.plugin = example-authz
ovirt.engine.aaa.authn.mapping.plugin = example-http-mapping
config.artifact.name = HEADER
config.artifact.arg = X-Remote-User
```

12.

检查授权配置文件。配置配置文件位置必须与 LDAP 配置文件位置匹配。所有字段都可保留为默认值。

```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

例 3.13. 授权配置文件示例

```
ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.ldap.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties
```

13.

检查验证映射配置文件。配置配置文件位置必须与 LDAP 配置文件位置匹配。配置配置集扩展名称必须与身份验证配置文件中的 `ovirt.engine.aaa.authn.mapping.plugin` 值匹配。所有字段都可保留为默认值。

```
# vi /etc/ovirt-engine/extensions.d/example-http-mapping.properties
```

例 3.14. 身份验证映射文件示例

```
ovirt.engine.extension.name = example-http-mapping
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.mapping.MappingExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Mapping
config.mapAuthRecord.type = regex
config.mapAuthRecord.regex.mustMatch = true
```

```
config.mapAuthRecord.regex.pattern = ^(?<user>.*?)(\\|\/(?<at>@)(?<suffix>.*?)@.*|(?<realm>@.*))$
config.mapAuthRecord.regex.replacement = ${user}${at}${suffix}
```

14.

确保配置文件的所有权和权限是适当的：

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-http-authn.properties
# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-http-mapping.properties
# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-authz.properties
# chmod 600 /etc/ovirt-engine/aaa/example.properties
# chmod 640 /etc/ovirt-engine/extensions.d/example-http-authn.properties
# chmod 640 /etc/ovirt-engine/extensions.d/example-http-mapping.properties
# chmod 640 /etc/ovirt-engine/extensions.d/example-authz.properties
```

15.

重启 Apache 服务和 ovirt-engine 服务：

```
# systemctl restart httpd.service
# systemctl restart ovirt-engine.service
```

3.6.5. 安装和配置红帽单点登录

要使用 Red Hat Single Sign-On 作为您的授权方法，您需要：

- 安装 Red Hat SSO。
- 配置 LDAP 组映射程序。
- 在 Manager 中配置 Apache。

- 配置 OVN 提供程序凭据。
- 配置监控门户(Grafana)



注意

如果配置了 Red Hat SSO，之前的 LDAP 符号将无法正常工作，因为一次只能使用单个授权协议。

3.6.5.1. Installing Red Hat SSO

您可以通过下载 ZIP 文件并解包它，或使用 RPM 文件来安装 Red Hat Single Sign-On。

按照 [Red Hat SSO](#) 安装中的安装说明

准备以下信息：

- Open ID Connect 服务器的路径/位置。
- 正确的仓库的订阅频道。
- 有效的红帽订阅登录凭证。

3.6.5.2. 配置 LDAP 组映射器

流程

1. 使用以下信息添加 LDAP 组映射程序：
 - 名称：ldapgroups

- 映射器类型 : `group-ldap-mapper`
 - LDAP 组 DN: `ou=groups,dc=example,dc=com`
 - 组对象类 : `组ofuniquenames` (*根据您的 LDAP 服务器设置调整本课程*)
 - 成员资格 LDAP 属性 : `唯一的成员` (*根据您的 LDAP 服务器设置 调整这个类*)
2. 点 **Save**。
 3. 单击 **Sync LDAP Groups to KeyCloak**。
 4. 在 **User Federation Provider** 页面的底部, 单击 **Synchronize all users**。
 5. 在 **Clients** 选项卡中, 在 **Add Client** 下, 添加 `ovirt-engine` 作为客户端 ID, 并输入 `engine url` 作为 **Root URL**。
 6. 修改 客户端协议, 以 `openid-connect` 和 **Access Type to 机密**。
 7. 在 **Clients** 选项卡中, 在 **Ovirt-engine > Advanced Settings** 下, 增大 **Access Token Lifespan**。
 8. 添加 `https://rhvm.example.com:443/*` 作为有效的重定向 **URI**。
 9. 已生成客户端 `secret`, 可以在 **Credentials** 选项卡中查看。
 10. 在" **创建映射程序协议** "下的" **客户端** "选项卡中, 使用以下设置创建一个映射程序 :
 - 名称 : 组

- 映射器类型 : Group Membership
- 令牌声明名称 : 组
- 完整组路径:ON
- 添加到 ID 令牌:ON
- 添加到访问令牌:ON
- 添加到 userinfo:ON

11. 为用户名添加内置协议映射程序。
12. 创建 `ovirt-engine`、`ovirt-app-api`、`ovirt-app-admin` 和 `ovirt-ext=auth:sequence-priority=~` 所需的范围。
13. 使用上一步中创建的范围来为 `ovirt-engine` 客户端设置可选客户端范围。

3.6.5.3. 在 Manager 中配置 Apache

1. 启用 `mod_auth_openidc` 模块。

```
# dnf module enable mod_auth_openidc:2.3 -y
```

2. 在 Manager 中配置 Apache

```
# dnf install mod_auth_openidc
```

3. 使用以下内容，在 `/etc/httpd/conf.d/` 中数据一个新的 `httpd` 配置文件 `ovirt-openidc.conf` :

■

```

LoadModule auth_openidc_module modules/mod_auth_openidc.so

OIDCProviderMetadataURL https://SSO.example.com/auth/realms/master/.well-known/openid-configuration
OIDCSSLValidateServer Off

OIDCClientID ovirt-engine
OIDCClientSecret <client_SSO_generated_key>
OIDCRedirectURI https://rhvm.example.com/ovirt-engine/callback
OIDCDefaultURL https://rhvm.example.com/ovirt-engine/login?scope=ovirt-app-admin+ovirt-app-portal+ovirt-ext%3Dauth%3Asequence-priority%3D%7E

# maps the preferred_username claim to the REMOTE_USER environment variable:

OIDCRemoteUserClaim <preferred_username>
OIDCCryptoPassphrase <random1234>

<LocationMatch ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/token-http-auth)|^/ovirt-engine/callback>
  <If "req('Authorization') !~ /^(Bearer|Basic)/i">

    Require valid-user
    AuthType openid-connect

    ErrorDocument 401 "<html><meta http-equiv='refresh' content='0'; url=/ovirt-engine/sso/login-unauthorized"/><body><a href="/ovirt-engine/sso/login-unauthorized"/>Here</a></body></html>"
    </If>
  </LocationMatch>

OIDCOAuthIntrospectionEndpoint
https://SSO.example.com/auth/realms/master/protocol/openid-connect/token/introspect
OIDCOAuthSSLValidateServer Off
OIDCOAuthIntrospectionEndpointParams token_type_hint=access_token
OIDCOAuthClientID ovirt-engine
OIDCOAuthClientSecret <client_SSO_generated_key>
OIDCOAuthRemoteUserClaim sub

<LocationMatch ^/ovirt-engine/(api$|api/)>
  AuthType oauth20
  Require valid-user
</LocationMatch>

```

4.

要保存配置更改，请重启 **httpd** 和 **ovirt-engine**：

```

# systemctl restart httpd
# systemctl restart ovirt-engine

```

5.

在 **/etc/ovirt-engine/extensions.d/** 中创建文件 **openidc-authn.properties**，其内容如下：

```

ovirt.engine.extension.name = openidc-authn

```

```
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthnExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = openidhttp
ovirt.engine.aaa.authn.authz.plugin = openidc-authz
ovirt.engine.aaa.authn.mapping.plugin = openidc-http-mapping
config.artifact.name = HEADER
config.artifact.arg = OIDC_CLAIM_preferred_username
```

6.

在 `/etc/ovirt-engine/extensions.d/` 中创建文件 `openidc-http-mapping.properties`，其内容如下：

```
ovirt.engine.extension.name = openidc-http-mapping
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.mapping.MappingExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Mapping
config.mapAuthRecord.type = regex
config.mapAuthRecord.regex.mustMatch = false
config.mapAuthRecord.regex.pattern = ^(?<user>.*?)(\\|\\|(?<at>@)(?<suffix>.*?)@.*|(?
<realm>@.*))$
config.mapAuthRecord.regex.replacement = ${user}${at}${suffix}
```

7.

在 `/etc/ovirt-engine/extensions.d/` 中创建文件 `openidc-authz.properties`，其内容如下：

```
ovirt.engine.extension.name = openidc-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.artifact.name.arg = OIDC_CLAIM_preferred_username
config.artifact.groups.arg = OIDC_CLAIM_groups
```

8.

在 `/etc/ovirt-engine/engine.conf.d/` 中创建文件 `99-enable-external-auth.conf`，其内容如下：

```
ENGINE_SSO_ENABLE_EXTERNAL_SSO=true
ENGINE_SSO_EXTERNAL_SSO_LOGOUT_URI="${ENGINE_URI}/callback"
EXTERNAL_OIDC_USER_INFO_END_POINT=https://SSO.example.com/auth/realms/master
/protocol/openid-connect/userinfo
EXTERNAL_OIDC_TOKEN_END_POINT=https://SSO.example.com/auth/realms/master/pr
otocol/openid-connect/token
EXTERNAL_OIDC_LOGOUT_END_POINT=https://SSO.example.com/auth/realms/master/pr
otocol/openid-connect/logout
EXTERNAL_OIDC_CLIENT_ID=ovirt-engine
```

```
EXTERNAL_OIDC_CLIENT_SECRET="<client_SSO_generated_key>"
EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE_PASSWORD=""
EXTERNAL_OIDC_SSL_VERIFY_CHAIN=false
EXTERNAL_OIDC_SSL_VERIFY_HOST=false
```

3.6.5.4. 配置 OVN

如果您在 Manager 中配置了 `ovirt-ovn-provider`，则需要配置 OVN 供应商凭证。

流程

1. 使用以下内容在 `/etc/ovirt-provider-ovn/conf.d/` 中创建文件 `20-setup-ovirt-provider-ovn.conf`，其中 `user1` 属于 LDAP 组 `ovirt-administrator`，`openidhttp` 是为 `aaa-ldap-misc` 配置的配置集。

```
[OVIRT]
ovirt-admin-user-name=user1@openidhttp
```

2. 重启 `ovirt-provider-ovn`：

```
# systemctl restart ovirt-provider-ovn
```

3. 登录管理门户，导航到 **Administration** → **Providers**，选择 `ovirt-provider-ovn`，然后单击 **Edit** 以更新 `ovn` 提供程序的密码。

3.6.5.5. 配置监控门户(Grafana)

流程

1. 配置客户端的有效重定向 URL：
 - a. 选择前面步骤中配置的客户端（例如 `ovirt-engine`）
 - b. 为 **Monitoring Portal (Grafana)** 添加额外的有效的重定向 URI。有效的 **Redirect URI**: `https://rhvm.example.com:443/ovirt-engine-grafana/login/generic_oauth/`
 - c. 选择"映射程序"选项卡。

d. 点击 **Create** 以创建新映射程序，并填写以下字段：

- **Name: realm 角色**
- **映射器类型： User Realm Role**
- **令牌声明名称： realm_access.roles**
- **claim JSON Type: String**

2. 配置特定于 Grafana 的角色：

a. 从主菜单中选择 **Roles**。

b. 添加以下角色： **管理员、编辑器 查看器**。

3. 为所需组分配 Grafana 特定角色：

a. 从主菜单中选择 **组**，然后选择所需组。

b. 选择 **Role 映射**。

c. 将所需的角色从 **Available Roles** 移到 **Assigned Roles** 中。

4. 配置 Grafana - 修改 `/etc/grafana/grafana.ini` 中的 `auth.generic_oauth` 部分，如下所示。根据需要替换箭头方括号 `<>` 中的值。

```
(...)
##### Generic OAuth #####
[auth.generic_oauth]
name = oVirt Engine Auth
```

```
enabled = true
allow_sign_up = true
client_id = ovirt-engine
client_secret = <client-secret-of-RH-SSO>
scopes = openid,ovirt-app-admin,ovirt-app-portal,ovirt-ext=auth:sequence-priority=~
email_attribute_name = email:primary
role_attribute_path = "contains(realm_access.roles[*], 'admin') && 'Admin' ||
contains(realm_access.roles[*], 'editor') && 'Editor' || 'Viewer'"
auth_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-
connect/auth
token_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-
connect/token
api_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-
connect/userinfo
team_ids =
allowed_organizations =
tls_skip_verify_insecure = false
tls_client_cert =
tls_client_key =
tls_client_ca = /etc/pki/ovirt-engine/apache-ca.pem
send_client_credentials_via_post = false
(...)
```

3.6.6. 用户授权

3.6.6.1. 用户授权模型

Red Hat Virtualization 根据三个组件的组合应用授权控制：

- 执行操作的用户
- 正在执行的操作类型
- 操作要对其执行的对象

3.6.6.2. 用户操作

要成功执行某个操作，用户必须具有正在操作的对象适当权限。每种类型的操作都具有相应的权限。

在多个对象上执行一些操作。例如，将模板复制到另一个存储域将影响模板和目标存储域。执行操作的用户必须具有操作所影响的所有对象的适当权限。

3.6.7. 从管理门户管理用户任务

3.6.7.1. 帐户设置窗口

Administration → **Account Settings** 窗口允许您查看或编辑以下管理门户用户设置：

- **常规 标签：**
 - **用户名 - 只读。**
 - **电子邮件 - 只读。**
 - **主页：**
 - 默认 - #dashboard-main。
 - 自定义主页 - 仅输入 URL 的最后一部分，包括 hash 标记(#)。例如：#vms-snapshots;name-testVM。
 - **串行控制台**
 - 用户的公钥 - 输入用于使用串行控制台访问 **Manager** 的 SSH 公钥。
 - **表**
 - 永久网格设置 - 保存服务器上的网格列设置。
- **确认 标签页：**
 - 在 **Suspend VM** 上显示确认对话框 - 在虚拟机被暂停时启用确认对话框。

3.6.7.2. 添加用户和分配虚拟机门户权限

用户必须创建好，然后才能添加和分配角色和权限。此流程中分配的角色和权限授予用户登录到虚拟机门户的权限，并开始创建虚拟机。该流程也适用于组帐户。

流程

1. 在标题栏中，单击 **Administration** → **Configure**。这将打开 **Configure** 窗口。
2. 点 **System Permissions**。
3. 点 **Add**。此时将打开 **Add System Permission to User** 窗口。
4. 在搜索 下选择一个配置集。该配置集是您要搜索的域。在搜索文本字段中输入名称或部分，然后点 **GO**。或者，单击 "运行"以查看所有用户和组的列表。
5. 为适当的用户或组选中复选框。
6. 选择要分配在 **Role to Assign** 下的相应角色。**UserRole** 角色授予用户登录虚拟机门户的权限。
7. 点击 **OK**。

登录虚拟机门户，以验证用户帐户是否具有登录的权限。

3.6.7.3. 查看用户信息

流程

1. 单击 **Administration** → **Users** 以显示授权用户列表。
2. 点用户名。这会打开详情视图，通常使用 常规选项卡 显示常规信息，如用户名、电子邮件和状态。

3. 其他标签页允许您为用户查看组、权限、配额和事件。

例如，要查看用户所属的组，请单击 **Directory Groups** 选项卡。

3.6.7.4. 查看用户权限资源

可以为用户分配特定资源的权限或资源层次结构。您可以查看分配的用户及其对每个资源的权限。

流程

1. 查找并单击资源名称。这会打开详情视图。
2. 单击 **Permissions** 选项卡，以列出分配的用户、用户的角色以及所选资源的继承权限。

3.6.7.5. 删除用户

当不再需要用户帐户时，将其从 **Red Hat Virtualization** 中删除。

流程

1. 单击 **Administration** → **Users** 以显示授权用户列表。
2. 选择要删除的用户。确保用户没有运行任何虚拟机。
3. 单击 **Remove**，然后单击确定。

用户已从 **Red Hat Virtualization** 中删除，但不从外部目录中删除。

3.6.7.6. 查看 Logged-In 用户

您可以查看当前登录的用户，以及会话时间和其他详情。点 **Administration** → **Active User Sessions** 查看每个登录的用户的 **Session DB ID**, **User Name**, **Authorization provider**, **User id**, **Source IP**, **Session Start Time**, 和 **Session Last Active Time**。

3.6.7.7. 终止用户会话

您可以终止当前登录的用户会话。

终止用户会话

1. 单击 **Administration** → **Active User Sessions**。
2. 选择要终止的用户会话。
3. 点 **Terminate Session**。
4. 单击 **OK**。

3.6.8. 从命令行管理用户任务

您可以使用 `ovirt-aaa-jdbc-tool` 工具管理内部域中的用户帐户。使用工具所做的更改立即生效，不需要您重新启动 `ovirt-engine` 服务。如需用户选项的完整列表，请运行 `ovirt-aaa-jdbc-tool user --help`。本节中提供了常见示例。



重要

您必须登录到 **Manager** 机器。

3.6.8.1. 创建新用户

您可以创建新用户帐户。可选的 `--attribute` 命令指定帐户详情。如需完整的选项列表，请运行 `ovirt-aaa-jdbc-tool user add --help`。

```
# ovirt-aaa-jdbc-tool user add test1 --attribute=firstName=John --attribute=lastName=Doe
adding user test1...
user added successfully
```

您可以在管理门户中添加新创建的用户，并为用户分配相应的角色和权限。如需更多信息，请参阅添加用户。

3.6.8.2. 设置用户密码

您可以创建密码。您必须为 `--password-valid-to` 设置一个值，否则密码到期时间默认为当前时间。

+ 日期格式为 `yyyy-MM-dd HH:mm:ssX`。其中 X 是 UTC 中的时区偏移。在这个示例中，`-0800` 代表 GMT minus 8 小时。对于零偏移，请使用值 `Z`。

+ 如需了解更多选项，请运行 `ovirt-aaa-jdbc-tool user password-reset --help`。

```
# ovirt-aaa-jdbc-tool user password-reset test1 --password-valid-to="2025-08-01 12:00:00-0800"
Password:
updating user test1...
user updated successfully
```

注意

默认情况下，内部域中用户帐户的密码策略有以下限制：

- 至少 6 个字符。
- 密码更改时，不能再次设置先前使用的密码。

如需有关密码策略和其他默认设置的更多信息，请运行 `ovirt-aaa-jdbc-tool` 设置可显示。

更新 `admin` 密码后，必须手动将更改传播到 `ovirt-provider-ovn`。否则，`admin` 用户将被锁定，因为 Red Hat Virtualization Manager 将继续使用旧密码来同步来自 `ovirt-provider-ovn` 的网络。要将新密码检查为 `ovirt-provider-ovn`，请执行以下操作：

1. 在管理门户中，单击 **Administration** → **Providers**。
2. 选择 `ovirt-provider-ovn`。

3. 单击 **Edit**，然后在 **Password** 字段中输入新密码。
4. 单击 **Test** 以测试身份验证是否使用您提供的凭证成功。
5. 身份验证测试成功后，单击 **确定**。

3.6.8.3. 设置用户超时

您可以设置用户超时时间：

```
# engine-config --set UserSessionTimeOutInterval=integer
```

3.6.8.4. 预加密用户密码

您可以使用 `ovirt-engine-crypto-tool` 脚本创建预加密用户密码。如果您要通过脚本将用户和密码添加到数据库，则此选项很有用。



注意

密码以加密的形式存储在 **Manager** 数据库中。使用 `ovirt-engine-crypto-tool` 脚本，因为所有密码都必须使用相同的算法加密。

如果预加密密码，则无法执行密码有效期测试。即使密码不符合密码验证策略，也会接受密码。

1. 运行以下命令：

```
# /usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh pbe-encode
```

该脚本将提示您输入密码。

或者，您可以使用 `--password=file: file` 选项来加密显示为文件的第一行的单个密码。这个选项对自动化非常有用。在以下示例中，**文件**是包含单个密码用于加密的文本文件：

```
# /usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh pbe-encode --  
password=file:file
```

2. 使用 `--encrypted` 选项，使用 `ovirt-aaa-jdbc-tool` 脚本设置新密码：

```
# ovirt-aaa-jdbc-tool user password-reset test1 --password-valid-to="2025-08-01  
12:00:00-0800" --encrypted
```

3. 输入并确认加密的密码：

```
Password:  
Reenter password:  
updating user test1...  
user updated successfully
```

3.6.8.5. 查看用户信息

您可以查看详细的用户帐户信息：

```
# ovirt-aaa-jdbc-tool user show test1
```

此命令显示比 **Administration** → **Users** 屏幕中更多的信息。

3.6.8.6. 编辑用户信息

您可以更新用户信息，如电子邮件地址：

```
# ovirt-aaa-jdbc-tool user edit test1 --attribute=email=jdoe@example.com
```

3.6.8.7. 删除用户

您可以删除用户帐户：

```
# ovirt-aaa-jdbc-tool user delete test1
```

从管理门户中删除用户。如需更多信息，请参阅 [删除用户](#)。

3.6.8.8. 禁用内部管理用户

您可以禁用本地域中的用户，包括 `engine-setup` 中创建的 `admin@internal` 用户。在禁用默认的 `admin` 用户前，请确保至少有一个用户具有完整管理权限。

流程

1. 登录到安装 Red Hat Virtualization Manager 的机器。
2. 确保将拥有 SuperUser 角色的用户添加到环境中。如需更多信息，请参阅添加用户。
3. 禁用默认的 `admin` 用户：

```
# ovirt-aaa-jdbc-tool user edit admin --flag=+disabled
```



注意

要启用禁用的用户，请运行 `ovirt-aaa-jdbc-tool user edit username --flag=-disabled`

3.6.8.9. 管理组

您可以使用 `ovirt-aa-jdbc-tool` 工具管理内部域中的组帐户。管理组帐户与管理用户帐户类似。如需组选项的完整列表，请运行 `ovirt-aaa-jdbc-tool group --help`。本节中提供了常见示例。

创建组

此流程演示了如何创建组帐户，将用户添加到组中，以及查看组的详情。

1. 登录到安装 Red Hat Virtualization Manager 的机器。
2. 创建新组：

```
# ovirt-aaa-jdbc-tool group add group1
```


3. 将用户添加到组中。用户必须已创建。

```
# ovirt-aaa-jdbc-tool group-manage useradd group1 --user=test1
```



注意

如需 `group-manage` 选项的完整列表，请运行 `ovirt-aaa-jdbc-tool group-manage --help`。

4. 查看组帐户详情：

```
# ovirt-aaa-jdbc-tool group show group1
```

5. 在管理门户中添加新创建的组，并分配相应的角色和权限。组中的用户继承组的角色和权限。如需更多信息，请参阅添加用户。

创建嵌套组

此流程演示了如何在组内创建组。

1. 登录到安装 Red Hat Virtualization Manager 的机器。
2. 创建第一个组：

```
# ovirt-aaa-jdbc-tool group add group1
```

3. 创建第二个组：

```
# ovirt-aaa-jdbc-tool group add group1-1
```

4. 将第二个组添加到第一个组中：

```
# ovirt-aaa-jdbc-tool group-manage groupadd group1 --group=group1-1
```

5. 在管理门户中添加第一个组，并分配相应的角色和权限。如需更多信息，请参阅添加用户。

3.6.8.10. 查询用户和组

`query` 模块允许您查询用户和组信息。如需完整的选项列表，请运行 `ovirt-aaa-jdbc-tool query --help`。

列出所有用户或组帐户详情

此步骤显示如何列出所有帐户信息。

1. 登录到安装 Red Hat Virtualization Manager 的机器。

2. 列出帐户详细信息。

- 所有用户帐户详情：

```
# ovirt-aaa-jdbc-tool query --what=user
```

- 所有组帐户详情：

```
# ovirt-aaa-jdbc-tool query --what=group
```

列出过滤的帐户详情

此流程演示了如何在列出帐户信息时应用过滤器。

1. 登录到安装 Red Hat Virtualization Manager 的机器。

2. 使用 `--pattern` 参数过滤帐户详情。

- 使用以字符 *j* 开头的名称列出用户帐户详细信息。

```
# ovirt-aaa-jdbc-tool query --what=user --pattern="name=j"
```

- 列出将部门属性设置为 *marketing* 的组：

```
# ovirt-aaa-jdbc-tool query --what=group --pattern="department=marketing"
```

3.6.8.11. 管理帐户设置

若要更改默认帐户设置，可使用 `ovirt-aaa-jdbc-tool` 设置 模块。

更新帐户设置

此流程演示了如何更新默认帐户设置。

1. 登录到安装 Red Hat Virtualization Manager 的机器。
2. 运行以下命令以显示所有可用的设置：

```
# ovirt-aaa-jdbc-tool settings show
```

3. 更改所需设置：

- 本例为所有用户帐户将默认登录会话时间更新为 60 分钟。默认值为 10080 分钟。

```
# ovirt-aaa-jdbc-tool settings set --name=MAX_LOGIN_MINUTES --value=60
```

- 本例更新了用户在用户帐户锁定前可以执行的失败登录尝试次数。默认值为 5。

```
# ovirt-aaa-jdbc-tool settings set --name=MAX_FAILURES_SINCE_SUCCESS --value=3
```



注意

要解锁锁定的用户帐户，请运行 `ovirt-aaa-jdbc-tool` 用户 `unlock test1`。

3.6.9. 配置附加本地域

也支持创建除默认内部域以外的其他本地域。这可以使用 `ovirt-engine-extension-aaa-jdbc` 扩展进行，并允许您创建多个域而无需附加外部目录服务器，但用例可能不适用于企业环境。

另外，在标准 Red Hat Virtualization 升级过程中不会自动升级本地域，需要为每个将来的版本手动升级。有关创建其他本地域以及如何升级域的更多信息，请参阅 `/usr/share/doc/ovirt-engine-extension-aaa-jdbc-版本/README.admin` 中的 README 文件。



注意

`ovirt-engine-extension-aaa-jdbc` 扩展已弃用。对于新安装，请使用 Red Hat Single Sign On。如需更多信息，请参阅《管理指南》中的 [安装和配置 Red Hat Single Sign-On](#)。

3.7. 配额和服务等级协议政策

3.7.1. Quota 简介

配额是 Red Hat Virtualization 提供的资源限制工具。根据用户权限设定的限制层，配额可以被视为限制层。

配额是数据中心对象。

配额允许 Red Hat Virtualization 环境管理员限制用户对内存、CPU 和存储的访问。配额定义了管理员可分配用户的内存资源和存储资源。因此，用户只可能对分配给它们的资源进行绘制。当配额资源耗尽时，Red Hat Virtualization 不允许进一步的用户操作。

有两个不同的配额类型：

表 3.3. Quota 的两个不同 Kind

配额类型	定义
run-time Quota	此配额限制运行时资源的消耗，如 CPU 和内存。
存储配额	此配额限制可用的存储量。

配额（如 SELinux）有三种模式：

表 3.4. 定额模式

配额模式	功能
已强制	这个模式使您在 Audit 模式中设置的配额生效，将资源限制到由配额影响的组或用户。
Audit	这个模式在不阻止用户的情况下记录配额违反情况，并可用于测试配额。在 Audit 模式中，您可以增加或减少运行时配额的数量，以及受它影响的用户的存储配额量。
Disabled	这个模式关闭配额定义的运行时和存储限制。

当用户尝试运行虚拟机时，虚拟机的规格将与存储允许以及适用配额中的运行时允许集进行比较。

如果启动虚拟机导致配额涵盖的所有正在运行的虚拟机的聚合资源超过配额中定义的允许资源，则 **Manager** 将拒绝运行虚拟机。

当用户创建新磁盘时，请求的磁盘大小将添加到适用配额涵盖的所有其他磁盘的聚合磁盘使用情况中。如果新磁盘采用配额所允许的总聚合磁盘用量，则磁盘创建会失败。

配额允许共享同一硬件的资源。它支持硬和软阈值。管理员可以使用配额在资源上设置阈值。会显示这些阈值，从用户的角度看该资源的 100% 使用量。为了防止客户意外超过这个阈值时失败，接口支持可简要超过阈值的“正常”量。超过阈值会导致向客户发送警告。



重要

配额会对运行虚拟机施加限制。忽略这些限制可能会导致情形您无法使用您的虚拟机和虚拟磁盘。

当配额以强制模式运行时，无法使用没有分配配额的虚拟机和磁盘。

要打开虚拟机电源，必须将配额分配给该虚拟机。

要创建虚拟机快照，与虚拟机关联的磁盘必须分配配额。

从虚拟机创建模板时，系统会提示您选择您希望模板使用的配额。这可让您设置模板（以及从模板创建的所有机器）以使用与生成模板的虚拟机和磁盘不同的配额。

3.7.2. 共享配额和个别定义配额

具有 **SuperUser** 权限的用户可以为单个用户或组群创建配额。

可以为 **Active Directory** 用户设置组配额。如果组 10 个用户获得 1 TB 的存储配额，另一个用户占据了整个 TB，则整个组将超额使用，其中 10 个用户将能够使用与其组关联的任何存储。

单独用户的配额只为个人设置。单个用户使用自己的所有存储或运行时配额后，用户将超过配额，用户将不再能够使用与其配额关联的存储。

3.7.3. 配额帐户

当为使用者或资源分配配额时，消费者或涉及存储、vCPU 或内存的资源的每个操作都会导致配额消耗或配额发布。

由于配额充当上限，将用户访问限制到资源，因此配额计算可能与用户的实际使用不同。为最大增长潜力计算配额，而非当前使用量。

例 3.15. 会计示例

用户运行具有 1 个 vCPU 和 1024 MB 内存的虚拟机。该操作会消耗分配给该用户的 1 个 vCPU 和

1024 MB 的配额。当虚拟机停止 1 个 vCPU 和 1024 MB RAM 时，将返回到分配给该用户的配额。仅在消费者的实际运行时考虑运行时配额消耗。

用户创建虚拟精简配置的磁盘 10 GB。实际磁盘使用量可能仅代表实际正在使用的磁盘 3 GB。但是，配额消耗的消费应该是 10 GB，该磁盘的最大增长潜力。

3.7.4. 在 Data Center 中启用和更改配额模式

这个过程启用或更改数据中心中的配额模式。您必须选择配额模式，然后才能定义配额。您必须登录到管理门户，请按照以下步骤执行。

使用 Audit 模式测试配额，以验证它是否按预期工作。您不需要在 Audit 模式中使用配额来创建或更改配额。

流程

1. 点 **Compute** → **Data Centers** 并选择一个数据中心。
2. 点 **Edit**。
3. 在 **Quota Mode** 下拉列表中，将配额模式更改为 **Enforced**。
4. 点击 **OK**。

如果在测试过程中将配额模式设置为 **Audit**，则必须将其更改为 **Enforced** 才能使配额设置生效。

3.7.5. 创建新配额策略

您已启用配额模式，可以是 **Audit** 或 **Enforcing** 模式。您要定义配额策略来管理数据中心中的资源使用量。

流程

1. 单击 **Administration** → **Quota**。
2. 点 **Add**。
3. 填写 **Name** 和 **Description** 字段。
4. 选择一个 **数据中心**。
5. 在 **Memory & CPU** 部分中，使用绿色滑块来设置 **Cluster Threshold**。
6. 在 **Memory & CPU** 部分中，使用蓝色滑块来设置 **Cluster Grace**。
7. 单击 **All Clusters** 或特定集群单选按钮。如果选择了 **Specific Clusters**，请选择您要在其中添加配额策略的集群的复选框。
8. 点 **Edit**。这将打开 **Edit Quota** 窗口。
 - a. 在 **Memory** 字段下，选择 **Unlimited** 单选按钮（允许无限地使用集群中的内存资源），或者选择按单选按钮设定的限值来设置这个配额设定的内存量。如果将 **限制** 选为单选按钮，在 **MB** 字段中以 **MB** 为单位输入内存大小。
 - b. 在 **CPU** 字段中，选择 **Unlimited** 单选按钮，或选择 **限制** 为单选按钮来设置这个配额设置的 CPU 数量。如果您选择了 **限制** 单选按钮，在 **vCpus** 字段中输入 vCPU 数量。
 - c. 在 **Edit Quota** 窗口中，单击 **OK**。
9. 在 **Storage** 部分中，使用绿色的滑块来设置 **Storage Threshold**。
10. 在 **Storage** 部分中，使用蓝色滑块来设置 **存储评测**。
- 11.

单击 **All Storage Domains** 或 **Specific Storage Domains** 单选按钮。如果您选择 **Specific Storage Domains**，请选择您要在其中添加配额策略的存储域的复选框。

12.

点 **Edit**。这将打开 **Edit Quota** 窗口。

a.

在 **Storage Quota** 字段中，选择 **Unlimited** 单选按钮（允许无限使用存储），或者 **限制** 为单选按钮，以设置配额限制用户的存储量。如果您选择了 **限制** 单选按钮，在 **GB** 字段中以 **GB** 为单位输入存储配额大小(**GB**)。

b.

在 **Edit Quota** 窗口中，单击 **OK**。

13.

在 **New Quota** 窗口中，单击 **OK**。

3.7.6. Quota Threshold Settings 的解释

表 3.5. 配额阈值和宽限期

设置	定义
Cluster Threshold	每个数据中心可用的集群资源数量。
Cluster Grace	在数据中心耗尽后，集群数量会耗尽数据中心的 Cluster Threshold。
Storage Threshold	每个数据中心可用的存储资源量。
存储分级	在数据中心 Storage Threshold 耗尽后，数据中心的可用存储量。

如果将配额设定为有 20% 的 100 GB，则消费者在使用 120 GB 存储后被禁止使用存储。如果同一配额将 **Threshold** 设置为 70%，则消费者在超过 70 GB 的存储消耗时收到警告（但它们仍然可以使用存储，直到它们达到 120 GB 存储消耗为止）。"**Threshold**"和"**Grace**"都设置为相对于配额。"**threshold**"可以被视为"软限制"，超过它会生成警告。"**安全**"可能认为是"硬限制"，超过它就无法消耗更多存储资源。

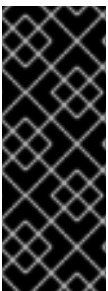
3.7.7. 为对象分配配额

为虚拟机分配配额

1. 单击 **Compute** → **Virtual Machines** 并选择虚拟机。
2. 点 **Edit**。
3. 从 **Quota** 下拉列表中，选择您要消耗的虚拟机的配额。
4. 单击 **OK**。

为磁盘分配配额

1. 单击 **Compute** → **Virtual Machines**。
2. 点虚拟机名称。这会打开详情视图。
3. 点 **Disks** 选项卡，选择您要与配额关联的磁盘。
4. 点 **Edit**。
5. 从 **Quota** 下拉列表中选择您要消耗的虚拟磁盘的配额。
6. 单击 **OK**。



重要

必须为与虚拟机关联的所有对象选择配额，才能让该虚拟机正常工作。如果您无法为与虚拟机关联的对象选择配额，则虚拟机将无法工作。**Manager** 在这种情形中抛出错误是通用的，这很难知道错误被抛出，因为您没有将配额与与虚拟机关联的所有对象关联。无法对没有分配配额的虚拟机快照进行快照。不能创建虚拟磁盘没有分配配额的虚拟机模板。

3.7.8. 使用配额限制用户的资源

这个步骤描述了如何使用配额来限制用户有权访问的资源。

流程

1. 单击 **Administration** → **Quota**。
2. 点目标配额的名称。这会打开详情视图。
3. 点 **Consumers** 选项卡。
4. 点 **Add**。
5. 在 **Search** 字段中，输入您要与配额关联的用户名。
6. 点 **GO**。
7. 选中用户名旁边的复选框。
8. 点击 **OK**。

短时间后，用户会显示在详情视图中的 **Consumers** 选项卡中。

3.7.9. 编辑配额

这个步骤描述了如何更改现有配额。

流程

1. 单击 **Administration** → **Quota**，再选择配额。

2. 点 **Edit**。
3. 根据需要编辑字段。
4. 点击 **OK**。

3.7.10. 删除配额

这个步骤描述了如何删除配额。

流程

1. 单击 **Administration** → **Quota**，再选择配额。
2. 单击 **Remove**。
3. 单击 **OK**。

3.7.11. 服务等级协议政策强制

这个步骤描述了如何设置服务级别协议 CPU 功能。

流程

1. 单击 **Compute** → **Virtual Machines**。
2. 单击**新建**，或选择虚拟机，然后单击 **编辑**。
3. 单击 **资源分配** 选项卡。
4. 指定 CPU 共享。可能的选项包括 **Low**, **Medium**, **High**, **Custom**, and **Disabled**。设置为 **High** 的虚拟机设置为 **High** 两次，且虚拟机设置为 **Medium**，虚拟机设置为 **Medium** 时接收两次

共享，因为虚拟机设置为 **Low**。禁用指示 **VDSM** 使用较旧的算法来确定共享冲突；通常这些条件下共享的数量为 **1020**。

用户的 **CPU** 消耗现在受您设定的策略控制。

3.8. 事件通知

3.8.1. 在管理门户中配置事件通知

Red Hat Virtualization Manager 可以在 **Red Hat Virtualization Manager** 管理的环境中发生特定事件时，通过电子邮件通知指定用户。要使用这个功能，您必须设置邮件传输代理来发送邮件。只有电子邮件通知可以通过管理门户进行配置。**SNMP** 陷阱必须在 **Manager** 机器上配置。

流程

1. 确保您有权访问电子邮件服务器，该服务器可接受来自 **Manager** 自动消息并将其传送到分发列表。
2. 点 **Administration** → **Users** 并选择一个用户。
3. 点用户的 **User Name** 进入详情页面。
4. 在 **Event Notifier** 选项卡中，单击 **Manage Events**。
5. 使用 **Expand All** 按钮或特定主题的扩展按钮来查看事件。
6. 选中适当的复选框。
7. 在 **Mail Recipient** 字段中输入电子邮件地址。



注意

电子邮件地址可以是文本消息电子邮件地址（例如 `1234567890@carrierdomainname.com`）或包含电子邮件地址和文本邮件电子邮件地址的电子邮件地址。

8.

点击 **OK**。

9.

在 **Manager** 计算机上，将 `ovirt-engine-notifier.conf` 复制到名为 `90-email-notify.conf` 的新文件：

```
# cp /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf
/etc/ovirt-engine/notifier/notifier.conf.d/90-email-notify.conf
```

10.

编辑 `90-email-notify.conf`，删除所有除 **EMAIL 通知** 部分外的所有内容。

11.

输入正确的电子邮件变量，如下例所示。此文件覆盖原始 `ovirt-engine-notifier.conf` 文件中的值。

```
#-----#
# EMAIL Notifications #
#-----#

# The SMTP mail server address. Required.
MAIL_SERVER=myemailserver.example.com

# The SMTP port (usually 25 for plain SMTP, 465 for SMTP with SSL, 587 for SMTP with
# TLS)
MAIL_PORT=25

# Required if SSL or TLS enabled to authenticate the user. Used also to specify 'from' user
# address if mail server
# supports, when MAIL_FROM is not set. Address is in RFC822 format
MAIL_USER=

# Required to authenticate the user if mail server requires authentication or if SSL or TLS is
# enabled
SENSITIVE_KEYS="${SENSITIVE_KEYS},MAIL_PASSWORD"
MAIL_PASSWORD=

# Indicates type of encryption (none, ssl or tls) should be used to communicate with mail
# server.
MAIL_SMTP_ENCRYPTION=none

# If set to true, sends a message in HTML format.
```

```
HTML_MESSAGE_FORMAT=false

# Specifies 'from' address on sent mail in RFC822 format, if supported by mail server.
MAIL_FROM=rhevm2017@example.com

# Specifies 'reply-to' address on sent mail in RFC822 format.
MAIL_REPLY_TO=

# Interval to send smtp messages per # of IDLE_INTERVAL
MAIL_SEND_INTERVAL=1

# Amount of times to attempt sending an email before failing.
MAIL_RETRIES=4
```



注意

如需了解更多选项，请参阅 `/etc/ovirt-engine/notifier/notifier.conf.d/README`。

12.

启用并重启 `ovirt-engine-notifier` 服务以激活您所做的更改：

```
# systemctl daemon-reload
# systemctl enable ovirt-engine-notifier.service
# systemctl restart ovirt-engine-notifier.service
```

指定用户现在根据 Red Hat Virtualization 环境中的事件接收电子邮件。所选事件显示在该用户的 **Event Notifier** 标签页中。

3.8.2. 在管理门户中取消事件通知

用户配置了一些不必要的电子邮件通知，并希望这些通知被取消。

流程

1. 单击 **Administration** → **Users**。
2. 单击用户的 **User Name**。这会打开详情视图。
3. 点 **Event Notifier** 选项卡，列出用户接收电子邮件通知的事件。

4. 单击 **Manage Events**。
5. 使用 **Expand All** 按钮或特定主题的扩展按钮查看事件。
6. 清除适当的复选框以删除该事件的通知。
7. 单击 **OK**。

3.8.3. ovirt-engine-notifier.conf 中的事件通知参数

事件通知程序配置文件可以在 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf` 中找到。

表 3.6. ovirt-engine-notifier.conf variables

变量名称	默认	备注
SENSITIVE_KEYS	none	不会记录的以逗号分隔的键列表。
JBOSS_HOME	/opt/rh/eap7/root/usr/share/wildfly	管理器所使用的 JBoss 应用服务器的位置。
ENGINE_ETC	/etc/ovirt-engine	管理器使用的 etc 目录的位置。
ENGINE_LOG	/var/log/ovirt-engine	Manager 使用的日志目录的位置。
ENGINE_USR	/usr/share/ovirt-engine	管理器使用的 usr 目录的位置。
ENGINE_JAVA_MODULEPATH	\${ENGINE_USR}/modules	JBoss 模块附加到的文件路径。
NOTIFIER_DEBUG_ADDRESS	none	可用于对通知程序使用的 Java 虚拟机进行远程调试的机器地址。
NOTIFIER_STOP_TIME	30	服务将超时的时间（以秒为单位）。
NOTIFIER_STOP_INTERVAL	1	超时计数器将递增的时间（以秒为单位）。
INTERVAL_IN_SECONDS	120	将消息分配给订阅者的时间间隔（以秒为单位）。

变量名称	默认	备注
IDLE_INTERVAL	30	执行低优先级任务的间隔（以秒为单位）。
DAYS_TO_KEEP_HISTORY	0	这个变量设定在历史记录表中保留的天数。如果没有设置此变量，事件会无限期地保留在历史记录表中。
FAILED_QUERIES_NOTIFICATION_THRESHOLD	30	发送通知电子邮件的失败查询数。在第一次获取通知失败后会收到通知电子邮件，然后每次达到此变量指定的失败次数后，都会发送通知电子邮件。如果您指定一个 0 或 1 的值，则会为每个失败发送一封电子邮件。
FAILED_QUERIES_NOTIFICATION_RECIPIENTS	none	发送通知电子邮件的收件人的电子邮件地址。必须使用逗号分隔电子邮件地址。 FILTER 变量已弃用此条目。
DAYS_TO_SEND_ON_STARTUP	0	通知程序启动时将处理并发送的旧事件的天数。如果值为 0，且服务在一段时间后停止并启动，则服务停止和服务启动时间之间的所有通知都将丢失，如果您想在服务停止和启动时间间发生的事件上收到通知，请将此值设置为 1 或更大值。
FILTER	exclude:*	用于决定电子邮件通知的触发器的算法。这个变量的值包括 include 或 exclude 、事件和接收者的组合。For example, include:VDC_START(smtp:mail@example.com) \${FILTER}
MAIL_SERVER	none	SMTP 邮件服务器地址。必需。
MAIL_PORT	25	用于通信的端口。可能的值有 25 个用于普通 SMTP， 465 用于使用 SSL 的 SMTP，以及 587 用于使用 TLS 的 SMTP。
MAIL_USER	none	如果启用了 SSL 来验证用户，则必须设置此变量。如果没有设置 MAIL_FROM 变量时，此变量也用于指定“from”用户地址。有些邮件服务器不支持此功能。该地址采用 RFC822 格式。

变量名称	默认	备注
SENSITIVE_KEYS	<code>`\${SENSITIVE_KEYS}`,MAIL_PASSWORD</code>	如果邮件服务器需要身份验证，或者启用了 SSL 或 TLS，则需要验证该用户。
MAIL_PASSWORD	none	如果邮件服务器需要身份验证，或者启用了 SSL 或 TLS，则需要验证该用户。
MAIL_SMTP_ENCRYPTION	none	通信中使用的加密类型。可能的值为 none, ssl, tls 。
HTML_MESSAGE_FORMAT	false	如果此变量设为 true ，则邮件服务器以 HTML 格式发送消息。
MAIL_FROM	none	如果邮件服务器支持，则此变量以 RFC822 格式指定发件人地址。
MAIL_REPLY_TO	none	此变量在发送邮件中指定 RFC822 格式的回复地址（如果邮件服务器支持）。
MAIL_SEND_INTERVAL	1	每个 IDLE_INTERVAL 发送的 SMTP 消息数
MAIL_RETRIES	4	在失败前尝试发送电子邮件的次数。
SNMP_MANAGERS	none	将充当 SNMP 管理器的计算机的 IP 地址或完全限定域名。条目必须由空格分开，并且可以包含一个端口号。例如， manager1.example.com manager2.example.com:164
SNMP_COMMUNITY	public	（仅 SNMP 版本 2）SNMP 社区。
SNMP_OID	1.3.6.1.4.1.2312.13.1.1	警报的默认 trap 对象标识符。定义此 OID 时，所有 trap 类型都会向 SNMP Manager 发送并附加了事件信息。请注意，更改默认陷阱可防止生成的陷阱遵守管理器的管理信息库。
SNMP_VERSION	2	定义要使用的 SNMP 版本。支持 SNMP 版本 2 和版本 3 陷阱。可能的值： 2 或 3 。

变量名称	默认	备注
SNMP_ENGINE_ID	none	(SNMPv3)用于 SNMPv3 陷阱管理器 ID。这个 ID 是通过 SNMP 连接的设备的唯一标识符。
SNMP_USERNAME	none	(SNMPv3)用于 SNMPv3 陷阱的用户名。
SNMP_AUTH_PROTOCOL	none	(SNMPv3) SNMPv3 授权协议。可能的值： MD5、SHA
SNMP_AUTH_PASSPHRASE	none	(SNMPv3) SNMP_SECURITY_LEVEL 时使用的密码短语设置为 AUTH_NOPRIV 和 AUTH_PRIV。
SNMP_PRIVACY_PROTOCOL	none	(SNMPv3) SNMPv3 隐私协议。可能的值有： AES128、AES192、AES256
		 <p>重要</p> <p>RFC3826 中没有定义 AES192 和 AES256，因此验证您的 SNMP 服务器在启用这些协议前是否支持这些协议。</p>
SNMP_PRIVACY_PASSPHRASE	none	SNMP_SECURITY_LEVEL 设置为 AUTH_PRIV 时使用的 SNMPv3 隐私密码。
SNMP_SECURITY_LEVEL	1	(SNMPv3) SNMPv3 安全级别。可能的值有： * 1 - NOAUTH_NOPRIV * 2 - AUTH_NOPRIV * 3 - AUTH_PRIV
ENGINE_INTERVAL_IN_SECONDS	300	监控安装 Manager 的机器之间的间隔（以秒为单位）。间隔从监控完成的时间测量。
ENGINE_MONITOR_RETRIES	3	通知程序尝试监控故障后以给定间隔内安装的机器状态的次数。
ENGINE_TIMEOUT_IN_SECONDS	30	在通知程序尝试监控管理器在故障后以给定间隔安装的机器的状态前，等待的时间（以秒为单位）。

变量名称	默认	备注
IS_HTTPS_PROTOCOL	false	如果 JBoss 在安全模式下运行，则此条目必须设为 true 。
SSL_PROTOCOL	TLS	启用 SSL 时 JBoss 配置连接器使用的协议。
SSL_IGNORE_CERTIFICATE_ERRORS	false	如果 JBoss 在安全模式下运行并且需要忽略 SSL 错误，则必须将此值设置为 true 。
SSL_IGNORE_HOST_VERIFICATION	false	如果 JBoss 在安全模式下运行并且要忽略主机名验证，则必须将此值设置为 true 。
REPEAT_NON_RESPONSIVE_NOTIFICATION	false	此变量指定是否安装 Manager 的机器将向订阅者发送重复失败的信息。
ENGINE_PID	/var/lib/ovirt-engine/ovirt-engine.pid	Manager PID 的路径和文件名。

3.8.4. 配置 Red Hat Virtualization Manager 以发送 SNMP Traps

将您的 Red Hat Virtualization Manager 配置为发送简单网络管理协议(SNMP)陷阱到一个或多个外部 SNMP 管理器。SNMP 陷阱包含系统事件信息；它们用于监控您的红帽虚拟化环境。发送到 SNMP 管理器的陷阱数量和类型可在 Red Hat Virtualization Manager 中定义。

Red Hat Virtualization 支持 SNMP 版本 2 和版本 3。SNMP 版本 3 支持以下安全级别：

NoAuthNoPriv

SNMP 陷阱在没有授权或隐私的情况下发送。

AuthNoPriv

SNMP 陷阱是通过密码授权发送，但没有隐私。

AuthPriv

SNMP 陷阱通过密码授权和隐私发送。

前提条件

- 一个或多个外部 SNMP 管理器配置为接收陷阱。
- 将充当 SNMP 管理器的计算机的 IP 地址或完全限定域名。（可选）决定 Manager 接收陷阱通知的端口。默认值为 UDP 端口 162。
- SNMP 社区（仅 SNMP 版本 2）。多个 SNMP 管理器可以属于单个社区。管理系统和代理只能在同一社区内进行通信。默认社区为公共。
- 警报的陷阱对象标识符。Red Hat Virtualization Manager 提供 1.3.6.1.4.1.2312.13.1.1. 的默认 OID。定义此 OID 时，所有 trap 类型都会向 SNMP Manager 发送并附加了事件信息。请注意，更改默认陷阱可防止生成的陷阱遵守管理器的管理信息库。
- SNMP 用户名，表示 SNMP 版本 3、安全级别 1、2 和 3。
- SNMP 密语，表示 SNMP 版本 3、安全级别 2 和 3。
- SNMP 专用密语，表示 SNMP 版本 3，安全级别 3。



注意

Red Hat Virtualization Manager 在 `/usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt` 和 `/usr/share/doc/ovirt-engine/mibs/REDHAT-MIB.txt` 中提供管理信息基础。在继续操作前，请加载 SNMP 经理中的 MIBs。

默认 SNMP 配置值存在于事件通知守护进程配置文件 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf` 中。以下流程中概述的值基于此文件中提供的默认值或示例值。不要直接编辑此文件，因为系统更改（如升级）可能会删除您对此文件所做的任何更改。相反，将此文件复制到 `/etc/ovirt-engine/notifier/notifier.conf.d/<integer>-snmp.conf`，其中 `<integer>` 是一个数字，表示应运行该文件的优先级。

流程

1. 在 Manager 中，创建名为 `<integer>-snmp.conf` 的 SNMP 配置文件，其中 `<integer>` 是一个整数，表示处理文件的顺序。例如：

```
# vi /etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf
```

提示

复制事件通知守护进程配置文件 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf` 中的默认 SNMP 设置。此文件包含所有设置的内联注释。

2.

指定 SNMP Manager (s)、SNMP 版本 2，以及示例中的格式 OID：

```
SNMP_MANAGERS="manager1.example.com manager2.example.com:162"
SNMP_COMMUNITY=public
SNMP_OID=1.3.6.1.4.1.2312.13.1.1
```

3.

定义是否使用 SNMP 版本 2（默认）还是 3：

```
SNMP_VERSION=3
```

4.

为 `SNMP_ENGINE_ID` 指定一个值。例如：

```
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05"
```

5.

使用 SNMP 版本 3，为 SNMP 陷阱指定安全级别：

安全级别 1, NoAuthNoPriv traps:

```
SNMP_USERNAME=NoAuthNoPriv
SNMP_SECURITY_LEVEL=1
```

安全级别 2, AuthNoPriv 陷阱（以用户 `ovirtengine` 的身份）使用 SNMP Auth passphrase `authpass`。

```
SNMP_USERNAME=ovirtengine
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass
SNMP_SECURITY_LEVEL=2
```

安全级别 3, AuthPriv 陷阱，用户 `ovirtengine` 有 SNMP Auth 密码短语 `authpass` 和 SNMP Priv 密码短语 `privpass`。例如：

```
SNMP_USERNAME=ovirtengine
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass
SNMP_PRIVACY_PROTOCOL=AES128
SNMP_PRIVACY_PASSPHRASE=privpass
SNMP_SECURITY_LEVEL=3
```

6.

定义要发送到 SNMP 管理器的事件：

例 3.16. 事件示例

将所有事件发送到默认的 SNMP 配置集：

```
FILTER="include:*(snmp:) ${FILTER}"
```

将严重性为 ERROR 或 ALERT 的所有事件 发送到默认的 SNMP 配置集：

```
FILTER="include:*:ERROR(snmp:) ${FILTER}"
```

```
FILTER="include:*:ALERT(snmp:) ${FILTER}"
```

将 *VDC_START* 的事件发送到指定的电子邮件地址：

```
FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"
```

将事件发送到默认的 SNMP 配置集，但 *VDC_START* 发送到默认的 SNMP 配置集：

```
FILTER="exclude:VDC_START include:*(snmp:) ${FILTER}"
```

这个默认过滤器在 *ovirt-engine-notifier.conf* 中定义；如果您没有禁用此过滤器或应用覆盖过滤器，则不会发送任何通知：

```
FILTER="exclude:*"
```

VDC_START 是可用审计日志消息的示例。审计日志消息的完整列表可在 */usr/share/doc/ovirt-engine/AuditLogMessages.properties* 中找到。或者，在您的 SNMP

Manager 中过滤结果。

7. 保存该文件。
8. 启动 `ovirt-engine-notifier` 服务，并确保该服务在引导时启动：

```
# systemctl start ovirt-engine-notifier.service
# systemctl enable ovirt-engine-notifier.service
```

检查您的 SNMP 管理器，以确保收到陷阱。

**注意**

`SNMP_MANAGERS`、`MAIL_SERVER` 或两者都必须在 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf` 或以覆盖文件的形式定义，以便运行通知程序服务。

SNMP 配置文件示例

此示例配置文件基于 `ovirt-engine-notifier.conf` 中的设置。专用的 SNMP 配置文件（如此配置文件）会覆盖 `ovirt-engine-notifier.conf` 中的设置。

提示

将事件通知守护进程配置文件 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf` 中的默认 SNMP 设置复制到 `/etc/ovirt-engine/notifier/notifier.conf.d/<_integer_>-snmp.conf`，其中 `<_integer_>` 指示应运行该文件的优先级。此文件包含所有设置的内联注释。

`/etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf`

```
SNMP_MANAGERS="manager1.example.com manager2.example.com:162" 1
SNMP_COMMUNITY=public 2
SNMP_OID=1.3.6.1.4.1.2312.13.1.1 3
FILTER="include:*(snmp:)" 4
SNMP_VERSION=3 5
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05" 6
SNMP_USERNAME=<username> 7
SNMP_AUTH_PROTOCOL=MD5 8
```



```
SNMP_AUTH_PASSPHRASE=<authpass> 9
SNMP_PRIVACY_PROTOCOL=AES128 10
SNMP_PRIVACY_PASSPHRASE=<privpass> 11
SNMP_SECURITY_LEVEL=3 12
```

1

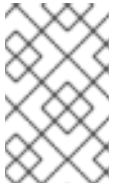
将充当 SNMP 管理器的计算机的 IP 地址或完全限定域名。条目必须由空格分开，并且可以包含一个端口号。例如，manager1.example.com manager2.example.com:164

2

(仅 SNMP 版本 2) 默认 SNMP 社区字符串。

3

用于传出通知的 SNMP Trap Object Identifier。iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) redhat (2312) ovirt (13) engine (1) notifier (1)



注意

更改默认将阻止生成的陷阱符合 OVIRT-MIB.txt。

4

用于确定 SNMP 通知的触发器和收件人的算法。

5

SNMP 版本支持 SNMP 版本 2 和版本 3 陷阱。2 = SNMPv2, 3 = SNMPv3.

6

(仅 SNMP 版本 3) 用于 SNMP 陷阱引擎 ID。

7

(仅 SNMP 版本 3) 用于 SNMP 陷阱的用户名。

8

9

(仅SNMP 版本 3) N SNMP auth密语。SNMP_SECURITY_LEVEL 设为 2 (AUTH_NOPRIV) 或 3 (AUTH_PRIV)时是必需的。

10

(仅SNMP 版本 3) SNMP 隐私协议。支持的值有 AES128、AES192 和 AES256。请注意，AES192 和 AES256 没有在 RFC3826 中定义，因此验证您的 SNMP 服务器在启用这些协议前是否支持这些协议。SNMP_SECURITY_LEVEL 设为 3 时需要(AUTH_PRIV)。

11

(仅SNMP 版本 3) SNMP 隐私密码短语。SNMP_SECURITY_LEVEL 设为 3 时需要 (AUTH_PRIV)。

12

(仅SNMP 版本 3) SNMP 安全级别。1 = NOAUTH_NOPRIV, 2 = AUTH_NOPRIV, 3 = AUTH_PRIV。

3.9. 工具

3.9.1. oVirt Engine Rename 工具

3.9.1.1. oVirt Engine Rename 工具

当 `engine-setup` 命令在干净环境中运行时，命令会生成多个证书和密钥，该证书和密钥使用设置过程中提供的 Manager 的完全限定域名。如果稍后需要修改 Manager 的全限定域名（例如，由于将 Manager 托管管理器的计算机迁移到其他域），则必须更新完全限定域名的记录，以反映新的名称。`ovirt-engine-rename` 命令自动执行此任务。

`ovirt-engine-rename` 命令会在以下位置更新 Manager 的完全限定域名记录：

- `/etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf`
- `/etc/ovirt-engine/isouploader.conf.d/10-engine-setup.conf`
- `/etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf`

- `/etc/pki/ovirt-engine/cert.conf`
- `/etc/pki/ovirt-engine/cert.template`
- `/etc/pki/ovirt-engine/certs/apache.cer`
- `/etc/pki/ovirt-engine/keys/apache.key.nopass`
- `/etc/pki/ovirt-engine/keys/apache.p12`

注意

您确定要执行此操作吗？

从 4.0.4 开始，可以添加更多名称来访问 Manager Web 界面。

1. 通过向 DNS 服务器添加相关记录或 `/etc/hosts`（使用 `ping enginename` 或 `getent hosts enginename`）检查，确保您选择的名称可以解析到 Manager 机器的 IP 地址。
2. 运行以下命令：

```
----
# echo 'SSO_ALTERNATE_ENGINE_FQDNS="alias1.example.com
alias2.example.com"' \
> /etc/ovirt-engine/engine.conf.d/99-custom-sso-setup.conf
# systemctl restart ovirt-engine.service
----
```

. List the alternate names separated by spaces.

也可以添加 Manager 机器的 IP 地址。但是，使用 IP 地址而不是 DNS 名称并非好的做法。

**警告**

虽然 `ovirt-engine-rename` 命令为管理器运行的 Web 服务器创建新证书，但它不会影响 Manager 或证书颁发机构的证书。因此，使用 `ovirt-engine-rename` 命令有一些风险，特别是在从 Red Hat Enterprise Virtualization 3.2 及更早版本升级的环境中。因此，建议尽可能运行 `engine-cleanup` 和 `engine-setup` 更改管理器的完全限定域名。

**警告**

在升级过程中，必须解析旧主机名。如果 oVirt Engine Rename Tool 失败并显示消息 `[ERROR] Host name is not valid: <OLD FQDN>` 没有解析到 IP 地址，请将旧主机名添加到 `/etc/hosts` 文件中，使用 oVirt Engine Rename Tool，然后从 `/etc/hosts` 文件中删除旧主机名。

3.9.1.2. oVirt Engine Rename 命令的语法

`ovirt-engine-rename` 命令的基本语法为：

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

该命令还接受以下选项：

```
--newname=[new name]
```

允许您为 Manager 指定新的全限定域名，而无需用户交互。

```
--log=[file]
```

允许您指定要写入重命名操作日志的文件的完整路径和名称。

```
--config=[file]
```

允许您指定要加载到重命名操作的配置文件的路径和文件名。

```
--config-append=[file]
```

允许您指定配置文件的路径和文件名，以附加到重命名操作。此选项可用于指定现有回答文件的路径和文件名来自动重命名操作。

--generate-answer=[file]

允许您指定记录您的答案和 `ovirt-engine-rename` 命令更改的文件的的路径和文件名。

3.9.1.3. 使用 oVirt Engine Rename 工具重命名 Manager

您可以使用 `ovirt-engine-rename` 命令更新 Manager 的完全限定域名(FQDN)的记录。

工具可检查 Manager 是否提供本地 ISO 还是数据存储域。如果存在，工具会提示用户弹出、关闭或置于维护模式，然后再继续操作。这样可确保虚拟机不会与其虚拟磁盘的连接，并防止 ISO 存储域在重命名过程中丢失连接。

流程

1. 为新的 FQDN 准备所有 DNS 和其他相关记录。
2. 如果使用 DHCP，请更新 DHCP 服务器配置。
3. 更新 Manager 上的主机名。
4. 运行以下命令：

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

5. 提示时，按 Enter 停止引擎服务：

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

6. 出现提示时，输入 Manager 的新 FQDN：

```
New fully qualified server name:new_engine_fqdn
```

`ovirt-engine-rename` 命令会更新 Manager 的 FQDN 记录。

对于自托管引擎，请完成以下步骤：

1. 在每个现有的自托管引擎节点上运行以下命令：

```
# hosted-engine --set-shared-config fqdn new_engine_fqdn --type=he_local
```

此命令修改每个自托管引擎节点的 `/etc/ovirt-hosted-engine-ha/hosted-engine.conf` 的本地副本中的 FQDN

2. 在其中一个自托管引擎节点上运行以下命令：

```
# hosted-engine --set-shared-config fqdn new_engine_fqdn --type=he_shared
```

此命令修改共享存储域上 `/etc/ovirt-hosted-engine-ha/hosted-engine.conf` 主副本中的 FQDN。

现在，所有新的和现有的自托管引擎节点都使用新的 FQDN。



注意

`oVirt Engine Rename` 工具旨在仅在本地机器上工作。更改 Manager 名称不会自动更新远程数据仓库计算机上的名称。更改远程 DWH 计算机上的名称必须手动执行。

对于远程数据仓库部署，请在远程计算机上执行这些步骤（而不是在 Manager 机器上）：

1. 删除以下 PKI 文件：

```
/etc/pki/ovirt-engine/apache-ca.pem/etc/pki/ovirt-engine/apache-grafana-ca.pem/etc/pki/ovirt-engine/certs the/etc/pki/ovirt-engine/keys the
```

2. 在以下文件中，将 Manager fqdn 更新为新名称（如 `vm-new-`

name.local_lab_server.redhat.com) :

```
/etc/grafana/grafana.ini/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-
database.conf/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

3.

使用 `--offline switch` 运行 `engine-setup` 以防止此时间更新 :

```
# engine-setup --offline
```

3.9.2. Engine 配置工具

3.9.2.1. Engine 配置工具

引擎配置工具是用于为您的 Red Hat Virtualization 环境配置全局设置的命令行实用程序。该工具与存储在引擎数据库中的键值映射列表交互，并允许您检索和设置单个键的值，并且检索所有可用的配置键和值的列表。另外，可以为 Red Hat Virtualization 环境中的每个配置级别存储不同的值。



注意

Red Hat Virtualization Manager 或 Red Hat JBoss Enterprise Application Platform 都不需要运行来检索或设置配置密钥的值。由于配置键值映射存储在引擎数据库中，因此可以在 `postgresql` 服务运行时更新它们。然后，当 `ovirt-engine` 服务重启时应用更改。

3.9.2.2. engine-config 命令的语法

您可以从安装 Red Hat Virtualization Manager 的机器上运行引擎配置工具。如需有关使用方法的详细信息，请打印该命令的帮助输出 :

```
# engine-config --help
```

常见任务 :

- 列出可用的配置密钥

```
# engine-config --list
```

- 列出可用的配置值

```
# engine-config --all
```

- 检索配置密钥的值

```
# engine-config --get KEY_NAME
```

将 *KEY_NAME* 替换为首选键的名称，以检索该密钥的给定版本的值。使用 `--cver` 参数指定要检索的值的配置版本。如果没有提供版本，则会返回所有现有版本的值。

- 设置配置密钥值

```
# engine-config --set KEY_NAME=KEY_VALUE --cver=VERSION
```

使用要设置的特定键的名称替换 *KEY_NAME*，并将 *KEY_VALUE* 替换为要设置的值。您必须在具有多个配置版本的环境中指定 *VERSION*。

- 重启 `ovirt-engine` 服务以加载更改

需要重启 `ovirt-engine` 服务以使您的更改生效。

```
# systemctl restart ovirt-engine.service
```

3.9.3. USB 过滤器编辑器

3.9.3.1. 安装 USB 过滤器编辑器

USB Filter Editor 是一个 Windows 工具，用于配置 `usbfilter.txt` 策略文件。此文件中定义的策略规则则会允许或拒绝特定 USB 设备从客户端机器自动透传到使用 Red Hat Virtualization Manager 管理的虚拟机。策略文件位于以下位置的 Red Hat Virtualization Manager 中：`/etc/ovirt-engine/usbfilter.txt` 更改 USB 过滤器策略不会生效，除非 Red Hat Virtualization Manager 上的 `ovirt-engine` 服务被重启。

从此 ["Installers and Images for Red Hat Virtualization Manager"](#) 主题中下载 USB Filter Editor。

流程

1. 在 Windows 计算机上，从 .zip 文件提取 .msi intaller，并运行 .msi 安装程序。
2. 按照安装向导的步骤进行操作。除非另有指定，否则 USB 过滤器编辑器将默认安装在 C:\Program Files\RedHat\RedHat\USB Filter Editor or C:\Program Files (x86)\RedHat\USB Filter Editor)，具体取决于您的 Windows 版本。
3. 在桌面上创建 USB 过滤编辑器快捷方式图标。



重要

使用 [WinSCP](#) 等安全复制(SCP)客户端从 Red Hat Virtualization Manager 中导入和导出过滤策略。

默认 USB 设备策略为虚拟机提供对 USB 设备的基本访问权限；更新策略以允许使用其他 USB 设备。

3.9.3.2. USB 过滤器编辑器接口

双击桌面上的 USB 过滤编辑器快捷方式图标。

Red Hat USB Filter Editor 界面显示每个 USB 设备的 Class, Vendor, Product, Revision, 和 Action。允许在 Action 列中将允许 USB 设备设为 Allow；禁止的设备设置为 Block。

表 3.7. USB 编辑器字段

Name	Description
类	USB 设备的类型，例如打印机，大容量存储控制器。
Vendor	所选设备类型的制造商。
产品	特定的 USB 设备模型。
Revision (修订)	产品的修订。
操作	允许或阻止指定的设备。

USB 设备策略规则按照其列出的顺序处理。使用 Up 和 Down 按钮在列表中移动或低于规则。通用块规则需要保留为最低条目，以确保所有 USB 设备都被拒绝，除非 USB 过滤器编辑器中明确允许。

3.9.3.3. 添加 USB 策略

双击桌面上的 USB 过滤编辑器快捷方式图标。这会打开编辑器。

流程

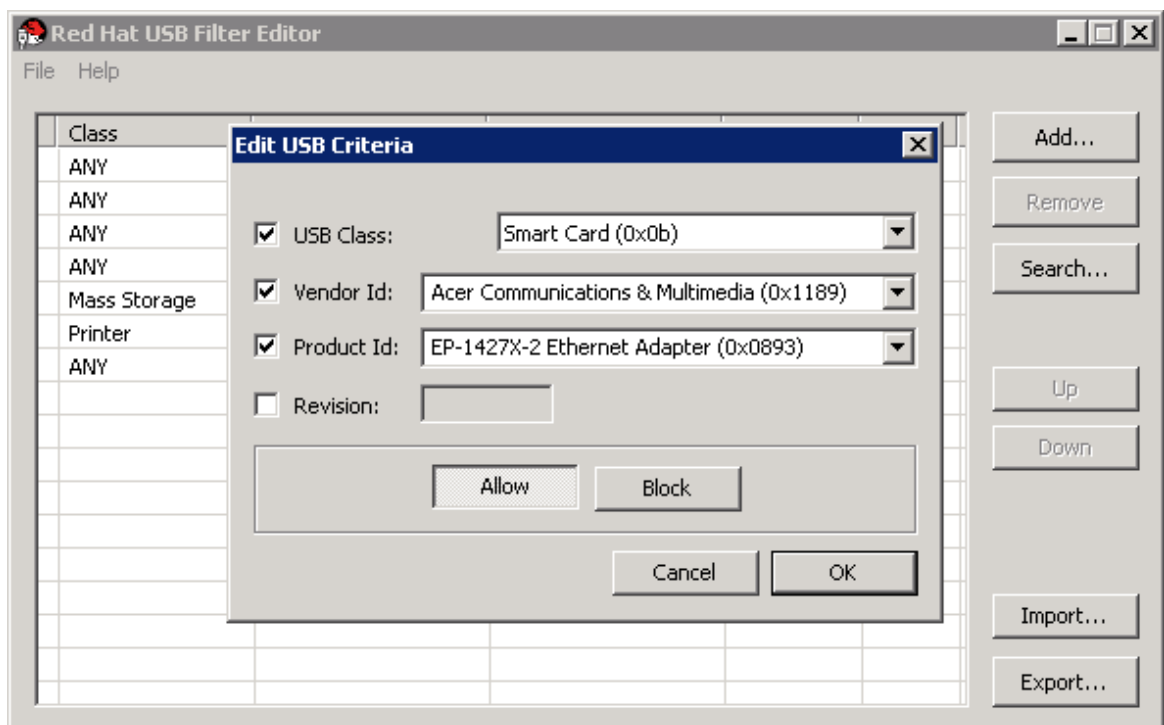
1. 点 **Add**。
2. 使用 **USB 类**、**供应商 ID**、**产品 ID** 和 **Revision** 复选框和列表来指定设备。

点击 **Allow** 按钮允许虚拟机使用 **USB** 设备；点击 **Block** 按钮禁止虚拟机中的 **USB** 设备。

单击确定，将选定的过滤器规则添加到列表中并关闭窗口。

例 3.17. 添加设备

以下是如何将 **USB Class Smartcard**、设备 **EP-1427X-2 以太网适配器** 从 **manufacturer Acer Communications & Multimedia** 添加到允许的设备列表中。



3. 单击 **File** → **Save** 以保存更改。

您已在 **USB Filter Editor** 中添加 **USB** 策略。您需要将 **USB** 过滤策略导出到 **Red Hat Virtualization Manager**，以便它们生效。

其他资源

- [导出 USB 策略](#)

3.9.3.4. 删除 USB 策略

双击桌面上的 **USB** 过滤编辑器快捷方式图标。这会打开编辑器。

流程

1. 选择要删除的策略。
2. 单击 **Remove**。这时将显示一条消息，提示您确认要删除策略。
3. 单击 **Yes** 以确认要删除该策略。
4. 单击 **File** → **Save** 以保存更改。

您已从 **USB Filter Editor** 中删除了 **USB** 策略。您需要将 **USB** 过滤策略导出到 **Red Hat Virtualization Manager**，以便它们生效。

其他资源

- [导出 USB 策略](#)

3.9.3.5. 搜索 USB 设备策略

在 **USB** 过滤器编辑器中搜索连接的 **USB** 设备以允许或阻止它们。

双击桌面上的 **USB 过滤编辑器快捷方式图标**。这会打开编辑器。

流程

1. 单击 **Search**。**附加 USB 设备** 窗口显示所有附加设备的列表。
2. 选择设备并单击 **Allow** 或 **Block**（根据情况而定）。双击所选设备以关闭该窗口。设备的策略规则添加到列表中。
3. 使用 **Up** 和 **Down** 按钮更改列表中新策略规则的位置。
4. 单击 **File** → **Save** 以保存更改。

您已搜索附加的 **USB 设备**。**USB 过滤策略**需要导出到 **Red Hat Virtualization Manager** 才能生效。

3.9.3.6. 导出 USB 策略

USB 设备策略更改需要导出并上传到 **Red Hat Virtualization Manager** 中，以便更新的策略生效。上传策略并重启 **ovirt-engine** 服务。

双击桌面上的 **USB 过滤编辑器快捷方式图标**。这会打开编辑器。

流程

1. 单击 **Export; Save As** 窗口将打开。
2. 使用 **usbfilter.txt** 的文件名保存文件。
3. 使用 **Secure Copy** 客户端，如 **WinSCP**，将 **usbfilter.txt** 文件上传到运行 **Red Hat Virtualization Manager** 的服务器。该文件必须放在服务器上的以下目录中：**/etc/ovirt-engine/**
4. 在运行 **Red Hat Virtualization Manager** 的服务器中，以 **root** 用户身份重启 **ovirt-engine** 服务。

```
# systemctl restart ovirt-engine.service
```

3.9.3.7. 导入 USB 策略

在编辑前，必须下载并导入到 USB Filter Editor 中现有的 USB 设备策略。

流程

1. 使用 Secure Copy 客户端，如 WinSCP，从运行 Red Hat Virtualization Manager 的服务器下载 `usbfilter.txt` 文件。文件可以在服务器中的以下目录中找到：`/etc/ovirt-engine/`
2. 双击桌面上的 USB 过滤编辑器快捷方式图标。这会打开编辑器。
3. 点 Import。此时将打开 Open 窗口。
4. 打开从服务器下载的 `usbfilter.txt` 文件。

3.9.4. 镜像差异工具

3.9.4.1. 使用镜像差异工具监控快照健康状况

RHV 镜像离散工具分析存储域和 RHV 数据库中的镜像数据。如果发现卷和卷属性的差异，它会警告您，当不会修复这些差异。在各种情况下使用该工具，例如：

- 在升级版本之前，为了避免将损坏的卷或链移至新版本。
- 出现失败的存储操作后，用于检测处于错误状态的卷或属性。
- 从备份中恢复 RHV 数据库或存储后。
- 在潜在问题发生之前定期对其进行检测。

- 要分析快照或实时迁移相关的问题，并在修复这些类型的问题后验证系统健康状况。

先决条件

- 所需版本：此工具是在 RHV 版本 4.3.8 中引入的，它带有 `rhv-log-collector-analyzer-0.2.15-0.el7ev`。
- 由于数据收集在不同位置上同时运行且并不具有原子性，因此请停止环境中可以修改存储域的所有活动。也就是说，请勿创建或删除快照、编辑、移动、创建或删除磁盘。否则，可能会出现错误检测不一致的情况。虚拟机可以在此过程中保持正常运行。

流程

1. 要运行该工具，在 RHV Manager 中输入以下命令：

```
# rhv-image-discrepancies
```

2. 如果工具发现差异，则重新运行以确认结果，特别是工具运行时可能会执行一些操作。



注意

此工具包含任何导出和 ISO 存储域，并可报告它们的差异。如果是这样，可以忽略它们，因为这些存储域没有 RHV 数据库中镜像的条目。

了解结果

工具报告以下内容：

- 如果在存储中显示但没有在数据库中，或者卷显示在数据库中，但没有出现在存储中。
- 如果存储和数据库之间有一些卷属性不同：

输出示例：

```
Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
```

```

Looking for missing images...
No missing images found
Checking discrepancies between SD/DB attributes...
image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
storage(2696984576) and on DB(2696986624)
image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
storage(5424252928) and on DB(5424254976)

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
Looking for missing images...
No missing images found
Checking discrepancies between SD/DB attributes...
No discrepancies found

```

3.9.5. Log Collector 工具

3.9.5.1. 日志收集器

一个日志集合工具包括在 Red Hat Virtualization Manager 中。这可让您在请求支持时从 Red Hat Virtualization 环境中轻松收集相关日志。

`log collection` 命令是 `ovirt-log-collector`。您需要以 `root` 用户身份登录，并为 Red Hat Virtualization 环境提供管理凭证。`ovirt-log-collector -h` 命令显示使用情况信息，包括 `ovirt-log-collector` 命令的所有有效选项列表。

3.9.5.2. `ovirt-log-collector` 命令的语法

日志收集器命令的基本语法为：

```

# ovirt-log-collector options list all/clusters/datacenters
# ovirt-log-collector options collect

```

两种支持的操作模式是 列出 并收集。

- `list` 参数列出了附加到 Red Hat Virtualization Manager 的主机、集群或数据中心。您可以基于列出的对象过滤日志集合。
- `collect` 参数从 Red Hat Virtualization Manager 执行日志集合。收集的日志放置在 `/tmp/logcollector` 目录下的存档文件中。`ovirt-log-collector` 命令为每个日志分配一个特定文件名。

除非指定了另一个参数，否则默认操作是将可用的主机与它们所属的数据中心和集群一起列出。系统会提示您输入用户名和密码来检索某些日志。

有大量参数可以进一步优化 `ovirt-log-collector` 命令。

常规选项

`--version`

显示使用的命令的版本号，并返回提示符。

`-h,--help`

显示命令用法信息，并返回到提示符。

`--conf-file=PATH`

将 *PATH* 设置为工具要使用的配置文件。

`--local-tmp=PATH`

将 *PATH* 设置为保存日志的目录。默认目录为 `/tmp/logcollector`。

`--ticket-number=TICKET`

将 *TICKET* 设置为 `ticket` 或问题单号，以与 SOS 报告关联。

`--upload=FTP_SERVER`

设置 *FTP_SERVER* 作为检索日志的目的地，以使用 FTP 发送。

除非被红帽支持代表建议，否则不要使用这个选项。

`--log-file=PATH`

将 *PATH* 设置为命令用于日志输出的特定文件名。

`--quiet`

设置静默模式，将控制台输出减小到最低限度。静默模式默认为关闭。

`-v,--verbose`

设置详细模式，提供更多的控制台输出。详细模式默认为关闭。

--time-only

仅显示主机间时间差异的信息，而不生成完整的 SOS 报告。

Red Hat Virtualization Manager Options

这些选项过滤日志集合，并指定 Red Hat Virtualization Manager 的身份验证详情。

这些参数可以合并用于特定命令。例如，`ovirt-log-collector --user=admin@internal --cluster ClusterA,ClusterB --hosts "SalesHost"*` 将用户指定为 `admin@internal`，并将日志集合限制为仅限在 A 和 B 中的 SalesHost 主机。

--no-hypervisors

从日志集合中省略虚拟化主机。

--one-hypervisor-per-cluster

从每个集群中收集一个主机的日志（如果有 SPM）。

-u USER, --user=USER

设置登录的用户名。*USER* 的格式为 `user@domain`，其中 *user* 是用户名，*domain* 是使用的目录服务域。用户必须存在于目录服务中，且对 Red Hat Virtualization Manager 所知。

-R FQDN, --rhevm=FQDN

设置从中收集日志的 Red Hat Virtualization Manager 的完全限定域名，其中 *FQDN* 替换为 Manager 的完全限定域名。假设日志收集器正在与 Red Hat Virtualization Manager 相同的本地主机上运行，默认值为 `localhost`。

-c CLUSTER, --cluster=CLUSTER

除了来自 Red Hat Virtualization Manager 的日志外，还从 nominated *CLUSTER* 中的虚拟化主机收集日志。包含的集群必须使用逗号分隔的集群名称列表或匹配模式指定。

-d DATACENTER, --data-center=DATACENTER

除了 Red Hat Virtualization Manager 日志外，还需要从 nominated *DATACENTER* 中的虚拟化主机收集日志。包含的数据中心必须使用逗号分隔的数据中心名称或匹配模式指定。

-H HOSTS_LIST, --hosts=HOSTS_LIST

除了 Red Hat Virtualization Manager 日志外，还需要从 nominated *HOSTS_LIST* 中的虚拟化主机收集日志。包含的主机必须在主机名、完全限定域名或 IP 地址的逗号分隔列表中指定。匹配模式也有效。

SSH 配置

--SSH-port=*PORT*

将 *PORT* 设置为用于与虚拟化主机 SSH 连接的端口。

-k *KEYFILE*, --key-file=*KEYFILE*

将 *KEYFILE* 设置为用于访问虚拟化主机的公共 SSH 密钥。

--max-connections=*MAX_CONNECTIONS*

设置 *MAX_CONNECTIONS* 作为虚拟化主机日志的最大并发 SSH 连接。默认值为 10。

PostgreSQL 数据库选项

必须指定数据库用户名和数据库名称，如果使用 *pg-user* 和 *dbname* 参数（如果从默认值更改了）

如果数据库不在本地主机上，则使用 *pg-dbhost* 参数。使用可选的 *pg-host-key* 参数来收集远程日志。必须在数据库服务器上安装 PostgreSQL SOS 插件，才能远程日志收集才能成功。

--no-postgresql

禁用数据库集合。日志收集器将连接到 Red Hat Virtualization Manager PostgreSQL 数据库，并在日志中包括数据，除非指定了 *--no-postgresql* 参数。

--pg-user=*USER*

将 *USER* 设置为用于与数据库服务器的连接的用户名。默认值为 *postgres*。

--pg-database=*DBNAME*

将 *DBNAME* 设置为用于连接数据库服务器的数据库名称。默认值为 *rhev*。

--pg-dbhost=*DBHOST*

将 **DBHOST** 设置为数据库服务器的主机名。默认值为 **localhost**。

--pg-host-key=KEYFILE

将 **KEYFILE** 设置为数据库服务器的公共身份文件（私钥）。默认情况下不设置这个值；只需要本地主机上不存在数据库的位置。

3.9.5.3. 基本日志收集器使用情况

当在未指定附加参数的情况下运行 **ovirt-log-collector** 命令时，其默认行为是从 Red Hat Virtualization Manager 及其附加的主机收集所有日志。它还会收集数据库日志，除非添加了 **--no-postgresql** 参数。在以下示例中，运行日志收集器以从 Red Hat Virtualization Manager 和三个附加的主机收集所有日志。

例 3.18. 日志收集器使用

```
# ovirt-log-collector
INFO: Gathering oVirt Engine information...
INFO: Gathering PostgreSQL the oVirt Engine database and log files from localhost...
Please provide REST API password for the admin@internal oVirt Engine user (CTRL+D to abort):
About to collect information from 3 hypervisors. Continue? (Y/n):
INFO: Gathering information from selected hypervisors...
INFO: collecting information from 192.168.122.250
INFO: collecting information from 192.168.122.251
INFO: collecting information from 192.168.122.252
INFO: finished collecting information from 192.168.122.250
INFO: finished collecting information from 192.168.122.251
INFO: finished collecting information from 192.168.122.252
Creating compressed archive...
INFO Log files have been collected and placed in /tmp/logcollector/sosreport-rhn-account-20110804121320-ce2a.tar.xz.
The MD5 for this file is 6d741b78925998caff29020df2b2ce2a and its size is 26.7M
```

3.9.6. Engine Vacuum 工具

3.9.6.1. Engine Vacuum 工具

Engine Vacuum 工具通过更新表和删除死行来维护 **PostgreSQL** 数据库，允许重复使用磁盘空间。有关 **VACUUM** 命令及其参数的信息，请参阅 [PostgreSQL 文档](#)。

Engine Vacuum 命令是 **engine-vacuum**。您必须以 **root** 用户身份登录，并为 Red Hat Virtualization 环境提供管理凭证。

或者，在使用 `engine-setup` 命令自定义现有安装时，也可以运行引擎 **Vacuum** 工具：

```
$ engine-setup
...
[ INFO ] Stage: Environment customization
...
Perform full vacuum on the engine database engine@localhost?
This operation may take a while depending on this setup health and the
configuration of the db vacuum process.
See https://www.postgresql.org/docs/12/static/sql-vacuum.html
(Yes, No) [No]:
```

Yes 选项在完全详细模式下运行引擎 **Vacuum** 工具。

3.9.6.2. 引擎 Vacuum 模式

引擎 **Vacuum** 有两种模式：

标准 Vacuum

建议使用频繁的标准清空。

标准 **vacuum** 将删除表中的死行版本和索引，并将空间标记为可用，以备将来重复使用。通常更新的表应定期清空。但是，标准撤离不会将空间返回到操作系统。

标准清空（无参数）处理当前数据库中的每个表。

完整 Vacuum

不建议在常规使用中完全撤离，但只有在需要从表中回收大量空间时才运行。

通过写入没有死空间的表文件的新副本来完全清空表，从而使操作系统能够回收空间。完全撤离可能需要很长时间。

full vacuum 要求额外磁盘空间用于表的新副本，直到操作完成并且旧副本被删除为止。由于完整撤离需要在表上有一个独占锁定，所以无法与其他表的使用并行运行。

3.9.6.3. engine-vacuum 命令的语法

`engine-vacuum` 命令的基本语法为：

```
# engine-vacuum
```

```
# engine-vacuum option
```

运行 `engine-vacuum` 命令，不带选项来执行标准撤离。

有几个参数可以进一步优化 `engine-vacuum` 命令。

常规选项

`-h --help`

介绍如何使用 `engine-vacuum` 命令的信息。

`-a`

运行标准撤离，分析数据库并更新优化器统计信息。

`-A`

分析数据库并更新优化器统计信息，而无需撤离。

`-f`

运行完全撤离。

`-v`

以详细模式运行，提供更多控制台输出。

`-t table_name`

Vacuum 特定表或表。

```
# engine-vacuum -f -v -t vm_dynamic -t vds_dynamic
```

3.9.7. VDSM 到网络名称映射工具

3.9.7.1. 将 VDSM 名称映射到逻辑网络名称

如果逻辑网络的名称超过 15 个字符，或包含非 ASCII 字符，系统会自动生成一个主机标识符 (*vdsml_name*) 名称；它包含字符 *on*，以及网络唯一标识符的前 13 个字符，例如 *ona1b2c3d4e5f6g*。这是显示在主机的日志文件中的名称。要查看逻辑网络名称及其自动生成的网络名称列表，请使用位于 */usr/share/ovirt-engine/bin/* 中的 **VDSM-to-Network-Name Mapping** 工具。

流程

1. 您第一次运行该工具时，定义 **PASSWORD** 环境变量，它是数据库用户的密码，该用户对 **Manager** 数据库具有读取访问权限。例如，运行：

```
# export PASSWORD=DatabaseUserPassword
```

2. 运行 **VDSM-to-Network-Name** 映射工具：

```
# vdsml_to_network_name_map --user USER
```

其中 **USER** 是有关访问 **Manager** 数据库的数据库用户，其密码被分配给 **PASSWORD** 环境变量。

工具显示逻辑网络名称列表，它们映射到其对等主机标识符。

附加标记

您可以使用以下标记运行该工具：

--host 是数据库服务器的 **hostname/IP** 地址。默认值为 **localhost**。

--port 是数据库服务器的端口号。默认值为 **5432**。**--database** 是数据库的名称。默认值为 **engine**，即 **Manager** 数据库。

--secure 启用与数据库的安全连接。默认情况下，工具会在没有安全连接的情况下运行。

第 4 章 收集有关环境的信息

4.1. 监控和可观察性

本章提供了从 Red Hat Virtualization 系统监控和获取指标和日志的方法。这些方法包括：

- 使用数据仓库和 Grafana 监控 RHV
- 将指标发送到 Elasticsearch 的远程实例
- Deploying Insights in Red Hat Virtualization Manager

4.1.1. 使用数据仓库和 Grafana 监控 RHV

4.1.1.1. Grafana 概述

Grafana 是一个基于 Web 的 UI 工具，用于根据数据库名称 `ovirt_engine_history` 中的 oVirt Data Warehouse PostgreSQL 数据库收集的数据显示报告。有关可用报告仪表板的详情，请查看 [Grafana 仪表盘](#) 和 [Grafana 网站 - 仪表盘](#)。

来自 Manager 的数据将每分钟收集一次，并在每小时和每日聚合时进行汇总。根据 `engine-setup` (基本或完整扩展) 在数据仓库配置中定义的扩展设置来保留这些数据：

- **Basic (默认)** - 为 24 小时保存的样本数据，每小时的数据针对 1 个月、每天保存的数据 - 不会保存每日聚合。
- **完全 (推荐)** 保存的样本数据为 24 小时，每小时数据保存了 2 个月，每天 5 年保存的聚合。

完整的样本扩展可能需要将数据仓库迁移到单独的虚拟机。

- 有关数据仓库扩展说明，请参阅 [更改数据仓库采样扩展](#)。
-

有关将数据仓库迁移至独立机器或安装的说明，请参阅 [Migrating Data Warehouse to a Separate Machine](#) 和 [Installing and Configuring Data Warehouse on a Separate Machine](#)。



注意

红帽只支持安装数据仓库数据库、数据仓库服务和 Grafana，它们都与彼此相同，尽管您可以在独立的机器上分别安装这些组件。

4.1.1.2. 安装

当您在 Stand Alone Manager 安装以及自托管引擎安装中运行 Red Hat Virtualization Manager engine-setup 时，Grafana 集成会被默认启用并安装。



注意

Grafana 不会被默认安装，您可能需要在一些情况下手动安装，比如从 RHV 的早期版本执行、恢复备份，或者在将数据仓库迁移到独立的机器时。

手动启用 Grafana 集成：

1. 将环境设置为全局维护模式：

```
# hosted-engine --set-maintenance --mode=global
```

2. 登录到要安装 Grafana 的机器。这应该是配置 Data Warehouse 的同一计算机，通常是 Manager 计算机。

3. 按照如下所示运行 engine-setup 命令：

```
# engine-setup --reconfigure-optional-components
```

4. 回答 Yes 在该机器上安装 Grafana：

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


5. 禁用全局维护模式：

```
# hosted-engine --set-maintenance --mode=none
```

访问 Grafana 仪表板：

- 进入 `https://<engine FQDN 或 IP 地址>/ovirt-engine-grafana`

或者

- 在管理门户的 Web 管理欢迎页面中，点 **Monitoring Portal**。

4.1.1.2.1. 为单点登录配置 Grafana

`Manager engine-setup` 自动配置 Grafana，以允许 Manager 上的现有用户通过管理门户中的 SSO 登录，但不会自动创建用户。您需要创建新用户（Grafana UI 中的 Invite），确认新用户，然后登录。

1. 如果尚未定义，在 Manager 中为该用户设置电子邮件地址。

2. 使用现有 admin 用户（初始配置管理员）登录到 Grafana。

3. 进入 **Configuration** → **Users** 并选择 **Invite**。

4. 输入电子邮件地址和名称，然后选择一个角色。

5. 使用以下选项之一发送邀请：

- 选择发送邀请邮件，然后单击提交。对于这个选项，您需要在 Grafana 机器上配置的操作本地邮件服务器。

或者

- 选择 **Pending Invites**
 - 找到您想要的条目
 - 选择 **Copy invite**
 - 通过直接进入浏览器地址栏或将其发送到另一个用户，复制并使用此链接来创建帐户。

如果您使用 **Pending Invites** 选项，则不会发送任何电子邮件，且电子邮件地址实际上不需要存在 - 只要作为管理器用户的电子邮件地址配置，任何有效的查找地址都将可以正常工作。

使用这个帐户登录：

1. 使用具有此电子邮件地址的帐户登录到 **Red Hat Virtualization Web 管理** 欢迎页面。
2. 选择 **Monitoring Portal** 来打开 **Grafana** 仪表板。
3. 选择 **Sign in with oVirt Engine Auth.**

4.1.1.3. 内置 Grafana 仪表板

以下仪表板可在初始 **Grafana** 设置中报告 **Data Center**、**Cluster**、**Host** 和 **Virtual Machine** 数据：

表 4.1. 内置 Grafana 仪表板

仪表板类型	内容
-------	----

仪表板类型	内容
<p>执行仪表板</p>	<ul style="list-style-type: none"> ● 系统仪表板 - 根据最新配置，在系统中的主机和存储域的资源使用和时间。 ● 数据中心仪表板 - 根据最新配置，在所选数据中心中的集群、主机和存储域的资源使用、峰值和时间。 ● 集群仪表板 - 根据最新配置，对所选集群中的主机和虚拟机的资源使用、峰值、过量和运行时间。 ● 主机仪表板 - 选择期间内选定主机的最新和历史配置详情和资源使用情况指标。 ● Virtual Machine dashboard - 在所选时间段内为所选虚拟机的最新和历史配置详情和资源使用情况指标。 ● 执行仪表板 - 在选定时间段内为选定集群中主机和虚拟机的用户资源使用情况和操作系统数量。
<p>清单仪表板</p>	<ul style="list-style-type: none"> ● 清单仪表板 - 根据最新配置，对所选数据中心的主机、虚拟机和运行虚拟机、资源使用量和过量使用率的数量。 ● 主机清单仪表板 - FQDN、VDSM 版本、操作系统、CPU 模型、CPU 内核、内存大小、创建日期、删除日期，以及所选主机的硬件详情。 ● Storage Domains Inventory dashboard - 域类型、存储类型、可用磁盘大小、使用磁盘大小、创建日期以及所选存储域中删除日期。 ● 虚拟机清单仪表板 - 根据最新配置，模板名称、操作系统、CPU 内核、内存大小、创建日期和删除选定虚拟机的日期。

仪表板类型	内容
服务级别仪表板	<ul style="list-style-type: none"> ● 运行时间仪表板 - 计划停机、计划外停机时间以及主机、高可用性虚拟机和选定集群中所有虚拟机的总时间。 ● 主机正常运行时间仪表板 - 选择期间内所选主机的正常运行时间、计划停机时间和计划外停机时间。 ● 虚拟机正常运行时间仪表板 - 选择期间内所选虚拟机的正常运行时间、计划停机时间和计划外停机时间。 ● 集群服务质量 <ul style="list-style-type: none"> ○ 主机仪表板 - 所选主机在选定时间段内执行以上的时间及低于 CPU 和内存阈值。 ○ Virtual Machines 仪表板 - 所选虚拟机在所选时间段内执行的虚拟机的时间及低于 CPU 和内存阈值。
趋势仪表板	<ul style="list-style-type: none"> ● 趋势仪表板 - 按内存和所选集群中 CPU 按内存和 CPU 在选定期间内 5 个最多使用和最少使用的虚拟机和主机的用量率。 ● 主机 Trend dashboard - 在所选时间段内为所选主机使用资源用量（虚拟机、CPU、内存和网络 Tx/Rx）。 ● 虚拟机 Trend 仪表板 - 在所选时间段内为所选虚拟机消耗(CPU、内存、网络 Tx/Rx、磁盘 I/O)。 ● 主机资源使用仪表板 - 在选定时间段内为所选主机（虚拟机、CPU、内存、网络 Tx/Rx）的每日和每小时资源使用量（虚拟机数量、CPU、内存、网络 Tx/Rx）。 ● 虚拟机资源使用仪表板 - 在选定时间段内为所选虚拟机(CPU、内存、网络 Tx/Rx、磁盘 I/O)的每日和每小时的资源使用量(CPU、内存、网络 Tx/Rx、磁盘 I/O)。



注意

Grafana 仪表板包括到 Red Hat Virtualization 管理门户的直接链接，允许您快速查看集群、主机和虚拟机的详情。

4.1.1.4. 自定义 Grafana 仪表板

您可以根据报告需求创建自定义仪表板或复制并修改现有仪表板。



注意

无法自定义内置仪表板。

4.1.2. 将指标和日志发送到 Elasticsearch 的远程实例



注意

红帽不拥有或维护 Elasticsearch。您需要熟悉 Elasticsearch 设置和维护来部署这个选项。

您可以配置 Red Hat Virtualization Manager 和主机，将指标数据和日志发送到现有的 Elasticsearch 实例。

为此，请运行 Ansible 角色，它将在 Manager 和所有主机上配置 collectd 和 rsyslog，以收集 engine.log、vdsm.log 和 collectd 指标，并将它们发送到 Elasticsearch 实例。

如需更多信息，包括可用 Metrics Schema 的说明的完整列表，请参阅[将 RHV 监控数据发送到远程 Elasticsearch 实例](#)。

4.1.2.1. 安装 collectd 和 rsyslog

在主机上部署 collectd 和 rsyslog，以收集日志和指标。



注意

您不需要为新主机重复此步骤。每个添加的新主机由 Manager 自动配置，以便在 host-deploy 期间将数据发送到 Elasticsearch。

流程

1. 使用 SSH 登录 Manager 机器。

2.

复制 `/etc/ovirt-engine-metrics/config.yml.example` 以创建 `/etc/ovirt-engine-metrics/config.yml.d/config.yml` :

```
# cp /etc/ovirt-engine-metrics/config.yml.example /etc/ovirt-engine-
metrics/config.yml.d/config.yml
```

3.

编辑 `config.yml` 中的 `ovirt_env_name` 和 `elasticsearch_host` 参数，并保存文件。以下附加参数可添加到文件中：

```
use_omasticsearch_cert: false
rsyslog_elasticsearch_usehttps_metrics: !!str off
rsyslog_elasticsearch_usehttps_logs: !!str off
```

- 使用证书时，将 `use_omasticsearch_cert` 设置为 `true`。
- 要禁用日志或指标，请使用 `rsyslog_elasticsearch_usehttps_metrics` 和/或 `rsyslog_elasticsearch_usehttps_logs` 参数。

4.

在主机上部署 `collectd` 和 `rsyslog` :

```
# /usr/share/ovirt-engine-
metrics/setup/ansible/configure_ovirt_machines_for_metrics.sh
```

`configure_ovirt_machines_for_metrics.sh` 脚本运行包含 `linux-system-roles`（请参阅使用 [RHEL 中的系统角色管理和配置任务](#)）的 Ansible 角色，并使用它来在主机上部署和配置 `rsyslog`。`rsyslog` 从 `collectd` 收集指标并将其发送到 `Elasticsearch`。

4.1.2.2. 日志记录模式和分析日志

使用 [Discover](#) 页面以交互方式探索从 RHV 收集的数据。收集的每个结果集合都被称为文档。文档从以下日志文件收集：

- `engine.log` - 包含所有 oVirt Engine UI 崩溃、Active Directory 查找、数据库问题和其他事件。
- `vdsm.log` - VDSM 的日志文件、虚拟化主机上的管理器代理，包含主机相关事件。

以下字段可用：

parameter	description
_id	文档的唯一 ID
_index	文档所属索引的 ID。带有 project.ovirt-logs 前缀的索引是 Discover 页面中的唯一相关索引。
hostname	对于 engine.log，这是 Manager 的主机名。对于 vdsm.log，这是主机的主机名。
level	日志记录严重性为：TRACE、DEBUG、INFO、WARN、ERROR、FATAL。
message	文档消息的正文。
ovirt.class	生成此日志的 Java 类名称。
ovirt.correlationid	仅限 engine.log。此 ID 用于关联 Manager 执行单个任务的多个部分。
ovirt.thread	生成日志记录的 Java 线程的名称。
tag	可用于过滤数据的预定义元数据集合。
@timestamp	所发出的 [time](Troubleshooting#information-is-is-kibana)。
_score	N/A
_type	N/A
ipaddr4	机器的 IP 地址。
ovirt.cluster_name	仅限 vdsms.log。主机所属的集群名称。
ovirt.engine_fqdn	Manager 的 FQDN。
ovirt.module_lineno	运行在 ovirt.class 中定义的命令的文件和行号。

4.1.3. 部署 Insights

要在安装有 Red Hat Virtualization Manager 的现有 Red Hat Enterprise Linux (RHEL) 系统中部署 Red Hat Insights，请完成以下步骤：

- 将该系统注册到 Red Hat Insights 应用程序。
- 启用 Red Hat Virtualization 环境中的数据收集。

4.1.3.1. 将系统注册到 Red Hat Insights

注册系统，以与 Red Hat Insights 服务通信，并查看 Red Hat Insights 控制台中显示的结果。

```
[root@server ~]# insights-client --register
```

4.1.3.2. 启用 Red Hat Virtualization 环境中的数据收集

修改 `/etc/ovirt-engine/rhv-log-collector-analyzer/rhv-log-collector-analyzer.conf` 文件以包含以下行：

```
upload-json=True
```

4.1.3.3. 查看 Insights 结果以 Insights 控制台

可以在 [智能分析工具控制台](#) 中查看系统和基础架构结果。**Overview** 选项卡提供基础架构当前风险的仪表盘视图。从起点开始，您可以调查特定规则如何影响您的系统，或者采用基于系统的方法来查看与系统造成风险的所有匹配。

流程

1. 选择 **Rule hits by severity**，按照它们对基础架构构成的 **Total Risk** 来查看规则(关键、重要、中等或低)。或者
2. 根据类型选择 **Rule hits** 查看您的基础架构中的潜在风险的类型 (**Availability, Stability, Performance, 或 Security**)。或者
3. 按名称搜索特定规则，或者滚动规则列表来查看有关风险、系统公开和可用性的 **Ansible Playbook** 的高级别信息，以自动进行修复。

4. 点击规则查看规则的描述，从知识库文章中了解更多相关信息，并查看受影响的系统列表。
5. 点系统查看有关检测到的问题的具体信息，以及解决问题的步骤。

4.2. 日志文件

4.2.1. Manager 安装日志文件

表 4.2. 安装

日志文件	Description
<code>/var/log/ovirt-engine/engine-cleanup-yyyy_mm_dd_hh_mm_ss.log</code>	engine-cleanup 命令的日志。这是重置 Red Hat Virtualization Manager 安装的命令。每次运行命令时都会生成一个日志。运行的日期和时间在文件名中使用，以允许存在多个日志。
<code>/var/log/ovirt-engine/engine-db-install-yyyy_mm_dd_hh_mm_ss.log</code>	使用 engine-setup 命令的日志，详细介绍了引擎数据库的创建和配置。
<code>/var/log/ovirt-engine/ovirt-engine-dwh-setup-yyyy_mm_dd_hh_mm_ss.log</code>	来自 ovirt-engine-dwh-setup 命令的日志。这是用于创建报告的 <code>ovirt_engine_history</code> 数据库的命令。每次运行命令时都会生成一个日志。运行的日期和时间在文件名中使用，以便允许多个日志同时存在。
<code>/var/log/ovirt-engine/setup/ovirt-engine-setup-yyyymmddhhmmss.log</code>	从 engine-setup 命令的日志。每次运行命令时都会生成一个日志。运行的日期和时间在文件名中使用，以便允许多个日志同时存在。

4.2.2. Red Hat Virtualization Manager Log Files

表 4.3. 服务活动

日志文件	Description
<code>/var/log/ovirt-engine/engine.log</code>	反映所有 Red Hat Virtualization Manager GUI 崩溃、Active Directory 查找、数据库问题和其他事件。
<code>/var/log/ovirt-engine/host-deploy</code>	从 Red Hat Virtualization Manager 部署的主机的日志文件。
<code>/var/lib/ovirt-engine/setup-history.txt</code>	跟踪与 Red Hat Virtualization Manager 相关的软件包的安装和升级。

日志文件	Description
<code>/var/log/httpd/ovirt-requests-log</code>	<p>通过 HTTPS 向 Red Hat Virtualization Manager 发出的请求记录日志文件，包括每个请求所需的时间。</p> <p>包含 Correlation-Id 标头，允许您在将日志文件与 <code>/var/log/ovirt-engine/engine.log</code> 进行比较时比较请求。</p>
<code>/var/log/ovn-provider/ovirt-provider-ovn.log</code>	记录 OVN 提供程序的活动。有关 Open vSwitch 日志的详情，请查看 Open vSwitch 文档 。

4.2.3. SPICE 日志文件

在对 **SPICE** 连接问题进行故障排除时，**SPICE** 日志文件很有用。要启动 **SPICE** 调试，请将日志级别更改为 **调试**。然后，标识日志位置。

用于访问客户机机器和客户机机器的客户端本身都有 **SPICE** 日志文件。对于客户端日志，如果使用下载了 `console.vv` 文件的原生客户端启动 **SPICE** 客户端，请使用 `remote-viewer` 命令启用调试和生成日志输出。

4.2.3.1. 适用于 Hypervisor SPICE 服务器的 SPICE 日志

表 4.4. 适用于 Hypervisor SPICE 服务器的 SPICE 日志

日志类型	日志位置	更改日志级别：
主机/Hypervisor SPICE 服务器	<code>/var/log/libvirt/qemu/(guest_name).log</code>	<p>在启动客户机前，在主机/hypervisor 上运行 导出 SPICE_DEBUG_LEVEL=5。此变量由 QEMU 解析，如果运行系统范围的将打印系统中所有虚拟机的调试信息。此命令必须在集群中的每个主机上运行。这个命令只在主机/管理程序为基础工作，而不是按集群为基础。</p>

4.2.3.2. 适用于客户机机器的 SPICE 日志

表 4.5. spice-vdagent Logs for Guest Machines

日志类型	日志位置	更改日志级别：
Windows 客户机	<code>C:\Windows\Temp\vdagent.log</code> <code>C:\Windows\Temp\vdservice.log</code>	Not applicable

日志类型	日志位置	更改日志级别：
Red Hat Enterprise Linux Guest	使用 journalctl 作为 root 用户。	<p>要在调试模式下运行 spice-vdagentd 服务，以 root 用户身份创建一个带有此条目的 <code>/etc/sysconfig/spice-vdagentd</code> 文件：</p> <pre>SPICE_VDAGENTD_EXTRA_ARGS="-d"</pre> <p>要在命令行中运行 spice-vdagent，请从命令行运行：</p> <pre>\$ killall -u \$USER spice-vdagent \$ spice-vdagent -x -d [-d] [& tee spice-vdagent.log]</pre>

4.2.3.3. 使用 console.vv 文件启动 SPICE 客户端的 SPICE 日志

对于 Linux 客户端机器：

1. 使用 `--spice-debug` 选项运行 `remote-viewer` 命令来启用 SPICE 调试。出现提示时，输入连接 URL，例如 `spice://virtual_machine_IP : 端口`。

```
# remote-viewer --spice-debug
```

2. 要使用 `debug` 参数运行 SPICE 客户端并将 `.vv` 文件传递给该文件，请下载 `console.vv` 文件，并使用 `--spice-debug` 选项运行 `remote-viewer` 命令并指定 `console.vv` 文件的完整路径。

```
# remote-viewer --spice-debug /path/to/console.vv
```

对于 Windows 客户端机器：

1. 在版本 `virt-viewer 2.0-11.el7ev` 或更高版本中，`virt-viewer.msi` 会安装 `virt-viewer` 和 `debug-viewer.exe`。
2. 使用 `spice-debug` 参数运行 `remote-viewer` 命令，并在控制台的路径上指示命令：

```
remote-viewer --spice-debug path\to\console.vv
```

3.

要查看日志、连接到虚拟机，您会看到运行 GDB 的命令提示，该提示打印了 `remote-viewer` 的标准输出和标准错误。

4.2.4. 主机日志文件

日志文件	Description
<code>/var/log/messages</code>	<code>libvirt</code> 使用的日志文件。使用 <code>journalctl</code> 查看日志。您需要是 <code>adm</code> , <code>systemd-journal</code> , 或 <code>wheel</code> 组的成员才可以查看日志。
<code>/var/log/vdsm/spm-lock.log</code>	详细主机在存储池管理程序角色上获取租用的日志文件。主机获取、发布、续订或无法更新租期的日志详情。
<code>/var/log/vdsm/vdsm.log</code>	VDSM 的日志文件，即主机上的 Manager 代理。
<code>/tmp/ovirt-host-deploy-Date.log</code>	主机部署日志，作为 <code>/var/log/ovirt-engine/host-deploy/ovirt-Date-HostCorrelation_ID.log</code> 复制到 Manager 中。
<code>/var/log/vdsm/import/import-UUID-Date.log</code>	详细说明虚拟机从 KVM 主机、VMWare 供应商或 RHEL 5 Xen 主机导入的日志文件，包括导入失败信息。 <code>UUID</code> 是导入的虚拟机的 UUID， <code>日期</code> 是导入开始的日期和时间。
<code>/var/log/vdsm/supervdsm.log</code>	记录使用超级用户权限执行的 VDSM 任务。
<code>/var/log/vdsm/upgrade.log</code>	VDSM 在主机升级过程中使用此日志文件来记录配置更改。
<code>/var/log/vdsm/mom.log</code>	记录 VDSM 内存过量使用管理器的活动。

4.2.5. 为 Red Hat Virtualization 服务设置 debug 级日志记录



注意

将日志记录设置为调试级别可能会公开敏感信息，如密码或内部虚拟机数据。确保不受信任或未授权的用户无法访问调试日志。

您可以通过修改每个服务的 `sysconfig` 文件，将以下 Red Hat Virtualization (RHV) 服务的日志设置为 `debug` 级别。

表 4.6. RHV 服务和 `sysconfig` 文件路径

Service	文件路径
ovirt-engine.service	/etc/sysconfig/ovirt-engine
ovirt-engine-dwhd.service	/etc/sysconfig/ovirt-engine-dwhd
ovirt-fence-kdump-listener.service	/etc/sysconfig/ovirt-fence-kdump-listener
ovirt-websocket-proxy.service	/etc/sysconfig/ovirt-websocket-proxy

这个修改会影响 Python 打包程序执行的日志记录，而不是主服务进程。

将日志记录设置为 **debug-level** 有助于调试与启动相关的问题 - 例如，如果主进程因为缺失或不正确的 **Java** 运行时或库而无法启动。

前提条件

- 验证您要修改的 **sysconfig** 文件是否存在。如有必要，请创建它。

流程

1. 将以下内容添加到服务的 **sysconfig** 文件中：

```
OVIRT_SERVICE_DEBUG=1
```

2. 重启服务：

```
# systemctl restart <service>
```

服务的 **sysconfig** 日志文件现在设置为 **debug-level**。

此设置导致的日志记录进入系统日志，因此其生成的日志可以在 **/var/log/messages** 中找到，而不是在特定于服务的日志文件中，也可以使用 **journalctl** 命令。

4.2.6. Red Hat Virtualization 服务的主配置文件

除了 `sysconfig` 文件外，每个 Red Hat Virtualization (RHV) 服务还包含另一个常用的配置文件。

表 4.7. RHV 服务和配置文件

Service	sysconfig 文件路径	主配置文件
<code>ovirt-engine.service</code>	<code>/etc/sysconfig/ovirt-engine</code>	<code>/etc/ovirt-engine/engine.conf.d/*.conf</code>
<code>ovirt-engine-dwhd.service</code>	<code>/etc/sysconfig/ovirt-engine-dwhd</code>	<code>/etc/ovirt-engine-dwhd/ovirt-engine-dwhd.conf.d/*.conf</code>
<code>ovirt-fence-kdump-listener.service</code>	<code>/etc/sysconfig/ovirt-fence-kdump-listener</code>	<code>/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/*.conf</code>
<code>ovirt-websocket-proxy.service</code>	<code>/etc/sysconfig/ovirt-websocket-proxy</code>	<code>/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/*.conf</code>

4.2.7. 设置主机日志记录服务器

主机生成和更新日志文件，记录它们的操作和问题。收集这些日志文件可以集中进行调试。

这个步骤应该用于集中式日志服务器。您可以使用单独的日志记录服务器，或使用此流程在 Red Hat Virtualization Manager 中启用主机日志记录。

流程

1. 检查防火墙是否允许 UDP 514 端口上的流量，并打开到 `syslog` 服务流量：

```
# firewall-cmd --query-service=syslog
```

如果输出没有，允许 UDP 514 端口上的流量：

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

2. 在 `syslog` 服务器上创建一个新的 `.conf` 文件，例如 `/etc/rsyslog.d/from_remote.conf`，并添加以下行：

```
template(name="DynFile" type="string"
string="/var/log/%HOSTNAME%/%%PROGRAMNAME%.log")
RuleSet(name="RemoteMachine"){ action(type="omfile" dynaFile="DynFile") }
Module(load="imudp")
Input(type="imudp" port="514" ruleset="RemoteMachine")
```

3.

重启 rsyslog 服务：

```
# systemctl restart rsyslog.service
```

4.

登录到虚拟机监控程序，并在 `/etc/rsyslog.conf` 中添加以下行：

```
*.info;mail.none;authpriv.none;cron.none @<syslog-FQDN>:514
```

5.

重新启动 hypervisor 上的 rsyslog 服务。

```
# systemctl restart rsyslog.service
```

您的集中式日志服务器现在已配置为从虚拟主机接收和存储消息和安全日志。

4.2.8. 启用 SyslogHandler 将 RHV Manager 日志传递给远程 syslog 服务器

此实施使用 JBoss EAP SyslogHandler 日志管理器，并支持将日志记录从 `engine.log` 和 `server.log` 传递到 syslog 服务器。

注意

RHV 版本早于 RHV 4.4.10，功能类似于 `ovirt-engine-extension-logger-log4j` 的功能。该软件包已在 RHV 4.4.10 中删除，并使用 JBoss EAP SyslogHandler 日志管理器替代了新的实现。如果您在以前的 RHV 版本中使用 `ovirt-engine-extension-logger-log4j`，请按照升级到 RHV 4.4.10 执行以下步骤：

- 使用本章中提供的准则，手动配置日志记录到远程 syslog 服务器。
- 手动删除 `ovirt-engine-extension-logger-log4j` 配置文件（删除 `/etc/ovirt-engine/extensions.d/Log4jLogger.properties` 配置文件）。

在中央 **syslog** 服务器上使用这个步骤。您可以使用单独的日志记录服务器，或使用此流程将 **engine.log** 和 **server.log** 文件从 **Manager** 传递给 **syslog** 服务器。另请参阅 [配置步骤 设置主机日志记录服务器](#)。

配置 SyslogHandler 实施

1. 在 `/etc/ovirt-engine/engine.conf.d` 目录中创建配置文件 `90-syslog.conf`，并添加以下内容：

```
SYSLOG_HANDLER_ENABLED=true
SYSLOG_HANDLER_SERVER_HOSTNAME=localhost
SYSLOG_HANDLER_FACILITY=USER_LEVEL
```

2. 安装和配置 **rsyslog**。

```
# dnf install rsyslog
```

3. 配置 **SELinux** 以允许 **rsyslog** 流量。

```
# semanage port -a -t syslogd_port_t -p udp 514
```

4. 创建配置文件 `/etc/rsyslog.d/rhvm.conf` 并添加以下内容：

```
user.* /var/log/jboss.log
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")
```

5. 重启 **rsyslog** 服务。

```
# systemctl restart rsyslog.service
```

6. 如果启用了并激活防火墙，请运行以下命令在 **Firewalld** 中打开 **rsyslog** 端口：

```
# firewall-cmd --permanent --add-port=514/udp
# firewall-cmd --reload
```

7. 重启 **Red Hat Virtualization Manager**。

-

```
# systemctl restart ovirt-engine
```

syslog 服务器现在可以接收和存储 **engine.log** 文件。

附录 A. VDSM 服务和 HOOK

Red Hat Virtualization Manager 使用 VDSM 服务来管理 Red Hat Virtualization 主机(RHVH)和 Red Hat Enterprise Linux 主机。VDSM 管理和监控主机的存储、内存和网络资源。它还协调虚拟机创建、统计收集、日志收集和其他主机管理任务。VDSM 作为由 Red Hat Virtualization Manager 管理的每个主机中的守护进程运行。它应答来自客户端的 XML-RPC 调用。Red Hat Virtualization Manager 作为 VDSM 客户端的功能。

VDSM 可通过 hook 扩展。挂钩是关键事件发生时在主机上执行的脚本。当支持的事件发生时，VDSM 会按字母数字顺序在 `/usr/libexec/vdsm/hooks/nn_event-name` 中运行任何可执行 hook 脚本。按照惯例，每个 hook 脚本都会分配两个数字（包含在文件名的前面），以确保以脚本运行的顺序明确。您可以使用任何编程语言创建 hook 脚本，但 Python 仍将用于本章中包含的示例。

请注意，主机上为事件定义的所有脚本都会被执行。如果您要求给定 hook 仅针对主机上运行的虚拟机的子集执行，则必须通过评估与虚拟机关联的自定义属性来处理此要求。



警告

VDSM hook 可能会干扰 Red Hat Virtualization 的运作。VDSM hook 中的错误可能导致虚拟机崩溃和数据丢失。VDSM hook 应谨慎实施并经过严格测试。Hooks API 是新的，可能会在以后有重大变化。

您可以使用事件驱动的 hook 扩展 VDSM。使用 hook 扩展 VDSM 是一个实验性技术，本章面向有经验的开发人员。

通过在虚拟机上设置自定义属性，可以将特定于给定虚拟机的其他参数传递给 hook 脚本。

A.1. 安装 VDSM HOOK

默认情况下不会安装 VDSM hook。如果需要特定的 hook，您必须手动安装它。

前提条件

- 主机存储库必须启用。
- 使用 root 权限登录到主机。

流程

1. 获取可用 hook 列表：

```
# dnf list vdsm\*hook\*
```

2. 将主机置于维护模式。

3. 在主机上安装所需的 VDSM hook 软件包：

```
# dnf install <vds-hook-name>
```

例如，要在主机上安装 `vds-hook-vhostmd` 软件包，请输入以下内容：

```
# dnf install vds-hook-vhostmd
```

4. 重启主机。

其他资源

- [启用 Red Hat Virtualization 主机存储库](#)
- [启用 Red Hat Enterprise Linux 主机存储库](#)

A.2. 支持的 VDSM 事件

表 A.1. 支持的 VDSM 事件

Name	Description
before_vm_start	在虚拟机启动前。

Name	Description
after_vm_start	虚拟机启动后。
before_vm_cont	在虚拟机继续之前。
after_vm_cont	虚拟机继续后。
before_vm_pause	在虚拟机暂停之前。
after_vm_pause	虚拟机暂停后。
before_vm_hibernate	虚拟机休眠之前。
after_vm_hibernate	虚拟机休眠后。
before_vm_dehibernate	在虚拟机离开之前。
after_vm_dehibernate	虚拟机离开后。
before_vm_migrate_source	在虚拟机迁移之前，在进行迁移的源主机上运行。
after_vm_migrate_source	虚拟机迁移后，在进行迁移的源主机上运行。
before_vm_migrate_destination	在虚拟机迁移之前，在进行迁移的目标主机上运行。
after_vm_migrate_destination	虚拟机迁移后，在进行迁移的目标主机上运行。
after_vm_destroy	虚拟机销毁后。
before_vdsm_start	在主机上启动 VDSM 之前。 before_vdsm_start hook 以 root 用户身份执行，不继承 VDSM 进程的环境。
after_vdsm_stop	在主机上停止 VDSM 后。 after_vdsm_stop hook 以 root 用户身份执行，且不会继承 VDSM 进程的环境。
before_nic_hotplug	在 NIC 被热插到虚拟机之前。
after_nic_hotplug	NIC 热插到虚拟机后。
before_nic_hotunplug	在 NIC 被拔掉虚拟机前
after_nic_hotunplug	NIC 热插虚拟机后。
after_nic_hotplug_fail	将 NIC 热插到虚拟机后会失败。
after_nic_hotunplug_fail	热拔虚拟机中的 NIC 后会失败。

Name	Description
before_disk_hotplug	在磁盘被热插到虚拟机之前。
after_disk_hotplug	磁盘热插到虚拟机后。
before_disk_hotunplug	在磁盘被热插前
after_disk_hotunplug	在磁盘被热拔掉虚拟机后。
after_disk_hotplug_fail	热插拔到虚拟机后，对虚拟机进行热插拔后。
after_disk_hotunplug_fail	从虚拟机热拔磁盘后，虚拟机会失败。
before_device_create	在创建一个支持自定义属性的设备前。
after_device_create	创建支持自定义属性的设备后。
before_update_device	在更新支持自定义属性的设备前。
after_update_device	在更新支持自定义属性的设备后。
before_device_destroy	在销毁支持自定义属性的设备前。
after_device_destroy	销毁支持自定义属性的设备后。
before_device_migrate_destination	在设备迁移前，在目标主机上运行迁移。
after_device_migrate_destination	在设备迁移后，在目标主机上运行迁移。
before_device_migrate_source	在设备迁移前，在进行迁移的源主机上运行。
after_device_migrate_source	在设备迁移后，在进行迁移的源主机上运行。
after_network_setup	启动主机机器时设置网络。
before_network_setup	在启动主机机器时设置网络前。

A.3. VDSM HOOK 环境

大多数 hook 脚本都以 vdsd 用户身份运行，并继承 VDSM 进程的环境。例外是，hook 脚本由 before_vdsm_start 和 after_vdsm_stop 事件触发。这些事件触发的 hook 脚本以 root 用户身份运行，不继承 VDSM 进程的环境。

A.4. VDSM HOOK 域 XML 对象

VDSM 使用 **libvirt 域 XML 格式来定义** 虚拟机。虚拟机的 UUID 可以从域 XML 中分离，但也可作为环境变量 `vmId` 提供。

当启动 `hook` 脚本时，`_hook_domxml` 变量会附加到环境中。这个变量包含相关虚拟机的 **libvirt 域 XML 表示** 的路径。

某些 `hook` 是此规则的一个例外。以下 `hook` 包含 NIC 的 XML 表示，而不是虚拟机：

- `*_nic_hotplug_*`
- `*_nic_hotunplug_*`
- `*_update_device`
- `*_device_create`
- `*_device_migrate_*`



重要

`before_migration_destination` 和 `before_dehibernation` `hook` 当前从源主机接收域 XML。目标上的域 XML 会有所不同。

A.5. 定义自定义属性

Red Hat Virtualization Manager 接受的自定义属性（并被传递给自定义 `hook`）使用 `engine-config` 命令定义。作为安装 Red Hat Virtualization Manager 的主机上的 `root` 用户运行这个命令。

`UserDefinedVMProperties` 和 `CustomDeviceProperties` 配置键用于存储支持的自定义属性的名称。定义每个指定自定义属性的有效值的正则表达式也包含在这些配置键中。

多个自定义属性由分号分隔。请注意，在设置配置键时，其中包含的现有值都会被覆盖。在结合新的和现有的自定义属性时，必须包括用来设置键值的命令中的所有自定义属性。

更新配置密钥后，必须重启 **ovirt-engine** 服务以使新值生效。

例 A.1. 虚拟机属性 - 定义 智能卡 自定义属性

1. 使用以下命令，检查 **UserDefinedVMProperties** 配置键定义的现有自定义属性：

```
# engine-config -g UserDefinedVMProperties
```

如以下输出所示，已定义了自定义属性 **内存**。正则表达式 **^[0-9]+\$** 可确保自定义属性仅包含数字字符。

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 4.3
UserDefinedVMProperties: version: 4.4
UserDefinedVMProperties : memory=^[0-9]+$ version: 4.4
```

2. 因为 **memory custom** 属性已在 **UserDefinedVMProperties** 配置键中定义，所以新的自定义属性必须附加到其中。其他自定义属性 **smartcard** 添加到配置键的值中。新的自定义属性可以容纳值 **true** 或 **false**。

```
# engine-config -s UserDefinedVMProperties='memory=^[0-9]+$;smartcard=^(true|false)$'
--cver=4.4
```

3. 验证 **UserDefinedVMProperties** 配置键定义的自定义属性已正确更新。

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 4.3
UserDefinedVMProperties: version: 4.4
UserDefinedVMProperties : memory=^[0-9]+$;smartcard=^(true|false)$ version: 4.4
```

4. 最后，必须重启 **ovirt-engine** 服务才能使配置更改生效。

```
# systemctl restart ovirt-engine.service
```

例 A.2. 设备属性 - 定义 接口 自定义属性

1. 使用以下命令，检查 **CustomDeviceProperties** 配置键定义的现有自定义属性：

```
# engine-config -g CustomDeviceProperties
```

如以下输出所示，尚未定义任何自定义属性。

```
# engine-config -g CustomDeviceProperties
CustomDeviceProperties: version: 4.3
CustomDeviceProperties: version: 4.4
```

2. 接口自定义属性尚不存在，因此可以将其附加为。在本例中，速度子操作的值设置为 0 到 99999，而 **duplex** 子选项的值设定为 **full** 或 **half**。

```
# engine-config -s CustomDeviceProperties="{type=interface;prop={speed=^[0-9]{1,5}$;duplex=^(full|half)$}}" --cver=4.4
```

3. 验证 **CustomDeviceProperties** 配置键定义的自定义属性已正确更新。

```
# engine-config -g CustomDeviceProperties
UserDefinedVMProperties: version: 4.3
UserDefinedVMProperties: version: 4.4
UserDefinedVMProperties : {type=interface;prop={speed=^[0-9]{1,5}$;duplex=^(full|half)$}} version: 4.4
```

4. 最后，必须重启 **ovirt-engine** 服务才能使配置更改生效。

```
# systemctl restart ovirt-engine.service
```

A.6. 设置虚拟机自定义属性

在 **Red Hat Virtualization Manager** 中定义自定义属性后，您可以在虚拟机上设置它们。自定义属性在管理门户中 **New Virtual Machine** 和 **Edit Virtual Machine** 窗口的 **Custom Properties** 选项卡中设置。

您还可以从 **Run Virtual Machine (s)** 对话框中设置自定义属性。从 **Run Virtual Machine (s)** 对话框中设置的自定义属性仅适用于虚拟机，直到关闭为止。

Custom Properties 选项卡为您提供了可从定义的自定义属性列表中选择的功能。选择自定义属性键后，将显示一个额外字段，供您输入该键的值。单击 + 按钮，再单击 - 按钮并将它们移除，从而添加额外的键/值对。

A.7. 在 VDSM HOOK 中评估虚拟机自定义属性

在虚拟机的 **Custom Properties** 字段中设置的每个键都会在调用 **hook** 脚本时作为环境变量附加。虽然用于验证 **Custom Properties** 字段的正则表达式提供一些保护，但应确保脚本也会验证提供的输入是否与预期相符。

例 A.3. 评估自定义属性

此短 Python 示例检查是否存在自定义属性 **key1**。如果设置了 **custom** 属性，则该值将输出到标准错误。如果没有设置自定义属性，则不会执行任何操作。

```
#!/usr/bin/python

import os
import sys

if os.environ.has_key('key1'):
    sys.stderr.write('key1 value was : %s\n' % os.environ['key1'])
else:
    sys.exit(0)
```

A.8. 使用 VDSM HOOKING 模块

VDSM 附带了一个 Python **hooking** 模块，为 VDSM **hook** 脚本提供帮助程序功能。这个模块作为一个示例提供，它只与使用 Python 编写的 VDSM **hook** 相关联。

hooking 模块支持将虚拟机的 **libvirt XML** 读入 **DOM** 对象。然后，**hook** 脚本可以使用 Python 的内置 **xml.dom** 库来操作对象。

然后，可以使用 **hook** 模块将修改后的对象保存到 **libvirt XML**。**hooking** 模块提供以下功能来支持 **hook** 开发：

表 A.2. **hook** 模块功能

Name	参数	Description
------	----	-------------

Name	参数	Description
tobool	字符串	将字符串 "true" 或 "false" 转换为布尔值
read_domxml	-	将虚拟机的 libvirt XML 读入 DOM 对象
write_domxml	DOM 对象	从 DOM 对象写入虚拟机的 libvirt XML

A.9. VDSM HOOK 执行

before_vm_start 脚本可以编辑域 XML，以在到达 libvirt 之前更改虚拟机的 VDSM 定义。在进行操作时必须小心。hook 脚本可能会破坏 VDSM 的运作，而错误脚本可能会导致 Red Hat Virtualization 环境中断。特别是，请确保从未更改域的 UUID，且不会尝试在没有足够背景知识的情况下从域中删除设备。

before_vdsm_start 和 **after_vdsm_stop** hook 脚本都以 root 用户身份运行。需要 root 访问权限的系统的其他 hook 脚本必须编写为使用 **sudo** 命令进行特权升级。要支持此 **/etc/sudoers**，必须更新该 **/etc/sudoers**，以便 **vdsm** 用户无需重新输入密码即可使用 **sudo**。这是必要的，因为 hook 脚本以非交互方式执行。

例 A.4. 为 VDSM hook 配置 sudo

在本示例中，将把 **sudo** 命令配置为允许 **vdsm** 用户以 **root** 身份运行 **/bin/chown** 命令。

1. 以 **root** 用户身份登录虚拟化主机。
2. 在文本编辑器中打开 **/etc/sudoers** 文件。
3. 将此行添加到文件中：

```
vdsm ALL=(ALL) NOPASSWD: /bin/chown
```

这将指定 **vdsm** 用户能够以 **root** 用户身份运行 **/bin/chown** 命令。**NOPASSWD** 参数表示在调用 **sudo** 时不会提示用户输入密码。

完成此配置更改后，VDSM hook 能够使用 **sudo** 命令以 **root** 用户身份运行 **/bin/chown**。此

Python 代码使用 `sudo` 在文件 `/my_file` 上以 `root` 身份执行 `/bin/chown`。

```
retcode = subprocess.call( ["/usr/bin/sudo", "/bin/chown", "root", "/my_file"] )
```

在 VDSM 的日志中收集了 `hook` 脚本的标准错误流。此信息用于调试 `hook` 脚本。

A.10. VDSM HOOK 返回代码

`hook` 脚本必须返回 [hook 返回代码中的其中一个返回代码](#)。返回代码将决定 VDSM 是否处理进一步的 `hook` 脚本。

表 A.3. `hook` 返回代码

代码	Description
0	<code>hook</code> 脚本成功终止
1	<code>hook</code> 脚本失败，应处理其他 <code>hook</code>
2	<code>hook</code> 脚本失败，不应处理任何进一步 <code>hook</code>
>2	保留

A.11. VDSM HOOK 示例

本节中提供的示例 `hook` 脚本严格不受红帽的支持。您必须确保安装到您的系统的任何和所有 `hook` 脚本（无论源如何）都已针对您的环境进行了全面的测试。

例 A.5. NUMA 节点调节

目的：

此 `hook` 脚本允许根据 `numaset` 自定义属性调整 NUMA 主机上的内存分配。如果 `custom` 属性没有设置任何操作。

配置字符串：

```
numaset=^(interleave|strict|preferred):[^\d+(-\d+)?(,[^\d+(-\d+)?]*$
```

使用的正则表达式，允许给定虚拟机的 `numaset` 自定义属性来指定分配模式 (`interleave`, `strict`, `preferred`) 以及使用的节点。这两个值用冒号(:)分隔。正则表达式允许将 `nodeset` 的规格设置为：

- 特定节点(`numaset=strict:1`)指定只使用节点 1，或者
- 使用一系列节点(`numaset=strict:1- 4`)指定节点 1 到 4 的节点，或者
- 未使用特定节点(`numaset=strict:^3`，指定不使用节点 3)或
- 上述任意以逗号分隔的组合(`numaset=strict:1-4,6`，指定要使用的节点为节点 1 到 4 和节点 6)。

script:

```
/usr/libexec/vdsm/hooks/before_vm_start/50_numa
```

```
#!/usr/bin/python

import os
import sys
import hooking
import traceback

"""
numa hook
=====
add numa support for domain xml:

<numatune>
  <memory mode="strict" nodeset="1-4,^3" />
</numatune>

memory=interleave|strict|preferred

numaset="1" (use one NUMA node)
numaset="1-4" (use 1-4 NUMA nodes)
numaset="^3" (don't use NUMA node 3)
numaset="1-4,^3,6" (or combinations)

syntax:
```

```
    numa=strict:1-4
'''
if os.environ.has_key('numa'):
    try:
        mode, nodeset = os.environ['numa'].split(':')

        domxml = hooking.read_domxml()

        domain = domxml.getElementsByTagName('domain')[0]
        numas = domxml.getElementsByTagName('numatune')

        if not len(numas) > 0:
            numatune = domxml.createElement('numatune')
            domain.appendChild(numatune)

            memory = domxml.createElement('memory')
            memory.setAttribute('mode', mode)
            memory.setAttribute('nodeset', nodeset)
            numatune.appendChild(memory)

            hooking.write_domxml(domxml)
        else:
            sys.stderr.write('numa: numa already exists in domain xml')
            sys.exit(2)
    except:
        sys.stderr.write('numa: [unexpected error]: %s\n' % traceback.format_exc())
        sys.exit(2)
```

附录 B. 自定义网络属性

B.1. BRIDGE_OPTS 参数的说明

表 B.1. bridge_opts parameters

参数	Description
forward_delay	设定时间（以秒为单位），网桥将在侦听和学习状态花费。如果此时没有发现切换循环，则网桥将进入转发状态。这将允许时间在正常网络操作前检查网络的流量和布局。
group_addr	要发送常规查询，将此值设置为零。要发送特定于组和特定于组源的查询，请将该值设置为 6 字节 MAC 地址，而不是 IP 地址。允许的值是 01:80:C2:00:00:0x ，但 01:80:C2:00:00:01 、 01:80:80:C2:00:00:02 和 01:80:C2:00:00:03 。
group_fwd_mask	启用网桥转发链接本地组地址。从默认值更改此值将允许非标准桥接行为。
hash_max	散列表中 bucket 的最大数量。这会立即生效，且无法设置为小于当前多播组条目的数量的值。值必须是两个的幂。
hello_time	在发送"hello"消息(nouncing 桥接在网络拓扑中)之间设置时间间隔（以 deciseconds 为单位）。仅在此网桥是 Spanning Tree root 网桥时才应用。
max_age	设置该网桥从另一个 root 网桥接收"hello"消息的最长时间，以减秒，然后再将该网桥视为死机并启动。
multicast_last_member_count	从主机接收 'leave group' 消息后，设置发送到多播组的 'last member' 查询数量。
multicast_last_member_interval	在 'last member' 查询之间设置时间（以 deciseconds）。
multicast_membership_interval	在网桥停止向主机发送多播流量之前，设置以秒为单位的时间将等待来自多播组的成员。

参数	Description
multicast_querier	设置网桥是否主动运行多播伪装。当网桥从另一个网络主机接收"多播主机成员资格"查询时，将根据接收查询的时间（以及多播查询间隔时间）跟踪该主机。如果以后网桥尝试转发该多播成员资格的流量，或者正在与查询多播路由器通信，则计时器会确认不学者的有效性。如果有效，则多播流量通过网桥的现有多播成员资格表进行交付；如果不再有效，流量将通过所有网桥端口发送。通过所有网桥端口发送流量。或预期，多播成员资格应该至少运行一个多播实体来提高性能。
multicast_querier_interval	设置从主机接收的最后"多播主机成员资格"查询之间的最长时间（以秒为单位），以确保其仍然有效。
multicast_query_use_ifaddr	布尔值。默认为 '0'，这样 querier 使用 0.0.0.0 作为 IPv4 消息的源地址。更改此网桥 IP 作为源地址。
multicast_query_interval	在网桥发送的消息之间设置时间（以秒为单位），以确保多播成员资格的有效性。此时，或者要求网桥发送该成员资格的多播查询，网桥会根据请求检查的时间检查其自身多播查询，该状态会基于请求检查的时间加上 multicast_query_interval。如果这个成员资格的多播查询在最后的 multicast_query_interval 中发送，则不会再次发送。
multicast_query_response_interval	在发送后，主机就可以对查询进行响应的长度（以秒为单位）。Must 小于或等于 multicast_query_interval 的值。
multicast_router	允许您启用或禁用端口附加多播路由器。具有一个或多个多播路由器的端口将接收所有多播流量。0 代表完全禁用，1 值可让系统根据查询自动检测路由器是否存在，2 值可让端口始终接收所有多播流量。
multicast_snooping	切换是否启用或禁用 snooping。snooping 可让网桥侦听路由器和主机之间的网络流量，以维护映射将多播流量过滤到适当的链接。此选项允许用户因哈希冲突而自动禁用，但如果哈希冲突没有解决，则不会重新启用 snoop。
multicast_startup_query_count	设置在启动时发送的查询数量，以确定成员资格信息。
multicast_startup_query_interval	设置在启动时发送的查询之间的时间（以秒为单位），以确定成员资格信息。

B.2. 如何设置 RED HAT VIRTUALIZATION MANAGER 以使用 ETHTOOL

您可以从管理门户中为主机网络接口卡配置 `ethtool` 属性。`ethtool_opts` 键默认不可用，需要使用 `engine` 配置工具将其添加到 Manager 中。您还需要在主机上安装所需的 VDSM hook 软件包。

将 `ethtool_opts` Key 添加到 Manager 中

1. 在 Manager 中运行以下命令添加密钥：

```
# engine-config -s UserDefinedNetworkCustomProperties=ethtool_opts=. * --cver=4.4
```

2. 重启 `ovirt-engine` 服务：

```
# systemctl restart ovirt-engine.service
```

3. 在您要配置 `ethtool` 属性的主机上，安装 VDSM hook 软件包。软件包默认在 Red Hat Virtualization 主机上可用，但需要在 Red Hat Enterprise Linux 主机上安装。

```
# dnf install vds-hook-ethtool-options
```

`ethtool_opts` 密钥现在包括在管理门户中。请参阅[编辑主机网络接口和将逻辑网络分配到主机](#)，以将 `ethtool` 属性应用到逻辑网络。

B.3. 如何设置 RED HAT VIRTUALIZATION MANAGER 以使用 FCOE

您可以从管理门户中为主机网络接口卡配置光纤通道(FCoE)属性。`fcoe` 密钥默认不可用，需要使用引擎配置工具将其添加到 Manager 中。您可以运行以下命令来检查是否启用了 `fcoe`：

```
# engine-config -g UserDefinedNetworkCustomProperties
```

您还需要在主机上安装所需的 VDSM hook 软件包。根据主机上的 FCoE 卡，可能需要特殊配置；请参阅 [Red Hat Enterprise Linux 管理存储设备中的以太网配置光纤通道](#)。

流程

1. 在 Manager 中运行以下命令添加密钥：


```
# engine-config -s
UserDefinedNetworkCustomProperties='fcoe=^((enable|dcb|auto_vlan)=(yes|no),?)*$'
```

2.

重启 ovirt-engine 服务：

```
# systemctl restart ovirt-engine.service
```

3.

在您要配置 FCoE 属性的每个 Red Hat Enterprise Linux 主机上安装 VDSM hook 软件包。软件包默认在 Red Hat Virtualization Host (RHVH)上可用。

```
# dnf install vds-hook-fcoe
```

fcoe 键现在包括在管理门户中。请参阅 [编辑主机网络接口和将逻辑网络分配给主机](#)，以将 FCoE 属性应用到逻辑网络。

附录 C. RED HAT VIRTUALIZATION USER INTERFACE PLUGINS

C.1. ABOUT RED HAT VIRTUALIZATION USER INTERFACE PLUG-INS

Red Hat Virtualization 支持提供非标准功能的插件。这样，使用 Red Hat Virtualization 管理门户可以更轻松地与其他系统集成。每个接口插件代表一组用户界面扩展，可以打包并分发到用于 Red Hat Virtualization。

Red Hat Virtualization 的用户界面插件使用 JavaScript 编程语言直接与管理门户集成。插件由管理门户调用，并在 Web 浏览器的 JavaScript 运行时执行。用户界面插件可以使用 JavaScript 语言及其库。

在运行时，管理门户通过代表 Administration-Portal-to-plugin 通信的事件处理程序函数调用各个插件。虽然管理门户支持多个 event-handler 功能，但插件会声明仅对其实施相关的功能。每个插件都必须将相关事件处理程序功能注册为插件 bootstrap 序列的一部分，然后才能供管理门户使用。

为便于插件驱动用户界面扩展的插件到管理员的门户通信，管理门户将插件 API 公开为全局（顶级）插件 JavaScript 对象，单独插件可以使用。每个插件获取了一个单独的 pluginApi 实例，允许每个插件的管理门户控制插件 API-function 调用，并遵循插件的生命周期。

C.2. RED HAT VIRTUALIZATION USER INTERFACE PLUGIN LIFECYCLE

用户界面插件的基本生命周期分为三个阶段：

- 插件发现。
- 插件加载。
- 插件引导。

C.2.1. Red Hat Virtualization User Interface Plug-in Discovery

创建插件描述符是插件发现过程中的第一个步骤。插件描述符包含重要的插件元数据和可选的默认插件特定配置。

作为处理管理门户 HTML 页面请求(HTTP GET)的一部分，用户界面插件基础架构会尝试从本地文件系统发现和加载插件描述符。对于每个插件描述符，基础架构还会尝试加载用于覆盖默认插件配置（若存在）和 `tweak` 插件运行时行为的相应插件用户配置。插件用户配置是可选的。在载入描述符和相应的用户配置文件后，oVirt Engine 会聚合用户界面插件数据，并将其嵌入到管理门户 HTML 页面中以进行运行时评估。

默认情况下，插件描述符位于 `$ENGINE_USR/ui-plug-ins` 中，默认映射 `ENGINE_USR=/usr/share/ovirt-engine`，如 oVirt Engine 本地配置定义。插件描述符预期遵循 JSON 格式规格，但插件描述符除了 JSON 格式规格外，还允许 Java/C++ 风格注释（`/*` 和 `//` varieties）。

默认情况下，插件用户配置文件位于 `$ENGINE_ETC/ui-plug-ins` 中，默认映射 `ENGINE_ETC=/etc/ovirt-engine`（由 oVirt Engine 本地配置定义）。插件用户配置文件应该遵循与插件描述符相同的内容格式规则。



注意

插件用户配置文件通常遵循 `<descriptorFileName>-config.json` 命名规则。

C.2.2. Red Hat Virtualization User Interface Plug-in Loading

在发现插件后，其数据被嵌入到管理门户 HTML 页面中，管理门户会尝试将插件加载为应用程序启动的一部分（除非您将其配置为应用启动的一部分）。

对于已发现的每个插件，管理门户会创建一个 HTML `iframe` 元素，用于加载其主机页面。需要插件主机页面来启动插件 `bootstrap` 过程，该过程(`bootstrap` 过程)用于在插件的 `iframe` 元素的上下文中评估插件代码。用户界面插件基础架构支持本地文件系统上的 `servng` 插件资源文件（如插件主机页面）。插件主机页面加载到 `iframe` 元素中，并评估插件代码。评估了插件代码后，插件通过插件 API 与管理门户通信。

C.2.3. Red Hat Virtualization User Interface Plug-in Bootstrapping

典型的插件 `bootstrap` 序列由以下步骤组成：

插件 Bootstrap 序列

1. 获取给定插件的 `pluginApi` 实例

2. 获取运行时插件配置对象（可选）
3. 注册相关事件处理程序功能
4. 通知 UI 插件基础架构以继续插件初始化

以下代码片段演示了实践中提到的步骤：

```
// Access plug-in API using 'parent' due to this code being evaluated within the context of an
// iframe element.
// As 'parent.pluginApi' is subject to Same-Origin Policy, this will only work when WebAdmin
// HTML page and plug-in
// host page are served from same origin. WebAdmin HTML page and plug-in host page will
// always be on same origin
// when using UI plug-in infrastructure support to serve plug-in resource files.
var api = parent.pluginApi('MyPlugin');

// Runtime configuration object associated with the plug-in (or an empty object).
var config = api.configObject();

// Register event handler function(s) for later invocation by UI plug-in infrastructure.
api.register({
  // Uilnit event handler function.
  Uilnit: function() {
    // Handle Uilnit event.
    window.alert('Favorite music band is ' + config.band);
  }
});

// Notify UI plug-in infrastructure to proceed with plug-in initialization.
api.ready();
```

C.3. 用户界面插件相关的文件和位置

表 C.1. UI 插件相关的文件及其位置

File	位置	备注
插件描述符文件(meta-data)	/usr/share/ovirt-engine/ui-plugins/my-plugin.json	
插件用户配置文件	/etc/ovirt-engine/ui-plugins/my-plugin-config.json	

File	位置	备注
插件资源文件	/usr/share/ovirt-engine/ui-plugins/<resourcePath>/PluginHostPage.html	<resourcePath > 由插件描述符中的对应属性定义。

C.4. 用户界面插件部署示例

按照这些说明，在登录 Red Hat Virtualization Manager 管理门户时，创建运行 Hello World! 程序的用户界面插件。

部署 Hello World! 插件

1. 通过在位于 /usr/share/ovirt-engine/ui-plugins/helloWorld.json 的 Manager 中创建以下文件来创建插件描述符：

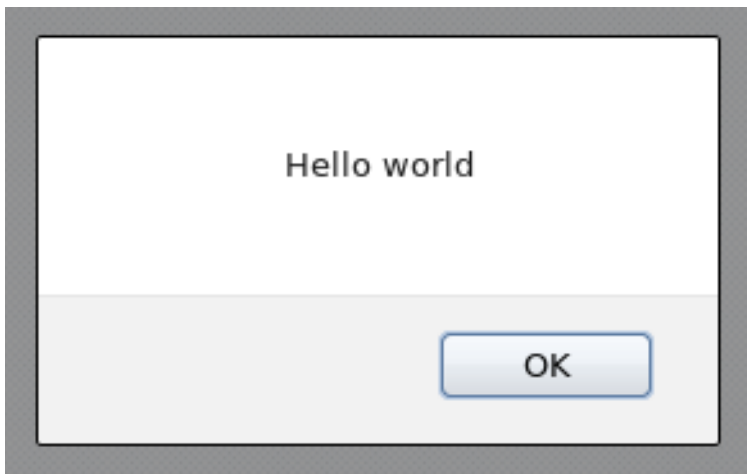
```
{
  "name": "HelloWorld",
  "url": "/ovirt-engine/webadmin/plugin/HelloWorld/start.html",
  "resourcePath": "hello-files"
}
```

2. 通过在位于 /usr/share/ovirt-engine/ui-plugins/hello-files/start.html 的 Manager 中创建以下文件来创建插件主机页面：

```
<!DOCTYPE html><html><head>
<script>
  var api = parent.pluginApi('HelloWorld');
  api.register({
    Uilnit: function() { window.alert('Hello world'); }
  });
  api.ready();
</script>
</head><body></body></html>
```

如果您成功实施 Hello World! 插件，当您登录管理门户时，您将看到此屏幕：

图 C.1. Hello World!的成功实施.插件



附录 D. 在 RED HAT VIRTUALIZATION 中启用 FIPS

您可以将 Red Hat Virtualization 设置为与联邦信息处理标准(FIPS)兼容，特别是 FIPS 140-2。您可以根据机构的 FIPS 合规性要求，选择在特定虚拟机、裸机或整个环境中启用 FIPS 模式。

您可以通过以 FIPS 模式安装操作系统，或者在安装操作系统后将系统切换到 FIPS 模式，在 RHV 4.4 中创建启用了 FIPS 的裸机机器。但是，您必须在安装和配置 Red Hat Virtualization 前切换到 FIPS 模式，以避免引入系统冲突。



重要

红帽建议使用启用了 FIPS 模式安装 RHEL 8，而不是在以后启用 FIPS 模式。在安装过程中启用 FIPS 模式可确保系统使用 FIPS 批准的算法生成所有的密钥，并持续监控测试。

您首先在裸机机器上启用 FIPS，然后在 Manager 中启用。

- [在自托管引擎中启用 FIPS](#)
- [在 RHEL 主机和独立管理器中启用 FIPS](#)

D.1. 在自托管引擎中启用 FIPS

使用命令行时，您可以在部署期间启用 FIPS。

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 Do you want to enable FIPS? 时，输入 Yes

验证

在主机上输入 `fips-mode-setup --check` 命令，验证是否已启用 FIPS。该命令应该返回 FIPS 模式：

```
# fips-mode-setup --check  
FIPS mode is enabled.
```

D.2. 在 RHV 主机和独立管理器中启用 FIPS

您可在安装 Red Hat Enterprise Linux (RHEL) 主机或 Red Hat Virtualization Host (RHVH) 时启用 FIPS 模式。详情请参阅 Red Hat Enterprise Linux 8 的 *Security hardening* 指南中的[安装启用了 FIPS 模式的 RHEL 8 系统](#)。红帽不支持将置备的主机或 Manager 机器切换到 FIPS 模式

验证

在主机上输入 `fips-mode-setup --check` 命令，验证是否已启用 FIPS。该命令应该返回 FIPS 模式：

```
# fips-mode-setup --check  
FIPS mode is enabled.
```

D.3. 其他资源

- [安装 Red Hat Virtualization 主机](#)
- [在安装过程中配置和应用 SCAP 策略](#)
- [Red Hat Virtualization Manager 的安装程序和镜像 \(v.4.4 for x86_64\)](#)
- [SCAP 安全指南中提供的安全策略](#)
- [Red Hat Enterprise Linux 8 的安全强化](#)

附录 E. RED HAT VIRTUALIZATION 和加密通信

E.1. 替换 RED HAT VIRTUALIZATION MANAGER CA 证书

您可以配置机构的第三方 CA 证书，以通过 HTTPS 对连接到 Red Hat Virtualization Manager 的用户进行身份验证。

第三方 CA 证书不用于 Manager 和主机 [或磁盘传输 URL 进行验证](#)。这些 HTTPS 连接使用 Manager 生成的自签名证书。

**重要**

当您切换到自定义 HTTPS 证书时，必须使用自己的 CA 证书分发来在客户端上提供该证书。

如果您要与 Red Hat Satellite 集成，则需要手动将正确的证书导入到 Satellite 中。

如果您在 P12 文件中从 CA 收到私钥和证书，请使用以下步骤提取它们。如需其他文件格式，请联系您的 CA。提取私钥和证书后，继续 [替换 Red Hat Virtualization Manager Apache CA 证书](#)。

E.1.1. 从 P12 捆绑包中提取证书和私钥

内部 CA 将内部生成的密钥和证书存储在一个 P12 文件中（`/etc/pki/ovirt-engine/keys/apache.p12`）。将新文件存储在上一位置。以下步骤假定新的 P12 文件位于 `/tmp/apache.p12` 中。

**警告**

不要更改 `/etc/pki` 目录或任何子目录的权限和所有权。`/etc/pki` 和 `/etc/pki/ovirt-engine` 目录的权限必须保留为默认值 `755`。

流程

1.

备份当前 `apache.p12` 文件：

```
# cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12.bck
```

2.

将当前文件替换为新文件：

```
# cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

3.

将私钥和证书提取到所需位置：

```
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nocerts -nodes > /tmp/apache.key
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys > /tmp/apache.cer
```

如果文件受密码保护，请在命令中添加 `-passin pass:password`，用 *所需的密码* 替换 `password`。



重要

对于新的 Red Hat Virtualization 安装，您必须完成此流程中的所有步骤。

E.1.2. 替换 Red Hat Virtualization Manager Apache CA 证书

您可以配置您组织的第三方 CA 证书，以通过 HTTPS 对连接到管理门户和虚拟机门户的验证身份。



警告

不要更改 `/etc/pki` 目录或任何子目录的权限和所有权。`/etc/pki` 和 `/etc/pki/ovirt-engine` 目录的权限必须保留为默认值 `755`。

前提条件

-

第三方 CA（证书授权）证书。它作为 PEM 文件提供。证书链必须完成为 root 证书。链的顺序非常重要，且必须是从最后的中间证书到 root 证书。此流程假定 `/tmp/3rd-party-ca-`

cert.pem 中提供第三方 CA 证书。

- 要用于 Apache httpd 的私钥。它不能有密码。此流程假定它位于 /tmp/apache.key 中。
- CA 发布的证书。此流程假定它位于 /tmp/apache.cer 中。

流程

1. 如果您使用自托管引擎，请将环境设置为全局维护模式。

```
# hosted-engine --set-maintenance --mode=global
```

如需更多信息，请参阅 [维护自托管引擎](#)。

2. 将 CA 证书添加到主机范围内的信任存储中：

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ca-trust/source/anchors
# update-ca-trust
```

3. 管理器已配置为使用 /etc/pki/ovirt-engine/apache-ca.pem，它符号链接到 /etc/pki/ovirt-engine/ca.pem。删除符号链接：

```
# rm /etc/pki/ovirt-engine/apache-ca.pem
```

4. 将您的 CA 证书保存为 /etc/pki/ovirt-engine/apache-ca.pem：

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ovirt-engine/apache-ca.pem
```

5. 备份现有的私钥和证书：

```
# cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-engine/keys/apache.key.nopass.bck
# cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
```

6. 将私钥复制到所需位置：

```
# cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

7.

将私钥所有者设置为 **root**，并将权限设置为 **0640**：

```
# chown root:ovirt /etc/pki/ovirt-engine/keys/apache.key.nopass
# chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

8.

将证书复制到所需位置：

```
# cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

9.

将证书所有者设置为 **root**，并将权限设置为 **0644**：

```
# chown root:ovirt /etc/pki/ovirt-engine/certs/apache.cer
# chmod 644 /etc/pki/ovirt-engine/certs/apache.cer
```

10.

重启 **Apache** 服务器：

```
# systemctl restart httpd.service
```

11.

使用以下参数，创建一个新的信任存储配置文件 `/etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf`：

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

12.

复制 `/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf` 文件，并使用大于 10 的索引号进行重命名（如 `99-setup.conf`）。在新文件中添加以下参数：

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

13.

重启 **websocket-proxy** 服务：

```
# systemctl restart ovirt-websocket-proxy.service
```

14.

如果您手动更改了 `/etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf` 文件，或使用较旧的安装中的配置文件，请确保管理器仍然配置为使用 `/etc/pki/ovirt-`

`engine/apache-ca.pem` 作为证书源。

15.

创建 `/etc/ovirt-engine-backup/engine-backup-config.d` 目录：

```
# mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d
```

16.

使用以下内容创建 `/etc/ovirt-engine-backup/engine-backup-config.d/update-system-wide-pki.sh` 文件：这将启用 `ovirt-engine-backup` 以在恢复时自动更新系统。

```
BACKUP_PATHS="${BACKUP_PATHS}
/etc/ovirt-engine-backup"
cp -f /etc/pki/ovirt-engine/apache-ca.pem \
/etc/pki/ca-trust/source/anchors/3rd-party-ca-cert.pem
update-ca-trust
```

17.

重启 `ovirt-provider-ovn` 服务：

```
# systemctl restart ovirt-provider-ovn.service
```

18.

重启 `ovirt-imageio` 服务：

```
# systemctl restart ovirt-imageio.service
```

19.

重启 `ovirt-engine` 服务：

```
# systemctl restart ovirt-engine.service
```

20.

如果您使用自托管引擎，请关闭全局维护模式：

```
# hosted-engine --set-maintenance --mode=none
```

现在，您可以在不看到证书警告的情况下连接到管理门户和虚拟机门户。

E.2. 在 MANAGER 和 LDAP 服务器间设置加密通信

要设置 Red Hat Virtualization Manager 和 LDAP 服务器之间的加密通信，获取 LDAP 服务器的 root CA 证书，将 root CA 证书复制到 Manager，并创建 PEM 编码的 CA 证书。密钥存储类型可以是任何支

持 Java 的类型。以下流程使用 Java KeyStore (JKS)格式。



注意

有关创建 PEM 编码的 CA 证书并导入证书的更多信息，请参阅 README 文件（位于 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-<version>`）的 X.509 CERTIFICATE TRUST STORE 部分。



注意

`ovirt-engine-extension-aaa-ldap` 已被弃用。对于新安装，请使用 Red Hat Single Sign On。如需更多信息，请参阅《管理指南》中的 [安装和配置 Red Hat Single Sign On](#)。

流程

1.

在 Red Hat Virtualization Manager 中，将 LDAP 服务器的 root CA 证书复制到 `/tmp` 目录中，并使用 `keytool` 创建 PEM 编码的 CA 证书导入 root CA 证书。以下命令在 `/tmp/myrootca.pem` 中导入 root CA 证书，并在 `/etc/ovirt-engine/aaa/` 下创建一个 PEM 编码的 CA 证书 `myrootca.jks`。记下证书的位置和密码。如果您使用交互式设置工具，则这是您需要的所有信息。如果要手动配置 LDAP 服务器，请按照其余步骤更新配置文件。

```
$ keytool -importcert -noprompt -trustcacerts -alias myrootca -file /tmp/myrootca.pem
-keystore /etc/ovirt-engine/aaa/myrootca.jks -storepass password
```

2.

使用证书信息更新 `/etc/ovirt-engine/aaa/profile1.properties` 文件：



注意

`${local:_basedir}` 是 LDAP 属性配置文件所在的目录，并指向 `/etc/ovirt-engine/aaa` 目录。如果您在不同的目录中创建 PEM 编码的 CA 证书，请使用证书的完整路径替换 `${local:_basedir}`。

•

使用 startTLS（推荐）：

```
# Create keystore, import certificate chain and uncomment
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
pool.default.ssl.truststore.password = password
```

- 使用 SSL :

```
# Create keystore, import certificate chain and uncomment
pool.default.serverset.single.port = 636
pool.default.ssl.enable = true
pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
pool.default.ssl.truststore.password = password
```

要继续配置外部 LDAP 供应商，请参阅[配置外部 LDAP 提供程序](#)。要继续为单点登录配置 LDAP 和 Kerberos，请参阅[为单点登录配置 LDAP 和 Kerberos](#)。

E.3. 为 FIPS 启用加密的 VNC 控制台

您可以将加密的 VNC 控制台设置为与启用了 FIPS 的 Red Hat Virtualization (RHV) 管理器和主机一起使用。

要设置加密的 VNC 控制台，您可以完成以下步骤：

- 在 [RHV 中启用 FIPS](#)。
- [配置集群以启用 VNC 加密](#)。
- 在每个主机上运行 [VNC SASL ansible playbook](#)。
- [配置远程查看器以信任 Manager 的 CA 证书](#)。

E.3.1. 配置集群以启用 VNC 加密

前提条件

- 集群中必须启用 FIPS。

流程

1. 在管理门户中，点 **Compute** → **Clusters**。
2. 选择您要启用 VNC 加密的集群并点 **Edit**。这会打开 **Edit Cluster** 窗口。
3. 选择 **Console** 选项卡。
4. 选择 **Enable VNC Encryption**，点 **OK**。

E.3.2. 为每个主机运行 VNC SASL Ansible playbook

流程

1. 在管理门户中，将启用了 **FIPS** 的主机置于维护模式：
 - a. 单击 **Compute** → **Hosts**。
 - b. 在 **Virtual Machines** 列中，验证每个主机都有零个虚拟机。

如果需要，执行实时迁移以从主机中删除虚拟机。请参阅 [主机之间迁移虚拟机](#)。
 - c. 选择每个主机，再单击 **Management** → **Maintenance** 和 **OK**。
2. 连接到运行 **Manager** 的机器的命令行。
 - 独立管理器：

```
# ssh root@rhvm
```
 - 自托管引擎：单击 **Compute** → **Virtual Machines** 以选择自托管引擎虚拟机（默认名为 **HostedEngine**），然后单击 **Console**。

3. 为每个主机运行 VNC SASL Ansible playbook:

```
# cd /usr/share/ovirt-engine/ansible-runner-service-project/project/
# ansible-playbook --ask-pass --inventory=<hostname> ovirt-vnc-sasl.yml <1>
```

指定 **Compute** → **Hosts** 上显示的主机名。

4. 选择主机并点 **Installation** → **Reinstall**。
5. 重新安装后，选择主机并点 **Management** → **Restart**。
6. 重新引导后，选择主机，再单击 **Management** → **Activate**。

VNC SASL Ansible playbook 错误消息

在运行 VNC SASL Ansible playbook 时，该任务可能会失败并显示以下错误消息：

```
Using a SSH password instead of a key is not possible because Host Key checking is enabled
and sshpass does not support this. Please add this host's fingerprint to your known_hosts
file to manage this host.
```

要解决这个问题，请通过以下操作之一禁用主机密钥检查：

- 通过取消注释 `/etc/ansible/ansible.cfg` 中的以下行来永久检查主机密钥：

```
#host_key_checking = False
```

- 运行以下命令，临时禁用主机密钥检查：

```
export ANSIBLE_HOST_KEY_CHECKING=False
```

其他资源

- [在安装过程中配置和应用 SCAP 策略](#)

Red Hat Virtualization Manager 的安装程序和镜像 (v.4.3 for x86_64)

E.3.3. 配置远程查看器以信任 Manager 的 CA 证书

在客户端机器 `virt-viewer` 或 `remote-viewer` 上配置 Remote Viewer 控制台，以信任 RHV Manager 的证书颁发机构(CA)

流程

1. 导航到 `https://<engine_address>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`。
2. 启用所有信任设置。
3. 在您要运行 VNC 控制台的客户端机器中，为证书文件创建一个目录：

```
$ mkdir ~/.pki/CA
```



警告

如果此步骤生成错误，例如 `mkdir: 无法创建目录 '/home/example_user/.pki/CA': File exists`，则采取 precautions 来避免在下一步中覆盖 `~/.pki/CA/cacert.pem`。例如，在文件名中包含当前的日期。

4. 下载证书：

```
$ curl -k -o ~/.pki/CA/cacert-<today's date>.pem 'https://<engine_address>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA'
```

5. 在浏览器中安装证书颁发机构：

- [Firefox](#)
- [Internet Explorer](#)
- [Google Chrome.](#)

6. 在客户端机器上安装 SASL SCRAM 库：

```
$ sudo dnf install cyrus-sasl-scram
```

验证步骤

1. 在您创建的一台启用了 **FIPS** 的主机上运行虚拟机。
2. 使用 VNC 控制台连接至虚拟机。

其他资源

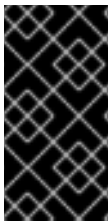
- [安装控制台组件](#)
- [替换 Manager CA 证书](#)

附录 F. 代理

F.1. SPICE 代理

F.1.1. SPICE 代理概述

当 SPICE 客户端位于连接管理程序的网络之外，SPICE 代理是用于将 SPICE 客户端连接到虚拟机的工具。设置 SPICE 代理包括在机器上安装 Squid 并配置防火墙以允许代理流量。在上打开 SPICE 代理包括使用 engine-config（管理器上使用 engine-config）组成，将主要 SpiceProxyDefault 设置为包含代理的名称和端口的值。关闭 SPICE 代理包括使用 Manager 上的 engine-config 来移除设置关键 SpiceProxyDefault 的值。



重要

SPICE 代理只能与独立 SPICE 客户端结合使用，且不能用于使用 noVNC 连接到虚拟机。

F.1.2. SPICE 代理机器设置

此流程解释了如何将机器设置为 SPICE 代理。通过 SPICE 代理，可以从网络外部连接到 Red Hat Virtualization 网络。我们在此过程中使用 Squid 提供代理服务。

流程

1. 在 Proxy 机器上安装 Squid：

```
# dnf install squid
```

2. 打开 /etc/squid/squid.conf。更改：

```
http_access deny CONNECT !SSL_ports
```

改为：

```
http_access deny CONNECT !Safe_ports
```

3. 启动 squid 服务并使其在重启后自动运行：

■

```
# systemctl enable squid.service --now
```

4. 在默认 `firewalld` 区中启用对 `squid` 服务的传入请求：

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

5. 在运行时配置中保留此防火墙规则：

```
# firewall-cmd --reload
```

6. 确认 `squid` 服务出现在防火墙服务列表中：

```
# firewall-cmd --list-services  
ssh dhcpv6-client squid
```

您现在已将机器设置为 **SPICE** 代理。从网络外部连接到 Red Hat Virtualization 网络前，请激活 **SPICE** 代理。

F.1.3. 开启 SPICE 代理

此流程解释了如何激活（或打开）**SPICE** 代理。

流程

1. 在 `Manager` 中，使用 `engine-config` 工具设置代理：

```
# engine-config -s SpiceProxyDefault=someProxy
```

2. 重启 `ovirt-engine` 服务：

```
# systemctl restart ovirt-engine.service
```

代理必须具有以下形式：

```
protocol://[host]:[port]
```



注意

只有 Red Hat Enterprise Linux 6.7、Red Hat Enterprise Linux 7.2 或更高版本附带的 SPICE 客户端支持 HTTPS 代理。较早的客户端只支持 HTTP。如果为以前的客户端指定了 HTTPS，客户端将忽略代理设置，并尝试与主机的直接连接。

SPICE 代理现已激活（打开）。现在，可以通过 SPICE 代理连接到 Red Hat Virtualization 网络。

F.1.4. 关闭 SPICE 代理

此流程解释了如何关闭（激活） SPICE 代理。

流程

1.

登录到 Manager:

```
$ ssh root@[IP of Manager]
```

2.

运行以下命令以清除 SPICE 代理：

```
# engine-config -s SpiceProxyDefault=""
```

3.

重启 Manager:

```
# systemctl restart ovirt-engine.service
```

SPICE 代理现已被取消激活（关闭）。无法通过 SPICE 代理连接到 Red Hat Virtualization 网络。

F.2. SQUID PROXY

F.2.1. 安装和配置 Squid 代理

这部分论述了如何在虚拟机门户中安装和配置 Squid 代理。Squid 代理服务器用作内容加速器。它缓存经常查看的内容，减少了带宽并改进响应时间。

流程

1.

获取 Squid 代理服务器的 HTTPS 端口的密钥对和证书。您可以像获取另一个 SSL/TLS 服务的密钥对一样获得此密钥对。密钥对采用两个 PEM 文件的形式，其中包含私钥和签名证书。对于这个步骤，我们假定它们名为 `proxy.key` 和 `proxy.cer`。



注意

密钥对和证书也可以使用引擎的证书颁发机构生成。如果您已有代理的私钥和证书，并且不想使用引擎证书颁发机构生成它，请跳至下一步。

2.

为代理选择主机名。然后，选择代理的可识别证书名称的其他组件。



注意

最好使用由引擎本身使用的相同国家和相同的组织名称。登录到安装 Manager 并运行以下命令的机器，查找此信息：

```
openssl x509 -in /etc/pki/ovirt-engine/ca.pem -noout -text | grep DirName
```

这个命令输出如下：

```
subject= /C=US/O=Example Inc./CN=engine.example.com.81108
```

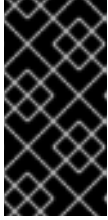
此处的相关部分为 `/C=US/O=Example Inc.`。使用它来为代理构建证书的完整可分辨名称：

```
/C=US/O=Example Inc./CN=proxy.example.com
```

3.

登录到代理机器并生成证书签名请求：

```
# openssl req -newkey rsa:2048 -subj '/C=US/O=Example Inc./CN=proxy.example.com' -nodes -keyout proxy.key -out proxy.req
```



重要

您必须包括与证书可分辨名称相关的引号。-nodes 选项确保私钥没有加密，这意味着您不需要输入密码才能启动代理服务器。

该命令生成两个文件：`proxy.key` 和 `proxy.req`。`proxy.key` 是私钥。使此文件保持安全。`proxy.req` 是证书签名请求。`proxy.req` 不需要任何特殊保护。

4.

要生成签名证书，请将代理机器中的证书签名请求文件复制到 Manager 机器：

```
# scp proxy.req engine.example.com:/etc/pki/ovirt-engine/requests/.
```

5.

登录到 Manager 机器并签署证书：

```
# /usr/share/ovirt-engine/bin/pki-enroll-request.sh --name=proxy --days=3650 --subject='/C=US/O=Example Inc./CN=proxy.example.com'
```

这为证书签名，并使其有效期为 10 年(3650 天)。如果您愿意，将证书设置为更早过期。

6.

生成的证书文件位于 `/etc/pki/ovirt-engine/certs` 目录，并且应命名为 `proxy.cer`。在代理机器中，将此文件从 Manager 机器复制到您的当前目录中：

```
# scp engine.example.com:/etc/pki/ovirt-engine/certs/proxy.cer .
```

7.

确保代理机器上存在 `proxy.key` 和 `proxy.cer`：

```
# ls -l proxy.key proxy.cer
```

8.

在代理机器上安装 Squid 代理服务器软件包：

```
# dnf install squid
```

9.

将私钥和签名证书移到代理可以访问它们的位置，例如：

```
# cp proxy.key proxy.cer /etc/squid/.
```


10. 设置权限，以便 **squid** 用户可以读取这些文件：

```
# chgrp squid /etc/squid/proxy.*
# chmod 640 /etc/squid/proxy.*
```

11. **Squid** 代理必须验证引擎使用的证书。将 **Manager** 证书复制到代理机器中。这个示例使用文件路径 `/etc/squid`：

```
# scp engine.example.com:/etc/pki/ovirt-engine/ca.pem /etc/squid/.
```



注意

默认 **CA** 证书位于 **Manager** 机器的 `/etc/pki/ovirt-engine/ca.pem` 中。

12. 设置权限，以便 **squid** 用户可以读取证书文件：

```
# chgrp squid /etc/squid/ca.pem
# chmod 640 /etc/squid/ca.pem
```

13. 如果 **SELinux** 处于 **enforcing** 模式，使用 **semanage** 工具将端口 **443** 上下文更改为允许 **Squid** 使用端口 **443**：

```
# dnf install polycycoreutils-python
# semanage port -m -p tcp -t http_cache_port_t 443
```

14. 使用以下内容替换现有的 **Squid** 配置文件：

```
https_port 443 key=/etc/squid/proxy.key cert=/etc/squid/proxy.cer ssl-bump
defaultsite=engine.example.com
cache_peer engine.example.com parent 443 0 no-query originserver ssl
sslcafile=/etc/squid/ca.pem name=engine login=PASSTHRU
cache_peer_access engine allow all
ssl_bump allow all
http_access allow all
```

15. 重启 **Squid** 代理服务器：

```
# systemctl restart squid.service
```



注意

默认配置中的 **Squid Proxy** 会在 15 idle 分钟后终止其连接。要在 **Squid** 代理终止闲置连接前增加时间量，请调整 `squid.conf` 中的 `read_timeout` 选项（用于实例 `read_timeout 10` 小时）。

F.3. WEBSOCKET 代理

F.3.1. Websocket 代理概述

websocket 代理允许用户通过 **noVNC** 控制台连接到虚拟机。

可在 **Red Hat Virtualization Manager** 机器上安装和配置 **websocket** 代理（请参阅 [配置 Red Hat Virtualization Manager](#)）。

附录 G. BRANDING

G.1. BRANDING

G.1.1. 重新添加管理器

可以自定义 Red Hat Virtualization Manager 的各个方面，如弹出窗口中显示的图标以及欢迎页面上显示的链接。这样，您可以重新控制 Manager 并让您能够精细地控制最终用户的外观和感觉。

自定义管理器所需的文件位于安装 Manager 的系统上的 `/etc/ovirt-engine/branding/` 目录中。文件含有一组级联式风格表文件，这些文件用于样式化图形用户界面的各个方面，以及一组属性文件，其中包含在 Manager 的各个组件中的消息和链接。

要自定义组件，请编辑该组件的文件并保存更改。下次打开或刷新该组件时，会应用更改。

G.1.2. 登录屏幕

登录屏幕是管理门户和虚拟机门户使用的登录屏幕。可以自定义的登录屏幕的元素如下：

- 边栏
- 左侧的标头镜像
- 右侧的标头镜像
- 标头文本

登录屏幕的类位于 `common.css` 中。

G.1.3. 管理门户屏幕

管理门户屏幕是您登录管理门户时显示的主要屏幕。自定义的管理门户页面的元素如下：

- 徽标
- 左后台镜像
- 数据中心背景镜像
- 正确的背景镜像
- 徽标右侧的文本

管理门户屏幕的类位于 `web_admin.css` 中。

G.1.4. 虚拟机门户屏幕

虚拟机门户屏幕是您登录虚拟机门户时显示的屏幕。可自定义的虚拟机门户屏幕的元素如下：

- 徽标
- 数据中心背景镜像
- 正确的背景镜像
- 主要网格的边框
- `Logged in user` 标签上方的文本

虚拟机门户屏幕的类位于 `user_portal.css` 中。

G.1.5. 弹出 Windows

弹出窗口是 **Manager** 中的所有窗口，允许您创建、编辑或更新主机或虚拟机等实体。可以自定义的弹出窗口的元素如下：

- 边栏
- 左侧的标头镜像
- 标题中心镜像(repeated)

弹出窗口的类位于 **common.css** 中。

G.1.6. 标签页

管理门户中的很多弹出窗口包含选项卡。您可以自定义这些标签页的元素如下：

- **Active**
- **inactive**

选项卡的类位于 **common.css** 和 **user_portal.css** 中。

G.1.7. Welcome Page

在访问 **Manager** 的主页时，欢迎页面是初始显示的页面。除了自定义总体外观和感觉外，您还可以通过编辑模板文件，在页面中添加指向页面的链接。可以自定义的 **Welcome Page** 的元素如下：

- 页面标题
- 标题（左、中心和右）

- 错误消息
- 在该链接中转发及相关消息的链接
- 添加消息横幅或前言

Welcome Page 的类位于 `welcome_style.css` 中。

Template 文件

Welcome Page 的模板文件是名称 `welcome_page.template` 的常规 HTML 文件，它不包含 HTML、HEAD 或 BODY 标签。此文件直接插入到 Welcome Page 本身中，并充当 Welcome Page 中显示的内容的容器。因此，您必须编辑此文件来添加新链接或更改内容本身。模板文件的另一项功能是，它在处理 Welcome Page 时，其中包含了 `{user_portal}` 所替换为 `消息.properties` 文件中的相应文本所替换的占位符文本。

Preamble

您可以通过在 Welcome Page 中添加自定义消息横幅，添加包含横幅文本的 `preamble.template` 和 `a preamble.css` 文件，并在 `branding.properties` 文件中链接它们。示例文件位于 [示例预言模板](#)。



注意

在引擎升级中，自定义消息横幅仍保留下来，并不会出现问题。在引擎恢复过程中，以下引擎备份和恢复需要手动恢复和验证自定义消息标题。

G.1.8. 页面未找到页面

当您打开指向一个页面的链接时，页面 **Not Found** 页会显示一个页面，该页面无法在 Red Hat Virtualization Manager 中找到。可以自定义页面 **Not Found** 页的元素如下：

- 页面标题

- 标题（左、中心和右）
- 错误消息
- 在该链接中转发及相关消息的链接

Page Not Found 页面的类位于 `welcome_style.css` 中。

附录 H. 系统帐户

H.1. RED HAT VIRTUALIZATION MANAGER USER ACCOUNTS

创建多个系统用户帐户以便在安装 `rhev` 软件包时支持 Red Hat Virtualization。每个系统用户都有默认用户标识符(UID)。创建的系统用户帐户有：

- `vdsm` 用户(UID 36)。需要支持挂载和访问 NFS 存储域的工具。
- `ovirt` 用户(UID 108)。ovirt-engine 红帽 JBoss 企业应用平台实例的所有者。
- `ovirt-vmconsole` 用户(UID 498)。客户端串口控制台需要。

H.2. RED HAT VIRTUALIZATION MANAGER GROUPS

创建多个系统用户组以便在安装 `rhev` 软件包时支持 Red Hat Virtualization。每个系统用户组都有默认的组标识符(GID)。创建的系统用户组有：

- `kvm` 组(GID 36)。组成员包括：
 - `vdsm` 用户。
- `ovirt` 组(GID 108)。组成员包括：
 - `ovirt` 用户。
- `ovirt-vmconsole` 组(GID 498)。组成员包括：
 - `ovirt-vmconsole` 用户。

H.3. 虚拟化主机用户帐户

安装 `vdsmd` 和 `qemu-kvm-rhev` 软件包时，会在虚拟化主机上创建很多系统用户帐户。每个系统用户都有默认用户标识符(UID)。创建的系统用户帐户有：

- `vdsmd` 用户(UID 36)。
- `qemu` 用户(UID 107)。
- `sanlock` 用户(UID 179)。
- `ovirt-vmconsole` 用户(UID 498)。



重要

分配的用户标识符(UID)和组群标识符(GID)可能因系统而异。`vdsmd` 用户已固定到 UID 36, `kvm` 组被固定到 GID 36。

如果系统上的另外一个账户已使用了 UID 36 或 GID 36, 在安装 `vdsmd` 和 `qemu-kvm-rhev` 软件包时会引发冲突。

H.4. 虚拟化主机组

安装 `vdsmd` 和 `qemu-kvm-rhev` 软件包时，会在虚拟化主机上创建多个系统用户组。每个系统用户组都有默认的组标识符(GID)。创建的系统用户组有：

- `kvm` 组(GID 36)。组成员包括：
- `qemu` 用户。
- `sanlock` 用户。
- `qemu` 组(GID 107)。组成员包括：

- **vdsm 用户。**
- **sanlock 用户。**
- **ovirt-vmconsole 组(GID 498)。组成员包括：**
- **ovirt-vmconsole 用户。**



重要

分配的用户标识符(UID)和组群标识符(GID)可能因系统而异。**vdsm 用户已固定到 UID 36, kvm 组被固定到 GID 36。**

如果系统上的另外一个账户已使用了 **UID 36 或 GID 36**, 在安装 **vdsm 和 qemu-kvm-rhev** 软件包时会引发冲突。

附录 I. 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。