



Red Hat Virtualization 4.3

管理指南

Red Hat Virtualization 中的管理任务

Red Hat Virtualization 4.3 管理指南

Red Hat Virtualization 中的管理任务

Enter your first name here. Enter your surname here.

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

Enter your email address here.

法律通告

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Administration_Guide.ent file |.

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

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

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

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

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

Linux[®] 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

部分 I. 管理和维护 RED HAT VIRTUALIZATION	14
第 1 章 全局配置	15
1.1. 角色	15
1.1.1. 创建新角色	15
1.1.2. 编辑或复制角色	15
1.1.3. 用户角色和授权示例	16
1.2. 系统权限	17
1.2.1. 用户属性	18
1.2.2. 用户和管理员角色	18
1.2.3. 用户角色介绍	19
1.2.4. 管理员角色已说明	20
1.2.5. 将管理员或用户角色分配给资源	21
1.2.6. 从资源中删除管理员或用户角色	21
1.2.7. 管理系统权限	22
1.2.8. 数据中心管理员角色说明	22
1.2.9. 管理系统权限	23
1.2.10. 集群管理员角色已说明	23
1.2.11. 管理系统权限	24
1.2.12. 网络管理员和用户角色说明	24
1.2.13. 管理系统权限	25
1.2.14. 主机管理员角色已说明	25
1.2.15. 为存储域管理系统权限	25
1.2.16. 存储管理员角色已说明	26
1.2.17. 为虚拟机池管理系统权限	26
1.2.18. 虚拟机池管理员角色说明	27
1.2.19. 为虚拟磁盘管理系统权限	27
1.2.20. 虚拟磁盘用户角色已说明	27
1.2.21. 设置传统 SPICE 密码	28
1.3. 调度策略	28
1.3.1. 创建调度策略	30
1.3.2. 新调度策略和编辑调度策略窗口中的设置说明	30
1.4. 实例类型	34
1.4.1. 创建实例类型	34
1.4.2. 编辑实例类型	35
1.4.3. 删除实例类型	35
1.5. MAC 地址池	35
1.5.1. 创建 MAC 地址池	36
1.5.2. 编辑 MAC 地址池	36
1.5.3. 编辑 MAC 地址池权限	37
1.5.4. 删除 MAC 地址池	37
第 2 章 DASHBOARD	39
2.1. 先决条件	39
2.2. 全局清单	39
2.3. 全局利用率	41
2.3.1. top Utilized Resources	41
2.4. CLUSTER UTILIZATION	42
2.4.1. CPU	42
2.4.2. 内存	42
2.5. STORAGE UTILIZATION	42

第 3 章 搜索	44
3.1. 在 RED HAT VIRTUALIZATION 中执行搜索	44
3.2. 搜索语法和示例	44
3.3. 搜索 AUTO-COMPLETION	44
3.4. 搜索结果类型选项	45
3.5. 搜索标准	45
3.6. 搜索：多个标准和通配符	46
3.7. 搜索：确定搜索顺序	47
3.8. 搜索数据中心	47
3.9. 搜索集群	47
3.10. 搜索主机	48
3.11. 搜索网络	50
3.12. 搜索存储	50
3.13. 搜索磁盘	51
3.14. 搜索卷	53
3.15. 搜索虚拟机	53
3.16. 搜索池	55
3.17. 搜索模板	56
3.18. 搜索用户	57
3.19. 搜索事件	58
第 4 章 书签	60
4.1. 将查询字符串保存为书签	60
4.2. 编辑书签	60
4.3. 删除书签	60
第 5 章 TAGS	61
5.1. 使用标签来自定义 RED HAT VIRTUALIZATION	61
5.2. 创建标签	61
5.3. 修改标签	61
5.4. 删除标签	61
5.5. 为对象添加和删除标签	62
5.6. 使用标签搜索对象	62
5.7. 使用标签自定义主机	62
部分 II. 管理资源	63
第 6 章 服务质量	64
6.1. 存储服务质量	64
6.1.1. 创建存储服务质量服务条目	64
6.1.2. 删除存储服务质量服务条目	64
6.2. 虚拟机网络服务质量	65
6.2.1. 创建虚拟机网络服务质量服务条目	65
6.2.2. New Virtual Machine Network QoS 和 Edit Virtual Machine Network QoS Windows 中的设置说明	65
6.2.3. 删除虚拟机网络服务质量服务条目	66
6.3. 主机网络服务质量	66
6.3.1. 创建主机网络服务质量服务条目	66
6.3.2. New Host Network Quality of Service and Edit Host Network Quality of Service Windows 中的内容	67
6.3.3. 删除主机网络服务质量条目	68
6.4. CPU 服务质量	68
6.4.1. 创建 CPU 服务质量条目	68
6.4.2. 删除 CPU 服务质量条目	68
第 7 章 数据中心	70

7.1. 数据中心介绍	70
7.2. 存储池管理程序	70
7.3. SPM 优先级	71
7.4. 数据中心任务	71
7.4.1. 创建新数据中心	71
7.4.2. New Data Center 和 Edit Data Center Windows 中的设置说明	71
7.4.3. 重新初始化数据中心：恢复过程	72
7.4.4. 删除数据中心	73
7.4.5. 强制删除数据中心	73
7.4.6. 更改数据中心存储类型	73
7.4.7. 更改数据中心兼容性版本	74
7.5. 数据中心和存储域	74
7.5.1. 将现有数据域附加到数据中心	74
7.5.2. 将现有的 ISO 域附加到数据中心	75
7.5.3. 将现有导出域附加到数据中心	75
7.5.4. 将存储域从数据中心分离	75
第 8 章 集群	77
8.1. 集群简介	77
8.2. 集群任务	77
8.2.1. 创建新集群	77
8.2.2. 常规集群设置说明	79
8.2.3. 优化设置说明	81
8.2.4. 迁移策略设置说明	82
8.2.5. 调度策略设置说明	85
8.2.6. 集群控制台设置说明	88
8.2.7. 隔离策略设置说明	89
8.2.8. 为集群中的主机设置负载和电源管理策略	89
8.2.9. 更新集群中的主机上的 MoM 策略	91
8.2.10. 创建 CPU 配置集	91
8.2.11. 删除 CPU 配置集	92
8.2.12. 导入现有的 Red Hat Gluster Storage 集群	92
8.2.13. Add Hosts 窗口中的设置信息	93
8.2.14. 删除集群	93
8.2.15. Memory Optimization	94
8.2.15.1. 内存优化和内存过量使用	94
8.2.15.2. swap Space 和 Memory Overcommitment	95
8.2.15.3. Memory Overcommit Manager (MoM)	95
8.2.15.4. 内存膨胀	95
8.2.15.5. 内核同页合并(KSM)	96
8.2.16. 更改集群兼容性版本	96
第 9 章 逻辑网络	98
9.1. 逻辑网络任务	98
9.1.1. 执行网络任务	98
9.1.2. 在数据中心或集群中创建新的逻辑网络	98
9.1.3. 编辑逻辑网络	99
9.1.4. 删除逻辑网络	100
9.1.5. 将非管理逻辑网络配置为默认路由	100
9.1.6. 查看或编辑逻辑网络的网关	101
9.1.7. 逻辑网络常规设置说明	101
9.1.8. 逻辑网络集群设置说明	103
9.1.9. 逻辑网络 vNIC 配置文件设置说明	103

9.1.10. 使用 Manage Networks Window 为逻辑网络指定特定流量类型	103
9.1.11. Manage Networks 窗口中的 Settings 解释	104
9.1.12. 编辑 NIC 上的虚拟功能配置	104
9.2. 虚拟网络接口卡	105
9.2.1. vNIC 配置文件概述	105
9.2.2. 创建或编辑 vNIC 配置集	105
9.2.3. VM Interface Profile 窗口中的设置信息	106
9.2.4. 在 vNIC 配置文件中启用 Passthrough	107
9.2.5. 删除 vNIC 配置集	108
9.2.6. 为 vNIC 配置集分配安全组	109
9.2.7. vNIC 配置集的用户权限	109
9.2.8. 为 UCS 集成配置 vNIC 配置集	110
9.3. 外部提供商网络	111
9.3.1. 从外部提供程序导入网络	111
9.3.2. 使用外部提供程序网络的限制	111
9.3.3. 在外部提供程序逻辑网络上配置子网	112
9.3.4. 将子网添加到外部提供程序逻辑网络	112
9.3.5. 从外部提供程序逻辑网络中删除子网	112
9.3.6. 为逻辑网络和端口分配安全组	112
9.4. 主机和网络	113
9.4.1. 刷新主机功能	113
9.4.2. 编辑主机网络接口并将逻辑网络分配给主机	113
9.4.3. 同步主机网络	116
9.4.4. 编辑主机的 VLAN 设置	118
9.4.5. 使用逻辑网络在单一网络接口中添加多个 VLAN	118
9.4.6. 为主机网络分配额外的 IPv4 地址	119
9.4.7. 在主机网络接口中添加网络标签	120
9.4.8. 更改主机的 FQDN	121
9.4.9. IPv6 网络支持	122
9.4.10. 设置和配置 SR-IOV	122
9.4.10.1. 前提条件	122
9.4.10.2. 设置并配置 SR-IOV	122
9.4.10.3. 其它资源	124
9.5. 网络绑定	124
9.5.1. 在管理门户中创建绑定设备	124
9.5.2. 使用 LLDP Labeler 服务创建绑定设备	125
9.5.3. 绑定模式	126
9.6. 分析和监控网络连接	127
9.6.1. Skydive 简介	127
9.6.2. 安装 Skydive	128
9.6.3. 使用 Skydive 测试网络连接	129
第 10 章 主机	131
10.1. 主机简介	131
10.2. RED HAT VIRTUALIZATION HOST	131
10.3. RED HAT ENTERPRISE LINUX 主机	132
10.4. SATELLITE 主机提供程序主机	132
10.5. 主机任务	132
10.5.1. 在 Red Hat Virtualization Manager 中添加标准主机	133
10.5.2. 添加 Satellite 主机提供程序主机	133
10.5.3. 为主机配置 Satellite 勘误管理	134
10.5.4. New Host 和 Edit Host Windows 中的设置和控件的说明	135
10.5.5. 主机常规设置说明	135

10.5.6. 主机电源管理设置说明	137
10.5.7. SPM 优先级设置说明	139
10.5.8. 主机控制台设置说明	139
10.5.9. 网络供应商设置介绍	139
10.5.10. 内核设置说明	140
10.5.11. 托管引擎设置说明	141
10.5.12. 配置主机电源管理设置	141
10.5.13. 配置主机存储池管理程序设置	142
10.5.14. 为 PCI Passthrough 配置主机	143
10.5.15. 将主机移到维护模式	144
10.5.16. 从维护模式激活主机	145
10.5.17. 配置主机防火墙规则	145
10.5.18. 删除主机	146
10.5.19. 更新次版本之间的主机	146
10.5.19.1. 更新集群中的所有主机	146
10.5.19.2. 更新单个主机	147
10.5.19.3. 手动更新主机	149
10.5.20. 重新安装主机	150
10.5.21. 查看主机勘误	150
10.5.22. 查看主机的 Health 状态	151
10.5.23. 查看主机设备	151
10.5.24. 从管理门户访问 Cockpit	151
10.5.25. 设置传统 SPICE 密码	152
10.6. 主机弹性	152
10.6.1. 主机高可用性	152
10.6.2. Red Hat Virtualization 中的代理电源管理	153
10.6.3. 在主机上设置隔离参数	153
10.6.4. fence_kdump 高级配置	154
10.6.4.1. fence_kdump listener Configuration	155
10.6.4.2. 在 Manager 上配置 fence_kdump	156
10.6.5. 软隔离主机	158
10.6.6. 使用主机电源管理功能	158
10.6.7. 手动隔离或隔离不响应的主机	159
第 11 章 存储	160
11.1. 了解存储域	161
11.2. 准备和添加 NFS 存储	161
11.2.1. 准备 NFS 存储	161
11.2.2. 添加 NFS 存储	162
11.2.3. 增加 NFS 存储	162
11.3. 准备和添加本地存储	163
11.3.1. 准备本地存储	163
11.3.2. 添加本地存储	163
11.4. 准备和添加兼容 POSIX 的文件系统存储	164
11.4.1. 准备兼容 POSIX 的文件系统存储	164
11.4.2. 添加兼容 POSIX 的文件系统存储	164
11.5. 准备和添加块存储	165
11.5.1. 准备 iSCSI 存储	165
11.5.2. 添加 iSCSI 存储	166
11.5.3. 配置 iSCSI 多路径	167
11.5.4. 将逻辑网络迁移到 iSCSI 绑定	168
11.5.5. 准备 FCP 存储	169
11.5.6. 添加 FCP 存储	170

11.5.7. 增加 iSCSI 或 FCP 存储	171
11.5.8. 重新使用 LUN	172
11.6. 准备和添加红帽 GLUSTER 存储	172
11.6.1. 准备 Red Hat Gluster Storage	172
11.6.2. 添加 Red Hat Gluster Storage	172
11.7. 导入现有存储域	172
11.7.1. 导入现有存储域概述	173
11.7.2. 导入存储域	173
11.7.3. 在 Same 环境中数据中心之间迁移存储域	174
11.7.4. 在不同环境中在数据中心间迁移存储域	175
11.7.5. 从导入的 Data Storage Domains 导入虚拟机	176
11.7.6. 从导入的 Data Storage Domains 导入模板	177
11.8. 存储任务	178
11.8.1. 将镜像上传到数据存储域	178
11.8.2. 将存储域移到维护模式	179
11.8.3. 编辑存储域	179
11.8.4. 更新 OVF	180
11.8.5. 从维护模式激活存储域	181
11.8.6. 将存储域从数据中心分离	181
11.8.7. 将存储域附加到数据中心	181
11.8.8. 删除存储域	182
11.8.9. 销毁存储域	182
11.8.10. 创建磁盘配置集	182
11.8.11. 删除磁盘配置集	183
11.8.12. 查看存储域的 Health 状态	183
11.8.13. 在为存储域删除后设置 Discard	184
11.8.14. 在有超过 250 个主机的环境中启用 4K 支持	184
11.8.15. 禁用 4K 支持	184
第 12 章 池	186
12.1. 虚拟机池简介	186
12.2. 创建虚拟机池	186
12.3. 新池和编辑池 WINDOWS 中的设置和控制的说明	190
12.3.1. 新池和编辑池常规设置说明	190
12.3.2. 新池和编辑池类型设置说明	191
12.3.3. 新池和编辑池控制台设置说明	191
12.3.4. 虚拟机池主机设置说明	192
12.3.5. 新池和编辑池资源分配设置说明	195
12.4. 编辑虚拟机池	195
12.5. 预启动池中的虚拟机	196
12.6. 将虚拟机添加到虚拟机	196
12.7. 从虚拟机池中分离虚拟机	196
12.8. 删除虚拟机池	197
12.9. 可信计算池	197
12.9.1. 将 OpenAttestation 服务器连接到 Manager	197
12.9.2. 创建可信集群	198
12.9.3. 添加可信主机	198
第 13 章 虚拟磁盘	200
13.1. 了解虚拟机存储	200
13.2. 了解虚拟磁盘	200
13.3. 在删除后将设置为 WIPE VIRTUAL DISKS	201
13.4. RED HAT VIRTUALIZATION 中的可共享磁盘	202

13.5. 在 RED HAT VIRTUALIZATION 中只读磁盘	202
13.6. 虚拟磁盘任务	203
13.6.1. 创建虚拟磁盘	203
13.6.2. New Virtual Disk Window 中的设置说明	204
13.6.3. 实时迁移概述	209
13.6.4. 移动虚拟磁盘	210
13.6.5. 更改磁盘接口类型	210
13.6.6. 复制虚拟磁盘	211
13.6.7. 将镜像上传到数据存储域	211
13.6.8. 从导入的存储域导入磁盘镜像	211
13.6.9. 从导入的存储域导入未注册的磁盘镜像	212
13.6.10. 从 OpenStack Image Service 导入虚拟磁盘	212
13.6.11. 将虚拟磁盘导出到 OpenStack 镜像服务	213
13.6.12. 重新声明虚拟磁盘空间	213
第 14 章 外部供应商	215
14.1. RED HAT VIRTUALIZATION 中的外部提供程序简介	215
14.2. 添加外部供应商	216
14.2.1. 为主机调配添加 Red Hat Satellite 实例	216
14.2.2. 为镜像管理添加 OpenStack Image (Glance)实例	216
14.2.3. 为网络设备添加 OpenStack 网络(Neutron)实例	217
14.2.4. 为存储管理添加 OpenStack Block Storage (Cinder)实例	219
14.2.5. 将 VMware 实例添加为虚拟机提供程序	221
14.2.6. 将 RHEL 5 Xen 主机添加为虚拟机提供程序	223
14.2.7. 将 KVM 主机添加为虚拟机提供程序	224
14.2.8. 添加 Open Virtual Network (OVN)作为外部网络提供程序	226
14.2.8.1. 安装新的 OVN 网络提供程序	226
14.2.8.2. 添加现有 OVN 网络提供程序	229
14.2.8.3. 使用 Ansible playbook 修改 OVN 隧道网络	232
14.2.8.4. 为 OVN Tunnel 网络配置主机	234
14.2.8.5. 将 OVN 网络连接到物理网络	235
14.2.9. 添加外部网络提供程序	237
14.2.10. 添加 Provider General Settings Explained	238
14.2.11. 添加 Provider Agent Configuration Settings Explained	243
14.3. 编辑外部供应商	244
14.4. 删除外部供应商	244
部分 III. 管理环境	245
第 15 章 管理自托管引擎	246
15.1. 维护自托管引擎	246
自托管引擎维护模式	246
设置本地维护	246
设置全局维护	247
15.2. 管理 MANAGER 虚拟机	248
15.2.1. 更新自托管引擎配置	248
15.2.2. 配置电子邮件通知	249
15.3. 在附加主机上为自托管引擎配置 MEMORY SLOTS 保留	250
15.4. 在 RED HAT VIRTUALIZATION MANAGER 中添加自托管引擎节点	250
15.5. 将现有主机重新安装为自托管引擎节点	252
15.6. 在救援模式中引导 MANAGER 虚拟机	252
15.7. 从自托管引擎环境中删除主机	254
15.8. 更新自托管引擎	255
启用全局维护模式	255

更新 Red Hat Virtualization Manager	255
禁用全局维护模式	257
15.9. 在自托管引擎中更改 MANAGER 的 FQDN	258
第 16 章 备份和迁移	259
16.1. 备份和恢复 RED HAT VIRTUALIZATION MANAGER	259
16.1.1. 备份 Red Hat Virtualization Manager - 概述	259
16.1.2. engine-backup 命令的语法	259
16.1.3. 使用 engine-backup 命令创建备份	260
16.1.4. 使用 engine-backup 命令恢复备份	261
16.1.5. 将备份恢复到刷新安装	262
16.1.6. 恢复备份以覆盖现有安装	263
16.1.7. 使用不同凭证恢复备份	264
16.1.8. 备份和恢复自托管引擎	267
16.1.8.1. 备份原始管理器	268
16.1.8.2. 在新的自托管引擎中恢复备份	269
16.1.8.3. 启用 Red Hat Virtualization Manager 存储库	274
16.1.8.4. 重新安装主机	275
16.1.8.5. 删除存储域	276
16.1.9. 从现有的备份中恢复自托管引擎	277
16.1.9.1. 在新的自托管引擎中恢复备份	278
16.1.9.2. 启用 Red Hat Virtualization Manager 存储库	282
16.1.9.3. 重新安装主机	284
16.1.9.4. 删除存储域	285
16.1.10. 从现有的备份覆盖自托管引擎	286
16.1.10.1. 启用全局维护模式	286
16.1.10.2. 恢复备份以覆盖现有安装	287
16.1.10.3. 禁用全局维护模式	288
16.2. 将 RED HAT VIRTUALIZATION 数据库迁移到远程服务器	289
16.2.1. 将 Manager 数据库迁移到远程服务器	289
16.2.1.1. 启用 Red Hat Virtualization Manager 存储库	289
将 Manager 数据库迁移到远程服务器	290
16.2.2. 将自托管引擎数据库迁移到远程服务器	291
启用 Red Hat Virtualization Manager 存储库	291
将自托管引擎数据库迁移到远程服务器	293
16.2.3. 将数据仓库迁移到独立机器	294
16.2.3.1. 将数据仓库数据库迁移到独立机器	294
启用 Red Hat Virtualization Manager 存储库	294
将数据仓库数据库迁移到独立机器	295
16.2.3.2. 将数据仓库服务迁移到独立机器	296
16.2.3.2.1. 设置新的数据仓库机器	297
16.2.3.2.2. 在 Manager 机器上停止数据仓库服务	298
16.2.3.2.3. 配置新的数据仓库 (Data Warehouse 机器)	299
16.2.3.2.4. 在 Manager 机器上禁用数据仓库服务	300
16.3. 使用备份存储域备份和恢复虚拟机	301
16.3.1. 备份存储域解释	301
16.3.2. 将数据存储域设置为备份域	303
16.3.3. 使用备份域备份或恢复虚拟机或快照	303
16.4. 使用备份和恢复 API 备份和恢复虚拟机	305
16.4.1. 备份和恢复 API	305
16.4.2. 备份虚拟机	305
16.4.3. 恢复虚拟机	308

第 17 章 使用 RED HAT SATELLITE 管理勘误	310
第 18 章 使用 ANSIBLE 自动化配置任务	312
18.1. ANSIBLE 角色	312
18.1.1. 安装 Ansible 角色	313
18.1.2. 使用 Ansible 角色配置 Red Hat Virtualization	313
第 19 章 用户和角色	316
19.1. 用户简介	316
19.2. DIRECTORY 服务器介绍	316
19.3. 配置外部 LDAP 供应商	318
19.3.1. 配置外部 LDAP 提供程序 (活动设置)	318
19.3.2. 附加 Active Directory	324
19.3.3. 配置外部 LDAP 提供程序(Manual Method)	328
19.3.4. 删除外部 LDAP 供应商	331
19.4. 为单点登录配置 LDAP 和 KERBEROS	332
19.5. 安装和配置红帽单点登录	338
19.5.1. Installing Red Hat Single Sign-On	338
19.5.2. 配置 LDAP 组映射器	339
19.5.3. 在 Manager 中配置 Apache	341
19.5.4. 配置 OVN	343
19.6. 用户授权	344
19.6.1. 用户授权模型	344
19.6.2. 用户操作	344
19.7. 从管理门户管理用户任务	344
19.7.1. 添加用户和分配虚拟机门户权限	344
19.7.2. 查看用户信息	345
19.7.3. 查看用户权限资源	345
19.7.4. 删除用户	346
19.7.5. 查看 Logged-In 用户	346
19.7.6. 终止用户会话	346
19.8. 从命令行管理用户任务	347
19.8.1. 创建新用户	347
19.8.2. 设置用户密码	347
19.8.3. 设置用户超时	348
19.8.4. 预加密用户密码	348
19.8.5. 查看用户信息	349
19.8.6. 编辑用户信息	349
19.8.7. 删除用户	350
19.8.8. 禁用内部管理用户	350
19.8.9. 管理组	350
19.8.10. 查询用户和组	352
19.8.11. 管理帐户设置	353
19.9. 配置附加本地域	354
第 20 章 配额和服务等级协议政策	355
20.1. QUOTA 简介	355
20.2. 共享配额和个别定义配额	356
20.3. 配额帐户	357
20.4. 在 DATA CENTER 中启用和更改配额模式	357
20.5. 创建新配额策略	358
20.6. QUOTA THRESHOLD SETTINGS 的解释	359
20.7. 为对象分配配额	360
20.8. 使用配额限制用户的资源	361

20.9. 编辑配额	362
20.10. 删除配额	362
20.11. 服务等级协议政策强制	363
第 21 章 事件通知	364
21.1. 在管理门户中配置事件通知	364
21.2. 在管理门户中取消事件通知	366
21.3. OVIRT-ENGINE-NOTIFIER.CONF 中的事件通知参数	367
21.4. 配置 RED HAT VIRTUALIZATION MANAGER 以发送 SNMP TRAPS	370
第 22 章 工具	373
22.1. OVIRT ENGINE RENAME 工具	373
22.1.1. oVirt Engine Rename 工具	373
22.1.2. oVirt Engine Rename 命令的语法	374
22.1.3. 使用 oVirt Engine Rename 工具重命名 Manager	375
22.2. ENGINE 配置工具	377
22.2.1. Engine 配置工具	377
22.2.2. engine-config 命令的语法	377
22.3. USB 过滤器编辑器	378
22.3.1. 安装 USB 过滤器编辑器	378
22.3.2. USB 过滤器编辑器接口	379
22.3.3. 添加 USB 策略	380
22.3.4. 删除 USB 策略	381
22.3.5. 搜索 USB 设备策略	382
22.3.6. 导出 USB 策略	382
22.3.7. 导入 USB 策略	383
22.4. LOG COLLECTOR 工具	383
22.4.1. 日志收集器	383
22.4.2. ovirt-log-collector 命令的语法	384
22.4.3. 基本日志收集器使用情况	387
22.5. ISO 上传程序工具	388
22.5.1. ISO 上传程序工具	388
22.5.2. engine-iso-uploader 命令的语法	388
22.5.3. 指定 NFS 服务器	391
22.5.4. 基本 ISO 上传程序使用	391
22.5.5. 将 VirtIO 和客户机工具镜像文件上传到 ISO 存储域	392
22.6. ENGINE VACUUM 工具	393
22.6.1. Engine Vacuum 工具	393
22.6.2. 引擎 Vacuum 模式	394
22.6.3. engine-vacuum 命令的语法	394
22.7. VDSM 到网络名称映射工具	395
22.7.1. 将 VDSM 名称映射到逻辑网络名称	395
部分 IV. 收集有关环境的信息	397
第 23 章 在 RED HAT VIRTUALIZATION MANAGER 中部署 INSIGHTS	398
第 24 章 日志文件	400
24.1. MANAGER 安装日志文件	400
24.2. RED HAT VIRTUALIZATION MANAGER 日志文件	400
24.3. SPICE 日志文件	401
24.3.1. 适用于 Hypervisor SPICE 服务器的 SPICE 日志	401
24.3.2. 适用于客户机机器的 SPICE 日志	401
24.3.3. 使用 console.vv 文件启动 SPICE 客户端的 SPICE 日志	402

24.4. 主机日志文件	403
24.5. 设置主机日志记录服务器	403
24.6. 启用 OVIRT ENGINE EXTENSION LOGGER LOG4J	404
附录 A. VDSM 和 HOOK	407
A.1. VDSM	407
A.2. VDSM HOOK	407
A.3. 使用 HOOK 扩展 VDSM	407
A.4. 支持的 VDSM 事件	407
A.5. VDSM HOOK 环境	409
A.6. VDSM HOOK 域 XML 对象	410
A.7. 定义自定义属性	410
A.8. 设置虚拟机自定义属性	412
A.9. 在 VDSM HOOK 中评估虚拟机自定义属性	413
A.10. 使用 VDSM HOOKING 模块	413
A.11. VDSM HOOK 执行	414
A.12. VDSM HOOK 返回代码	415
A.13. VDSM HOOK 示例	415
附录 B. 自定义网络属性	418
B.1. BRIDGE_OPTS 参数的说明	418
B.2. 如何设置 RED HAT VIRTUALIZATION MANAGER 以使用 ETHTOOL	419
B.3. 如何设置 RED HAT VIRTUALIZATION MANAGER 以使用 FCOE	420
附录 C. RED HAT VIRTUALIZATION 用户界面插件	422
C.1. RED HAT VIRTUALIZATION 用户界面插件	422
C.2. RED HAT VIRTUALIZATION 用户界面插件生命周期	422
C.2.1. Red Hat Virtualization 用户界面插件生命周期	422
C.2.2. Red Hat Virtualization 用户界面插件发现	422
C.2.3. Red Hat Virtualization 用户界面插件	423
C.2.4. Red Hat Virtualization 用户界面插件	423
C.3. 用户界面插件相关的文件和位置	424
C.4. 用户界面插件部署示例	425
附录 D. RED HAT VIRTUALIZATION 和加密通信	427
D.1. 替换 RED HAT VIRTUALIZATION MANAGER CA 证书	427
D.2. 在 MANAGER 和 LDAP 服务器间设置加密通信	431
D.3. 为 VDSM 手动设置加密通信 流程	432 432
附录 E. 代理	434
E.1. SPICE 代理	434
E.1.1. SPICE 代理概述	434
E.1.2. SPICE 代理机器设置	434
E.1.3. 开启 SPICE 代理	435
E.1.4. 关闭 SPICE 代理	436
E.2. SQUID PROXY	436
E.2.1. 安装和配置 Squid 代理	437
E.3. WEBSOCKET 代理	440
E.3.1. Websocket 代理概述	440
E.3.2. 将 Websocket 代理迁移到一个独立的机器 从 Manager 机器中删除 Websocket 代理 在独立的机器中安装 Websocket 代理	440 441 441
附录 F. BRANDING	445

F.1. BRANDING	445
F.1.1. 重新添加管理器	445
F.1.2. 登录屏幕	445
F.1.3. 管理门户屏幕	445
F.1.4. 虚拟机门户屏幕	446
F.1.5. 弹出 Windows	446
F.1.6. 标签页	447
F.1.7. Welcome Page	447
F.1.8. 页面未找到页面	448
附录 G. 系统帐户	449
G.1. 系统帐户	449
G.1.1. Red Hat Virtualization Manager 用户帐户	449
G.1.2. Red Hat Virtualization Manager Groups	449
G.1.3. 虚拟化主机用户帐户	450
G.1.4. 虚拟化主机组	450

部分 I. 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。

第 1 章 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. 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. 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。

创建新角色

1. 单击 **Administration** → **Configure** 以打开 **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 **OK** 以应用更改。新角色显示在角色列表中。

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。

编辑或复制角色

1. 单击 **Administration** → **Configure** 以打开 **Configure** 窗口。窗口中显示默认 **User** 和 **Administrator** 角色列表，以及任何自定义角色。
2. 选择您要更改的角色。单击 **Edit** 以打开 **Edit Role** 窗口，或者单击 **Copy** 以打开 **Copy Role** 窗口。
3. 如有必要，编辑角色的 **Name** 和 **Description**。

4. 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。
5. 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。
6. 单击**确定**以应用您所做的更改。

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。

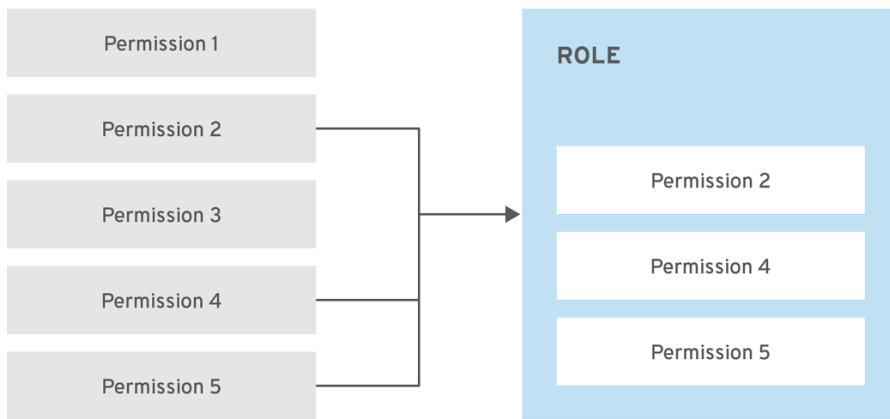
图 1.1. UserManager 自定义角色

上面显示的 **UserManager** 自定义角色允许操作用户、权限和角色。这些步骤在 **System** 下组织 - 图 1.3 “Red Hat Virtualization 对象层次结构” 中显示的层次结构的顶级对象。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。

1.2. 系统权限

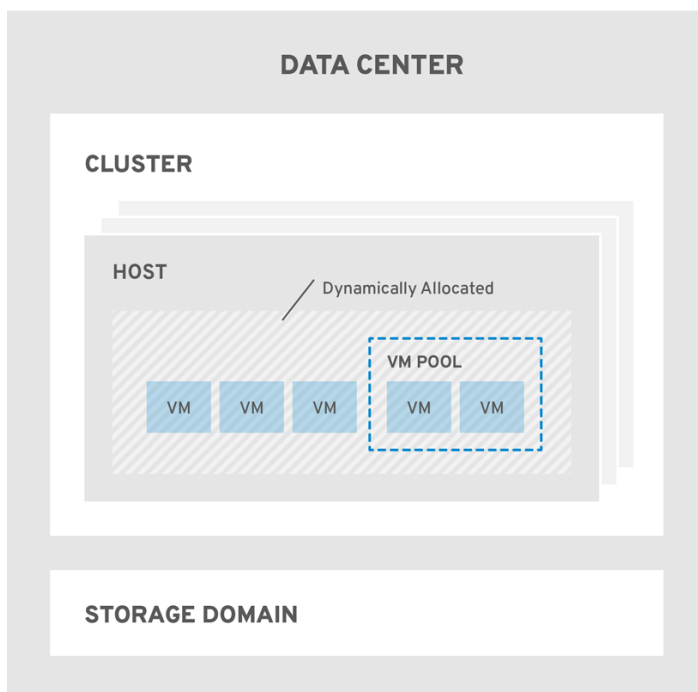
权限允许用户对对象执行操作，其中对象可以是单个对象或容器对象。适用于容器对象的任何权限也适用于该容器的所有成员。

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

1.2.1. 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。

1.2.2. 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。

1.2.3. 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。
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。

角色	权限	备注
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。

1.2.4. 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。

1.2.5. 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。

将角色分配到一个资源

1. 找到并单击资源的名称以打开详情视图。
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. 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. 单击 **OK**。

用户现在为该资源启用了该角色的继承权限。

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。

从资源中删除角色

1. 找到并单击资源的名称以打开详情视图。
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. 单击 **OK**。

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。

1.2.8. 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。

角色	权限	备注
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。

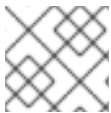
1.2.9. 管理系统权限

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。

1.2.10. 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
----	----	----

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>

1.2.11. 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。

1.2.12. 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。

1.2.13. 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。

1.2.14. 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。

1.2.15. 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。

1.2.16. 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。

1.2.17. 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。

1.2.18. 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。

1.2.19. 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。

1.2.20. 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。

1.2.21. 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
```

另外，您还可以将 **--extra-vars** 选项与变量 **host_deploy_spice_cipher_string** 使用 Ansible playbook **ovirt-host-deploy** 重新配置主机，如下所示：

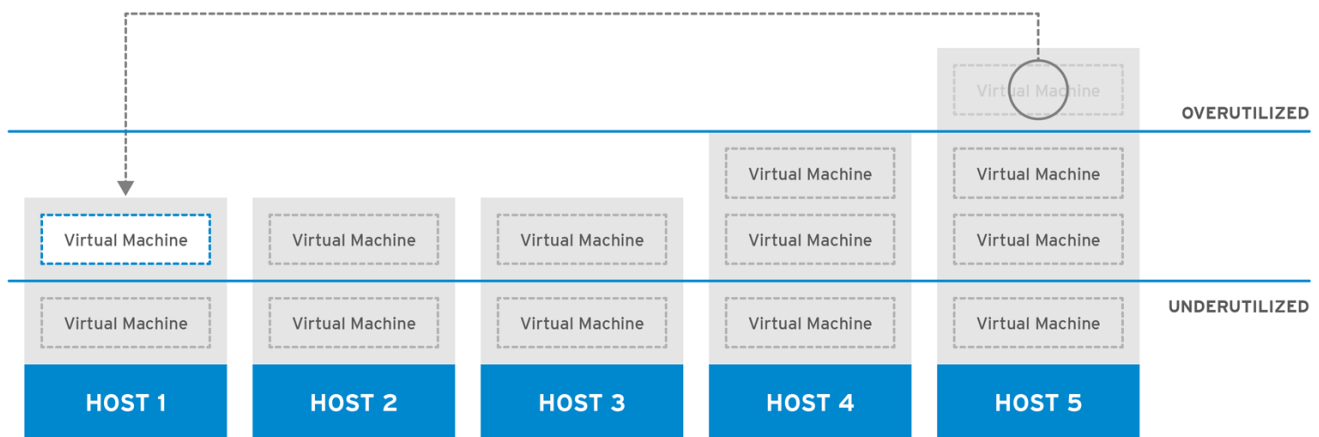
```
# ansible-playbook -i hostname \
  --extra-vars host_deploy_spice_cipher_string="DEFAULT:-RC4:-3DES:-DES" \
  /usr/share/ovirt-engine/playbooks/ovirt-host-deploy.yml
```

1.3. 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。有关每个调度策略的属性的更多信息，请参阅 [第 8.2.5 节“调度策略设置说明”](#)。

图 1.4. 平均分布式调度策略

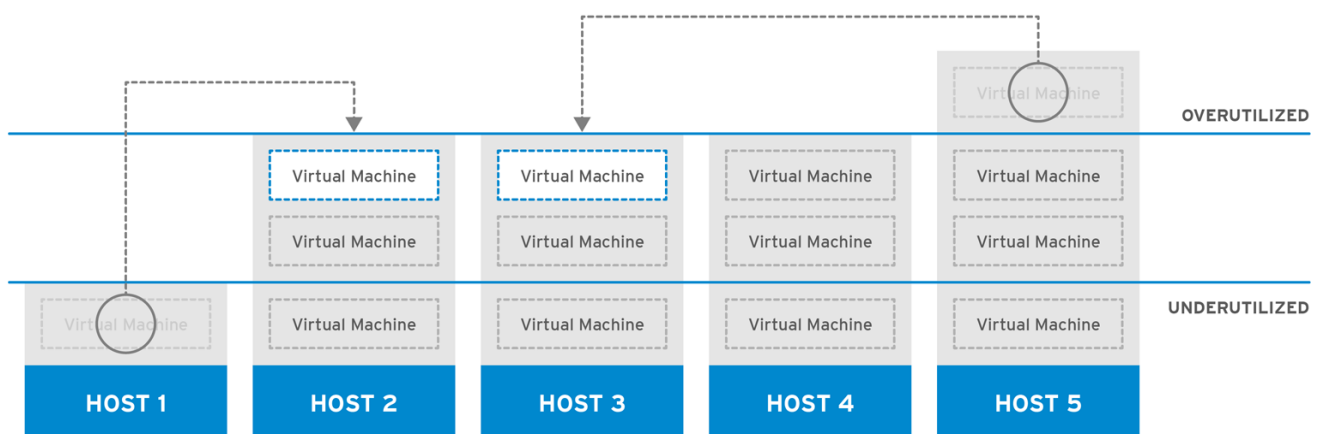


RHV_ 444396_0417

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** 或 **MaxFreeMemoryForOverUtilized**，则附加到主机的其他虚拟机将不会启动。

VM_Evenly_Distried 调度策略虚拟机根据虚拟机数量在主机之间平均分配。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。

1.3.1. 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。

创建调度策略

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**。

1.3.2. 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。

字段名称	Description
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"> ● CpuPinning : 无法满足 CPU 固定定义的主机。 ● Migration: 防止迁移到同一主机。 ● 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。 ● CPU : CPU 数量少于分配给虚拟机的主机。 ● memory : 没有足够的内存来运行虚拟机的主机。 ● VmAffinityGroups : 不符合关联性组成员虚拟机指定条件的主机。例如，关联性组中的虚拟机必须在同一主机上运行或在单独的主机上运行。 ● 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主机上运行，或者在组中排除的独立主机上运行。 ● InClusterUpgrade : 运行操作系统早于当前运行虚拟机的主机。 ● 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。 ● 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。 ● 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。 ● Label: 没有所需关联性标签的主机。 ● compatibility-Version : 仅在具有正确兼容性版本的主机上运行虚拟机。 ● CPUOverloaded : CPU 超载的主机。

字段名称	Description
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"> ● 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。 ● OptimalForHaReservation : 根据主机的高可用性分数。 ● none : 根据 even distribution 模块来放置主机。 ● OptimalForEvenGuestDistribution : 根据这些主机上运行的虚拟机数量, Wights 主机。 ● VmAffinityGroups : 根据为虚拟机定义的关联性组, Wights 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。 ● VmToHostsAffinityGroups : 根据为虚拟机定义的关联性组, Wights 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。 ● OptimalForCPUPowerSaving : 根据 CPU 使用率, 为具有更高 CPU 使用量的主机赋予优先级。 ● OptimalForEvenCpuDistribution : 根据 CPU 使用率, 为 CPU 使用率较低的主机赋予优先级。 ● HA : 根据主机的高可用性分数来放置主机。 ● PreferredHosts : 首选主机在虚拟机设置期间具有优先级。 ● OptimalForMemoryPowerSaving: 根据内存使用情况, 为可用内存较低的主机赋予优先级。 ● 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。
Load Balancer	<p>此下拉菜单允许您选择要应用的负载平衡模块。负载平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。</p>

字段名称	Description
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。

1.4. 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。

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
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。

New Virtual Machine 和 **Edit Virtual Machine** 窗口中的字段绑定到实例类型，其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。

1.4.1. 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。

创建实例类型

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“新建虚拟机”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。

1.4.2. 编辑实例类型

管理员可以从 **Configure** 窗口编辑现有的实例类型。

编辑实例类型属性

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. 单击 **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。

1.4.3. 删除实例类型

删除实例类型

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. 单击 **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）。

1.5. 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 [第 8.2.1 节“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。

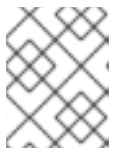
MAC 地址池分配返回到池的最后一个地址之后的下一个可用 MAC 地址。如果范围中没有剩余地址，则搜索将从范围的开头重新开始。如果有多个 MAC 地址范围中定义了可用 MAC 地址，则范围将以与选择可用 MAC 地址相同的方式为传入的请求提供服务。

1.5.1. 创建 MAC 地址池

您可以创建新的 MAC 地址池。

创建 MAC 地址池

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**。

1.5.2. 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。

编辑 MAC 地址池属性

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. 点击 **OK**。

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详情，请参考 [第 1.1 节“角色”](#)。

编辑 MAC 地址池权限

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。

1.5.4. 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。

删除 MAC 地址池

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**。

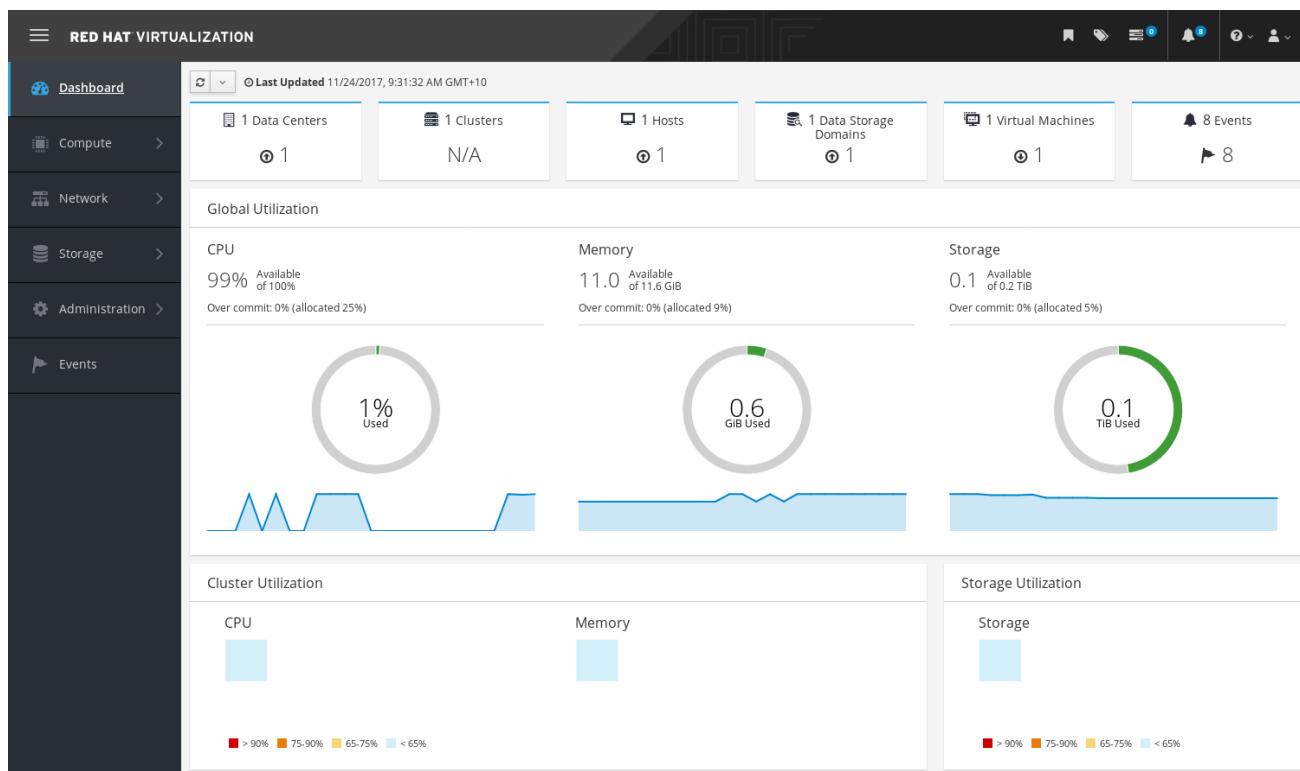
5. 单击 **OK**。

第 2 章 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 2.1. 控制面板



2.1. 先决条件

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

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 2.2. 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 2.1. 资源状态

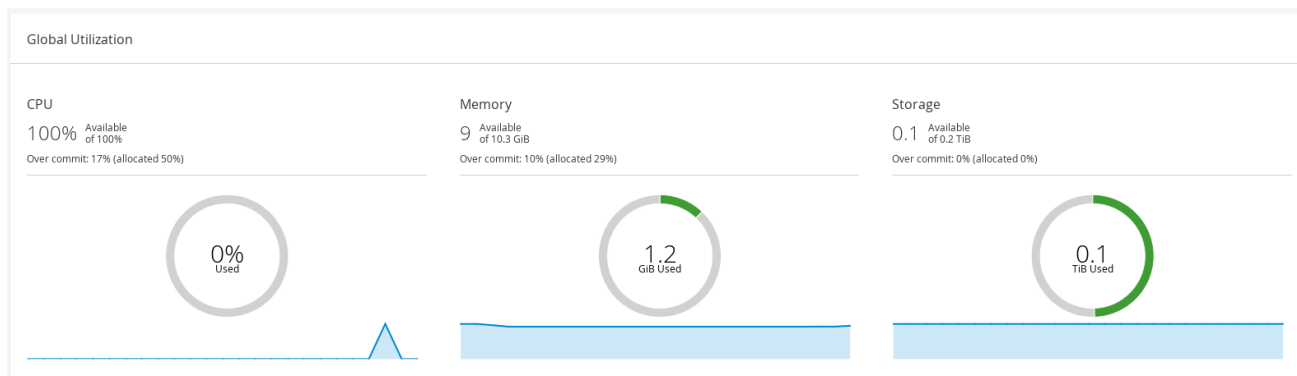
图标	状态
	这些资源都不添加到 Red Hat Virtualization 中。
	<p>显示具有警告状态的资源数。单击图标可导航到相应的页面，搜索范围仅限于该资源，且具有警告状态。每个资源的搜索都会有所不同：</p> <ul style="list-style-type: none"> ● Data Centers: 搜索仅限于不正常运行或不响应的数据中心。 ● Gluster 卷：搜索仅限于正在启动、暂停、迁移、等待、暂停或关机的 gluster 卷。 ● 主机：搜索仅限于未分配、处于维护模式、安装、重新启动、准备维护、待处理批准或连接的主机。 ● 存储域：搜索仅限于未初始化、未附加、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。
	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>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。
	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。

图标	状态
	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。

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。

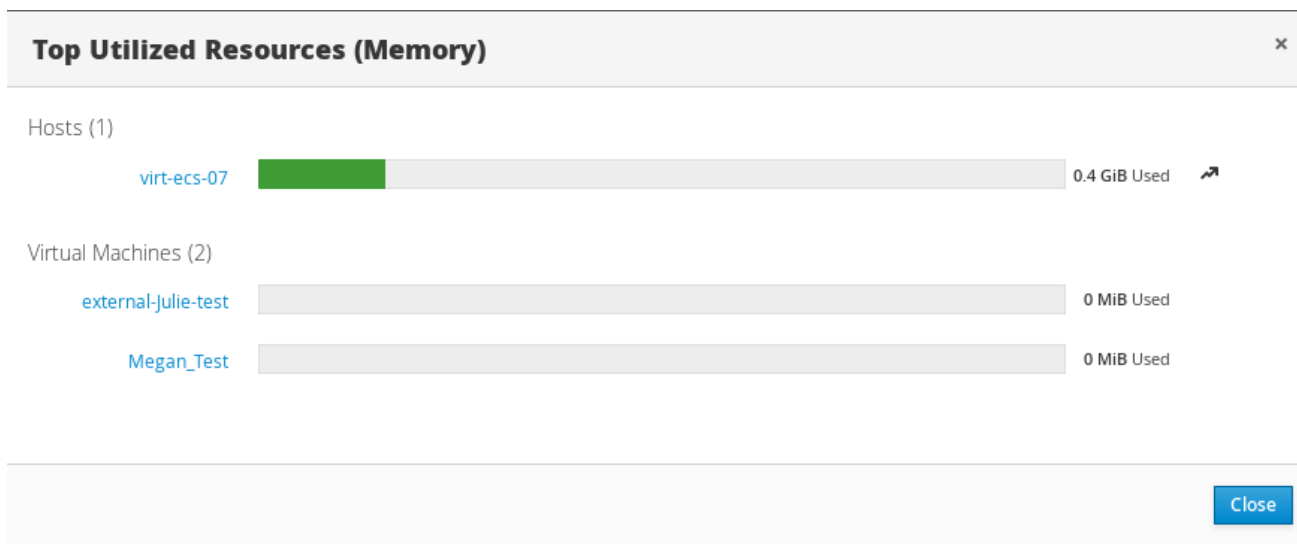
图 2.3. 全局利用率



- 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。

2.3.1. top Utilized Resources

图 2.4. top Utilized Resources (Memory)

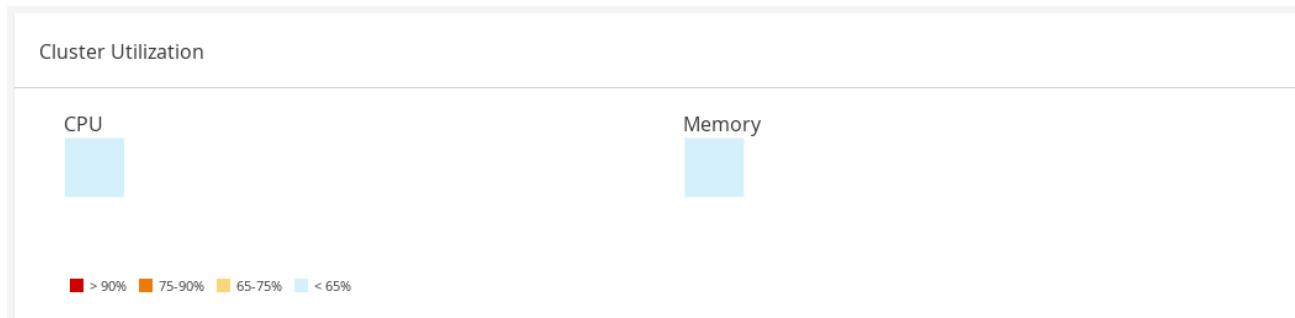


点控制面板的全局使用部分中的圆环，将显示 CPU、内存或存储占用最多的资源的列表。对于 CPU 和内存，弹出框显示使用率最高的十个主机和虚拟机列表。对于存储，弹出显示占用的十大存储域和虚拟机的列表。使用栏右侧的箭头显示该资源在最后一分钟内的使用情况。

2.4. CLUSTER UTILIZATION

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

图 2.5. Cluster Utilization



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。

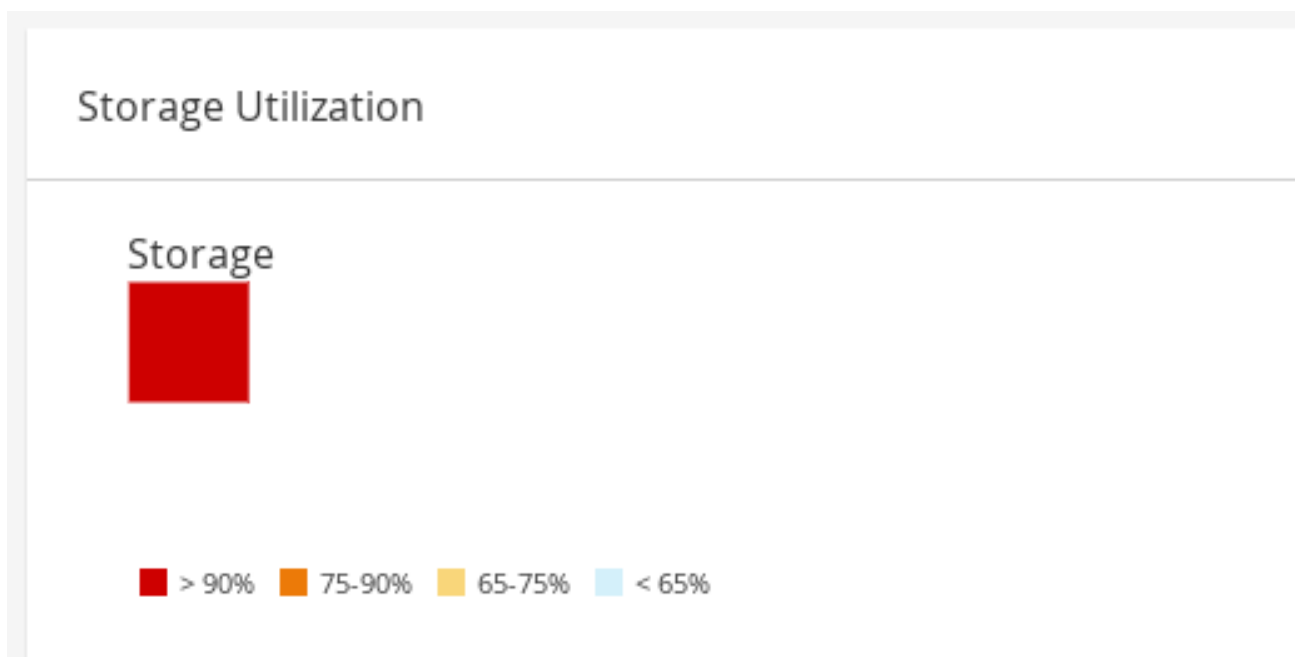
2.4.2. 内存

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。

2.5. STORAGE UTILIZATION

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

图 2.6. 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**。

第 3 章 搜索

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。

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 3.1. 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。

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 3.2. 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

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。

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 3.3. 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

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**。

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）。

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 3.4. 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。

3.9. 搜索集群

下表描述了集群的所有搜索选项。

表 3.5. 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。

3.10. 搜索主机

下表描述了主机的所有搜索选项。

表 3.6. 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。

属性 (资源或资源类型)	类型	描述 (参考)
cluster	字符串	主机所属的集群。
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。

3.11. 搜索网络

下表描述了网络的所有搜索选项。

表 3.7. 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。

3.12. 搜索存储

下表描述了存储的所有搜索选项。

表 3.8. 搜索存储

属性 (资源或资源类型)	类型	描述 (参考)
--------------	----	---------

属性 (资源或资源类型)	类型	描述 (参考)
<i>主机.host-prop</i>	取决于属性类型	与存储关联的主机的属性。
<i>cluster.cluster-prop</i>	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。
size	整数	存储的大小。
使用的	整数	使用的存储量。
已提交	整数	提交的存储量。
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: size > 200 或 use < 50

这个示例返回一个存储空间总量大于 200 GB 的存储列表，或者存储空间小于 50 GB。

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 3.9. 搜索磁盘

属性 (资源或资源类型)	类型	描述 (参考)
<i>Datcenters.datacenters-prop</i>	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
共享	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。

3.14. 搜索卷

下表描述了卷的所有搜索选项。

表 3.10. 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 and 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。

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 3.11. 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>vmnic-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。

3.16. 搜索池

下表描述了池的所有搜索选项。

表 3.12. 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。

3.17. 搜索模板

下表描述了模板的所有搜索选项。

表 3.13. 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。

属性（资源或资源类型）	类型	描述（参考）
cluster	字符串	与模板关联的集群。
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。

3.18. 搜索用户

下表描述了用户的所有搜索选项。

表 3.14. 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。

属性（资源或资源类型）	类型	描述（参考）
status	字符串	用户的状态。
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。

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 3.15. 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。
重要性	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。


第 4 章 书签

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。

将查询字符串保存为书签


1. 在搜索栏中输入所需的搜索查询，并执行搜索。
2. 单击搜索栏右侧的星号小 **书签** 按钮以打开 **新书签** 窗口。
3. 输入书签的 **Name**。
4. 如果需要，编辑 **Search string** 字段。
5. 单击 **OK**。

点击标题栏中的 **书签** 图标()找到并选择书签。

4.2. 编辑书签

您可以修改书签的名称和搜索字符串。


编辑书签

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. 单击 **OK**。

4.3. 删除书签

当不再需要书签时，将其删除。

删除书签

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

第 5 章 TAGS

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 Administration Portal 标签，请点标题栏中的 **标签** 图标 ()。

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。

创建标签

1. 点击标题栏中的 **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**。

5.3. 修改标签

您可以编辑标签的名称和描述。

修改标签

1. 点击标题栏中的 **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**。

5.4. 删除标签

当不再需要某个标签时，将它删除。

删除标签


1. 点击标题栏中的 **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。

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。

为对象添加和删除标签

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。

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。

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。有关搜索的详情请参考 [第 3 章 搜索](#)。

使用标签自定义主机

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. 点击 **OK**。

您已添加有关主机的额外可搜索信息作为标签。

部分 II. 管理资源

第 6 章 服务质量

Red Hat Virtualization 允许您定义服务质量条目，对环境中资源的输入和输出、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。

6.1. 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。

6.1.1. 创建存储服务质量服务条目

创建存储服务质量服务条目

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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. 点击 **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。

6.1.2. 删除存储服务质量服务条目

删除现有存储服务质量条目。

删除存储服务质量服务条目

1. 单击 **Compute → Data Centers**。

2. 点数据中心的名称打开详情视图。
3. 点 **QoS** 选项卡。
4. 在 **Storage** 下，选择 storage quality of service 条目，再单击 **Remove**。
5. 点击 **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]**。

6.2. 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。

6.2.1. 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. 点击 **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。

6.2.2. 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 6.1. 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
```

6.2.3. 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。

删除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**。

6.3. 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。

6.3.1. 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。

创建主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**。

6.3.2. 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 6.2. 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 名称	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
```

6.3.3. 删除主机网络服务质量条目

删除现有的服务质量。

删除主机网络服务质量条目

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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**。

6.4. 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。

6.4.1. 创建 CPU 服务质量条目

创建服务条目的 CPU 质量。

创建 CPU 服务质量条目

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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。

6.4.2. 删除 CPU 服务质量条目

删除服务条目的现有 CPU 质量。

删除 CPU 服务质量条目

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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]**。

第 7 章 数据中心

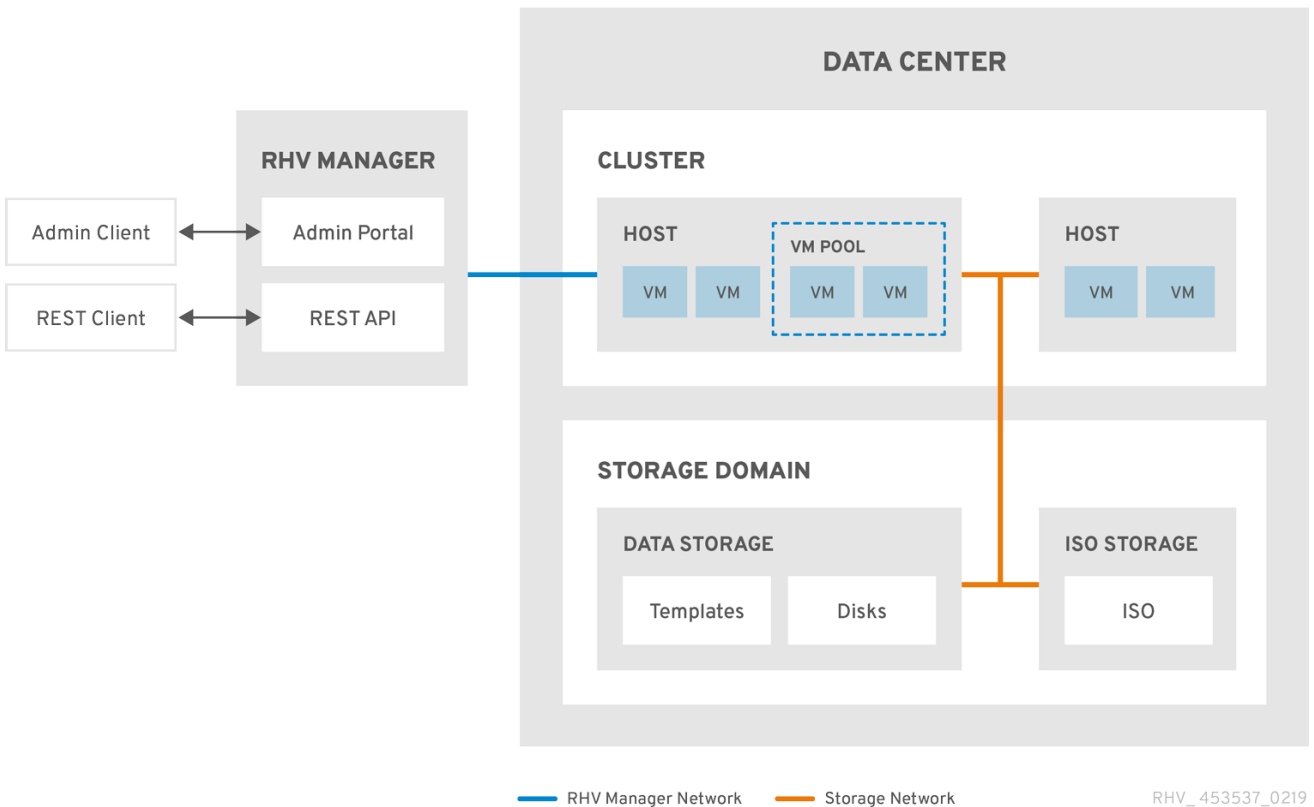
7.1. 数据中心介绍

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 7.1. 数据中心



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。

7.2. 存储池管理程序

存储池管理程序 (SPM) 是提供给数据中心的某一主机的角色，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。

7.3. SPM 优先级

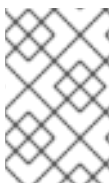
SPM 角色使用部分主机的可用资源。主机的 SPM 优先级设置将更改被分配 SPM 角色的主机的可能性：在具有高 SPM 优先级的主机将在主机具有低 SPM 优先级前分配 SPM 角色。具有低 SPM 优先级的主机上的关键虚拟机不必与主机资源的 SPM 操作相交。

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

7.4. 数据中心任务

7.4.1. 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

在设置了 **Compatibility Version** 后，它无法在以后的版本中降低；不允许版本回归。

为数据中心指定 MAC 池范围的选项已被禁用，现在在集群级别完成。

创建新数据中心

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. 单击 **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。

7.4.2. 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 7.1. 数据中心属性

字段	description/Action
----	--------------------

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。请参阅第 7.4.6 节“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。


7.4.3. 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。

重新初始化数据中心

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。

7.4.4. 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。

删除数据中心

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**。

7.4.5. 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。

强制删除数据中心

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 **确定**

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

7.4.6. 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。

更改数据中心存储类型

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**。

7.4.7. 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。



重要

要更改数据中心兼容性版本，您必须首先更新数据中心中所有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。

7.5. 数据中心和存储域

7.5.1. 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)。

将现有数据域附加到数据中心

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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。

7.5.2. 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。

将现有的 ISO 域附加到数据中心

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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. 点击 **OK**。

ISO 域连接到数据中心，并自动激活。

7.5.3. 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。有关导入存储域的详情，请参考 [第 11.7 节“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。

将现有导出域附加到数据中心

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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. 点击 **OK**。

导出域连接到数据中心，并自动激活。

7.5.4. 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。

**注意**

如果 master 存储是最后可用的存储域，则无法删除。

将存储域从数据中心分离

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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。

第 8 章 集群

8.1. 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。

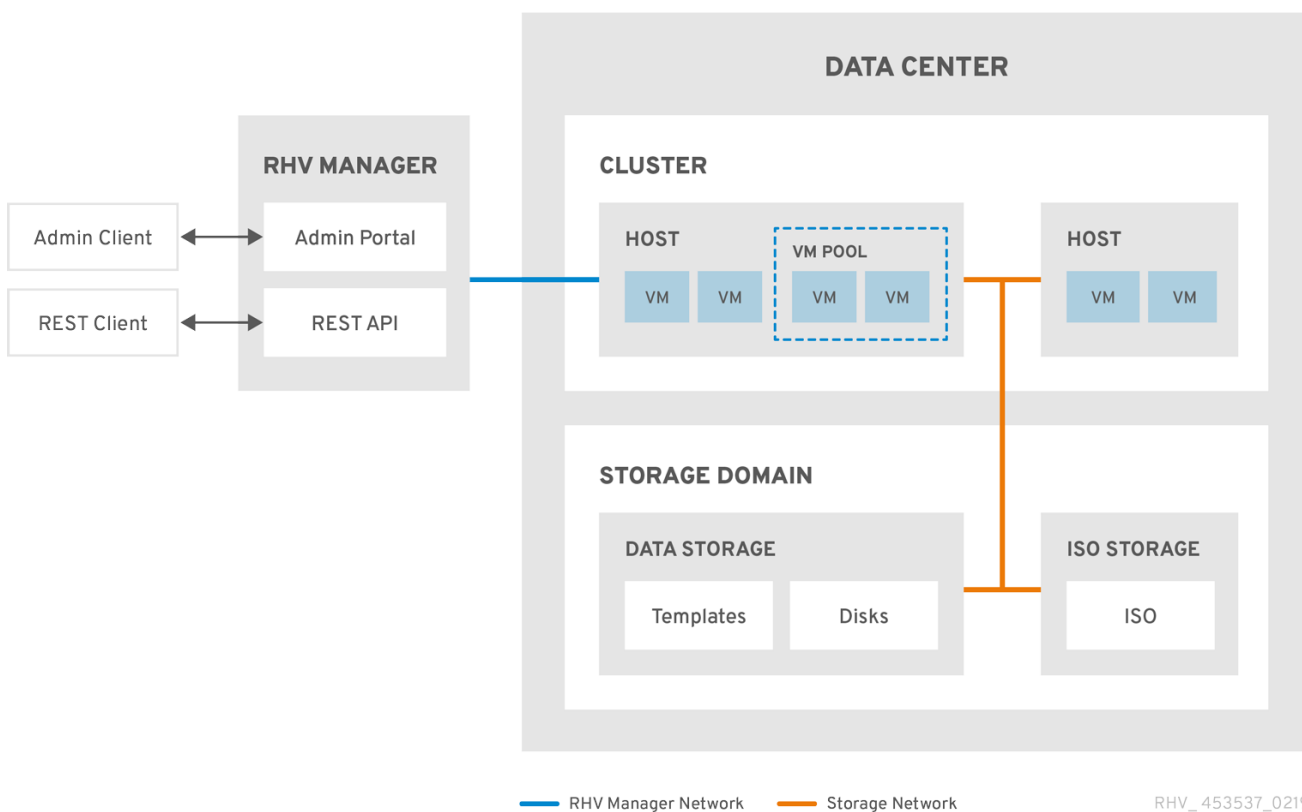
系统中的每个集群都必须属于一个数据中心，系统中的每一主机都必须属于一个集群。虚拟机会动态分配到集群中的任何主机，并根据虚拟机中定义的策略在它们之间进行迁移。集群是可定义电源和加载共享策略的最高级别。

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 8.1. 集群



8.2. 集群任务



注意

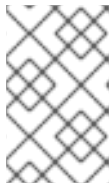
有些集群选项不适用于 Gluster 集群。有关在 Red Hat Virtualization 中使用 Red Hat Gluster Storage 的更多信息，请参阅使用 [Red Hat Gluster Storage 配置 Red Hat Virtualization](#)。

8.2.1. 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是相同的 CPU 类型 (Intel 或 AMD)。建议您在创建集群时创建主机以确保 CPU 类型优化。但是，您可以稍后使用 [引导我按钮配置主机](#)。

创建新集群

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. 从下拉列表中选择 **CPU 架构和 CPU 类型**。务必要将 CPU 处理器系列与您要附加到集群的主机的最小 CPU 处理器类型匹配，否则主机将无法正常工作。



注意

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。如果您的集群包含具有不同 CPU 模型的主机，请选择最旧的 CPU 模型。有关每个 CPU 模型的详情请参考 <https://access.redhat.com/solutions/634853>。


7. 从下拉列表中选择集群的 **Compatibility Version**。
8. 从下拉列表中选择 **Switch Type**。
9. 选择 **集群中主机的防火墙类型**，可以是 `iptables` 或 `firewalld`。



注意

`iptables` 已被弃用。

10. 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。
11. (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。
12. (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。
13. (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)。
14. 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。
15. 单击 **Migration Policy** 选项卡定义集群的虚拟机迁移策略。
16. 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 并添加自定义序列号策略。

17. 点击 **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。
18. 点击 **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。
19. 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 地址池的详情请参考 [第 1.5 节“MAC 地址池”](#)。
20. 点击 **OK** 创建集群并打开 **Cluster - Guide Me** 窗口。
21. **Guide Me** 窗口列出了需要为集群配置的实体。点 **Configure Later** 按钮配置这些实体或 postpone 配置。通过选择集群并点 **More Actions** () 来恢复配置，然后点 **引导我**。

8.2.2. 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 8.1. 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。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 CPU 类型都可用。 ● x86_64：所有可用的 Intel 和 AMD CPU 类型。 ● ppc64：只有 IBM POWER 8 可用。

字段	description/Action
CPU 类型	集群的 CPU 类型。如需支持的 CPU 类型列表，请参阅《 规划与先决条件指南 》中的 CPU 要求。集群中的所有主机都必须运行 Intel、AMD 或 IBM POWER 8 CPU 类型，在创建后无法更改，而不会有重大中断。CPU 类型应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。
兼容性版本	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。
切换类型	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。
防火墙类型	指定集群中主机的防火墙类型，可以是 iptables 或 firewalld 。 注意 iptables 已被弃用。 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。
默认网络提供程序	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。 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。
最大日志内存阈值	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% 。
启用 Virt Service	如果选择了此单选按钮，则此集群中的主机将用于运行虚拟机。
启用 Gluster 服务	如果选择了此单选按钮，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。

字段	description/Action
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"> ● 地址：输入 Gluster 主机服务器的 IP 或完全限定域名。 ● 指纹：Red Hat Virtualization Manager 获取主机的指纹，以确保您使用正确的主机进行连接。 ● Root Password：输入与主机通信所需的 root 密码。
启用以设置虚拟机维护原因	<p>如果选中此复选框，则当集群中的虚拟机从 Manager 关闭时会出现一个可选原因字段。这样，您可以解释维护，该维护将出现在日志中，以及虚拟机再次开机的时间。</p>
启用以设置主机维护原因	<p>如果选中此复选框，则当集群中的主机从 Manager 移到维护模式时会出现一个可选原因字段。这样，您可以解释维护，该维护将出现在日志中，以及主机再次激活的时间。</p>
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>

8.2.3. 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，您可以使用超过主机内核数的处理器内核总数运行虚拟机。这样做可启用以下内容：
 - 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 8.2. 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的虚拟机，且处理器内核总数大于主机中的内核数。</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>
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 第 8.2.9 节“更新集群中的主机上的 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>

8.2.4. 迁移策略设置说明

迁移策略定义了在主机的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 8.3. 迁移策略详细说明

策略	Description
legacy	3.6 版本的传统行为。 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。
post-copy migration	<p>虚拟机不应遇到任何与最小停机时间策略类似的停机时间。post-copy 策略首先尝试预复制来验证是否可能会发生聚合。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。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> <p>如果在 post-copy 阶段（如主机间迁移网络的网络故障）中出现错误，则迁移过程会产生不一致并暂停的虚拟机，结果会丢失虚拟机。因此，无法在 post-copy 阶段中止迁移。</p> <div style="background-color: #fff9c4; padding: 10px; border: 1px solid #ccc;"> <p style="text-align: center;"> 警告</p> <p>如果在完成 post-copy 进程前网络连接会破坏，Manager 会暂停，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，则不要使用 post-copy 迁移。</p> </div>
如果需要，挂起工作负载	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。

带宽设置定义每个主机传出和传入迁移的最大带宽。

表 8.4. 带宽详细说明

策略	Description
----	-------------

策略	Description
auto	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。
Hypervisor 默认	带宽由发送主机上的本地 VDSM 设置控制。
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 8.5. 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。

Additional Properties 仅适用于 Legacy 迁移策略。

表 8.6. 额外的属性说明

属性	Description
----	-------------

属性	Description
<p>自动聚合迁移</p>	<p>允许您设置在虚拟机迁移过程中使用 auto-convergence。具有高负载的大型虚拟机可以比实时迁移过程中实现的传输率快得多，并防止迁移聚合。QEMU 中的自动聚合功能允许您强制进行虚拟机迁移。QEMU 自动检测缺乏聚合并触发虚拟机上 vCPU 节流。auto-convergence 默认禁用。</p> <ul style="list-style-type: none"> ● 从全局设置中选择 Inherit 使用在全局级别设置的 auto-convergence 设置。默认选择这个选项。 ● 选择 Auto Converge 来覆盖全局设置，并允许虚拟机的自动集合。 ● 选择 Don't Auto Converge 来覆盖全局设置，并防止虚拟机的自动集合。
<p>启用迁移压缩</p>	<p>允许您设置是否在实时迁移过程中使用迁移压缩。此功能使用 Xor Binary Zero Run-Length-Encoding 以减少虚拟机停机时间，并减少了运行内存写入负载的虚拟机的实时迁移时间，或适用于具有稀疏内存更新模式的任何应用程序。默认全局禁用迁移压缩。</p> <ul style="list-style-type: none"> ● 从全局设置中选择 Inherit 使用在全局级别设置的压缩设置。默认选择这个选项。 ● 选择 Compress 覆盖全局设置并允许虚拟机的压缩。 ● 选择 Don't compress 以覆盖全局设置，并阻止虚拟机的压缩。

8.2.5. 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。有关调度策略的更多信息，请参阅 [第 1.3 节“调度策略”](#)。

表 8.7. 调度策略选项卡属性

字段	description/Action
----	--------------------

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"> ● none : 将策略值设置为 none, 使其在已经运行的虚拟机的主机间没有负载均衡或节能功能。这是默认模式。虚拟机已启动, 内存和 CPU 处理负载则均匀分布到集群中的所有主机上。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 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>根据所选的策略显示以下属性, 并可以根据需要编辑:</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, 以启用负载均衡。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, 才会启用负载均衡。 ● 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

字段	description/Action
	<p>虚拟机的插槽数量。SPM 主机的负载比其他主机轻的负载，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。</p> <ul style="list-style-type: none"> ● 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。 ● 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值低的 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 : 为最低服务级别设置 MB 所需的最小可用内存。如果主机的可用内存存在或低于这个值下运行, 则 Red Hat Virtualization Manager 会将虚拟机迁移到集群中的其他主机, 而主机的可用内存低于最低服务阈值。将 MaxFreeMemoryForOverUtilized 和 MinFreeMemoryForUnderUtilized 设置为 0 MB 可禁用基于内存的平衡。如果设置了 MaxFreeMemoryForOverUtilized, 则必须将 MinFreeMemoryForUnderUtilized 设置为避免意外行为。这是一个可选属性, 可添加到 power_saving 和 evenly_distributed 策略中。 ● MinFreeMemoryForUnderUtilized : 设置主机被视为使用不足前所需的最小可用内存 (以 MB 为单位)。如果主机的可用内存超过这个值, Red Hat Virtualization Manager 会将虚拟机迁移到集群中的其他主机, 并自动关闭主机机器, 并在负载均衡需要或集群中没有足够的空闲主机时重启它。将 MaxFreeMemoryForOverUtilized 和 MinFreeMemoryForUnderUtilized 设置为 0MB 可禁用基于内存的平衡。如果设置了

字段	MinFreeMemoryForUnderUtilized, 还必须 description/Action:FreeMemoryForOverUtilized 以避免意外行为。这是一个可选属性,可添加到 power_saving 和 evenly_distributed 策略中。
	<ul style="list-style-type: none"> ● 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机权重。
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。更多信息请参阅 第 12.9 节“可信计算池”。</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>
提供自定义序列号策略	<p>这个复选框允许您为集群中的虚拟机指定序列号策略。选择以下选项之一：</p> <ul style="list-style-type: none"> ● 主机 ID : 将主机的 UUID 设置为虚拟机的序列号。 ● VM ID : 将虚拟机的 UUID 设置为它的序列号。 ● 自定义序列号 : 允许您指定自定义序列号。

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。

8.2.6. 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 8.8. 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。
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]

8.2.7. 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 8.9. 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。

8.2.8. 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，请参阅第 8.2.5 节“调度策略设置说明”。

为主机设置负载和电源管理策略

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** 字段中启用负载平衡。
 - 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，请参阅第 15.3 节“在附加主机上为自托管引擎配置 Memory Slots 保留”。
 - **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. 在 **MinFreeMemoryForUnderUtilized** 中，在上述部分输入所需的最小可用内存（以 MB 为单位），虚拟机开始迁移到 **MinFreeMemoryForUnderUtilized** 中的其他主机。
 - d. 在下面输入最大需要可用内存，以 MB 为单位，虚拟机开始迁移至 **MaxFreeMemoryForOverUtilized** 中的其他主机。
 - e. （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，请参阅第 15.3 节“在附加主机上为自托管引擎配置 Memory Slots 保留”。
 - **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. 在 `MinFreeMemoryForUnderUtilized` 中，在上述部分输入所需的最小可用内存（以 MB 为单位），虚拟机开始迁移到 `MinFreeMemoryForUnderUtilized` 中的其他主机。
 - e. 在下面输入最大需要可用内存，以 MB 为单位，虚拟机开始迁移至 `MaxFreeMemoryForOverUtilized` 中的其他主机。
 - f. （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，请参阅第 15.3 节“在附加主机上为自托管引擎配置 Memory Slots 保留”。
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。
 7. （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。
 8. （可选）选择 **Provide custom serial number policy** 复选框来为集群中的虚拟机指定序列号策略，然后选择以下选项之一：
 - 选择 **Host ID**，将主机的 UUID 设置为虚拟机的序列号。
 - 选择 **Vm ID** 将虚拟机的 UUID 设为其序列号。
 - 选择 **Custom serial number**，然后在文本字段中指定自定义序列号。
 9. 点击 **OK**。

8.2.9. 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。在集群级别上对这些功能的更改仅在下次重新引导或处于维护模式后移至启动状态时才会传递给主机。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。

主机上同步 MoM 策略

1. 单击 **Compute → Clusters**。
2. 点集群名称打开详情视图。
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。

8.2.10. 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。

创建 CPU 配置集

1. 单击 Compute → Clusters。
2. 点集群名称打开详情视图。
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. 点击 OK。

8.2.11. 删除 CPU 配置集

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

删除 CPU 配置集

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

8.2.12. 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。

将现有的 Red Hat Gluster Storage 集群导入到 Red Hat Virtualization Manager

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。

8.2.13. 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 8.10. 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。

8.2.14. 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。

删除集群

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 确定

8.2.15. 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。

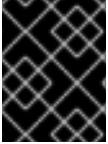
8.2.15.1. 内存优化和内存过量使用

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。请参阅第 8.2.3 节“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。

8.2.15.2. 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。

8.2.15.3. 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`）。

8.2.15.4. 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。将模块列入黑名单或卸载将禁用 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](#)。
- 红帽建议在增加虚拟机密度（经济）比性能更重要时，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[第 8.2.3 节“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[第 8.2.9 节“更新集群中的主机上的 MoM 策略”](#)。

8.2.15.5. 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](#)。
- 红帽建议在增加虚拟机密度（经济）比性能更重要时，红帽建议 KSM。

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[第 8.2.3 节“优化设置说明”](#)。

8.2.16. 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。



重要

要更改集群兼容性版本，您必须首先将集群中的所有主机更新为支持所需兼容性级别的级别。检查主机旁边是否存在指示有可用的更新的图标。

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。

更新集群的兼容性版本后，您必须通过从管理门户重启或使用 REST API（而不是从客户机操作系统中）来更新所有正在运行的或暂停虚拟机的集群兼容性版本。需要重新启动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 centers 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。

第 9 章 逻辑网络

9.1. 逻辑网络任务

9.1.1. 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

9.1.2. 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。

在数据中心或集群中创建新的逻辑网络

1. 点 Compute → Data Centers 或 Compute → Clusters。
2. 点数据中心或集群名称打开详情视图。
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 (可选)。
7. (可选) 禁用 VM Network。
8. (可选) 选择 Create on external provider 复选框。这禁用 Network Label、VM Network 和 MTU 选项。详情请查看 [第 14 章 外部供应商](#)。
9. 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。您可以通过在 External Provider 列表上选择 ovirt-provider-ovn 并离开 连接到物理网络 未选择来创建一个内部隔离网络。
10. 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。
11. 将 MTU 值设为 Default (1500) 或 Custom。
12. 如果您从 External Provider 下拉列表中选择了 ovirt-provider-ovn，请定义网络是否应该实施安全组。详情请查看 [第 9.1.7 节 “逻辑网络常规设置说明”](#)。
13. 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。
14. 如果选择了 外部提供程序上的 Create，则子网选项卡 将可见。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。
15. 在 vNIC Profiles 选项卡中，根据需要将 vNIC 配置集添加到逻辑网络中。
16. 点击 OK。

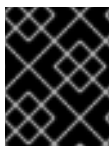
如果您为逻辑网络输入标签，则会自动添加到具有该标签的所有主机网络接口。



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。

9.1.3. 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 [第 9.4.2 节 “编辑主机网络接口并将逻辑网络分配给主机”](#) 如何同步您的网络。

编辑逻辑网络

1. 单击 Compute → Data Centers。
2. 点数据中心的名称打开详情视图。

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。

9.1.4. 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。

删除逻辑网络

1. 单击 **Compute → Data Centers**。
2. 点数据中心的名称打开详情视图。
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。

9.1.5. 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 以打开 Manage Network 窗口。
5. 为适当的集群选择默认路由复选框。
6. 点击 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"。

9.1.6. 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。

查看或编辑逻辑网络的网关

1. 单击 Compute → Hosts。
2. 点主机名打开详情视图。
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，然后单击铅笔图标以打开 编辑管理网络 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。

9.1.7. 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 9.1. 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>
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。
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。
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。
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。详情请查看 第 9.3.6 节“为逻辑网络和端口分配安全组” 。

9.1.8. 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 9.2. 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>

9.1.9. 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 9.3. 新的逻辑网络 设置

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 配置集的网络质量服务(QoS)配置集。</p>

9.1.10. 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。

为逻辑网络指定流量类型

1. 单击 Compute → Clusters。
2. 点集群名称打开详情视图。
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. 点击 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。

9.1.11. Manage Networks 窗口中的 Settings 解释

下表描述了 Manage Networks 窗口的设置。

表 9.4. 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ovirtmgmt）。

9.1.12. 编辑 NIC 上的虚拟功能配置



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)使单个 PCIe 端点用作多个单独的设备。这通过引入两个 PCIe 功能来实现：物理功能(PF)和虚拟功能(VF)。PCIe 卡可以有一个到 8 个 PF，但每个 PF 都可以支持多个 VF（依赖于该设备）。

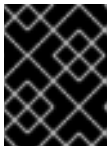
您可以通过 Red Hat Virtualization Manager 编辑支持 SR-IOV 功能的 Network Interface Controller (NIC)的配置，包括每个 NIC 上的 VF 数量，并指定允许访问 VF 的虚拟网络。

创建 VF 后，每个 VF 都可以视为独立 NIC。这包括为它们分配了一个或多个逻辑网络，使用它们创建绑定接口，直接将 vNIC 分配给它们以进行直接设备透传。

vNIC 必须启用 passthrough 属性才能直接附加到 VF。请参阅 [第 9.2.4 节“在 vNIC 配置文件中启用 Passthrough”](#)。

编辑 NIC 上的虚拟功能配置

1. 单击 Compute → Hosts。
2. 点击支持 SR-IOV 的主机的名称打开详情视图。
3. 点击 Network Interfaces 选项卡。
4. 单击 Setup Host Networks。
5. 选择支持 SR-IOV 的 NIC，使用  标记并点击铅笔图标。
6. 要编辑虚拟功能的数量，请点击 VFs 设置下拉菜单的数量，并编辑 VFs 文本字段的数量。



重要

更改 VF 的数量将在创建新 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. 默认选择 All Networks 复选框，允许所有网络访问虚拟功能。要指定允许访问虚拟功能的虚拟网络，请选择 Specific network 单选按钮来列出所有网络。然后，您可以选择所需网络的复选框，也可以使用 Labels 文本字段根据一个或多个网络标签自动选择网络。
8. 单击 OK。
9. 在 Setup Host Networks 窗口中，单击 OK。

9.2. 虚拟网络接口卡

9.2.1. 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。

9.2.2. 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。

创建或编辑 vNIC 配置集

1. 单击 Network → Networks。
2. 点击逻辑网络的名称打开详情视图。
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，请参阅第 9.2.4 节“[在 vNIC 配置文件中启用 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。

9.2.3. VM Interface Profile 窗口中的设置信息

表 9.5. 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。

字段名称	Description
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 vds-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 &lt;No Network Filter&gt; 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>
端口镜像	<p>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。</p>
设备自定义属性	<p>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。</p>
允许所有用户使用这个配置集	<p>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。</p>

9.2.4. 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](#)。

启用 Passthrough

1. 单击 Network → Networks。
2. 单击逻辑网络的名称打开详情视图。
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](#)中的第 9.4.2 节“编辑主机网络接口并将逻辑网络分配给主机”和[添加新网络接口](#)。

9.2.5. 删除 vNIC 配置集

删除 vNIC 配置集，将其从虚拟环境中删除。

删除 vNIC 配置集

1. 单击 Network → Networks。
2. 单击逻辑网络的名称打开详情视图。
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. 单击 OK。

9.2.6. 为 vNIC 配置集分配安全组



注意

只有将 OpenStack Networking (neutron) 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 OpenStack 创建安全组。有关更多信息，请参阅 Red Hat OpenStack Platform [用户和身份管理指南](#) 中的项目安全管理。

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

安全组是使用 OpenStack 网络实例中注册的安全组的 ID 标识。您可以在安装了 OpenStack Networking 的系统中运行以下命令来查找给定租户的安全组群 ID：

```
# neutron security-group-list
```

为 vNIC 配置集分配安全组

1. 单击 Network → Networks。
2. 点击逻辑网络的名称打开详情视图。
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。

9.2.7. 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。

9.2.8. 为 UCS 集成配置 vNIC 配置集

Cisco 的统一计算系统(UCS)用于管理数据中心，如计算、网络和存储资源。

`vdsm-hook-vmfex-dev` hook 允许虚拟机通过配置 vNIC 配置集连接到 Cisco 的 UCS 定义的端口配置文件。UCS 定义的端口配置集包含用于在 UCS 中配置虚拟接口的属性和设置。`vdsm-hook-vmfex-dev` hook 使用 VDSM 安装。如需更多信息，请参阅 [附录 A, VDSM 和 Hook](#)。

创建使用 vNIC 配置集的虚拟机时，它将使用 Cisco vNIC。

为 UCS 集成配置 vNIC 配置集的过程涉及首先配置自定义设备属性。在配置自定义 device 属性时，其中包含的现有值都会被覆盖。在合并新的和现有的自定义属性时，请在命令中包含用于设置密钥值的所有自定义属性。多个自定义属性由分号分隔。



注意

在配置 vNIC 配置集前，必须在 Cisco UCS 中配置 UCS 端口配置集。

配置自定义设备属性

1. 在 Red Hat Virtualization Manager 中，配置 `vmfex` 自定义属性并使用 `--cver` 设置集群兼容性级别。

```
# engine-config -s CustomDeviceProperties='{type=interface;prop={vmfex='^[a-zA-Z0-9_.-]{2,32}$}}' --cver=3.6
```

2. 验证 `vmfex` 自定义设备属性是否已添加。

```
# engine-config -g CustomDeviceProperties
```

3. 重新启动 `ovirt-engine` 服务。

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

用于配置的 vNIC 配置集可以属于新的或现有的逻辑网络。有关配置新逻辑网络的步骤，请参阅 [第 9.1.2 节 “在数据中心或集群中创建新的逻辑网络”](#)。

为 UCS 集成配置 vNIC 配置文件

1. 单击 **Network** → **Networks**。
2. 单击逻辑网络的名称打开详情视图。
3. 点 **vNIC Profiles** 选项卡。
4. 单击 **新建**，或选择 vNIC 配置集并点 **Edit**。
5. 输入配置文件的名称和描述。

6. 从自定义属性列表中选择 `vmfex` 自定义属性并输入 UCS 端口配置集名称。
7. 点击 OK。

9.3. 外部提供商网络

9.3.1. 从外部提供程序导入网络

要从外部网络提供程序(OpenStack 网络或实施 OpenStack Neutron REST API 的任何第三方供应商)使用网络, 请通过 Manager 注册该提供程序。如需更多信息, 请参阅[为网络置备添加 OpenStack Network Service Neutron](#) 或[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。

从外部提供程序导入网络

1. 单击 Network → Networks。
2. 点 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. 点 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](#)。

9.3.2. 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。

9.3.3. 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。

9.3.4. 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。

将子网添加到外部提供程序逻辑网络

1. 单击 Network → Networks。
2. 单击逻辑网络的名称打开详情视图。
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。

9.3.5. 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。

从外部提供程序逻辑网络中删除子网

1. 单击 Network → Networks。
2. 单击逻辑网络的名称打开详情视图。
3. 单击子网选项卡。
4. 选择子网，再单击删除。
5. 单击 OK。

9.3.6. 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。

为逻辑网络分配安全组

1. 单击 **Compute** → **Clusters**。
2. 点集群名称打开详情视图。
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**。更多信息请参阅 [第 9.1.2 节“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 [第 9.1.7 节“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。

9.4. 主机和网络

9.4.1. 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。

刷新主机功能

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。

9.4.2. 编辑主机网络接口并将逻辑网络分配给主机

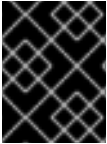
您可以更改物理主机网络接口的设置，将管理网络从一个物理主机网络接口移到另一个，并将逻辑网络分配到物理主机网络接口。也支持 `bridge` 和 `ethtool` 自定义属性。



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 [第 9.4.4 节“编辑主机的 VLAN 设置”](#)。



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。红帽建议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。

编辑主机网络接口并将逻辑网络分配给主机

1. 单击 Compute → Hosts。
2. 点主机名打开详情视图。
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，然后单击铅笔图标以打开编辑管理网络窗口。
 - 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。有关这些参数的详情请参考第 B.1 节“bridge_opts 参数的说明”。

```
forward_delay=1500
gc_timer=3765
group_addr=1:80:c2:0:0:0
group_fwd_mask=0x0
hash_elasticity=4
hash_max=512
hello_time=200
hello_timer=70
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：

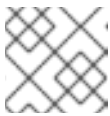
```
--coalesce em1 rx-usecs 14 sample-interval 3 --offload em2 rx on lro on tso off --change
em1 speed 1000 duplex half
```

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 [第 B.2 节“如何设置 Red Hat Virtualization 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=` 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 [第 B.3 节“如何设置 Red Hat Virtualization 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 [第 9.1.5 节“将非管理逻辑网络配置为默认路由”](#)。
- 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详情，请参考 [第 9.4.3 节“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. 单击 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。

9.4.3. 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。在主机的

Network Interfaces 选项卡中，无同步网络会出现 ，并在 Setup Host Networks 窗口中显示此图标 。

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。

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. 根据第 9.4.4 节“编辑主机的 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. 点主机名打开详情视图。
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，然后单击铅笔图标打开 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](#)。

9.4.4. 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。

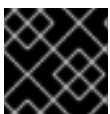
要保持网络同步，请执行以下操作：

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。

9.4.5. 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。

使用逻辑网络在网络接口中添加多个 VLAN

1. 单击 Compute → Hosts。
2. 点主机名打开详情视图。

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。

9.4.6. 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（例如 /etc/sysconfig/network-scripts/ifcfg-eth01）配置了多个 IP 地址，则只有第一个列出的 IP 地址才会被分配给主机网络。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 [附录 A, 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。

为主机网络分配额外的 IPv4 地址

1. 在您要为其配置额外 IPv4 地址的主机上，安装 VDSM hook 软件包。软件包默认在 Red Hat Virtualization 主机上可用，但需要在 Red Hat Enterprise Linux 主机上安装。

```
# yum 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_addrs=.'
```

3. 重启 `ovirt-engine` 服务：

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

4. 在管理门户中，点 `Compute` → `Hosts`。
5. 点主机名打开详情视图。
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 `5.5.5.5/24`）。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。

9.4.7. 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

在管理门户中添加网络标签

1. 单击 `Compute` → `Hosts`。
2. 点主机名打开详情视图。
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. 单击 `OK`。

使用 `LLDP Labeler` 服务添加网络标签

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。

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。

9.4.8. 更改主机的 FQDN

使用以下步骤更改主机的完全限定域名。

更新主机的 FQDN

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 [第 10.5.15 节“将主机移到维护模式”](#)。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 [第 10.5.1 节“在 Red Hat Virtualization Manager 中添加标准主机”](#)。

9.4.9. 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的动态 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。

9.4.10. 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。

9.4.10.1. 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

9.4.10.2. 设置并配置 SR-IOV

要设置和配置 SR-IOV，请完成以下任务。

1. [为 PCI 透传配置主机](#)
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 [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。
- RHV 版本 4.1 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

```

9.4.10.3. 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](#)

9.5. 网络绑定

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。

9.5.1. 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. 点主机名打开详情视图。
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。详情请查看 [第 9.5.3 节“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。具体步骤请查看 [第 9.4.2 节“编辑主机网络接口并将逻辑网络分配给主机”](#)。



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。

9.5.2. 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。

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
```

5. 将逻辑网络附加到新绑定并进行配置。具体步骤请查看 [第 9.4.2 节“编辑主机网络接口并将逻辑网络分配给主机”](#)。



注意

您不能直接将逻辑网络附加到绑定中的独立 NIC。

9.5.3. 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)

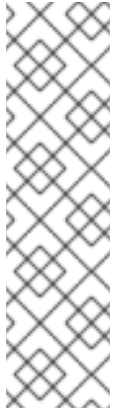
通过对源 MAC 地址和目的地 MAC 地址执行 XOR 操作来选择传输数据包的 NIC，乘以 NIC 总数的 `modulo`。此算法确保为每个目标 MAC 地址选择相同的 NIC。

(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
```

请参阅 <https://access.redhat.com/solutions/67546>。

Red Hat Virtualization 不支持以下绑定模式，因为它们无法用于桥接网络，因此与虚拟机逻辑网络不兼容：

(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 流量接收负载平衡相结合。ARP 协商用于平衡接收负载。

9.6. 分析和监控网络连接

9.6.1. Skydive 简介

Skydive 可用于监控逻辑网络，包括已定义为外部网络 [提供程序](#) 的 Open Virtual Networks (OVN)。Skydive 为您提供了网络拓扑、依赖性和流的实时视图，生成报告并执行配置审计。

您可以使用 Skydive 提供的数据来：

- 检测数据包丢失
- 通过捕获集群的网络拓扑，包括桥接和接口，检查您的部署是否正常工作
- 检查是否正确应用了预期的 MTU 设置
- 在虚拟机和主机之间捕获网络流量

有关 Skydive 功能集的更多信息，请参阅 <http://skydive.network>。



注意

Skydive 只是一个技术预览功能。技术预览功能不包括在红帽生产服务级别协议 (SLA) 中，且其功能可能并不完善。因此，红帽不建议在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

如需红帽技术预览功能支持范围的更多信息，请参阅 <https://access.redhat.com/support/offerings/techpreview/>。

9.6.2. 安装 Skydive

流程

1. 在 Manager 机器上安装 skydive-ansible:

```
# yum --disablerepo="*" --enablerepo="rhel-7-server-rpms,rhel-7-server-extras-rpms,rhel-7-server-rh-common-rpms,rhel-7-server-openstack-14-rpms" install skydive-ansible
```

2. 将 `/usr/share/ovirt-engine/playbooks/install-skydive.inventory.sample` 复制到当前目录并将其重命名为 `inventory`。
3. 按如下方式修改 `inventory/01_hosts` 文件 (请参阅以下的完整内容) :
 - a. 使用 Manager 的 FQDN 更新 `skydive_os_auth_url`。OVN 使用与 Manager 相同的 FQDN 来使用。
 - b. 使用用于 OVN 提供程序的用户名更新 `ovn_provider_username`。默认值在 `/etc/ovirt-provider-ovn/ovirt-provider-ovn.conf` 中定义。
 - c. 更新 `ovn_provider_password`。
 - d. 在 `[agents:children] <host_group >` 下, 定义您要在其上安装 Skydive 代理的主机、群集或数据中心。
您可以运行以下命令来查看有效的组列表 :

```
/usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-inventory | python -m json.tool
```



注意

不需要显式列出每个主机。要在集群中的所有主机上安装代理, 请添加 `ovirt_cluster_Default`。另外, 若要在数据中心中的所有主机上安装代理, 请添加 `ovirt_datacenter_Default`。

清单文件示例

```
[agents]
[analyzers]
[skydive:children]
  analyzers
  agents

[skydive:vars]
skydive_listen_ip=0.0.0.0
skydive_deployment_mode=package
skydive_extra_config={'agent.topology.probes': ['ovsdb', 'neutron'],
'agent.topology.neutron.ssl_insecure': true}

skydive_fabric_default_interface=ovirtmgmt

skydive_os_auth_url=https://MANAGERS_FQDN:35357/v2.0
skydive_os_service_username=ovn_provider_username
skydive_os_service_password=ovn_provider_password
```

```

skydive_os_service_tenant_name=service
skydive_os_service_domain_name=Default
skydive_os_service_region_name=RegionOne

[agents:vars]
ansible_ssh_private_key_file=/etc/pki/ovirt-engine/keys/engine_id_rsa

[agents:children]
host_group

[analyzers]
localhost ansible_connection=local

```

4. 运行 playbook :

```

# ansible-playbook -i inventory /usr/share/ovirt-engine/playbooks/install-skydive.yml
/usr/share/skydive-ansible/playbook.yml.sample

```

5. 通过转至 `http://MANAGERS_FQDN:8082`，选择虚拟机，并检查 Capture 选项卡的 Metadata 部分中的以下字段，验证 Skydive 识别虚拟机的端口：

- Manager: Neutron
- networkName: network_name
- IPV4 : IP_address, 如果使用子网

请参阅 [第 9.6.3 节“使用 Skydive 测试网络连接”](#) 查看如何使用 Skydive 捕获您的网络活动示例。

9.6.3. 使用 Skydive 测试网络连接

本例测试两个使用 IPv4 地址的 NIC 间的连接。NIC 连接到标记为 VLAN 4 的逻辑网络。有关为逻辑网络分配 IP 地址的详情，请参考 [第 9.4.2 节“编辑主机网络接口并将逻辑网络分配给主机”](#)。

流程

1. [安装 Skydive](#).
2. Open Skydive from `http://MANAGERS_FQDN:80 82`.
3. 在网络映射中，选择 rhv-host1 上的 network_4。
4. 单击 Capture 选项卡中的 Create，再单击 Start。
5. 对 rhv-host0 上的 network_4 重复前面的步骤。
6. 点 Generate 标签页。
7. 在 rhv-host0 上选择 eth0 作为 Source，选择 rhv-host1 上的 eth0 作为目标。
8. 从 Type 下拉列表中，选择 ICMPv4/Echo Request。
9. 单击 Inject 以注入数据包。
10. 打开 Flows 选项卡。ping 的结果会显示在表中。如果 ping 成功，则会显示包含 ICMPv4 的行和源 IP 地址。当您在该行上移动光标时，network_4 将突出显示在网络地图上带有黄色圆圈。

有关使用 Skydrive 的更多信息，请参阅 [Skydrive 文档](#)。

对于安装是 :Testing!

第 10 章 主机

10.1. 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打开详情视图，并在 Red Hat Virtualization Manager 中识别单个主机的主机类型，方法是选择主机名以打开详情视图，并在软件 下检查 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 7 性能调优指南](#)。

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>

10.2. 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，如配置网络和部署自托管引擎，也可用于通过终端子选项卡运行终端命令。

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。

RHVH 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

红帽建议不要在 RHVH 上创建不受信任的用户，因为这可能导致利用本地安全漏洞。

10.3. 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（如配置网络和部署自托管引擎）之前执行的任务提供了一个图形用户界面，也可用于通过 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。

10.4. 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。

10.5. 主机任务

10.5.1. 在 Red Hat Virtualization Manager 中添加标准主机

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



重要

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

流程

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

10.5.2. 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。

添加 Satellite 主机提供程序主机

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，然后选择要从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. 单击确定以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**。

10.5.3. 为主机配置 Satellite 勘误管理

Red Hat Virtualization 可以配置为查看 Red Hat Satellite 的勘误。这可让主机管理员在用于管理主机配置的同时仪表板中接收有关可用勘误表的更新及其重要性。有关 Red Hat Satellite 的更多信息，请参阅 [Red Hat Satellite 文档](#)。

Red Hat Virtualization 4.3 支持使用 Red Hat Satellite 6.5 进行勘误管理。



重要

主机在卫星服务器中通过其 FQDN 识别。使用 IP 地址添加的主机将无法报告勘误表。这样可确保外部内容主机 ID 不需要在 Red Hat Virtualization 中维护。

用于管理主机的卫星帐户必须具有管理员权限和默认的组织。

为主机配置 Satellite 勘误管理

1. 将卫星服务器添加为外部提供程序。如需更多信息，请参阅 [第 14.2.1 节“为主机调配添加 Red Hat Satellite 实例”](#)。
2. 将所需的主机与卫星服务器关联。



注意

主机必须注册到 Satellite 服务器，并安装了 `katello-agent` 软件包。

有关如何配置主机注册以及如何注册主机并安装 `katello-agent` 软件包的详情，请参考 Red Hat Satellite 管理主机 文档中的 [注册主机](#)。

- a. 单击 `Compute` → `Hosts`，再选择主机。
- b. 点 `Edit`。
- c. 选中 `Use Foreman/Satellite` 复选框。
- d. 从下拉列表中选择所需的 Satellite 服务器。
- e. 点击 `OK`。

现在，主机已配置为显示在用于管理主机配置的另一仪表盘中可用的勘误表及其重要。

10.5.4. New Host 和 Edit Host Windows 中的设置和控件的说明

10.5.5. 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 10.1. 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。

字段名称	Description
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(IPv4 和 IPv6)以匹配主机的管理网络(IPv4 和 IPv6)。
密码	主机的 root 用户的密码。这只能在添加主机时指定，它不能对其进行编辑。
SSH 公钥	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。
自动配置主机防火墙	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。这会被默认启用。这是一个 高级参数 。
SSH 指纹	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 。

10.5.6. 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 10.2. 电源管理设置

字段名称	Description
启用电源管理	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。
kdump 集成	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。如果情况如此，请参阅 第 10.6.4 节“fence_kdump 高级配置” 。
禁用电源管理的策略控制	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。
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 下拉列表中选择一个隔离代理。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	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。
电源管理代理首选项	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。

下表包含 `Edit fence agent` 窗口中所需的信息。

表 10.3. 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。
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。

字段名称	Description
服务配置文件	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>
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。

10.5.7. 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 10.4. 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 。

10.5.8. 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 10.5. 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。

10.5.9. 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。

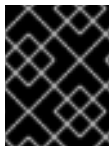
表 10.6. *Network Provider* 设置

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。

10.5.10. 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](#)。

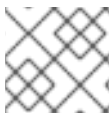


重要

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 10.7. 内核 设置

字段名称	Description
hostdev Passthrough 和 SR-IOV	在内核中启用 IOMMU 标志，允许虚拟机使用主机设备，就像设备是直接连接到虚拟机本身的设备一样。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，以便您在虚拟机中运行虚拟机。这个选项仅用于评估目的，不支持用于生产目的。主机上必须安装 <code>vdsm-hook-nestedvt</code> hook。
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。
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**。

10.5.11. 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 10.8. 托管引擎设置

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。

10.5.12. 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](#)。

配置电源管理设置

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 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。

10.5.13. 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。

配置 SPM 设置

1. 单击 Compute → Hosts。
2. 点 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。

10.5.14. 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

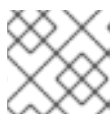
- 确保主机硬件满足 PCI 设备直通和分配的要求。如需更多信息，请参阅[PCI 设备要求](#)。

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 `intel_iommu=on` 或 `amd_iommu=on` 可以正常工作，您可以尝试添加 `iommu=pt` 或 `amd_iommu=pt`。pt 选项只为用于透传的设备启用 IOMMU，并提供更好的主机性能。但是，该选项可能并不在所有硬件上受到支持。如果 pt 选项不适用于您的主机，则恢复为上一选项。

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

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

2. 刷新 `grub.cfg` 文件并重启主机以使这些更改生效：

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

# reboot
```

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

10.5.15. 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` 以打开 `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。



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 [第 8.2.2 节“常规集群设置说明”](#)。

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。

10.5.16. 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。

从维护模式激活主机

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。

10.5.17. 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**，而不是 **iptables**。



注意

iptables 已被弃用。

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。

10.5.18. 删除主机

从虚拟环境中删除主机。

删除主机

1. 单击 `Compute → Hosts`，再选择主机。
2. 单击 `Management → Maintenance`。
3. 当主机处于维护模式时，点 `Remove` 打开 `Remove Host (s)` 确认窗口。
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`。

10.5.19. 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。

10.5.19.1. 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。如需有关用于自动更新的 Ansible 角色的更多信息，请参阅 <https://github.com/oVirt/ovirt-ansible-cluster-upgrade/blob/master/README.md>。

红帽建议一次更新一个集群。

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。
- 如果在集群级别启用了迁移，虚拟机会自动迁移到集群中的其他主机。

- 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。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

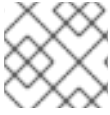
1. 在管理门户中，点 Compute → Clusters 并选择集群。
2. 单击 Upgrade。
3. 选择要更新的主机，然后单击 Next。
4. 配置选项：
 - Stop Pinned VMs 会关闭固定到集群中主机的任何虚拟机，这个选项被默认选择。您可以清除此复选框以跳过更新这些主机，从而使固定虚拟机保持运行，例如当固定虚拟机运行重要服务或进程时，您不希望它在更新过程中在未知时间关闭。
 - Upgrade Timeout (Minutes) 设置在集群升级失败并显示超时前等待各个主机更新的时间。默认值为 60。您可以为可能不足 60 分钟的大型集群增加它，或者为主机快速更新的小型集群减少它。
 - 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。
 - 使用维护策略 在更新过程中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. 检查将受影响的主机和虚拟机的摘要。
7. 单击 Upgrade。

您可以在 Compute → Hosts 视图中跟踪主机更新的进度，以及通知 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。

10.5.19.2. 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。
- 如果在集群级别启用了迁移，虚拟机会自动迁移到集群中的其他主机。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。
- 不要同时更新所有主机，因为一个主机必须保持可用以执行存储池管理程序 (SPM) 任务。
- 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的列表，请运行 `yum repolist`。

- 对于 Red Hat Virtualization 主机：

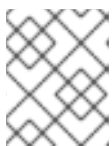
```
# subscription-manager repos --enable=rhel-7-server-rhvh-4-rpms
```

- 对于 Red Hat Enterprise Linux 主机：

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

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 (🔔)，再展开 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。

红帽建议从管理门户更新主机。但是，您可以使用 `yum update` 更新主机：

10.5.19.3. 手动更新主机

您可以使用 `yum` 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。
- 如果在集群级别启用了迁移，虚拟机会自动迁移到集群中的其他主机。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。
- 不要同时更新所有主机，因为一个主机必须保持可用以执行存储池管理程序 (SPM) 任务。
- 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 `yum repolist` 检查当前启用哪些软件仓库。

- 对于 Red Hat Virtualization 主机：

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

- 对于 Red Hat Enterprise Linux 主机：

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

2. 在管理门户中，点 **Compute** → **Hosts** 并选择要更新的主机。
3. 单击 **Management** → **Maintenance**。
4. 更新主机：

```
# yum update
```

5. 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。

10.5.20. 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。

先决条件

- 如果在集群级别启用了迁移，则虚拟机会自动迁移到集群中的其他主机。因此，建议在主机使用相对较低的时执行主机重新安装。
- 确保集群有足够的内存，以便其主机执行维护。如果集群缺少足够内存，虚拟机迁移操作将挂起，然后失败。您可以在将主机移到维护之前，通过关闭一些或所有虚拟机来减少此操作的内存用量。
- 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，因为一个主机必须保持可用才能执行存储池管理器(SPM)任务。

流程

1. 单击 `Compute` → `Hosts`，再选择主机。
2. 单击 `Management` → `Maintenance`。
3. 单击 `Installation` 以打开 `Install Host` 窗口。
4. 单击确定以重新安装主机。

成功重新安装后，主机会显示 `Up` 状态。任何从主机迁移的虚拟机现在都可以迁移到该主机。



重要

在 Red Hat Virtualization Manager 成功注册到 Red Hat Virtualization Manager 后，它可能会错误地出现在管理门户中，状态为 `Install Failed`。单击 `Management` → `Activate`，主机将更改为 `Up` 状态并可供使用。

10.5.21. 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 [第 10.5.3 节“为主机配置 Satellite 勘误管理”](#)

查看主机勘误

1. 单击 `Compute` → `Hosts`。
2. 点主机名打开详情视图。

3. 点 **Errata** 选项卡。

10.5.22. 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：

要查看有关主机健康状态的更多详情，请单击主机名以打开详情视图，然后单击 **Events** 选项卡。

也可以使用 REST API 查看主机的健康状态。主机上的 **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 中设置主机健康状态。如需更多信息，请参阅 REST API 指南中的 [添加事件](#)。

10.5.23. 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。

有关直接设备分配的硬件要求的更多信息，请参阅 [实施 SR-IOV 时硬件分配的其他硬件注意事项](#)。

有关配置主机以进行直接设备分配的详情，请参考 [第 10.5.14 节“为 PCI Passthrough 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。

查看主机设备

1. 单击 **Compute** → **Hosts**。
2. 点主机名打开详情视图。
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。

10.5.24. 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。

从管理门户访问 Cockpit

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。

10.5.25. 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 -l hostname /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

另外，您还可以将 `--extra-vars` 选项与变量 `host_deploy_spice_cipher_string` 使用 Ansible playbook `ovirt-host-deploy` 重新配置主机，如下所示：

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

10.6. 主机弹性

10.6.1. 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、负载平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 `PMHealthCheckIntervalInSec`（默认为 3600 sec）`engine-config` 选项。

当设置为 `true` 时，`PackpmHealthCheckEnabled` 会按照 `PMHealthCheckIntervalInSec` 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，请参阅第 22.2.2 节“`engine-config` 命令的语法”。

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。

10.6.2. 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。

10.6.3. 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。电源管理使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。

在主机上设置隔离参数

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 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。



注意

有关如何设置自定义电源管理设备的详情请参考 <https://access.redhat.com/articles/1238743>。

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. 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 **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。

10.6.4. 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, 其中一个是面向公众的, 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。有关 fence_kdump 侦听器的配置选项, 请参阅 [fence_kdump 侦听器配置](#)。有关在 Manager 上配置 kdump, 请参阅在 Manager [中配置 fence_kdump](#)。

10.6.4.1. fence_kdump listener Configuration

编辑 fence_kdump 侦听器的配置。这只在默认配置不够时才需要。

手动配置 fence_kdump Listener

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

如第 10.6.4.2 节“在 Manager 上配置 fence_kdump”的 fence_kdump Listener 配置选项表中所述, 还必须在 engine-config 中更改编辑的值。

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 10.9. fence_kdump Listener Configuration Options

变量	Description	默认	备注
LISTENER_ADDRESS	定义要接收 fence_kdump 消息的 IP 地址。	0.0.0.0	如果更改了此参数的值，它必须与 engine-config 中的 FenceKdumpDestinationAddress 的值匹配。
LISTENER_PORT	定义要接收 fence_kdump 消息的端口。	7410	如果更改了此参数的值，它必须与 engine-config 中的 FenceKdumpDestinationPort 的值匹配。
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。

10.6.4.2. 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
```

使用 engine-config 手动配置 Kdump

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。请参阅第 10.6.4.1 节“`fence_kdump listener Configuration`”。

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 10.10. `kdump` 配置选项

变量	Description	默认	备注
<code>FenceKdumpDestinationAddress</code>	定义要向发送 <code>fence_kdump</code> 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 <code>fence_kdump</code> 侦听器配置文件中的 LISTENER_ADDRESSES 的值匹配，且所有启用了 <code>Kdump</code> 集成的所有主机都需要被重新安装。
<code>FenceKdumpDestinationPort</code>	定义将 <code>fence_kdump</code> 消息发送到的端口。	7410	如果更改了此参数的值，它必须与 <code>fence_kdump</code> 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 <code>Kdump</code> 集成的所有主机。
<code>FenceKdumpMessageInterval</code>	定义 <code>fence_kdump</code> 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 <code>fence_kdump</code> 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 <code>Kdump</code> 集成的所有主机。
<code>FenceKdumpListenerTimeout</code>	定义最后心跳后的最大超时时间（以秒为单位），以考虑 <code>fence_kdump</code> 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 <code>fence_kdump</code> 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。

10.6.5. 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）+ [DelayResetPerVmlnSeconds（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。

10.6.6. 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。

使用主机电源管理功能

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。

10.6.7. 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

不要使用 Confirm host has been rebooted 选项，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。

手动隔离或隔离不响应的主机

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，选择主机并点击 More Actions (⋮)，然后点 Confirm 'Host has 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
```

第 11 章 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)
- GlusterFS exports
- 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，您需要为虚拟化企业创建、配置、附加和维护存储。您应该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 存储管理指南](#)，以了解有关概念、协议、要求或常规存储使用方法的更多信息。

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：

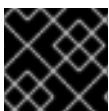
- **数据域：** 一个数据域在数据中心中保存所有虚拟机和模板的虚拟硬盘和 OVF 文件。另外，虚拟机的快照也存储在数据域中。
数据域无法在数据中心之间共享。可向同一数据中心添加多个类型的数据域 (iSCSI、NFS、FC、POSIX 和 Gluster)，它们都是共享的，而不是本地域。

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。有关导入存储域的详情，请参考 [第 11.7 节“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。

11.1. 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。

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，请查看 Red Hat Enterprise Linux Logical Volume Manager 管理指南。

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。

11.2. 准备和添加 NFS 存储

11.2.1. 准备 NFS 存储

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

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

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

Red Hat Virtualization 需要特定的系统用户帐户和系统用户组，以便管理器可以将数据存储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。

流程

1. 创建组 `kvm` :

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

2. 在组 `kvm` 中创建用户 `vdsm` :

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

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

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

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

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

11.2.2. 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

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

11.2.3. 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，请参阅第 11.2.2 节“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。

增加现有 NFS 存储域

1. 点 Storage → Domains。
2. 点击 NFS 存储域的名称打开详情视图。
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](#)。
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。

11.3. 准备和添加本地存储

11.3.1. 准备本地存储

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



重要

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

为 Red Hat Enterprise Linux 主机准备本地存储

1. 在主机上，创建要用于本地存储的目录：

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

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

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

为 Red Hat Virtualization 主机准备本地存储

红帽建议在逻辑卷中创建本地存储，如下所示：

1. 创建本地存储目录：

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

2. 挂载新的本地存储，然后修改权限和所有权：

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

11.3.2. 添加本地存储

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

流程

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

您的主机在其所在的数据中心上线。

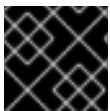
11.4. 准备和添加兼容 POSIX 的文件系统存储

11.4.1. 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。

11.4.2. 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 兼容文件系统存储域作为数据域附加到 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。

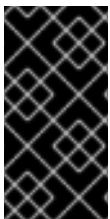
7. 输入 POSIX 文件系统的路径，因为您通常会将其提供给 `mount` 命令。
8. 输入 VFS 类型，因为您通常会使用 `-t` 参数将其提供给 `mount` 命令。有关有效 VFS 类型的列表，请参阅 `man mount`。
9. 输入其他挂载选项，因为您通常使用 `-o` 参数将它们提供给 `mount` 命令。挂载选项应以逗号分隔列表形式提供。有关有效挂载选项列表，请参阅 `man mount`。
10. 另外，您还可以配置高级参数。
 - a. 点 Advanced Parameters。
 - b. 在 Warning Low Space Indicator 字段中输入百分比值。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。

11.5. 准备和添加块存储

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



重要

如果您使用的是块存储，并且打算在裸设备上部署虚拟机或直接 LUN 并用逻辑卷管理器 (LVM) 管理它们，您必须创建一个过滤器来隐藏 guest 逻辑卷。这将防止在主机引导时激活 guest 逻辑卷，这种情况可能会导致逻辑卷过时并导致数据崩溃。详情请查看 <https://access.redhat.com/solutions/2662261>。



重要

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

重要

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

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

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

11.5.2. 添加 iSCSI 存储

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

流程

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

重要

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

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

**注意**

在环境外部使用的 LUN 也会显示。

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

- b. 在 Address 字段中输入 iSCSI 主机的 FQDN 或 IP 地址。
- c. 在 Port 字段中，输入在浏览目标时要连接到主机的端口。默认值为 3260。

- d. 如果使用 CHAP 保护存储，请选中 User Authentication 复选框。输入 CHAP 用户名和 CHAP 密码。



注意

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

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



重要

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

8. 点所需目标旁边的 + 按钮。这会展开条目并显示附加到目标的所有未使用的 LUN。
9. 选中您正在使用的每个 LUN 的复选框，以创建存储域。
10. 另外，您可以配置高级参数：
- 点 Advanced Parameters。
 - 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。
 - 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。
 - 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。
 - 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。

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

11.5.3. 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](#)
 - [在与 iSCSI 绑定中的其他逻辑网络相同的 VLAN 和子网中分配静态 IP 地址](#)

流程

1. 单击 [Compute](#) → [Data Centers](#)。
2. 点 [数据中心名称](#) 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](#)。

11.5.4. 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](#) 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. 单击 [Add Network](#) 以打开 [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，然后单击 [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. 单击 [主机名](#) 以打开详情视图。

- 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 的铅笔图标以打开 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, 然后单击确定。
4. 创建 iSCSI 绑定 :
- a. 单击 Compute → Data Centers。
 - b. 点数据中心名称打开详情视图。
 - 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, 然后单击确定。

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。

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



重要

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

重要

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

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

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

11.5.6. 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。

11.5.7. 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 [第 11.5.2 节“添加 iSCSI 存储”](#)。
- 通过重新定义底层 LUN 的大小扩展存储域。

有关在 Red Hat Enterprise Linux 7 系统中创建、配置或调整 iSCSI 存储大小的详情，请参考 [Red Hat Enterprise Linux 7 存储管理指南](#)。

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** > **LUN** 并点 **Discover Targets expansion** 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** 并选择新可用 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. 单击 LUNs > Targets。
4. 在 Additional Size 列中，点 LUN 的 Add Additional_Storage_Size 按钮刷新。
5. 单击 OK 刷新 LUN 以指示新的存储大小。

11.5.8. 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：

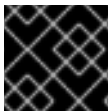
```
Physical device initialization failed. Please check that the device is empty and accessible by the host.
```

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。

从 LUN 清除分区表



重要

您必须在正确的 LUN 上运行此步骤，以便不会意外破坏数据。

使用您要重复使用的 LUN ID、一次读取和写入的最大字节数以及要复制的输入块的数量，运行 dd 命令：

```
# dd if=/dev/zero of=/dev/mapper/LUN_ID bs=1M count=200 oflag=direct
```

11.6. 准备和添加红帽 GLUSTER 存储

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

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

11.7. 导入现有存储域

11.7.1. 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

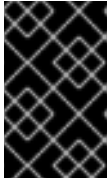
将存储域附加到目标 Data-Center 时，它可能会升级到较新的存储域格式，且可能无法重新连接到源 Data-Center。这会破坏使用 Data-Domain 作为导出域的替代。

11.7.2. 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. 从主机下拉列表选择一个主机。



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，用于指定存储域详细的字段。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. 单击 **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

- [第 11.7.5 节“从导入的 Data Storage Domains 导入虚拟机”](#)
- [第 11.7.6 节“从导入的 Data Storage Domains 导入模板”](#)

11.7.3. 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。

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。



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。

11.7.4. 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。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](#)。

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. 点存储域的名称打开详情视图。
5. 点 Data Center 选项卡。
6. 点 Maintenance。



重要

不要选中 Ignore OVF 更新失败 复选框。存储域中的维护操作应该更新 OVF。

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。

11.7.5. 从导入的 Data Storage Domains 导入虚拟机

从您导入到 Red Hat Virtualization 环境中的数据存储域中将虚拟机导入到一个或多个集群中。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. 点导入的存储域的名称打开详情视图。
3. 单击 VM Import 选项卡。
4. 选择要导入的一个或多个虚拟机。
5. 点 Import。
6. 对于 Import Virtual Machine(s) 窗口中的每个虚拟机，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. 单击 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 Virtual Machine(s) 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. 单击 OK。
8. 如果检测到 MAC 地址冲突，虚拟机名称旁边会出现一个感叹号。将鼠标悬停在图标上，以查看显示所发生的错误类型的工具提示。
选中 Reassign Bad MACs 复选框，将新 MAC 地址重新分配给所有有问题的虚拟机。或者，您也可以选中每个虚拟机的 Reassign 复选框。



注意

如果没有可分配的地址，导入操作将失败。但是，如果 MAC 地址位于集群的 MAC 地址池范围之外，可以在不重新分配新的 MAC 地址的情况下导入虚拟机。

9. 单击 OK。

导入的虚拟机不再显示在 VM Import 选项卡下的列表中。

11.7.6. 从导入的 Data Storage Domains 导入模板

从您导入 Red Hat Virtualization 环境中的数据存储空间中导入模板。此流程假设导入的数据存储空间已附加到数据中心，并已激活。

流程

1. 点 Storage → Domains。
2. 点导入的存储域的名称打开详情视图。
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. 单击 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. 单击 OK。
8. 单击 OK。

导入的模板将不再显示在模板导入选项卡下的列表中。

11.8. 存储任务

11.8.1. 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。

先决条件

上传功能使用 HTML 5 API，这需要您的环境包含以下内容：

- 镜像 I/O 代理([ovirt-imageio-proxy](#))，使用 [engine-setup](#) 配置。详情请参阅 [配置 Red Hat Virtualization Manager](#)。
- 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。

上传镜像至数据存储域

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 [第 13.6.2 节“New Virtual Disk Window 中的设置说明”](#)。
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。

增加上传超时值

1. 如果上传超时并看到消息 Reason: timeout due to transfer inactivity, 则增加超时值：

```
# engine-config -s TransferImageClientInactivityTimeoutInSeconds=6000
```

2. 重启 ovirt-engine 服务：

```
# systemctl restart ovirt-engine
```

11.8.2. 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主数据域。



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。

将存储域移到维护模式

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。



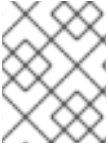
注意

您还可以在与其关联的数据中心的详情视图中使用 Storage 选项卡激活、分离和将域置于维护模式。

11.8.3. 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。请参阅更新 REST API 指南中的存储连接。

编辑 Active Storage 域

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. 点存储域的名称打开详情视图。
 - b. 点 Data Center 选项卡。
 - c. 点 Activate。

11.8.4. 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 OVFs。

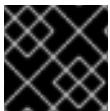
更新 OVF

1. 点 Storage → Domains。
2. 选择存储域并点击 More Actions (⋮)，然后点 Update OVFs。
OVF 已更新，并显示在 Events 中。

11.8.5. 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. 点一个不活跃存储域的名称打开详情视图。
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。

11.8.6. 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。

将存储域从数据中心分离

1. 点 Storage → Domains。
2. 点存储域的名称打开详情视图。
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。

11.8.7. 将存储域附加到数据中心

将存储域连接到数据中心。

将存储域附加到数据中心

1. 点 Storage → Domains。
2. 点存储域的名称打开详情视图。
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。

11.8.8. 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. 点击 **OK**。

存储域已从环境中永久移除。

11.8.9. 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。

销毁存储域

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. 点击 **OK**。

11.8.10. 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。

创建磁盘配置集

1. 点 Storage → Domains。
2. 点数据存储域的名称打开详情视图。
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。

11.8.11. 删除磁盘配置集

从 Red Hat Virtualization 环境中删除现有磁盘配置集。

删除磁盘配置集

1. 点 Storage → Domains。
2. 点数据存储域的名称打开详情视图。
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. 点击 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。

11.8.12. 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以打开详情视图，然后单击 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](#)。

11.8.13. 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](#)。

11.8.14. 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。

当主机数量上限为 250 时，Sanlock 分配的锁定空间区域为 1 MB。当您在启用 4K 存储时增加主机的最大数量时，锁定空间区域会较大。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
```

11.8.15. 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。

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
```

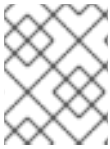
第12章 池

12.1. 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。

12.2. 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”。

创建虚拟机池

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 下拉列表为 Desktop 或 Server 优化虚拟机。



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 12.1. 池名称和虚拟机编号示例

- pool: MyPool
虚拟机 : MyPool-1, MyPool-2, ... MyPool-10
- 池 : 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 12.2. 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 12.3. 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 虚拟机是否使用 unattend 文件连接的软盘设备，例如 `A:\Unattend.xml`。
2. 点 Start，点 Run，在 Open 文本框中键入 `regedit`，然后点 OK。
3. 在左侧窗格中，前往 `HKEY_LOCAL_MACHINE → SYSTEM → 设置`。
4. 右键单击右侧窗格并选择 `New → String Value`。
5. 输入 `UnattendFile` 作为密钥名称。
6. 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。
7. 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。

12.3. 新池和编辑池 WINDOWS 中的设置和控制的说明

12.3.1. 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 12.1. 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《 虚拟机管理指南 》中的“ 新建模板和编辑模板 Windows ”中的“ 虚拟机常规设置说明 ”和 说明 设置。
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。

字段名称	Description
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。

12.3.2. 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 12.2. 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。

12.3.3. 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 12.3. 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。

字段名称	Description
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>

12.3.4. 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 12.4. 虚拟机池：主机设置

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。
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。

字段名称	子元素	Description
	使用自定义迁移策略	<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"> ● Legacy - 3.6 版本的传统行为。vdsm.conf 中的覆盖仍在应用。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 QEMU 迭代，且最多为 500 毫秒），迁移将中止。客户机代理 hook 机制已启用。 ● 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。
	使用自定义迁移停机时间	<p>此复选框允许您指定在实时迁移期间虚拟机可以下线的最大毫秒数。根据工作负载和 SLA 要求为每个虚拟机配置不同的停机时间。输入 0 以使用 VDSM 默认值。</p>

字段名称	子元素	Description
	自动聚合迁移	<p>只有使用 传统迁移策略 激活。允许您设置在虚拟机实时迁移过程中是否使用 auto-convergence。具有高负载的大型虚拟机可以比实时迁移过程中实现的传输率快得多，并防止迁移聚合。QEMU 中的自动聚合功能允许您强制进行虚拟机迁移。QEMU 自动检测缺乏聚合并触发虚拟机上 vCPU 节流。auto-convergence 默认禁用。</p> <ul style="list-style-type: none"> ● 从 cluster 设置中选择 Inherit，以使用在集群级别上设置的自动协调设置。默认选择这个选项。 ● 选择 Auto Converge 来覆盖集群设置或全局设置，并为虚拟机允许自动协调。 ● 选择 Don't Auto Converge 来覆盖集群设置或全局设置，并阻止虚拟机的自动协调。
	启用迁移压缩	<p>只有使用 传统迁移策略 激活。选项允许您设置在虚拟机实时迁移过程中是否使用迁移压缩。此功能使用 Xor Binary Zero Run-Length-Encoding 以减少虚拟机停机时间，并减少了运行内存写入负载的虚拟机的实时迁移时间，或适用于具有稀疏内存更新模式的任何应用程序。默认全局禁用迁移压缩。</p> <ul style="list-style-type: none"> ● 从集群设置中选择 Inherit，使用在集群级别上设置的压缩设置。默认选择这个选项。 ● 选择 Compress 来覆盖集群设置或全局设置，并允许虚拟机的压缩。 ● 选择 Don't compress 来覆盖集群设置或全局设置，并阻止虚拟机的压缩。
	透传主机 CPU	<p>此复选框允许虚拟机利用所处主机的物理 CPU 的功能。</p>

字段名称	子元素	Description
配置 NUMA	NUMA 节点数	分配给虚拟机的虚拟 NUMA 节点数量。如果 Tune 模式是 Preferred，则该值必须设置为 1。
	调优模式	用于分配内存的方法。 <ul style="list-style-type: none"> ● Strict : 如果无法在目标节点上分配内存，则内存分配将失败。 ● Preferred : 从单个首选节点分配内存。如果没有足够的内存可用，可以从其他节点分配内存。 ● interleave : 以轮询算法在节点间分配内存。
	NUMA 固定	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。点每个 vNUMA 从右侧的方框将虚拟 NUMA 节点拖到左侧的 NUMA 节点，以固定虚拟 NUMA 节点以托管 NUMA 节点。

12.3.5. 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 12.5. 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，并且始终显示 QCOW2，除非存储域类型是 OpenStack Volume (Cinder)，其格式为 Raw。

12.4. 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。

编辑虚拟机池

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。

12.5. 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。

预启动池中的虚拟机

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。

12.6. 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。

将虚拟机添加到虚拟机池

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。

12.7. 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。

从虚拟机池中分离虚拟机

1. 点 Compute → Pools。
2. 点池的名称打开详情视图。
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。

12.8. 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。

删除虚拟机池

1. 点 Compute → Pools 并选择虚拟机池。
2. 单击 Remove。
3. 点击 OK。

12.9. 可信计算池

受信任的计算池是基于 Intel 受信任的执行技术(Intel TXT)的安全集群。可信集群仅允许 Intel OpenAttestation 验证的主机，该主机会根据 White List 数据库测量主机硬件和软件的完整性。可以为可信主机和其上运行的虚拟机分配需要更高安全性的任务。有关 Intel TXT、可信系统和测试的更多信息，请参阅 <https://software.intel.com/en-us/articles/intel-trusted-execution-technology-intel-txt-enabling-guide>。

创建可信计算池涉及以下步骤：

- 配置管理器与 OpenAttestation 服务器通信。
- 创建只能运行可信主机的可信集群。
- 将可信主机添加到可信集群。主机必须运行 OpenAttestation 代理才能被 OpenAttestation sever 信任。

12.9.1. 将 OpenAttestation 服务器连接到 Manager

在创建可信集群前，必须配置 Red Hat Virtualization Manager 以识别 OpenAttestation 服务器。使用 engine-config 添加 OpenAttestation 服务器 FQDN 或 IP 地址：

```
# engine-config -s AttestationServer=attestationserver.example.com
```

如果需要，也可以更改以下设置：

表 12.6. engine-config 的 OpenAttestation Settings

选项	默认值	描述
AttestationServer	oat-server	OpenAttestation 服务器的 FQDN 或 IP 地址。这必须为 Manager 设置，才能与 OpenAttestation 服务器通信。
AttestationPort	8443	OpenAttestation 服务器用来与 Manager 通信的端口。
AttestationTruststore	TrustStore.jks	用于保护与 OpenAttestation 服务器通信的信任存储。
AttestationTruststorePass	password	用于访问信任存储的密码。
AttestationFirstStageSize	10	用于快速初始化。不建议在不做好原因的情况下更改这个值。
SecureConnectionWithOATServers	true	启用或禁用与 OpenAttestation 服务器的安全通信。
PollUri	AttestationService/resources/PollHosts	用于访问 OpenAttestation 服务的 URI。

12.9.2. 创建可信集群

可信集群与 OpenAttestation 服务器通信，以评估主机的安全性。当主机添加到可信集群时，OpenAttestation 服务器会根据 White List 数据库来测量主机的硬件和软件。虚拟机可以在可信集群中的可信主机之间迁移，允许在安全的环境中实现高可用性。

创建可信集群

1. 单击 **Compute** → **Clusters**。
2. 单击 **New**。
3. 为集群输入 **Name**。
4. 选择 **Enable Virt Service** 复选框。
5. 单击 **Scheduling Policy** 选项卡，再选择 **Enable Trusted Service** 复选框。
6. 单击 **OK**。

12.9.3. 添加可信主机

Red Hat Enterprise Linux 主机可以添加到可信集群，并根据 OpenAttestation 服务器提供的 White List 数据库进行测量。主机必须满足以下要求，才能被 OpenAttestation 服务器信任：

- 在 BIOS 中启用 Intel TXT。
- OpenAttestation 代理已安装并运行。
- 主机上运行的软件与 OpenAttestation 服务器的 White List 数据库匹配。

添加可信主机

1. 单击 Compute → Hosts。
2. 单击 New。
3. 从 Host Cluster 下拉列表中选择一个可信集群。
4. 输入主机的 Name。
5. 输入主机的主机名。
6. 输入主机的 root 密码。
7. 单击 OK。

主机添加到可信集群后，它由 OpenAttestation 服务器评估它。如果主机不受 OpenAttestation 服务器信任，它将移到 Non Operational 状态，并应该从可信集群中移除。

第 13 章 虚拟磁盘

13.1. 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 兼容数据中心中，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。

13.2. 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。



注意

在创建 Cinder 虚拟磁盘时，磁盘的格式和类型由 Cinder 在内部处理，不由 Red Hat Virtualization 管理。

下表介绍了存储类型和格式的可能组合。

表 13.1. 允许的存储组合

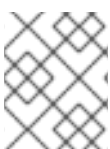
存储	格式	类型	备注
NFS	Raw	预分配	此文件的初始大小等于为虚拟磁盘定义的存储大小，并且没有格式设置。
NFS	Raw	稀疏	此文件的初始大小接近零，并且没有格式设置。
NFS	QCOW2	稀疏	此文件的初始大小接近零，并且具有 QCOW2 格式。随后的层将是 QCOW2 格式。
SAN	Raw	预分配	具有初始大小等于为虚拟磁盘定义的存储大小的块设备，并且没有格式设置。
SAN	QCOW2	稀疏	具有初始大小小于为虚拟磁盘定义的大小（目前为 1 GB）的块设备，并且具有根据需要分配的 QCOW2 格式（目前为 1 GB 增量）。

13.3. 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': limgsPar(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`。

13.4. 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。

13.5. 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。

13.6. 虚拟磁盘任务

13.6.1. 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。Cinder 磁盘需要使用外部提供者窗口访问添加到 Red Hat Virtualization 环境中的 OpenStack 卷实例；如需更多信息，请参阅第 14.2.4 节“[为存储管理添加 OpenStack Block Storage \(Cinder\) 实例](#)”。

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可使用附加的选项，如第 13.6.2 节“[New Virtual Disk Window 中的设置说明](#)”中指定的。

创建附加到虚拟机的虚拟磁盘

1. 单击 Compute → Virtual Machines。
2. 单击虚拟机的名称打开详情视图。
3. 单击 Disks 选项卡。
4. 单击 New。
5. 单击相应的按钮，指定虚拟磁盘是映像、直接 LUN 还是 Cinder 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，请参阅第 13.6.2 节“[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，一些选项不可用，如第 13.6.2 节“[New Virtual Disk Window 中的设置说明](#)”中指定的。

创建浮动虚拟磁盘



重要

创建浮动虚拟磁盘只是一个技术预览功能。技术预览功能不包括在红帽生产服务级别协议 (SLA) 中，且其功能可能并不完善。因此，红帽不建议在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

如需红帽技术预览功能支持范围的更多信息，请参阅 <https://access.redhat.com/support/offerings/techpreview/>。

1. 单击 Storage → Disks。

2. 单击 **New**。
3. 单击相应的按钮，指定虚拟磁盘是映像、直接 LUN 还是 Cinder 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，请参阅第 13.6.2 节“[New Virtual Disk Window 中的设置说明](#)”。
5. 单击 **OK**。

13.6.2. New Virtual Disk Window 中的设置说明

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 13.2. 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 不包括这些驱动程序，但可以从客户机工具 ISO 或虚拟软盘磁盘安装。IDE 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>
存储域	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。

字段名称	Description
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 1GB，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 1GB，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 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。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 <code>discard_zeroes_data</code> 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。</p>

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 13.3. 新虚拟磁盘并编辑虚拟磁盘设置：Direct LUN

字段名称	Description
Alias	虚拟磁盘的名称，限制为 40 个字符。
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 <code>engine-config</code> 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>

字段名称	Description
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，但可以从客户机工具 ISO 或虚拟软盘磁盘安装。IDE 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>
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>

字段名称	Description
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>

如果没有可用的 OpenStack 卷存储域，则 Cinder 设置表单将被禁用，您可以在相关数据中心的创建磁盘。Cinder 磁盘需要使用外部提供者窗口访问添加到 Red Hat Virtualization 环境中的 OpenStack 卷实例；如需更多信息，请参阅 [第 14.2.4 节“为存储管理添加 OpenStack Block Storage \(Cinder\) 实例”](#)。

表 13.4. 新虚拟磁盘并编辑虚拟磁盘设置：Cinder

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。

字段名称	Description
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，但可以从客户机工具 ISO 或虚拟软盘磁盘安装。IDE 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>
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>
卷类型	<p>虚拟磁盘的卷类型。下拉列表显示所有可用的卷类型。卷类型将在 OpenStack Cinder 上管理和配置。</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>
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>



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。

13.6.3. 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。

13.6.4. 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。

移动虚拟磁盘

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. 点击 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。

13.6.5. 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. 点击虚拟机的名称打开详情视图。
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. 点击虚拟机的名称打开详情视图。
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。

13.6.6. 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。

复制虚拟磁盘

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. 单击 OK。

在复制时，虚拟磁盘的状态为 Locked。

13.6.7. 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。请参阅第 11.8.1 节“将镜像上传到数据存储域”。

13.6.8. 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。

导入磁盘镜像

1. 点 Storage → Domains。
2. 点击导入的存储域的名称打开详情视图。
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。

13.6.9. 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。

导入磁盘镜像

1. 点 Storage → Domains。
2. 点存储域的名称打开详情视图。
3. 点击 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。

13.6.10. 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 域名以打开详情视图。
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。

13.6.11. 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。

13.6.12. 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。这会将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。

红帽建议在克隆虚拟机前执行此操作，然后基于虚拟机创建模板，或者清理存储域的磁盘空间。

限制

- NFS 存储域必须使用 NFS 版本 4.2 或更高版本。
- 您不能对使用直接 LUN 或 Cinder 的磁盘进行解析。
- 您无法对使用预分配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. 点击虚拟机的名称打开详情视图。
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。

第 14 章 外部供应商

14.1. 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。如需安装 Red Hat Satellite 和使用 Red Hat Satellite 管理主机的信息，请参阅 [Red Hat Satellite Installation Guide](#) 和 [Red Hat Satellite Host Configuration Guide](#)。

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。

用于网络置备的 OpenStack 网络(Neutron)

OpenStack 网络提供软件定义型网络。在 Red Hat Virtualization 中，可以将 OpenStack 网络提供的网络导入到 Red Hat Virtualization Manager 中，并用来承载所有类型的流量并创建复杂的网络拓扑。将 OpenStack 网络添加到管理器后，您可以通过手动导入 OpenStack 网络来访问 OpenStack 网络所提供的网络。

用于存储管理的 OpenStack 卷(Cinder)

OpenStack 卷为虚拟硬盘提供永久块存储管理。OpenStack Cinder 卷由 Ceph 存储调配。在 Red Hat Virtualization 中，您可以在 OpenStack 卷存储中创建可用作浮动磁盘或附加到虚拟机的磁盘。将 OpenStack 卷添加到 Manager 后，您可以在 OpenStack 卷提供的存储上创建磁盘。

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。

用于网络置备的外部网络供应商

支持的外部 software 定义的网络提供程序包括实施 OpenStack Neutron REST API 的任何提供程序。与 OpenStack 网络(Neutron)不同，Neutron 代理不用作主机上的虚拟接口驱动程序实施。相反，需要由外部网络提供程序的实施程序提供虚拟接口驱动程序。

所有外部资源供应商都会使用适合您的输入的单个窗口来添加。您必须先添加资源供应商，然后才能使用它在 Red Hat Virtualization 环境中提供的资源。

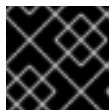
14.2. 添加外部供应商

14.2.1. 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。

为主机调配添加 Satellite 实例

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，则打开 Import provider certificate 窗口；单击 OK 以导入 Satellite 实例提供的证书，以确保管理器可以与实例通信。
9. 单击 OK。

14.2.2. 为镜像管理添加 OpenStack Image (Glance)实例

为 Red Hat Virtualization Manager 添加用于镜像管理的 OpenStack Image (Glance)实例。

为镜像管理添加 OpenStack Image (Glance)实例

1. 单击 Administration → Providers。
2. 点 Add，然后在 General Settings 选项卡中输入详情。有关这些字段的详情请参考 [第 14.2.10 节“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. 单击 OK。

14.2.3. 为网络置备添加 OpenStack 网络(Neutron)实例

将 OpenStack Networking (neutron)实例添加到 Red Hat Virtualization Manager。要添加实现 OpenStack Neutron REST API 的其他第三方网络提供程序, 请参考第 14.2.9 节“添加外部网络提供程序”。



重要

Red Hat Virtualization 支持 Red Hat OpenStack Platform 版本 10、13 和 14 作为外部网络供应商。

- OpenStack 10 应该部署有 OVS 驱动程序。
- OpenStack 13 应当通过 OVS、OVN 或 ODL 驱动程序进行部署。
- OpenStack 14 应该使用 OVN 或 ODL 驱动程序进行部署。

要使用 neutron 网络, 主机必须配置有 neutron 代理。您可以将代理手动配置, 或者使用 Red Hat OpenStack Platform director 部署 Networker 角色, 然后再将网络节点作为主机添加到 Manager 中。建议使用 director。不支持通过 New Host 窗口中的 Network Provider 选项卡自动部署 neutron 代理。

虽然网络节点和常规主机可以在同一集群中使用, 但使用 neutron 网络的虚拟机只能在网络节点上运行。

将网络节点添加为主机

1. 使用 Red Hat OpenStack Platform director 在网络节点上部署 Networker 角色。请参阅 Red Hat OpenStack Platform 高级 Overcloud 自定义指南中的 [创建新角色](https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/10/html/advanced_overcloud_customization/Roles#Standalone_Networker) 和网络程序。https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/10/html/advanced_overcloud_customization/Roles#Standalone_Networker
2. 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 Enterprise Linux Server 和 Red Hat Virtualization 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=poolid
```

- d. 配置存储库：

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

- e. 确保当前安装的所有软件包都为最新版本：

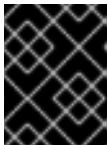
```
# yum update
```

- f. 如果更新任何内核软件包，请重启机器。

3. 安装 Openstack Networking hook：

```
# yum install vdsm-hook-openstacknet
```

4. 将网络节点作为主机添加到 Manager 中。请参阅 [第 10.5.1 节“在 Red Hat Virtualization Manager 中添加标准主机”](#)。

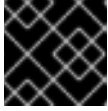


重要

不要从 Network Provider 选项卡选择 OpenStack Networking provider。目前不支持。

为网络置备添加 OpenStack 网络(Neutron)实例

1. 单击 Administration → Providers。
2. 点 Add，然后在 General Settings 选项卡中输入详情。有关这些字段的详情请参考 [第 14.2.10 节“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 Networking。
5. 确保在 Networking Plugin 字段中选择了 Open vSwitch。
6. (可选) 选择 Automatic Synchronization 复选框。这可让外部网络提供程序与现有网络进行自动同步。
7. 在提供者 URL 文本字段中输入安装 OpenStack Networking 实例的机器的 URL 或全限定域名，后跟端口号。默认选择 Read-Only 复选框。这可防止用户修改 OpenStack 网络实例。



重要

您必须选中 Read-Only 复选框，才能支持您的设置。

8. (可选) 选择 Requires Authentication 复选框，然后为 Keystone 中注册的 OpenStack Networking 用户输入 Username 和 Password。您还必须通过定义协议、主机名、API 端口和 API 版本 来定义 Keystone 服务器的身份验证 URL。
对于 API 版本 2.0，请输入 OpenStack Networking 实例的租户。对于 API 版本 3，请输入用户名、项目名称和 Project Domain Name。
9. 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 网络实例成功进行身份验证。
 - b. 如果 OpenStack Networking 实例使用 SSL，则打开 Import provider certificate 窗口；单击 OK 以导入 OpenStack Networking 实例提供的证书，以确保管理器可以与实例通信。
10. 单击 代理配置选项卡。



警告

以下步骤仅作为技术预览提供。Red Hat Virtualization 只支持预先配置的 neutron 主机。

11. 在 Interface Mappings 字段中输入 Open vSwitch 代理的接口映射列表。
12. 从 Broker Type 列表中选择 OpenStack Networking 实例使用的消息代理类型。
13. 在 Host 字段中输入托管消息代理的主机的 URL 或完全限定域名。
14. 输入用于连接消息代理的端口。如果消息代理没有配置为使用 SSL，则此端口号为 5762，如果该端口号被配置为使用 SSL，则默认为 5761。
15. 输入在消息代理实例中注册的 OpenStack Networking 用户的 Username 和 Password。
16. 单击 OK。

您已将 OpenStack 网络实例添加到 Red Hat Virtualization Manager。在使用它提供的网络之前，先将网络导入到 Manager 中。请参阅 [第 9.3.1 节“从外部提供程序导入网络”](#)。

14.2.4. 为存储管理添加 OpenStack Block Storage (Cinder) 实例



重要

使用 OpenStack Block Storage (Cinder) 实例进行存储管理，只是一个技术预览功能。技术预览功能不包括在红帽生产服务级别协议 (SLA) 中，且其功能可能并不完善。因此，红帽不建议在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

如需红帽技术预览功能支持范围的更多信息，请参阅 <https://access.redhat.com/support/offerings/techpreview/>。

为 Red Hat Virtualization Manager 添加用于存储管理的 OpenStack Block Storage (Cinder) 实例。OpenStack Cinder 卷由 Ceph 存储调配。

为存储管理添加 OpenStack Block Storage (Cinder) 实例

1. 单击 Administration → Providers。
2. 点 Add，然后在 General Settings 选项卡中输入详情。有关这些字段的详情请参考第 14.2.10 节“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 Block Storage。
5. 选择将 OpenStack Block Storage 卷附加到的数据中心。
6. 在 Provider URL 文本字段中输入安装 OpenStack Block Storage 实例的机器的 URL 或全限定域名。
7. (可选) 选择 Requires Authentication 复选框，然后在 Keystone 中注册的 OpenStack Block Storage 实例用户输入 Username 和 Password。通过定义协议 (必须是 HTTP)、主机名和 API 端口，定义 Keystone 服务器的身份验证 URL。
输入 OpenStack Block Storage 实例的租户。
8. 单击 Test 来测试您可以使用提供的凭据通过 OpenStack Block Storage 实例成功进行身份验证。
9. 点击 OK。
10. 如果启用了客户端 Ceph 身份验证(cephx)，还必须完成以下步骤。cephx 协议默认启用。
 - a. 在 Ceph 服务器上，使用 `ceph auth get-or-create` 命令为 `client.cinder` 用户创建一个新的 secret 密钥。如需有关 为新用户创建密钥的更多信息，请参阅 [Cephx 配置参考](#)，以及 [管理用户](#)。如果 `client.cinder` 用户已存在密钥，则使用相同的命令检索密钥。
 - b. 在管理门户中，从 Providers 列表中选择新创建的 Cinder 外部提供程序。
 - c. 点 Authentication Keys 选项卡。
 - d. 单击 New。

- e. 在 Value 字段中输入 secret 键。
- f. 复制自动生成的 UUID，或者在文本字段中输入现有 UUID。
- g. 在 Cinder 服务器上，将上一步中的 UUID 和 cinder 用户添加到 `/etc/cinder/cinder.conf`：

```

| rbd_secret_uuid = UUID
| rbd_user = cinder

```

有关创建 OpenStack Block Storage (Cinder) 磁盘的更多信息，请参阅 [第 13.6.1 节“创建虚拟磁盘”](#)。

14.2.5. 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。

将 VMware vCenter 实例添加为虚拟机提供程序

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；点击 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 外部供应商导入虚拟机，请参阅《虚拟机管理指南》中的从 VMware 提供程序 导入虚拟机。

14.2.6. 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。

将 RHEL 5 Xen 实例添加为虚拟机提供程序

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 vdsd 用户生成 SSH 密钥。

```
# sudo -u vdsd ssh-keygen
```

- b. 将 vdsd 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 vdsd 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 vdsd 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。

14.2.7. 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。

将 KVM 主机添加为虚拟机提供程序

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 vdsms 用户生成 SSH 密钥。**

```
# sudo -u vdsms ssh-keygen
```

- b. **将 vdsms 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 vdsms 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 vdsms 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。

14.2.8. 添加 Open Virtual Network (OVN)作为外部网络提供程序

Open Virtual Network (OVN)允许您创建没有添加 VLAN 或更改基础架构的网络。OVN 是一种 Open vSwitch (OVS)扩展，通过添加对虚拟 L2 和 L3 覆盖的原生 OVS 支持，支持虚拟网络。

您可以安装新的 OVN 网络供应商 或 添加新的 OVN 网络供应商。

您还可以将 OVN 网络连接到原生 Red Hat Virtualization 网络。如需更多信息，请参阅第 14.2.8.5 节“[将 OVN 网络连接到物理网络](#)”。这个功能仅作为技术预览提供。

与 Neutron 类似的 REST API 由 `ovirt-provider-ovn` 公开，允许您创建网络、子网、端口和路由器（请参阅 [OpenStack 网络 API v2.0](#) 来获取详细信息）。这些覆盖网络可启用虚拟机间的通信。



注意

借助 OpenStack (Neutron) API，CloudForms 支持 OVN 作为外部提供者。详情请参阅 Red Hat CloudForms 中的 [Network Managers: 管理供应商](#)。

如需有关 OVS 和 OVN 的更多信息，请参阅 OVS 文档 <http://docs.openvswitch.org/en/latest/> 和 <http://openvswitch.org/support/dist-docs/>。

14.2.8.1. 安装新的 OVN 网络提供程序

**警告**

如果已安装 `openvswitch` 软件包，如果版本为 1:2.6.1（版本 2.6.1，epoch 1），则 OVN 安装将在尝试安装最新的 `openvswitch` 软件包时失败。详情请参阅 [BZ#1505398](#) 中的 Doc 文本信息。

使用 `engine-setup` 安装 OVN 时，会自动执行以下步骤：

- 在 Manager 机器上设置 OVN 中央服务器。
- 将 OVN 添加为外部网络提供程序。
- 将 Default 集群的默认网络提供程序设置为 `ovirt-provider-ovn`。
- 配置主机，以便在添加到集群时与 OVN 进行通信。

如果您使用带有 `engine-setup` 的预配置应答文件，可以添加以下条目来安装 OVN：

```
OVESETUP_OVN/ovirtProviderOvn=bool:True
```

安装新的 OVN 网络提供程序

1. 使用 `engine-setup` 在 Manager 上安装 OVN。在安装过程中，`engine-setup` 询问以下问题：

```
# Install ovirt-provider-ovn(Yes, No) [Yes]?:
```

- 如果是，`engine-setup` 会安装 `ovirt-provider-ovn`。如果 `engine-setup` 更新系统，则只有在之前没有安装 `ovirt-provider-ovn` 时，才会出现此提示。

如果没有，在下次运行 `engine-setup` 时不会再次询问。如果要查看这个选项，请运行 `engine-setup --reconfigure-optional-components`。

```
# 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。有关 OVN 身份验证的更多信息，请参阅 <https://github.com/oVirt/ovirt-provider-ovn/blob/master/README.adoc>。

2.

将主机添加到 **Default** 集群。添加至此集群的主机会自动配置为与 OVN 进行通信。要添加新主机，请参阅第 10.5.1 节“在 Red Hat Virtualization Manager 中添加标准主机”。

要将主机配置为使用现有的非默认网络，请参考第 14.2.8.4 节“为 OVN Tunnel 网络配置主机”。

3.

将网络添加到默认集群；请参阅第 9.1.2 节“在数据中心或集群中创建新的逻辑网络”并选择 **Create on external provider** 复选框。默认选择 `ovirt-provider-ovn`。

4.

要将 OVN 网络连接到原生 Red Hat Virtualization 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。如需更多信息和先决条件，请参阅第 14.2.8.5 节“将 OVN 网络连接到物理网络”。

5.

定义网络是否应该从 **Security Groups** 下拉菜单中使用 **Security Groups**。有关可用选项的详情请参考第 9.1.7 节“逻辑网络常规设置说明”。现在，您可以创建使用 OVN 网络的虚拟机。

14.2.8.2. 添加现有 OVN 网络提供程序

在 Red Hat Virtualization 中将现有的 OVN 中央服务器添加为外部网络提供程序，涉及以下关键步骤：

- **安装 OVN 供应商，即经理用来与 OVN 交互的代理。OVN 提供程序可以安装在任何机器上，但必须能够与 OVN 中央服务器和管理器通信。**
- **将 OVN 供应商作为外部网络供应商添加到 Red Hat Virtualization。**
- **创建一个新集群，它使用 OVN 作为其默认网络供应商。添加至此集群的主机会自动配置为与 OVN 进行通信。**

先决条件

OVN 供应商需要以下软件包，且必须在供应商机器中可用：

- **`openvswitch-ovn-central`**
- **`openvswitch`**
- **`openvswitch-ovn-common`**
- **`python-openvswitch`**

如果这些软件包不在供应商机器上启用的存储库中可用，可以从 OVS 网站下载它们：
<http://openvswitch.org/download/>。

添加现有 OVN 网络提供程序

1. **安装和配置 OVN 供应商。**

a.

在供应商机器上安装供应商：

```
# yum install ovirt-provider-ovn
```

b.

如果您没有在与 Manager 相同的机器上安装供应商，请在 `/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` 文件中添加以下条目：

```
[OVIRT]
ovirt-host=https://Manager_host_name
```

如果启用了身份验证，这将用于身份验证。

c.

如果您没有在与 OVN 中央服务器相同的机器上安装供应商，请在 `/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` 文件中添加以下条目：

```
[OVN REMOTE]
ovn-remote=tcp:OVN_central_server_IP:6641
```

d.

在防火墙中打开端口 9696、6641 和 6642，以允许 OVN 提供程序、OVN 中央服务器和管理器之间的通信。这可以通过手动将 `ovirt-provider-ovn` 和 `ovirt-provider-ovn-central` 服务添加到适当的区：

```
# firewall-cmd --zone=ZoneName --add-service=ovirt-provider-ovn --permanent
# firewall-cmd --zone=ZoneName --add-service=ovirt-provider-ovn-central --permanent
# firewall-cmd --reload
```

e.

启动并启用该服务：

```
# systemctl start ovirt-provider-ovn
# systemctl enable ovirt-provider-ovn
```

f.

将 OVN 中央服务器配置为监听来自端口 6642 和 6641 的请求：

```
# ovn-sbctl set-connection tcp:6642
# ovn-nbctl set-connection tcp:6641
```

2.

在管理门户中，单击 **Administration** → **Providers**。

3. 点 **Add**, 然后在 **General Settings** 选项卡中输入详情。有关这些字段的详情请参考第 14.2.10 节“[添加 Provider General Settings Explained](#)”。
4. 输入名称和描述。
5. 从 **Type** 列表, 选择 **External Network Provider**。
6. 点 **Networking Plugin** 文本框, 从下拉菜单中选择 **oVirt Network Provider for OVN**。
7. (可选) 选择 **Automatic Synchronization** 复选框。这可让外部网络提供程序与现有网络进行自动同步。



注意

在 `engine-setup` 工具创建的 `ovirt-provider-ovn` 网络供应商上默认启用自动同步。

8. 在 **Provider URL** 文本字段中输入 OVN 提供程序的 URL 或全限定域名, 后跟端口号。如果 OVN 供应商和 OVN 中央服务器位于独立的机器上, 这是供应商机器的 URL, 而不是中央服务器。如果 OVN 供应商位于与 Manager 相同的机器上, 则 URL 可以保持默认的 <http://localhost:9696>。
9. 清除 **Read-Only** 复选框, 以允许从 Red Hat Virtualization Manager 创建新的 OVN 网络。
10. (可选) 选择 **Requires Authentication** 复选框, 然后为 Keystone 中注册的外部网络提供程序用户输入 **Username** 和 **Password**。您还必须通过定义协议、主机名和 API 端口来定义 Keystone 服务器的身份验证 URL。

(可选) 输入 外部网络提供程序的租户。

身份验证方法必须在 `/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` 文件中配置 (如果不存在, 请创建此文件)。重启 `ovirt-provider-ovn` 服务以使更改生效。有关 OVN 身份验证的更多信息, 请参阅 <https://github.com/oVirt/ovirt-provider-ovn/blob/master/README.adoc>。

11.

测试凭证：

a.

单击 **Test** 来测试您能否使用提供的凭证成功与 OVN 进行身份验证。

b.

如果 OVN 实例使用 SSL，则打开 **Import provider certificate** 窗口；单击 **OK** 以导入 OVN 实例提供的证书，以确保管理器可以与实例通信。

12.

单击 **OK**。

13.

创建一个新集群，它使用 OVN 作为其默认网络供应商。请参阅 [第 8.2.1 节“创建新集群”](#)，从 **Default Network Provider** 下拉列表中选择 **OVN 网络供应商**。

14.

将主机添加到集群中。添加至此集群的主机会自动配置为与 OVN 进行通信。要添加新主机，请参阅 [第 10.5.1 节“在 Red Hat Virtualization Manager 中添加标准主机”](#)。

15.

将 OVN 网络导入或添加到新集群中。要导入网络，请参阅 [导入网络](#)。要使用 OVN 创建新网络，请参阅在 [数据中心或集群中创建新的逻辑网络](#)，然后选择 **Create on external provider** 复选框。默认选择 **ovirt-provider-ovn**。

要将主机配置为使用现有的非默认网络，请参考 [第 14.2.8.4 节“为 OVN Tunnel 网络配置主机”](#)。

要将 OVN 网络连接到原生 Red Hat Virtualization 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。如需更多信息和先决条件，请参阅 [第 14.2.8.5 节“将 OVN 网络连接到物理网络”](#)。

现在，您可以创建使用 OVN 网络的虚拟机。

14.2.8.3. 使用 Ansible playbook 修改 OVN 隧道网络

您可以使用 **ovirt-provider-ovn-driver Ansible playbook** 来修改 OVN 控制器的隧道网络。

用于修改 OVN 隧道网络的 Ansible playbook

```
# ansible-playbook --key-file <path_to_key_file> -i <path_to_inventory> --extra-vars " cluster_name=
<cluster_name> ovn_central=<ovn_central_ip_address> ovirt_network=<ovirt network name>
ovn_tunneling_interface=<vdsd_network_name>" ovirt-provider-ovn-driver.yml
```

参数

key-file

要登录到主机的密钥文件。默认密钥文件通常位于 `/etc/pki/ovirt-engine/keys` 目录中。

inventory

oVirt VM 清单。要找到清单值，请使用此脚本：`/usr/share/ovirt-engine-metrics/bin/ovirt-engine-hosts-ansible-inventory`。

cluster_name

要更新名称的集群名称。

ovn_central

OVN 中央服务器的 IP 地址。该 IP 地址必须可以被所有主机访问。

ovirt_network

oVirt 网络名称。

ovn_tunneling_interface

VDSM 网络名称。



注意

ovirt-provider-ovn-driver Ansible playbook 支持使用 `ovirt_network` 参数或 `ovn_tunneling_interface` 参数。如果同一 `playbook` 中存在这两个参数，则此 `playbook` 将失败。

带有 `ovirt_network` 参数的 `playbook`

```
# ansible-playbook --key-file /etc/pki/ovirt-engine/keys/engine_id_rsa -i /usr/share/ovirt-engine-
metrics/bin/ovirt-engine-hosts-ansible-inventory --extra-vars " cluster_name=test-cluster
ovn_central=192.168.200.2 ovirt_network=\"Long\ Network\ Name\ with\ \Ascii\ character\ |⊙|\"" ovirt-
provider-ovn-driver.yml
```

带有 `ovn_tunneling_interface` 参数的 `playbook`

```
# ansible-playbook --key-file /etc/pki/ovirt-engine/keys/engine_id_rsa -i /usr/share/ovirt-engine-
metrics/bin/ovirt-engine-hosts-ansible-inventory --extra-vars " cluster_name=test-cluster
ovn_central=192.168.200.2 ovn_tunneling_interface=on703ea21ddbc34" ovirt-provider-ovn-driver.yml
```

在 **Manager** 计算机上，导航到 `/usr/share/ovirt-engine/playbooks` 目录以运行 **Ansible** `playbook`。

14.2.8.4. 为 OVN Tunnel 网络配置主机

您可以将主机配置为使用默认 `ovirtmgmt` 网络以外的现有网络，以及 `ovirt-provider-ovn-driver` **Ansible** `playbook`。该网络必须可以被集群中的所有主机访问。



注意

`ovirt-provider-ovn-driver` **Ansible** `playbook` 更新现有主机。如果向集群添加新主机，则必须再次运行 `playbook`。

为 OVN Tunnel 网络配置主机

1. 在 **Manager** 计算机上，进入 `playbooks` 目录：

```
# cd /usr/share/ovirt-engine/playbooks
```

2. 使用以下参数运行 `ansible-playbook` 命令：

```
# ansible-playbook --private-key=/etc/pki/ovirt-engine/keys/engine_id_rsa -i /usr/share/ovirt-
engine-metrics/bin/ovirt-engine-hosts-ansible-inventory --extra-vars
" cluster_name=Cluster_Name ovn_central=OVN_Central_IP
ovn_tunneling_interface=VDSM_Network_Name" ovirt-provider-ovn-driver.yml
```

例如：

```
# ansible-playbook --private-key=/etc/pki/ovirt-engine/keys/engine_id_rsa -i /usr/share/ovirt-
engine-metrics/bin/ovirt-engine-hosts-ansible-inventory --extra-vars
" cluster_name=MyCluster ovn_central=192.168.0.1 ovn_tunneling_interface=MyNetwork"
ovirt-provider-ovn-driver.yml
```



注意

OVN_Central_IP 可以在新网络上，但这不是必需的。**OVN_Central_IP** 必须可以被所有主机访问。

VDSM_Network_Name 仅限于 15 个字符。如果您定义了一个超过 15 个字符或包含非 ASCII 字符的逻辑网络名称，则自动生成 15 个字符。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。

在单主机上更新 OVN Tunnel Network

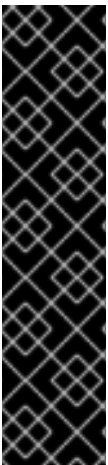
您可以使用 **vdsmd-tool** 更新单一主机上的 OVN 隧道网络：

```
# vdsmd-tool ovn-config OVN_Central_IP Tunneling_IP_or_Network_Name
```

例 14.1. 使用 **vdsmd-tool** 更新主机

```
# vdsmd-tool ovn-config 192.168.0.1 MyNetwork
```

14.2.8.5. 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。

如需红帽技术预览功能支持范围的更多信息，请参阅 <https://access.redhat.com/support/offerings/techpreview/>。

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）。

创建新的外部网络连接到物理网络

1. 单击 **Compute** → **Clusters**。
2. 点集群名称打开详情视图。
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. 单击 **OK**。

14.2.9. 添加外部网络提供程序

任何实施 OpenStack Neutron REST API 的网络提供程序都可添加到 Red Hat Virtualization。虚拟接口驱动程序需要由外部网络提供程序的实施人员提供。一个网络供应商和虚拟接口驱动程序的参考实现，请访问 <https://github.com/mmirecki/ovirt-provider-mock> 和 https://github.com/mmirecki/ovirt-provider-mock/blob/master/docs/driver_instalation。

为网络置备添加外部网络提供程序

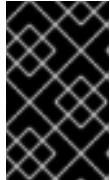
1. 单击 **Administration** → **Providers**。
2. 点 **Add**，然后在 **General Settings** 选项卡中输入详情。有关这些字段的详情请参考第 14.2.10 节“[添加 Provider General Settings Explained](#)”。
3. 输入名称和描述。
4. 从 **Type** 下拉列表中，选择 **External Network Provider**。
5. (可选) 单击 **Networking Plugin** 文本框，并从下拉菜单中选择适当的驱动程序。
6. (可选) 选择 **Automatic Synchronization** 复选框。这可使外部网络提供程序与现有网络进行自动同步。添加外部网络提供程序时，此功能默认为禁用。

**注意**

在 `engine-setup` 工具创建的 `ovirt-provider-ovn` 网络供应商上默认启用自动同步。

7.

在提供者 URL 文本字段中输入安装外部网络提供程序的机器的 URL 或全限定域名，后跟端口号。默认选择 `Read-Only` 复选框。这可防止用户修改外部网络提供程序。

**重要**

您必须选中 `Read-Only` 复选框，才能支持您的设置。

8.

(可选) 选择 `Requires Authentication` 复选框，然后在 `Keystone` 中注册的外部网络提供程序用户输入 `Username` 和 `Password`。您还必须通过定义协议、主机名和 API 端口来定义 `Keystone` 服务器的身份验证 URL。

(可选) 输入 外部网络提供程序的租户。

9.

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外部网络提供程序成功进行身份验证。

b.

如果外部网络提供程序使用 `SSL`，则打开 `Import provider certificate` 窗口；单击 `OK` 以导入外部网络提供程序提供的证书，以确保管理器可以与实例通信。

10.

单击 `OK`。

在使用此提供程序的网络前，您必须在主机上安装虚拟接口驱动程序并导入网络。要导入网络，请参阅 [第 9.3.1 节“从外部提供程序导入网络”](#)。

14.2.10. 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 14.1. 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>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>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。 ● 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

设置	解释
	<p>租户名称：OpenStack 网络服务所属的 OpenStack 租户的名称。</p> <p>OpenStack 网络</p> <ul style="list-style-type: none"> ● 网络插件：用于连接 OpenStack 网络服务器的联网插件。对于 OpenStack 网络，Open vSwitch 是唯一选项，默认选择。 ● 自动同步：允许您指定供应商是否会与现有网络同步。 ● 提供程序 URL：托管 OpenStack 网络实例的计算机的 URL 或完全限定域名。您必须将 OpenStack 网络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 9696。 ● 只读：允许您指定 OpenStack 网络实例是否可以从管理门户进行修改。 ● 需要 Authentication：允许您指定是否需要身份验证才能访问 OpenStack 网络服务。 ● 用户名：用于连接 OpenStack 网络实例的用户名。此用户名必须是在 OpenStack 网络实例所属的 Keystone 实例中注册的 OpenStack 网络的用户名。 ● Password：上面用户名要进行身份验证的密码。此密码必须是在 OpenStack 网络实例所属的 Keystone 实例中注册的 OpenStack Networking 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。这会出现在 URL 中。如果显示 v2.0，请选择 v2.0。如果 v3 出现选择 v3。 <p>当您从 API Version 字段中选择 v3 时会出现以下字段：</p> <ul style="list-style-type: none"> ● User Domain Name：域中定义的用户名称。 使用 Keystone API v3 时，域用于决定 OpenStack 中服务实体的管理边界。域允许您将用户分组到一起以实现不同的目的，如设置域特定配置或安全选项。有关更多信息，请参阅 Red Hat OpenStack Platform 架构指南中的 OpenStack Identity (keystone)。 ● 项目名称：定义 OpenStack Identity API v3 的项目名称。 ● Project Domain Name：定义 OpenStack Identity API v3 的项目域名。 <p>从 API Version 字段中选择 v2.0 时会出现以下字段：</p>

设置	解释
	<ul style="list-style-type: none"> ● 租户名称：仅在从 API Version 字段选择 v2 时应用。OpenStack 网络实例所属的 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。 <p>VMware</p> <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

设置	解释
	<p>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）。</p> <ul style="list-style-type: none"> ● 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>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）。 ● 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。 <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。

设置	解释
	<ul style="list-style-type: none"> ● 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 <code>username@domain@auth_profile</code> 而不是默认的 <code>username@domain</code>。 ● 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。
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。

14.2.11. 添加 Provider Agent Configuration Settings Explained

通过 **Add Provider** 窗口中的 **Agent Configuration** 选项卡，用户可以注册网络插件的详细信息。此选项卡仅适用于 **OpenStack 网络供应商** 类型。

表 14.2. 添加 Provider: Agent Configuration Settings

设置	解释
接口映射	标签:接口 以逗号分隔的映射列表。
代理类型	OpenStack 网络实例使用的消息代理类型。选择 RabbitMQ 或 Qpid 。
主机	安装消息代理的机器的 URL 或全限定域名。

设置	解释
端口	与上述主机连接时使用的远程端口。默认情况下，如果主机上没有启用 SSL，则此端口为 5762，如果启用了 SSL，则 5761。
用户名	使用上述消息代理验证 OpenStack 网络实例的用户名。默认情况下，这个用户名是 neutron 。
密码	对以上用户名进行身份验证的密码。

14.3. 编辑外部供应商

编辑外部供应商

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**。

14.4. 删除外部供应商

删除外部供应商

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**。

部分 III. 管理环境

第 15 章 管理自托管引擎

15.1. 维护自托管引擎

自托管引擎维护模式

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。

可以强制实施三种维护模式：

- **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。

设置本地维护

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**。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。

在管理门户中，单击 **Compute** → **Hosts** 并选择任何自托管引擎节点。

- 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
```

设置全局维护

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
```

15.2. 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**。

15.2.1. 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：

he_local	在本地主机上设置 etc/ovirt-hosted-engine/hosted-engine.conf 在本地实例中的值，因此仅将该主机使用新的值。要启用新值，请重启 ovirt-ha-agent 和 ovirt-ha-broker 服务。
he_shared	在共享存储上设置 etc/ovirt-hosted-engine.conf 的值，以便在配置更改后部署所有主机。要在主机上启用新值，请重新部署该主机。
ha	在本地存储的 /var/lib/ovirt-hosted-engine-ha/ha.conf 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。
---------------	--

15.2.2. 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 [第 15.1 节“维护自托管引擎”](#)。

15.3. 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 [第 15.4 节“在 Red Hat Virtualization Manager 中添加自托管引擎节点”](#)。

在附加主机上为自托管引擎配置 Memory Slots 保留

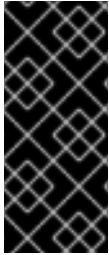
1. 点 **Compute** → **Clusters** 并选择包含自托管引擎节点的集群。
2. 点 **Edit**。
3. 单击 **Scheduling Policy** 选项卡。
4. 单击 **+**，然后选择 **HeSparesCount**。
5. 输入可保留足够可用内存的额外自托管引擎节点数量，以启动 Manager 虚拟机。
6. 点击 **OK**。

15.4. 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，需要额外的步骤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。红帽建议至少有两个自托管引擎节点，以确保 Manager 虚拟机高度可用。也可以使用 REST API 添加其他主机。请参阅 [REST API 指南中的主机](#)。

先决条件

- 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](#)。



重要

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

流程

1. 在管理门户中，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。**

15.5. 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。

流程

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

15.6. 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。

15.7. 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。

从自托管引擎环境中删除主机

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** 并点 **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** 打开 **Remove Host (s)** 确认窗口，然后单击确定。

15.8. 更新自托管引擎

要将当前版本的 4.3 的自托管引擎更新至 4.3 的最新版本，您必须将环境设置为全局维护模式，然后按照标准步骤在次版本间进行更新。

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. 在继续之前，确认环境处于维护模式：

```
# hosted-engine --vm-status
```

您应当会看到指出集群处于维护模式的消息。

更新 Red Hat Virtualization Manager

Red Hat Virtualization Manager 的更新将通过内容交付网络发布。

流程

1. **登录到 Manager 虚拟机。**

2. **检查更新的软件包是否可用：**

```
# engine-upgrade-check
```

3. **更新设置软件包：**

```
# yum update ovirt-*setup* rh-*vm-setup-plugins
```

4. **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
```

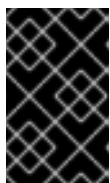
当脚本成功完成时，会显示以下信息：

```
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。

5.

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
```



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。

15.9. 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 [第 22.1.3 节“使用 oVirt Engine Rename 工具重命名 Manager”](#)。

第 16 章 备份和迁移

16.1. 备份和恢复 RED HAT VIRTUALIZATION MANAGER

16.1.1. 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。

16.1.2. `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
```

这两个模式由一组参数进一步扩展，允许您指定引擎数据库的备份和不同凭据的范围。对参数及其功能的完整列表运行 `engine-backup --help`。

基本选项

`--mode`

指定命令是执行备份操作还是恢复操作。有两个可用选项 - `backup` 和 `restore`。这是必需参数。

`--file`

指定要在备份模式中执行备份的文件的 *路径和名称*，以及从恢复模式中读取备份数据的路径和名称。在 `backup` 模式和 `restore` 模式中，这是必需参数。

`--log`

指定要写入备份或恢复操作日志的文件的 *路径和名称*。在 `backup` 模式和 `restore` 模式中都需要这个参数。

`--scope`

指定 `backup` 或 `restore` 操作的范围。有四个选项：*所有* 都是，备份或恢复所有数据库和配置数据；*这些文件* 仅备份或恢复系统上的文件；*db* 则可备份或恢复管理器数据库，以及 `dwhdb`，后者仅备份或恢复数据仓库数据库。默认范围 *都是*。

--scope 参数可以在同一 `engine-backup` 命令中多次指定。

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

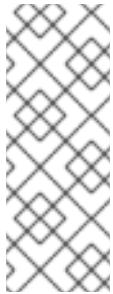
创建供要恢复到的 Manager 数据库备份的 PostgreSQL 数据库。在远程主机上恢复备份或全新安装没有配置 PostgreSQL 数据库时，这是必需参数。

--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。如需此参数所需的额外参数，请参阅 `engine-backup --help`。

--restore-permissions 或 **--no-restore-permissions**

恢复（或不恢复）数据库用户的权限。恢复备份时需要这些参数之一。



注意

如果备份包含对额外数据库用户授予访问权限，则使用 `--restore-permissions` 和 `--provision-db`（或 `--provision-dwh-db`）选项恢复备份，则使用随机密码创建额外的用户。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 <https://access.redhat.com/articles/2686731>。

16.1.3. 使用 `engine-backup` 命令创建备份

在 Manager 处于活动状态时，可以使用 `engine-backup` 命令备份 Red Hat Virtualization Manager。在 `--scope` 中附加以下选项之一以指定要执行的备份：

- **All** : Manager 中所有数据库和配置文件的完整备份
- **文件** : 仅备份系统中的文件

- **db** : 仅备份 **Manager** 数据库
- **dwhdb** : 仅 **Data Warehouse** 数据库的备份



重要

要将数据库恢复到全新安装的 **Red Hat Virtualization Manager**, 仅数据库备份是不够的, 管理器也需要访问配置文件。指定默认范围以外的任何备份都必须由 **文件范围**或**文件系统备份**配套。

engine-backup 命令的使用情况示例

1. 登录到运行 **Red Hat Virtualization Manager** 的机器。

2. 创建备份 :

例 16.1. 创建完整备份

```
# engine-backup --scope=all --mode=backup --file=file_name --log=log_file_name
```

例 16.2. 创建 **Manager** 数据库备份

```
# engine-backup --scope=files --scope=db --mode=backup --file=file_name --log=log_file_name
```

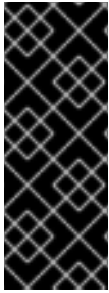
将 **db** 选项替换为 **dwhdb** 以备份数据仓库数据库。

使用提供的路径和文件名创建包含备份的 **tar** 文件。

现在, 可以使用包含备份的 **tar** 文件来恢复环境。

16.1.4. 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地来创建备份。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

备份只能恢复到与备份环境同一主版本的环境。例如，Red Hat Virtualization 版本 4.2 环境的备份只能恢复到另一个 Red Hat Virtualization 版本 4.2 环境。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。

16.1.5. 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。

将备份恢复到刷新安装

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 --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 --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 --provision-db --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 --provision-dwh-db --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.
```

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，请参阅第 22.1.1 节“oVirt Engine Rename 工具”。

16.1.6. 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
```

16.1.7. 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证未知，则必须在恢复备份前更改它们。

使用不同凭证恢复备份

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. **如果该用户的凭证未知，则更改引擎数据库所有者的密码：**

- a. **输入 `postgresql` 命令行：**

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

16.1.8. 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。

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。备份文件中的管理器版本必须与新管理器的版本匹配。请参阅 [《升级指南》中的更新 Red Hat Virtualization Manager](#)。

- 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 [第 15.7 节“从自托管引擎环境中删除主机”](#)。
- 添加新的常规主机。请参阅 [第 10.5.1 节“在 Red Hat Virtualization Manager 中添加标准主机”](#)。

16.1.8.1. 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。

16.1.8.2. 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。如果您要在 Red Hat Virtualization Host 上部署，则默认提供自托管引擎部署工具。如果要在 Red Hat Enterprise Linux 上部署，必须安装该软件包：

```
# yum install ovirt-hosted-engine-setup
```

3. 红帽建议使用 `screen` 工具程序运行该脚本，以避免在网络或终端中断时丢失会话。安装并运行 `screen`：

```
# yum install screen  
# screen
```

如果发生会话超时或连接中断，请运行 `screen -d -r` 来恢复部署会话。

4. 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。

5.

选择 **Yes** 以开始部署。

6.

配置网络。脚本会检测可能的 NIC，以用作环境的管理网桥。

7.

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。

8.

指定 Manager 虚拟机的 FQDN。

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.

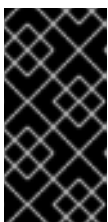
输入虚拟机的 CPU 和内存配置。

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。

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 3 Gluster 存储。确定您有以下配置：

- 在所有三个 Gluster 服务器上的 `/etc/glusterfs/glusterd.vol` 文件中，将 `rpc-auth-allow-insecure` 设置为 `on`。

```
option rpc-auth-allow-insecure on
```

- 配置卷，如下所示：

```
gluster volume set _volume_ cluster.quorum-type auto
gluster volume set _volume_ network.ping-timeout 10
gluster volume set _volume_ auth.allow \*
gluster volume set _volume_ group virt
gluster volume set _volume_ storage.owner-uid 36
gluster volume set _volume_ storage.owner-gid 36
gluster volume set _volume_ server.allow-insecure on
```

- 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。要重复使用现有的 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。

16.1.8.3. 启用 Red Hat Virtualization Manager 存储库

在 Red Hat Subscription Manager 中注册系统，附加 Red Hat Virtualization Manager 订阅并启用 Manager 软件仓库。

流程

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

```
# subscription-manager register
```



注意

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

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

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

3. 使用池 ID 将订阅附加到系统：

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



注意

查看当前附加的订阅：

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

列出所有启用的软件仓库：

```
# yum repolist
```

4.

配置存储库：

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

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。

16.1.8.4. 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。

先决条件

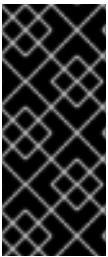
- 如果在集群级别启用了迁移，则虚拟机会自动迁移到集群中的其他主机。因此，建议在主机使用相对较低的时执行主机重新安装。
- 确保集群有足够的内存，以便其主机执行维护。如果集群缺少足够内存，虚拟机迁移操作将挂起，然后失败。您可以在将主机移到维护之前，通过关闭一些或所有虚拟机来减少此操作的内存用量。
- 在执行重新安装前，请确保集群包含多个主机。不要尝试同时重新安装所有主机，因为一个主机必须保持可用才能执行存储池管理器(SPM)任务。

流程

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

3. 单击 **Installation** 以打开 **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**。

成功重新安装后，主机会显示 **Up** 状态。任何从主机迁移的虚拟机现在都可以迁移到该主机。



重要

在 Red Hat Virtualization Manager 成功注册到 Red Hat Virtualization Manager 后，它可能会错误地出现在管理门户中，状态为 **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。

16.1.8.5. 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. 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。

16.1.9. 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。

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。

16.1.9.1. 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。如果您要在 Red Hat Virtualization Host 上部署，则默认提供自托管引擎部署工具。如果您要在 Red Hat Enterprise Linux 上部署，必须安装该软件包：

```
# yum install ovirt-hosted-engine-setup
```

3.

红帽建议使用 **screen** 工具程序运行该脚本，以避免在网络或终端中断时丢失会话。安装并运行 **screen**：

```
# yum install screen
# screen
```

如果发生会话超时或连接中断，请运行 **screen -d -r** 来恢复部署会话。

4.

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。

5.

选择 **Yes** 以开始部署。

6.

配置网络。脚本会检测可能的 **NIC**，以用作环境的管理网桥。

7.

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**。

8.

指定 **Manager** 虚拟机的 **FQDN**。

9.

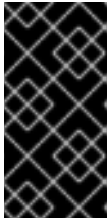
输入 **Manager** 的 **root** 密码。

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。
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 3 Gluster 存储。确定您有以下配置：

- 在所有三个 Gluster 服务器上的 `/etc/glusterfs/glusterd.vol` 文件中，将 `rpc-auth-allow-insecure` 设置为 `on`。

```
option rpc-auth-allow-insecure on
```

- 配置卷，如下所示：

```
gluster volume set _volume_ cluster.quorum-type auto
gluster volume set _volume_ network.ping-timeout 10
gluster volume set _volume_ auth.allow \*
gluster volume set _volume_ group virt
gluster volume set _volume_ storage.owner-uid 36
gluster volume set _volume_ storage.owner-gid 36
gluster volume set _volume_ server.allow-insecure on
```

- 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。要重复使用现有的 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。

16.1.9.2. 启用 Red Hat Virtualization Manager 存储库

在 Red Hat Subscription Manager 中注册系统，附加 Red Hat Virtualization Manager 订阅并启用 Manager 软件仓库。

流程

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

```
# subscription-manager register
```

**注意**

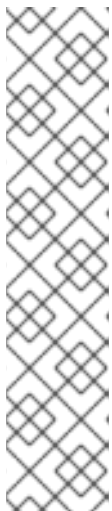
如果您使用 IPv6 网络，请使用 IPv6 转换机制来访问 **Content Delivery Network** 和 **subscription Manager**。

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

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

3. 使用池 ID 将订阅附加到系统：

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

**注意**

查看当前附加的订阅：

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

列出所有启用的软件仓库：

```
# yum repolist
```

4. 配置存储库：

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-7-server-rpms \
  --enable=rhel-7-server-supplementary-rpms \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
```

```
--enable=rhel-7-server-rhv-4-manager-tools-rpms \
--enable=rhel-7-server-ansible-2.9-rpms \
--enable=jb-eap-7.2-for-rhel-7-server-rpms
```

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。

16.1.9.3. 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。

先决条件

- 如果在集群级别启用了迁移，则虚拟机会自动迁移到集群中的其他主机。因此，建议在主机使用相对较低的时执行主机重新安装。
- 确保集群有足够的内存，以便其主机执行维护。如果集群缺少足够内存，虚拟机迁移操作将挂起，然后失败。您可以在将主机移到维护之前，通过关闭一些或所有虚拟机来减少此操作的内存用量。
- 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，因为一个主机必须保持可用才能执行存储池管理器(SPM)任务。

流程

1. 单击 **Compute** → **Hosts**，再选择主机。
2. 单击 **Management** → **Maintenance**。
3. 单击 **Installation** 以打开 **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。

成功重新安装后，主机会显示 Up 状态。任何从主机迁移的虚拟机现在都可以迁移到该主机。



重要

在 Red Hat Virtualization Manager 成功注册到 Red Hat Virtualization Manager 后，它可能会错误地出现在管理门户中，状态为 **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。

16.1.9.4. 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。

16.1.10. 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` 选项的详情请参考 [第 16.1 节“备份和恢复 Red Hat Virtualization Manager”](#)。

16.1.10.1. 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.

在继续之前，确认环境处于维护模式：

```
# hosted-engine --vm-status
```

您应当会看到指出集群处于维护模式的消息。

16.1.10.2. 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
```

16.1.10.3. 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预期执行。

16.2. 将 RED HAT VIRTUALIZATION 数据库迁移到远程服务器

16.2.1. 将 Manager 数据库迁移到远程服务器

在最初配置 Red Hat Virtualization Manager 后，您可以将 Manager (引擎)数据库迁移到远程数据库服务器。使用 `engine-backup` 创建数据库备份，并在新的数据库服务器中恢复它。

新的数据库服务器必须安装有 Red Hat Enterprise Linux 7 并启用所需的存储库：

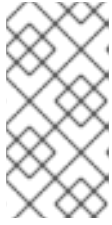
16.2.1.1. 启用 Red Hat Virtualization Manager 存储库

在 Red Hat Subscription Manager 中注册系统，附加 Red Hat Virtualization Manager 订阅并启用 Manager 软件仓库。

流程

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

```
# subscription-manager register
```

**注意**

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

2.

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

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

3.

使用池 ID 将订阅附加到系统：

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

**注意**

查看当前附加的订阅：

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

列出所有启用的软件仓库：

```
# yum repolist
```

4.

配置存储库：

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

将 Manager 数据库迁移到远程服务器

1.

登录到 Red Hat Virtualization Manager 机器并停止 ovirt-engine 服务，使其不会影响到引擎备份：

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

2.

创建 engine 数据库备份：

```
# engine-backup --scope=files --scope=db --mode=backup --file=file_name --
log=log_file_name
```

3.

将备份文件复制到新的数据库服务器：

```
# scp /tmp/engine.dump root@new.database.server.com:/tmp
```

4.

登录到新的数据库服务器并安装 engine-backup：

```
# yum install ovirt-engine-tools-backup
```

5.

在新数据库服务器上恢复数据库。file_name 是从 Manager 复制的备份文件。

```
# engine-backup --mode=restore --scope=files --scope=db --file=file_name --
log=log_file_name --provision-db --no-restore-permissions
```

6.

现在数据库已迁移，启动 ovirt-engine 服务：

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

16.2.2. 将自托管引擎数据库迁移到远程服务器

在对 Red Hat Virtualization Manager 进行了初始配置后，也可以将自托管引擎的 engine 数据库迁移到远程数据库服务器。使用 engine-backup 创建数据库备份，并在新的数据库服务器中恢复它。

新的数据库服务器必须安装有 Red Hat Enterprise Linux 7 并启用所需的存储库：

启用 Red Hat Virtualization Manager 存储库

在 Red Hat Subscription Manager 中注册系统，附加 Red Hat Virtualization Manager 订阅并启用 Manager 软件仓库。

流程

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

```
# subscription-manager register
```

**注意**

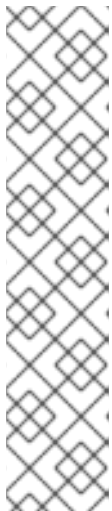
如果您使用 IPv6 网络，请使用 IPv6 转换机制来访问 Content Delivery Network 和 subscription Manager。

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

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

3. **使用池 ID 将订阅附加到系统：**

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

**注意**

查看当前附加的订阅：

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

列出所有启用的软件仓库：

```
# yum repolist
```

4. **配置存储库：**

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


将自托管引擎数据库迁移到远程服务器

1. **登录自托管引擎节点，并将环境置于全局维护模式。这会禁用高可用性代理，并防止 Manager 虚拟机在流程中迁移：**

```
# hosted-engine --set-maintenance --mode=global
```

2. **登录到 Red Hat Virtualization Manager 机器并停止 ovirt-engine 服务，使其不会影响到引擎备份：**

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

3. **创建 engine 数据库备份：**

```
# engine-backup --scope=files --scope=db --mode=backup --file=file_name --log=backup_log_name
```

4. **将备份文件复制到新的数据库服务器：**

```
# scp /tmp/engine.dump root@new.database.server.com:/tmp
```

5. **登录到新的数据库服务器并安装 engine-backup：**

```
# yum install ovirt-engine-tools-backup
```

6. **在新数据库服务器上恢复数据库。file_name 是从 Manager 复制的备份文件。**

```
# engine-backup --mode=restore --scope=files --scope=db --file=file_name --log=restore_log_name --provision-db --no-restore-permissions
```

7. **现在数据库已迁移，启动 ovirt-engine 服务：**

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

8. **登录到自托管引擎节点并关闭维护模式，启用高可用性代理：**

```
# hosted-engine --set-maintenance --mode=none
```

16.2.3. 将数据仓库迁移到独立机器

本节论述了如何将数据仓库数据库和服务从 Red Hat Virtualization Manager 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，并可以使每个服务避免与其他进程共享 CPU 和内存资源导致的潜在冲突。

您可以迁移数据仓库服务，并将它与现有的数据仓库数据库(ovirt_engine_history)连接，也可以在迁移数据仓库服务之前将数据仓库数据库迁移到单独的计算机。如果数据仓库数据库托管在 Manager 上，在 Data Warehouse 服务之外迁移数据库也会进一步降低 Manager 计算机上资源的竞争。您可以将数据库迁移到将数据仓库服务迁移到与 Manager 机器和新数据仓库服务机器独立的机器上。

16.2.3.1. 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。

要只迁移数据仓库服务，请参阅第 16.2.3.2 节“将数据仓库服务迁移到独立机器”。

新的数据库服务器必须安装有 Red Hat Enterprise Linux 7。在新数据库服务器上启用所需的存储库。

启用 Red Hat Virtualization Manager 存储库

在 Red Hat Subscription Manager 中注册系统，附加 Red Hat Virtualization Manager 订阅并启用 Manager 软件仓库。

流程

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

```
# subscription-manager register
```



注意

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

2.

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

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

3.

使用池 ID 将订阅附加到系统 :

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



注意

查看当前附加的订阅 :

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

列出所有启用的软件仓库 :

```
# yum repolist
```

4.

配置存储库 :

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

将数据仓库数据库迁移到独立机器

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=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** :

```
# yum install ovirt-engine-tools-backup
```

4.

安装 **PostgreSQL** 服务器软件包 :

```
# yum install rh-postgresql10 rh-postgresql10-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 :

```
# scl enable rh-postgresql10 -- postgresql-setup --initdb
# systemctl enable rh-postgresql10-postgresql
# systemctl start rh-postgresql10-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=dwhdb --file=file_name --
log=log_file_name --provision-dwh-db --no-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。

16.2.3.2. 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 [第 16.2.3.1 节“将数据仓库数据库迁移到独立机器”](#)。

先决条件

•

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 [第 16.2.3.1 节](#) “将数据仓库数据库迁移到独立机器” 迁移了 `ovirt_engine_history` 数据库，备份包括这些凭证，您可以在该机器的数据库设置过程中定义这些凭证。**

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](#)

16.2.3.2.1. 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 7 机器上安装 Data Warehouse setup 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-7-server-rpms \
  --enable=rhel-7-server-supplementary-rpms \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=rhel-7-server-rhv-4-manager-tools-rpms \
  --enable=rhel-7-server-ansible-2.9-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms
```

2.

确保当前安装的所有软件包都为最新版本 :

```
# yum update
```

3.

安装 ovirt-engine-dwh-setup 软件包 :

```
# yum install ovirt-engine-dwh-setup
```

16.2.3.2.2. 在 Manager 机器上停止数据仓库服务

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/opt/rh/rh-postgresql10/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。

有关如何配置和迁移数据仓库数据库的更多信息，请参阅第 16.2.3.1 节“将数据仓库数据库迁移到独立机器”。

3.

重启 postgresql 服务：

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

16.2.3.2.3. 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.

运行 `engine-setup` 命令，开始在机器上配置数据仓库：

```
# engine-setup
```

3.

按 **Enter** 键配置数据仓库：

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

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。

16.2.3.2.4. 在 **Manager** 机器上禁用数据仓库服务

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
```

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。

16.3. 使用备份存储域备份和恢复虚拟机

16.3.1. 备份存储域解释

备份存储域是一个用来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center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。

16.3.2. 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。

16.3.3. 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 [第 16.3.2 节“将数据存储域设置为备份域”](#)。
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[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 [第 11.7.5 节“从导入的 Data Storage Domains 导入虚拟机”](#)。

相关信息

- [第 11.7.2 节“导入存储域”](#)
- [第 11.7.3 节“在 Same 环境中数据中心之间迁移存储域”](#)
- [第 11.7.4 节“在不同环境中在数据中心间迁移存储域”](#)
- [第 11.7.5 节“从导入的 Data Storage Domains 导入虚拟机”](#)

16.4. 使用备份和恢复 API 备份和恢复虚拟机

16.4.1. 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](#)。

16.4.2. 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。

备份虚拟机

1.

使用 REST API，创建要备份的虚拟机的快照：

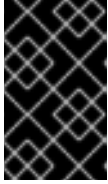
```
POST /api/vms/{vm:id}/snapshots/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

<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在快照下 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**

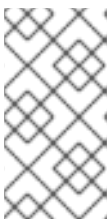
在这里，将 {vm:id} 替换为备份虚拟机的 ID，而不是您之前生成快照的虚拟机。将 {snapshot:id} 替换为快照 ID。

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。

16.4.3. 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。

恢复虚拟机

1. 在管理门户中，创建一个浮动磁盘来恢复备份。如需了解如何创建浮动磁盘的详情，请参阅第 13.6.1 节“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} 替换为此备份虚拟机的 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>
```

+ 备注：这里，将 {vm:id} 替换为此备份虚拟机的 ID，而不是您之前生成快照的虚拟机。将 {disk:id} 替换为磁盘 ID。

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。

第 17 章 使用 RED HAT SATELLITE 管理勘误

Red Hat Virtualization 可以配置为查看 Red Hat Virtualization Manager 中的 Red Hat Satellite 的勘误。这可让管理员收到有关可用勘误表的更新，以及主机、虚拟机和管理器在与 Red Hat Satellite 供应商相关联后的重要性。然后，管理员可以选择通过在所需主机、虚拟机或 Manager 上运行更新来应用更新。有关 Red Hat Satellite 的更多信息，请参阅 [Red Hat Satellite 文档](#)。

Red Hat Virtualization 4.3 支持使用 Red Hat Satellite 6.5 进行勘误管理。



重要

Manager、主机和虚拟机通过其 FQDN 在卫星服务器中标识。这样可确保外部内容主机 ID 无需在 Red Hat Virtualization 中维护。

用于管理 Manager、主机和虚拟机的卫星帐户必须具有管理员权限和默认的组织集。

Configuring Red Hat Virtualization Errata

要将管理器、主机和虚拟机与 Red Hat Satellite 供应商相关联，首先管理器必须与提供程序相关联。然后，主机与同一提供程序进行了关联并进行了配置。最后，虚拟机与同一提供程序并进行了配置。

1. 将所需的卫星服务器添加为外部提供者来关联 Manager。如需更多信息，请参阅 [第 14.2.1 节“为主机调配添加 Red Hat Satellite 实例”](#)。



注意

管理器必须作为内容主机注册到卫星服务器，并且安装了 `katello-agent` 软件包。

有关如何配置主机注册的更多信息，请参阅 Red Hat Satellite 文档中的注册主机。https://access.redhat.com/documentation/en-us/red_hat_satellite/6.5/html/managing_hosts/registering_hosts

2. (可选) 配置所需的主机以显示可用的勘误表。如需更多信息，请参阅 [第 10.5.3 节“为主机配置 Satellite 勘误管理”](#)。

3. (可选) 配置所需的虚拟机以显示可用的勘误表。在配置所需的虚拟机之前，需要配置相关的主机。如需更多信息，请参阅虚拟机管理指南中的虚拟机配置 [Red Hat Satellite 勘误管理](#)。

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。

有关查看主机的可用勘误的详情，请参考 [第 10.5.21 节“查看主机勘误”](#) 和虚拟机，请参阅 [虚拟机管理指南中的虚拟机的 Red Hat Satellite 勘误](#)。

第 18 章 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。Ansible 包含对 Red Hat Virtualization 的支持，Ansible 模块可用于自动执行安装后任务，如数据中心设置和配置、管理用户或虚拟机操作。

Ansible 提供了与 REST API 和 SDK 相比自动化 Red Hat Virtualization 配置的简单方法，并允许您与其他 Ansible 模块集成。有关 Red Hat Virtualization 可用的 Ansible 模块的更多信息，请参阅 Ansible 文档中的 [Ovirt 模块](#)。



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。

Ansible 由 Red Hat Virtualization 提供。要安装 Ansible，请在 Manager 机器中运行以下命令：

```
# yum install ansible
```

有关使用 [Ansible](#) 的替代安装说明，请参阅 [Ansible 文档](#)。



注意

要在运行 Ansible playbook 时永久提高 Manager 的详细级别，请在 `/etc/ovirt-engine/engine.conf.d/` 中创建配置文件，并添加以下行：

```
ANSIBLE_PLAYBOOK_VERBOSE_LEVEL=4
```

运行 `systemctl restart ovirt-engine` 创建该文件后，您必须重启 Manager。

18.1. ANSIBLE 角色

有多个 Ansible 角色可用于帮助配置和管理 Red Hat Virtualization 基础架构的各个部分。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。

可用于 Red Hat Virtualization 的 Ansible 角色由各种内部组件分类。如需有关 Ansible 角色的更多信息，请参阅 [oVirt Ansible Roles](#) 文档。有关使用 Ansible 角色安装的文档，请参阅 [第 18.1.1 节“安装 Ansible 角色”](#)。

18.1.1. 安装 Ansible 角色

您可以从 Red Hat Virtualization Manager 仓库为 Red Hat Virtualization 安装 Ansible 角色。使用以下命令在 Manager 机器上安装 Ansible 角色：

```
# yum install ovirt-ansible-roles
```

默认情况下，角色安装到 `/usr/share/ansible/roles` 中。ovirt-ansible-roles 软件包的结构如下：

- `/usr/share/ansible/roles` - 存储角色。
- `/usr/share/doc/ovirt-ansible-roles/` - 存储示例、基本概述和 licence。
- `/usr/share/doc/ansible/roles/role_name` - 存储特定于该角色的文档。

18.1.2. 使用 Ansible 角色配置 Red Hat Virtualization

以下流程指导您创建并运行使用 Ansible 角色配置 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。

先决条件

- 确保 `/etc/ansible/ansible.cfg` 中的 `roles_path` 选项指向 Ansible 角色的位置 (`/usr/share/ansible/roles`)。
- 确保在运行 playbook 的机器上安装了 Python SDK。

使用 Ansible 角色配置 Red Hat Virtualization

1. 在工作目录中创建用于存储 Red Hat Virtualization Manager 用户密码的文件：

```
# cat passwords.yml
---
engine_password: youruserpassword
```

2. 加密用户密码。系统将要求您提供 Vault 密码。

```
# ansible-vault encrypt passwords.yml
New Vault password:
Confirm New Vault password:
```

3. 创建存储 Manager 详情的文件，如 URL、证书位置和用户。

```
# cat engine_vars.yml
---
engine_url: https://example.engine.redhat.com/ovirt-engine/api
engine_user: admin@internal
engine_cafile: /etc/pki/ovirt-engine/ca.pem
```



注意

如果您愿意，可以直接将这些变量添加到 **playbook** 中。

4. 创建 **playbook**。要简化这一操作，您可以在 `/usr/share/doc/ovirt-ansible-roles/examples` 中复制和修改示例。

```
# cat rhv_infra.yml
---
- 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:
- name: Login to RHV
  ovirt_auth:
    url: "{{ engine_url }}"
    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: 4.1

roles:
- ovirt-datacenters

post_tasks:
- name: Logout from RHV
  ovirt_auth:
    state: absent
    ovirt_auth: "{{ ovirt_auth }}"
  tags:
    - always

```

5.

运行 `playbook`。

```
# ansible-playbook --ask-vault-pass rhv_infra.yml
```

您已成功使用 `ovirt-datacenters` Ansible 角色创建名为 `mydatacenter s` 的数据中心。

第 19 章 用户和角色

19.1. 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。

19.2. DIRECTORY 服务器介绍

在安装过程中，Red Hat Virtualization Manager 在内部域中创建一个 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 Standard Schema*
- *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 (rhev)** 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 <http://technet.microsoft.com/en-us/library/cc732336.aspx>。

有关 Active Directory 中控制委托的详情，请参考 <http://technet.microsoft.com/en-us/library/cc732524.aspx>。

19.3. 配置外部 LDAP 供应商

19.3.1. 配置外部 LDAP 提供程序（活动设置）

`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，请参阅第 19.3.3 节“配置外部 LDAP 提供程序(Manual Method)”。

有关 Active Directory 示例，请参考第 19.3.2 节“附加 Active Directory”。

先决条件：

- 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。

配置外部 LDAP 供应商

1.

在 **Red Hat Virtualization Manager** 中，安装 **LDAP 扩展软件包**：

```
# yum 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 [第 19.3.2 节“附加 Active Directory”](#) 的步骤操作。

```
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 19.1. 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，如要登录到虚拟机门户，请参阅 [第 19.7 节“从管理门户管理用户任务”](#)。

```
# 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。

19.3.2. 附加 Active Directory

先决条件

- 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 [第 D.2 节“在 Manager 和 LDAP 服务器间设置加密通信”](#)。
- 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。

配置外部 LDAP 供应商

1. 在 Red Hat Virtualization Manager 中，安装 LDAP 扩展软件包：

```
# yum 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.

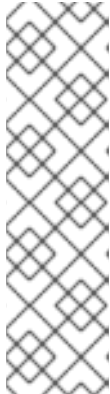
Only in cases in which the startTLS is not supported, fallback to non standard ldaps protocol.

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 [第 D.2 节“在 Manager 和 LDAP 服务器间设置加密通信”](#)。

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 19.2. 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，如要登录到虚拟机门户，请参阅第 19.7 节“从管理门户管理用户任务”。



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。

19.3.3. 配置外部 LDAP 提供程序(Manual Method)

`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。

手动配置外部 LDAP 供应商

1.

在 Red Hat Virtualization Manager 中，安装 LDAP 扩展软件包：

```
# yum 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 19.1. 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 [第 D.2 节“在 Manager 和 LDAP 服务器间设置加密通信”](#)。

例 19.2. 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 19.3. 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-
extensions.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.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 19.4. 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-
extensions.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
```

```
org.ovirt.engineextensions.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。要在 LDAP 服务器中为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 [第 19.7 节“从管理门户管理用户任务”](#)。



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。

19.3.4. 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。

删除外部 LDAP 供应商

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**。

19.4. 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。

本例假定如下：

- 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。

在 Red Hat Virtualization Manager 中

- 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。

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-rhev@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-rhev@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@rhev.example.com:/etc/httpd
```

在虚拟机门户或管理门户中配置单点登录

1. 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
```

2.

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：

```
# yum install ovirt-engine-extension-aaa-misc ovirt-engine-extension-aaa-ldap
mod_auth_gssapi mod_session
```

3.

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
```

4.

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
```

5.

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 19.5. 身份验证方法文件示例

```
<LocationMatch ^/ovirt-engine/sss/(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>

```

6.

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
```

7.

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 19.6. 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>

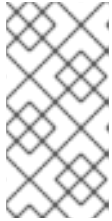
# Server
#
vars.server = ldap1.company.com

# 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，请参阅第 D.2 节“在 Manager 和 LDAP 服务器间设置加密通信”。

例 19.7. 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
```

8.

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 19.8. 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-
extensions.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.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
```

9.

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 19.9. 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-
extensions.aaa ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.aaa ldap.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties
```

10.

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 19.10. 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-
extensions.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.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}
```

11.

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
```

12.

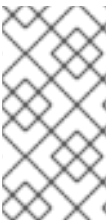
重启 Apache 服务和 ovirt-engine 服务：

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

19.5. 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：

- **Install 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。**



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。

19.5.1. Installing Red Hat Single Sign-On

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。**

19.5.2. 配置 LDAP 组映射器

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` 和 `ovirt-app-admin` 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。**

19.5.3. 在 Manager 中配置 Apache

1. **在 Manager 中配置 Apache。**

```
# yum install mod_auth_openidc
```

2. **在 `/etc/httpd/conf.d` 中创建一个新的 `httpd` 配置文件 `ovirt-openidc.conf`，其内容如下：**

```
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>
```

3.

要保存配置更改，请重启 `httpd` 和 `ovirt-engine`：

```
# systemctl restart httpd
# systemctl restart ovirt-engine
```

4.

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-extensions.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.aaa.misc.http.AuthnExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = openidchttp
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
```

5.

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-extensions.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.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}
```

6.

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-extensions.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.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
```

7.

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
```

19.5.4. 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。

1.

在 `/etc/ovirt-provider-ovn/conf` 中创建文件 `20-setup-ovirt-provider-ovn/conf.d/`，其中 `user1` 属于 LDAP 组 `ovirt-administrator`，而 `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。

19.6. 用户授权

19.6.1. 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

19.6.2. 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。

19.7. 从管理门户管理用户任务

19.7.1. 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。

添加用户和分配虚拟机门户权限

1. 在标题栏中，单击 **Administration** → **Configure** 以打开 **Configure** 窗口。
2. 点 **System Permissions**。

3. 单击 **Add** 以打开 **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. 单击 **OK**。

登录虚拟机门户，以验证用户帐户是否具有登录的权限。

19.7.2. 查看用户信息

查看用户信息

1. 单击 **Administration** → **Users** 以显示授权用户列表。
2. 单击用户名以打开详情视图，通常使用 **General** 选项卡显示常规信息，如用户的域名、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。

19.7.3. 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。

查看用户权限资源

1. 找到并单击资源的名称以打开详情视图。
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。

19.7.4. 删除用户

当不再需要用户帐户时，将其从 Red Hat Virtualization 中删除。

删除用户

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。

19.7.5. 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**。

19.7.6. 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. 点击 **OK**。

19.8. 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。

19.8.1. 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，请参阅第 19.7.1 节“添加用户和分配虚拟机门户权限”。

19.8.2. 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`。在这个示例中，`-0800` 代表 GMT minus 8 小时。如需了解更多选项，请运行 `ovirt-aaa-jdbc-tool 用户密码-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。

19.8.3. 设置用户超时

您可以设置用户超时时间：

```
# engine-config --set UserSessionTimeoutInterval=integer
```

19.8.4. 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
```

19.8.5. 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。

19.8.6. 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
```

19.8.7. 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 [第 19.7.4 节“删除用户”](#)。

19.8.8. 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。

禁用内部管理用户

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 [第 19.7.1 节“添加用户和分配虚拟机门户权限”](#)。
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`

19.8.9. 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。

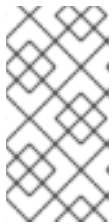
1. 登录到安装 Red Hat Virtualization Manager 的机器。

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，请参阅第 19.7.1 节“添加用户和分配虚拟机门户权限”。

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，请参阅第 19.7.1 节“添加用户和分配虚拟机门户权限”。

19.8.10. 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"
```

19.8.11. 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`。

19.9. 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。

第 20 章 配额和服务等级协议政策

20.1. 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 20.1. 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 20.2. 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。

20.2. 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。

20.3. 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 20.1. 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。

20.4. 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。

在数据中心中启用和更改配额

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。

20.5. 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。

创建新配额策略

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. 单击 **Edit**，以打开 **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. 单击 **Edit**, 以打开 **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**。

20.6. QUOTA THRESHOLD SETTINGS 的解释

表 20.3. 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。

设置	定义
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。

20.7. 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. 点击 **OK**。

为虚拟磁盘分配配额

1. 单击 **Compute** → **Virtual Machines**。
2. 点虚拟机名称打开详情视图。

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. 点击 **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。

20.8. 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。

将用户分配给配额

1. 单击 **Administration** → **Quota**。
2. 点击目标配额的名称打开详情视图。
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。

20.9. 编辑配额

这个步骤描述了如何更改现有配额。

编辑配额

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。**

20.10. 删除配额

这个步骤描述了如何删除配额。

删除配额

1. **单击 Administration → Quota, 再选择配额。**

2. 单击 **Remove**。
3. 单击 **OK**。

20.11. 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。

设置服务级别协议 CPU 策略

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。

第 21 章 事件通知

21.1. 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。**

配置事件通知

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。

21.2. 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。

取消事件通知

1. 单击 **Administration** → **Users**。
2. 点用户的 **User Name** 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. 点击 **OK**。

21.3. 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 21.1. `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）。
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。

变量名称	默认	备注
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。
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。例如， 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。
SENSITIVE_KEYS	\${SENSITIVE_KEYS},MAIL_PASSWORD	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。

变量名称	默认	备注
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_MANAGER	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	默认 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。
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）。
IS_HTTPS_PROTOCOL	false	如果 JBoss 在安全模式下运行，则此条目必须设为 true 。

变量名称	默认	备注
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。

21.4. 配置 RED HAT VIRTUALIZATION MANAGER 以发送 SNMP TRAPS

配置您的 Red Hat Virtualization Manager，将简单的网络管理协议陷阱发送到一个或多个外部 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。

此流程假设您配置了一个或多个外部 SNMP 管理器以接收陷阱，并且您具有以下详情：

- 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；默认情况下，这是 UDP 端口 162。
- SNMP 社区。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。



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。以下流程中所述的值基于该文件中提供的默认值或示例值。建议您定义一个覆盖文件，而不是编辑 `ovirt-engine-notifier.conf` 文件，以在系统升级等更改后保留您的配置选项。

在 Manager 上配置 SNMP Traps

1. 在 Manager 中，创建 **SNMP** 配置文件：

```
# vi /etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf
```

2. 指定 **SNMP Manager (s)**、**NMP 社区** 和 **OID**，格式为：

```
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. 定义要发送到 **SNMP** 管理器的事件：

例 21.1. 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。

4.

保存该文件。

5.

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。

第 22 章 工具

22.1. OVIRT ENGINE RENAME 工具

22.1.1. 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`

**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。

22.1.2. 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` 命令更改的文件的路径和文件名。

22.1.3. 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。



重要

`ovirt-engine-rename` 命令不会更新 SSL 证书，如 `imageio-proxy` 或 `websocket-proxy`。在运行 `ovirt-engine-rename` 后，必须手动更新这些。请参阅以下 [更新 SSL 证书](#)。

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。

使用 oVirt Engine Rename 工具

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的 `/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**。

更新 SSL 证书

在 **ovirt-engine-rename** 命令后面运行以下命令以更新 **SSL 证书**：

```
1. # names="websocket-proxy imageio-proxy"
```

```
2. # subject="$(\n  openssl x509 \n
```

```
-in /etc/pki/ovirt-engine/certs/apache.cer \
-noout \
-subject | \
  sed \
    's;subject= \(.*\);|1;'
)"
```

```
3. # ./usr/share/ovirt-engine/bin/engine-prolog.sh
```

```
4. # for name in $names; do
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --keep-key \
    --san=DNS:"${ENGINE_FQDN}"
done
```

22.2. ENGINE 配置工具

22.2.1. 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。

22.2.2. 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
```

22.3. USB 过滤器编辑器

22.3.1. 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“安装与 Red Hat Virtualization Manager 的镜像”下载 USB 过滤编辑器 安装程序。

安装 USB 过滤器编辑器

1. 在 Windows 计算机上，运行您为 USB 过滤器编辑器 下载的 .msi 文件。
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 Secure Copy (SCP) 客户端从 Red Hat Virtualization Manager 中导入和导出过滤策略。适用于 Windows 机器的安全复制工具是 WinSCP (<http://winscp.net>)。

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。

22.3.2. 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 22.1. 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。

Name	Description
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。

22.3.3. 添加 USB 策略

双击桌面上的 **USB 过滤编辑器** 快捷键图标来打开编辑器。

添加 USB 策略

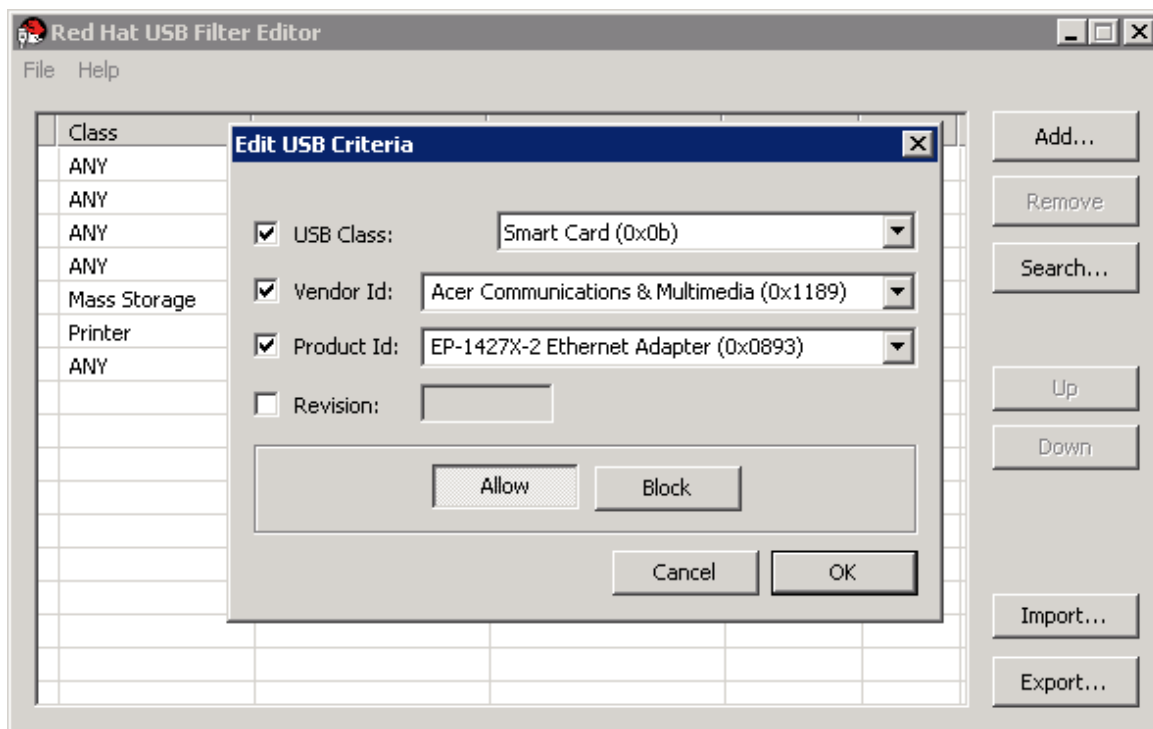
1. 点 **Add**。
2. 使用 **USB 类**、**供应商 ID**、**产品 ID** 和 **Revision** 复选框和列表来指定设备。

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 22.1. 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。USB 过滤器策略必须导出到 *Red Hat Virtualization Manager* 以生效。

22.3.4. 删除 USB 策略

双击桌面上的 *USB 过滤编辑器* 快捷键图标来打开编辑器。

删除 USB 策略

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**。**USB 过滤器策略**必须导出到 **Red Hat Virtualization Manager** 以生效。

22.3.5. 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**快捷图标来打开编辑器。

搜索 USB 设备策略

1. 点 **Search**。**附加 USB 设备** 窗口显示所有附加设备的列表。
2. 选择设备并点击 **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。

22.3.6. 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**快捷图标来打开编辑器。

导出 USB 策略

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
```

22.3.7. 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。

导入 USB 策略

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** 快捷键图标来打开编辑器。
3. 单击 **Import** 以打开 **Open** 窗口。
4. 打开从服务器下载的 `usbfilter.txt` 文件。

22.4. LOG COLLECTOR 工具

22.4.1. 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。

22.4.2. 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 选项

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=DATABASE

将 **DATABASE** 设置为用于连接数据库服务器的数据库名称。默认值为 **rhevm**。

--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。

22.4.3. 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 22.2. 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

```

22.5. ISO 上传程序工具

22.5.1. ISO 上传程序工具



注意

ISO 上传程序工具已弃用。红帽建议使用管理门户或 REST API 将 ISO 镜像上传到数据域。详情请查看 [第 11.8.1 节“将镜像上传到数据存储域”](#)。

ISO 上传程序是将 ISO 镜像上传到 ISO 存储域的工具。它作为 Red Hat Virtualization Manager 的一部分安装。

ISO uploader 命令是 `engine-iso-uploader`。您必须以 root 用户身份登录，并提供 Red Hat Virtualization 环境的管理凭证才能使用此命令。`engine-iso-uploader -h` 命令显示使用信息，包括 `engine-iso-uploader` 命令的所有有效选项列表。

22.5.2. engine-iso-uploader 命令的语法

ISO 上传程序命令的基本语法为：

```

# engine-iso-uploader options list
# engine-iso-uploader options upload file file file

```

ISO 上传程序命令支持两个操作 - 列表，并上传。

- 列表 操作列出了 ISO 文件可以上传到的 ISO 存储域。Red Hat Virtualization Manager 在安装过程中在安装 Manager 的机器中创建此列表。
- 上传 操作会将单个 ISO 文件或多个 ISO 文件上传到指定的 ISO 存储域。默认使用 NFS，但也有可用的 SSH。



注意

如果使用 SSH，系统会多次提示您输入 SSH 用户密码。您可在上传 ISO 文件前将 SSH 密钥上传到 iso 域服务器，然后使用 `--key-file=KEYFILE` 选项来避免这些提示。上传公共 SSH 密钥的一种方法是使用 `ssh-copy-id -i ~/.ssh/mykey user@host` 命令。

使用 ISO 上传程序命令时，您必须指定以上操作之一。此外，您还必须至少指定一个本地文件才能使用上传操作。

有几个参数可以进一步完善 `engine-iso-uploader` 命令。

常规选项

`--version`

显示 ISO 上传程序命令的版本。

`-h,--help`

显示如何使用 ISO 上传程序命令的信息。

`--conf-file=PATH`

将 PATH 设置为要使用的命令的配置文件。默认为 `/etc/ovirt-engine/isouploader.conf`。

`--log-file=PATH`

将 PATH 设置为命令用于写入日志输出的特定文件名。默认值为 `/var/log/ovirt-engine/ovirt-iso-uploader/ovirt-iso-uploader_date.log`。

`--cert-file=PATH`

将 **PATH** 设置为验证引擎的证书。默认为 `/etc/pki/ovirt-engine/ca.pem`。

--insecure

指定不会进行验证引擎的尝试。

--nossll

指定 **SSL** 不会用于连接引擎。

--quiet

设置静默模式，将控制台输出减小到最低限度。

-v,--verbose

设置详细模式，提供更多的控制台输出。

-f,--force

当上传的源文件与目标 **ISO** 域中的现有文件相同时，需要强制模式。此选项强制覆盖现有文件。

Red Hat Virtualization Manager 选项

-u USER, --user=USER

指定用来执行命令的用户。**USER** 以 `用户名@域` 指定。用户必须存在于指定的域中，且对 **Red Hat Virtualization Manager** 所知。

-R FQDN, --engine=FQDN

指定从中上传镜像的 **Red Hat Virtualization Manager** 的 **IP 地址** 或完全限定域名。假设镜像上传器正在从安装 **Red Hat Virtualization Manager** 的同一机器上运行。默认值为 `localhost:443`。

ISO 存储域选项

以下选项指定映像要上传到的 **ISO** 域。这些选项不能同时使用；您必须使用 **-i** 选项或 **-n** 选项。

-i,--iso-domain=ISODOMAIN

将存储域 **ISODOMAIN** 设置为上传的目的地。

-n, --nfs-server=NFSSERVER

将 NFS 路径 NFSSERVER 设置为用于上传的目的地。

连接选项

ISO 上传程序使用 NFS 作为默认上传文件。这些选项指定 SSH 文件传输。

--ssh-user=USER

将 USER 设置为用于上传的 SSH 用户名。默认为 root。

--ssh-port=PORT

将 PORT 设置为在连接到 SSH 时使用的端口。

-k KEYFILE, --key-file=KEYFILE

将 KEYFILE 设置为要用于 SSH 身份验证的私钥。如果没有设置密钥，系统会提示您输入 --ssh-user=USER 指定的用户的密码。在上传 ISO 文件前，您必须将公共 SSH 密钥上传到 ISO 域服务器。其中一种实现方式是使用 `ssh-copy-id -i ~/.ssh/mykey user@host` 命令。

22.5.3. 指定 NFS 服务器

例 22.3. 上传到 NFS 服务器

```
# engine-iso-uploader --nfs-server=storage.demo.redhat.com:/iso/path upload RHEL6.0.iso
```

22.5.4. 基本 ISO 上传程序使用

以下示例演示了 ISO 上传程序和 list 参数。第一个命令列出可用的 ISO 存储域；使用 `admin@internal` 用户，因为命令中没有指定用户。第二个命令将 ISO 文件通过 NFS 上传到指定的 ISO 域。

例 22.4. 列出域和上传镜像

```
# engine-iso-uploader list
Please provide the REST API password for the admin@internal oVirt Engine user (CTRL+D to
abort):
ISO Storage Domain Name | Datacenter      | ISO Domain Status
ISODomain               | Default        | active
```

```
# engine-iso-uploader --iso-domain=[ISODomain] upload [RHEL6.iso]
Please provide the REST API password for the admin@internal oVirt Engine user (CTRL+D to
abort):
```

22.5.5. 将 VirtIO 和客户机工具镜像文件上传到 ISO 存储域



注意

ISO 域是已弃用的存储域类型。ISO 上传程序工具已弃用。红帽建议使用管理门户或 REST API 将 ISO 镜像上传到数据域。详情请查看 [第 11.8.1 节“将镜像上传到数据存储域”](#)。

`virtio-win.iso` 镜像和 Virtual Floppy Drive (VFD) 镜像包含适用于 Windows 虚拟机的 VirtIO 驱动程序，而 `RHV-toolsSetup_version.iso` 包含适用于 Windows 虚拟机的红帽虚拟化客户机工具。这些镜像文件提供您可以在虚拟机上安装的软件，以提高性能和可用性。

要安装并上传 `virtio-win` 和 `RHV-toolsSetup_version.iso` 文件的最新版本：

1.

在 Manager 机器上安装镜像文件：

```
# yum -y install virtio-win rhv-guest-tools-iso*
```

在 Manager 机器上安装后，这些镜像文件是：

- `/usr/share/virtio-win/virtio-win_amd64.vfd (symbolic link)`
- `/usr/share/virtio-win/virtio-win_servers_amd64.vfd (symbolic link)`
- `/usr/share/virtio-win/virtio-win_servers_x86.vfd (symbolic link)`
- `/usr/share/virtio-win/virtio-win_x86.vfd (symbolic link)`
- `/usr/share/virtio-win/virtio-win.iso (symbolic link)`

• `/usr/share/rhv-guest-tools-iso/RHV-toolsSetup_version.iso`



注意

以上符号链接引用名称中版本的文件。当复制或使用 `rsync` 等工具时，请确保复制符号链接的目标。

2.

将镜像文件上传到在安装过程中没有在本机创建的 ISO 存储域中：

```
# yum -y install virtio-win rhv-guest-tools-iso*
# engine-iso-uploader --iso-domain=ISODomain upload \
  /usr/share/virtio-win/virtio-win_amd64.vfd \
  /usr/share/virtio-win/virtio-win_servers_amd64.vfd \
  /usr/share/virtio-win/virtio-win_servers_x86.vfd \
  /usr/share/virtio-win/virtio-win_x86.vfd \
  /usr/share/virtio-win/virtio-win.iso \
  /usr/share/rhv-guest-tools-iso/RHV-toolsSetup_version.iso
```

3.

将镜像文件附加到虚拟机。

虚拟机现在可以使用 `virtio` 驱动程序和客户机工具。

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](#)。

22.6. ENGINE VACUUM 工具

22.6.1. 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/10/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。

22.6.2. 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。

22.6.3. 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
```

22.7. VDSM 到网络名称映射工具

22.7.1. 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

(`vdsm_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：

```
# vdsm_to_network_name_map --user USER
```

其中 `USER` 是有权访问 `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。

部分 IV. 收集有关环境的信息

第 23 章 在 RED HAT VIRTUALIZATION MANAGER 中部署 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。

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
```

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
```

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板视图。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。

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**)。
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，从相关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. **点一个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。**

第 24 章 日志文件

24.1. MANAGER 安装日志文件

表 24.1. 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。

24.2. RED HAT VIRTUALIZATION MANAGER 日志文件

表 24.2. 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。
<code>/var/log/httpd/ovirt-requests-log</code>	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。 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。
<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 。

24.3. 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。

24.3.1. 适用于 Hypervisor SPICE 服务器的 SPICE 日志

表 24.3. 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	/var/log/libvirt/qemu/(guest_name).log	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。

24.3.2. 适用于客户机机器的 SPICE 日志

表 24.4. spice-vmagent Logs for Guest Machines

日志类型	日志位置	更改日志级别：
Windows 客户机	C:\Windows\Temp\vmagent.log C:\Windows\Temp\vmagent-service.log	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>

24.3.3. 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。

24.4. 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。

24.5. 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。

设置主机日志记录服务器

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。

24.6. 启用 OVIRT ENGINE EXTENSION LOGGER LOG4J

日志记录器实施需要 **ovirt-engine-extension-logger-log4j** 软件包。通过实施，**Red Hat Had Virtualization Manager** 将记录委托为 **log4j**。**Log4j** 是一个可自定义框架，可为各种技术（包括 **SNMP** 和 **syslog**）提供附加器。

oVirt Engine Extension Logger log4j 将 engine.log 文件传递给现有的 syslog 服务器。配置过程与设置主机日志记录服务器 重叠。

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 文件从 Manager 传递给 syslog 服务器。

注意

要为此扩展定义 syslog 服务器，请导航到 `/etc/ovirt-engine/extensions.d` 目录，并编辑 `log4j.appender.myappender.myappender.SyslogHost` 的值。

要定义 syslog 工具，请导航到 `/etc/ovirt-engine/extensions.d` 目录，并编辑 `Log4j.appender.myappender.Facility` 文件中的 `log4jLogger.properties` 文件中的值。例如，`log4j.appender.myappender.Facility=local1`。

配置 oVirt Engine Extension Logger log4j

1. 安装扩展名。

```
# yum install ovirt-engine-extension-logger-log4j
```

2. 在 `/etc/ovirt-engine/extensions.d/` 目录中创建 `Log4jLogger.properties` 文件，并包含以下内容：

```
ovirt.engine.extension.name = log4jlogger
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.logger.Logger
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine-extensions.logger.log4j
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.logger.log4j.Log4jLogger
log4j.rootLogger=DEBUG, myappender
log4j.appender.myappender=org.apache.log4j.net.SyslogAppender
log4j.appender.myappender.SyslogHost=localhost
log4j.appender.myappender.layout=org.apache.log4j.PatternLayout
log4j.appender.myappender.layout.ConversionPattern=[%c] %m%n
```

3. 安装和配置 `rsyslog`。

```
# yum install rsyslog
```

4.

配置 SELinux 以允许 rsyslog 流量。

```
# semanage port -a -t syslogd_port_t -p udp 514
```

5.

编辑 `/etc/rsyslog.conf` 并添加以下行：

```
$template TmplAuth, "/var/log/%fromhost%/secure"  
$template TmplMsg, "/var/log/%fromhost%/messages"  
  
$RuleSet remote  
authpriv.* ?TmplAuth  
*.info,mail.none;authpriv.none,cron.none ?TmplMsg  
$RuleSet RSYSLOG_DefaultRuleset  
$InputUDPServerBindRuleset remote
```

6.

取消注释以下两行：

```
#$ModLoad imudp  
#$UDPServerRun 514
```

7.

重启 rsyslog 服务：

```
# systemctl restart rsyslog.service
```

8.

如果启用了防火墙并处于活动状态，请运行以下命令添加在 Firewalld 中打开 rsyslog 端口所需的规则。

```
# firewall-cmd --permanent --add-port=514/udp  
# firewall-cmd --reload
```

9.

重启 Red Hat Virtualization Manager。

```
# restart ovirt-engine
```

现有的 syslog 服务器现在可以接收和存储 engine.log 文件。

附录 A. VDSM 和 HOOK

A.1. VDSM

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。它还联合创建虚拟机创建、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。

A.2. VDSM HOOK

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。

A.3. 使用 HOOK 扩展 VDSM

本章论述了如何通过事件驱动的 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.4. 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。
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。

Name	Description
after_nic_hotunplug_fail	热拔虚拟机中的 NIC 后会失败。
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.5. VDSM HOOK 环境

大多数 hook 脚本都以 vdsmd 用户身份运行，并继承 VDSM 进程的环境。例外是，hook 脚本由 before_vdsmd_start 和 after_vdsmd_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.6. VDSM HOOK 域 XML 对象

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。如下方所述，几个 hook 是此规则的一个例外。以下 hook 的 `_hook_domxml` 变量包含 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的 XML。目标上域的 XML 将具有不同的区别。

VDSM 使用 libvirt 域 XML 格式来定义虚拟机。有关 libvirt 域 XML 格式的详情，请参考 <http://libvirt.org/formatdomain.html>。虚拟机的 UUID 可以从域 XML 中分离，但它也是环境变量 `vmlid`。

A.7. 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: 3.6
UserDefinedVMProperties: version: 4.0
UserDefinedVMProperties : memory=^[0-9]+$ version: 4.0
```

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=4.0
```

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: 3.6
UserDefinedVMProperties: version: 4.0
UserDefinedVMProperties : memory=^[0-9]+$;smartcard=^(true|false)$ version: 4.0
```

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: 3.6
CustomDeviceProperties: version: 4.0
```

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=4.0
```

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: 3.6
UserDefinedVMProperties: version: 4.0
UserDefinedVMProperties : {type=interface;prop={speed=^[0-9]{1,5}$;duplex=^(full|half)$}} version: 4.0
```

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.8. 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.9. 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.10. 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 **xml.dom** 库 (<http://docs.python.org/release/2.6/library/xml.dom.html>) 构建的 Python 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.11. 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 UID，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.12. VDSM HOOK 返回代码

hook 脚本必须返回表 A.3 “hook 返回代码”中显示的返回代码之一。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	hook 脚本成功终止
1	hook 脚本失败，应处理其他 hook
2	hook 脚本失败，不应处理任何进一步 hook
>2	保留

A.13. 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。
gc_timer	设置垃圾回收时间（以秒为单位），之后将检查转发数据库并清除超时条目。
group_addr	在发送常规查询时，设置为零。在发送组特定查询或特定于组的查询时，设置为 IP 多播地址。
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_elasticity	hash 表中允许的最大链长度。在添加了下一个新的多播组前，不会生效。如果在重新哈希后无法满足这种情况，则会发生哈希冲突并禁用侦听。
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。
hello_timer	时间，以 deciseconds，因为发送了最后的 'hello' 消息。
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=4.0
```

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。

```
# yum install vds-hook-ethtool-options
```

`ethtool_opts` 密钥现在包括在管理门户中。请参阅 [第 9.4.2 节“编辑主机网络接口并将逻辑网络分配给主机”](#) 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，可能还需要特殊配置；请参阅 [Red Hat Enterprise Linux Storage Administration Guide](#) 中的[通过以太网接口配置光纤通道](#)。

将 `fcoe` Key 添加到 Manager

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。

```
# yum install vdsm-hook-fcoe
```

fcoe 键现在包括在管理门户中。请参阅 [第 9.4.2 节“编辑主机网络接口并将逻辑网络分配给主机”](#) 将 FCoE 属性应用到逻辑网络。

附录 C. RED HAT VIRTUALIZATION 用户界面插件

C.1. RED HAT VIRTUALIZATION 用户界面插件

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 用户界面插件生命周期

C.2.1. Red Hat Virtualization 用户界面插件生命周期

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.2.2. Red Hat Virtualization 用户界面插件发现

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.2.3. Red Hat Virtualization 用户界面插件

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 serving 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.2.4. Red Hat Virtualization 用户界面插件

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)	<code>/usr/share/ovirt-engine/ui-plugins/my-plugin.json</code>	

File	位置	备注
插件用户配置文件	/etc/ovirt-engine/ui-plugins/my-plugin-config.json	
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!Plug-in

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：

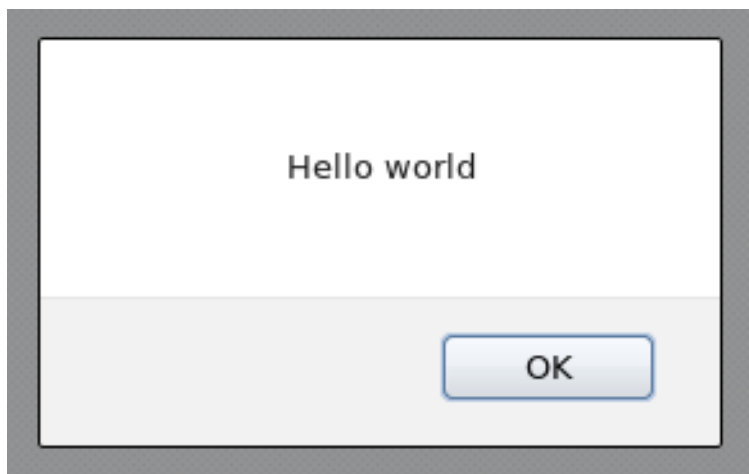
```
{
  "name": "HelloWorld",
  "url": "/ovirt-engine/webadmin/plugin/HelloWorld/start.html",
  "resourcePath": "hello-files"
}
```

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



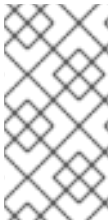
附录 D. RED HAT VIRTUALIZATION 和加密通信

D.1. 替换 RED HAT VIRTUALIZATION MANAGER CA 证书

**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`。

您可以配置您组织的第三方 CA 证书，以标识通过 HTTPS 连接的用户。

**注意**

将第三方 CA 证书用于 HTTPS 连接不会影响在 Manager 和主机之间进行身份验证的证书。它们将继续使用由 Manager 生成的自签名证书。

先决条件

- 第三方 CA 证书。这是发布您要使用的证书的 CA（证书授权）的证书。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。

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](#)。

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)。红帽建议将新文件保存在同一位置。以下步骤假定新的 P12 文件位于 /tmp/apache.p12 中。

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。如果文件受密码保护，您必须添加 `-passin pass:_password_`，用所需的密码替换 `password`。

```
# 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
```

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。如果您从已配置有商业签名的证书的 Red Hat Enterprise Virtualization 3.6 环境升级，则只需要步骤 1、8 和 9。

替换 Red Hat Virtualization Manager Apache CA 证书

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
```

更多信息请参阅 [第 15.1 节“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.

重启 Apache 服务器：

```
# systemctl restart httpd.service
```

10.

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=""
```

11.

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
```

12.

重启 `websocket-proxy` 服务：

```
# systemctl restart ovirt-websocket-proxy.service
```

13.

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。

14.

通过创建新文件 `/etc/ovirt-engine-backup/engine-backup-config.d/update-system-wide-pki.sh` 来启用 `engine-backup` 以在恢复时更新系统：

```
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
```

15.

重启 `ovirt-provider-ovn` 服务：

```
# systemctl restart ovirt-provider-ovn.service
```

16.

重启 `ovirt-engine` 服务：

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

17.

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
```

您的用户现在可以连接到管理门户和虚拟机门户，而不会看到有关加密 HTTPS 流量的证书的真实警告。

D.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 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-version` 的 README 文件的 X.509 CERTIFICATE TRUST STORE 部分。

创建 PEM 编码的 CA 证书

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](#)。

D.3. 为 VDSM 手动设置加密通信

您可以使用 Manager 以及其他 VDSM 实例为 VDSM 手动设置加密通信。

只有集群级别 3.6、4.0 和 4.1 的集群中的主机需要手动配置。具有 4.2 级别的集群中的主机会在主机重新安装过程中自动重新配置为强大的加密。



注意

RHVH 3.6、4.0 和 4.1 主机不支持强大的加密。RHVH 4.2 和 RHEL 主机支持它。

如果您有 3.6、4.0 或带有 RHVH 4.2 主机的 4.1 集群，您可以使用强大的加密功能。

流程

1. 单击 **Compute** → **Hosts**，再选择 **主机**。
2. 单击 **Management** → **Maintenance** 以打开 **Maintenance Host (s)** 确认窗口。
3. 单击 **OK** 以启动维护模式。

4.

在主机上，使用以下设置创建 `/etc/vdsm/vdsm.conf.d/99-custom-ciphers.conf` :

```
[vars]
ssl_ciphers = HIGH
```

如需更多信息，请参阅 [OpenSSL Cipher Strings](#)。

5.

重启 VDSM :

```
# systemctl restart vdsm
```

6.

单击 **Compute** → **Hosts**，再选择 **主机**。

7.

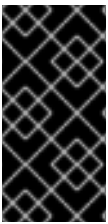
点 **Management** → **Activate** 重新激活主机。

附录 E. 代理

E.1. SPICE 代理

E.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。

E.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。

在 Red Hat Enterprise Linux 上安装 Squid

1. 在 Proxy 机器上安装 Squid :

```
# yum 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。

E.1.3. 开启 **SPICE** 代理

此流程解释了如何激活（或打开）**SPICE** 代理。

激活 **SPICE** 代理

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。

E.1.4. 关闭 SPICE 代理

此流程解释了如何关闭（激活）SPICE 代理。

关闭 SPICE 代理

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。

E.2. SQUID PROXY

E.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。

配置 Squid 代理

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 -subject
```

这个命令输出如下：

```
subject= /C=US/O=Example Inc./CN=engine.example.com.81108
```

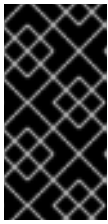
此处的相关部分为 `/C=US/O=Example Inc.`。使用它来为代理构建证书的完整可分辨名称：

```
/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：

```
# yum 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：

```
# yum install polycoreutils-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）。

E.3. WEBSOCKET 代理

E.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。

可在初始配置（请参阅 [配置 Red Hat Virtualization Manager](#)）或单独计算机上在 [Red Hat Virtualization Manager](#) 机器上安装和配置 `websocket` 代理（请参阅在 [9 月 9 日安装 Websocket 代理](#)）。

`websocket` 代理也可以从 `Manager` 机器迁移到独立的机器。请参阅 [第 E.3.2 节“将 Websocket 代理迁移到一个独立的机器”](#)。

E.3.2. 将 Websocket 代理迁移到一个独立的机器

**重要**

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

为了安全起见，`websocket` 代理可以在不运行 `Red Hat Virtualization Manager` 的单独机器上运行。将 `websocket` 代理从 `Manager` 机器迁移到单独的计算机涉及从 `Manager` 机器中删除 `websocket` 代理配置，然后在单独的机器上安装代理。

engine-cleanup 命令可用于从 Manager 机器中删除 websocket 代理：

从 Manager 机器中删除 Websocket 代理

1. 在 Manager 计算机上，运行 **engine-cleanup** 删除所需的配置。

```
# engine-cleanup
```

2. 在要求删除所有组件时键入 **No**，然后按 **Enter** 键。

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

3. 当被要求删除引擎时输入 **No**，然后按 **Enter** 键。

```
Do you want to remove the engine? (Yes, No) [Yes]: No
```

4. 当被要求删除 websocket 代理时，键入 **Yes** 并按 **Enter**。

```
Do you want to remove the WebSocket proxy? (Yes, No) [No]: Yes
```

如果被要求删除任何其他组件，请选择 **No**。

在独立的机器中安装 Websocket 代理

重要

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

websocket 代理允许用户通过 **noVNC** 控制台连接到虚拟机。**noVNC** 客户端使用 **websocket** 传递 **VNC** 数据。但是，**QEMU** 中的 **VNC** 服务器不提供 **websocket** 支持，因此必须在客户端和 **VNC** 服务器之间放置 **websocket** 代理。代理可以在任何可访问网络的机器中运行，包括 **Manager** 机器。

出于安全性和性能的原因，用户可能希望在单独的计算机上配置 **websocket** 代理。

流程

1. **安装 websocket 代理：**

```
# yum install ovirt-engine-websocket-proxy
```

2. **运行 engine-setup 命令以配置 websocket 代理。**

```
# engine-setup
```



注意

如果也安装了 `rhvm` 软件包，则在要求在此主机上配置管理器 (Engine) 时，请选择 **No**。

3. **按 Enter 键，允许 engine-setup 在机器上配置 websocket 代理服务器。**

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

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

```
Host fully qualified DNS name of this server [host.example.com]:
```

5. **按 Enter 键允许 engine-setup 配置防火墙并打开外部通信所需的端口。如果不允许 engine-setup 修改防火墙配置，则必须手动打开所需端口。**

```
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]:
```

6. **输入 Manager 机器的 FQDN，然后按 Enter 键。**

```
Host fully qualified DNS name of the engine server []: manager.example.com
```

7. **按 Enter 键，允许 engine-setup 在 Manager 机器上执行操作，或按 2 以手动执行操作。**

Setup will need 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]:

a.

按 Enter 接受默认的 SSH 端口号，或者输入 Manager 机器的端口号。

ssh port on remote engine server [22]:

b.

输入 root 密码以登录到 Manager 计算机，然后按 Enter 键。

root password on remote engine server engine_host.example.com:

8.

选择是否查看 iptables 规则与当前设置不同。

Generated iptables rules are different from current ones.

Do you want to review them? (Yes, No) [No]:

9.

按 Enter 键确认配置设置。

==== CONFIGURATION PREVIEW ====

```
Firewall manager           : iptables
Update Firewall           : True
Host FQDN                  : host.example.com
Configure WebSocket Proxy  : True
Engine Host FQDN           : engine_host.example.com
```

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

提供了相应的说明，将 Manager 计算机配置为使用配置的 websocket 代理。

Manual actions are required on the engine host
in order to enroll certs for this host and configure the engine about it.

Please execute this command on the engine host:

```
engine-config -s WebSocketProxy=host.example.com:6100
and than restart the engine service to make it effective
```

10.

登录 Manager 机器并执行提供的说明。

```
# engine-config -s WebSocketProxy=host.example.com:6100  
# systemctl restart ovirt-engine.service
```


附录 F. BRANDING

F.1. BRANDING

F.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。

F.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。

F.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。

F.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。

F.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。

F.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。

F.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

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。

F.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 G. 系统帐户

G.1. 系统帐户

G.1.1. Red Hat Virtualization Manager 用户帐户

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。

G.1.2. 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**。

G.1.3. 虚拟化主机用户帐户

安装 `vdsm` 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：

- `vdsm` 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。`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。

G.1.4. 虚拟化主机组

安装 `vdsm` 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。