



Red Hat Virtualization 4.0

管理ガイド

Red Hat Virtualization の管理タスク

Red Hat Virtualization 4.0 管理ガイド

Red Hat Virtualization の管理タスク

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.

法律上の通知

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.

概要

本書には、Red Hat Virtualization の管理者に関する情報および手順が記載されています。

目次

パート I. RED HAT VIRTUALIZATION 環境の管理と保守	13
第1章 グローバル設定	14
1.1. ロール	14
1.1.1. 新しいロールの作成	14
1.1.2. ロールの編集またはコピー	15
1.1.3. ユーザーロールと承認の例	16
1.2. システムパーティション	18
1.2.1. ユーザープロパティー	19
1.2.2. ユーザーおよび管理者ロール	19
1.2.3. ユーザーロールの概要	20
1.2.4. 管理者ロールの概要	21
1.3. スケジューリングポリシー	23
1.3.1. スケジューリングポリシーの作成	24
1.3.2. New Scheduling Policy および Edit Scheduling Policy ウィンドウの設定の説明	26
1.4. インスタンスタイプ	29
1.4.1. インスタンスタイプの作成	30
1.4.2. インスタンスタイプの編集	31
1.4.3. インスタンスタイプの削除	31
1.5. MAC アドレスプール	31
1.5.1. MAC アドレスプールの作成	32
1.5.2. MAC アドレスプールの編集	33
1.5.3. MAC アドレスプールのパーティションの編集	33
1.5.4. MAC アドレスプールの削除	34
第2章 ダッシュボード	35
2.1. 前提条件	35
2.2. グローバルインベントリー	35
2.3. グローバルでの活用	37
2.3.1. 最も使用されているリソース	37
2.4. クラスターの活用	38
2.4.1. CPU	38
2.4.2. メモリー	38
2.5. ストレージの活用	39
パート II. リソースの管理	40
第3章 QOS (QUALITY OF SERVICE)	41
3.1. ストレージ QoS	41
3.1.1. ストレージ QoS エントリーの作成	41
3.1.2. ストレージ Quality of Service エントリーの削除	42
3.2. 仮想マシンのネットワーク QoS	42
3.2.1. 仮想マシンのネットワーク QoS エントリーの作成	42
3.2.2. New Virtual Machine Network QoS および Edit Virtual Machine Network QoS ウィンドウの設定の説明	43
3.2.3. 仮想マシンのネットワーク QoS(Quality of Service) エントリーの削除	43
3.3. ホストネットワーク QoS	44
3.3.1. ホストネットワーク QoS エントリーの作成	44
3.3.2. New Host Network Quality of Service および Edit Host Network Quality of Service ウィンドウの設定の説明	44
3.3.3. ホストネットワーク QoS エントリーの削除	45
3.4. CPU QOS (QUALITY OF SERVICE)	45

3.4.1. CPU QoS エントリーの作成	46
3.4.2. CPU QoS エントリーの削除	46
第4章 データセンター	47
4.1. データセンターの概要	47
4.2. STORAGE POOL MANAGER	48
4.3. SPM の優先度	48
4.4. イベントタブを使用したデータセンターの問題オブジェクトの特定	48
4.5. データセンタータスク	49
4.5.1. 新規データセンターの作成	49
4.5.2. New Data Center および Edit Data Center Windows の設定についての説明	50
4.5.3. データセンターの再初期化: リカバリーハンドル	51
4.5.4. データセンターの削除	52
4.5.5. データセンターの強制削除	52
4.5.6. データセンターの互換バージョンの変更	52
4.6. データセンターおよびストレージドメイン	53
4.6.1. 既存のデータドメインをデータセンターにアタッチ	53
4.6.2. 既存の ISO ドメインをデータセンターにアタッチ	53
4.6.3. 既存のエクスポートドメインをデータセンターにアタッチ	54
4.6.4. データセンターからストレージドメインをデタッチ	54
4.7. データセンターおよびパーミッション	55
4.7.1. データセンターのシステムパーミッションの管理	55
4.7.2. データセンター管理者ロールの概要	55
4.7.3. 管理者またはユーザーロールのリソースへの割り当て	56
4.7.4. リソースからの管理者またはユーザーロールの削除	56
第5章 クラスター	58
5.1. クラスターの概要	58
5.2. クラスタータスク	58
5.2.1. 新規クラスターの作成	58
5.2.2. 新規クラスターの設定および制御の説明およびクラスター ウィンドウの編集	60
5.2.2.1. 一般的なクラスター設定に関する説明	60
5.2.2.2. 最適化設定の説明	64
5.2.2.3. 移行ポリシー設定の説明	65
5.2.2.4. スケジューリングポリシー設定に関する説明	67
5.2.2.5. クラスター コンソール設定の説明	72
5.2.2.6. フェンシングポリシー設定の説明	73
5.2.3. リソースの編集	73
5.2.4. クラスター内のホストの負荷および電源管理ポリシーの設定	73
5.2.5. クラスター内のホストでの MoM ポリシーの更新	76
5.2.6. CPU プロファイル	76
5.2.6.1. CPU プロファイルの作成	76
5.2.6.2. CPU プロファイルの削除	76
5.2.7. 既存の Red Hat Gluster Storage クラスターのインポート	77
5.2.8. ホスト ウィンドウの追加設定の説明	78
5.2.9. クラスターの削除	78
5.2.10. クラスターの互換バージョンの変更	79
5.3. クラスターおよびパーミッション	80
5.3.1. クラスターのシステムパーミッションの管理	80
5.3.2. クラスター管理者ロールの概要	80
5.3.3. 管理者またはユーザーロールのリソースへの割り当て	81
5.3.4. リソースからの管理者またはユーザーロールの削除	81
第6章 論理ネットワーク	83

6.1. 論理ネットワークタスク	83
6.1.1. ネットワークタブの使用	83
6.1.2. データセンターまたはクラスターでの新しい論理ネットワークの作成	83
6.1.3. 論理ネットワークの編集	85
6.1.4. 論理ネットワークの削除	85
6.1.5. 論理ネットワークのゲートウェイの表示と編集	86
6.1.6. 新しい論理ネットワークおよび論理ネットワークの編集ウィンドウの設定とコントロールの説明	86
6.1.6.1. 論理ネットワーク一般設定の説明	86
6.1.6.2. 論理ネットワーククラスターの設定の説明	87
6.1.6.3. 論理ネットワークの vNIC プロファイル設定の説明	88
6.1.7. ネットワークの管理ウィンドウでの論理ネットワークに対する特定のトラフィックタイプの指定	88
6.1.8. ネットワーク管理画面での設定内容の説明	89
6.1.9. NIC の仮想機能設定の編集	90
6.2. 仮想ネットワークインターフェイスカード	91
6.2.1. vNIC プロファイルの概要	91
6.2.2. vNIC プロファイルの作成と編集	91
6.2.3. VM インターフェイスプロファイルウィンドウの設定内容の説明	93
6.2.4. vNIC プロファイルでのパススルーの有効化	94
6.2.5. vNIC プロファイルの削除	95
6.2.6. vNIC プロファイルへのセキュリティーグループの割り当て	95
6.2.7. vNIC プロファイルのユーザー権限	96
6.2.8. UCS 統合用の vNIC プロファイルの設定	96
6.3. 外部プロバイダーネットワーク	97
6.3.1. 外部プロバイダーからのネットワークのインポート	97
6.3.2. 外部プロバイダーネットワークの使用に関する制限	99
6.3.3. 外部プロバイダーの論理ネットワークのサブネット設定	99
6.3.3.1. 外部プロバイダーの論理ネットワークのサブネット設定	99
6.3.3.2. 外部プロバイダー論理ネットワークへのサブネットの追加	100
6.3.3.3. 外部プロバイダー論理ネットワークからのサブネットの削除	100
6.4. 論理ネットワークとパーミッション	101
6.4.1. ネットワークのシステムパーミッションの管理	101
6.4.2. ネットワーク管理者およびユーザーロールの概要	101
6.4.3. 管理者またはユーザーロールのリソースへの割り当て	102
6.4.4. リソースからの管理者またはユーザーロールの削除	102
6.5. ホストとネットワーキング	103
6.5.1. ホスト機能のリフレッシュ	103
6.5.2. ホストのネットワークインターフェイスの編集とホストへの論理ネットワークの割り当て	103
6.5.3. 論理ネットワークを使用した単一のネットワークインターフェイスへの複数の VLAN の追加	107
6.5.4. ホストネットワークへの追加の IPv4 アドレスの割り当て	108
6.5.5. ホストネットワークインターフェイスへのネットワークラベルの追加	109
6.5.6. ボンド	110
6.5.6.1. Red Hat Virtualization でのロゴのボンディング	110
6.5.6.2. ボンド	111
ボンディングモード	111
6.5.6.3. 管理ポータルを使用したボンドデバイスの作成	113
6.5.6.4. ホストインターフェイスでのカスタムボンディングオプションの使用例	113
6.5.7. ホストの FQDN の変更	114
第7章 ホスト	115
7.1. ホストの HQL の概要	115
7.2. RED HAT VIRTUALIZATION HOST	116
7.3. RED HAT ENTERPRISE LINUX HOSTS	116
7.4. サテライトホストプロバイダーホスト	117

7.5. ホストのタスク	117
7.5.1. Red Hat Virtualization Manager へのホストの追加	117
7.5.2. サテライトホストプロバイダー ホストの追加	118
7.5.3. ホストの Satellite エラータ管理の設定	119
7.5.4. 新規ホスト、ホスト編集ウィンドウの設定とコントロールの説明	120
7.5.4.1. ホストの一般設定の説明	120
7.5.4.2. ホストパワーマネージメント設定の説明	122
7.5.4.3. SPM のプライオリティー設定の説明	125
7.5.4.4. ホストクラスター設定の説明	125
7.5.4.5. ネットワークプロバイダー設定の説明	126
7.5.4.6. カーネル設定の説明	126
7.5.4.7. ホストエンジン設定の説明	127
7.5.5. ホストパワーマネージメントの設定	128
7.5.6. ホストストレージプールマネージャーの設定	129
7.5.7. ホストのメンテナンスモードへの切り替え	130
7.5.8. メンテナンスモードからホストを起動する	130
7.5.9. ホストの削除	131
7.5.10.マイナーリリース間でのホストの更新	131
7.5.11. ホストの再インストール	131
7.5.12. タグを使用したホストのカスタマイズ	132
7.5.13. ホスト Errata の表示	133
7.5.14. ホストのヘルステータスの表示	133
7.5.15. ホストデバイスの表示	134
7.5.16. GPU パススルー用ホストおよびゲストシステムの準備	134
7.5.17. 管理ポータルからのコックピットへのアクセス	137
7.6. ホストの耐障害性	137
7.6.1. 高可用性	137
7.6.2. Red Hat Virtualization の Proxy による電源管理	138
7.6.3. ホストでのフェンシングパラメーターの設定	138
7.6.4. fence_kdump の高度な設定	141
7.6.4.1. fence_kdump リスナーの設定	142
7.6.4.2. マネージャーでの fence_kdump の設定	143
7.6.5. ソフトフェンシングホスト	145
7.6.6. ホストの電源管理機能の利用	146
7.6.7. 反応しないホストを手動でフェンシングまたは分離する	146
7.7. ホストとパーミッション	147
7.7.1. ホストのシステムパーミッションの管理	147
7.7.2. ホスト管理者ロールの概要	148
7.7.3. 管理者またはユーザーロールのリソースへの割り当て	148
7.7.4. リソースからの管理者またはユーザーロールの削除	148
第8章 ストレージ	150
8.1. ストレージドメインについて	151
8.2. NFS ストレージの準備と追加	151
8.2.1. NFS ストレージの準備	151
8.2.2. NFS ストレージのアタッチ	152
8.2.3. NFS ストレージの増設	154
8.3. ローカルストレージの準備と追加	154
8.3.1. ローカルストレージの準備	154
8.3.2. ローカルストレージの追加	155
8.4. POSIX 準拠ファイルシステムストレージの追加	156
8.4.1. POSIX 準拠ファイルシステムストレージのアタッチ	157
8.5. ブロックストレージの追加	158

8.5.1. iSCSI ストレージの追加	158
8.5.2. Configuring iSCSI Multipathing	161
8.5.3. FCP ストレージの追加	162
8.5.4. iSCSI または FCP ストレージの増設	164
8.5.5. Red Hat Virtualization で使用できない LUN	165
8.6. 既存のストレージドメインのインポート	166
8.6.1. 既存のストレージドメインのインポートの概要	166
8.6.2. ストレージドメインのインポート	166
8.6.3. 同じ環境内のデータセンター間でのストレージドメインの移行	168
8.6.4. 異なる環境内のデータセンター間でのストレージドメインの移行	168
8.6.5. インポート済みデータストレージドメインからの仮想マシンのインポート	171
8.6.6. インポートされたデータストレージドメインからのテンプレートのインポート	171
8.6.7. インポートされたストレージドメインからのディスクイメージのインポート	171
8.6.8. インポートされたストレージドメインからの未登録のディスクイメージのインポート	172
8.7. ストレージタスク	172
8.7.1. ISO ストレージドメインの設定	172
8.7.2. ストレージドメインのメンテナンスマードへの移行	173
8.7.3. ストレージドメインの編集	174
8.7.4. メンテナンスマードからのストレージドメインのアクティブ化	175
8.7.5. ストレージドメインの削除	175
8.7.6. ストレージドメインの破棄	175
8.7.7. データセンターからストレージドメインをデタッチ	176
8.7.8. ストレージドメインのデータセンターへのアタッチ	176
8.7.9. ディスクプロファイル	176
8.7.9.1. ディスクプロファイルの作成	176
8.7.9.2. ディスクプロファイルの削除	177
8.7.10. ストレージドメインのヘルスステータスの表示	177
8.8. ストレージおよびパーミッション	178
8.8.1. ストレージドメインのシステムパーミッションの管理	178
8.8.2. ストレージ管理者ロールの概要	178
8.8.3. 管理者またはユーザーロールのリソースへの割り当て	179
8.8.4. リソースからの管理者またはユーザーロールの削除	179
第9章 RED HAT GLUSTER STORAGE の使用	180
9.1. RED HAT GLUSTER STORAGE ノード	180
9.1.1. Red Hat Gluster Storage ノードの追加	180
9.1.2. Red Hat Gluster Storage ノードの削除	180
9.2. ストレージドメインとしての RED HAT GLUSTER STORAGE の使用	181
9.2.1. Red Hat Gluster Storage (GlusterFS)ボリュームの概要	181
9.2.2. Gluster Storage の用語	181
9.2.3. Red Hat Gluster Storage ボリュームをストレージドメインとして割り当てる	183
9.2.4. ストレージボリュームの作成	185
9.2.5. ボリュームへのブリックの追加	186
9.2.6. ブリックウィンドウの追加設定の説明	186
9.2.7. 仮想マシンイメージの保存への Red Hat Gluster Storage ボリュームの最適化	187
9.2.8. ボリュームの起動	187
9.2.9. ボリュームのチューニング	188
9.2.10. ボリュームオプションの編集	188
9.2.11. ボリュームのリセットオプション	189
9.2.12. ボリュームからのブリックの削除	189
9.2.13. Red Hat Gluster Storage ボリュームの停止	190
9.2.14. Red Hat Gluster Storage ボリュームの削除	190
9.2.15. ボリュームのリバランス	190

9.3. クラスターおよび GLUSTER フック	190
9.3.1. Gluster フックの管理	190
9.3.2. フックの一覧表示	191
9.3.3. フックの内容の表示	191
9.3.4. フックの有効化または無効化	191
9.3.5. フックの更新	192
9.3.6. 競合の解決	192
9.3.7. コンテンツの競合の解決	192
9.3.8. 欠落しているフックの競合の解決	193
9.3.9. ステータスの競合の解決	193
9.3.10. 複数の競合の解決	194
9.3.11. Gluster 同期の管理	194
第10章 POOLS	196
10.1. 仮想マシンプールの概要	196
10.2. 仮想マシンプールタスク	196
10.2.1. 仮想マシンプールの作成	196
10.2.2. 新しいプールとプールの編集ウィンドウの設定およびコントロールの説明	197
10.2.2.1. 新しいプールと編集プールの一般設定の説明	197
10.2.2.2. 新規およびプールタイプ設定の編集の説明	198
10.2.2.3. 新しいプールおよびプールコンソール設定の編集の説明	199
10.2.2.4. 仮想マシンプールのホスト設定の説明	199
10.2.3. 仮想マシンプールの編集	204
10.2.3.1. 仮想マシンプールの編集	204
10.2.3.2. プール内の仮想マシンの事前起動	205
10.2.3.3. 仮想マシンプールへの仮想マシンの追加	205
10.2.3.4. 仮想マシンプールからの仮想マシンのデタッチ	205
10.2.4. 仮想マシンプールの削除	206
10.3. プールおよびパーミッション	206
10.3.1. 仮想マシンプールのシステムパーミッションの管理	206
10.3.2. 仮想マシンプール管理者ロールの概要	207
10.3.3. 管理者またはユーザーロールのリソースへの割り当て	207
10.3.4. リソースからの管理者またはユーザーロールの削除	207
10.4. 信頼できるコンピュートプール	208
10.4.1. OpenAttestation サーバーの Manager への接続	208
10.4.2. 信頼できるクラスターの作成	209
10.4.3. 信頼できるホストの追加	209
第11章 仮想ディスク	211
11.1. 仮想マシンストレージを理解する	211
11.2. 仮想ディスクの概要	211
11.3. 削除後に仮想ディスクをワイプするための設定	213
11.4. RED HAT VIRTUALIZATION の共有可能ディスク	214
11.5. RED HAT VIRTUALIZATION の読み取り専用ディスク	214
11.6. 仮想ディスクタスク	215
11.6.1. Floating 仮想ディスクの作成	215
11.6.2. 新しい仮想ディスクウィンドウの設定の説明	216
11.6.3. ライブストレージ移行の概要	221
11.6.4. 仮想ディスクの移動	222
11.6.5. ディスクインターフェイスタイプの変更	222
11.6.6. 仮想ディスクのコピー	223
11.6.7. ストレージドメインへのディスクイメージのアップロード	223
11.6.8. インポートされたストレージドメインからのディスクイメージのインポート	225

11.6.9. インポートされたストレージドメインからの未登録のディスクイメージのインポート	226
11.6.10. OpenStack Image サービスからの仮想ディスクイメージのインポート	226
11.6.11. OpenStack Image Service への仮想ディスクのエクスポート	227
11.7. 仮想ディスクおよびパーティション	227
11.7.1. 仮想ディスクのシステムパーティションの管理	227
11.7.2. 仮想ディスクユーザーロールの概要	228
11.7.3. 管理者またはユーザー ロールのリソースへの割り当て	228
11.7.4. リソースからの管理者またはユーザー ロールの削除	229
第12章 外部プロバイダー	230
12.1. RED HAT VIRTUALIZATION における外部プロバイダーの紹介	230
12.2. 外部プロバイダーの追加	231
12.2.1. ホストのプロビジョニング用の Red Hat Satellite インスタンスの追加	231
12.2.2. イメージ管理用の OpenStack Image (Glance) インスタンスの追加	232
12.2.3. ネットワークプロビジョニング用の OpenStack Networking (Neutron) インスタンスの追加	234
12.2.4. ストレージ管理用の OpenStack Volume (Cinder) インスタンスの追加	236
12.2.5. 仮想マシンプロバイダーとしての VMware インスタンスの追加	238
12.2.6. 外部ネットワークプロバイダーの追加	240
12.2.7. プロバイダーの一般設定の説明を追加	242
12.2.8. プロバイダーエージェントの設定設定に関する説明の追加	246
12.3. 外部プロバイダーの編集	246
12.3.1. 外部プロバイダーの編集	246
12.4. 外部プロバイダーの削除	246
12.4.1. 外部プロバイダーの削除	246
パート III. 環境の管理	248
第13章 バックアップおよび移行	249
13.1. RED HAT VIRTUALIZATION MANAGER のバックアップおよび復元	249
13.1.1. Red Hat Virtualization Manager のバックアップ - 概要	249
13.1.2. engine-backup コマンドの構文	249
13.1.3. engine-backup コマンドを使用したバックアップの作成	250
13.1.4. engine-backup コマンドを使用したバックアップの復元	251
13.1.5. バックアップを新規インストールに復元する	251
13.1.6. バックアップを復元して既存のインストールを上書き	252
13.1.7. 異なる認証情報を使用したバックアップの復元	253
13.1.8. エンジンデータベースのリモートサーバーデータベースへの移行	255
13.2. バックアップおよび RESTORE API を使用した仮想マシンのバックアップおよび復元	256
13.2.1. バックアップおよび Restore API	256
13.2.2. 仮想マシンのバックアップ	256
13.2.3. 仮想マシンの復元	258
第14章 RED HAT SATELLITE でのエラータ管理	260
第15章 ユーザーとロール	262
15.1. ユーザーの概要	262
15.2. DIRECTORY SERVER の概要	262
15.3. 外部 LDAP プロバイダーの設定	263
15.3.1. 外部 LDAP プロバイダーの設定 (対話型セットアップ)	263
15.3.2. Active Directory の接続	267
15.3.3. 外部 LDAP プロバイダーの設定 (手動による方法)	270
15.3.4. 外部 LDAP プロバイダーの削除	273
15.4. SINGLE SIGN-ON 用の LDAP および KERBEROS の設定	273
15.5. ユーザーの承認	279

15.5.1. ユーザー認証モデル	279
15.5.2. ユーザーアクション	279
15.6. 管理ポータルからのユーザータスクの管理	279
15.6.1. ユーザーの追加およびユーザーPortalパーティションの割り当て	279
15.6.2. ユーザー情報の表示	280
15.6.3. リソースでのユーザーパーティションの表示	280
15.6.4. ユーザーの削除	281
15.6.5. ログインしたユーザーの表示	281
15.6.6. ユーザーセッションの終了	281
15.7. コマンドラインからのユーザータスクの管理	281
15.7.1. ユーザーの管理	281
15.7.2. 内部管理ユーザーのパスワード変更	283
15.7.3. 内部管理ユーザーの無効化	283
15.7.4. グループの管理	284
15.7.5. ユーザーおよびグループのクエリー	285
15.7.6. アカウント設定の管理	286
15.8. 追加のローカルドメインの設定	286
第16章 クォータとサービスレベル契約ポリシー	287
16.1. クォータの概要	287
16.2. 共有クォータおよび個別定義されたクォータ	288
16.3. クォータアカウンティング	288
16.4. データセンターにおけるクォータモードの有効化および変更	289
16.5. 新しいクォータポリシーの作成	289
16.6. クォータしきい値の設定の説明	290
16.7. オブジェクトへのクォータの割り当て	291
16.8. クォータを使用してユーザーごとにリソースを制限する	292
16.9. クォータの編集	292
16.10. クォータの削除	293
16.11. サービスレベルアグリーメントポリシーの実施	293
第17章 イベント通知	295
17.1. 管理ポータルでのイベント通知の設定	295
17.2. 管理ポータルでのイベント通知のキャンセル	297
17.3. OVIRT-ENGINE-NOTIFIER.CONF のイベント通知のパラメーター	297
17.4. SNMP トラップを送信するための RED HAT VIRTUALIZATION MANAGER の設定	301
第18章 ユーティリティー	304
18.1. OVIRT エンジンの名前変更ツール	304
18.1.1. oVirt エンジンの名前変更ツール	304
18.1.2. oVirt Engine Rename コマンドの構文	304
18.1.3. oVirt エンジンの名前変更ツールの使用	305
18.2. エンジン設定ツール	306
18.2.1. エンジン設定ツール	306
18.2.2. engine-config コマンドの構文	306
18.3. イメージアップローダーツール	307
18.3.1. イメージアップローダーツール	307
18.3.2. engine-image-uploader コマンドの構文	307
18.3.3. イメージアップローダーと互換性のある OVF アーカイブの作成	310
18.3.4. 基本的な engine-image-uploader 使用例	310
18.4. USB フィルターエディター	310
18.4.1. USB Filter Editor のインストール	311
18.4.2. USB フィルターエディターインターフェイス	311
18.4.3. USB ポリシーの追加	312

18.4.4. USB ポリシーの削除	314
18.4.5. USB デバイスピリシーの検索	316
18.4.6. USB ポリシーのエクスポート	316
18.4.7. USB ポリシーのインポート	317
18.5. ログコレクターツール	317
18.5.1. ログコレクター	318
18.5.2. ovirt-log-collector コマンドの構文	318
18.5.3. ログコレクターの基本的な使用法	321
18.6. ISO アップローダーツール	321
18.6.1. ISO アップローダーツール	321
18.6.2. engine-iso-uploader コマンドの構文	321
18.6.3. NFS サーバーの指定	323
18.6.4. 基本的な ISO アップローダーの使用法	323
18.6.5. VirtIO およびゲストツールのイメージファイルの ISO ストレージドメインへのアップロード	324
18.6.6. VirtIO およびゲストツールのイメージファイル	324
18.7. エンジンバキュームツール	325
18.7.1. エンジンバキュームツール	325
18.7.2. エンジンバキュームモード	325
Standard Vacuum	325
Full Vacuum	325
18.7.3. エンジンバキュームの構文	325
パート IV. 環境に関する情報の収集	327
第19章 ログファイル	328
19.1. RED HAT VIRTUALIZATION MANAGER のインストールログファイル	328
19.2. RED HAT VIRTUALIZATION MANAGER ログファイル	328
19.3. SPICE ログファイル	328
19.3.1. ハイパーバイザ SPICE サーバーの SPICE ログ	329
19.3.2. ゲストマシンの SPICE ログ	329
19.3.3. console.vv ファイルを使用して起動された SPICE クライアントの SPICE ログ	330
19.4. RED HAT VIRTUALIZATION ホストのログファイル	330
19.5. 仮想化ホストのロギングサーバーの設定	331
第20章 プロキシー	333
20.1. SPICE プロキシー	333
20.1.1. SPICE プロキシーの概要	333
20.1.2. SPICE プロキシーマシンの設定	333
20.1.3. SPICE プロキシーの有効化	334
20.1.4. SPICE プロキシーをオフにする	334
20.2. SQUID プロキシー	335
20.2.1. Squid プロキシーのインストールおよび設定	335
20.3. WEBSOCKET プロキシー	337
20.3.1. WebSocket プロキシーの概要	337
20.3.2. Websocket プロキシーを別のマシンに移行する	338
付録A VDSM およびフック	339
A.1. VDSM	339
A.2. VDSM フック	339
A.3. フックを使用した VDSM の拡張	339
A.4. サポートされている VDSM イベント	339
A.5. VDSM フック環境	342
A.6. VDSM フックドメイン XML オブジェクト	342
A.7. カスタムプロパティーの定義	342

A.8. 仮想マシンのカスタムプロパティーの設定	344
A.9. VDSM フックでの仮想マシンのカスタムプロパティーの評価	344
A.10. VDSM フックモジュールの使用	345
A.11. VDSM フックの実行	345
A.12. VDSM フックの戻りコード	346
A.13. VDSM フックの例	347
付録B カスタムネットワークプロパティー	349
B.1. BRIDGE_OPTS パラメーターの説明	349
B.2. RED HAT VIRTUALIZATION MANAGER を使用するように RED HAT VIRTUALIZATION MANAGER を設定する方法	351
B.3. FCOE を使用するように RED HAT VIRTUALIZATION MANAGER を設定する方法	352
付録C RED HAT VIRTUALIZATION ユーザーインターフェイスプラグイン	354
C.1. RED HAT VIRTUALIZATION ユーザーインターフェイスプラグイン	354
C.2. RED HAT VIRTUALIZATION USER INTERFACE PLUGIN LIFECYCLE	354
C.2.1. Red Hat Virtualization User Interface Plug-in のライフサイクル	354
C.2.2. Red Hat Virtualization ユーザーインターフェイスプラグインの検出	354
C.2.3. Red Hat Virtualization User Interface Plug-in のロード	355
C.2.4. Red Hat Virtualization ユーザーインターフェイスプラグインポートストラップ	355
C.3. ユーザーインターフェイスプラグイン関連のファイルとその場所	356
C.4. ユーザーインターフェイスプラグインのデプロイメント例	356
C.5. RED HAT サポートプラグインの使用	357
付録D RED HAT VIRTUALIZATION および SSL	362
D.1. RED HAT VIRTUALIZATION MANAGER SSL/TLS 証明書の置き換え	362
D.2. MANAGER と LDAP サーバー間の SSL または TLS 接続の設定	364
付録E 検索、ブックマーク、およびタグの使用	366
E.1. 検索	366
E.1.1. Red Hat Virtualization での検索	366
E.1.2. 検索構文と例	366
E.1.3. 自動完了の検索	366
E.1.4. 検索結果タイプオプション	367
E.1.5. 検索基準	367
E.1.6. 検索: 複数の基準およびワイルドカード	369
E.1.7. 検索: 検索順序の決定	369
E.1.8. データセンターの検索	370
E.1.9. クラスターの検索	370
E.1.10. ホストの検索	371
E.1.11. ネットワークの検索	373
E.1.12. ストレージの検索	374
E.1.13. ディスクの検索	375
E.1.14. ボリュームの検索	377
E.1.15. 仮想マシンの検索	378
E.1.16. プールの検索	380
E.1.17. テンプレートの検索	380
E.1.18. ユーザーの検索	382
E.1.19. イベントの検索	383
E.2. ブックマーク	384
E.2.1. クエリー文字列をブックマークとして保存	384
E.2.2. ブックマークの編集	385
E.2.3. ブックマークの削除	385
E.3. タグ	386

E.3.1. タグを使用して Red Hat Virtualization とのやり取りをカスタマイズ	386
E.3.2. タグの作成	386
E.3.3. タグの変更	386
E.3.4. タグの削除	387
E.3.5. オブジェクトに対するタグの追加および削除	387
E.3.6. タグを使用したオブジェクトの検索	387
付録F ブランド化	388
F.1. ブランド化	388
F.1.1. Manager の再ブランド化	388
F.1.2. ログイン画面	388
F.1.3. 管理ポータルの画面	388
F.1.4. ユーザーポータル画面	388
F.1.5. ポップアップウィンドウ	389
F.1.6. タブ	389
F.1.7. Welcome ページ	389
F.1.8. Page Not Found ページ	390
付録G システムアカウント	391
G.1. システムアカウント	391
G.1.1. Red Hat Virtualization Manager のユーザーアカウント	391
G.1.2. Red Hat Virtualization Manager グループ	391
G.1.3. 仮想化ホストのユーザーアカウント	391
G.1.4. 仮想化ホストグループ	392

パート I. RED HAT VIRTUALIZATION 環境の管理と保守

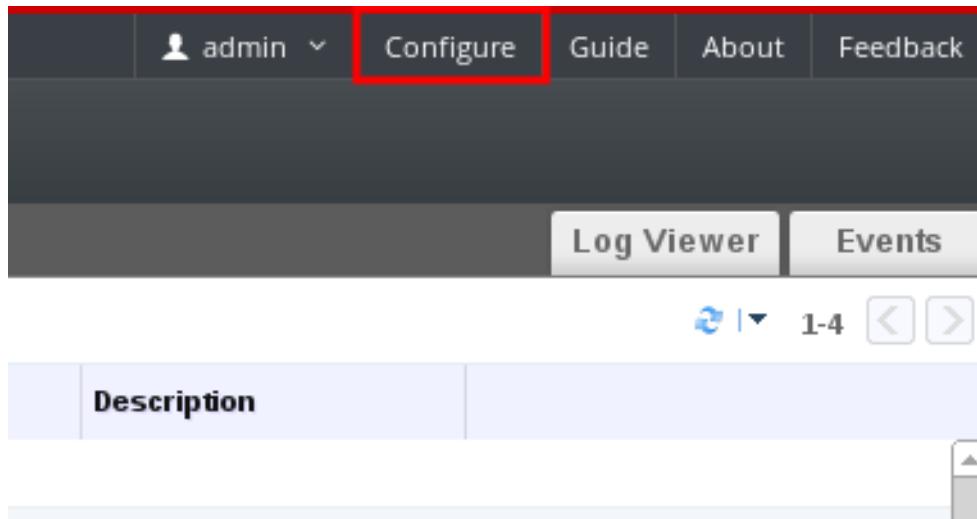
Red Hat Virtualization 環境の稼働を維持するには管理者が必要です。管理者のタスクには以下が含まれます。

- ホストや仮想マシンなどの物理リソースおよび仮想リソースの管理。これには、ホストのアップグレードおよび追加、ドメインのインポート、外部ハイパーバイザーで作成された仮想マシンの変換、および仮想マシンプールの管理が含まれます。
- ホストのいずれかに対する極端な負荷、メモリーやディスク容量不足、必要なアクション(仮想マシンをシャットダウンして仮想マシンの別ホストへの移行して負荷を軽減したりリソースを解放するなど)などの潜在的な問題について、全体的なシステムリソースのモニタリングを行います。
- 仮想マシンの新しい要件に対応します(たとえば、オペレーティングシステムのアップグレードまたはより多くのメモリーの割り当てなど)。
- タグを使用したカスタムオブジェクトプロパティーの管理。
- パブリックブックマークとして保存された検索の管理。
- ユーザー設定の管理とパーミッションレベルの設定。
- システム機能全体の特定ユーザーまたは仮想マシンのトラブルシューティング。
- 一般および特定レポートの生成。

第1章 グローバル設定

管理ポータルのヘッダーバーからアクセスすると、Configure ウィンドウで、ユーザー、ロール、システムパーミッション、スケジューリングポリシー、インスタンスタイプ、MAC アドレスプールなどの Red Hat Virtualization 環境用に多数のグローバルリソースを設定できます。このウィンドウでは、ユーザーが環境のリソースと対話する方法をカスタマイズし、複数のクラスターに適用できるオプションを設定する一元的な場所を提供します。

図1.1 Configure ウィンドウへのアクセス



1.1. ロール

ロールは、Red Hat Virtualization Manager から設定できる事前定義された権限のセットです。ロールは、データセンター内の異なるレベルのリソースや、特定の物理リソースおよび仮想リソースに対するアクセスおよび管理のパーミッションを提供します。

マルチレベル管理では、コンテナオブジェクトに適用されるパーミッションは、そのコンテナー内のすべての個別オブジェクトにも適用されます。たとえば、特定のホスト上のユーザーにホスト管理者ロールが割り当てられた場合、そのユーザーは利用可能なホスト操作のいずれかを実行する権限を得ますが、割り当てられたホスト上でのみ実行できます。ただし、ホスト管理者ロールがデータセンターのユーザーに割り当てられている場合、ユーザーはデータセンターのクラスター内の全ホストでホスト操作を実行するパーミッションを取得します。

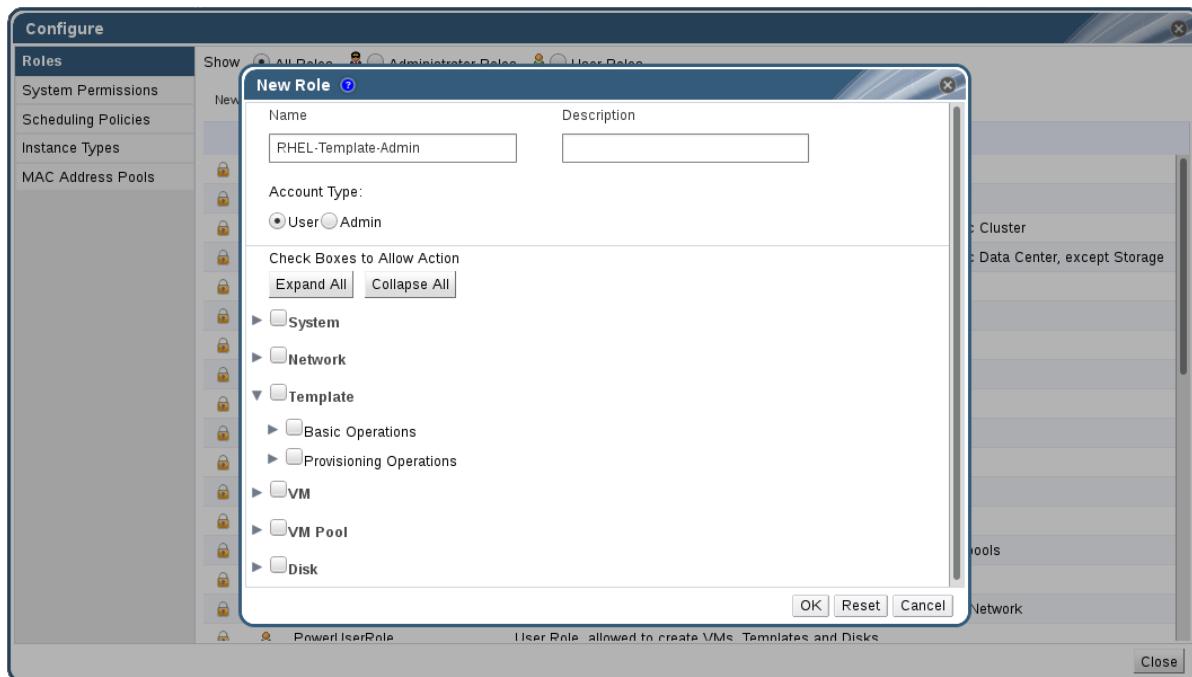
1.1.1. 新しいロールの作成

必要なロールが Red Hat Virtualization のデフォルトロールリストにない場合は、新しいロールを作成して、目的に合わせてカスタマイズできます。

手順1.1 新しいロールの作成

1. ヘッダーバーで Configure ボタンをクリックして Configure ウィンドウを開きます。ウィンドウには、デフォルトの User および Administrator ロールのリストとカスタムロールが表示されます。
2. New をクリックします。New Role ダイアログボックスが表示されます。

図1.2 新規ロールダイアログ



3. 新規ロールの **Name** および **Description** を入力します。
4. **Account Type** として **Admin** または **User** を選択します。
5. **Expand All** または **Collapse All** ボタンを使用して、**Check Boxes to Allow Action** リストに記載されているオブジェクトのパーミッションを増減します。また、各オブジェクトのオプションを展開したり、折りたたんだりすることもできます。
6. それぞれのオブジェクトについて、設定しているロールを許可または拒否するアクションを選択または消去します。
7. **OK** をクリックして、加えた変更を適用します。ロールの一覧に新しいロールが表示されます。

1.1.2. ロールの編集またはコピー

作成したロールの設定を変更できますが、デフォルトのロールを変更することはできません。デフォルトのロールを変更するには、そのロールのクローンを作成して、要件に合わせて変更します。

手順1.2 ロールの編集またはコピー

1. ヘッダーバーで **Configure** ボタンをクリックして **Configure** ウィンドウを開きます。ウィンドウには、デフォルトの User および Administrator ロールのリストとカスタムロールが表示されます。
2. 変更するロールを選択します。**Edit** をクリックして **Edit Role** ウィンドウを開くか、**Copy** をクリックして **Copy Role** ウィンドウを開きます。
3. 必要に応じて、ロールの **Name** および **Description** を編集します。
4. **Expand All** または **Collapse All** ボタンを使用して、一覧表示されたオブジェクトのパーミッションの表示を拡大または縮小します。また、各オブジェクトのオプションを展開したり、折りたたんだりすることもできます。

5. それぞれのオブジェクトについて、編集するロールを許可または拒否するアクションを選択または消去します。
6. **OK** をクリックして、加えた変更を適用します。

1.1.3. ユーザーロールと承認の例

以下の例は、本章で説明する承認システムの異なる機能を使用して、さまざまなシナリオに対して承認制御を適用する方法を示しています。

例1.1 クラスターパーミッション

Sarah は、ある企業の経理部門のシステム管理者です。各部署のすべての仮想リソースは、**Accounts** と呼ばれる Red Hat Virtualization クラスターの下に編成されています。アカウントクラスターで **ClusterAdmin** ロールが割り当てられています。これにより、仮想マシンはクラスターの子オブジェクトであるため、彼女はクラスター内のすべての仮想マシンを管理できます。仮想マシンの管理には、ディスクなどの仮想リソースの編集、追加、削除、およびスナップショットの作成などが含まれます。このクラスターの外部にあるリソースを管理することはできません。**ClusterAdmin** は管理者ロールであるため、管理ポータルを使用してこれらのリソースを管理できますが、ユーザーportalからのアクセスは付与されません。

例1.2 VM PowerUser パーミッション

John は、経理部のソフトウェア開発者です。彼は仮想マシンを使用してソフトウェアを構築し、テストします。Sarah は、John に **johndesktop** という仮想デスクトップを作成しました。John には、**johndesktop** 仮想マシンの **UserVmManager** ロールが割り当てられています。これにより、ユーザーportalを使用してこの単一の仮想マシンにアクセスできます。**UserVmManager** のパーミッションを持っているため、新しい仮想ディスクなど、仮想マシンを変更してリソースを追加できます。**UserVmManager** はユーザーロールであるため、管理ポータルを使用できません。

例1.3 データセンターパワーユーザーロールパーミッション

Penelope はオフィスマネージャーです。自分の仕事に加えて、面接の日程調整やリファレンスチェックのフォローアップなど、人事マネージャーの採用業務を手伝うこともあります。会社の方針により、Penelope は採用業務に特定のアプリケーションを使用する必要があります。

Penelope はオフィス管理用に自分のマシンを持っていますが、採用アプリケーションを実行するために別の仮想マシンを作成したいと考えています。新しい仮想マシンが存在するデータセンターの **PowerUserRole** パーミッションが割り当てられています。これは、新しい仮想マシンを作成するため、ストレージドメインでの仮想ディスクイメージの作成など、データセンター内の複数のコンポーネントに変更を加える必要があるためです。

これは、Penelope に **DataCenterAdmin** 権限を割り当てるることは異なります。データセンターの PowerUser として、Penelope は User Portal にログインし、データセンター内の仮想マシン固有のアクションを実行できます。彼女は、ホストまたはストレージをデータセンターに割り当てるなど、データセンターレベルの操作を実行できません。

例1.4 ネットワーク管理者のパーミッション

Chris は、IT 部門のネットワーク管理者です。その日常的な責任として、部署の Red Hat Virtualization 環境でのネットワークの作成、操作、および削除が含まれます。彼女には、リソースおよび各リソースのネットワークにおける管理者権限が必要です。たとえば、Chris が IT 部署の

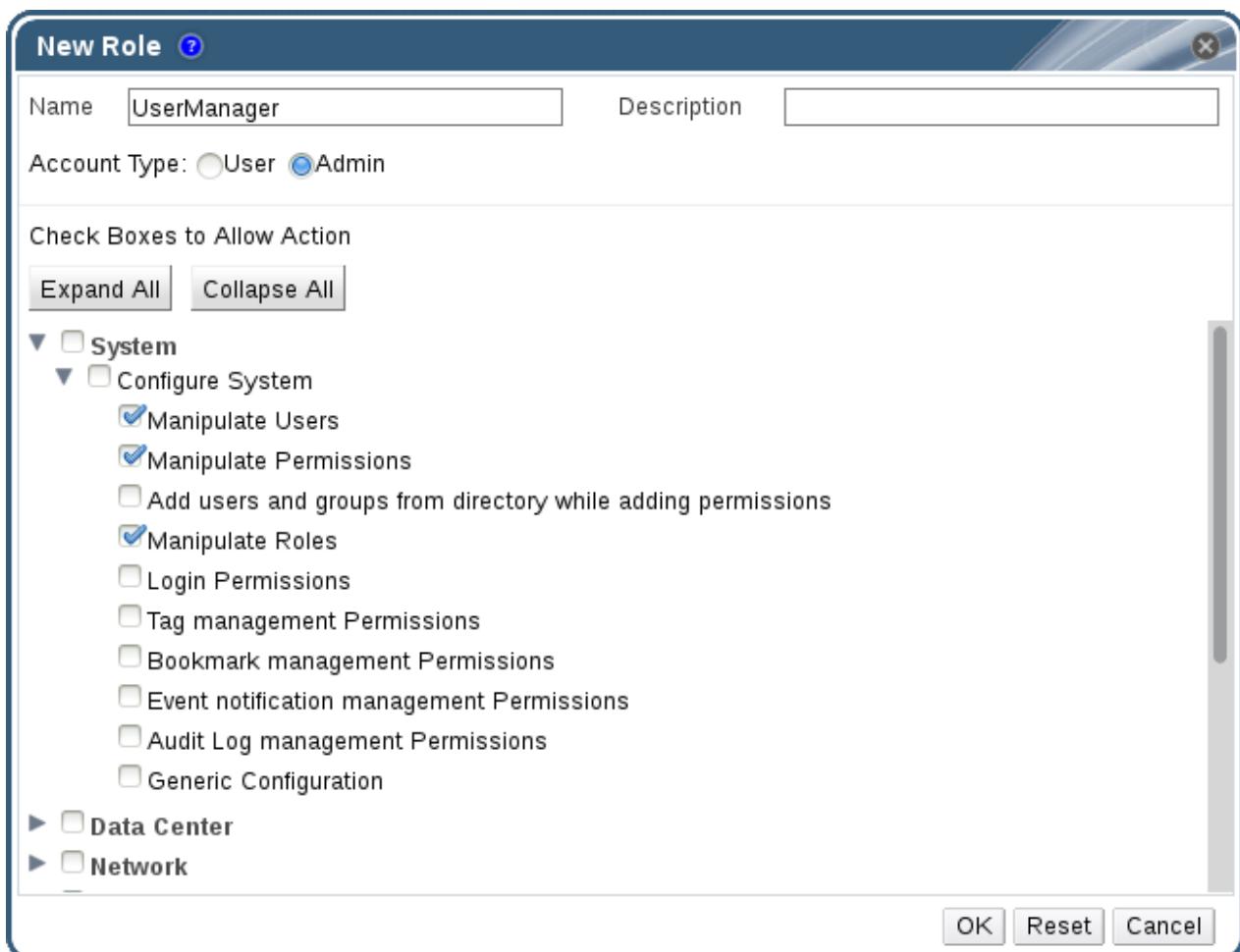
データセンターの **NetworkAdmin** 権限を持っている場合、データセンター内のネットワークを追加および削除したり、データセンターに属するすべての仮想マシンのネットワークをアタッチおよびデタッチできます。

会社の仮想化インフラストラクチャーのネットワークを管理する以外に、Chrisには、その企業の仮想化インフラストラクチャーのネットワーク管理者もレポートします。Junior ネットワーク管理者であるPatは、会社の内部トレーニング部門向けに小規模な仮想化環境を管理しています。Chrisには、内部トレーニング部門が使用する仮想マシンの **Pat VnicProfileUser** パーミッションと **UserVmManager** パーミッションが割り当てられています。これらのパーミッションを使用すると、Patはユーザーportalの **Extended** タブでネットワークインターフェイスを仮想マシンに追加するなどの簡単な管理タスクを実行できます。ただし、仮想マシンを実行するホストのネットワークや、仮想マシンが属するデータセンターのネットワークを変更するパーミッションがありません。

例1.5 カスタムロールパーミッション

レイチェルはIT部門に所属し、Red Hat Virtualizationのユーザーアカウント管理を担当しています。彼女には、ユーザーアカウントを追加し、適切なロールおよびパーミッションを割り当てる権限が必要です。彼女自身は仮想マシンを使用せず、ホスト、仮想マシン、クラスター、データセンターの管理にアクセスしてはいけません。彼女にこのような特定のパーミッションを与える組み込みのロールはありません。Rachelの位置に適したパーミッションセットを定義するために、カスタムロールを作成する必要があります。

図1.3 UserManager カスタムロール



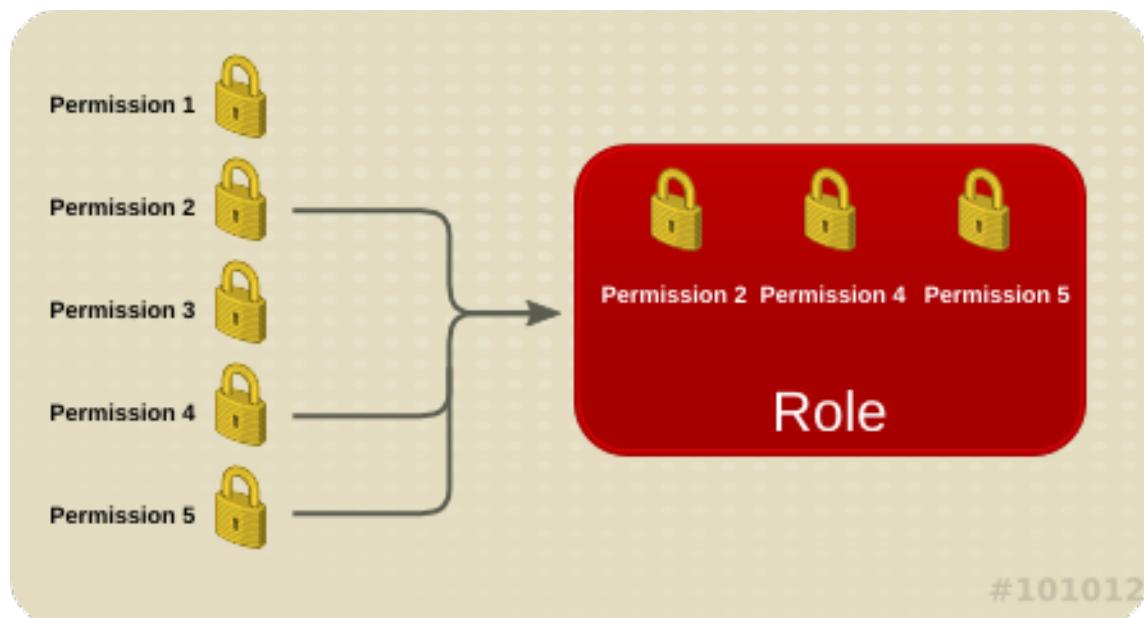
上記の **UserManager** カスタムロールは、ユーザー、パーミッション、およびロールの操作を許可します。これらのアクションは、[図1.3 「UserManager カスタムロール」](#) に示されている階層の最上位

オブジェクトである **System** の下に整理されています。これは、システム内のすべてのオブジェクトに適用されることを意味します。ロールの **Account Type** は **Admin** に設定されます。つまり、このロールが割り当てられている場合、Rachel はユーザーportalではなく管理portalのみを使用できます。

1.2. システムパーミッション

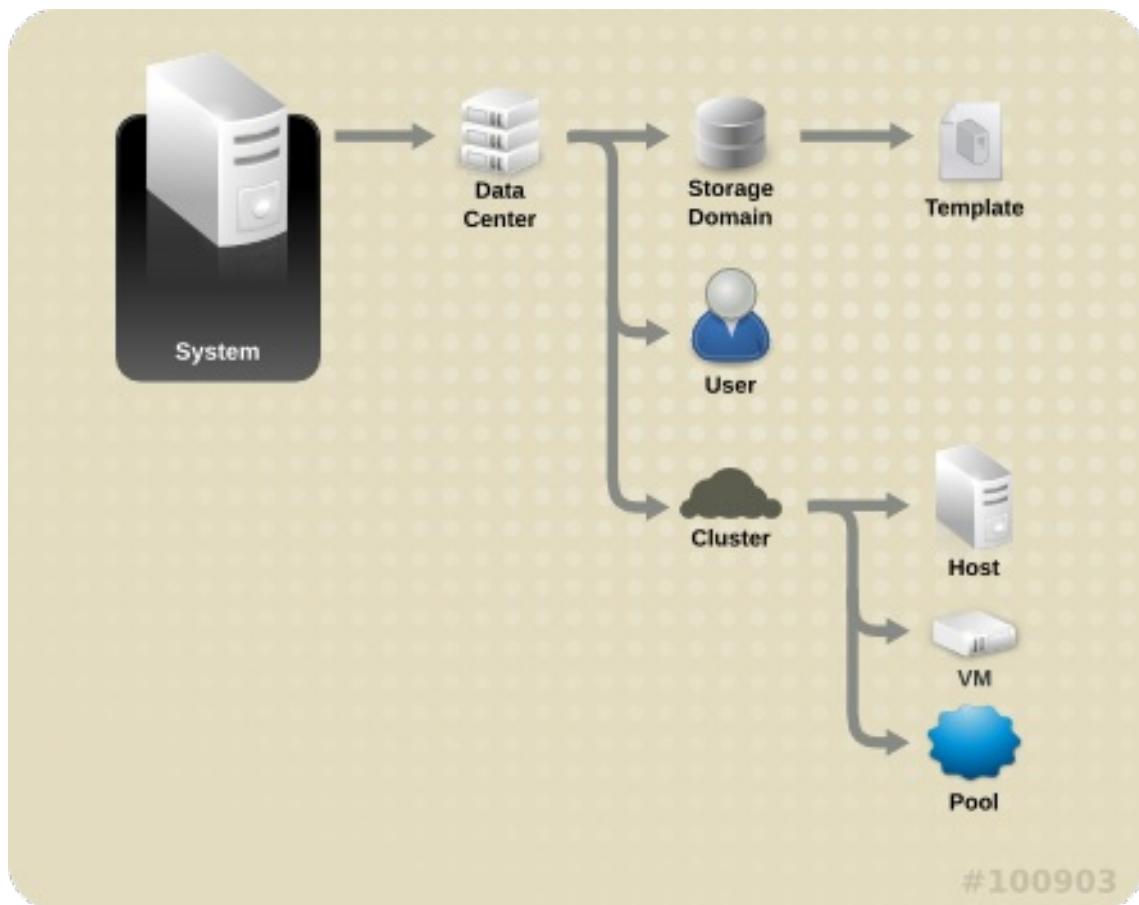
パーミッションにより、ユーザーはオブジェクトに対してアクションを実行できます。オブジェクトは個別のオブジェクトまたはコンテナーオブジェクトのいずれかになります。

図1.4 パーミッションおよびロール



コンテナーオブジェクトに適用されるパーミッションは、そのコンテナーのすべてのメンバーにも適用されます。以下の図は、システム内のオブジェクトの階層を示しています。

図1.5 Red Hat Virtualization オブジェクトの階層



1.2.1. ユーザープロパティー

ロールおよびパーミッションはユーザーのプロパティです。ロールとは、異なるレベルの物理および仮想リソースへのアクセスを許可する、事前定義された一連の権限のことです。マルチレベル管理では、パーミッションを細かく階層化できます。たとえば、データセンター管理者はデータセンター内の全オブジェクトを管理するパーミッションを持ち、ホスト管理者は1つの物理ホストのシステム管理者パーミッションを持ちます。あるユーザーは、単一の仮想マシンを使用するパーミッションを持っていても、仮想マシンの設定を変更できません。一方、別のユーザーは、仮想マシンのシステムパーミッションを割り当てることができます。

1.2.2. ユーザーおよび管理者ロール

Red Hat Virtualization は、システム全体のパーミッションを持つ管理者から、1台の仮想マシンにアクセスできるエンドユーザーまで、事前設定されたさまざまなロールを提供します。デフォルトのロールを変更または削除することはできませんが、そのロールのクローンを作成してカスタマイズしたり、要件に合わせて新しいロールを作成したりできます。以下の2つのタイプがあります。

- 管理者ロール：物理リソースおよび仮想リソースを **管理するための管理ポータル**へのアクセスを許可します。管理者ロールは、ユーザーportalで実行できるアクションのパーミッションを制限しますが、ユーザーがユーザーportalで表示できる内容には影響しません。
 - ユーザーロール：仮想マシンおよびテンプレートを管理およびアクセスするための **ユーザーportal**へのアクセスを許可します。ユーザーロールは、ユーザーがユーザーportalで表示できるものを決定します。管理者ロールを持つユーザーに付与されるパーミッションは、ユーザーportalでそのユーザーが利用できるアクションに反映されます。

たとえば、クラスターに管理 者 ロールがある場合は、管理 ポータル を使用してクラスター内のすべての仮想マシンを管理 できます。ただし、ユーザー ポータル のこれらの仮想マシンにはアクセスできません。これには ユーザー ロールが必要です。

1.2.3. ユーザーロールの概要

以下の表は、ユーザー ポータル で仮想マシンにアクセスして設定するパーミッションを付与する基本的なユーザー ロールについて説明しています。

表1.1 Red Hat Virtualization ユーザーロール: 基本

ロール	権限	注記
UserRole	仮想マシンおよびプールにアクセスし、使用できる。	ユーザー ポータル へのログイン、割り当てられた仮想マシンおよびプールの使用、仮想マシンの状態と詳細の表示が可能です。
PowerUserRole	仮想マシンおよびテンプレートを作成および管理できる。	このロールを Configure ウィンドウを使用して環境全体のユーザーに適用するか、または特定のデータセンターまたはクラスターのユーザーに適用します。たとえば、PowerUserRole がデータセンター レベルに適用されると、PowerUser はデータセンターで仮想マシンおよびテンプレートを作成できます。
UserVmManager	仮想マシンのシステム管理者。	仮想マシンの管理、スナップショットの作成と使用が可能。ユーザー ポータル で仮想マシンを作成するユーザーには、マシンの UserVmManager ロールが自動的に割り当てられます。

以下の表は、ユーザー ポータル のリソースに対するパーミッションの細かな調整を可能にする高度なユーザー ロールについて説明しています。

表1.2 Red Hat Virtualization のユーザー ロール - 高度

ロール	権限	注記
UserTemplateBasedVm	テンプレートのみを使用できる限定的な権限。	テンプレートを使用して仮想マシンを作成できます。
DiskOperator	仮想ディスクユーザー。	仮想ディスクの使用、表示、編集が可能です。仮想ディスクが接続されている仮想マシンを使用するパーミッションを継承します。

ロール	権限	注記
VmCreator	ユーザーportalで仮想マシンを作成できます。	このロールは特定の仮想マシンには適用されません。 Configure ウィンドウで環境全体のユーザーにこのロールを適用します。または、特定のデータセンターまたはクラスターにこのロールを適用することもできます。このロールをクラスターに適用する場合、データセンター全体または特定のストレージドメインに DiskCreator ロールを適用する必要もあります。
TemplateCreator	割り当てられたリソース内で仮想マシンテンプレートを作成、編集、管理、および削除できる。	このロールは特定のテンプレートには適用されません。 Configure ウィンドウで環境全体のユーザーにこのロールを適用します。また、特定のデータセンター、クラスター、またはストレージドメインにこのロールを適用することもできます。
DiskCreator	割り当てられたクラスターまたはデータセンター内の仮想ディスクを作成、編集、管理、および削除できる。	このロールは特定の仮想ディスクには適用されません。 Configure ウィンドウで環境全体のユーザーにこのロールを適用します。また、特定のデータセンターまたはストレージドメインにこのロールを適用することもできます。
TemplateOwner	テンプレートの編集および削除、テンプレートのユーザー権限の割り当ておよび管理が可能。	このロールは、テンプレートを作成したユーザーに自動的に割り当てられます。テンプレートに TemplateOwner 権限を持たない他のユーザーは、テンプレートを表示または使用することはできません。
VnicProfileUser	仮想マシンおよびテンプレートの論理ネットワークおよびネットワークインターフェイスユーザー。	特定の論理ネットワークからネットワークインターフェイスを接続または切断できます。

1.2.4. 管理者ロールの概要

以下の表は、管理ポータルのリソースにアクセスおよび設定する権限を付与する基本的な管理者ロールについて説明しています。

表1.3 Red Hat Virtualization システム管理者ロール - 基本

ロール	権限	注記
SuperUser	Red Hat Virtualization 環境のシステム管理者	すべてのオブジェクトおよびレベルでの完全なパーミッションを持ち、全データセンターで全オブジェクトを管理できます。
ClusterAdmin	クラスター管理者。	特定のクラスターアー下にある全オブジェクトの管理パーミッションを持ちます。
DataCenterAdmin	データセンター管理者。	特定のデータセンターの下にある、ストレージを除くすべてのオブジェクトの管理権限を保有しています。



重要

ディレクトリーサーバーの管理ユーザーを、Red Hat Virtualization の管理ユーザーとして使用しないでください。Red Hat Virtualization の管理ユーザーとして使用するように、ディレクトリーサーバーにユーザーを作成します。

以下の表は、管理者ポータルのリソースに対するパーミッションの細かな調整を可能にする高度な管理者ロールについて説明しています。

表1.4 Red Hat Virtualization システム管理者ロール - 高度

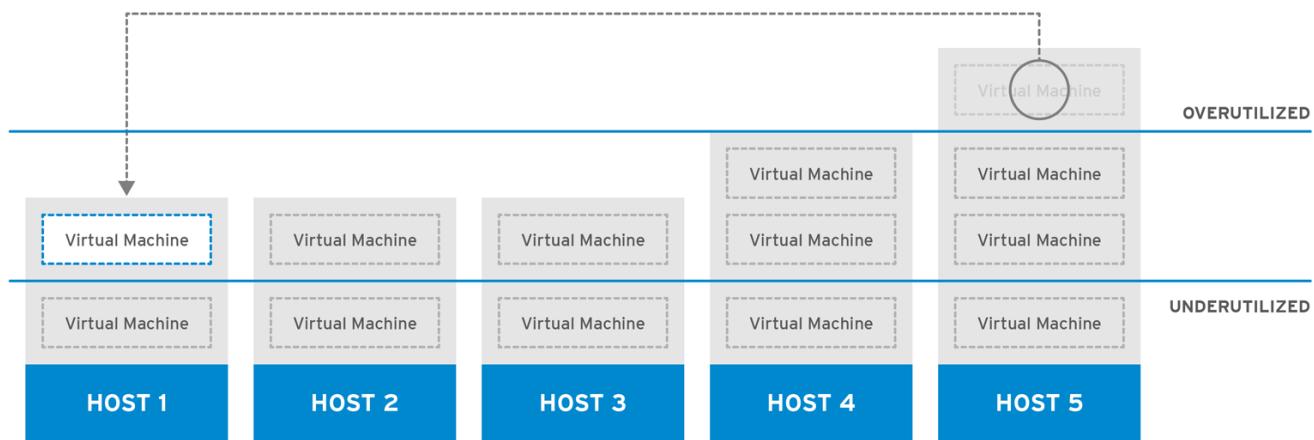
ロール	権限	注記
TemplateAdmin	仮想マシンテンプレートの管理者。	テンプレートのストレージドメインやネットワークの詳細を作成、削除、設定したり、ドメイン間でテンプレートを移動できます。
StorageAdmin	ストレージ管理者。	割り当てられたストレージドメインを作成、削除、設定、および管理できます。
HostAdmin	ホスト管理者。	特定のホストをアタッチ、削除、設定、および管理できます。
NetworkAdmin	ネットワーク管理者。	特定のデータセンターまたはクラスターのネットワークを設定および管理できます。データセンターまたはクラスターのネットワーク管理者は、クラスター内の仮想プールのネットワークパーミッションを継承します。

ロール	権限	注記
VmPoolAdmin	仮想プールのシステム管理者。	仮想プールを作成、削除、および設定できます。仮想プールユーザーを割り当ておよび削除し、プールの仮想マシンに基本操作を実行できます。
GlusterAdmin	Gluster Storage 管理者。	Gluster ストレージボリュームを作成、削除、設定、および管理できます。
VmImporterExporter	仮想マシンの管理者をインポートおよびエクスポートします。	仮想マシンをインポートおよびエクスポートできます。他のユーザーがエクスポートした仮想マシンおよびテンプレートをすべて表示できます。

1.3. スケジューリングポリシー

スケジューリングポリシーは、スケジューリングポリシーが適用されるクラスター内のホスト間で仮想マシンが分散されるロジックを定義するルールのセットです。スケジューリングポリシーは、フィルター、重み付け、および負荷分散ポリシーの組み合わせにより、このロジックを決定します。Red Hat Virtualization Manager は、**Evenly_Distributed**、**InClusterUpgrade**、**None**、**Power_Saving**、および**VM_Evenly_Distributed** の 5 つのデフォルトスケジューリングポリシーを提供します。また、新しいスケジューリングポリシーを定義することで、仮想マシンの配布をきめ細かく制御することができます。スケジューリングポリシーに関わらず、CPU が過負荷状態のホストでは仮想マシンが起動しません。デフォルトでは、ホストの CPU が 5 分間 80% を超える負荷がかかった場合に過負荷であると見なされますが、この値はスケジューリングポリシーを使用して変更できます。各スケジューリングポリシーのプロパティーに関する詳細は、「[スケジューリングポリシー設定に関する説明](#)」を参照してください。

図1.6 Evenly Distributed スケジューリングポリシー

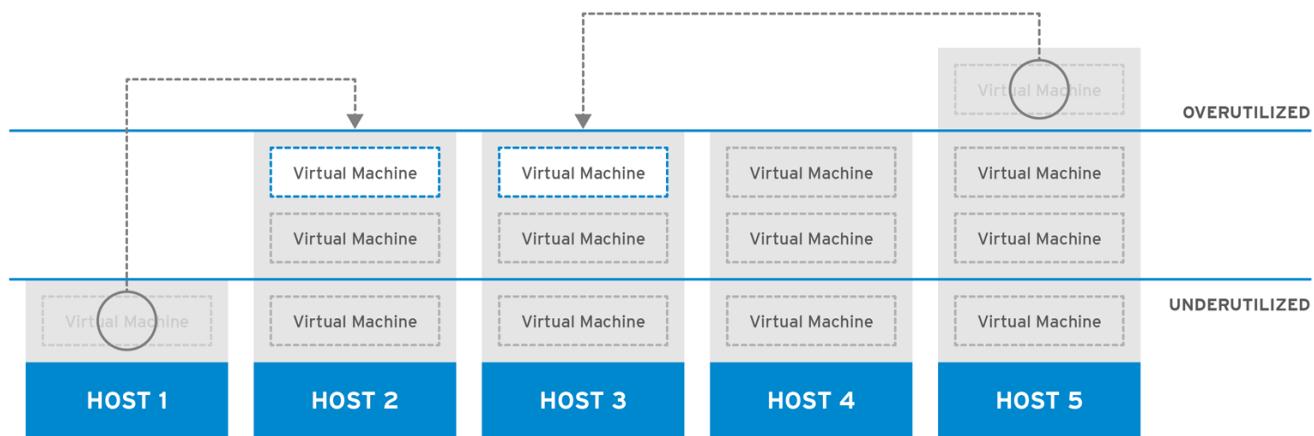


RHV_444396_0417

Evenly_Distributed スケジューリングポリシーは、クラスター内のすべてのノードにメモリーと CPU 処理の負荷を均等に分散します。ホストが定義された **CpuOverCommitDurationMinutes**、**HighUtilization**、または **MaxFreeMemoryForOverUtilized** に達した場合、ホストにアタッチされた追加の仮想マシンは起動しません。

VM_Evenly_Distributed スケジューリングポリシー仮想マシンは、仮想マシンの数に基づいてホスト間で均等に分散されます。HighVmCount より多くの仮想マシンを実行しているホストがあり、仮想マシン数を持つホストが MigrationThreshold の外にあるホストが1つ以上ある場合、クラスターはアンバランスとみなされます。

図1.7 Power Saving スケジューリングポリシー



RHV_444396_0417

Power_Saving スケジューリングポリシーは、利用可能なホストのサブセットにメモリーおよびCPU処理負荷を分散し、使用率の低いホストの電力消費を減らします。CPU 負荷が低稼働率の値を下回っている状態が定義された時間以上続いたホストは、すべての仮想マシンを他のホストに移行させ、電源を切れるようにします。ホストにアタッチされた追加の仮想マシンは、そのホストが定義された高使用率値に達した場合には起動しません。

仮想マシンを実行するホスト間で負荷や電源を共有しないように **None** ポリシーを設定します。これはデフォルトのモードです。仮想マシンが起動すると、メモリーと CPU 処理の負荷がクラスター内の全ホストに均等に分散されます。ホストが定義された

CpuOverCommitDurationMinutes、**HighUtilization**、または **MaxFreeMemoryForOverUtilized** に達した場合、ホストにアタッチされた追加の仮想マシンは起動しません。

InClusterUpgrade スケジューリングポリシーは、ホストオペレーティングシステムのバージョンに基づいて仮想マシンを配布します。現在実行している仮想マシンよりも新しいオペレーティングシステムを持つホストは、同じオペレーティングシステムを持つホストよりも優先されます。新しいオペレーティングシステムを持つホストに移行する仮想マシンは、古いオペレーティングシステムに移行されません。仮想マシンは、クラスター内の任意のホストで再起動できます。このポリシーにより、クラスターでオペレーティングシステムのバージョンが混在するようにすることで、クラスター内のホストをアップグレードできます。ポリシーを有効にする前に、前提条件を満たす必要があります。Red Hat Enterprise『Virtualization 3.6 Upgrade Guide』の [Upgrading Hosts in a Cluster from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7](#) を参照してください。



重要

InClusterUpgrade スケジューリングポリシーは、メジャーバージョン間のアップグレードのみに使用されます。たとえば、Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 7 へのアップグレードは以下のようになります。

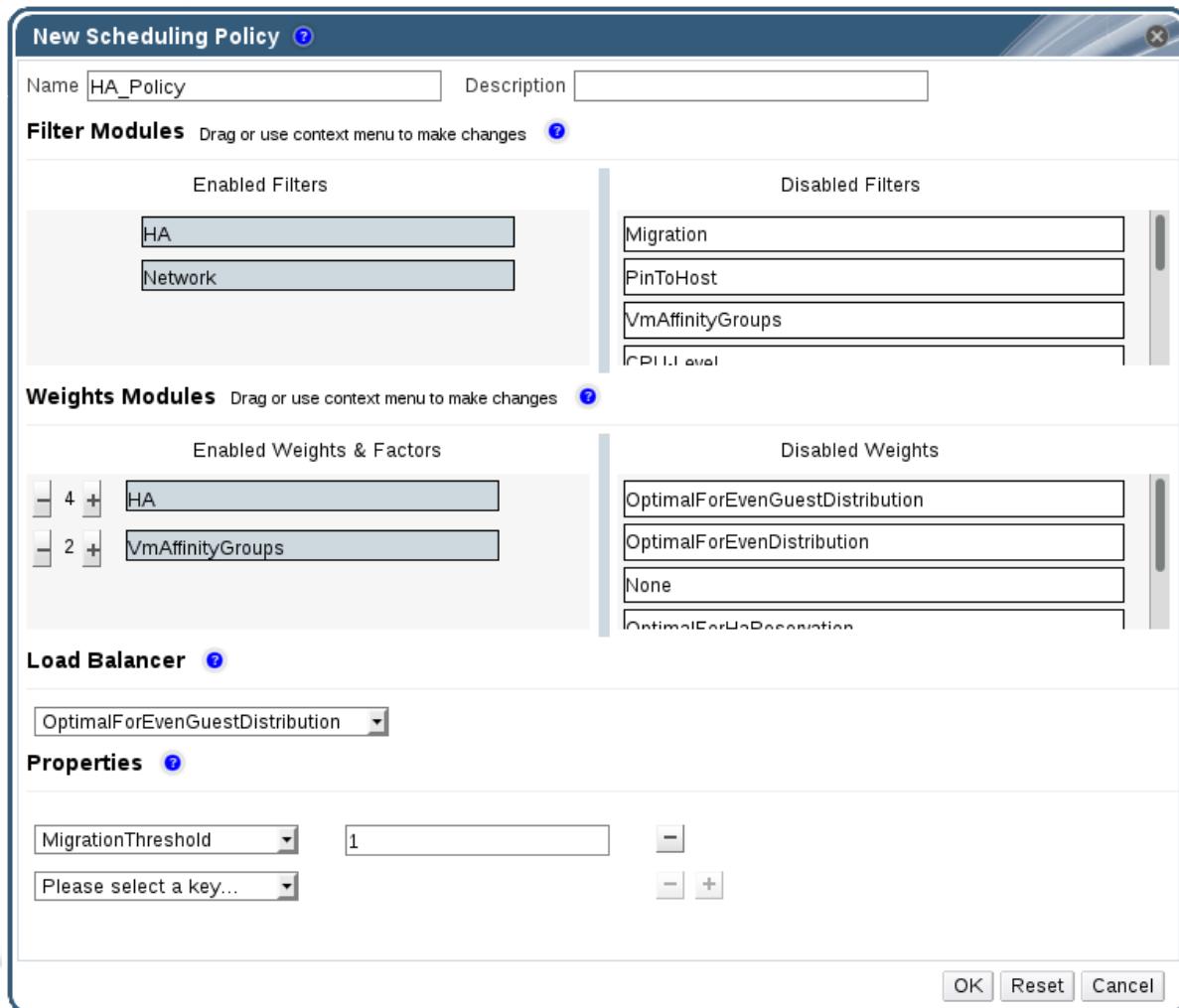
1.3.1. スケジューリングポリシーの作成

新規のスケジューリングポリシーを作成して、仮想マシンを Red Hat Virtualization 環境の特定のクラスターに分散するロジックを制御できます。

手順1.3 スケジューリングポリシーの作成

1. 管理ポータルのヘッダーバーの **Configure** ボタンをクリックして、**Configure** ウィンドウを開きます。
2. **Scheduling Policies** をクリックして、スケジューリングポリシータブを表示します。
3. **New** をクリックして **New Scheduling Policy** ウィンドウを開きます。

図1.8 新しいスケジューリングポリシーウィンドウ



4. スケジューリングポリシーの **Name** および **Description** を入力します。
5. フィルターモジュールを設定します。
 - a. **Filter Modules** セクションで、**Disabled Filters** セクションから **Enabled Filters** セクションに、優先するフィルターモジュールをドラッグアンドドロップしてスケジューリングポリシーに適用します。
 - b. 特定のフィルターモジュールは **First** として設定して、優先度が高い(**Last**)で、基本的な最適化のために優先度を最も低いものにすることもできます。
優先度を設定するには、フィルターモジュールを右クリックし、**Position** にカーソルを合わせ、**First** または **Last** を選択します。
6. 加重モジュールを設定します。

- a. **Weights Modules** セクションにて、**Disabled weights** セクションから **Enabled weights** セクションに、優先する重みモジュールをドラッグアンドドロップしてスケジューリングポリシーに適用します。
 - b. 有効な加重モジュールの左側にある + および - ボタンを使用して、これらのモジュールの重みを増減します。
7. ロードバランシングポリシーを指定します。
- a. **Load Balancer** セクションのドロップダウンメニューから、スケジューリングポリシーに適用する負荷分散ポリシーを選択します。
 - b. **Properties** セクションのドロップダウンメニューから、スケジューリングポリシーに適用する負荷分散プロパティーを選択し、そのプロパティーの右側にある text フィールドを使用して値を指定します。
 - c. + ボタンおよび - ボタンを使用して、プロパティーを追加または削除します。
8. **OK** をクリックします。

1.3.2. New Scheduling Policy および Edit Scheduling Policy ウィンドウの設定の説明

以下の表は、**New Scheduling Policy** および **Edit Scheduling Policy** ウィンドウで利用可能なオプションの詳細を示しています。

表1.5 New Scheduling Policy および Edit Scheduling Policy の設定

フィールド名	説明
Name	スケジューリングポリシーの名前。これは、Red Hat Virtualization Manager のスケジューリングポリシーを参照するために使用される名前です。
説明	スケジューリングポリシーの説明。このフィールドは推奨されますが、必須ではありません。

フィールド名	説明
Filter Modules	<p>クラスター内の仮想マシンが実行できるホストを制御するフィルターセット。フィルターを有効にすると、以下のように、フィルターで指定された条件を満たさないホストが除外されます。</p> <ul style="list-style-type: none"> ● CpuPinning: CPU ピニングの定義を満たさないホスト。 ● Migration: 同じホストへの移行を防ぎます。 ● PinToHost: 仮想マシンが固定されているホスト以外のホスト。 ● CPU-Level: 仮想マシンの CPU トポロジーを満たさないホスト。 ● CPU: 仮想マシンに割り当てられた数よりも少ない CPU を持つホスト。 ● Memory: 仮想マシンを実行するために十分なメモリーを持たないホスト。 ● VmAffinityGroups: アフィニティグループのメンバーである仮想マシンに指定した条件を満たさないホスト。たとえば、アフィニティグループの仮想マシンは、同じホストまたは別のホストで実行される必要があることなど。 ● InClusterUpgrade: 現在実行している仮想マシンよりも古いオペレーティングシステムを実行するホスト。 ● hostdevice: 仮想マシンに必要なホストデバイスに対応していないホスト。 ● HA: ホストエンジンの仮想マシンは、正の高可用性スコアを持つホストでのみ強制的に実行されます。 ● Emulated-Machine: 適切なエミュレートされたマシンをサポートしていないホスト。 ● ネットワーク: 仮想マシンのネットワークインターフェイスコントローラーで必要なネットワークがインストールされていないホスト、またはクラスターのディスプレイネットワークがインストールされていないホスト。

フィールド名	説明
Weights Modules	<p>仮想マシンを実行できるクラスター内のホストを決定する際に考慮される要因の相対優先度を制御する重みのセット。</p> <ul style="list-style-type: none"> ● InClusterUpgrade: オペレーティングシステムのバージョンに応じてホストを重み付けします。重みは、同じオペレーティングシステムを持つホストよりも古いオペレーティングシステムを持つホストを固定し、新しいオペレーティングシステムを持つホストを優先します。 ● OptimalForHaReservation: 高可用性スコアに従ってホストを重み付けします。 ● None: 均等割り付けモジュールに基づいてホストの重み付けを行います。 ● OptimalForEvenGuestDistribution: ホスト上で稼働している仮想マシンの数に応じて、ホストを重み付けします。 ● VmAffinityGroups: 仮想マシンに定義されたアフィニティーグループに応じて、ホストを重み付けします。この加重モジュールは、あるアフィニティーグループの仮想マシンが、そのアフィニティーグループのパラメーターに応じて、同じホスト上で実行される可能性や、別々のホスト上で実行される可能性を決定します。 ● OptimalForPowerSaving: CPU 使用率に応じてホストを重み付けし、CPU 使用率が高いホストを優先します。 ● OptimalForEvenDistribution: CPU 使用率に応じてホストを重み付けし、CPU 使用率が低いホストに優先度を提供します。 ● HA: 高可用性スコアに応じてホストを重み付けします。
ロードバランサー	このドロップダウンメニューでは、適用する負荷分散モジュールを選択できます。負荷分散モジュールは、使用率が高いホストから、使用率が低いホストに仮想マシンを移行するために使用されるロジックを決定します。
プロパティー	このドロップダウンメニューでは、負荷分散モジュールのプロパティーを追加または削除でき、スケジューリングポリシーに負荷分散モジュールを選択している場合にのみ利用できます。デフォルトではプロパティーは定義されておらず、利用可能なプロパティーは、選択された負荷分散モジュールに固有です。+ および - ボタンを使用して、負荷分散モジュールにプロパティーを追加または削除します。

1.4. インスタンスタイプ

インスタンスタイプを使用して、仮想マシンのハードウェア設定を定義できます。仮想マシンの作成時または編集時にインスタンスタイプを選択すると、ハードウェア設定フィールドが自動的に入力されます。これにより、すべてのフィールドを手動で入力しなくても、同じハードウェア設定で複数の仮想マシンを作成できます。

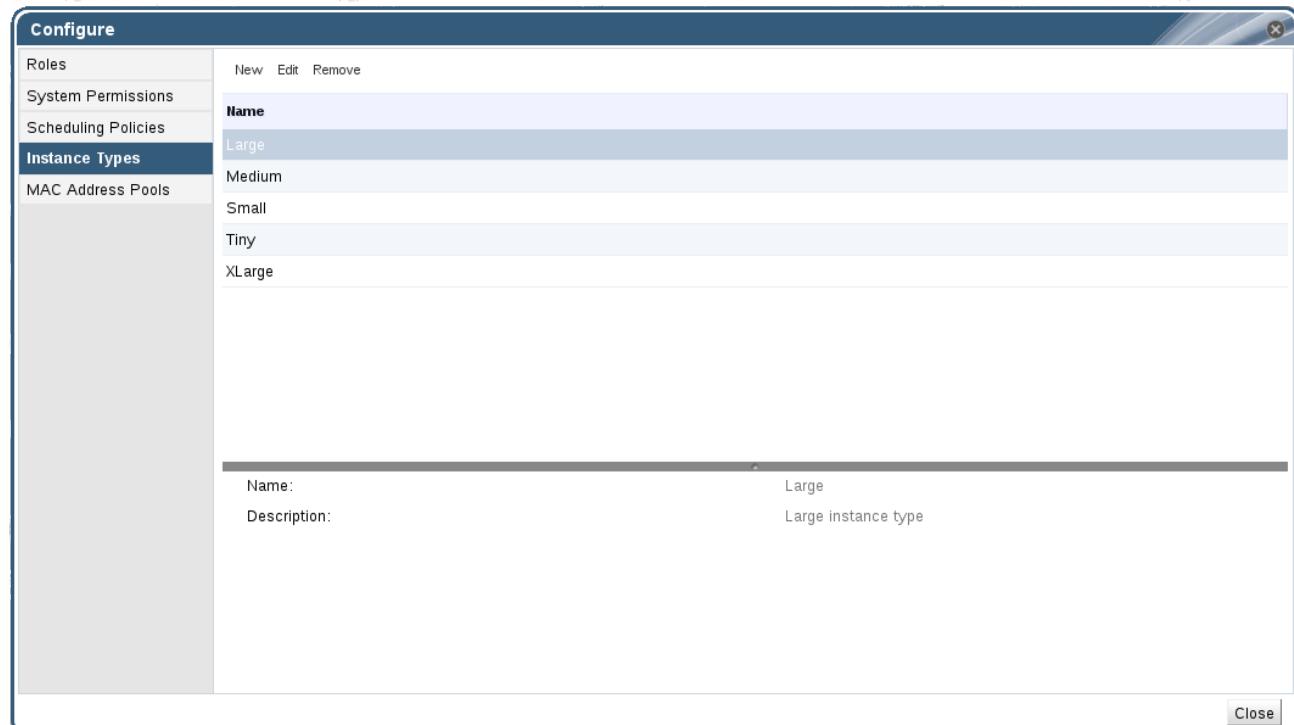
以下の表で説明されているように、事前定義されたインスタンスタイプのセットはデフォルトで利用できます。

表1.6 事前定義されたインスタンスタイプ

Name	メモリー	vCPU
Tiny	512 MB	1
Small	2 GB	1
中	4 GB	2
Large	8 GB	2
XLarge	16 GB	4

管理者は **Configure** ウィンドウの **Instance Types** タブからインスタンスタイプを作成、編集、および削除することもできます。

図1.9 インスタンスタイプタブ



インスタンスタイプにバインドされる **New Virtual Machine** および **Edit Virtual Machine** ウィンドウのフィールドの横にチェーンリンクイメージがあります（ これらのフィールドの値のいずれかが変更されると、仮想マシンはインスタンスタイプから切り離され、**Custom** に変更され、チェーンが破

損しているように見えます（ しかし、値が元に戻されると、チェーンは再度リンクし、インスタンスタイプは選択されたものに戻ります。

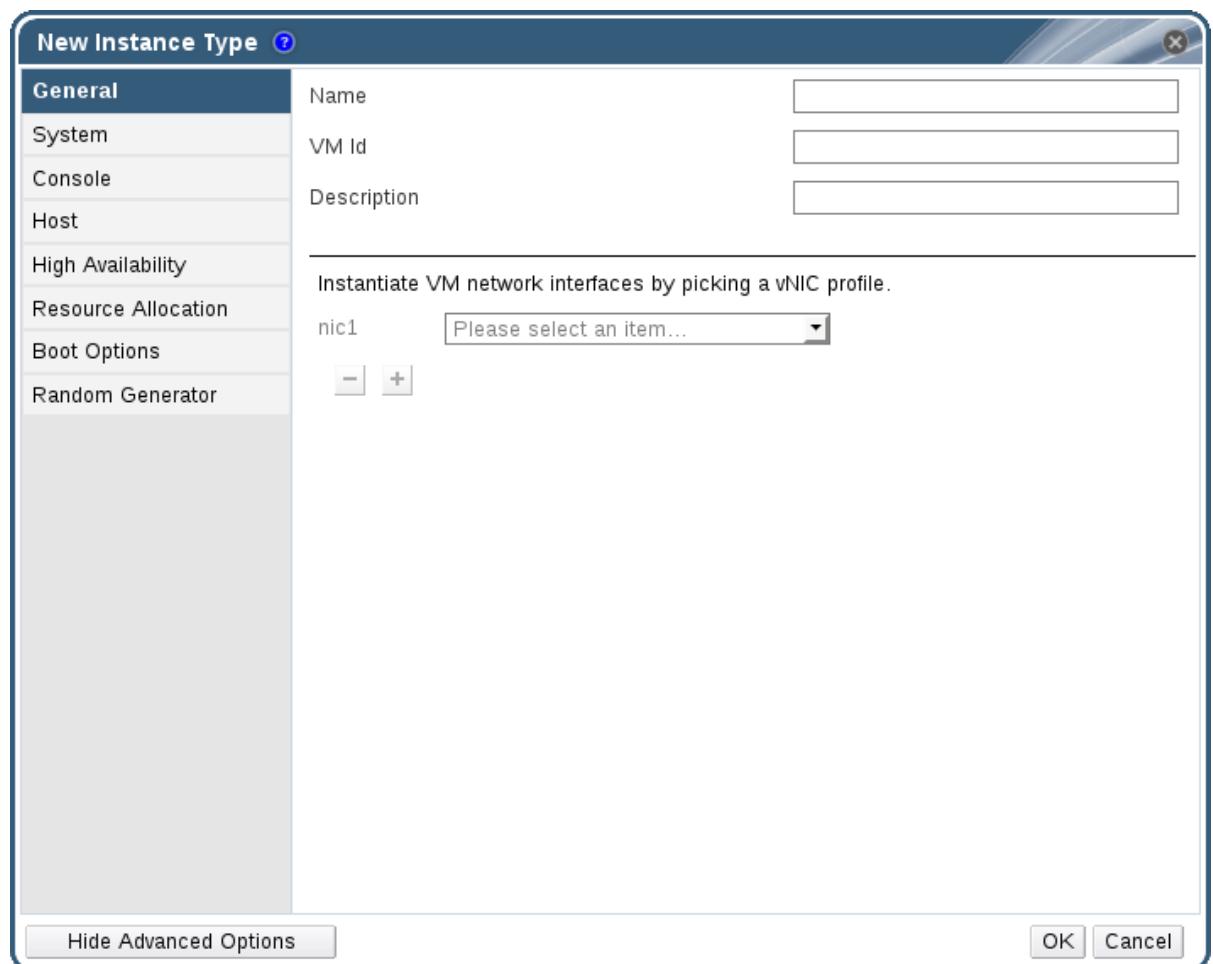
1.4.1. インスタンスタイプの作成

管理者は、仮想マシンの作成時または編集時にユーザーが選択する新しいインスタンスタイプを作成できます。

手順1.4 インスタンスタイプの作成

1. ヘッダーバーで **Configure** をクリックします。
2. **Instance Types** タブをクリックします。
3. **New** をクリックして **New Instance Type** ウィンドウを開きます。

図1.10 New Instance Type ウィンドウ



4. インスタンスタイプの **Name** および **Description** を入力します。
5. **Show Advanced Options** をクリックし、必要に応じてインスタンスタイプの設定を設定します。 **New Instance Type** ウィンドウに表示される設定は、**New Virtual Machine** ウィンドウの設定と同じですが、関連するフィールドのみが表示されます。『Virtual Machine Management Guide』の [Explanation of Settings in the New Virtual Machine and Edit Virtual Machine Windows](#) を参照してください。
6. **OK** をクリックします。

新規インスタンスタイプは **Configure** ウィンドウの **Instance Types** タブに表示され、仮想マシンの作成時または編集時に **Instance Type** ドロップダウンリストから選択できます。

1.4.2. インスタンスタイプの編集

管理者は **Configure** ウィンドウから既存のインスタンスタイプを編集できます。

手順1.5 インスタンスタイププロパティーの編集

1. ヘッダーバーで **Configure** をクリックします。
2. **Instance Types** タブをクリックします。
3. 編集するインスタンスタイプを選択します。
4. **Edit** をクリックして **Edit Instance Type** ウィンドウを開きます。
5. 必要に応じて設定を変更します。
6. **OK** をクリックします。

インスタンスタイプの設定が更新されます。このインスタンスタイプに基づく新しい仮想マシンが作成されるか、このインスタンスタイプに基づく既存の仮想マシンが更新されると、新しい設定が適用されます。

このインスタンスタイプに基づく既存の仮想マシンには、更新されるチェーンアイコンが付いたフィールドが表示されます。インスタンスタイプの変更時に既存の仮想マシンが稼働していた場合は、その横にオレンジ色の Pending Changes アイコンが表示され、次回の再起動時にチェーンのアイコンが付いたフィールドが更新されます。

1.4.3. インスタンスタイプの削除

手順1.6 インスタンスタイプの削除

1. ヘッダーバーで **Configure** をクリックします。
2. **Instance Types** タブをクリックします。
3. 削除するインスタンスタイプを選択します。
4. **Remove** をクリックして、**Remove Instance Type** ウィンドウを開きます。
5. 削除するインスタンスタイプに基づいた仮想マシンがある場合は、アタッチされた仮想マシンをリストする警告ウィンドウが表示されます。インスタンスタイプの削除を続行するには、**Approve Operation** チェックボックスを選択します。それ以外の場合は、**Cancel** をクリックします。
6. **OK** をクリックします。

インスタンスタイプが **Instance Types** 一覧から削除され、新規仮想マシンの作成時に使用できなくなりました。削除されたインスタンスタイプにアタッチされた仮想マシンは **Custom**（インスタンスタイプなし）にアタッチされます。

1.5. MAC アドレスプール

MAC アドレスプールは、各データセンターに MAC アドレスを割り当てる MAC アドレスの範囲を定義します。各データセンターに MAC アドレスプールが指定されます。MAC アドレスプールを使用すると、Red Hat Virtualization は MAC アドレスを自動的に新しい仮想ネットワークデバイスに割り当て、MAC アドレスの重複を防ぐことができます。MAC アドレスプールは、データセンターに関連するすべての MAC アドレスが、割り当てられた MAC アドレスプールの範囲内にあると、メモリー効率が高くなります。

同じ MAC アドレスプールを複数のデータセンターで共有できますが、各データセンターには MAC アドレスプールが1つ割り当てられます。デフォルトの MAC アドレスプールは Red Hat Virtualization によって作成され、別の MAC アドレスプールが割り当てられない場合に使用されます。データセンターへの MAC アドレスプールの割り当ての詳細は、「[新規データセンターの作成](#)」を参照してください。

MAC アドレスプールでは、最後にプールに戻されたアドレスの次に利用可能な MAC アドレスが割り当てられます。範囲内に残されたアドレスがない場合には、範囲の先頭から検索を再開します。1つの MAC アドレスプールに、利用可能な MAC アドレスがある複数の MAC アドレスの範囲が定義されている場合、利用可能な MAC アドレスが選択されるのと同じように、範囲が順番に受信リクエストに対応します。

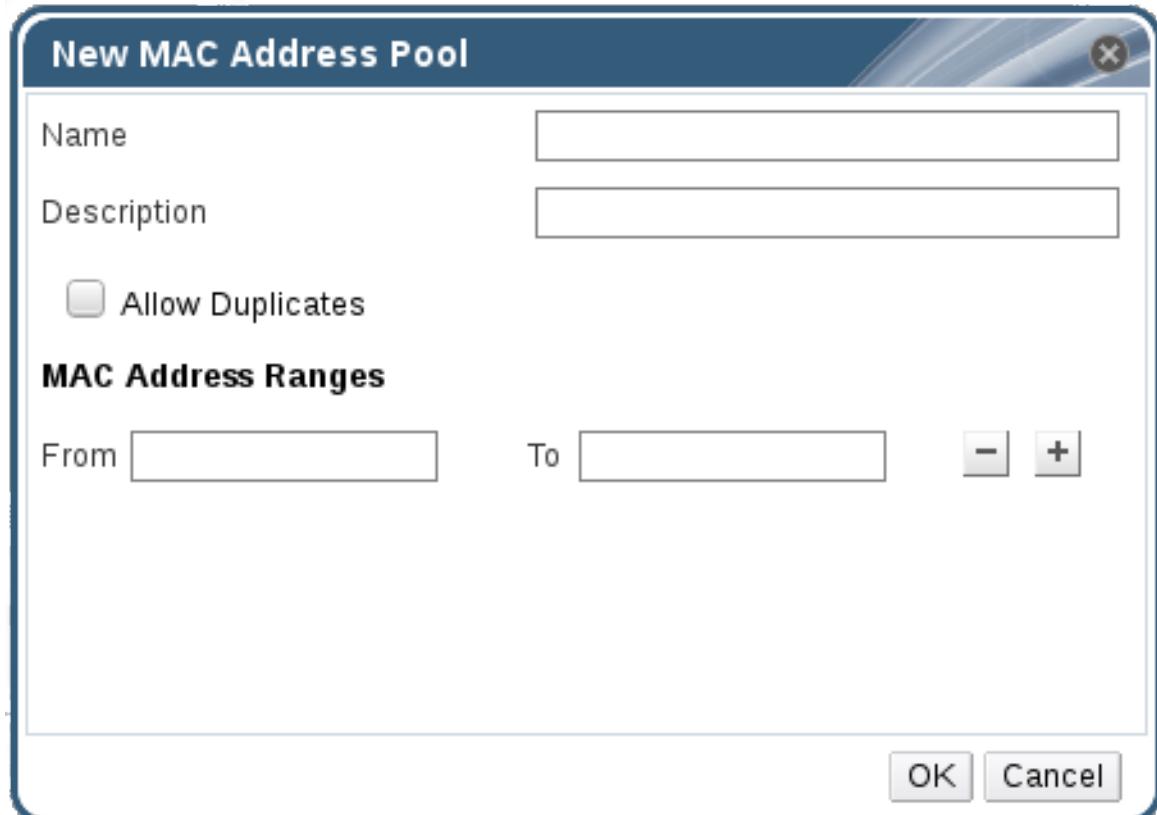
1.5.1. MAC アドレスプールの作成

新しい MAC アドレスプールを作成できます。

手順1.7 MAC アドレスプールの作成

1. ヘッダーバーで **Configure** ボタンをクリックして **Configure** ウィンドウを開きます。
2. **MAC Address Pools** タブをクリックします。
3. **Add** ボタンをクリックして **New MAC Address Pool** ウィンドウを開きます。

図1.11 新しい MAC アドレスプールウィンドウ



4. 新しい MAC アドレスプールの **Name** および **Description** を入力します。
5. **Allow Duplicates** チェックボックスを選択し、MAC アドレスをプールで複数回使用できるようになります。MAC アドレスプールでは、重複した MAC アドレスを自動的に使用することはできませんが、duplicates オプションを有効にすると、ユーザーが重複した MAC アドレスを手動で使用できます。



注記

ある MAC アドレスプールで重複を無効にし、別の MAC アドレスプールで重複を有効にした場合、重複を無効にしたプールでは各 MAC アドレスは1回しか使用できませんが、重複を有効にしたプールでは複数回使用できます。

6. 必要な **MAC Address Ranges** を入力します。複数の範囲を入力するには、**From** および **To** フィールドの横にあるプラスボタンをクリックします。
7. **OK** をクリックします。

1.5.2. MAC アドレスプールの編集

MAC アドレスプールを編集して、プールで利用可能な MAC アドレスの範囲や重複が許可されるかどうかなどの詳細を変更できます。

手順1.8 MAC アドレスプールプロパティーの編集

1. ヘッダーバーで **Configure** ボタンをクリックして **Configure** ウィンドウを開きます。
2. **MAC Address Pools** タブをクリックします。
3. 編集する MAC アドレスプールを選択します。
4. **Edit** ボタンをクリックして、**Edit MAC Address Pool** ウィンドウを開きます。
5. 必要に応じて **Name**、**Description**、**Allow Duplicates**、および **MAC Address Ranges** フィールドを変更します。



注記

MAC アドレス範囲を更新すると、既存の NIC の MAC アドレスは再割り当てされません。すでに割り当てられている MAC アドレスで、新しい MAC アドレスの範囲外のものは、ユーザー指定の MAC アドレスとして追加され、その MAC アドレスプールで追跡されます。

6. **OK** をクリックします。

1.5.3. MAC アドレスプールのパーミッションの編集

MAC アドレスプールの作成後に、そのユーザー権限を編集できます。ユーザー権限により、どのデータセンターが MAC アドレスプールを使用できるかが制御されます。新規ユーザー権限の追加に関する詳細は、「[ロール](#)」を参照してください。

手順1.9 MAC アドレスプールのパーミッションの編集

1. ヘッダーバーで **Configure** ボタンをクリックして **Configure** ウィンドウを開きます。

2. **MAC Address Pools** タブをクリックします。
3. 必要な MAC アドレスプールを選択します。
4. MAC アドレスプールのユーザー割り当てを編集します。
 - ユーザー割り当てを MAC アドレスプールに追加するには、以下を実行します。
 - a. **Configure** ウィンドウの下にあるユーザー権限ペインで **Add** をクリックします。
 - b. 必要なユーザーを検索して選択します。
 - c. **Role to Assign** ドロップダウンリストから必要なロールを選択します。
 - d. **OK** をクリックしてユーザー割り当てを追加します。
 - ユーザー割り当てを MAC アドレスプールから削除するには、以下を実行します。
 - a. **Configure** ウィンドウの下にあるユーザー権限ペインで削除するユーザー割り当てを選択します。
 - b. **削除** をクリックしてユーザー割り当てを削除します。

1.5.4. MAC アドレスプールの削除

作成した MAC アドレスプールを削除できますが、デフォルトの MAC アドレスプールは削除できません。

手順1.10 MAC アドレスプールの削除

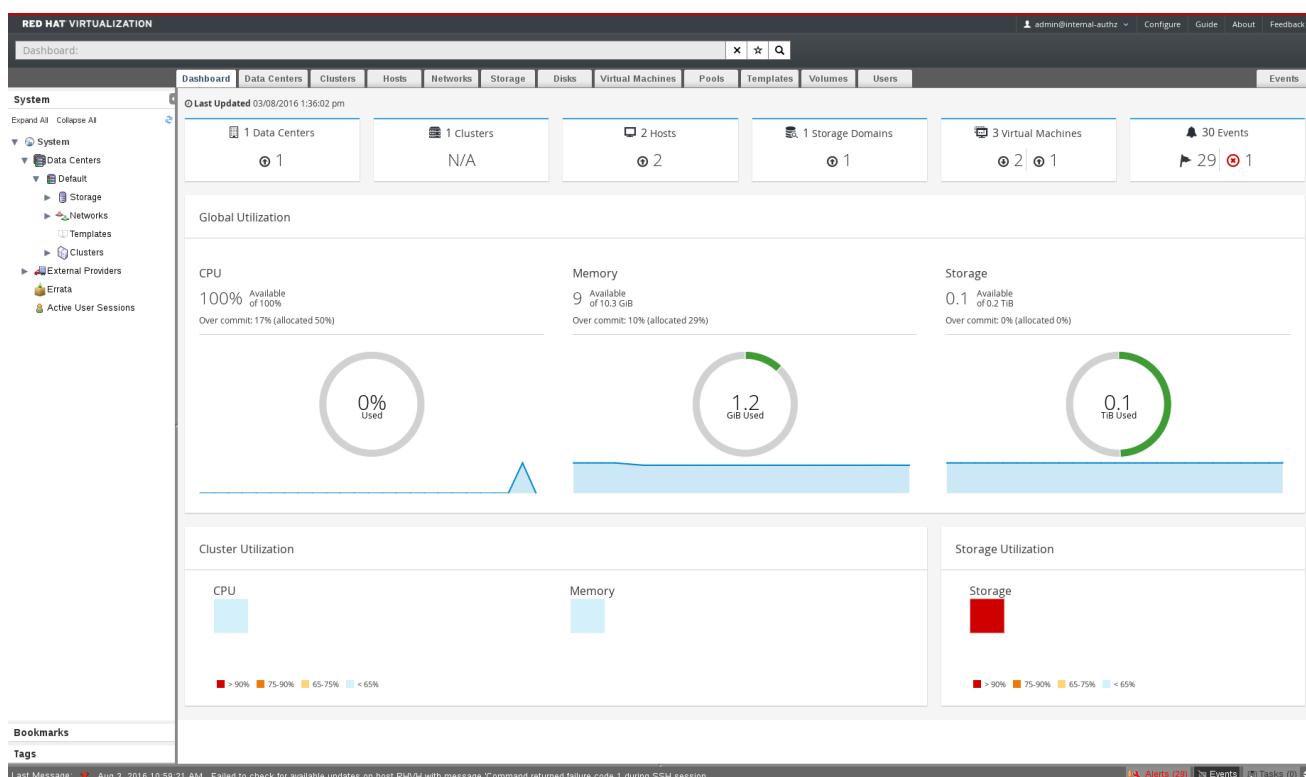
1. ヘッダーバーで **Configure** ボタンをクリックして **Configure** ウィンドウを開きます。
2. **MAC Address Pools** タブをクリックします。
3. 削除する MAC アドレスプールを選択します。
4. **Remove** ボタンをクリックして、**Remove MAC Address Pool** ウィンドウを開きます。
5. **OK** をクリックします。

第2章 ダッシュボード

ダッシュボードでは、Red Hat Virtualization のリソースと使用状況の概要を表示することで、Red Hat Virtualization のシステムステータスの概要を説明します。このサマリーはユーザーに問題を警告し、問題領域の分析を可能にします。

ダッシュボードの情報は、デフォルトで Data Warehouse から 15 分ごとに更新され、Manager API ではデフォルトで 15 秒ごと、またはダッシュボードが更新されるたびに更新されます。Dashboard は、ユーザーが別のタブから戻る場合や、手動で更新したときに更新されます。ダッシュボードは自動的に更新されません。インベントリーカードの情報は Manager API で提供され、使用状況の情報は Data Warehouse から提供されます。ダッシュボードは、UI プラグインコンポーネントとして実装されており、Managerと一緒に自動的にインストールおよびアップグレードされます。

図2.1 ダッシュボード



2.1. 前提条件

Dashboard では、Data Warehouse がインストールされ、設定されている必要があります。Data Warehouse のインストールおよび設定の詳細は、『Data Warehouse Guide』の [Installing and Configuring Data Warehouse](#) を参照してください。

2.2. グローバルインベントリー

ダッシュボードの上部には、Red Hat Virtualization リソースのグローバルインベントリーが表示され、データセンター、クラスター、ホスト、ストレージドメイン、仮想マシン、イベントなどの項目が含まれます。アイコンは各リソースの状態、数字はその状態にある各リソースの数量を表しています。

図2.2 グローバルインベントリー



タイトルにはリソースの種類別の数が表示され、その下にはステータスが表示されます。リソースのタイトルをクリックすると、Red Hat Virtualization Manager の関連タブに移動します。**Clusters** のステータスは常に N/A と表示されます。

表2.1 リソースの状況

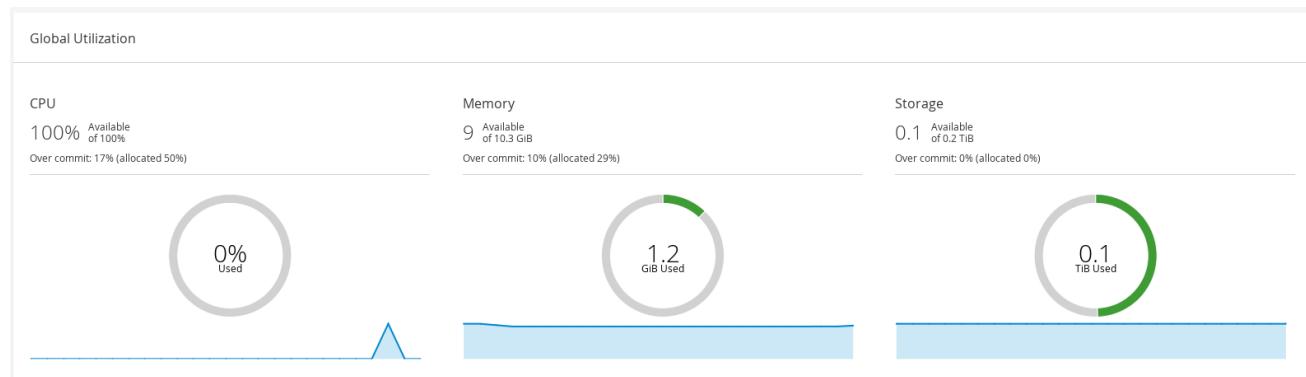
アイコン	Status
	Red Hat Virtualization にはそのようなリソースは一切追加されていません。
	<p>警告ステータスを持つリソースの番号を表示します。アイコンをクリックすると適切なタブに移動し、検索対象は警告ステータスでそのリソースに限定されます。検索の制限は、リソースごとに異なります。</p> <ul style="list-style-type: none"> Data Centers: 検索対象は、稼働していないデータセンターや応答しないデータセンターに限定されます。 ホスト: 検索は、割り当てられていない、メンテナーンスマード、インストール、再起動、メンテナーンスの準備、承認待ち、または接続中のホストに限定されます。 ストレージ ドメイン: 検索対象は、初期化されていない、アタッチされていない、非アクティブのストレージドメイン、メンテナーンスマードの準備、メンテナーンスの準備、デタッチ、またはアクティブ化のストレージドメインに限定されます。 仮想マシン: 検索は、起動、一時停止、移行、待機中、中断中、またはオフになっている仮想マシンに限定されます。 Events: 検索は重大度が警告のイベントに制限されます。
	up ステータスを持つリソースの番号を表示します。アイコンをクリックすると、適切なタブに移動し、検索対象は up になっているリソースに限定されます。
	<p>down 状態のリソースの番号を表示します。アイコンをクリックすると適切なタブに移動し、検索対象は down 状態のリソースに限定されます。検索の制限は、リソースごとに異なります。</p> <ul style="list-style-type: none"> Data Centers: 検索対象は、初期化されていないデータセンター、メンテナーンスマード、または down ステータスのデータセンターに限定されます。 ホスト: 検索対象は、応答しないホスト、エラーのある、インストールエラー、動作していない、初期化、またはダウンであるホストに限定されます。 ストレージ ドメイン: 検索対象は、デタッチまたは非アクティブのストレージドメインに限定されます。 仮想マシン: 検索対象は、ダウン中、応答していない、または再起動中の仮想マシンに限定されます。
	アラートステータスを持つイベントの数を表示します。アイコンをクリックすると Events タブに移動し、検索対象は重大度がアラートのイベントに限定されます。
	エラーステータスを持つイベントの数を表示します。アイコンをクリックすると Events タブに移動し、検索対象は重大度がエラーのイベントに限定されます。



2.3. グローバルでの活用

Global Utilization セクションには、CPU、メモリー、およびストレージのシステム使用率が表示されます。

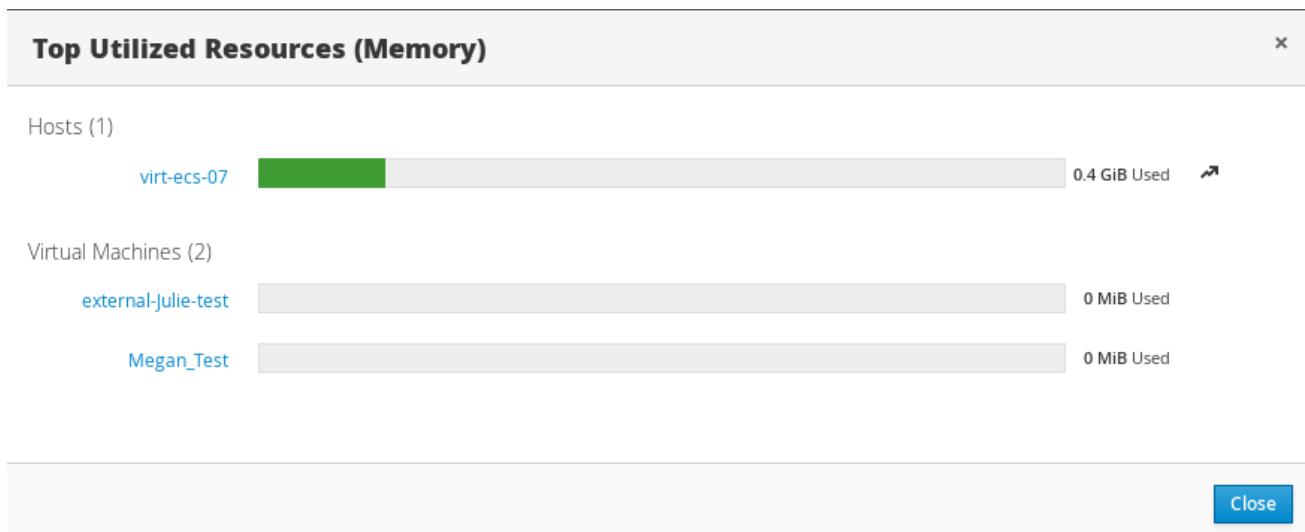
図2.3 グローバルでの活用



- 上段には、利用可能なCPU、メモリー、ストレージ、およびオーバーコミット率の割合が表示されます。たとえば、CPUのオーバーコミット率は、Data Warehouseの最新データに基づいて実行中の仮想マシンで利用可能な物理コアの数で仮想コア数を除算して計算されます。
- ドーナツは、CPU、メモリー、またはストレージの使用率をパーセンテージで表示し、過去5分間の平均使用率に基づいて、すべてのホストの平均使用率を表示します。ドーナツの断面にカーソルを合わせると、選択したセクションの値が表示されます。
- 下部の折れ線グラフは、過去24時間の傾向を表示しています。各データポイントは、特定の時間の平均使用量を示しています。グラフ上のポイントにカーソルを合わせると、CPUのグラフでは時間と使用率が、メモリーとストレージのグラフでは使用量が表示されます。

2.3.1. 最も使用されているリソース

図2.4 最も使用されているリソース(メモリー)

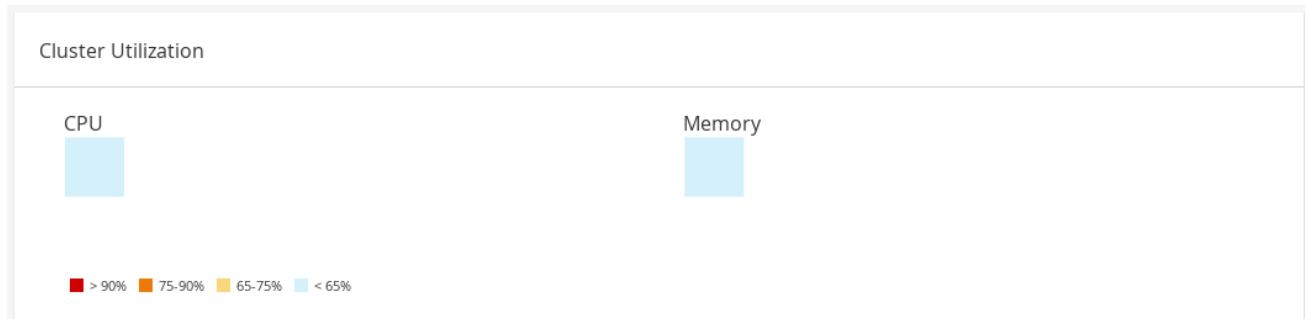


ダッシュボードのグローバル使用率の項目にあるドーナツをクリックすると、CPU、メモリー、ストレージのうち、使用率の高いリソースのリストが表示されます。CPUとメモリーについては、最も使用率の高い10台のホストと仮想マシンのリストがポップアップで表示されます。ストレージについては、利用しているストレージドメインと仮想マシンのトップ10のリストがポップアップで表示されます。使用量バーの右にある矢印は、そのリソースの直近1分間の使用量の傾向を示しています。

2.4. クラスターの活用

Cluster Utilization は、CPUおよびメモリーのクラスター使用率をヒートマップで表示します。

図2.5 クラスターの活用



2.4.1. CPU

過去24時間のCPUの平均使用率を示す特定クラスターのCPU使用率のヒートマップ。ヒートマップにカーソルを合わせると、クラスターネームが表示されます。ヒートマップをクリックすると、**ホスト**タブに移動し、特定のクラスターの検索をCPU使用率でソートした結果が表示されます。クラスターによるCPUの使用率を計算するために使用される式は、クラスターのホストCPU使用率の平均です。これは、クラスターによるCPUの合計平均使用率を出すために、過去24時間の各ホストのCPU使用率の平均値を用いて算出されます。

2.4.2. メモリー

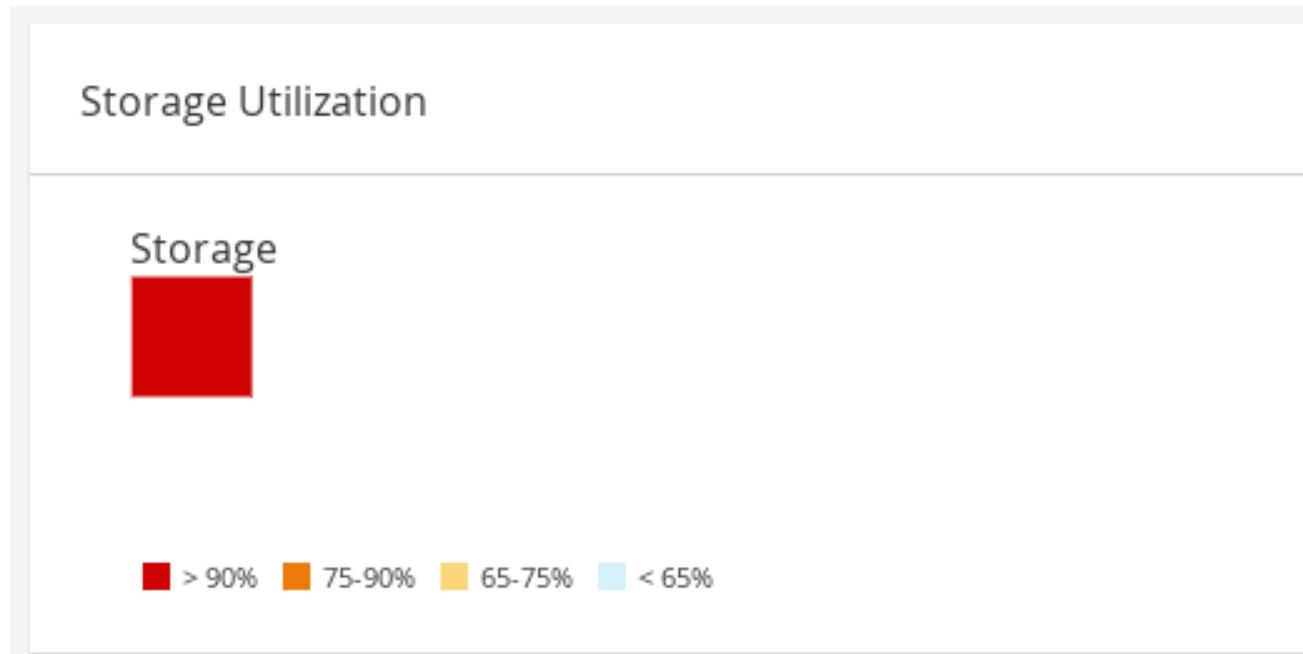
過去24時間のメモリーの平均使用率を示す特定クラスターのメモリー使用率のヒートマップ。ヒートマップにカーソルを合わせると、クラスターネームが表示されます。ヒートマップをクリックすると、**ホスト**タブに移動し、特定のクラスターの検索の結果がメモリー使用量でソートされます。クラスターによ

るメモリー使用率を計算するために使用される式は、クラスターのメモリー使用率の合計(GB単位)です。これは、クラスターによるメモリー合計平均使用率を出すために、過去24時間の各ホストの平均メモリー使用率を用いて算出されます。

2.5. ストレージの活用

Storage Utilization は、ヒートマップでストレージの使用状況を表示します。

図2.6 ストレージの活用



ヒートマップは、過去 24 時間のストレージの平均利用率を表します。クラスターによるストレージ使用率を計算するために使用される式は、クラスターのストレージ使用率の合計です。これは、クラスターによるストレージの合計平均使用率を出すために、過去 24 時間の各ホストの平均ストレージ使用率を用いて算出されます。ヒートマップにカーソルを合わせると、ストレージドメイン名が表示されます。ヒートマップをクリックすると、**Storage** タブに移動し、ストレージドメインが使用率別にソートされます。

パート II. リソースの管理

第3章 QOS (QUALITY OF SERVICE)

Red Hat Virtualization では、環境のリソースがアクセスできる入出力、処理、およびネットワーク機能のレベルを詳細に制御する QoS エントリーを定義できます。QoS (Quality of Service) エントリーはデータセンターレベルで定義され、クラスターおよびストレージドメイン下で作成されるプロファイルに割り当てられます。これらのプロファイルは、プロファイルが作成されたクラスターおよびストレージドメインの個々のリソースに割り当てられます。

3.1. ストレージ QoS

ストレージ QoS はスループットの最大レベルと、ストレージドメインの仮想ディスクの入出力操作の最大レベルを定義します。ストレージ QoS を仮想ディスクに割り当てるとき、ストレージドメインのパフォーマンスを細かく調整でき、1つの仮想ディスクに関連付けられたストレージ操作が、同じストレージドメインでホストされる他の仮想ディスクで利用できるストレージ機能に影響しないようにすることができます。

3.1.1. ストレージ QoS エントリーの作成

ストレージ QoS (Quality of Service) エントリーを作成します。

手順3.1 ストレージ QoS エントリーの作成

1. **Data Centers** resource タブをクリックし、データセンターを選択します。
2. 詳細ペインで **QoS** をクリックします。
3. **Storage** をクリックします。
4. **New** をクリックします。
5. **QoS Name** フィールドにサービス品質エントリーの名前を入力します。
6. **Description** フィールドに、Quality of Service エントリーの説明を入力します。
7. スループット QoS (Quality of Service) を指定します。
 - a. **Throughput** チェックボックスを選択します。
 - b. **Total** フィールドに最大許容合計スループットを入力します。
 - c. **Read** フィールドに、読み取り操作の最大許容スループットを入力します。
 - d. **Write** フィールドに、書き込み操作の最大許容スループットを入力します。
8. 入出力 QoS を指定します。
 - a. **IOps** チェックボックスを選択します。
 - b. **Total** フィールドに、1秒あたりの入出力操作の最大許容数を入力します。
 - c. **Read** フィールドに、1秒あたりの入力操作の最大許容数を入力します。
 - d. **Write** フィールドに、1秒あたりの出力操作の最大許容数を入力します。
9. **OK** をクリックします。

ストレージ QoS エントリーが作成され、データセンターに属するデータストレージドメインのそのエントリーに基づいてディスクプロファイルを作成できます。

3.1.2. ストレージ Quality of Service エントリーの削除

既存のストレージ QoS(Quality of Service) エントリーを削除します。

手順3.2 ストレージ Quality of Service エントリーの削除

1. **Data Centers** resource タブをクリックし、データセンターを選択します。
2. 詳細ペインで **QoS** をクリックします。
3. **Storage** をクリックします。
4. 削除するストレージの QoS エントリーを選択します。
5. **削除** をクリックします。
6. プロンプトが表示されたら **OK** をクリックします。

ストレージ QoS エントリーが削除され、そのエントリーは利用できなくなりました。そのエントリーに基づくディスクプロファイルが存在する場合、それらのプロファイルのストレージ QOS エントリーは自動的に **[unlimited]** に設定されます。

3.2. 仮想マシンのネットワーク QoS

仮想マシンネットワーク QoS は、個々の仮想ネットワークインターフェイスコントローラーの受信および送信トラフィックの両方を制限するためのプロファイルを作成できる機能です。この機能により、複数のレイヤーで帯域幅を制限し、ネットワークリソースの使用を制御できます。

3.2.1. 仮想マシンのネットワーク QoS エントリーの作成

仮想マシンネットワーク QoS エントリーを作成し、仮想ネットワークインターフェイスコントローラー (vNIC) プロファイル (仮想マシンネットワークインターフェイスプロファイル) に適用される際にネットワークトラフィックを規制します。

手順3.3 仮想マシンのネットワーク QoS エントリーの作成

1. **Data Centers** resource タブをクリックし、データセンターを選択します。
2. 詳細ペインの **QoS** タブをクリックします。
3. **VM Network** をクリックします。
4. **New** をクリックします。
5. 仮想マシンネットワーク QoS (Quality of Service) エントリーの名前を **Name** フィールドに入力します。
6. **Inbound** および **Outbound** ネットワークトラフィックの制限を入力します。
7. **OK** をクリックします。

仮想ネットワークインターフェイスコントローラーで使用可能な仮想マシンネットワーク QoS エントリーが作成されました。

3.2.2. New Virtual Machine Network QoS および Edit Virtual Machine Network QoS ウィンドウの設定の説明

仮想マシンのネットワーク QoS 設定により、3つの異なるレベルで送受信トラフィックの両方に帯域幅の制限を設定できます。

表3.1 仮想マシンネットワーク QoS 設定

フィールド名	説明
Data Center	仮想マシンのネットワーク QoS ポリシーを追加するデータセンター。このフィールドは、選択したデータセンターに応じて自動的に設定されます。
Name	Manager 内の仮想マシンネットワーク QoS ポリシーを表す名前。
Inbound	受信トラフィックに適用される設定。 Inbound チェックボックスを選択または選択解除して、これらの設定を有効または無効にします。 <ul style="list-style-type: none"> ● 平均: 受信トラフィックの平均速度。 ● ピーク: ピーク時の受信トラフィックの速度。 ● burst: バースト中の受信トラフィックの速度。
Outbound	送信トラフィックに適用される設定。 Outbound チェックボックスを選択または選択解除して、これらの設定を有効または無効にします。 <ul style="list-style-type: none"> ● 平均: 送信トラフィックの平均速度。 ● ピーク: ピーク時の送信トラフィックの速度。 ● burst: バースト中の送信トラフィックの速度。

3.2.3. 仮想マシンのネットワーク QoS(Quality of Service) エントリーの削除

既存の仮想マシンネットワーク QoS(Quality of Service) エントリーを削除します。

手順3.4 仮想マシンのネットワーク QoS(Quality of Service) エントリーの削除

1. **Data Centers** resource タブをクリックし、データセンターを選択します。
2. 詳細ペインの **QoS** タブをクリックします。

3. **VM Network** をクリックします。
4. 削除する仮想マシンネットワーク QoS エントリーを選択します。
5. **削除** をクリックします。
6. プロンプトが表示されたら **OK** をクリックします。

仮想マシンネットワーク QoS エントリーが削除され、そのエントリーは利用できなくなりました。

3.3. ホストネットワーク QoS

ホストネットワーク QoS は、ホスト上のネットワークを設定し、物理インターフェイス経由のネットワークトラフィックの制御を可能にします。ホストネットワーク QoS により、同じ物理ネットワークインターフェイスコントローラー上のネットワークリソースの使用を制御することで、ネットワークのパフォーマンスをより細かく調整できます。これにより、1つのネットワークが原因で、同じ物理ネットワークインターフェイスコントローラーにアタッチされている他のネットワークがトラフィックの輻輳により機能しなくなる状況を防ぐことができます。ホストネットワーク QoS 設定により、これらのネットワークは、輻輳問題なしに同じ物理ネットワークインターフェイスコントローラー上で機能できるようになります。

3.3.1. ホストネットワーク QoS エントリーの作成

ホストネットワーク QoS(Quality of Service) エントリーを作成します。

手順3.5 ホストネットワーク QoS エントリーの作成

1. **Data Centers** resource タブをクリックし、データセンターを選択します。
2. 詳細ペインで **QoS** をクリックします。
3. **Host Network** をクリックします。
4. **New** をクリックします。
5. **QoS Name** フィールドにサービス品質エントリーの名前を入力します。
6. **Description** フィールドに、Quality of Service エントリーの説明を入力します。
7. **Weighted Share**、**Rate Limit [Mbps]**、および **Committed Rate [Mbps]** に必要な値を入力します。
8. **OK** をクリックします。

3.3.2. New Host Network Quality of Service および Edit Host Network Quality of Service ウィンドウの設定の説明

ホストネットワーク QoS 設定により、送信トラフィックの帯域幅制限を設定できます。

表3.2 ホストネットワーク QoS 設定

フィールド名	説明

フィールド名	説明
Data Center	ホストネットワーク QoS ポリシーを追加するデータセンター。このフィールドは、選択したデータセンターに応じて自動的に設定されます。
QoS Name	Manager 内のホストネットワーク QoS ポリシーを表す名前。
説明	ホストネットワーク QoS ポリシーの説明
Outbound	<p>送信トラフィックに適用される設定。</p> <ul style="list-style-type: none"> 加重共有: 同じ論理リンクに接続されている他のネットワークと比較して、特定のネットワークを割り当てる必要がある論理リンクの容量を示します。正確な共有は、そのリンクの全ネットワークの共有の合計によって異なります。デフォルトでは、この値は 1-100 の範囲の数字になります。 Rate Limit [Mbps]: ネットワークが使用する最大帯域幅。 Committed Rate [Mbps]: ネットワークに必要な最小帯域幅。要求される Committed Rate は保証されず、ネットワークインフラストラクチャーおよび同じ論理リンクの他のネットワークによって要求される Committed Rate によって異なります。

3.3.3. ホストネットワーク QoS エントリーの削除

既存のネットワーク QoS(Quality of Service) エントリーを削除します。

手順3.6 ホストネットワーク QoS エントリーの削除

1. **Data Centers** resource タブをクリックし、データセンターを選択します。
2. 詳細ペインの **QoS** タブをクリックします。
3. **Host Network** をクリックします。
4. 削除するネットワーク QoS エントリーを選択します。
5. **削除** をクリックします。
6. プロンプトが表示されたら **OK** をクリックします。

3.4. CPU QOS (QUALITY OF SERVICE)

CPU QoS は、仮想マシンが実行するホストでアクセスできる最大処理機能を定義します。これは、そのホストで利用可能な合計処理機能のパーセントで表されます。CPU QoS を仮想マシンに割り当てるとき、クラスター内の1つの仮想マシンのワークロードが、そのクラスター内の他の仮想マシンで利用可能な処理リソースに影響を与えないようにすることができます。

3.4.1. CPU QoS エントリーの作成

CPU QoS (Quality of Service)エントリーを作成します。

手順3.7 CPU QoS エントリーの作成

1. **Data Centers** resource タブをクリックし、データセンターを選択します。
2. 詳細ペインで **QoS** をクリックします。
3. **CPU** をクリックします。
4. **New** をクリックします。
5. **QoS Name** フィールドにサービス品質エントリーの名前を入力します。
6. **Description** フィールドに、Quality of Service エントリーの**説明** を入力します。
7. **Limit** フィールドに許可されるサービス品質エントリーの最大処理機能をパーセンテージで入力します。%記号は含めないでください。
8. **OK** をクリックします。

CPU QoS エントリーが作成され、データセンターに属するクラスター内のそのエントリーに基づいて CPU プロファイルを作成できます。

3.4.2. CPU QoS エントリーの削除

既存の CPU QoS (Quality of Service)エントリーを削除します。

手順3.8 CPU QoS エントリーの削除

1. **Data Centers** resource タブをクリックし、データセンターを選択します。
2. 詳細ペインで **QoS** をクリックします。
3. **CPU** をクリックします。
4. 削除する CPU QoS エントリーを選択します。
5. **削除** をクリックします。
6. プロンプトが表示されたら **OK** をクリックします。

CPU QoS エントリーが削除され、そのエントリーは利用できなくなりました。CPU プロファイルがそのエントリーに基づいている場合、それらのプロファイルの CPU QoS エントリーは自動的に **[unlimited]** に設定されます。

第4章 データセンター

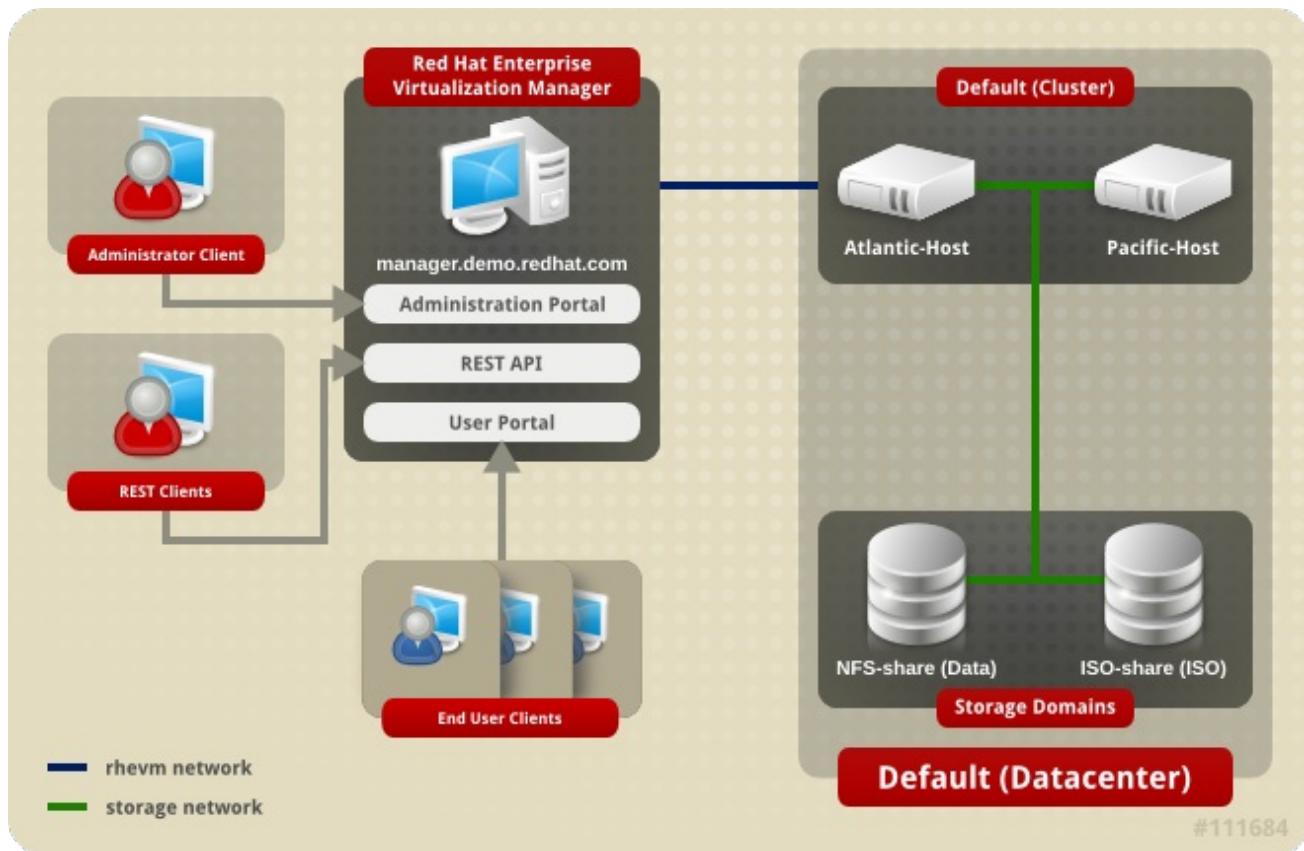
4.1. データセンターの概要

データセンターとは、特定の環境で使用するリソースのセットを定義する論理エンティティーです。データセンターは、コンテナリソース（クラスターとホストの形式の論理リソースで設定）、ネットワークリソース（論理ネットワークと物理 NIC の形式）、およびストレージリソース（ストレージドメインの形式）と見なされます。

データセンターには、複数のホストを含む複数のクラスターを含めることができます。複数のストレージドメインが関連付けられており、各ホスト上の複数の仮想マシンをサポートすることができます。Red Hat Virtualization 環境には複数のデータセンターを含めることができます。データセンターインフラストラクチャーを使用すると、これらのセンターを分離した状態にすることができます。

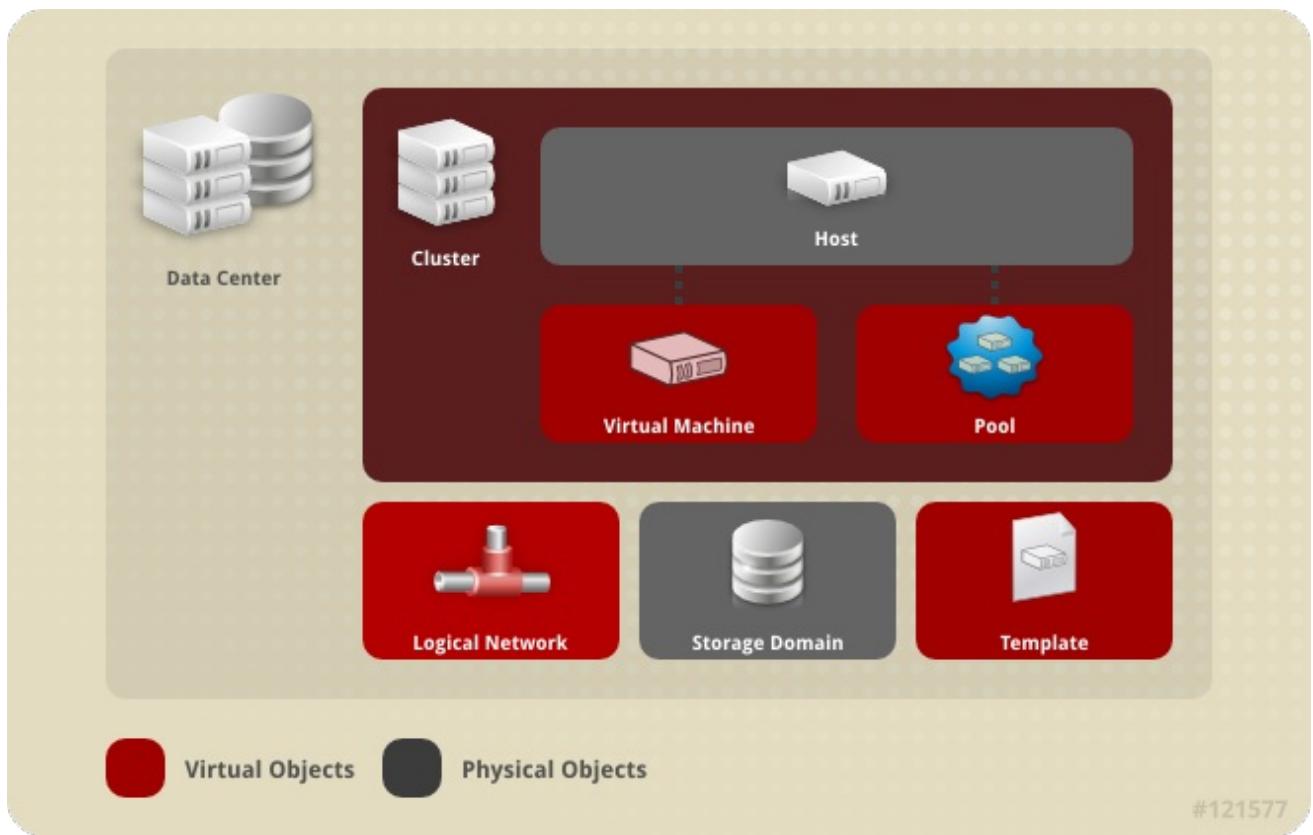
すべてのデータセンターは、1つの管理ポータルから管理されます。

図4.1データセンター



Red Hat Virtualization は、インストール時にデフォルトのデータセンターを作成します。デフォルトのデータセンターを設定するか、または適切に名前が付けられたデータセンターを設定できます。

図4.2 データセンターオブジェクト



4.2. STORAGE POOL MANAGER

Storage Pool Manager(SPM) は、データセンター内のホストのいずれかに渡すロールで、データセンターのストレージドメインを管理できるようにします。SPM エンティティーはデータセンター内の任意のホストで実行できます。Red Hat Virtualization Manager はいずれかのホストにロールを付与します。SPM は標準の操作からホストを事前に設定しません。SPM として実行されているホストは依然として仮想リソースをホストできます。

SPM エンティティーは、ストレージドメイン全体でメタデータを調整することにより、ストレージへのアクセスを制御します。これには、仮想ディスク(イメージ)、スナップショット、およびテンプレートの作成、削除、およびテンプレート、およびスペースブロックデバイス(SAN 上)のストレージの割り当てが含まれます。これは唯一の責任です。メタデータの整合性を確保するために、データセンターの SPM となるホスト 1 つのみです。

Red Hat Virtualization Manager は、SPM が常に利用できることを確認します。SPM ホストがストレージへのアクセスに問題がある場合は、Manager は SPM ロールを別のホストに移動します。SPM が起動すると、これがロールが付与された唯一のホストであることを確認します。したがって、ストレージ中心のリースを取得します。このプロセスには時間がかかる場合があります。

4.3. SPM の優先度

SPM ロールは、ホストの利用可能なリソースの一部を使用します。ホストの SPM 優先度の設定により、ホストが SPM ロールが割り当てられる可能性があります。SPM 優先度が高いホストには、SPM の優先度が低いホストの前に SPM ロールが割り当てられます。SPM 優先度が低いホストの重要な仮想マシンは、ホストリソースの SPM 操作と連動させる必要はありません。

ホストを編集することで、ホストの SPM の優先度を変更できます。

4.4. イベントタブを使用したデータセンターの問題オブジェクトの特定

データセンターの **Events** タブには、そのデータセンターに関連付けられたすべてのイベントが表示されます。イベントには、監査、警告、エラーが含まれます。結果一覧に表示される情報により、Red Hat Virtualization 環境の問題オブジェクトを識別できます。

Events results リストには、Basic と Advanced の 2 つのビューがあります。基本ビューには、イベントアイコン、イベントの時間、およびイベントの説明が表示されます。高度なビューでは、これらとインクルードも表示されます（該当する場合はイベント ID）。関連するユーザー、ホスト、仮想マシン、テンプレート、データセンター、ストレージ、およびクラスター、Gluster ボリューム、相関 ID。

4.5. データセンタータスク

4.5.1. 新規データセンターの作成

以下の手順では、お使いの仮想化環境にデータセンターを作成します。データセンターが機能するには、機能しているクラスター、ホスト、およびストレージドメインが必要です。



注記

ストレージ タイプは、最初のストレージドメインがデータセンターに追加されるまで編集できます。ストレージドメインが追加されると、ストレージ タイプを変更することはできません。

互換バージョンを設定すると、後で低くすることはできず、バージョンのリグレッションは許可されません。

手順4.1新規データセンターの作成

1. **Data Centers** resource タブを選択して、結果一覧内のすべてのデータセンターを一覧表示します。
2. **New** をクリックして **New Data Center** ウィンドウを開きます。
3. データセンターの **Name** および **Description** を入力します。
4. ドロップダウンメニューから、データセンターのストレージタイプ、互換バージョン、および クオータモードを選択します。
5. 必要に応じて、データセンターの MAC アドレスプールを変更します。デフォルトの MAC アドレスプールはデフォルトで事前に選択されます。MAC アドレスプールの作成に関する詳細は、「[MAC アドレスプール](#)」を参照してください。
 - a. **MAC Address Pool** タブをクリックします。
 - b. **MAC Address Pool** ドロップダウンリストから必要な MAC アドレスプールを選択します。
6. **OK** をクリックしてデータセンターを作成し、**New Data Center - Guide Me** ウィンドウを開きます。
7. **Guide Me** ウィンドウには、データセンター用に設定する必要のあるエンティティーが一覧表示されます。**Configure Later** ボタンをクリックして、これらのエンティティーを設定するか、または設定を延期します。設定は、データセンターを選択して **Guide Me** ボタンをクリックして再開できます。

新しいデータセンターが仮想化環境に追加されます。クラスター、ホスト、およびストレージドメインが設定されるまで **Uninitialized** のままになります。**Guide Me** を使用してこれらのエンティティーを設定します。

4.5.2. New Data Center および Edit Data Center Windows の設定についての説明

以下の表は、**New Data Center** および **Edit Data Center** ウィンドウに表示されるデータセンターの設定について説明しています。**OK** をクリックすると、無効なエントリーがオレンジ色で囲まれ、変更が承認されません。さらに、フィールドプロンプトは予想される値または値の範囲を示します。

表4.1データセンターのプロパティー

フィールド	説明/アクション
Name	データセンターの名前。このテキストフィールドには 40 文字の制限があり、大文字、小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。
説明	データセンターの説明このフィールドは推奨されますが、必須ではありません。
タイプ	ストレージタイプ。以下のいずれかを選択します。 <ul style="list-style-type: none"> ● 共有 ● Local <p>データドメインのタイプはデータセンターのタイプを決定し、大きな中断なしに作成後に変更することはできません。複数のタイプのストレージドメイン(iSCSI、NFS、FC、POSIX、および Gluster)を同じデータセンターに追加できますが、ローカルドメインと共有ドメインを混在させることはできません。</p>
互換バージョン	Red Hat Virtualization のバージョン。以下のいずれかを選択します。 <ul style="list-style-type: none"> ● 3.6 ● 4.0 <p>Red Hat Virtualization Manager をアップグレードした後には、ホスト、クラスター、およびデータセンターが以前のバージョンにある可能性があります。データセンターの互換性レベルをアップグレードする前に、すべてのホストをアップグレードし、クラスターをアップグレードしていることを確認します。</p>

フィールド	説明/アクション
クォータモード	<p>クォータは、Red Hat Virtualization で提供されるリソース制限ツールです。以下のいずれかを選択します。</p> <ul style="list-style-type: none"> ● Disabled: クォータを実装しない場合は選択します。 ● 監査: クォータ設定を編集する場合に選択します。 ● Enforced: クォータを実装する場合に選択します。
MAC アドレスプール	<p>データセンターの MAC アドレスプール。他の MAC アドレスプールが割り当てられていない場合は、デフォルトの MAC アドレスプールが使用されます。MAC アドレスプールの詳細は、「MAC アドレスプール」 を参照してください。</p>

4.5.3. データセンターの再初期化: リカバリーハンドル

この復旧手順は、データセンターのマスターデータドメインを新しいマスターデータドメインに置き換えます。これは、マスターデータドメインのデータが破損した場合に必要です。データセンターを再初期化すると、クラスター、ホスト、および問題以外のストレージドメインなど、データセンターに関連付けられた他のリソースをすべて復元できます。

バックアップまたはエクスポートした仮想マシンまたはテンプレートを新しいマスターデータドメインにインポートできます。

手順4.2 データセンターの再初期化

1. **Data Centers** resource タブをクリックし、再初期化するデータセンターを選択します。
2. データセンターに接続されたストレージドメインがメンテナンスモードにあることを確認します。
3. データセンターを右クリックし、ドロップダウンメニューから **Re-Initialize Data Center** を選択して、**Data Center Re-Initialize** ウィンドウを開きます。
4. **Data Center Re-Initialize** ウィンドウには、利用可能なすべての（割り当て解除あり、メンテナンスモードの場合）ストレージドメインが一覧表示されます。データセンターに追加するストレージドメインのラジオボタンをクリックします。
5. **Approve operation** チェックボックスを選択します。
6. **OK** をクリックしてウィンドウを閉じ、データセンターを再初期化します。

ストレージドメインは、マスターデータドメインとしてデータセンターにアタッチされ、アクティベートされます。バックアップまたはエクスポートした仮想マシンまたはテンプレートを新しいマスターデータドメインにインポートできるようになりました。

4.5.4. データセンターの削除

データセンターを削除するには、アクティブなホストが必要です。データセンターを削除しても、関連付けられたリソースは削除されません。

手順4.3 データセンターの削除

1. データセンターに接続されたストレージドメインがメンテナنسモードにあることを確認します。
2. **Data Centers** resource タブをクリックし、削除するデータセンターを選択します。
3. **Remove** をクリックして、**Remove Data Center (s)** 確認ウィンドウを開きます。
4. **OK** をクリックします。

4.5.5. データセンターの強制削除

アタッチされたストレージドメインが破損したり、ホストが **Non Responsive** になった場合、データセンターが **Non Responsive** になります。いずれの状況でもデータセンターを 削除 することはできません。

Force Remove では、アクティブなホストは必要ありません。また、アタッチされているストレージドメインも完全に削除します。

データセンターを **強制的に削除** する前に、破損したストレージドメインを **破棄** する必要がある場合があります。

手順4.4 データセンターの強制削除

1. **Data Centers** resource タブをクリックし、削除するデータセンターを選択します。
2. **Force Remove** をクリックして、**Force Remove Data Center** の確認ウィンドウを開きます。
3. **Approve operation** チェックボックスを選択します。
4. **OK** をクリックします。

データセンターおよび割り当てられたストレージドメインは、Red Hat Virtualization 環境から完全に削除されます。

4.5.6. データセンターの互換バージョンの変更

Red Hat Virtualization データセンターには、互換バージョンがあります。互換バージョンは、データセンターが互換性を持つ Red Hat Virtualization のバージョンを示します。データセンター内のクラスターは、すべて指定の互換性レベルをサポートする必要があります。



注記

データセンターの互換バージョンを変更するには、最初にデータセンター内のすべてのクラスターを、必要な互換性レベルをサポートするレベルに更新する必要があります。

手順4.5 データセンターの互換バージョンの変更

1. 管理ポータルから、**Data Centers** タブをクリックします。

2. 表示される一覧から変更するデータセンターを選択します。
3. **Edit** をクリックします。
4. **互換バージョン** を必要な値に変更します。
5. **OK** をクリックして **Change Data Center Compatibility Version** の確認ウィンドウを開きます。
6. **OK** をクリックして確定します。

データセンターの互換バージョンを更新しました。



重要

互換性をアップグレードすると、データセンターに属するすべてのストレージドメインもアップグレードされます。

4.6. データセンターおよびストレージドメイン

4.6.1. 既存のデータドメインをデータセンターにアタッチ

Unattached のデータドメインは、データセンターにアタッチすることができます。複数のタイプ (iSCSI、NFS、FC、POSIX、および Gluster) の共有ストレージドメインを同じデータセンターに追加できます。

手順4.6 既存のデータドメインをデータセンターにアタッチ

1. **Data Centers** resource タブをクリックし、適切なデータセンターを選択します。
2. 詳細ペインで **Storage** タブを選択して、データセンターにすでにアタッチされているストレージドメインを一覧表示します。
3. **Attach Data** をクリックして、**Attach Storage** ウィンドウを開きます。
4. データセンターにアタッチするデータドメインのチェックボックスを選択します。複数のデータドメインを割り当てる場合は、複数のチェックボックスを選択できます。
5. **OK** をクリックします。

データドメインはデータセンターにアタッチされ、自動的にアクティブになります。

4.6.2. 既存の ISO ドメインをデータセンターにアタッチ

Unattached の ISO ドメインは、データセンターにアタッチすることができます。ISO ドメインは、データセンターと同じストレージタイプである必要があります。

データセンターに1つの ISO ドメインのみをアタッチできます。

手順4.7 既存の ISO ドメインをデータセンターにアタッチ

1. **Data Centers** resource タブをクリックし、適切なデータセンターを選択します。
2. 詳細ペインで **Storage** タブを選択して、データセンターにすでにアタッチされているストレージドメインを一覧表示します。

3. **Attach ISO** をクリックして、**Attach ISO Library** ウィンドウを開きます。
4. 適切な ISO ドメインのラジオボタンをクリックします。
5. **OK** をクリックします。

ISO ドメインはデータセンターにアタッチされ、自動的にアクティブになります。

4.6.3. 既存のエクスポートドメインをデータセンターにアタッチ



注記

エクスポートストレージドメインは非推奨になりました。ストレージデータドメインはデータセンターから接続を解除し、同じ環境または別の環境にある別のデータセンターにインポートすることができます。仮想マシン、フローティング仮想ディスクイメージ、およびテンプレートは、インポートされたストレージドメインからアタッチされたデータセンターにアップロードできます。ストレージドメインのインポートに関する詳細は、「[既存のストレージドメインのインポート](#)」を参照してください。

Unattached のエクスポートドメインは、データセンターにアタッチすることができます。データセンターには、エクスポートドメインを1つだけアタッチできます。

手順4.8 既存のエクスポートドメインをデータセンターにアタッチ

1. **Data Centers** resource タブをクリックし、適切なデータセンターを選択します。
2. 詳細ペインで **Storage** タブを選択して、データセンターにすでにアタッチされているストレージドメインを一覧表示します。
3. **Attach Export** をクリックして、**Attach Export Domain** ウィンドウを開きます。
4. 適切な エクスポートドメイン のラジオボタンをクリックします。
5. **OK** をクリックします。

エクスポートドメインはデータセンターにアタッチされ、自動的にアクティブになります。

4.6.4. データセンターからストレージドメインをデタッチ

データセンターからストレージドメインをデタッチすると、データセンターがそのストレージドメインと関連付けられなくなります。ストレージドメインは Red Hat Virtualization 環境から削除されず、別のデータセンターにアタッチすることができます。

仮想マシンやテンプレートなどのデータは、引き続きストレージドメインにアタッチされます。



注記

マスターストレージ(これが最後の利用可能なストレージドメインである場合)は削除できません。

手順4.9 データセンターからストレージドメインをデタッチ

1. **Data Centers** resource タブをクリックし、適切なデータセンターを選択します。

2. 詳細ペインで **Storage** タブを選択して、データセンターに接続されているストレージドメインを一覧表示します。
3. デタッチするストレージドメインを選択します。ストレージドメインが **Active** の場合は、**Maintenance** をクリックして **Maintenance Storage Domain (s)** の確認ウィンドウを開きます。
4. **OK** をクリックしてメンテナンスマードを開始します。
5. **Detach** をクリックして、**Detach Storage** の確認ウィンドウを開きます。
6. **OK** をクリックします。

ストレージドメインをデータセンターから切り離している。ストレージドメインが詳細ペインから消えるまでに最長数分かかる場合があります。

4.7. データセンターおよびパーミッション

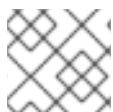
4.7.1. データセンターのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルのすべての側面を管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限された管理者ロールは、特定のリソースに制限される管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、そのデータセンターのストレージを除く、割り当てられたデータセンターの管理者権限のみを持ち、**ClusterAdmin** は割り当てられたクラスターに対してのみ管理者権限を持ちます。

データセンターの管理者は、特定のデータセンターのみのシステム管理ロールです。これは、各データセンターが管理者を必要とする複数のデータセンターを持つ仮想化環境で有用です。**DataCenterAdmin** ロールは階層モデルです。データセンターのデータセンター管理者ロールを割り当てられたユーザーは、そのデータセンターのストレージを除くすべてのオブジェクトを管理することができます。ヘッダーバーの **Configure** ボタンを使用して、環境内のすべてのデータセンターにデータセンター管理者を割り当てます。

データセンターの管理者ロールでは、以下のアクションが許可されます。

- データセンターに関連付けられたクラスターの作成と削除。
- データセンターに関連付けられたホスト、仮想マシン、およびプールを追加および削除。
- データセンターに関連付けられた仮想マシンのユーザーパーミッションの編集。



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てることができます。

既存のシステム管理者を削除し、新しいシステム管理者を追加すると、データセンターのシステム管理者を変更できます。

4.7.2. データセンター管理者ロールの概要

データセンターのパーミッションロール

以下の表は、データセンターの管理に適用される管理者ロールおよび権限を示しています。

表4.2 Red Hat Virtualization システム管理者ロール

ロール	権限	注記
DataCenterAdmin	データセンター管理者	クラスター、ホスト、テンプレート、仮想マシンなど、特定のデータセンター内の物理リソースおよび仮想リソースすべての作成、削除、管理が可能です。
NetworkAdmin	ネットワーク管理者	特定のデータセンターのネットワークを設定および管理できます。データセンターのネットワーク管理者は、データセンター内の仮想マシンのネットワークパーミッションも継承します。

4.7.3. 管理者またはユーザーロールのリソースへの割り当て

管理者またはユーザーロールをリソースに割り当て、ユーザーがそのリソースにアクセスしたり、管理したりできるようにします。

手順4.10 リソースへのロールの割り当て

- リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
- 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
- Add** をクリックします。
- Search** テキストボックスに既存ユーザーの名前またはユーザー名を入力し、**Go** をクリックします。表示された候補の中からユーザーを選択します。
- Role to Assign:** ドロップダウンリストからロールを選択します。
- OK** をクリックします。

ユーザーにロールを割り当てました。そのリソースで有効にしたそのロールの継承されたパーミッションが、ユーザーに付与されました。

4.7.4. リソースからの管理者またはユーザーロールの削除

管理者またはユーザーのロールをリソースから削除すると、ユーザーはそのリソースのロールに関連付けられ継承されたパーミッションを失います。

手順4.11 リソースからのロールの削除

- リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
- 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。

3. リソースから削除するユーザーを選択します。
4. **Remove** をクリックします。 **Remove Permission** 画面が開き、パーミッションの削除を確認します。
5. **OK** をクリックします。

ユーザーのロールおよび関連付けられたパーミッションをリソースから削除しました。

第5章 クラスター

5.1. クラスターの概要

クラスターは、同じストレージドメインを共有し、同じタイプのCPU(Intel または AMD)を持つホストの論理グループです。ホストに異なるCPUモデルの生成がある場合は、すべてのモデルに存在する機能のみを使用します。

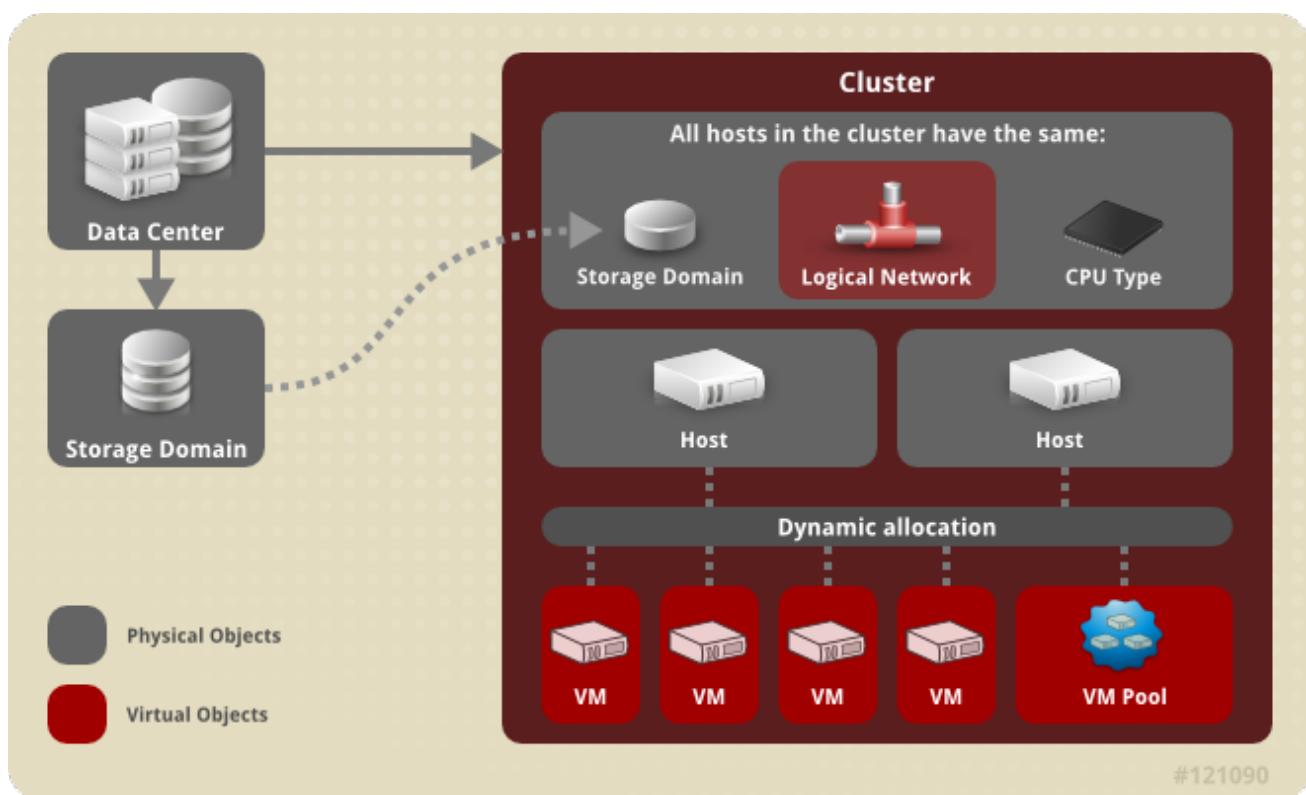
システム内の各クラスターはデータセンターに属し、システム内の各ホストはクラスターに属している必要があります。仮想マシンは、クラスター内の任意のホストに動的に割り当てられ、クラスタータブで定義されたポリシーとランタイム時に設定ツールで移行できます。クラスターは、電源および負荷分散ポリシーを定義できる最上位です。

クラスターに属するホストおよび仮想マシンの数は、**Host Count** および **VM Count** の結果の一覧にそれぞれ表示されます。

クラスターは仮想マシンまたは Red Hat Gluster Storage サーバーを実行します。これら 2 つの目的は相互排他的です。単一クラスターでは仮想化とストレージホストをまとめてサポートできません。

Red Hat Virtualization は、インストール時にデフォルトのデータセンターにデフォルトのクラスターを作成します。

図5.1 Cluster



5.2. クラスタータスク

5.2.1. 新規クラスターの作成

データセンターには複数のクラスターを含めることができます、クラスターには複数のホストを含めることができます。クラスター内のホストすべては、同じ CPU タイプ (Intel または AMD) である必要があります。

ます。CPU タイプの最適化を確保するには、クラスターを作成する前にホストを作成することが推奨されます。ただし、**Guide Me** ボタンを使用して、後でホストを設定できます。

手順5.1 新規クラスターの作成

1. **Clusters** resource タブを選択します。
2. **New** をクリックします。
3. ドロップダウンリストからクラスターが属する **Data Center** を選択します。
4. クラスターの **Name** および **Description** を入力します。
5. **Management Network** ドロップダウンリストからネットワークを選択して、管理ネットワークロールを割り当てます。
6. ドロップダウンリストから **CPU Architecture** および **CPU Type** を選択します。クラスターに接続するホストの最小 CPU プロセッサーティプと、CPU プロセッサーファミリーとを一致させることが重要です。そうでないと、ホストが機能しなくなります。



注記

Intel タイプおよび AMD CPU タイプの両方の場合、リストされた CPU モデルは、最も古いものから最新の順に論理的に使用されます。CPU モデルが異なるホストがクラスターに含まれる場合は、最も古い CPU モデルを選択します。各 CPU モデルの詳細は、[を参照してください](https://access.redhat.com/solutions/634853)

<https://access.redhat.com/solutions/634853>。

7. ドロップダウンリストから、クラスターの **互換バージョン** を選択します。
8. **Enable Virt Service** または **Enable Gluster Service** ラジオボタンを選択し、クラスターに仮想マシンホストまたは Gluster 対応ノードが設定されるかどうかを定義します。Red Hat Virtualization Host (RHVH)を Gluster 対応クラスターに追加できないことに注意してください。
9. Manager から仮想マシンをシャットダウンする際に任意の reason フィールドを有効にするには、**Enable to set VM maintenance reason** チェックボックスを選択し、管理者がメンテナансの説明を提供できるようにします。
10. ホストを Manager からメンテナスモードに移行する際に任意の reason フィールドを有効にするには、**Enable to set Host maintenance reason** チェックボックスを選択して、管理者がメンテナースの説明を提供できるようにします。
11. **/dev/random** ソース (Linux が提供するデバイス) または **/dev/hwrng** ソース (外部ハードウェアデバイス) のチェックボックスを選択し、クラスター内のすべてのホストが使用する乱数ジェネレーターデバイスを指定します。
12. **Optimization** タブをクリックして、クラスターのメモリーページ共有のしきい値を選択し、必要に応じてクラスター内のホストで CPU スレッド処理およびメモリーバルーンを有効にします。
13. **Migration Policy** タブをクリックして、クラスターの仮想マシンの移行ポリシーを定義します。

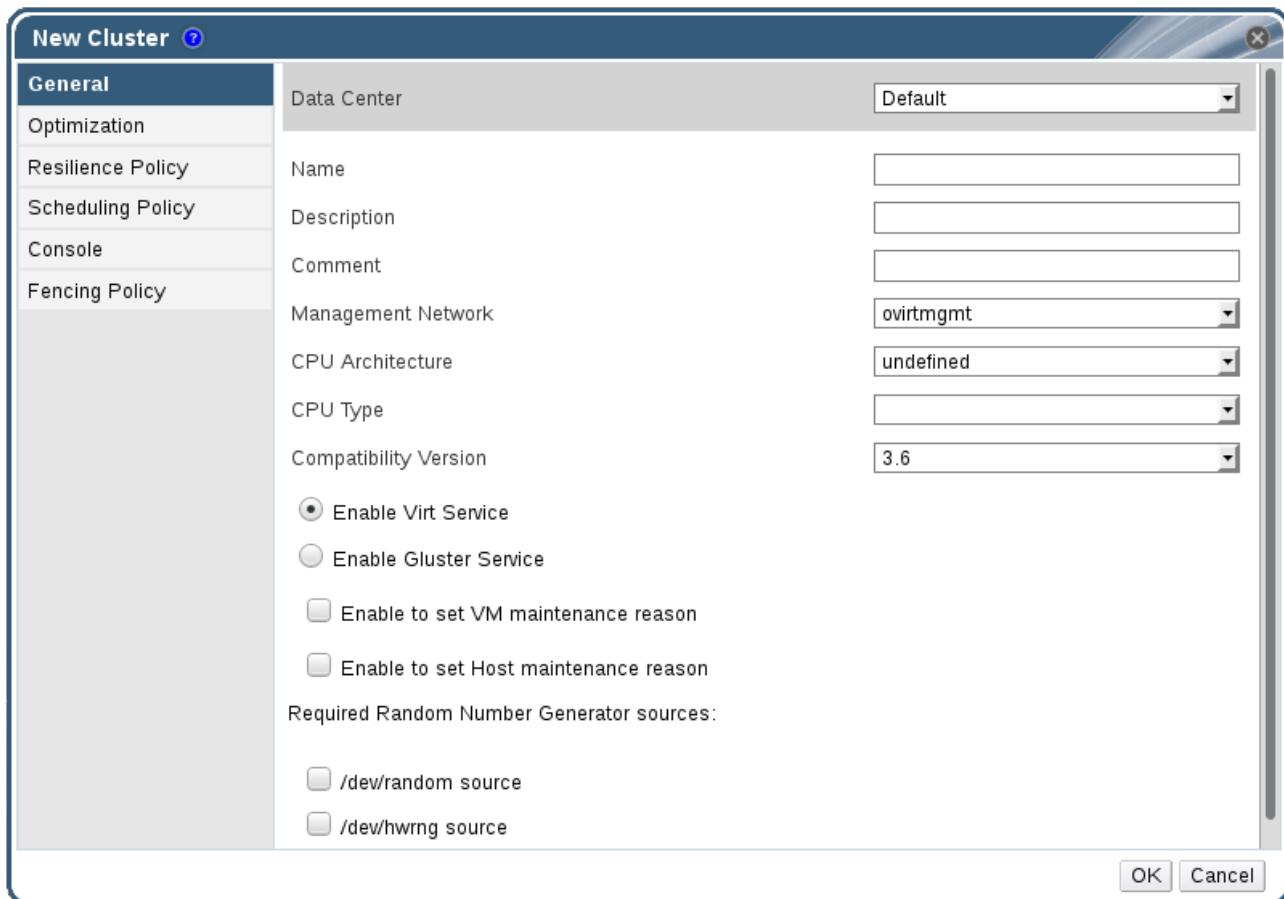
14. **Scheduling Policy** タブをクリックして、スケジューリングポリシーの設定、スケジューラー最適化の設定、クラスター内のホストの信頼できるサービスの有効化、HA Reservation の有効化、およびカスタムシリアル番号ポリシーの追加を行います。
15. **Console** タブをクリックしてオプションでグローバル SPICE プロキシーを上書きし（ある場合）、クラスター内のホストの SPICE プロキシーのアドレスを指定します。
16. **Fencing policy** タブをクリックして、クラスターでフェンシングを有効または無効にします。また、フェンスオプションを選択します。
17. **OK** をクリックしてクラスターを作成し、**New Cluster - Guide Me** ウィンドウを開きます。
18. **Guide Me** ウィンドウには、クラスター用に設定する必要のあるエンティティーが一覧表示されます。**Configure Later** ボタンをクリックしてこれらのエンティティーを設定するか、または設定を延期します。設定を再開するには、クラスターを選択し、**Guide Me** ボタンをクリックします。

新しいクラスターが仮想化環境に追加されます。

5.2.2. 新規クラスターの設定および制御の説明およびクラスター ウィンドウの編集

5.2.2.1. 一般的なクラスター設定に関する説明

図5.2 新規クラスター ウィンドウ



以下の表は、**New Cluster** および **Edit Cluster** ウィンドウの **General** タブの設定について説明しています。**OK** をクリックすると、無効なエントリーがオレンジに概要され、変更が受け入れられることが禁止されます。さらに、フィールドプロンプトは予想される値または値の範囲を示します。

表5.1一般的なクラスター設定

フィールド	説明/アクション
Data Center	クラスターが含まれるデータセンター。クラスターを追加する前にデータセンターを作成する必要があります。
Name	クラスターの名前。このテキストフィールドには 40 文字の制限があり、大文字、小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。
Description / Comment	クラスターまたは追加のメモの説明。これらのフィールドは推奨されますが、必須ではありません。
Management Network	管理ネットワークロールを割り当てる論理ネットワーク。デフォルトは ovirtmgmt です。既存のクラスターでは、詳細ペインの Logical Networks タブの Manage Networks ボタンからのみ管理ネットワークを変更できます。
CPU アーキテクチャー	クラスターの CPU アーキテクチャー。選択した CPU アーキテクチャーに応じて、さまざまな CPU タイプを利用できます。 <ul style="list-style-type: none"> ● undefined: すべての CPU タイプが利用できます。 ● x86_64: Intel および AMD CPU の全タイプが利用できます。 ● ppc64: IBM POWER 8 のみが利用できます。

フィールド	説明/アクション
CPU Type	<p>クラスターの CPU タイプ。以下のいずれかを選択します。</p> <ul style="list-style-type: none"> ● Intel Conroe ファミリー ● Intel Penryn Family ● Intel Nehalem ファミリー ● Intel Westmere ファミリー ● Intel SandyBridge ファミリー ● Intel Haswell ● AMD Opteron G1 ● AMD Opteron G2 ● AMD Opteron G3 ● AMD Opteron G4 ● AMD Opteron G5 ● IBM POWER 8 <p>クラスター内のホストはすべて、Intel、AMD、またはIBM POWER 8 の CPU タイプのいずれかを実行している必要があります、これは作成後には、大きな中断なしで変更することはできません。CPU タイプは、クラスター内の最も古い CPU モデルに設定する必要があります。すべてのモデルに存在する機能のみを使用できます。Intel タイプおよび AMD CPU タイプの両方の場合、リストされた CPU モデルは、最も古いものから最新の順に論理的に使用されます。</p>
互換バージョン	<p>Red Hat Virtualization のバージョン。以下のいずれかを選択します。</p> <ul style="list-style-type: none"> ● 3.6 ● 4.0 <p>データセンターに指定されたバージョンよりも古いバージョンを選択することはできません。</p>
Enable Virt Service	<p>このラジオボタンを選択すると、このクラスター内のホストは仮想マシンを実行するために使用されます。</p>

フィールド	説明/アクション
Enable Gluster Service	<p>このラジオボタンが選択される場合、このクラスターのホストは Red Hat Gluster Storage Server ノードとして使用されるため、仮想マシンの実行には使用されません。このオプションを有効にしたクラスターに Red Hat Virtualization Host を追加することはできません。</p>
Import existing gluster configuration	<p>このチェックボックスは、Enable Gluster Service ラジオボタンが選択されている場合にのみ利用できます。このオプションを使用すると、既存の Gluster 対応クラスターおよびその割り当てられたすべてのホストを Red Hat Virtualization Manager にインポートできます。</p> <p>以下のオプションは、インポートされているクラスター内のホストごとに必要になります。</p> <ul style="list-style-type: none"> ● アドレス: Gluster ホストサーバーの IP または完全修飾ドメイン名を入力します。 ● フィンガー プリント : Red Hat Virtualization Manager はホストのフィンガーリントを取得して、正しいホストに接続していることを確認します。 ● Root Password: ホストとの通信に必要な root パスワードを入力します。
Enable to set VM maintenance reason	<p>このチェックボックスを選択すると、クラスターの仮想マシンが Manager からシャットダウンすると、オプションの reason フィールドが表示されます。これにより、ログに表示されるメンテナーンスの説明と、仮想マシンの電源が再びオンになります。</p>
ホストのメンテナーンス理由の設定の有効化	<p>このチェックボックスを選択すると、クラスターのホストが Manager からメンテナーンスマードに移動すると、オプションの reason フィールドが表示されます。これにより、ログに表示されるメンテナーンスの説明と、ホストが再度アクティベートされたタイミングを指定できます。</p>
必要な乱数ジェネレーターソース :	<p>以下のチェックボックスを選択した場合には、クラスター内のすべてのホストにそのデバイスが利用可能な状態でなければなりません。これにより、乱数ジェネレーターデバイスから仮想マシンへのエントロピーのパススルーが可能になります。</p> <ul style="list-style-type: none"> ● /dev/random source: Linux が提供する乱数ジェネレーター。 ● /dev/hwrng source: 外部ハードウェアジェネレーター。

5.2.2.2. 最適化設定の説明

メモリーページの共有により、仮想マシンは、他の仮想マシンで未使用的メモリーを利用することで、割り当てられたメモリーの最大 200% を使用できます。このプロセスは、Red Hat Virtualization 環境内の仮想マシンが同時に実行されるという前提であり、未使用的メモリーを特定の仮想マシンに一時的に割り当てられるようにします。

CPU スレッド処理により、ホストは、ホストのコア数よりも大きいプロセッサーコアの合計数で仮想マシンを実行できます。これは、CPU 集約型ではないワークロードに役立ちます。これにより、より多くの仮想マシンを実行できるため、ハードウェアの要件を減らすことができます。また、特にゲストコアの数がホストコア数とホストスレッドの数の間にある場合に、仮想マシンが不可能な CPU トポロジーで実行できます。

以下の表は、**New Cluster** および **Edit Cluster** ウィンドウの **Optimization** タブの設定について説明しています。

表5.2 最適化の設定

フィールド	説明/アクション
メモリーの最適化	<ul style="list-style-type: none"> None - Disable memory overcommit: メモリーページの共有を無効にします。 Server Load - Allow scheduling of 150% of physical memory: 各ホストのシステムメモリーのメモリーページ共有しきい値を 150% に設定します。 For Desktop Load - Allow scheduling of 200% of physical memory: 各ホストのシステムメモリーの 200% にメモリーページ共有のしきい値を設定します。
CPU スレッド	<p>Count Threads As Cores チェックボックスを選択すると、ホストは、ホストのコア数よりも大きいプロセッサーコアの合計数で仮想マシンを実行できます。</p> <p>公開されるホストスレッドは、仮想マシンで使用できるコアとして処理されます。たとえば、コアごとに 2 つのスレッドがある 24 コアのシステム (全部で 48 スレッド) では、それぞれ最大 48 コアを持つ仮想マシンを実行できます。そして、ホストの CPU 負荷を計算するアルゴリズムは、使用量の多くのコアを 2 回比較します。</p>

フィールド	説明/アクション
メモリーバルーン	<p>Enable Memory Balloon Optimization チェックボックスを選択すると、このクラスターのホストで実行されている仮想マシンでメモリーのオーバーコミットが有効になります。このオプションを設定すると、Memory Overcommit Manager (MoM)はバルーンを開始します。可能な場合は、すべての仮想マシンのメモリーサイズが保証されます。</p> <p>バルーンが実行しているには、仮想マシンに適切なドライバーを持つバルーンデバイスが必要です。各仮想マシンには、特別に削除しない限り、バルーンデバイスが含まれます。このクラスター内の各ホストは、ステータスが Up に変わったときにバルーンポリシーの更新を受け取ります。必要に応じて、ステータスを変更せずに、ホストのバルーンポリシーを手動で更新できます。「クラスター内のホストでの MoM ポリシーの更新」を参照してください。</p> <p>シナリオのバルーンでは、KSM と一致している可能性がある点を理解することが重要です。このような場合は、MoM は競合の可能性を最小限に抑えるためにバルーンサイズの調整を試みます。さらに、シナリオのバルーンによっては、仮想マシンに対して最大のパフォーマンスが最適化される可能性があります。管理者は、バルーンの最適化を注意して使用することが推奨されます。</p>
KSM コントロール	<p>Enable KSM チェックボックスを選択すると、MoM は必要に応じて Kernel Same-page Merging (KSM)を実行できます。メモリーの保存により、CPU コストを上回る利点が得られます。</p>

5.2.2.3. 移行ポリシー設定の説明

移行ポリシーは、ホストに障害が発生した場合に仮想マシンのライブマイグレーションの条件を定義します。これらの状態には、移行中の仮想マシンのダウンタイム、ネットワーク帯域幅、および仮想マシンの優先順位が含まれます。

表5.3 移行ポリシーの説明

Policy	説明
Legacy	3.6 バージョンのレガシーアクション vdsctl.conf のオーバーライドは引き続き適用されます。ゲストエージェントフックメカニズムが無効になっている。
最小ダウンタイム	仮想マシンを一般的な状況で移行できるようにするポリシー。仮想マシンは、ダウンタイムを大幅に発生しません。移行は、長時間 (QEMU の反復により最大 500 ミリ秒) 後に仮想マシンの移行が収束されない場合に中止されます。ゲストエージェントフックメカニズムが有効になっている。

Policy	説明
必要に応じてワークロードを一時停止	負荷が大きい仮想マシンを含む、ほとんどの状況で仮想マシンが移行できるようにするポリシー。仮想マシンでは、より大きなダウンタイムが発生する可能性があります。移行は、極端なワークロードに対して中止される場合があります。ゲストエージェントフックメカニズムが有効になっている。

帯域幅設定は、ホストごとの送信移行と受信両方の最大帯域幅を定義します。

表5.4 帯域幅の説明

Policy	説明
Auto	帯域幅は、データセンターの Host Network QoS の Rate Limit [Mbps] 設定からコピーされます。レート制限が定義されていない場合は、ネットワークインターフェイス送受信の最小リンク速度として計算されます。レート制限が設定されていない場合や、リンク速度が利用できない場合には、ホスト送信時にローカルの VDSM 設定により決定されます。
ハイパーバイザーのデフォルト	帯域幅は、ホスト送信時にローカルの VDSM 設定によって制御されます。
カスタム	ユーザーで定義されます (Mbps 単位)。

耐障害性ポリシーは、移行での仮想マシンの優先順位を定義します。

表5.5 耐障害性ポリシーの設定

フィールド	説明/アクション
仮想マシンの移行	定義された優先順位で、すべての仮想マシンを移行します。
高可用性仮想マシンのみの移行	他のホストのオーバーロードを防ぐために、高可用性の仮想マシンのみを移行します。
Do not migrate Virtual Machines(仮想マシンを移行しない)	仮想マシンを移行しないようにします。

Additional Properties は、**Legacy** 移行ポリシーにのみ適用されます。

表5.6 その他のプロパティーの説明

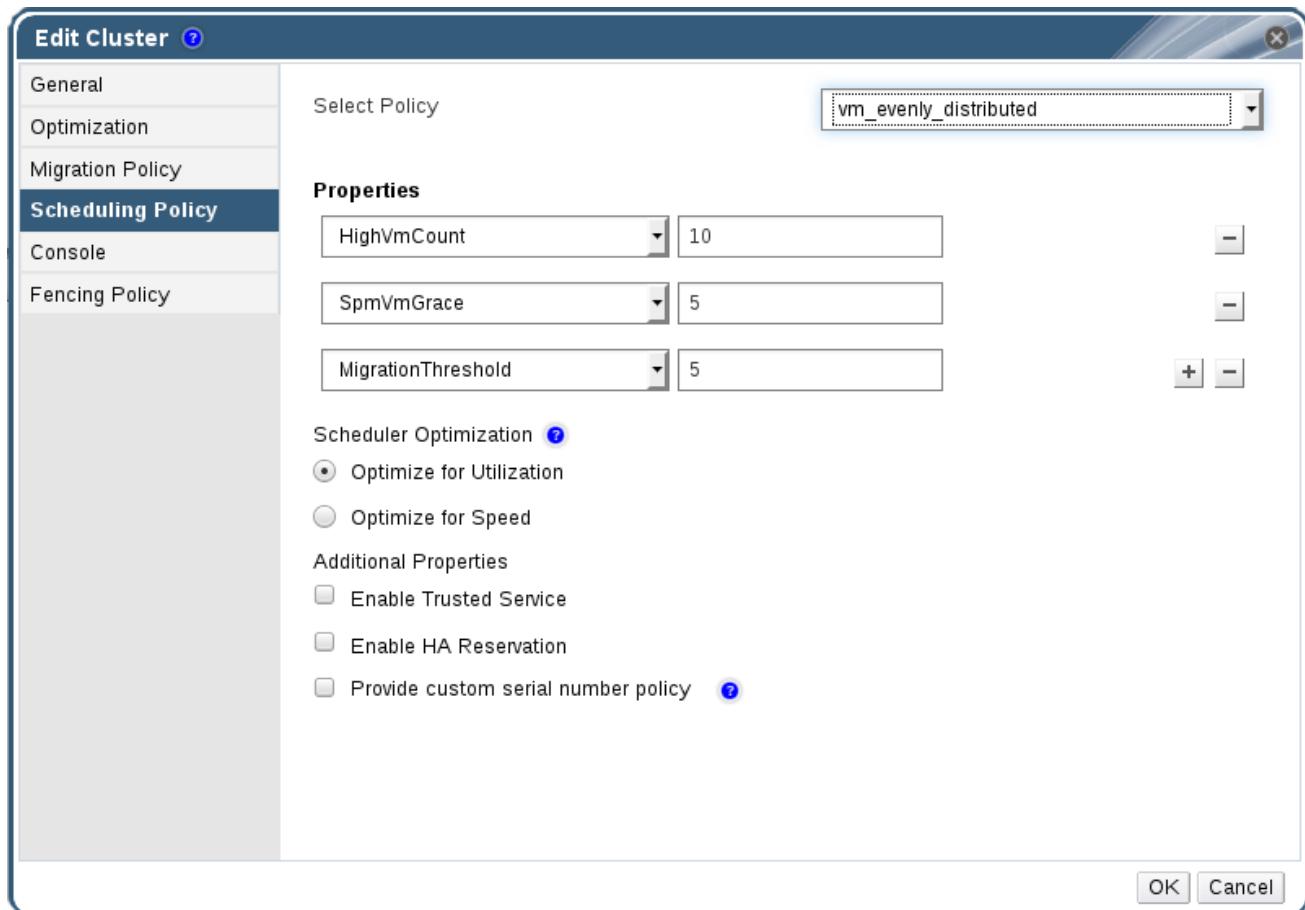
プロパティー	説明
自動コンバージション	<p>仮想マシンのライブマイグレーション中に自動コンバージェンスが使用されるかどうかを設定できます。負荷が大きいが大きい仮想マシンでは、ライブマイグレーション中に行われる転送速度よりも速くメモリーがダーティーなり、移行が収束できなくなります。QEMUの自動調整機能を使用すると、仮想マシン移行の収束を強制的に実行できます。QEMUは、コンバージェンスの欠如を自動的に検出し、仮想マシン上のvCPUのスロットルダウンをトリガります。オートコンバージェンスはデフォルトで無効になっています。</p> <ul style="list-style-type: none"> グローバルレベルで設定される自動収束設定を使用するには、Inherit from global setting を選択します。このオプションはデフォルトで選択されます。 Auto Converge を選択してグローバル設定を上書きし、仮想マシンの自動収束を許可します。 Don't Auto Converge を選択してグローバル設定を上書きし、仮想マシンの自動収束を防ぎます。
Enable migration compression	<p>このオプションを使用すると、仮想マシンのライブマイグレーション中に移行圧縮を使用するかどうかを設定できます。この機能は、Xor Binary Zero Run-Length-Encodingを使用して、メモリー書き込みを必要とするワークロードまたはスペースメモリー更新パターンを使用するアプリケーションに対して、仮想マシンのダウンタイムと合計移行時間を短縮します。移行圧縮は、デフォルトでは無効になっています。</p> <ul style="list-style-type: none"> グローバルレベルで設定される圧縮設定を使用するには、Inherit from global setting を選択します。このオプションはデフォルトで選択されます。 Compress を選択してグローバル設定を上書きし、仮想マシンの圧縮を許可します。 Don't compress を選択してグローバル設定を上書きし、仮想マシンの圧縮を防ぎます。

5.2.2.4. スケジューリングポリシー設定に関する説明

スケジューリングポリシーにより、利用可能なホスト間での仮想マシンの使用状況および分散を指定することができます。スケジューリングポリシーを定義して、クラスター内のホスト全体で自動負荷分散を有効にします。スケジューリングポリシーに関わらず、CPUが過負荷状態のホストでは仮想マシンが起動しません。デフォルトでは、ホストのCPUが5分間80%を超える負荷がかかった場合に過負荷であると見なされますが、この値はスケジューリングポリシーを使用して変更できます。スケジューリングポリシーの詳細情報は、「[スケジューリングポリシー](#)」を参照してください。

スケジューリングポリシーを既存クラスターに追加するには、Clusters タブをクリックし、Edit ボタンをクリックしてから Scheduling Policy タブをクリックします。

図5.3 スケジューリングポリシー設定 : vm_evenly_distributed



以下の表は、Scheduling Policy タブの設定について説明しています。

表5.7 スケジューリングポリシータブプロパティ

フィールド	説明/アクション
ポリシーの選択	<p>ドロップダウンリストからポリシーを選択します。</p> <ul style="list-style-type: none"> None: ポリシーの値を none に設定して、すでに実行中の仮想マシンのホスト間で負荷や電源を共有しないようにします。これはデフォルトのモードです。仮想マシンが起動すると、メモリーと CPU 処理の負荷がクラスター内の全ホストに均等に分散されます。ホストが定義された CpuOverCommitDurationMinutes、HighUtilization、または MaxFreeMemoryForOverUtilized に達した場合、ホストにアタッチされた追加の仮想マシンは起動しません。 evenly_distributed: メモリーおよび CPU 処理の負荷をクラスター内のすべてのホストで均等に分散します。ホストが定義された CpuOverCommitDurationMinutes、HighUtilization、または

フィールド	<p>MaxFreeMemoryForOverUtilized に達する場合、ホストにアタッチされた追加の仮想マシンは起動しません。</p> <ul style="list-style-type: none"> ● InClusterUpgrade: ホストオペレーティングシステムのバージョンに基づいて仮想マシンを分散します。現在実行している仮想マシンよりも新しいオペレーティングシステムを持つホストは、同じオペレーティングシステムを持つホストよりも優先されます。新しいオペレーティングシステムを持つホストに移行する仮想マシンは、古いオペレーティングシステムに移行されません。仮想マシンは、クラスター内の任意のホストで再起動できます。このポリシーにより、クラスターでオペレーティングシステムのバージョンが混在するようになります。クラスター内のホストをアップグレードできます。ポリシーを有効にする前に、前提条件を満たす必要があります。Red Hat Enterprise Virtualization 3.6 Upgrade Guide の Upgrading Hosts in a Cluster from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7 を参照してください。
プロパティー	<p>以下のプロパティーは選択したポリシーをもとに表示され、必要に応じて編集できます。</p> <ul style="list-style-type: none"> ● HighVmCount: 負荷分散を有効にするため



重要

InClusterUpgrade スケジューリングポリシーは、メジャー・バージョン間のアップグレードのみに使用されます。たとえば、Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 7 へのアップグレードは以下のようになります。

- **power_saving**: 利用可能なホストのサブセットにメモリーと CPU 処理の負荷を分散し、使用率の低いホストの電力消費を減らします。CPU 負荷が低稼働率の値を下回っている状態が定義された時間以上続いたホストは、すべての仮想マシンを他のホストに移行させ、電源を切れるようにします。ホストにアタッチされた追加の仮想マシンは、そのホストが定義された高使用率値に達した場合には起動しません。
- **vm_evenly_distributed**: 仮想マシンの数に基づいて、仮想マシンをホスト間で均等に分散します。**HighVmCount** よりも多くの仮想マシンを実行しているホストがあり、仮想マシン数を持つホストが **MigrationThreshold** の外にあるホストが 1つ以上ある場合、クラスターはアンバランスとみなされます。

プロパティー

以下のプロパティーは選択したポリシーをもとに表示され、必要に応じて編集できます。

- **HighVmCount**: 負荷分散を有効にするため

フィールド	説明/アクション
	<p>にホストごとに実行する必要のある仮想マシン数を設定します。デフォルト値は、1台のホストで仮想マシンを実行する10です。負荷分散は、少なくともHighVmCountが仮想マシンを実行するクラスターに1つ以上のホストがある場合のみ有効になります。</p> <ul style="list-style-type: none"> ● MigrationThreshold: 仮想マシンがホストから移行される前にバッファーを定義します。これは、最も高使用率の低いホストと最も使用率の低いホスト間の仮想マシン数の包含的な差異です。クラスターのすべてのホストが移行しきい値内に留まる仮想マシン数がある場合、クラスターが分散されます。デフォルト値は5です。 ● SpmVmGrace: SPMホストで予約される仮想マシンのスロット数を定義します。SPMホストの負荷は他のホストよりも低いため、この変数は、実行できる仮想マシンの数を他のホストよりも少なく定義します。デフォルト値は5です。 ● CpuOverCommitDurationMinutes: スケジューリングポリシーの実行前に、定義された使用率値以外のCPU負荷をホストが実行できる時間（分単位）を設定します。定義した時間間隔は、CPU負荷のスケジューリングポリシーで一時的な急増から保護し、不要な仮想マシンの移行を軽減します。最大2文字デフォルト値は2です。 ● HighUtilization: パーセンテージで表されます。定義された時間間隔で、ホストが使用率の高い値以上のCPU使用率で実行される場合、Red Hat Virtualization Managerは、ホストのCPU負荷が最大サービスしきい値を下回るまで、仮想マシンをクラスター内の他のホストに移行します。デフォルト値は80です。 ● LowUtilization: パーセンテージで表されます。定義された時間間隔で、ホストが使用率の低い値を下回る場合に、Red Hat Virtualization Managerは仮想マシンをクラスター内の他のホストに移行します。Managerは元のホストマシンの電源をオフにし、負荷分散が必要か、またはクラスターに空きホストが十分にない場合に再び再起動します。デフォルト値は20です。 ● Scaledown: ホストのスコアを指定された量で除算して、HA Reservation 加重関数の影響を減らします。これは、noneを含む、任意のポリシーに追加できる任意のプロパティです。 ● HostsInReserve: 実行中の仮想マシンがなくても実行し続けるホストの数を指定します。これは、power_savingポリシーに追加できる任意のプロパティです。 ● EnableAutomaticHostPowerManagement: クラスター内のすべてのホストの自動電源管理を有効にします。これ

フィールド	<p>は、power_saving ポリシーに追加できる 説明/アクションプロパティーです。デフォルト値は true です。</p> <ul style="list-style-type: none"> ● MaxFreeMemoryForOverUtilized: 最小サービスレベルに必要な最小空きメモリーを設定します(MB 単位)。ホストの使用可能なメモリーがこの値以下で実行される場合、Red Hat Virtualization Manager は、ホストで利用可能なメモリーが最小限のサービスしきい値を下回る間、仮想マシンをクラスター内の他のホストに移行します。MaxFreeMemoryForOverUtilized および MinFreeMemoryForUnderUtilized の両方を 0 MB に設定すると、メモリーベースのバランスングが無効になります。MaxFreeMemoryForOverUtilized が設定されている場合は、予期しない動作を回避するために MinFreeMemoryForUnderUtilized も設定する必要があります。これは、power_saving および evenly_distributed ポリシーに追加できる任意のプロパティーです。 ● MinFreeMemoryForUnderUtilized: ホストの使用率が低いと見なされる前に、最低限必要な空きメモリーを MB 単位で設定します。ホストの使用可能なメモリーがこの値を超えると、Red Hat Virtualization Manager は仮想マシンをクラスター内の他のホストに移行し、ホストマシンの電源を自動的に停止し、負荷分散が必要な場合や、クラスターに十分な空きホストがない場合に再起動します。MaxFreeMemoryForOverUtilized および MinFreeMemoryForUnderUtilized の両方を 0MB に設定すると、メモリーベースのバランスングが無効になります。MinFreeMemoryForUnderUtilized が設定されている場合は、予期しない動作を回避するために MaxFreeMemoryForOverUtilized も設定する必要があります。これは、power_saving および evenly_distributed ポリシーに追加できる任意のプロパティーです。
スケジューラーの最適化	<p>ホストの重み付け/順序のスケジューリングを最適化します。</p> <ul style="list-style-type: none"> ● Optimize for Utilization: スケジューリングに重みモジュールを追加して、最適な選択を可能にします。 ● Optimize for Speed: 保留中のリクエストが 10 個以上ある場合に、ホストの重みをスキップします。

フィールド	説明/アクション
信頼できるサービスの有効化	OpenAttestation サーバーとのインテグレーションを有効にします。これを有効にする前に、 engine-config ツールを使用して OpenAttestation サーバーの詳細を入力します。詳細は、「 信頼できるコンピュートプール 」を参照してください。
HA 予約の有効化	Manager が高可用性仮想マシンのクラスター容量を監視できるようにします。Manager は、既存のホストが予期せずに失敗した場合に移行するために、高可用性として指定された仮想マシンのクラスター内に適切な容量が存在することを確認します。
Provide custom serial number policy	<p>このチェックボックスを選択すると、クラスター内の仮想マシンのシリアル番号ポリシーを指定できます。以下のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> ● Host ID: ホストの UUID を仮想マシンのシリアル番号として設定します。 ● VM ID: 仮想マシンの UUID をシリアル番号として設定します。 ● Custom serial number: カスタムのシリアル番号を指定できます。

ホストの空きメモリーが 20% 未満になると、**mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580** のようなバルーンコマンドが `/var/log/vdsd/mom.log` に記録されます。`/var/log/vdsd/mom.log` は、Memory Overcommit Manager ログファイルです。

5.2.2.5. クラスターコンソール設定の説明

以下の表は、**New Cluster** および **Edit Cluster** ウィンドウの **Console** タブの設定について説明しています。

表5.8 コンソールの設定

フィールド	説明/アクション
クラスターの SPICE プロキシーの定義	このチェックボックスを選択し、グローバル設定で定義された SPICE プロキシーの上書きを有効にします。この機能は、ユーザー（ユーザーインターフェース経由で接続するなど）がハイパーバイザが存在するネットワーク外にある場合に役に立ちます。
SPICE プロキシーアドレスのオーバーライド	SPICE クライアントが仮想マシンに接続するプロキシー。アドレスは以下の形式でなければなりません。

`protocol://[host]:[port]`

5.2.2.6. フェンシングポリシー設定の説明

以下の表は、**New Cluster** および **Edit Cluster** ウィンドウの **Fencing Policy** タブの設定について説明しています。

表5.9 フェンシングポリシーの設定

フィールド	説明/アクション
フェンシングの有効化	クラスターのフェンシングを有効にします。フェンシングはデフォルトで有効になっていますが、必要に応じて無効にできます。たとえば、一時的なネットワークの問題が発生したり、予想される場合に、管理者は診断またはメンテナンスアクティビティーが完了するまでフェンシングを無効にできます。フェンシングが無効になっている場合は、応答しないホストで実行している高可用性仮想マシンは、別の場所で再起動されないことに注意してください。
ホストのストレージにライブリースがある場合はフェンシングをスキップ	このチェックボックスを選択しないと、Non Responsive のクラスター内のホストは、ストレージに接続されたホストはフェンスされません。
クラスター接続の問題のフェンシングをスキップ	このチェックボックスを選択すると、接続問題が発生しているクラスター内のホストのパーセンテージが定義された Threshold 以上になると、フェンシングが一時的に無効になります。 Threshold 値はドロップダウンリストから選択されます。利用可能な値は 25 、 50 、 75 、および 100 です。

5.2.3. リソースの編集

概要

リソースのプロパティを編集します。

手順5.2 リソースの編集

- リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
- Edit** をクリックして **Edit** ウィンドウを開きます。
- 必要なプロパティを変更し、**OK** をクリックします。

結果

新しいプロパティはリソースに保存されます。プロパティーフィールドが無効であれば、**Edit** ウィンドウは閉じません。

5.2.4. クラスター内のホストの負荷および電源管理ポリシーの設定

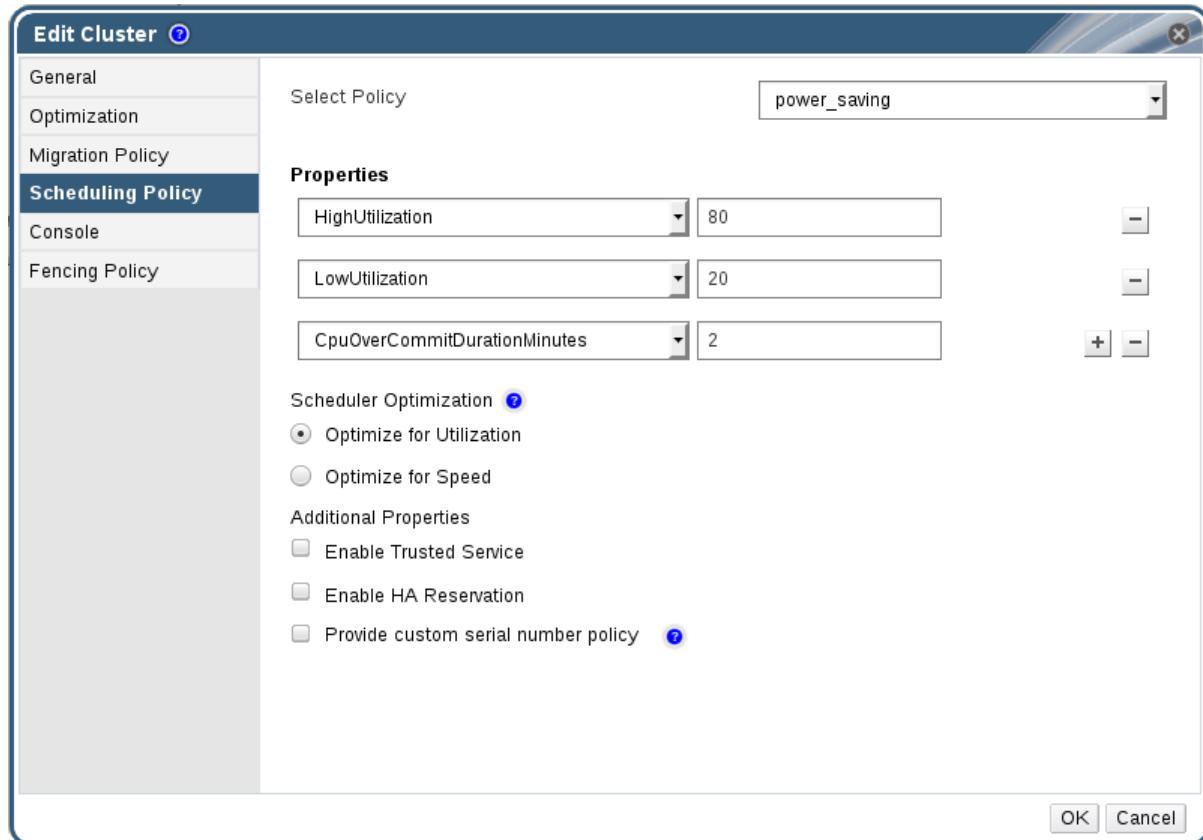
evenly_distributed および **power_saving** スケジューリングポリシーでは、受け入れ可能なメモリーと CPU 使用率の値、および仮想マシンを移行する必要があるポイントを指定できま

す。**vm_evenly_distributed** スケジューリングポリシーは、仮想マシンの数に基づいて、ホスト間で仮想マシンを均等に分散します。スケジューリングポリシーを定義して、クラスター内のホスト全体で自動負荷分散を有効にします。各スケジューリングポリシーの詳細は、「[スケジューリングポリシー設定に関する説明](#)」を参照してください。

手順5.3 ホストの負荷および電源管理ポリシーの設定

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. **Edit** をクリックして **Edit Cluster** ウィンドウを開きます。

図5.4 スケジューリングポリシーの編集



3. 以下のポリシーのいずれかを選択します。

- **none**
- **vm_evenly_distributed**
 - a. **HighVmCount** フィールドで負荷分散を有効にするために、少なくとも1台のホストで実行されている必要がある仮想マシンの最小数を設定します。
 - b. 最も使用率の高いホスト上の仮想マシン数と、**MigrationThreshold** フィールドで使用率の低いホストにある仮想マシン数との間の許容可能な最大差を定義します。
 - c. **SpmVmGrace** フィールドの SPM ホストで予約される仮想マシンのスロット数を定義します。
- **evenly_distributed**

- a. スケジューリングポリシーで **CpuOverCommitDurationMinutes** フィールドでアクションが実行される前に、定義された使用率値外でホストが CPU 負荷を実行できる時間（分単位）を設定します。
 - b. **HighUtilization** フィールドに、仮想マシンが他のホストへの移行を開始する CPU 使用率のパーセンテージを入力します。
 - c. **MinFreeMemoryForUnderUtilized** で、仮想マシンが他のホストへの移行を開始するのに必要な最小空きメモリーを MB 単位で入力します。
 - d. **MaxFreeMemoryForOverUtilized** で、仮想マシンが他のホストへの移行を開始するために必要な最大空きメモリーを MB 単位で入力します。
- **power_saving**
 - a. スケジューリングポリシーで **CpuOverCommitDurationMinutes** フィールドでアクションが実行される前に、定義された使用率値外でホストが CPU 負荷を実行できる時間（分単位）を設定します。
 - b. 以下の CPU 使用率の割合を入力します。このパーセンテージは、**LowUtilization** フィールドでホストの使用率が低いと見なされます。
 - c. **HighUtilization** フィールドに、仮想マシンが他のホストへの移行を開始する CPU 使用率のパーセンテージを入力します。
 - d. **MinFreeMemoryForUnderUtilized** で、仮想マシンが他のホストへの移行を開始するのに必要な最小空きメモリーを MB 単位で入力します。
 - e. **MaxFreeMemoryForOverUtilized** で、仮想マシンが他のホストへの移行を開始するために必要な最大空きメモリーを MB 単位で入力します。
4. クラスターの **Scheduler Optimization** として、以下のいずれかを選択します。
- **Optimize for Utilization** を選択し、スケジューリングに重みモジュールを追加して、最適な選択を可能にします。
 - **Optimize for Speed** を選択して、保留中のリクエストが 10 個以上ある場合にホストの重みをスキップします。
5. OpenAttestation サーバーを使用してホストを確認し、**engine-config** ツールを使用してサーバーの詳細を設定している場合は、**Enable Trusted Service** チェックボックスを選択します。
6. 必要に応じて、**Enable HA Reservation** チェックボックスを選択し、Manager が高可用性仮想マシンのクラスター容量を監視できるようにします。
7. オプションで **Provide custom serial number policy** チェックボックスを選択し、クラスター内の仮想マシンのシリアル番号ポリシーを指定し、以下のオプションのいずれかを選択します。
- **Host ID** を選択して、ホストの UUID を仮想マシンのシリアル番号として設定します。
 - **Vm ID** を選択して、仮想マシンの UUID をシリアル番号として設定します。
 - **Custom serial number** を選択し、テキストフィールドにカスタムのシリアル番号を指定します。
8. **OK** をクリックします。

5.2.5. クラスター内のホストでの MoM ポリシーの更新

Memory Overcommit Manager は、ホストのメモリーバルーンと KSM 機能を処理します。クラスター レベルでのこれらの機能への変更は、次回再起動またはメンテナنسモードでホストが **Up** のステータスに移行する場合にのみホストに渡されます。ただし、必要な場合は、ホストが **Up** 時に MoM ポリシーを同期することにより、重要な変更をホストをすぐに適用することができます。以下の手順は、各ホストで個別に実行する必要があります。

手順5.4 ホストでの MoM ポリシーの同期

1. **Clusters** タブをクリックして、ホストが属するクラスターを選択します。
2. 詳細ペインで **Hosts** タブをクリックし、更新された MoM ポリシーを必要とするホストを選択します。
3. **Sync MoM Policy** をクリックします。

ホストの MoM ポリシーは、ホストをメンテナансモードに移行し、をバックアップすることなく更新されます。

5.2.6. CPU プロファイル

CPU プロファイルは、クラスター内の仮想マシンが、実行しているホストでアクセスできる最大処理機能を定義します。これは、そのホストで利用可能な合計処理機能のパーセントで表されます。CPU プロファイルはデータセンターで定義された CPU プロファイルに基づいて作成され、クラスター内のすべての仮想マシンに自動的に適用されません。プロファイルを有効にするには、個々の仮想マシンに手動で割り当てる必要があります。

5.2.6.1. CPU プロファイルの作成

CPU プロファイルを作成します。この手順では、クラスターが属するデータセンターの下に1つ以上の CPU QoS エントリーがすでに定義されていることを前提としています。

手順5.5 CPU プロファイルの作成

1. **Clusters** resource タブをクリックし、クラスターを選択します。
2. 詳細ペインの **CPU プロファイル** サブタブをクリックします。
3. **New** をクリックします。
4. 名前 フィールドに CPU プロファイルの名前を入力します。
5. Description フィールドに、CPU プロファイルの **説明** を入力します。
6. **QoS** 一覧から CPU プロファイルに適用するサービスの品質を選択します。
7. **OK** をクリックします。

CPU プロファイルを作成し、その CPU プロファイルをクラスター内の仮想マシンに適用できる。

5.2.6.2. CPU プロファイルの削除

Red Hat Virtualization 環境から既存の CPU プロファイルを削除します。

手順5.6 CPU プロファイルの削除

1. **Clusters** resource タブをクリックし、クラスターを選択します。
2. 詳細ペインの **CPU プロファイル** サブタブをクリックします。
3. 削除する CPU プロファイルを選択します。
4. **削除** をクリックします。
5. **OK** をクリックします。

CPU プロファイルを削除し、その CPU プロファイルが利用できなくなりました。CPU プロファイルが仮想マシンに割り当てられている場合、それらの仮想マシンにはデフォルトの CPU プロファイルが自動的に割り当てられます。

5.2.7. 既存の Red Hat Gluster Storage クラスターのインポート

Red Hat Gluster Storage クラスターおよびクラスターに属するすべてのホストを Red Hat Virtualization Manager にインポートできます。

クラスター内のホストの IP アドレスまたはホスト名やパスワードなどの詳細を指定すると、SSH を介してそのホストで **gluster peer status** コマンドを実行すると、クラスターの一部であるホストの一覧が表示されます。各ホストのフィンガープリントを手動で検証し、パスワードを提供する必要があります。クラスター内のいずれかのホストが停止または到達できない場合、クラスターをインポートすることはできません。新規インポートされたホストに VDSM がインストールされていないため、ブートストラップスクリプトは、インポート後にホストに必要な VDSM パッケージをすべてインストールして再起動します。

手順5.7 既存の Red Hat Gluster Storage クラスターの Red Hat Virtualization Manager へのインポート

1. **Clusters** resource タブを選択して、結果一覧のすべてのクラスターを一覧表示します。
2. **New** をクリックして **New Cluster** ウィンドウを開きます。
3. ドロップダウンメニューから、クラスターが属する **データセンター** を選択します。
4. クラスターの **Name** および **Description** を入力します。
5. **Enable Gluster Service** ラジオボタンを選択し、**Import existing gluster configuration** チェックボックスを選択します。

Import existing gluster configuration フィールドは、**Enable Gluster Service** ラジオボタンを選択した場合にのみ表示されます。

6. **Address** フィールドに、クラスター内のサーバーのホスト名または IP アドレスを入力します。

ホスト **Fingerprint** が表示され、正しいホストに接続していることを確認します。ホストが到達不能な場合や、ネットワークエラーが発生した場合には、**Error in fetching fingerprint** のエラーが **Fingerprint** フィールドに表示されます。

7. サーバーの **Root パスワード** を入力し、**OK** をクリックします。
8. ホストの **追加** 画面が開き、クラスターの一部であるホストの一覧が表示されます。

9. 各ホストに **Name** および **Root Password** を入力します。
 10. すべてのホストに同じパスワードを使用する場合は、**Use a Common Password** チェックボックスを選択して、指定のテキストフィールドにパスワードを入力します。
- Apply** をクリックして、入力したパスワードをすべて設定します。
- フィンガープリントが有効であることを確認し、**OK** をクリックして変更を送信します。

ブートストラップスクリプトは、インポート後にホストに必要な VDSM パッケージをすべてインストールして再起動します。既存の Red Hat Gluster Storage クラスターを Red Hat Virtualization Manager に正常にインポートできるようになりました。

5.2.8. ホストウィンドウの追加設定の説明

ホストの **追加ウィンドウ** では、Gluster 対応クラスターの一部としてインポートされたホストの詳細を指定できます。このウィンドウは、**New Cluster** ウィンドウで **Enable Gluster Service** チェックボックスを選択し、必要なホストの詳細を指定すると表示されます。

表5.10 Gluster ホスト設定の追加

フィールド	説明
一般的なパスワードを使用します。	このチェックボックスにチェックマークを入れ、クラスターに属する全ホストに同じパスワードを使用します。パスワード フィールドにパスワードを入力し、 適用 ボタンをクリックしてすべてのホストにパスワードを設定します。
Name	ホストの名前を入力します。
ホスト名/IP	このフィールドには、 新規クラスター ウィンドウで指定したホストの完全修飾ドメイン名または IP が自動的に設定されます。
root パスワード	各ホストに異なる root パスワードを使用するには、このフィールドにパスワードを入力します。このフィールドは、クラスター内のすべてのホストに提供される共通のパスワードを上書きします。
Fingerprint	ホストのフィンガープリントが表示され、正しいホストに接続していることを確認します。このフィールドには、 新規クラスター ウィンドウで指定したホストのフィンガープリントが自動的に入力されます。

5.2.9. クラスターの削除

概要

クラスターを削除する前に、すべてのホストをクラスターから移動します。



注記

デフォルト クラスターは **Blank** テンプレートを保持するため、削除できません。ただし、**Default** クラスターの名前を変更し、新しいデータセンターに追加できます。

手順5.8 クラスターの削除

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. クラスターにホストがないことを確認します。
3. **Remove** をクリックして、**Remove Cluster (s)** 確認ウィンドウを開きます。
4. **OK** をクリックします。

結果

クラスターが削除されます。

5.2.10. クラスターの互換バージョンの変更

Red Hat Virtualization のクラスターには互換バージョンがあります。クラスターの互換バージョンは、そのクラスター内の全ホストがサポートする Red Hat Virtualization の機能を示します。クラスターの互換バージョンは、そのクラスター内で最も機能性の低いホストオペレーティングシステムのバージョンに応じて設定されます。



注記

クラスターの互換バージョンを変更するには、まず、クラスター内の全ホストを更新して、必要な互換性レベルをサポートするレベルにする必要があります。

クラスターのクラスター互換バージョンを更新したら、すべての実行中またはサスPEND中のすべての仮想マシンのクラスターの互換バージョンを更新し、変更が有効であることを確認する必要があります。これは、ゲストオペレーティングシステム内からではなく、Manager または REST API 呼び出し内から仮想マシンを再起動することで実現されます。仮想マシンは、再起動されるまで以前のクラスターの互換性レベルで引き続き実行されます。再起動が必要な仮想マシンには、**Next-Run** アイコン（感嘆符付き）のマークが付けられます。プレビュー中の仮想マシンスナップショットのクラスターの互換バージョンを変更することはできません。まずプレビューをコミットまたは元に戻す必要があります。

セルフホストエンジンの仮想マシンを再起動する必要はありません。セルフホストエンジン環境のアップグレードに関する詳細は、『セルフホストエンジンガイド』の [メンテナーンスおよびリソース](#) のアップグレードを参照してください。

手順5.9 クラスターの互換バージョンの変更

1. 管理ポータルで、**Clusters** タブをクリックします。
2. 表示される一覧から変更するクラスターを選択します。
3. **Edit** をクリックします。
4. **互換バージョン** を必要な値に変更します。
5. **OK** をクリックして、**Change Cluster Compatibility Version** の確認ウィンドウを開きます。

6. **OK** をクリックして確定します。

クラスターの互換バージョンを更新しました。データセンター内の全クラスターの互換バージョンを更新したら、データセンター自体の互換性バージョンを変更できます。



重要

互換性をアップグレードすると、データセンターに属するすべてのストレージドメインもアップグレードされます。

5.3. クラスターおよびパーティション

5.3.1. クラスターのシステムパーティションの管理

システム管理者は **SuperUser** として、管理ポータルのすべての側面を管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限された管理者ロールは、特定のリソースに制限される管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、そのデータセンターのストレージを除く、割り当てられたデータセンターの管理者権限のみを持ち、**ClusterAdmin** は割り当てられたクラスターに対してのみ管理者権限を持ちます。

クラスター管理者は、特定のデータセンターのみのシステム管理ロールです。これは、複数のクラスターを持つデータセンターで、各クラスターにシステム管理者が必要な場合に有効です。**ClusterAdmin** ロールは階層モデルです。クラスターのクラスター管理者ロールを割り当てられたユーザーは、クラスター内のすべてのオブジェクトを管理できます。ヘッダーバーの **Configure** ボタンを使用して、環境内のすべてのクラスターにクラスター管理者を割り当てます。

クラスター管理者ロールは以下のアクションを許可します。

- 関連付けられたクラスターの作成および削除。
- クラスターに関連付けられたホスト、仮想マシン、およびプールの追加および削除。
- クラスターに関連付けられた仮想マシンのユーザーパーティションを編集します。



注記

ロールやパーティションは、既存のユーザーにのみ割り当てることができます。

また、既存のシステム管理者を削除し、新しいシステム管理者を追加すると、クラスターのシステム管理者を変更できます。

5.3.2. クラスター管理者ロールの概要

クラスターパーティションロール

以下の表は、クラスターの管理に適用される管理者ロールおよび権限について説明しています。

表5.11 Red Hat Virtualization システム管理者ロール

ロール	権限	注記
-----	----	----

ロール	権限	注記
ClusterAdmin	クラスター管理者	<p>ホスト、テンプレート、および仮想マシンなど、特定のクラスター内の物理リソースおよび仮想リソースをすべて使用、作成、削除、管理することができます。</p> <p>ディスプレイネットワークの指定や、ネットワークを必須とマークするなど、クラスター内でネットワークプロパティを設定できます。</p> <p>ただし、ClusterAdmin には、ネットワークをクラスターにアタッチまたはデタッチするパーミッションがないため、NetworkAdmin パーミッションが必要になります。</p>
NetworkAdmin	ネットワーク管理者	特定のクラスターのネットワークを設定および管理できます。クラスターのネットワーク管理者は、データセンター内のクラスターネットワークパーミッションも継承します。

5.3.3. 管理者またはユーザーロールのリソースへの割り当て

管理者またはユーザーロールをリソースに割り当て、ユーザーがそのリソースにアクセスしたり、管理したりできるようにします。

手順5.10 リソースへのロールの割り当て

- リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
- 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
- Add** をクリックします。
- Search** テキストボックスに既存ユーザーの名前またはユーザー名を入力し、**Go** をクリックします。表示された候補の中からユーザーを選択します。
- Role to Assign:** ドロップダウンリストからロールを選択します。
- OK** をクリックします。

ユーザーにロールを割り当てました。そのリソースで有効にしたそのロールの継承されたパーミッションが、ユーザーに付与されました。

5.3.4. リソースからの管理者またはユーザーロールの削除

管理者またはユーザーのロールをリソースから削除すると、ユーザーはそのリソースのロールに関連付けられ継承されたパーミッションを失います。

手順5.11 リソースからのロールの削除

1. リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
2. 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
3. リソースから削除するユーザーを選択します。
4. **Remove** をクリックします。 **Remove Permission** 画面が開き、パーミッションの削除を確認します。
5. **OK** をクリックします。

ユーザーのロールおよび関連付けられたパーミッションをリソースから削除しました。

第6章 論理ネットワーク

6.1. 論理ネットワークタスク

6.1.1. ネットワークタブの使用

Networks resource タブは、ユーザーが論理ネットワーク関連の操作を実行し、各ネットワークのプロパティーや他のリソースとの関連付けに基づいて論理ネットワークを検索するための一元的な場所を提供します。

Red Hat Virtualization 環境のすべての論理ネットワークは、ネットワーク タブの結果一覧に表示されます。New、Edit、Remove ボタンを使用すると、データセンター内の論理ネットワークの作成、プロパティーの変更、および削除を行うことができます。

各ネットワーク名をクリックし、詳細ペインの **Clusters** タブ、**Hosts** タブ、**Virtual Machines** タブ、**Templates** タブ、および **Permissions** タブを使用して、以下のような機能を実行します。

- クラスターやホストにネットワークを割り当てまたは割り当て解除する
- 仮想マシンやテンプレートからネットワークインターフェイスを削除する
- ネットワークへのアクセスや管理を行うユーザーの権限を追加、削除する

これらの機能は、各リソースタブからもアクセスできます。



制限

データセンターやクラスターでは、ホストが動作している場合にはネットワークを変更しないでください。ホストに到達できなくなる危険性があります。



重要

Red Hat Virtualization ノードを使用してサービスを提供する予定の場合には、Red Hat Virtualization 環境が動作を停止すると、そのサービスが停止することに注意してください。

これはすべてのサービスに当てはまりますが、特に Red Hat Virtualization 上で以下を実行した場合の危険性に注意する必要があります。

- ディレクトリーサービス
- DNS
- ストレージ

6.1.2. データセンターまたはクラスターでの新しい論理ネットワークの作成

論理ネットワークを作成し、データセンターやデータセンター内のクラスターでの使用を定義します。

手順6.1 データセンターまたはクラスターでの新しい論理ネットワークの作成

1. **Data Centers** または **Clusters** リソースタブをクリックし、結果一覧でデータセンターまたはクラスターを選択します。
2. 詳細ペインの **Logical Networks** タブをクリックして、既存の論理ネットワークを一覧表示します。
3.
 - **Data Centers** の詳細ペインから **New** をクリックし、**New Logical Network** ウィンドウを開きます。
 - **Clusters** の詳細ペインで **Add Network** をクリックし、**New Logical Network** ウィンドウを開きます。
4. 論理ネットワークの **Name**、**Description**、および **Comment** を入力します。
5. オプションで、**Create on external provider** チェックボックスを選択します。ドロップダウンリストから **External Provider** を選択し、**Physical Network** の IP アドレスを指定します。**External Provider** ドロップダウンリストには、外部プロバイダーが読み取り専用モードで一覧表示されません。
外部プロバイダーで **Create** を選択すると、**Network Label**、**VM Network**、および **MTU** オプションが無効になります。
6. **Network Label** テキストフィールドに、論理ネットワークの新しいラベルを入力するか、既存のラベルを選択します。
7. 必要に応じて、**Enable VLAN tagging** を有効にします。
8. 必要に応じて、**VM Network** を無効にします。
9. **MTU** 値を **Default (1500)** または **Custom** に設定します。
10. **Cluster** タブで、ネットワークを割り当てるクラスターを選択します。また、論理ネットワークを必須ネットワークにするかどうかも指定できます。
11. 外部プロバイダーで **Create** を選択すると、サブネットタブが表示されます。サブネットタブで **サブネットの作成** を選択し、名前、**CIDR**、および **ゲートウェイアドレス**を入力し、論理ネットワークが提供するサブネットの **IP バージョン** を選択します。また、必要に応じて DNS サーバーを追加することもできます。
12. **vNIC Profiles** タブから、必要に応じて vNIC プロファイルを論理ネットワークに追加します。
13. **OK** をクリックします。

データセンター内のクラスターまたはクラスターに必要なリソースとして論理ネットワークを定義している。論理ネットワークのラベルを入力すると、そのラベルの付いたすべてのホストネットワークインターフェイスに自動的に追加されます。



注記

新しい論理ネットワークを作成したり、ディスプレイネットワークとして使用されている既存の論理ネットワークに変更を加えたりする場合には、そのネットワークを使用する、稼働中の仮想マシンは、ネットワークが使用可能になる前、または変更が適用される前に、再起動する必要があります。

6.1.3. 論理ネットワークの編集

論理ネットワークの設定を編集します。

手順6.2 論理ネットワークの編集



重要

ホスト上のネットワーク設定と同期していない場合には、論理ネットワークの編集や他のインターフェイスへの移動はできません。ネットワークの同期方法については、「[ホストのネットワークインターフェイスの編集とホストへの論理ネットワークの割り当て](#)」を参照してください。

1. **Data Centers** resource タブをクリックし、結果一覧で論理ネットワークのデータセンターを選択します。
2. 詳細ペインの **Logical Networks** タブをクリックして、データセンター内の論理ネットワークを一覧表示します。
3. 論理ネットワークを選択し、**編集** をクリックして論理ネットワークの **編集 ウィンドウ**を開きます。
4. 必要な設定を編集します。



注記

デフォルトのネットワーク除き、新規または既存のネットワークの名前は、仮想マシンを停止することなく編集することができます。

5. **OK** をクリックして変更を保存します。



注記

マルチホストネットワーク設定では、更新されたネットワーク設定を、ネットワークが割り当てられたデータセンター内のすべてのホストに自動適用します。変更は、ネットワークを使用する仮想マシンが停止しているときにのみ適用されます。すでにホストに設定されている論理ネットワークの名前は変更できません。**VM Network** オプションは、そのネットワークを使用する仮想マシンまたはテンプレートの実行中に無効にすることはできません。

6.1.4. 論理ネットワークの削除

Networks resource タブまたは **Data Centers** リソースタブから論理ネットワークを削除できます。以下の手順では、データセンターに関連付けられた論理ネットワークを削除する方法を説明します。稼働中の Red Hat Virtualization 環境には、**ovirtmgmt** 管理ネットワークとして少なくとも1つの論理ネットワークを使用する必要があります。

手順6.3 論理ネットワークの削除

1. **Data Centers** resource タブをクリックし、結果一覧で論理ネットワークのデータセンターを選択します。
2. 詳細ペインの **Logical Networks** タブをクリックして、データセンター内の論理ネットワークを一覧表示します。

3. 論理ネットワークを選択し、**Remove** をクリックして、**Remove Logical Network (s)** ウィンドウを開きます。
4. オプションで、**Remove external network (s) from the provider (s) well** チェックボックスを選択し、ネットワークが外部プロバイダーによって提供されている場合は Manager と外部プロバイダーの両方から論理ネットワークを削除します。外部プロバイダーが読み取り専用モードの場合、チェックボックスはグレーアウトされます。
5. **OK** をクリックします。

論理ネットワークが Manager から削除され、利用できなくなります。

6.1.5. 論理ネットワークのゲートウェイの表示と編集

論理ネットワークのゲートウェイ、IP アドレス、サブネットマスクを定義できます。これは、ホスト上に複数のネットワークが存在し、トラフィックがデフォルトゲートウェイではなく、指定したネットワークを経由しなければならない場合に必要です。

ホストに複数のネットワークが存在し、ゲートウェイが定義されていない場合には、リターントラフィックはデフォルトゲートウェイを経由することになり、意図した宛先に到達しない可能性があります。これにより、ユーザーがホストに対して ping を実行できなくなります。

Red Hat Virtualization は、インターフェイスがアップダウンするたびに、複数のゲートウェイを自動的に処理します。

手順6.4 論理ネットワークのゲートウェイの表示と編集

1. **Hosts** resource タブをクリックし、目的のホストを選択します。
2. 詳細ペインの **ネットワークインターフェイス** タブをクリックして、ホストに接続されているネットワークインターフェイスとその設定を一覧表示します。
3. **Setup Host Networks** ボタンをクリックして **Setup Host Networks** ウィンドウを開きます。
4. 割り当てられた論理ネットワークにカーソルを合わせ、鉛筆アイコンをクリックして **Edit Management Network** ウィンドウを開きます。

Edit Management Network ウィンドウには、ネットワーク名、ブートプロトコル、IP、サブネットマスク、ゲートウェイアドレスが表示されます。アドレス情報は、**静的** ブートプロトコルを選択して手動で編集できます。

6.1.6. 新しい論理ネットワークおよび論理ネットワークの編集ウィンドウの設定とコントロールの説明

6.1.6.1. 論理ネットワーク一般設定の説明

以下の表は、**New Logical Network** および **Edit Logical Network** ウィンドウの **General** タブの設定について説明しています。

表6.1新しい論理ネットワークと論理ネットワーク設定の編集

フィールド名	説明

フィールド名	説明
Name	論理ネットワークの名前。このテキストフィールドには15文字の制限があり、大文字、小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。
説明	論理ネットワークの説明。このテキストフィールドには40文字の制限があります。
Comment	論理ネットワークに関するプレーンテキストの人間が読めるコメントを追加するためのフィールド。
外部プロバイダーでの作成	外部プロバイダーとしてManagerに追加されたOpenStack Networkingインスタンスへの論理ネットワークを作成できます。 外部プロバイダー: 論理ネットワークが作成される外部プロバイダーを選択できます。
VLAN タグの有効化	VLANタグは、論理ネットワークで传送されるすべてのネットワークトラフィックに特別な特性を与えるセキュリティー機能です。VLANタグ付きのトラフィックは、その特性のないインターフェイスでは読み取れません。また、論理ネットワークにVLANを使用すると、1つのネットワークインターフェイスに、VLANタグが異なる論理ネットワークを複数、関連付けることができます。VLANタグ付けが有効な場合は、テキストエントリーフィールドに数値を入力します。
VM ネットワーク	仮想マシンのみがこのネットワークを使用する場合は、このオプションを選択します。ストレージの通信など、仮想マシンを介さないトラフィックにネットワークを使用する場合は、このチェックボックスを選択しないでください。
MTU	最大伝送単位(MTU)を括弧()で指定された値に設定するデフォルトのいずれかを選択するか、論理ネットワークのカスタムMTUを設定します。これを用いて、新しい論理ネットワークがサポートするMTUを、そのネットワークがインターフェイスするハードウェアがサポートするMTUに合わせることができます。カスタムが選択されている場合は、テキスト入力フィールドに数値を入力します。
ネットワークラベル	ネットワークの新しいラベルを指定したり、ホストネットワークインターフェイスに既に取り付けられている既存のラベルを選択したりすることができます。既存のラベルを選択した場合には、そのラベルが指定されたすべてのホストネットワークインターフェイスに論理ネットワークが自動的に割り当てられます。

6.1.6.2. 論理ネットワーククラスターの設定の説明

以下の表は、New Logical Network ウィンドウの Cluster タブの設定について説明しています。

表6.2新しい論理ネットワーク 設定

フィールド名	説明
クラスターへのネットワークの接続/クラスターからのネットワークの切断	<p>論理ネットワークをデータセンター内のクラスターにアタッチまたはデタッチでき、論理ネットワークを個々のクラスターに必要なネットワークとするかどうかを指定することができます。</p> <p>name: 設定が適用されるクラスターの名前。この値は編集できません</p> <p>Attach All - 論理ネットワークをデータセンター内のすべてのクラスターにアタッチまたはデタッチできます。または、各クラスターの名前の横にある Attach チェックボックスを選択または選択解除して、論理ネットワークを特定のクラスターにアタッチまたはデタッチします。</p> <p>Required All - 論理ネットワークがすべてのクラスターに必要なネットワークであるかどうかを指定できます。または、各クラスターの名前の横にある Required チェックボックスを選択または選択解除して、論理ネットワークが特定のクラスターに必要なネットワークであるかどうかを指定します。</p>

6.1.6.3. 論理ネットワークの vNIC プロファイル設定の説明

以下の表は、New Logical Network ウィンドウの vNIC Profiles タブの設定について説明しています。

表6.3新しい論理ネットワーク 設定

フィールド名	説明
vNIC Profiles	<p>論理ネットワークの1つまたは複数の vNIC プロファイルを指定できます。vNIC プロファイルの横にあるプラスボタンまたはマイナスボタンをクリックして、vNIC プロファイルを論理ネットワークに追加したり、論理ネットワークから削除したりすることができます。最初のフィールドでは、vNIC プロファイルの名前を入力します。</p> <p>public - プロファイルをすべてのユーザーが利用できるようにするかどうかを指定できます。</p> <p>QoS - vNIC プロファイルにネットワーク QoS (Quality of Service) プロファイルを指定できます。</p>

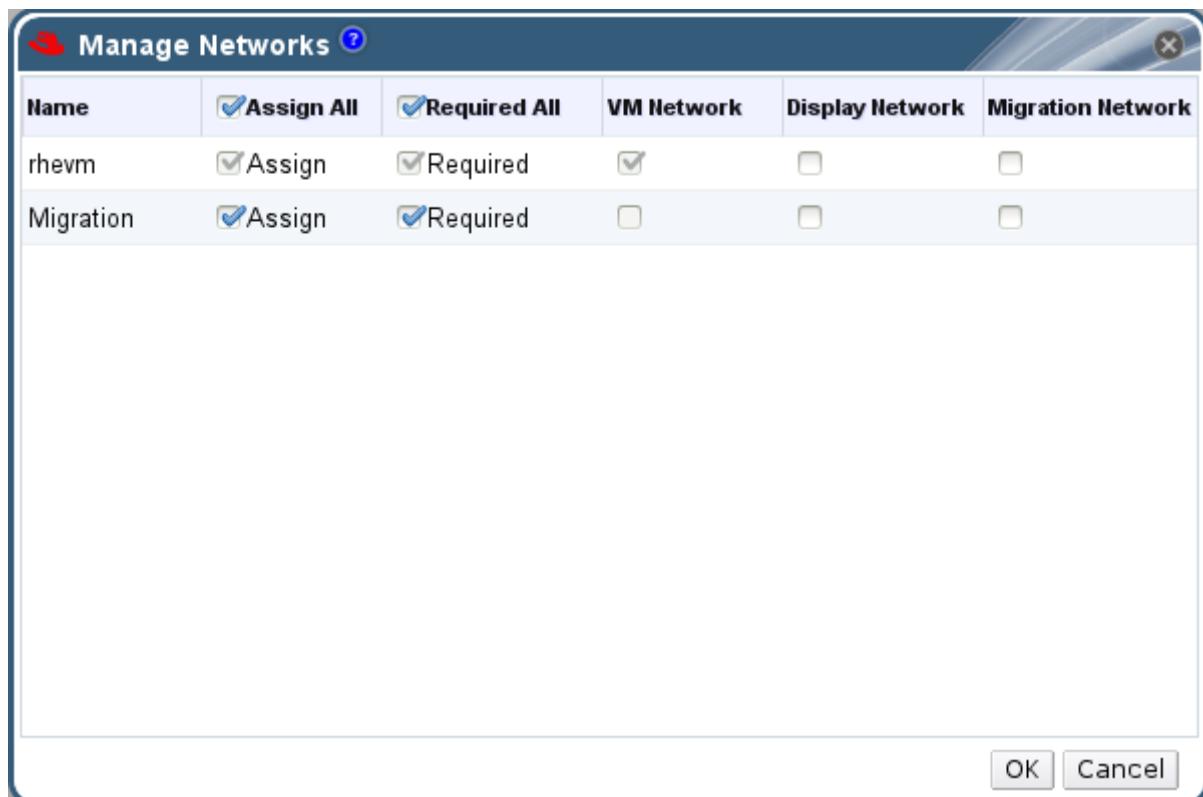
6.1.7. ネットワークの管理ウィンドウでの論理ネットワークに対する特定のトラフィックタイプの指定

ネットワークのトラフィックフローを最適化するために、論理ネットワークのトラフィックタイプを指定します。

手順6.5 論理ネットワークのトラフィックタイプの指定

1. **Clusters** resource タブをクリックし、結果リストからクラスターを選択します。
2. 詳細ペインの **Logical Networks** タブを選択して、クラスターに割り当てられた論理ネットワークを一覧表示します。
3. **Manage Networks** をクリックして、**Manage Networks** ウィンドウを開きます。

図6.1 ネットワークの管理



4. 適切なチェックボックスを選択します。
5. **OK** をクリックして変更を保存し、ウィンドウを閉じます。

特定のタイプのトラフィックを特定の論理ネットワークで伝送するように割り当てて、ネットワークトラフィックのフローを最適化している。



注記

外部のプロバイダーが提供する論理ネットワークは、仮想マシンのネットワークとして使用する必要があり、表示や移行などの特別なクラスターのロールを割り当てることはできません。

6.1.8. ネットワーク管理画面での設定内容の説明

以下の表は、**Manage Networks** ウィンドウの設定について説明しています。

表6.4 ネットワーク設定の管理

フィールド	説明/アクション
Assign	クラスター内の全ホストへの論理ネットワークの割り当てます。
必須。	Required (必須) と表示されたネットワークは、そのネットワークに関連するホストを正しく機能させるには、常に稼働している必要があります。必要なネットワークが機能しなくなると、そのネットワークに関連するホストはすべて動作しなくなります。
VM ネットワーク	VM ネットワークとマークされている論理ネットワークは、仮想マシンのネットワークに関連するネットワークトラフィックを伝送します。
ディスプレイネットワーク	ディスプレイネットワークとマークされた論理ネットワークは、SPICE と仮想ネットワークコントローラーに関連するネットワークトラフィックを伝送します。
移行ネットワーク	Migration Network とマークされた論理ネットワークは、仮想マシンとストレージの移行トラフィックを伝送します。

6.1.9. NIC の仮想機能設定の編集

Single Root I/O Virtualization (SR-IOV) では、単一の PCIe エンドポイントを複数の個別デバイスとして使用できるようになります。これは、物理機能 (PF) と仮想機能 (VF) の 2 つの PCIe 機能を導入することで実現されます。PCIe カードには 1~8 個の PF を含めることができますが、PF ごとにさらに多くの VF をサポートできます (デバイスによって異なります)。

各 NIC の VF の数を含め、Red Hat Virtualization Manager を介して SR-IOV 対応のネットワークインターフェイスコントローラー (NIC) の設定を編集し、VF へのアクセスを許可する仮想ネットワークを指定できます。

VF が作成されると、それぞれをスタンドアロンの NIC として扱うことができます。これには、1つ以上の論理ネットワークを割り当てる事、論理ネットワークとの結合インターフェイスを作成すること、および直接デバイスパススルーフォリオのため vNIC を論理ネットワークに直接割り当てることが含まれます。

VF に直接接続するには、vNIC プロパティーを有効にする必要があります。『vNIC プロファイルでのパススルーフォリオの有効化』を参照してください。

手順6.6 NIC の仮想機能設定の編集

- SR-IOV 対応ホストを選択し、詳細ペインで **ネットワークインターフェイス** タブをクリックします。
- Setup Host Networks** をクリックして **Setup Host Networks** ウィンドウを開きます。



3. SR-IOV 対応 NIC (SR-IOV が付いている)を選択し、鉛筆アイコンをクリックして **NICの Edit Virtual Functions (SR-IOV)**設定を開きます。
4. 仮想機能の数を編集するには、**Number of VFs setting** ドロップダウンボタンをクリックし、**Number of VFs** テキストフィールドを編集します。



重要

VF の数を変更すると、新しい VF を作成する前に、ネットワークインターフェイス上の以前の VF がすべて削除されます。これには、仮想マシンが直接接続されている VF が含まれます。

5. **All Networks** チェックボックスがデフォルトで選択され、すべてのネットワークが Virtual Function にアクセスできるようになります。Virtual Function へのアクセスを許可する仮想ネットワークを指定するには、Specified networks ラジオボタンを選択して、すべてのネットワークを一覧表示します。次に、任意のネットワークのチェックボックスを選択するか、**Labels** テキストフィールドを使用して1つ以上のネットワークラベルに基づいてネットワークを自動的に選択できます。
6. **OK** をクリックしてウィンドウを閉じます。Setup Host Networks ウィンドウの **OK** ボタンをクリックするまで、設定の変更は反映されません。

6.2. 仮想ネットワークインターフェイスカード

6.2.1. vNIC プロファイルの概要

仮想インターフェイスカード(vNIC)プロファイルは、Manager の個別の仮想ネットワークインターフェイスカードに適用できる設定のコレクションです。vNIC プロファイルを使用すると、ネットワーク QoS プロファイルの vNIC への適用、ポートミラーリングの有効化または無効化、カスタムプロパティーの追加または削除を行うことができます。また、vNIC プロファイルは、特定のユーザーにこれらのプロファイルを使用（消費）できるパーティションで、管理柔軟性を強化することもできます。このようにして、異なるユーザーが特定のネットワークから受けるサービスの質を制御できます。

6.2.2. vNIC プロファイルの作成と編集

Virtual Network Interface Controller (vNIC) のプロファイルを作成または編集して、ユーザーやグループのネットワーク帯域幅を調整できます。



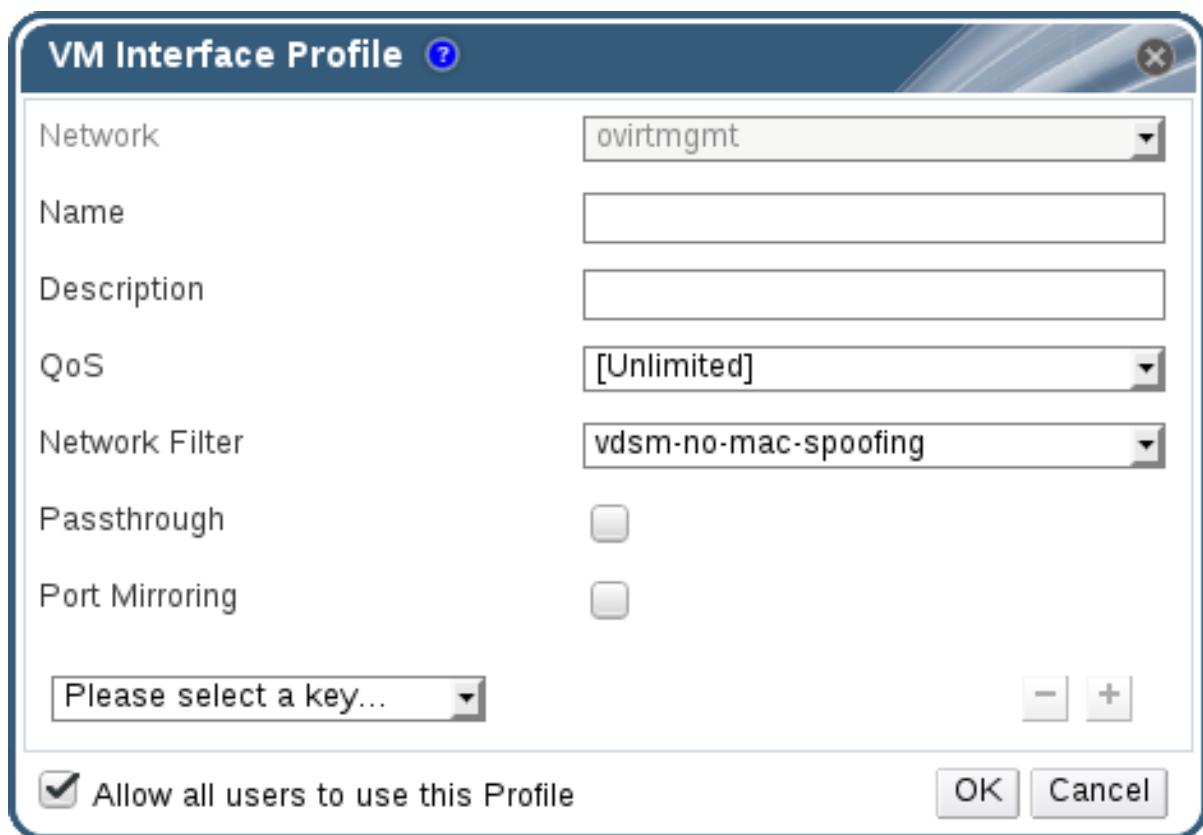
注記

ポートミラーリングを有効または無効にする場合には、編集する前に、関連するプロファイルを使用しているすべての仮想マシンがダウン状態になっている必要があります。

手順6.7 vNIC プロファイルの作成または編集

1. **Networks** resource タブをクリックし、結果一覧で論理ネットワークを選択します。
2. 詳細ペインで **vNIC Profiles** タブを選択します。ツリーモードで論理ネットワークを選択した場合は、結果一覧で **vNIC Profiles** タブを選択できます。
3. **New** または **Edit** をクリックして、**VM Interface Profile** ウィンドウを開きます。

図6.2 VM Interface Profile ウィンドウ



4. プロファイルの **Name** および **Description** を入力します。
5. **QoS** 一覧から該当する Quality of Service ポリシーを選択します。
6. ドロップダウンリストから **ネットワークフィルター** を選択して、仮想マシンとの間のネットワークパケットのトラフィックを管理します。ネットワークフィルターの詳細は、『Red Hat Enterprise Linux Virtualization Deployment and Administration Guide』の [Applying network filtering](#) を参照してください。
7. パススルー チェックボックスを選択して、vNIC のパススルーを有効にし、仮想機能を直接デバイス割り当てできるようにします。パススルーのプロパティーを有効にすると、QoS、ネットワークフィルタリング、ポートミラーリングに互換性がないため、これらが無効になります。パススルーの詳細は、[「vNIC プロファイルでのパススルーの有効化」](#) を参照してください。
8. **Port Mirroring** および **Allow all users to use this Profile** チェックボックスを使用して、これらのオプションを切り替えます。
9. カスタムプロパティーリストからカスタムプロパティーを選択すると、デフォルトで **Please select a key...** が表示されます。+ ボタンおよび - ボタンを使用して、カスタムプロパティーを追加または削除します。
10. **OK** をクリックします。

vNIC プロファイルを作成している。このプロファイルをユーザーやグループに適用して、ネットワークの帯域幅を調整します。vNIC プロファイルを編集した場合は、仮想マシンを再起動するか、ホットアンプラグしてから vNIC をホットプラグする必要があります。



注記

ゲストオペレーティングシステムは、vNIC ホットプラグとホットアンプラグをサポートしている必要があります。

6.2.3. VM インターフェイスプロファイルウィンドウの設定内容の説明

表6.5 VM インターフェイスプロファイルウィンドウ

フィールド名	説明
ネットワーク	vNIC プロファイルの適用先の利用可能なネットワークのドロップダウンリストです。
Name	vNIC プロファイルの名前。これは、1から 50 文字までの大文字と小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。
説明	vNIC プロファイルの説明。このフィールドは推奨されますが、必須ではありません。
QoS	vNIC プロファイルに適用する、利用可能な Network Quality of Service ポリシーのドロップダウンリストです。QoS ポリシーは、vNIC のインバウンドおよびアウトバウンドのネットワークトラフィックを規制します。
ネットワークフィルター	vNIC プロファイルに適用するネットワークフィルターのドロップダウンリストです。ネットワークフィルターは、仮想マシンとの間で送信可能なパケットの種類をフィルタリングして、ネットワークセキュリティーを向上させます。デフォルトのフィルターは、 vdsm-no-mac-spoofing で no-mac-spoofing と no-arp-mac-spoofing を組み合わせたものです。libvirt が提供するネットワークフィルターの詳細は、『Red Hat Enterprise Linux Virtualization Deployment and Administration Guide』の Pre-existing network filters セクションを参照してください。 <no Network Filter> は、仮想マシンの VLAN およびボンドに使用する必要があります。信頼できる仮想マシンでネットワークフィルターを使用しない場合には、パフォーマンスが向上します。
passthrough	パススルーのプロパティを切り替えるためのチェックボックス。パススルーでは、vNIC がホスト NIC の仮想機能に直接接続できるようになります。vNIC プロファイルが仮想マシンにアタッチされている場合には、パススルーのプロパティーは編集できません。 パススルーを有効にすると、vNIC プロファイルで QoS、ネットワークフィルター、ポートミラーリングが無効になります。

フィールド名	説明
Port Mirroring	ポートミラーリングを切り替えるためのチェックボックスです。ポートミラーリングは、論理ネットワーク上のレイヤー3のネットワークトラフィックを、仮想マシン上の仮想インターフェイスにコピーします。デフォルトでは選択されていません。詳細は、『Technical Reference』の Port Mirroring を参照してください。
Device Custom Properties	vNIC プロファイルに適用する利用可能なカスタムプロパティーを選択するためのドロップダウンメニューです。+ ボタンおよび- ボタンを使用してプロパティーをそれぞれ追加および削除します。
Allow all users to use this Profile	環境内の全ユーザーがプロファイルを利用できるかどうかを切り替えるためのチェックボックスです。これはデフォルトで選択されます。

6.2.4. vNIC プロファイルでのパススルーの有効化

vNIC プロファイルのパススルーのプロパティーを使用すると、SR-IOV 対応 NIC の仮想機能 (VF) に vNIC を直接接続できるようになります。次に、vNIC はソフトウェアによるネットワーク仮想化をバイパスして、VF に直接接続してデバイスを割り当てます。

vNIC プロファイルがすでに vNIC にアタッチされている場合、パススループロパティーは有効にできません。この手順では、これを避けるために新しいプロファイルを作成します。vNIC プロファイルでパススルーが有効になっている場合は、プロファイルの QoS およびポートミラーリングが無効になります。

SR-IOV、直接デバイスの割り当て、および Red Hat Virtualization でのこれらの実装に関するハードウェアの考慮事項は、[Hardware Considerations for Implementing SR-IOV](#) を参照してください。

手順6.8 パススルーの有効化

1. **Networks** results 一覧から論理ネットワークを選択し、詳細ペインの **vNIC Profiles** タブをクリックして、その論理ネットワークのすべての vNIC プロファイルを一覧表示します。
2. **New** をクリックして、**VM Interface Profile** ウィンドウを開きます。
3. プロファイルの **Name** および **Description** を入力します。
4. **Passthrough** チェックボックスを選択します。これにより、**QoS** および **ポートミラーリング** が無効になります。
5. 必要に応じて、カスタムプロパティーリストからカスタムプロパティーを選択すると、デフォルトで **Please select a key...** が表示されます。+ ボタンおよび- ボタンを使用して、カスタムプロパティーを追加または削除します。
6. **OK** をクリックしてプロファイルを保存し、ウィンドウを閉じます。

vNIC プロファイルがパススルーに対応するようになりました。このプロファイルを使用して仮想マシンを NIC または PCI VF に直接接続するには、論理ネットワークを NIC にアタッチし、パススルー

vNIC プロファイルを使用する必要な仮想マシンに新しい vNIC を作成します。これらの手順の詳細は、『Virtual Machine Management Guide』の「ホストのネットワークインターフェイスの編集とホストへの論理ネットワークの割り当て」および [Adding a New Network Interface](#) を参照してください。

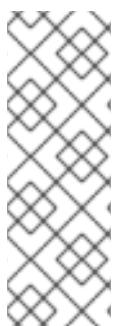
6.2.5. vNIC プロファイルの削除

vNIC プロファイルを削除すると、仮想化環境から削除されます。

手順6.9 vNIC プロファイルの削除

1. **Networks** resource タブをクリックし、結果一覧で論理ネットワークを選択します。
2. 詳細ペインで **Profiles** タブを選択して、利用可能な vNIC プロファイルを表示します。ツリーモードで論理ネットワークを選択した場合は、結果一覧で **VNIC Profiles** タブを選択します。
3. 1つ以上のプロファイルを選択し、**Remove** をクリックして **Remove VM Interface Profile (s)** ウィンドウを開きます。
4. **OK** をクリックしてプロファイルを削除し、ウィンドウを閉じます。

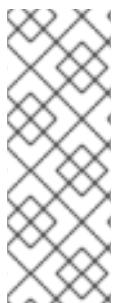
6.2.6. vNIC プロファイルへのセキュリティーグループの割り当て



注記

この機能は、OpenStack Neutron と統合しているユーザーのみが利用できます。セキュリティーグループは、Red Hat Virtualization Manager で作成できません。OpenStack 内にセキュリティーグループを作成する必要があります。詳細は、『Red Hat OpenStack Platform Users and Identity Management Guide』の <https://access.redhat.com/documentation/en/red-hat-openstack-platform/9/single/users-and-identity-management-guide#project-security> してください。

OpenStack Networking インスタンスからインポートされ、Open vSwitch プラグインを使用するネットワークの vNIC プロファイルに、セキュリティーグループを割り当てるすることができます。セキュリティーグループとは、厳密に適用されるルールの集合体であり、ネットワークインターフェイス上のインバウンドおよびアウトバウンドのトラフィックをフィルタリングできます。以下の手順では、vNIC プロファイルにセキュリティーグループをアタッチする方法について説明します。



注記

セキュリティーグループは、OpenStack Networking インスタンスに登録されているセキュリティーグループの ID を使用して識別されます。特定のテナントのセキュリティーグループ ID を特定するには、OpenStack Networking がインストールされているシステムで以下のコマンドを実行します。

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

手順6.10 vNIC プロファイルへのセキュリティーグループの割り当て

1. ネットワーク タブを クリック して、結果リストから論理ネットワークを選択します。
2. 詳細ペインの **vNIC Profiles** タブを クリック します。

3. **New** をクリックするか、既存の vNIC プロファイルを選択して **Edit** をクリックし、**VM Interface Profile** ウィンドウを開きます。
4. カスタムプロパティーのドロップダウンリストから、**SecurityGroups** を選択します。カスタムプロパティーのドロップダウンを空白のままにすると、デフォルトのセキュリティー設定が適用され、すべてのアウトバウンドトラフィックとの相互通信が許可されますが、デフォルトのセキュリティーグループ外からのインバウンドトラフィックはすべて拒否されます。後で **SecurityGroups** プロパティーを削除しても、適用されたセキュリティーグループには影響がないことに注意してください。
5. テキストフィールドに、vNIC プロファイルにアタッチするセキュリティーグループの ID を入力します。
6. **OK** をクリックします。

vNIC プロファイルにセキュリティーグループをアタッチしました。そのプロファイルが接続されている論理ネットワークを経由するすべてのトラフィックは、そのセキュリティーグループに定義されているルールに従ってフィルタリングされます。

6.2.7. vNIC プロファイルのユーザー権限

ユーザー権限を設定して、特定の vNIC プロファイルにユーザーを割り当てます。**VnicProfileUser** ロールをユーザーに割り当て、プロファイルを使用できるようにします。特定のプロファイルに対する権限を削除して、ユーザーを制限できます。

手順6.11 vNIC プロファイルのユーザー権限

1. ネットワーク タブを クリック して、結果リストから論理ネットワークを選択します。
2. **vNIC Profiles** resource タブをクリックして vNIC プロファイルを表示します。
3. 詳細ペインの **Permissions** タブをクリックして、プロファイルの現在のユーザーパーミッションを表示します。
4. **Add** ボタンをクリックして **Add Permission to User** ウィンドウを開き、**Remove** ボタンをクリックして **Remove Permission** ウィンドウを開き、vNIC プロファイルのユーザーパーミッションを変更します。
5. **Add Permissions to User** ウィンドウで **My Groups** をクリックし、ユーザーグループを表示します。このオプションを使用して、グループ内の他のユーザーに権限を付与できます。

vNIC プロファイルのユーザー権限を設定しました。

6.2.8. UCS 統合用の vNIC プロファイルの設定

Cisco の Unified Computing System (UCS)は、コンピューティング、ネットワーク、ストレージリソースなどのデータセンターの要素を管理するために使用されます。

vdsm-hook-vmfex-dev フックを使用すると、vNIC プロファイルを設定して、仮想マシンは Cisco の UCS 定義のポートプロファイルに接続できます。UCS で定義されたポートプロファイルには、UCS で仮想インターフェイスを設定するために使用されるプロパティーと設定が含まれています。**vdsm-hook-vmfex-dev** フックは、VDSM とともにデフォルトでインストールされます。詳細は、[付録A VDSM およびフック](#) を参照してください。

vNIC プロファイルを使用する仮想マシンが作成されると、Cisco vNIC が使用されます。

UCS 統合用の vNIC プロファイルを設定する手順では、最初にカスタムデバイスプロパティーを設定する必要があります。カスタムデバイスプロパティーを設定すると、そこに含まれる既存の値が上書きされます。新規および既存のカスタムプロパティーを組み合わせる場合は、キーの値を設定するために使用されるコマンドにすべてのカスタムプロパティーを含めます。複数のカスタムプロパティーはセミコロンで区切られます。



注記

vNIC プロファイルを設定する前に、UCS ポートプロファイルを Cisco UCS で設定する必要があります。

手順6.12 カスタムデバイスプロパティーの設定

- Red Hat Virtualization Manager で、**vmfex** カスタムプロパティーを設定し、**--cver** を使用してクラスターの互換性レベルを設定します。

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

- vmfex** カスタムデバイスプロパティーが追加されていることを確認します。

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

- エンジンを再始動します。

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

設定する vNIC プロファイルは、新規または既存の論理ネットワークに所属させることができます。新しい論理ネットワークを設定する手順は、「[データセンターまたはクラスターでの新しい論理ネットワークの作成](#)」を参照してください。

手順6.13 UCS 統合用の vNIC プロファイルの設定

- Networks** resource タブをクリックし、結果一覧で論理ネットワークを選択します。
- 詳細ペインで **vNIC Profiles** タブを選択します。ツリーモードで論理ネットワークを選択した場合は、結果一覧で **vNIC Profiles** タブを選択できます。
- New** または **Edit** をクリックして、**VM Interface Profile** ウィンドウを開きます。
- プロファイルの **Name** および **Description** を入力します。
- カスタムプロパティー リストから **vmfex** カスタムプロパティーを選択し、UCS ポートプロファイル名を入力します。
- OK** をクリックします。

6.3. 外部プロバイダーネットワーク

6.3.1. 外部プロバイダーからのネットワークのインポート

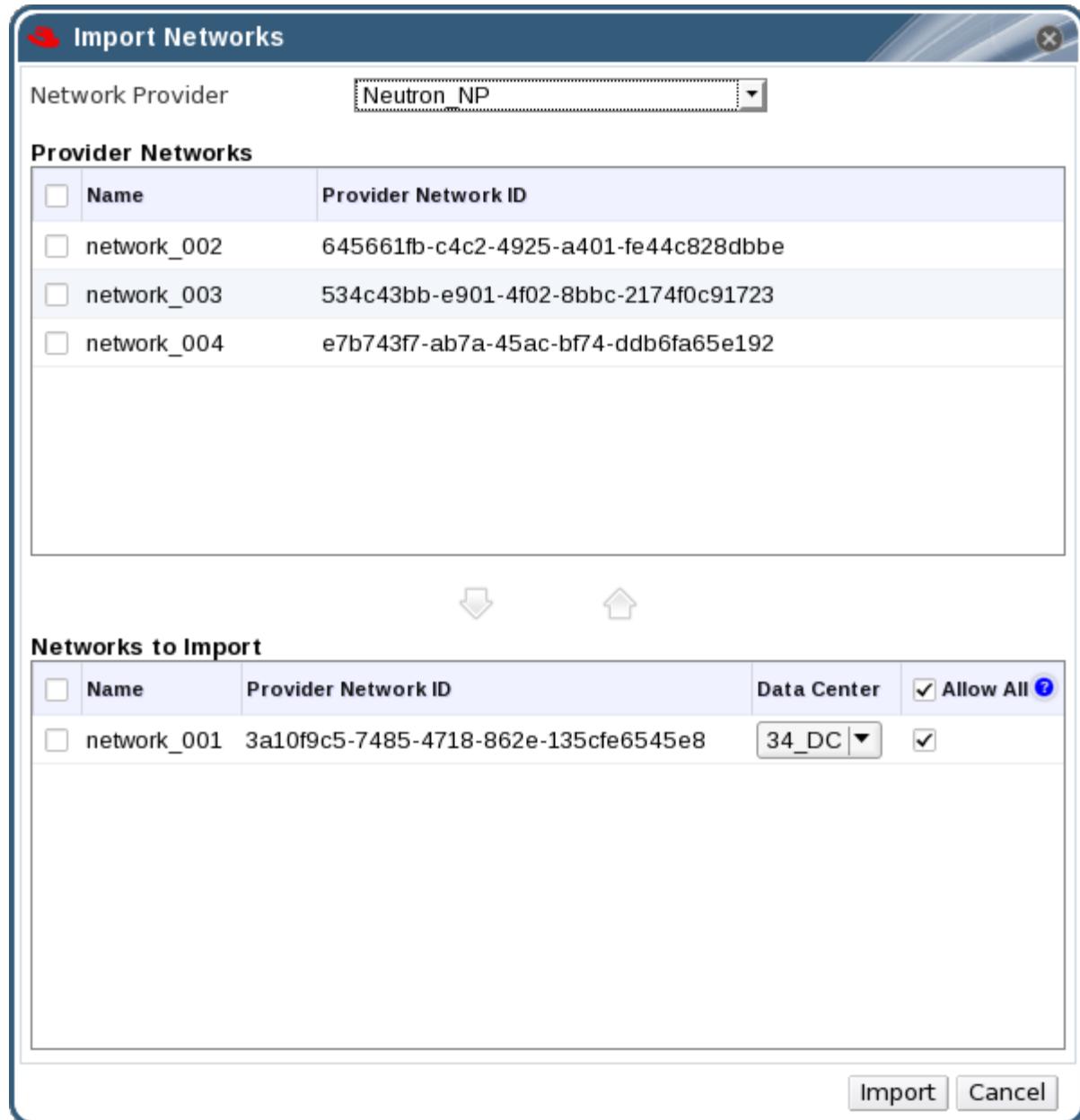
外部ネットワークプロバイダー (OpenStack Networking または OpenStack Neutron REST API を実装するサードパーティープロバイダー) からのネットワークを使用するには、プロバイダーを Manager に登

録します。詳細は、「[ネットワークプロビジョニング用の OpenStack Networking \(Neutron\) インスタンスの追加](#)」または「[外部ネットワークプロバイダーの追加](#)」を参照してください。その後、以下の手順でプロバイダーが提供するネットワークを Manager にインポートし、仮想マシンがネットワークを使用できるようにします。

手順6.14 外部プロバイダーからのネットワークのインポート

1. **Networks** タブをクリックします。
2. **Import** ボタンをクリックして、**Import Networks** ウィンドウを開きます。

図6.3 ネットワークのインポートウィンドウ



3. **Network Provider** ドロップダウンリストから、外部プロバイダーを選択します。そのプロバイダーが提供するネットワークは自動的に検出され、プロバイダーネットワークの一覧に表示されます。
4. チェックボックスを使用して、**Provider Networks** 一覧でインポートするネットワークを選択し、下矢印をクリックしてそれらのネットワークを **Networks to Import** 一覧に移動します。

5. インポートするネットワークの名前をカスタマイズすることができます。名前をカスタマイズするには、名前列でネットワークの名前をクリックし、テキストを変更します。
6. **Data Center** ドロップダウンリストから、ネットワークをインポートするデータセンターを選択します。
7. 必要に応じて、**Networks to Import** 一覧のネットワークの **Allow All** チェックボックスをオフにして、そのネットワークがすべてのユーザーで利用可能にならないようにします。
8. **Import** ボタンをクリックします。

選択されたネットワークはターゲットデータセンターにインポートされ、仮想マシンにアタッチできるようになります。詳細は、『Virtual Machine Management Guide』の [Adding a New Network Interface](#) を参照してください。

6.3.2. 外部プロバイダーネットワークの使用に関する制限

外部プロバイダーからインポートした論理ネットワークを Red Hat Virtualization 環境で使用する場合には、以下の制限があります。

- 外部プロバイダーが提供する論理ネットワークは、仮想マシンのネットワークとして使用する必要があります、ディスプレイネットワークとして使用できません。
- 同一の論理ネットワークを複数回インポートできますが、インポートできるのは異なるデータセンターのみです。
- 外部プロバイダーが提供する論理ネットワークを Manager で編集できません。外部のプロバイダーが提供する論理ネットワークの詳細を編集するには、対象の論理ネットワークを提供している外部のプロバイダーから直接編集する必要があります。
- 外部のプロバイダーが提供する論理ネットワークに接続された仮想ネットワークインターフェイスカードでは、ポートミラーリングは利用できません。
- 仮想マシンが外部のプロバイダーが提供する論理ネットワークを使用している場合には、その論理ネットワークが仮想マシンで使用されている間は、そのプロバイダーを Manager から削除できません。
- 外部のプロバイダーが提供するネットワークは必須ではありません。そのため、ホスト選択時には、このような論理ネットワークのインポート先のクラスターのスケジューリングでこれらの論理ネットワークは考慮されません。さらに、このような論理ネットワークのインポート先のクラスターで、ユーザーが責任を持ってホストで論理ネットワークを利用できるようにしてください。

6.3.3. 外部プロバイダーの論理ネットワークのサブネット設定

6.3.3.1. 外部プロバイダーの論理ネットワークのサブネット設定

外部のプロバイダーが提供する論理ネットワークは、その論理ネットワーク上に1つ以上のサブネットが定義されている場合にのみ、仮想マシンに IP アドレスを割り当てることができます。サブネットが定義されていない場合、仮想マシンには IP アドレスが割り当てられません。サブネットが1つある場合、仮想マシンにはそのサブネットから IP アドレスが割り当てられ、複数のサブネットがある場合には、仮想マシンには利用可能なサブネットのいずれかから IP アドレスが割り当てられます。論理ネットワークがホストされる外部ネットワークプロバイダーが提供する DHCP サービスは、これらの IP アドレスを割り当てます。

Red Hat Virtualization Manager は、インポートされた論理ネットワーク上で定義済みのサブネットを自動的に検出しますが、Manager 内で論理ネットワークにサブネットを追加したり、論理ネットワークからサブネットを削除したりすることもできます。

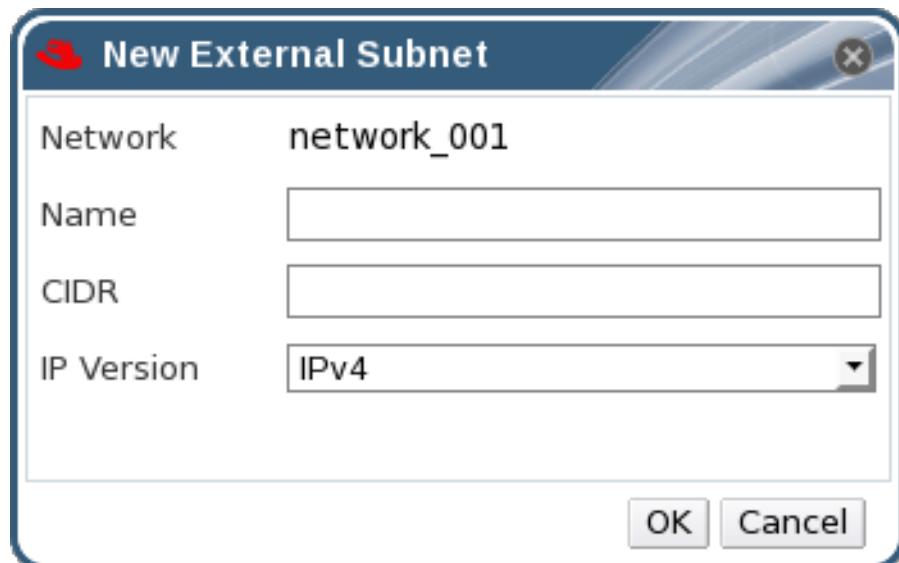
6.3.3.2. 外部プロバイダー論理ネットワークへのサブネットの追加

外部のプロバイダーが提供する論理ネットワーク上にサブネットを作成します。

手順6.15 外部プロバイダー論理ネットワークへのサブネットの追加

1. **Networks** タブをクリックします。
2. サブネットを追加する外部プロバイダーが提供する論理ネットワークをクリックします。
3. 詳細ペインの **サブネット** タブをクリックします。
4. 新規 ボタンをクリックして **新規外部サブネット** ウィンドウを開きます。

図6.4 新しい外部サブネットウィンドウ



5. 新規サブネットの **Name** および **CIDR** を入力します。
6. **IP Version** ドロップダウンメニューから、**IPv4** または **IPv6** のいずれかを選択します。
7. **OK** をクリックします。

6.3.3.3. 外部プロバイダー論理ネットワークからのサブネットの削除

外部プロバイダーが提供する論理ネットワークからサブネットを削除します。

手順6.16 外部プロバイダー論理ネットワークからのサブネットの削除

1. **Networks** タブをクリックします。
2. サブネットを削除する外部プロバイダーが提供する論理ネットワークをクリックします。
3. 詳細ペインの **サブネット** タブをクリックします。
4. 削除するサブネットをクリックします。

5. **Remove** ボタンをクリックし、プロンプトが表示されたら **OK** をクリックします。

6.4. 論理ネットワークとパーミッション

6.4.1. ネットワークのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルのすべての側面を管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限された管理者ロールは、特定のリソースに制限される管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、そのデータセンターのストレージを除く、割り当てられたデータセンターの管理者権限のみを持ち、**ClusterAdmin** は割り当てられたクラスターに対してのみ管理者権限を持ちます。

ネットワーク管理者は、特定のネットワークまたはデータセンター、クラスター、ホスト、仮想マシン、またはテンプレートにあるすべてのネットワークに適用できるシステム管理ロールです。ネットワークユーザーは、特定の仮想マシンまたはテンプレート上のネットワークの表示やアタッチなど、制限された管理ロールを実行できます。ヘッダーバーの **Configure** ボタンを使用して、環境内の全ネットワークにネットワーク管理者を割り当てることができます。

ネットワーク管理者ロールは以下のアクションを許可します。

- ネットワークの作成、編集、および削除。
- ポートミラーリングの設定など、ネットワークの設定を編集。
- クラスターや仮想マシンを含むリソースからのネットワークをアタッチおよびデタッチ。

ネットワークを作成するユーザーには、作成されたネットワークに **NetworkAdmin** パーミッションが自動的に割り当てられます。また、既存の管理者を削除し、新しい管理者を追加すると、ネットワークの管理者を変更できます。

6.4.2. ネットワーク管理者およびユーザーロールの概要

ネットワークパーミッションロール

以下の表は、ネットワークの管理に適用される管理者およびユーザーロールと権限について説明しています。

表6.6 Red Hat Virtualization ネットワーク管理者およびユーザーロール

ロール	権限	注記

ロール	権限	注記
NetworkAdmin	データセンター、クラスター、ホスト、仮想マシン、またはテンプレートのネットワーク管理者。ネットワークを作成するユーザーには、作成されたネットワークに NetworkAdmin パーミッションが自動的に割り当てられます。	特定のデータセンター、クラスター、ホスト、仮想マシン、またはテンプレートのネットワークを設定および管理できます。データセンターまたはクラスターのネットワーク管理者は、クラスター内の仮想プールのネットワークパーミッションを継承します。仮想マシンネットワークにポートミラーリングを設定するには、ネットワークに NetworkAdmin ロールを適用し、仮想マシンに UserVmManager ロールを適用します。
VnicProfileUser	仮想マシンおよびテンプレートの論理ネットワークおよびネットワークインターフェイスユーザー。	特定の論理ネットワークからネットワークインターフェイスを接続または切断できます。

6.4.3. 管理者またはユーザーロールのリソースへの割り当て

管理者またはユーザーロールをリソースに割り当て、ユーザーがそのリソースにアクセスしたり、管理したりできるようにします。

手順6.17 リソースへのロールの割り当て

- リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
- 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
- Add** をクリックします。
- Search** テキストボックスに既存ユーザーの名前またはユーザー名を入力し、**Go** をクリックします。表示された候補の中からユーザーを選択します。
- Role to Assign:** ドロップダウンリストからロールを選択します。
- OK** をクリックします。

ユーザーにロールを割り当てました。そのリソースで有効にしたそのロールの継承されたパーミッションが、ユーザーに付与されました。

6.4.4. リソースからの管理者またはユーザーロールの削除

管理者またはユーザーのロールをリソースから削除すると、ユーザーはそのリソースのロールに関連付けられ継承されたパーミッションを失います。

手順6.18 リソースからのロールの削除

1. リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
2. 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
3. リソースから削除するユーザーを選択します。
4. **Remove** をクリックします。 **Remove Permission** 画面が開き、パーミッションの削除を確認します。
5. **OK** をクリックします。

ユーザーのロールおよび関連付けられたパーミッションをリソースから削除しました。

6.5. ホストとネットワーキング

6.5.1. ホスト機能のリフレッシュ

ネットワークインターフェイスカードをホストに追加した場合、そのネットワークインターフェイスカードを Manager に表示するには、ホストの機能を更新する必要があります。

手順6.19 ホスト機能の更新

1. リソースタブ、ツリーモード、または検索機能を使用して、結果一覧でホストを見つけて選択します。
2. **Refresh Capabilities** ボタンをクリックします。

選択したホストの詳細ペインの **Network Interfaces** タブにあるネットワークインターフェイスカードの一覧が更新されます。新しいネットワークインターフェイスカードが、Manager で使用できるようになりました。

6.5.2. ホストのネットワークインターフェイスの編集とホストへの論理ネットワークの割り当て

物理ホストネットワークインターフェイスの設定を変更したり、管理ネットワークを別の物理ホストネットワークインターフェイスに移動したり、物理ホストネットワークインターフェイスに論理ネットワークを割り当てたりすることができます。また、ブリッジや ethtool のカスタムプロパティーにも対応しています。



警告

Red Hat Virtualization でホストの IP アドレスを変更する唯一の方法は、そのホストを削除してから再度追加することです。

ホストの VLAN 設定を変更するには、一旦 Manager からホストを削除し、再設定した後、再度 Manager に追加する必要があります。

ネットワークの同期を維持するには、以下の手順を実施します。ホストをメンテナーンスマードにし、ホストから管理ネットワークを手動で削除します。これにより、ホストは新しい VLAN 上で到達可能になります。ホストをクラスターに追加します。管理ネットワークに直接接続されていない仮想マシンは、ホスト間で安全に移行できます。

管理ネットワークの VLAN ID を変更すると、次のような警告メッセージが表示されます。

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?

続行すると、データセンター内のすべてのホストが Manager への接続を失い、新しい管理ネットワークへのホストの移行が失敗してしまいます。管理ネットワークは、非同期と報告されます。



重要

外部のプロバイダーが提供する論理ネットワークは、物理ホストのネットワークインターフェイスに割り当てるることはできません。このような論理ネットワークは、仮想マシンが必要なときに動的にホストに割り当てられます。

手順6.20 ホストのネットワークインターフェイスの編集とホストへの論理ネットワークの割り当て

1. **Hosts** resource タブをクリックし、目的のホストを選択します。
2. 詳細ペインの **ネットワークインターフェイス** タブをクリックします。
3. **Setup Host Networks** ボタンをクリックして **Setup Host Networks** ウィンドウを開きます。
4. 物理ホストネットワークインターフェイスの横にある **Assigned Logical Networks** 領域に論理ネットワークを選択してドラッグし、物理ホストネットワークインターフェイスに論理ネットワークをアタッチします。
または、論理ネットワークを右クリックして、ドロップダウンメニューからネットワークインターフェイスを選択します。
5. 論理ネットワークの設定
 - a. 割り当てられた論理ネットワークにカーソルを合わせ、鉛筆アイコンをクリックして **Edit Management Network** ウィンドウを開きます。

- b. IPv4 タブで、None、DHCP、または Static から Boot Protocol を選択します。Static を選択した場合は、IP、Netmask / Routing Prefix、および Gateway を入力します。



注記

各論理ネットワークには、管理ネットワークのゲートウェイとは別にゲートウェイを定義できます。これにより、論理ネットワークに到達するトラフィックは、管理ネットワークで使用されるデフォルトゲートウェイではなく、論理ネットワークのゲートウェイを使用して転送されます。



注記

IPv6 タブは現在サポートされていないため、使用しないでください。

- c. QoS タブを使用して、デフォルトのホストネットワーク QoS を上書きします。Override QoS を選択し、以下のフィールドに必要な値を入力します。

- **加重共有:** 同じ論理リンクに接続されている他のネットワークと比較して、特定のネットワークを割り当てる必要がある論理リンクの容量を示します。正確な共有は、そのリンクの全ネットワークの共有の合計によって異なります。デフォルトでは、この値は 1-100 の範囲の数字になります。
- **Rate Limit [Mbps]:** ネットワークが使用する最大帯域幅。
- **Committed Rate [Mbps]:** ネットワークに必要な最小帯域幅。要求される Committed Rate は保証されず、ネットワークインフラストラクチャーおよび同じ論理リンクの他のネットワークによって要求される Committed Rate によって異なります。

ホストネットワーク QoS の設定に関する詳細は、[を参照してください。「ホストネットワーク QoS」](#)

- d. ネットワークブリッジを設定するには、Custom Properties タブをクリックし、ドロップダウンリストから bridge_opts を選択します。key = value の構文で有効なキーと値を入力します。複数の項目を空白文字で区切ります。以下のキーが有効で、値は例として示されています。これらのパラメーターに関する詳しい情報は、[「bridge_opts パラメーターの説明」](#) を参照してください。

```
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. イーサネットプロパティーを設定するには、**Custom Properties** タブをクリックし、ドロップダウンリストから **ethtool_opts** を選択します。ethtool のコマンドライン引数の形式で、有効な値を入力してください。以下に例を示します。

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

このフィールドは、ワイルドカードを使用できます。たとえば、このネットワークのすべてのインターフェイスに同じオプションを適用するには、以下を使用します。

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

ethtool_opts オプションはデフォルトでは使用できないため、エンジン設定ツールを使用して追加する必要があります。詳細は、「[Red Hat Virtualization Manager を使用するように Red Hat Virtualization Manager を設定する方法](#)」を参照してください。ethtool プロパティーの詳細は、コマンドラインで **man ethtool** を入力して man ページを参照してください。

- f. Fibre Channel over Ethernet (FCoE)を設定するには、**Custom Properties** タブをクリックし、ドロップダウンリストから **fcoe** を選択します。key = value の構文で有効な キーと値を入力します。最低でも **enable=yes** が必要です。**dcb=[yes|no]** および **auto_vlan=[yes|no]** を追加することもできます。複数の項目を空白文字で区切れます。fcoe オプションはデフォルトでは使用できないため、エンジン設定ツールを使用して追加する必要があります。詳細は、「[FCoE を使用するように Red Hat Virtualization Manager を設定する方法](#)」を参照してください。



注記

FCoE を使用する場合は、別途、専用の論理ネットワークを用意することをお勧めします。

- g. 論理ネットワークの定義がホストのネットワーク設定と同期していない場合は、**ネットワークの同期** チェックボックスを選択します。論理ネットワークは、同期されるまで編集したり、別のインターフェイスに移動したりすることはできません。



注記

以下の条件のいずれかがある場合、ネットワークは同期されないと見なされます。

- **VM** ネットワークは、物理ホストネットワークとは異なります。
- VLAN 識別子は、物理ホストネットワークとは異なります。
- **カスタム MTU** は論理ネットワーク上に設定され、物理ホストネットワークとは異なります。

6. **Verify connectivity between Host and Engine** チェックボックスを選択し、ネットワーク接続を確認します。このアクションは、ホストがメンテナンスモードの場合にのみ機能します。

7. **Save network configuration** チェックボックスを選択し、環境の再起動時に変更を永続化します。
8. **OK** をクリックします。



注記

ホストのすべてのネットワークインターフェイスカードが表示されない場合は、**Refresh Capabilities** ボタンをクリックして、そのホストで利用可能なネットワークインターフェイスカードの一覧を更新します。

6.5.3. 論理ネットワークを使用した単一のネットワークインターフェイスへの複数の VLAN の追加

1つのネットワークインターフェイスに複数の VLAN を追加し、1つのホストのトラフィックを分離できます。



重要

複数の論理ネットワークを作成し、すべて **New Logical Network** または **Edit Logical Network** ウィンドウで **VLAN** タグ付けを有効にする チェックボックスを選択している必要があります。

手順6.21 論理ネットワークを使用したネットワークインターフェイスへの複数の VLAN の追加

1. **Hosts** resource タブをクリックして、結果に VLAN タグ付き論理ネットワークが割り当てられているクラスターに関連付けられたホストを一覧表示します。
2. 詳細ペインの **ネットワークインターフェイス** タブをクリックして、データセンターに接続された物理ネットワークインターフェイスを一覧表示します。
3. **Setup Host Networks** をクリックして **Setup Host Networks** ウィンドウを開きます。
4. VLAN タグ付き論理ネットワークを、物理ネットワークインターフェイスの横にある **Assigned Logical Networks** 領域にドラッグします。物理ネットワークインターフェイスには、VLAN タグがあるので複数の論理ネットワークを割り当ることができます。
5. 割り当てられた論理ネットワークの上にカーソルをかざし、鉛筆アイコンをクリックして **Edit Network** ウィンドウを開きます。

論理ネットワークの定義がホストのネットワーク設定と同期していない場合は、**ネットワークの同期** チェックボックスを選択します。

以下から **Boot Protocol** を選択します。

- なし、、
- **DHCP**、または
- 静的,

IP と サブネットマスク を指定します。

OK をクリックします。

6. **Verify connectivity between Host and Engine** チェックボックスを選択し、ネットワークチェックを実行します。これは、ホストがメンテナンスモードの場合にのみ機能します。
7. ネットワーク設定の保存 チェックボックスを選択します。
8. **OK** をクリックします。

クラスター内の各ホストの NIC を編集して、論理ネットワークをクラスター内の各ホストに追加します。これが完了すると、ネットワークは機能します。

複数の VLAN タグ付き論理ネットワークを単一のインターフェイスに追加しました。この作業を複数回繰り返し、それぞれのホストで同じネットワークインターフェイスを選択、編集して、異なる VLAN タグを割り当てた論理ネットワークを1つのネットワークインターフェイスに追加できます。

6.5.4. ホストネットワークへの追加の IPv4 アドレスの割り当て

ovirtmgmt 管理ネットワークなどのホストネットワークは、初期設定時に1つの IP アドレスのみで作成されます。つまり、NIC の設定ファイル（例：/etc/sysconfig/network-scripts/ifcfg-eth01）に複数の IP アドレスが設定されている場合、最初に一覧表示される IP アドレスのみがホストネットワークに割り当てられます。ストレージに接続する場合や、同じ NIC を使って別のプライベートサブネット上のサーバーに接続する場合は、追加の IP アドレスが必要になることがあります。

vdsm-hook-extra-ipv4-addrs フックでは、ホストネットワークに追加の IPv4 アドレスを設定することができます。フックに関する詳細は、[付録A VDSM およびフック](#) を参照してください。

以下の手順では、追加の IP アドレスを設定する各ホストで、ホスト固有のタスクを実行する必要があります。

手順6.22 ホストネットワークへの追加の IPv4 アドレスの割り当て

1. 追加の IPv4 アドレスを設定したいホストに、VDSM のフックパッケージをインストールします。Red Hat Virtualization Host ではこのパッケージがデフォルトで利用可能ですが、Red Hat Enterprise Linux ホストにインストールする必要があります。

```
# yum install vdsm-hook-extra-ipv4-addrs
```

2. Manager で以下のコマンドを実行してキーを追加します。

```
# engine-config -s 'UserDefinedNetworkCustomProperties=ipv4_addrs=.*'
```

3. ovirt-engine サービスを再起動します。

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

4. 管理ポータルで **Hosts** resource タブをクリックし、追加の IP アドレスを設定するホストを選択します。
5. 詳細ペインの **Network Interfaces** タブをクリックし、**Setup Host Networks** ボタンをクリックして **Setup Host Networks** ウィンドウを開きます。
6. 割り当てられた論理ネットワークの上にカーソルをかざし、鉛筆アイコンをクリックして、ホストネットワークインターフェイスを **編集** します。
7. **Custom Properties** ドロップダウンリストから **ipv4_addr** を選択し、IP アドレスと接頭辞を追加します(5.5.5.5/24 など)。複数の IP アドレスはコンマで区切る必要があります。

8. **OK** をクリックします。
9. ネットワーク設定の保存 チェックボックスを選択します。
10. **OK** をクリックします。

追加の IP アドレスは Manager には表示されませんが、ホストで **ip addr show** コマンドを実行して、追加されたことを確認できます。

6.5.5. ホストネットワークインターフェイスへのネットワークラベルの追加

ネットワークラベルを使用すると、ホストネットワークインターフェイスへの論理ネットワークの割り当てに関する管理ワークロードを大幅に簡素化できます。

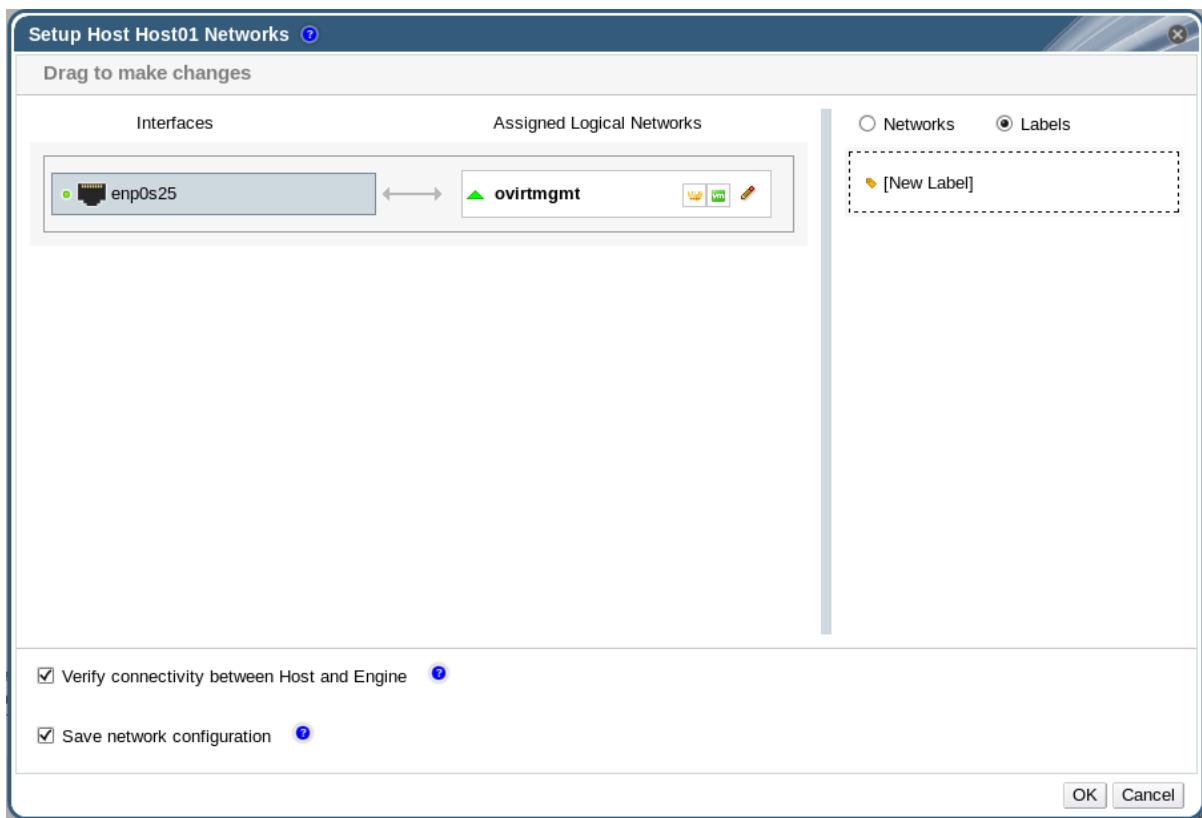


注記

ロールネットワーク（たとえば、移行ネットワークやディスプレイネットワーク）にラベルを設定すると、そのネットワークがすべてのホストに大量に展開されます。このようなネットワークの大量追加は、DHCP を使って実現しています。多くの静的 IP アドレスを入力するタスクのスケーラブルでない性質のため、この大量展開の方法は、静的アドレスを入力する方法よりも選択されました。

手順6.23 ホストネットワークインターフェイスへのネットワークラベルの追加

1. **Hosts** resource タブをクリックして、結果に VLAN タグ付き論理ネットワークが割り当てられているクラスターに関する情報を表示します。
2. 詳細ペインの **ネットワークインターフェイス** タブをクリックして、データセンターに接続された物理ネットワークインターフェイスを一覧表示します。
3. **Setup Host Networks** をクリックして **Setup Host Networks** ウィンドウを開きます。
4. **Labels** をクリックし、**[New Label]** を右クリックします。ラベルを貼る物理ネットワークインターフェイスを選択します。



5. ラベルテキストフィールドにネットワークラベルの名前を入力します。

6. **OK** をクリックします。

ホストのネットワークインターフェイスにネットワークラベルを追加しました。同じラベルを持つ新しく作成された論理ネットワークは、そのラベルを持つすべてのホストネットワークインターフェイスに自動的に割り当てられます。また、論理ネットワークからラベルを削除すると、そのラベルの付いたすべてのホストネットワークインターフェイスからの論理ネットワークが自動的に削除されます。

6.5.6. ボンド

6.5.6.1. Red Hat Virtualization でのロゴのボンディング

Red Hat Virtualization Manager 管理ポータルでは、グラフィカルインターフェイスを使用してボンディングデバイスを作成できます。それが独自のロジックを持つ個別のボンディング作成シナリオがあります。

ボンディングロジックに影響する 2 つの要因は次のとおりです。

- いずれのデバイスにもすでに論理ネットワークが搭載されていますか？
- デバイスは互換性のある論理ネットワークを提供していますか？

表6.7 ボンディングシナリオとその結果

ボンディングシナリオ	結果
------------	----

ボンディングシナリオ	結果
NIC + NIC	<p>Create New Bond ウィンドウが表示され、新しいボンドデバイスを設定できます。</p> <p>ネットワークインターフェイスに互換性のない論理ネットワークがある場合、互換性のない論理ネットワークを新しいボンディングを設定するデバイスからデタッチするまでボンディング操作は失敗します。</p>
NIC + Bond	<p>NIC がボンドデバイスに追加されます。NIC とボンディングが伝送する論理ネットワークはすべて、互換性がある場合は、結果として得られるボンドデバイスに追加されます。</p> <p>ボンディングデバイスに互換性のない論理ネットワークがある場合、互換性のない論理ネットワークをデバイスから切り離して新しいボンディングを作成するまで、ボンディング操作は失敗します。</p>
ボンディング + ボンディング	<p>ボンディングデバイスが論理ネットワークに接続されていない場合、または互換性のある論理ネットワークに接続されている場合は、新しいボンドデバイスが作成されます。これには、すべてのネットワークインターフェイスが含まれ、コンポーネントボンディングデバイスのすべての論理ネットワークが伝送されます。Create New Bond ウィンドウが表示され、新しいボンディングを設定できます。</p> <p>ボンディングデバイスに互換性のない論理ネットワークがある場合、互換性のない論理ネットワークをデバイスから切り離して新しいボンディングを作成するまで、ボンディング操作は失敗します。</p>

6.5.6.2. ボンド

ボンディングは、複数のネットワークインターフェイスカードを1つのソフトウェア定義デバイスに集約したものです。ボンディングされたネットワークインターフェイスは、ボンディングに含まれるネットワークインターフェイスカードの伝送機能を組み合わせて単一のネットワークインターフェイスとして機能するため、単一のネットワークインターフェイスカードよりも高速な伝送速度を提供できます。また、ボンド 자체が失敗するには、ボンド内のすべてのネットワークインターフェイスカードが失敗する必要があるため、ボンディングによってフォールトトレランスが向上します。ただし、1つの制限は、ボンディングされたネットワークインターフェイスを形成するネットワークインターフェイスカードは、ボンド内のすべてのネットワークインターフェイスカードが同じオプションとモードをサポートするように、同じメーカーとモデルである必要があることです。

結合のパケット分散アルゴリズムは、使用される結合モードによって決定されます。



重要

モード1、2、3、および4は、仮想マシン(ブリッジ)と非仮想マシン(ブリッジレス)の両方のネットワークタイプをサポートします。モード0、5、および6は、非仮想マシン(ブリッジレス)ネットワークのみをサポートします。

ボンディングモード

Red Hat Virtualization はデフォルトでモード 4 を使用しますが、以下の一般的なボンディングモードをサポートします。

Mode 0 (round-robin policy)

ネットワークインターフェイスカードを介してパケットを順番に送信します。パケットは、ボンディングで最初に利用可能なネットワークインターフェイスカードで始まり、ボンドで最後に使用可能なネットワークインターフェイスカードで終わるループで送信されます。その後のすべてのループは、最初に使用可能なネットワークインターフェイスカードから始まります。モード 0 はフォールトトレランスを提供し、ボンド内のすべてのネットワークインターフェイスカード間で負荷を分散します。ただし、モード 0 はブリッジと組み合わせて使用できないため、仮想マシンの論理ネットワークとの互換性はありません。

モード 1 (active-backup ポリシー)

1枚のネットワークインターフェイスカードがアクティブなまま、すべてのネットワークインターフェイスカードをバックアップ状態に設定します。アクティブなネットワークインターフェイスカードに障害が発生した場合、バックアップネットワークインターフェイスカードの1つが、ボンド内の唯一のアクティブなネットワークインターフェイスカードとしてそのネットワークインターフェイスカードに置き換わります。モード 1 のボンディングの MAC アドレスは、1つのポートにのみ表示され、ボンディングの MAC アドレスがアクティブなネットワークインターフェイスカードを反映するように変更された場合に混乱を防ぐことができます。モード 1 はフォールトトレランスを提供し、Red Hat Virtualization でサポートされています。

Mode 2 (XOR policy)

ネットワークインターフェイスカードのスレーブ数をモジュロとして、送信元および宛先 MAC アドレスでの XOR 操作の結果に基づいて、パケットの送信に使用するネットワークインターフェイスカードを選択します。この計算により、使用される宛先 MAC アドレスごとに同じネットワークインターフェイスカードが確実に選択されます。モード 2 は、フォールトトレランスと負荷分散を提供し、Red Hat Virtualization でサポートされています。

Mode 3 (broadcast policy)

すべてのパケットをすべてのネットワークインターフェイスカードに送信します。モード 3 はフォールトトレランスを提供し、Red Hat Virtualization でサポートされています。

Mode 4 (IEEE 802.3ad policy)

インターフェイスが同じ速度とデュプレックス設定を共有するアグリゲーショングループを作成します。モード 4 は、IEEE 802.3ad 仕様に従って、アクティブなアグリゲーショングループ内のすべてのネットワークインターフェイスカードを使用し、Red Hat Virtualization でサポートされます。

Mode 5 (adaptive send load balancing policy)

送信トラフィックの分散がボンド内の各ネットワークインターフェイスカードの負荷を考慮し、現在のネットワークインターフェイスカードがすべての受信トラフィックを受信するようにします。トラフィックの受信に割り当てられたネットワークインターフェイスカードに障害が発生した場合、別のネットワークインターフェイスカードが着信トラフィックの受信のロールに割り当てられます。モード 5 はブリッジと組み合わせて使用できないため、仮想マシンの論理ネットワークとは互換性ありません。

Mode 6 (adaptive load balancing policy)

特別なスイッチ要件なしで、モード 5 (適応型送信負荷分散ポリシー) と IPv4 トラフィックの受信負荷分散を組み合わせます。ARP ネゴシエーションは、受信負荷のバランスを取るために使用されます。モード 6 はブリッジと組み合わせて使用できないため、仮想マシンの論理ネットワークとは互換性ありません。

6.5.6.3. 管理ポータルを使用したボンドデバイスの作成

互換性のあるネットワークデバイスを結合できます。このタイプの設定では、利用可能な帯域幅と信頼性が向上します。複数のネットワークインターフェイス、既存のボンディングデバイス、および2つの組み合わせをボンディングできます。ボンディングは、VLANタグ付きトラフィックとVLAN以外のトラフィックの両方を伝送できます。

手順6.24 管理ポータルを使用したボンドデバイスの作成

1. **Hosts** resource タブをクリックし、結果一覧でホストを選択します。
2. 詳細ペインの **ネットワークインターフェイス** タブをクリックして、ホストに接続されている物理ネットワークインターフェイスを一覧表示します。
3. **Setup Host Networks** をクリックして **Setup Host Networks** ウィンドウを開きます。
4. 別のデバイスの上部にデバイスのいずれかを選択してドラッグし、これを削除して **Create New Bond** ウィンドウを開きます。または、デバイスを右クリックし、ドロップダウンメニューから別のデバイスを選択します。

デバイスが互換性のない場合は、ボンド操作が失敗し、互換性の問題を修正する方法を提案します。

5. ドロップダウンメニューから **Bond Name** および **Bonding Mode** を選択します。
ボンディングモード1、2、4、および5を選択できます。他のモードは、カスタムオプションを使用して設定できます。
6. **OK** をクリックしてボンディングを作成し、**Create New Bond** ウィンドウを閉じます。
7. 新しく作成されたボンドデバイスに論理ネットワークを割り当てます。
8. 必要に応じて、**ホストとエンジン間の接続の確認** と **ネットワーク設定の保存** を選択します。
9. **OK** をクリックして変更を受け入れ、**Setup Host Networks** ウィンドウを閉じます。

ネットワークデバイスがボンドデバイスにリンクされ、1つのインターフェイスとして編集できます。ボンディングデバイスは、選択したホストの詳細ペインの **ネットワークインターフェイス** タブに一覧表示されます。

ホストが使用するスイッチのポートに対してボンディングを有効にする必要があります。ボンディングを有効にするプロセスは、スイッチごとに若干異なります。ボンディングを有効にする方法の詳細は、スイッチベンダーが提供するマニュアルを参照してください。

6.5.6.4. ホストインターフェイスでのカスタムボンディングオプションの使用例

カスタマイズされたボンドデバイスを作成するには、**Create New Bond** ウィンドウの **Bonding Mode** から **Custom** を選択します。以下の例は、ニーズに合わせて調整する必要があります。ボンディングオプションとその説明の包括的な一覧は、Kernel.org の [『Linux Ethernet Bonding Driver HOWTO』](#) を参照してください。

例6.1 xmit_hash_policy

このオプションは、ボンディングモード2および4の送信負荷分散ポリシーを定義します。たとえば、トラフィックの大半が多数の異なるIPアドレス間である場合は、IPアドレスでバランスを取るようにポリシーを設定する必要がある場合があります。カスタムボンディングモードを選択し、テキストフィールドに以下を入力して、この負荷分散ポリシーを設定できます。

```
mode=4 xmit_hash_policy=layer2+3
```

例6.2 ARP 監視

ARP モニターは、ethtool を介してリンク状態を適切に報告できないシステムに役立ちます。カスタム ボンディングモードを選択し、テキストフィールドに以下を入力して、ホストのボンドデバイスに **arp_interval** を設定します。

```
mode=1 arp_interval=1 arp_ip_target=192.168.0.2
```

例6.3 プライマリー

より高いスループットの NIC をボンドデバイスのプライマリインターフェイスとして指定することができます。カスタム ボンディングモードを選択し、テキストフィールドに以下を入力して、どの NIC がプライマリーであるかを指定します。

```
mode=1 primary=eth0
```

6.5.7. ホストの FQDN の変更

以下の手順で、ホストの完全修飾ドメイン名を変更します。

手順6.25 ホストの FQDN の更新

- ホストをメンテナスマードにして、仮想マシンが別のホストにライブマイグレーションされるようにします。詳細は、「[ホストのメンテナスマードへの切り替え](#)」を参照してください。あるいは、すべての仮想マシンを手動でシャットダウンするか、別のホストに移行してください。詳細は、『Virtual Machine Management Guide』の [Manually Migrating Virtual Machines](#) を参照してください。
- Remove** をクリックし、**OK** をクリックして管理ポータルからホストを削除します。
- hostnamectl** ツールを使用してホスト名を更新します。その他のオプションは、『Red Hat Enterprise Linux 7 ネットワークガイド』の [ホスト名の設定](#) を参照してください。

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

- ホストを再起動します。
- ホストをマネージャーに再登録する。詳細は、「[Red Hat Virtualization Manager へのホストの追加](#)」を参照してください。

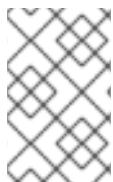
第7章 ホスト

7.1. ホストの HQL の概要

ホスト（ハイパーバイザーとも呼ばれる）は、仮想マシンが動作する物理サーバーです。Kernel-based Virtual Machine (KVM) と呼ばれるローダーブル Linux カーネルモジュールを使用することで、完全な仮想化が提供されます。

KVM は、Windows または Linux いずれかのオペレーティングシステムを実行する複数の仮想マシンを、同時にホストすることができます。仮想マシンはホストマシン上で個々の Linux プロセスやスレッドとして実行され、Red Hat Virtualization Manager によってリモートで管理されます。Red Hat Virtualization の環境には、それに接続された1つ以上のホストがあります。

Red Hat Virtualization は、ホストをインストールする2つの方法をサポートしています。Red Hat Virtualization Host (RHVH) のインストールメディアを使用するか、標準の Red Hat Enterprise Linux インストールにハイパーバイザーパッケージをインストールすることができます。



注記

Red Hat Virtualization Manager で個々のホストのホストタイプを特定するには、ホストを選択し、詳細ペインの **General** タブで **Software** をクリックし、**OS Description** を確認します。

ホストは、仮想化の最適化を提供する **tuned** プロファイルを使用します。**tuned** の詳細は、『[Red Hat Enterprise Linux 7 Performance Tuning Guide](#)』を参照してください。

Red Hat Virtualization Host は、セキュリティ機能が有効になっています。SELinux (Security Enhanced Linux) および iptables ファイアウォールは完全に設定されており、デフォルトでオンになっています。選択したホストの SELinux のステータスは、詳細ペインの **General** タブの **SELinux** モードで報告されます。Manager は、Red Hat Enterprise Linux ホストに必要なポートを環境に追加する際に開くことができます。

ホストとは、Red Hat Enterprise Linux 7 AMD64/Intel 64 版が動作する Intel VT または AMD-V 拡張機能を持つ物理的な 64 ビットサーバーのことです。

Red Hat Virtualization プラットフォーム上の物理的なホストのこと。

- システム内の1つのクラスターにのみ属すること。
- AMD-V または Intel VT ハードウェア仮想化拡張をサポートする CPU を搭載していること。
- クラスター作成時に選択された仮想 CPU タイプで提供されるすべての機能をサポートする CPU が必要です。
- 最小 2 GB のメモリー。
- システム権限を持つシステム管理者を割り当てることができる。

管理者は Red Hat Virtualization のウォッチリストから最新のセキュリティ勧告を受け取ることができます。Red Hat Virtualization ウォッチリストに登録すると、Red Hat Virtualization 製品の新しいセキュリティ勧告を電子メールで受け取ることができます。このフォームに必要事項を入力してください。

<http://www.redhat.com/mailman/listinfo/rhev-watch-list/>



警告

NetworkManager によるネットワークの設定(**nmcli**、**nmtui**、Cockpit ユーザーインターフェイスを含む)は、現在サポートされていません。ホストを Manager に追加する前に追加のネットワーク設定が必要な場合は、**ifcfg** ファイルを手動で作成する必要があります。詳細は、『Red Hat Enterprise Linux ネットワークガイド』を参照してください。

7.2. RED HAT VIRTUALIZATION HOST

Red Hat Virtualization Host (RHVH) は、仮想マシンをホストするのに必要なパッケージのみを搭載した Red Hat Enterprise Linux の特別なビルドを使用してインストールされます。Red Hat Enterprise Linux ホストで使用されているものをベースにした **Anaconda** インストールインターフェイスを使用し、Red Hat Virtualization Manager または **yum** を使用して更新できます。ただし、現在、追加のパッケージのインストールはサポートされていません。RHVH の更新ごとにインストールされる追加パッケージを再インストールする必要があります。

RHVH は、ホストのリソースを監視し、管理タスクを実行するための Cockpit ユーザーインターフェイスを特長としています。SSH またはコンソールを介した RHVH への直接アクセスはサポートされていないため、Cockpit ユーザーインターフェイスは、ホストが Red Hat Virtualization Manager に追加される前に実行されるタスクのグラフィカルユーザーインターフェイスを提供します（例：セルフホストエンジンのデプロイ）。また、ツール > **Terminal** サブタブでターミナルコマンドを実行するのに使用できます。

Web ブラウザーで <https://HostFQDNorIP:9090> で Cockpit ユーザーインターフェイスにアクセスします。RHVH 用の Cockpit には、ホストのヘルスステータス、SSH ホストキー、セルフホストエンジンのステータス、仮想マシン、および仮想マシンの統計を表示するカスタム仮想化ダッシュボードが含まれています。



注記

カスタムブートカーネル引数は、**grubby** ツールを使用して Red Hat Virtualization Host に追加できます。**grubby** ツールは、**grub.cfg** ファイルに永続的な変更を加えます。ホストの Cockpit ユーザーインターフェイスの **Tools** > **Terminal** サブタブに移動し、**grubby** コマンドを使用します。詳細は、『Red Hat Enterprise Linux System Administrator's Guide』を参照してください。



警告

Red Hat は、ローカルセキュリティの脆弱性が悪用される可能性があるため、RHVH で信頼できないユーザーを作成しないことを強くお勧めします。

7.3. RED HAT ENTERPRISE LINUX HOSTS

可能なハードウェアにインストールされた Red Hat Enterprise Linux 7 をホストとして使用することができます。Red Hat Virtualization は、Red Hat Enterprise Linux 7 Server AMD64/Intel 64 版の Intel VT

または AMD-V 拡張を実行するホストをサポートします。Red Hat Enterprise Linux マシンをホストとして使用するには、**Red Hat Enterprise Linux Server** エンタイトルメントと **Red Hat Virtualization** のエンタイトルメントも割り当てる必要があります。

仮想化チェック、パッケージのインストール、ブリッジの作成、およびホストの再起動など、プラットフォームによってホストの追加には時間がかかる場合があります。詳細ペインを使用して、ホストと管理システムが接続を確立するときにプロセスを監視します。



重要

サードパーティのウォッチドッグは、VDSM が提供するウォッチドッグデーモンに干渉する可能性があるため、Red Hat Enterprise Linux ホストにはインストールしないでください。

7.4. サテライトホストプロバイダーホスト

Satellite ホストプロバイダーによって提供されたホストは、Red Hat Virtualization Manager によって仮想化ホストとして使用することもできます。Satellite ホストプロバイダーが外部プロバイダーとして Manager に追加されると、そのプロバイダーが提供するホストは Red Hat Virtualization Hosts (RHVH) や Red Hat Enterprise Linux ホストと同じ方法で Red Hat Virtualization に追加して使用することができます。

7.5. ホストのタスク

7.5.1. Red Hat Virtualization Manager へのホストの追加

Red Hat Virtualization 環境にホストを追加するには、仮想化のチェック、パッケージのインストール、ブリッジの作成、およびホストの再起動など、プラットフォームによって完了するため、多少時間がかかる場合があります。詳細ペインを使用して、プロセスをホストとして監視し、Manager が接続を確立します。

手順7.1 Red Hat Virtualization Manager へのホストの追加

1. 管理ポータルから、**Hosts** resource タブをクリックします。
2. **New** をクリックします。
3. ドロップダウンリストを使用して、新規ホストの **Data Center** および **Host Cluster** を選択します。
4. 新規ホストの **名前** および **Address** を入力します。標準の SSH ポート 22 は、**SSH Port** フィールドに自動入力されます。
5. Manager がホストにアクセスするために使用する認証メソッドを選択します。
 - パスワード認証を使用するには、root ユーザーのパスワードを入力します。
 - または、**SSH PublicKey** フィールドに表示されるキーをホスト上の `/root/.ssh/authorized_keys` にコピーして、公開鍵認証を使用します。
6. **Advanced Parameters** ボタンをクリックして、高度なホスト設定を展開します。
 - a. オプションでファイアウォールの自動設定を無効にします

- b. 必要の応じてホストの SSH フィンガープリントを追加し、セキュリティーを強化する。手動での追加または自動取得が可能です。
7. オプションで、電源管理、SPM、コンソール、ネットワーク プロバイダー、および カーネルを設定します。詳細は、「[新規ホスト、ホスト編集ウィンドウの設定とコントロールの説明](#)」を参照してください。Hosted Engine は、セルフホストエンジンのデプロイメント用にホストのデプロイまたはアンデプロイ時に使用されます。
8. **OK** をクリックします。

新しいホストが **Installing** のステータスでホスト一覧に表示され、詳細ペインでインストールの進捗状況を確認できます。しばらくすると、ホストのステータスが Up に変わります。

7.5.2. サテライトホストプロバイダーhosztの追加

Satellite ホストプロバイダーのホストを追加するプロセスは、マネージャーでホストを識別する方法を除いて、Red Hat Enterprise Linux ホストを追加するプロセスとほぼ同じです。以下の手順では、サテライトホストプロバイダーが提供するホストを追加する方法について説明します。

手順7.2 サテライトホストプロバイダーhosztの追加

1. **Hosts** resource タブをクリックして、結果一覧のホストを一覧表示します。
2. **New** をクリックして、**New Host** ウィンドウを開きます。
3. ドロップダウンメニューを使用して、新規ホストの **Host Cluster** を選択します。
4. **Foreman/Satellite** チェックボックスを選択して、Satellite ホストプロバイダーhosztを追加するオプションを表示し、ホストを追加するプロバイダーを選択します。
5. **Discovered Hosts** または **Provisioned Hosts** を選択します。
 - **Discovered Hosts** (デフォルトオプション) : ドロップダウンリストからホスト、ホストグループ、およびコンピュートリソースを選択します。
 - **provisioned Hosts: Providers Hosts** ドロップダウンリストからホストを選択します。
6. 新規ホストの **Name**、**Address**、および **SSH Port** (Provisioned Hosts のみ)を入力します。
7. ホストで使用する認証方法を選択します。
 - パスワード認証を使用するには、root ユーザーのパスワードを入力します。
 - **SSH PublicKey** フィールドに表示されるキーをホスト上の `/root/.ssh/authorized_hosts` にコピーして、公開鍵認証を使用します (プロビジョニングされたホストのみ)。
8. これで、Red Hat Enterprise Linux ホストを追加するための必須手順が完了しました。**Advanced Parameters** ドロップダウンボタンをクリックして、高度なホスト設定を表示します。
 - a. オプションでファイアウォールの自動設定を無効にします
 - b. 必要の応じてホストの SSH フィンガープリントを追加し、セキュリティーを強化する。手動での追加または自動取得が可能です。

9. 現在該当するタブを使用して、**Power Management**、**SPM**、**Console**、および**Network Provider**を設定できます。ただし、これらは Red Hat Enterprise Linux ホストを追加する上で基本的ではないため、この手順では説明しません。
10. **OK**をクリックすると、ホストが追加され、ウィンドウが閉じます。

新しいホストが **Installing** のステータスでホスト一覧に表示され、詳細ペインでインストールの進捗状況を確認できます。インストールが完了すると、ステータスが **Reboot** に更新されます。ステータスが **Up** に変わるには、ホストが起動している必要があります。

7.5.3. ホストの Satellite エラータ管理の設定

Red Hat Virtualization は、Red Hat Satellite からエラータを表示するように設定できます。これにより、ホスト管理者は、ホスト設定の管理に使用されるのと同じダッシュボードで、利用可能なエラータとその重要性に関する更新を受け取ることができます。Red Hat Satellite の詳細は、Red Hat Satellite ユーザーガイド を参照してください。

Red Hat Virtualization 4.0 は、Red Hat Satellite 6.1 によるエラータ管理をサポートします。



重要

ホストは FQDN で Satellite サーバーで識別されます。IP アドレスを使用して追加したホストは、エラータを報告できません。これにより、Red Hat Virtualization で外部コンテンツホスト ID を維持する必要がなくなります。

ホストの管理に使用する Satellite アカウントには、Administrator 権限と、デフォルトの組織が設定されている必要があります。

手順7.3 ホストの Satellite エラータ管理の設定

1. 外部プロバイダーとして Satellite Server を追加します。詳細は、「[ホストのプロビジョニング用の Red Hat Satellite インスタンスの追加](#)」を参照してください。
2. 必要なホストを Satellite サーバーに関連付けます。



注記

ホストを Satellite Server に登録し、katello-agent パッケージがインストールされている必要があります。

ホスト登録の設定方法の詳細は、『Red Hat Satellite ユーザーガイド』の登録の [ためのホストの設定](#) を参照してください。ホストの登録および katello-agent パッケージのインストール方法は、『Red Hat Satellite ユーザーガイド』の [登録](#) を参照してください。

- a. ホストタブで、結果一覧でホストを選択します。
- b. **Edit**をクリックして **Edit Host** ウィンドウを開きます。
- c. **Use Foreman/Satellite** チェックボックスをオンにします。
- d. ドロップダウンリストから、必要な Satellite サーバーを選択します。
- e. **OK**をクリックします。

これで、ホストの設定を管理するための同じダッシュボードに、利用可能なエラッタとその重要性が表示されるようになりました。

7.5.4. 新規ホスト、ホスト編集ウィンドウの設定とコントロールの説明

7.5.4.1. ホストの一般設定の説明

これらの設定は、ホストの詳細を編集するとき、または新しい Red Hat Enterprise Linux ホストと Satellite ホストプロバイダー ホストを追加するときに適用されます。

General 設定の表には、**New Host** または **Edit Host** ウィンドウの **General** タブに必要な情報が含まれます。

表7.1一般的な設定

フィールド名	説明
Data Center	ホストが属するデータセンター。Red Hat Virtualization Host (RHVH)を Gluster 対応クラスターに追加することはできません。
Host Cluster	ホストが属するクラスター。

フィールド名	説明
Use Foreman/Satellite	<p>このチェックボックスを選択またはクリアすると、サテライトホストプロバイダーが提供するホストを追加するためのオプションが表示または非表示になります。以下のオプションを利用できます。</p> <p>検出されたホスト</p> <ul style="list-style-type: none"> ● 検出されたホスト: エンジンによって検出された Satellite ホストの名前が入力されたドロップダウンリストです。 ● ホストグループ - 利用可能なホストグループのドロップダウンリストです。 ● コンピュートリソース: コンピュートリソースを提供するハイパーバイザーのドロップダウンリストです。 <p>プロビジョニングされたホスト</p> <ul style="list-style-type: none"> ● Providers Hosts: 選択した外部プロバイダーが提供するホストの名前が入力されるドロップダウンリストです。このリストのエントリーは、プロバイダー検索フィルターで入力した検索クエリーに従ってフィルタリングされます。 ● プロバイダー検索フィルター: 選択した外部プロバイダーが提供するホストの検索を可能にするテキストフィールド。このオプションはプロバイダー固有です。特定のプロバイダーの検索クエリーの作成の詳細については、プロバイダーのドキュメントを参照してください。利用可能なすべてのホストを表示するには、このフィールドを空白にします。
Name	クラスターの名前。このテキストフィールドには 40 文字の制限があり、大文字、小文字、数字、ハイフン、およびアンダースコアの組み合わせが含まれる一意の名前である必要があります。
Comment	ホストに関するプレーンテキストで人間が読めるコメントを追加するためのフィールドです。
アドレス	ホストの IP アドレスまたは解決可能なホスト名。
Password	ホストの root ユーザーのパスワード。これは、ホストの追加時にのみ付与でき、後で編集することはできません。
SSH PublicKey	テキストボックスのコンテンツをホストの <code>/root/.known_hosts</code> ファイルにコピーし、パスワードを使用してホストで認証するのではなく、Manager の ssh キーを使用します。

フィールド名	説明
ホストのファイアウォールを自動的に設定	新規ホストを追加する場合、Manager はホストのファイアウォールで必要なポートを開くことができます。これはデフォルトで有効になっています。これは Advanced Parameter です。
SSH Fingerprint	ホストの SSH フィンガープリントを 取得 し、ホストが返すと予想されるフィンガープリントと比較し、一致することを確認します。これは Advanced Parameter です。

7.5.4.2. ホストパワーマネージメント設定の説明

電源管理 設定の表には、**New Host** または **Edit Host** ウィンドウの **Power Management** タブに必要な情報が含まれています。ホストにサポート対象の電源管理カードが搭載されている場合には、電源管理を設定することができます。

表7.2 電源管理 設定

フィールド名	説明
電源管理の有効化	ホストの電源管理を有効にする。 Power Management タブの残りのフィールドを有効にするには、このチェックボックスを選択します。
Kdump 統合	カーネルのクラッシュダンプの実行中にホストがフェンシングするのを防ぎ、クラッシュダンプが中断されないようにします。Red Hat Enterprise Linux 7.1以降では、デフォルトで kdump が利用できます。ホストで kdump が利用できるものの、その設定が有効でない場合(kdump サービスを開始できない)、 Kdump 統合 を有効にするとホスト（再）のインストールに失敗します。この場合は、 「fence_kdump の高度な設定」 を参照してください。
電源管理のポリシー制御を無効にする	電源管理は、ホストの クラスターのスケジューリングポリシー によって制御されます。パワーマネージメントが有効で、定義された低使用率の値に達した場合、マネージャーはホストマシンをパワードウンさせ、ロードバランシングが必要な場合や、クラスター内に十分な空きホストがない場合には、再びホストマシンを再起動させます。ポリシークトロールを無効にする場合は、このチェックボックスを選択します。

フィールド名	説明
順番待ちのエージェント	<p>ホストのフェンスエージェントを一覧表示します。フェンスエージェントには、シーケンシャル、コンカレント、またはその両方の組み合わせがあります。</p> <ul style="list-style-type: none"> フェンスエージェントが順次使用される場合、ホストの停止または起動にはまずプライマリーエージェントが使用され、それが失敗した場合にはセカンダリーエージェントが使用されます。 フェンスエージェントを同時に使用する場合、両方のフェンスエージェントが Stop コマンドに反応しなければホストは停止しませんが、一方のエージェントが Start コマンドに反応すればホストは立ち上がります。 <p>フェンスエージェントはデフォルトではシーケンシャルです。上下のボタンでフェンス剤の使用順序を変更できます。</p> <p>2つのフェンスエージェントを同時に作成するには、他のフェンスエージェントの横にある Concurrent with ドロップダウンリストからフェンスエージェントを1つ選択します。追加のフェンスエージェントの横にある Concurrent with ドロップダウンリストからグループを選択することにより、同時フェンスエージェントのグループに追加できます。</p>
フェンスエージェントの追加	プラス(+)ボタンをクリックして、新しいフェンスエージェントを追加します。 フェンスエージェントの編集 画面が開きます。このウィンドウのフィールドの詳細は、以下の表を参照してください。
電源管理プロキシープリファレンス	デフォルトでは、Manager がホストと同じ クラスター 内でフェンシングプロキシーを検索し、フェンシングプロキシーが見つからない場合は、同じ dc (データセンター) で検索するように指定します。上下のボタンで、これらのリソースの使用順序を変更することができます。このフィールドは、 Advanced Parameters で利用できます。

次の表は、**Edit fence agent** ウィンドウで必要な情報です。

表7.3 フェンスエージェント設定の編集

フィールド名	説明
アドレス	ホストの電源管理デバイスにアクセスするためのアドレス。解決可能なホスト名または IP アドレスのいずれか。
User Name	電源管理デバイスにアクセスするユーザー アカウント。デバイスにユーザーを設定するか、デフォルトのユーザーを使用します。

フィールド名	説明
Password	電源管理デバイスにアクセスするユーザーのパスワード。
タイプ	<p>ホストの電源管理デバイスのタイプ。</p> <p>以下のいずれかを選択します。</p> <ul style="list-style-type: none"> ● apc: APC MasterSwitch ネットワーク電源スイッチ。APC 5.x 電源スイッチデバイスとは使用しないでください。 ● apc_snmp - APC 5.x 電源スイッチデバイスで使用します。 ● アーキテクトセンター: IBM thecenter Remote Supervisor Adapter。 ● cisco_ucs: Cisco Unified Computing System。 ● drac5: Dell コンピューター用の Dell Remote Access Controller。 ● drac7: Dell コンピューター用の Dell Remote Access Controller。 ● eps: ePowerSwitch 8M+ ネットワーク電源スイッチ。 ● hpblade - HPPathParamSystem. ● iLO , ilo2,ilo3,ilo4 - HP Integrated Lights-Out。 ● ipmilan: Intelligent Platform Management Interface および Sun Integrated Lights Out Management デバイス。 ● RSA - IBM Remote Supervisor アダプター。 ● rsb - Fujitsu-Siemens RSB 管理インターフェイス。 ● wti: WTI ネットワーク電源スイッチ。
ポート	電源管理デバイスがホストとの通信に使用するポート番号。
Slot	電源管理デバイスのブレードを識別するための番号。
Service Profile	電源管理デバイスのブレードを識別するために使用されるサービスプロファイル名です。デバイスタイプが cisco_ucs の場合、 Slot の代わりにこのフィールドが表示されます。

フィールド名	説明
オプション	電源管理デバイス固有のオプション。これらを key=value として入力します。利用可能なオプションは、お使いのホストの電源管理デバイスのドキュメントを参照してください。
Secure	Red Hat Enterprise Linux 7 ホストの場合は、電源管理デバイスとして cisco_ucs を使用している場合は、 Options フィールドに ssl_insecure=1 を追加する必要があります。

7.5.4.3. SPM のプライオリティー設定の説明

SPM 設定の表には、 **New Host** または **Edit Host** ウィンドウの **SPM** タブに必要な情報の詳細が記載されています。

表7.4 SPM の設定

フィールド名	説明
SPM の優先度	ホストにストレージプールマネージャー (SPM) のロールが与えられる可能性を定義します。オプションは、 Low 、 Normal 、および High priority です。優先度が低いとは、ホストに SPM のロールが割り当てられる可能性が低いことを意味し、優先度が高いとは、その可能性が高いことを意味しています。デフォルト設定は Normal です。

7.5.4.4. ホストクラスター設定の説明

Console 設定の表には、 **New Host** または **Edit Host** ウィンドウの **Console** タブに必要な情報の詳細が記載されています。

表7.5 コンソールの設定

フィールド名	説明
表示アドレスの上書き	ホストの表示アドレスを上書きする場合は、このチェックボックスを選択します。この機能は、ホストが内部 IP で定義されており、NAT ファイアウォールの内側にある場合に有効です。ユーザーが内部ネットワークの外から仮想マシンに接続した場合、仮想マシンが動作しているホストのプライベートアドレスを返すのではなく、パブリック IP または FQDN(外部ネットワークではパブリック IP に解決される)を返します。

フィールド名	説明
表示アドレス	ここで指定した表示アドレスは、このホスト上で動作するすべての仮想マシンに使用されます。アドレスは、完全修飾ドメイン名または IP の形式でなければなりません。

7.5.4.5. ネットワークプロバイダー設定の説明

ネットワークプロバイダー 設定の表には、**New Host** または **Edit Host** ウィンドウの **Network Provider** タブに必要な情報の詳細が記載されています。

表7.6 ネットワークプロバイダーの設定

フィールド名	説明
外部ネットワークプロバイダー	外部ネットワークプロバイダーを追加し、ホストのネットワークを外部ネットワークプロバイダーによってプロビジョニングする場合は、一覧から1つ選択します。

7.5.4.6. カーネル設定の説明

カーネル 設定の表には、**New Host** または **Edit Host** ウィンドウの **Kernel** タブに必要な情報の詳細が記載されています。一般的なカーネルブートパラメーターのオプションはチェックボックスで表示されるので、簡単に選択することができます。より複雑な変更については、**カーネルコマンドライン** の横にあるフリーテキストエントリーフィールドを使用して、必要な追加パラメーターを追加します。



重要

ホストがすでに Manager に接続されている場合は、変更を適用する前にホストをメンテナンスモードに切り替えるようにしてください。**Reinstall** をクリックしてホストを再インストールし、再インストールの完了後にホストを再起動して変更を反映する必要があります。

表7.7 カーネル 設定

フィールド名	説明
Hostdev パススルーおよび SR-IOV	カーネルの IOMMU フラグを有効にして、デバイスが仮想マシン自体に直接アタッチされているデバイスであるかのように、ホストデバイスを仮想マシンで使用できるようにします。また、ホストのハードウェアとファームウェアも IOMMU に対応している必要があります。ハードウェア上で仮想化拡張機能と IOMMU 拡張機能が有効になっている必要があります。『インストールガイド』の Configuring a Host for PCI Passthrough を参照してください。IBM POWER8 では、デフォルトで IOMMU が有効になっています。

フィールド名	説明
Nested Virtualization	vmx フラグまたは svm フラグを有効にして、仮想マシン内で仮想マシンを実行できるようにします。このオプションは評価目的のみで、実稼働での使用はサポートされません。 vdsm-hook-nestedvtp フックはホストにインストールされている必要があります。
安全でない割り込み	IOMMU が有効になっているが、ハードウェアが割り込みの再マッピングをサポートしていないためにパススルーが失敗する場合は、このオプションを有効にすることを検討できます。このオプションは、ホスト上の仮想マシンが信頼できる場合にのみ有効にしてください。このオプションを有効にすると、仮想マシンからの MSI 攻撃を受ける可能性があります。このオプションは、評価目的で認定されていないハードウェアを使用する場合のみ、回避策として使用することを目的としています。
PCI 再割り当て	メモリーの問題で SR-IOV NIC が仮想機能を割り当てられない場合は、このオプションを有効にすることを検討してください。また、ホストのハードウェアとファームウェアが PCI の再配置をサポートしている必要があります。このオプションは、評価目的で認定されていないハードウェアを使用する場合のみ、回避策として使用することを目的としています。
カーネルコマンドライン	このフィールドでは、デフォルトのパラメーターにさらにカーネルパラメーターを追加することができます。



注記

カーネルブートパラメーターがグレーアウトしている場合は、**reset** ボタンをクリックすると、オプションが利用可能になります。

7.5.4.7. ホストエンジン設定の説明

Hosted Engine 設定の表には、**New Host** または **Edit Host** ウィンドウの **Hosted Engine** タブに必要な情報の詳細が記載されています。

表7.8 ホストエンジンの設定

フィールド名	説明
--------	----

フィールド名	説明
ホストされたエンジンの展開方法を選択	<p>利用可能な 3 つのオプションは以下のとおりです。</p> <ul style="list-style-type: none"> ● none: 必要なアクションはありません。 ● デプロイ: ホストをセルフホストエンジンノードとしてデプロイする場合は、このオプションを選択します。 ● undeploy: セルフホストエンジンノードの場合、このオプションを選択してホストをアンデプロイし、セルフホスト型エンジン関連の設定を削除できます。

7.5.5. ホストパワーマネージメントの設定

管理ポータルからホストのライフサイクル操作(停止、開始、再起動)を行うために、ホストパワーマネージメントデバイスの設定を行います。

ホストの高可用性と仮想マシンの高可用性を利用するには、ホストの電源管理を設定する必要があります。

重要

電源管理設定を設定する前に、ホストがメンテナーンスマードにあることを確認します。そうしないと、ホストの再起動時に、そのホストで実行しているすべての仮想マシンが正常に停止されるため、実稼働環境で中断が生じる可能性があります。ホストをメンテナーンスマードに正しく設定していない場合は、警告ダイアログが表示されます。

手順7.4 電源管理状態の設定

1. ホストタブで、結果一覧でホストを選択します。
2. **Edit** をクリックして **Edit Host** ウィンドウを開きます。
3. **Power Management** タブをクリックして、電源管理設定を表示します。
4. **Enable Power Management** チェックボックスを選択してフィールドを有効にします。
5. **Kdump integration** チェックボックスを選択して、カーネルクラッシュダンプの実行中にホストがフェンシングされないようにします。

重要

既存のホストで **Kdump 統合** を有効にする場合は、kdump を設定するためにホストを再インストールする必要があります。「[ホストの再インストール](#)」を参照してください。

6. オプションで、ホストの電源管理をホストの **クラスターのスケジューリング** ポリシーで制御したくない場合は、**Disable policy control of power management** チェックボックスを選択します。

7. プラス(+)ボタンをクリックして、新しい電源管理デバイスを追加します。フェンスエージェントの編集画面が開きます。
8. 電源管理デバイスの **Address**、**User Name**、**Password** を適切なフィールドに入力します。
9. ドロップダウンリストから電源管理デバイスの **種類** を選択します。
10. ホストとの通信に電源管理デバイスが使用する **SSH Port** 番号を入力します。
11. 電源管理デバイスのブレードを識別するために使用される **Slot** 番号を入力します。
12. 電源管理デバイスのオプションを入力します。*key=value* エントリーのコンマ区切りリストを使用します。
13. 電源管理デバイスがホストに安全に接続できるようにするには、**Secure** チェックボックスを選択します。
14. **Test** をクリックして、設定が正しいことを確認します。検証に成功すると、**Test Succeeded**、**Host Status is: on** が表示されます。
15. **OK** をクリックして、**Edit fence agent** ウィンドウを閉じます。
16. 電源管理タブで、オプションで詳細パラメーターを展開し、上下のボタンを使用して、Manager がホストのクラスターと dc (データセンター) でフェンシングプロキシーを検索する順序を指定します。
17. **OK** をクリックします。

これで、管理ポータルで **Power Management** ドロップダウンメニューが有効になります。

7.5.6. ホストストレージプールマネージャーの設定

ストレージプールマネージャー (SPM) は、データセンター内のホストの1つに与えられた管理者のロールで、ストレージドメインへのアクセス制御を維持します。SPM は常に利用可能でなければならず、SPM ホストが利用できなくなった場合、SPM ロールは別のホストに割り当てられます。SPM ロールはホストの利用可能なリソースの一部を使用するため、リソースに余裕のあるホストに優先順位を付けることが重要です。

ホストの SPM (Storage Pool Manager) 優先度の設定により、ホストが SPM ロールが割り当たる可能性があります。SPM 優先度が高いホストには、SPM の優先度が低いホストの前に SPM ロールが割り当たされます。

手順7.5 SPM 設定の設定

1. **Hosts** resource タブをクリックし、結果リストからホストを選択します。
2. **Edit** をクリックして **Edit Host** ウィンドウを開きます。
3. **SPM** タブをクリックして、SPM の **優先度** 設定を表示します。
4. ラジオボタンで、ホストに適した SPM の優先順位を選択します。
5. **OK** をクリックして設定を保存し、ウィンドウを閉じます。

ホストの SPM 優先度を設定している。

7.5.7. ホストのメンテナンスモードへの切り替え

ネットワークの設定やソフトウェアの更新など、一般的なメンテナンス作業では、ホストをメンテナンスモードにする必要があります。ホストは、再起動、ネットワークやストレージの問題など、VDSM が正常に動作しなくなる可能性があるイベントが発生する前に、メンテナンスモードにする必要があります。

ホストがメンテナンスモードになると、Red Hat Virtualization Manager は実行中のすべての仮想マシンを代替ホストに移行しようとします。ライブマイグレーションの標準的な前提条件が適用されます。特に、移行した仮想マシンを実行する能力を持つアクティブなホストが、クラスター内に少なくとも1つ存在する必要があります。

手順7.6 ホストのメンテナンスモードへの移行

1. **Hosts** resource タブをクリックし、目的のホストを選択します。
2. **Maintenance** をクリックして、メンテナーンスホストの確認ウィンドウを開きます。
3. 必要に応じて、**Maintenance Host (s)** 確認ウィンドウでホストをメンテナンスモードに移行する理由を入力します。これにより、ログに表示されるメンテナンスの説明と、ホストが再度アクティベートされたタイミングを指定できます。



注記

ホストメンテナーンス 理由 フィールドは、クラスター設定で有効になっている場合にのみ表示されます。詳細は、「一般的なクラスター設定に関する説明」を参照してください。

4. **OK** をクリックしてメンテナンスモードを開始します。

稼働中の仮想マシンはすべて代替ホストに移行されます。ホストが Storage Pool Manager (SPM) の場合、SPM のロールは別のホストに移行されます。ホストの **Status** フィールドは **Preparing for Maintenance** に変わり、操作が正常に完了すると最終的に **Maintenance** に変わります。ホストがメンテナンスモードになっても、VDSM は停止しません。



注記

いずれかの仮想マシンで移行に失敗した場合は、ホストで **Activate** をクリックして操作を停止し、メンテナンスモードにする操作を停止し、仮想マシンで **Cancel Migration** をクリックして移行を停止します。

7.5.8. メンテナンスモードからホストを起動する

メンテナンスモードになったホストや、最近環境に追加されたホストは、使用する前にアクティベートする必要があります。ホストの準備ができていないと、アクティベーションに失敗することがあります。ホストのアクティベーションを試みる前に、すべてのタスクが完了していることを確認してください。

手順7.7 メンテナンスモードからホストを起動する

1. ホストリソース タブをクリックし、ホストを選択します。
2. **Activate** をクリックします。

操作が完了すると、ホストの状態は **Unassigned** に変わり、最後に **Up** となります。仮想マシンがホス

ト上で動作するようになりました。メンテナンスモード時にホストから移行された仮想マシンは、ホストが起動したときに自動的には戻ってきませんが、手動で移行することができます。メンテナンスモードに移行する前にホストがストレージプールマネージャー (SPM) であった場合、ホストがアクティブになっても SPM のロールは自動的には戻りません。

7.5.9. ホストの削除

仮想化環境からホストを削除します。

手順7.8 ホストの削除

1. 管理ポータルで **Hosts** resource タブをクリックし、結果一覧でホストを選択します。
2. ホストをメンテナンスモードにします。
3. **Remove** をクリックして、**Remove Host (s)** 確認ウィンドウを開きます。
4. ホストが Red Hat Gluster Storage クラスターに含まれており、ボリュームブリックがある場合、またはホストが応答しない場合は、**Force Remove** チェックボックスを選択します。
5. **OK** をクリックします。

ホストが環境から削除され、ホストタブに表示されなくなりました。

7.5.10. マイナーリリース間でのホストの更新

ホストをマイナーリリース間で維持する方法については、アップグレードガイドの以下のセクションを参照し https://access.redhat.com/documentation/en/red-hat-virtualization/4.0/single/upgrade-guide/#chap-Updates_between_Minor_Releases てください。

7.5.11. ホストの再インストール

管理ポータルから Red Hat Virtualization Host (RHVH) および Red Hat Enterprise Linux ホストを再インストールします。この手順には、ホストの停止および再起動が含まれます。移行がクラスターレベルで有効にされている場合、仮想マシンはクラスター内の別のホストに自動的に移行されるため、ホストの使用が比較的低いときにホストの再インストールを実行することが推奨されます。

ホストが属するクラスターには、ホストがメンテナーンスを実行するために十分なメモリーが予約されている必要があります。ライブ仮想マシンを持つホストを、十分なメモリーがないクラスター内のメンテナーンスに移動すると、仮想マシンの移行操作がハングしてから失敗します。一部またはすべての仮想マシンをシャットダウンしてから、ホストをメンテナーンスに移行すると、この操作のメモリー使用量を減らすことができます。



重要

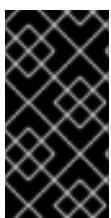
再インストールを実行する前に、クラスターに複数のホストが含まれていることを確認してください。Storage Pool Manager (SPM) のタスクを実行するには、1台のホストは使用可能な状態でなければならないので、すべてのホストを同時に再インストールしないでください。

手順7.9 Red Hat Virtualization Host または Red Hat Enterprise Linux ホストの再インストール

1. ホストリソース タブ、ツリーモード、または検索機能を使用して、結果一覧でホストを見つけて選択します。

2. **Maintenance** をクリックします。クラスターレベルで移行が有効になっている場合、ホストで実行されているすべての仮想マシンが他のホストに移行されます。ホストが SPM の場合、この機能は別のホストに移動します。メンテナーヌスモードになると、ホストのステータスが変わります。
3. **Reinstall** をクリックして、**Install Host** ウィンドウを開きます。
4. **OK** をクリックして、ホストを再インストールします。

正常に再インストールされると、ホストは **Up** のステータスを表示します。ホストから移行されたすべての仮想マシンは、この時点で移行することができます。



重要

Red Hat Virtualization Host が Red Hat Virtualization Manager に正常に登録されて再インストールされると、ステータスが **Install Failed** の状態で管理ポータルに誤って表示される可能性があります。**Activate** をクリックします。ホストは **Up** ステータスに変わり、使用できる状態になります。

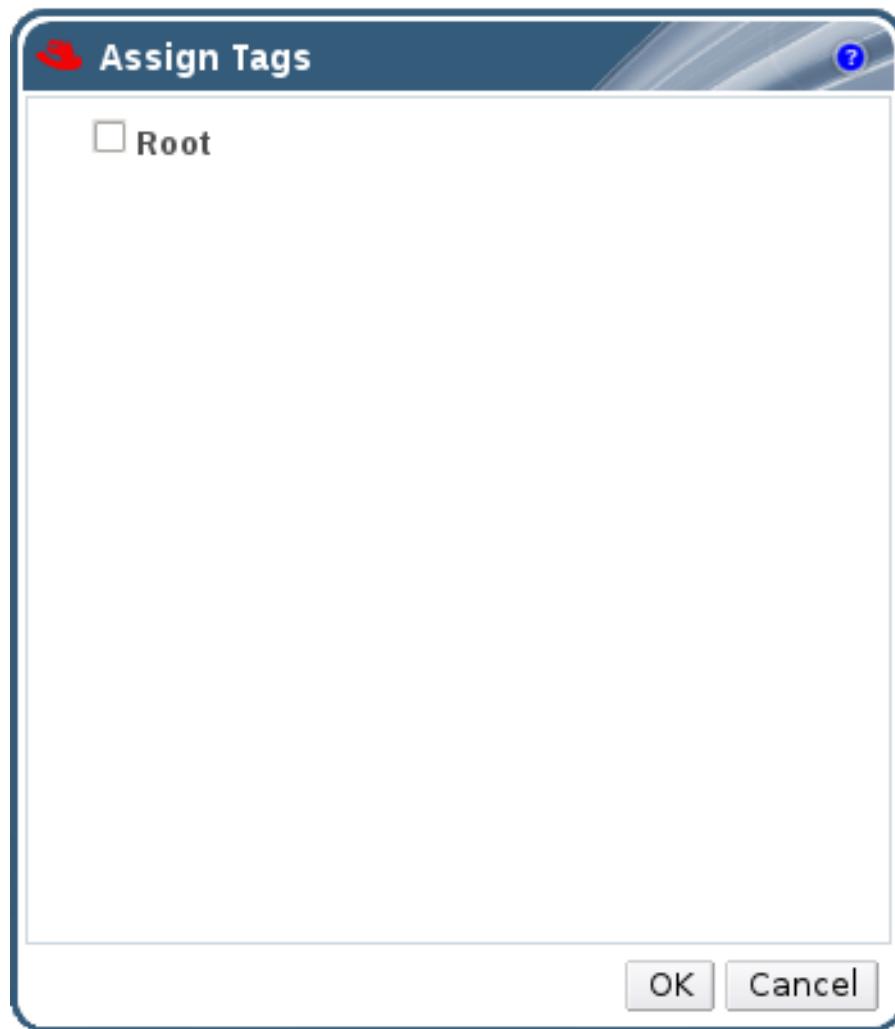
7.5.12. タグを使用したホストのカスタマイズ

タグを使用してホストに関する情報を保存できます。その後、タグに基づいてホストを検索できます。

手順7.10 タグを使用したホストのカスタマイズ

1. ホストリソース タブ、ツリーモード、または検索機能を使用して、結果一覧でホストを見つけて選択します。
2. **Assign Tags** をクリックして **Assign Tags** ウィンドウを開きます。

図7.1 Assign Tags ウィンドウ



3. **Assign Tags** ウィンドウには、利用可能なすべてのタグが一覧表示されます。該当するタグのチェックボックスを選択します。
4. **OK** をクリックしてタグを割り当て、ウィンドウを閉じます。

ホストに関する検索可能な追加情報がタグとして追加されます。

7.5.13. ホスト Errata の表示

各ホストの Errata は、Red Hat Satellite サーバーから Errata 情報を受信するようにホストが設定された後に表示されます。ホストを設定してエラータ情報を取得する方法の詳細は、「[ホストの Satellite エラータ管理の設定](#)」を参照してください。

手順7.11 ホスト Errata の表示

1. **Hosts** resource タブをクリックし、結果リストからホストを選択します。
2. 詳細ペインの **General** タブをクリックします。
3. **General** タブの **Errata** サブタブをクリックします。

7.5.14. ホストのヘルスステータスの表示

ホストは、通常のステータスに加えて、外部のヘルスステータスを持ちます。外部の正常性ステータスはプラグインまたは外部システムによって報告されるか、管理者が設定し、ホストの **Name** の左側に以下のいずれかのアイコンとして表示されます。

- **OK:** No icon

- **情報:** 

- **警告:** 

- **エラー:** 

- **失敗:** 

ホストのヘルスステータスの詳細を表示するには、ホストを選択し、イベントサブタブをクリックします。

また、REST API を使用してホストのヘルスステータスを表示することもできます。ホストの **GET** リクエストには、ヘルスステータスを含む **external_status** 要素が含まれます。

REST API では、**events** コレクションを介してホストのヘルスステータスを設定できます。詳細は、『REST API Guide』の [Adding Events](#) を参照してください。

7.5.15. ホストデバイスの表示

詳細ペインで、各ホストのホストデバイスを表示できます。ホストにデバイスの直接割り当てが設定されている場合、これらのデバイスを仮想マシンに直接接続してパフォーマンスを向上させることができます。

直接デバイス割り当てのハードウェア要件の詳細は、『Red Hat Virtualization Hardware Considerations for Implementing SR-IOV』の [Additional Hardware Considerations for Using Device Assignment](#) を参照してください。

直接デバイスを割り当てるようにホストを設定する方法は、『インストールガイド』の [PCI パススルー用のホストの設定](#) を参照してください。

仮想マシンにホストデバイスを割り当てる方法は、『Virtual Machine Management Guide』の [Host Devices](#) を参照してください。

手順7.12 ホストデバイスの表示

1. ホストリソースタブ、ツリーモード、または検索機能を使用して、結果リストからホストを見つけて選択します。
2. 詳細ペインの **ホストデバイス** タブをクリックします。

詳細ペインには、デバイスが仮想マシンに接続されているかどうか、およびその仮想マシンで現在使用されているかどうかなど、ホストデバイスの詳細が表示されます。

7.5.16. GPU パススルーホストおよびゲストシステムの準備

ホストからの Graphics Processing Unit (GPU) デバイスは、仮想マシンに直接割り当てるできます。これを実現する前に、ホストと仮想マシンの両方に **grub** 設定ファイルに修正が必要です。管理ポータルの **カーネルコマンドライン** のフリーテキストエントリーフィールドを使用して、ホスト **grub**

設定ファイルを編集できます。変更を反映するには、ホストマシンと仮想マシンの両方を再起動する必要があります。

この手順は、x86_64 または ppc64le アーキテクチャーのいずれかのホストに関連しています。

直接デバイス割り当てのハードウェア要件の詳細は、『インストールガイド』の [PCI デバイス要件](#) を参照してください。



重要

ホストがすでに Manager に接続されている場合は、変更を適用する前にホストをメンテナンスマードに切り替えるようにしてください。

手順7.13 GPU パススルー用ホストの準備

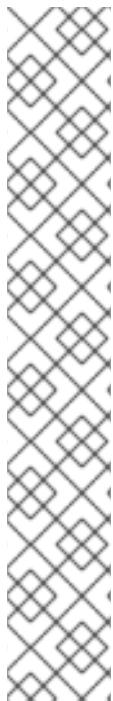
1. 管理ポータルからホストを選択します。
2. 詳細ペインの **General** タブをクリックし、**Hardware** をクリックします。GPU デバイス ベンダー ID: 製品 ID を見つけます。この例では、ID は **10de:13ba** および **10de:0fbc** です。
3. ホストを右クリックし、**Edit** を選択します。**Kernel** タブをクリックします。
4. **Kernel command line** free text entry フィールドに、前の手順で配置した ID を入力します。

```
pci-stub.ids=10de:13ba,10de:0fbc
```

5. ホスト上の対応するドライバーをブラックリストに指定します。たとえば、*pci-stub.ids=xxxx:xxxx* の横にある nVidia の nouveau ドライバーをブラックリストに登録するには、**rdblacklist=nouveau** を入力します。

```
pci-stub.ids=10de:13ba,10de:0fbc rdblacklist=nouveau
```

6. **OK** をクリックして変更を保存します。
7. **Reinstall** をクリックして、ホストへの変更をコミットします。
8. 再インストールが完了したら、ホストを再起動します。



注記

デバイスが **pci-stub** ドライバーにバインドされていることを確認するには、**lspci** コマンドを実行します。

```
# lspci -nnk
...
01:00.0 VGA compatible controller [0300]: NVIDIA Corporation GM107GL [Quadro K2200] [10de:13ba] (rev a2)
    Subsystem: NVIDIA Corporation Device [10de:1097]
    Kernel driver in use: pci-stub
01:00.1 Audio device [0403]: NVIDIA Corporation Device [10de:0fb] (rev a1)
    Subsystem: NVIDIA Corporation Device [10de:1097]
    Kernel driver in use: pci-stub
...
```

grub 設定ファイルを手動で編集して上記の変更を行う方法は、3.6 『Administration Guide』 の [Preparing Host and Guest Systems for GPU Passthrough](#) を参照してください。

次の手順に従って、ゲストシステム側で GPU パススルーを設定します。

手順7.14 GPU パススルー用のゲスト仮想マシンの準備

- ○ Linux の場合

- a. プロプライエタリー GPU ドライバーのみがサポートされます。**grub** 設定ファイルで、対応するオープンソースドライバーをブラックリストに指定します。以下に例を示します。

```
$ vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... rdblacklist=nouveau"
...
```

- b. GPU BusIDを見つけます。この例では、BusIDが00:**09.0**です。

```
# lspci | grep VGA
00:09.0 VGA compatible controller: NVIDIA Corporation GK106GL [Quadro K4000] (rev a1)
```

- c. **/etc/X11/xorg.conf** ファイルを編集し、以下の内容を追加します。

```
Section "Device"
Identifier "Device0"
Driver "nvidia"
VendorName "NVIDIA Corporation"
BusID "PCI:0:9:0"
EndSection
```

- d. 仮想マシンを再起動します。

- Windows の場合

- a. デバイスに対応するドライバーをダウンロードしてインストールします。たとえば、Nvidia ドライバーの場合は、[NVIDIA Driver Downloads](#) に移動します。
- b. 仮想マシンを再起動します。

ホスト GPU を準備済み仮想マシンに直接割り当てるようになります。仮想マシンにホストデバイスを割り当てる方法は、『Virtual Machine Management Guide』の [Host Devices](#) を参照してください。

7.5.17. 管理ポータルからのコックピットへのアクセス

Cockpit UI プラグインは、Red Hat Virtualization 環境にインストールできるオプションの機能です。このプラグインは、管理ポータルからホストリソースの監視および管理に使用される Cockpit ユーザーインターフェイスへのアクセスを提供します。Cockpit がインストールされているホストを選択すると、**Cockpit** サブタブに Cockpit ユーザーインターフェイスが管理ポータルの詳細ペインに直接表示されます。または、メインの **Hosts** メニューの **Cockpit** ボタンにより、新しいブラウザタブに Cockpit ユーザーインターフェイスが開きます。

Cockpit ユーザーインターフェイスは、Red Hat Virtualization Host (RHVH) ではデフォルトで利用可能です。現在、Red Hat Enterprise Linux ホストではサポートされません。

手順7.15 管理ポータルからのコックピットへのアクセス

1. Manager マシンに Cockpit UI プラグインをインストールします。

```
# yum install cockpit-ovirt-uiplugin
```

2. **ovirt-engine** サービスを再起動します。

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

3. 管理ポータルで ホスト タブをクリックして、ホストを選択します。

4. 新しいタブで Cockpit ユーザーインターフェイスを開くか、管理ポータルから直接表示します。
 - ホストを右クリックし、**Cockpit** を選択して、新しいブラウザタブで Cockpit ユーザーインターフェイスを開きます。
 - **Cockpit** サブタブをクリックし、**Hosts** タブの詳細ペインで Cockpit ユーザーインターフェイスを表示します。



注記

選択したホストで Cockpit が利用できない場合、Cockpit サブタブには基本的なトラブルシューティング手順が表示されます。

7.6. ホストの耐障害性

7.6.1. 高可用性

Red Hat Virtualization Manager はフェンシングを使用して、クラスター内のホストの応答を維持します。**Non Responsive** ホストは、**Non operational** ホストとは異なります。**非操作** ホストは、Manager

が通信できますが、論理ネットワークの欠落など、設定が正しくありません。Non Responsive ホストは、Manager が通信できません。

電源管理デバイスを備えたホストが Manager との通信を失った場合、管理ポータルからフェンス（再起動）できます。そのホストで実行されているすべての仮想マシンが停止し、高可用性仮想マシンが別のホストで起動します。

すべての電源管理操作は、Red Hat Virtualization Manager によって直接行われるのではなく、プロキシホストを使用して行われます。電源管理操作には、少なくとも 2 台のホストが必要です。

フェンシングにより、クラスターは予期しないホスト障害に対応できるだけでなく、省電力、負荷分散、および仮想マシンの可用性ポリシーを適用できます。ホストの電源管理デバイスのフェンシングパラメーターを設定し、時々その正確性をテストする必要があります。

ホストは、電源管理パラメーターを使用して自動的にフェンシングすることも、ホストを右クリックしてメニューのオプションを使用することで手動でフェンシングすることもできます。フェンシング操作では、応答しないホストが再起動され、ホストが規定された時間内にアクティブな状態に戻りない場合は、保留中の手動介入およびトラブルシューティングが応答しないままになります。

高可用性の仮想マシンを実行する必要がある場合は、電源管理を有効にして設定する必要があります。

7.6.2. Red Hat Virtualization の Proxy による電源管理

Red Hat Virtualization Manager は、フェンスエージェントと直接通信しません。その代わりに、Manager はプロキシーを使用してホストの電源管理デバイスに電源管理コマンドを送信します。Manager は VDSM を使用してパワーマネジメントデバイスのアクションを実行するため、環境内の別のホストをフェンシングプロキシーとして使用しています。

以下で選択することができます。

- フェンシングが必要なホストと同じクラスター内の任意のホスト。
- フェンシングが必要なホストと同じデータセンターにあるすべてのホスト。

実行可能なフェンシングプロキシホストのステータスは UP または Maintenance のいずれかです。

7.6.3. ホストでのフェンシングパラメーターの設定

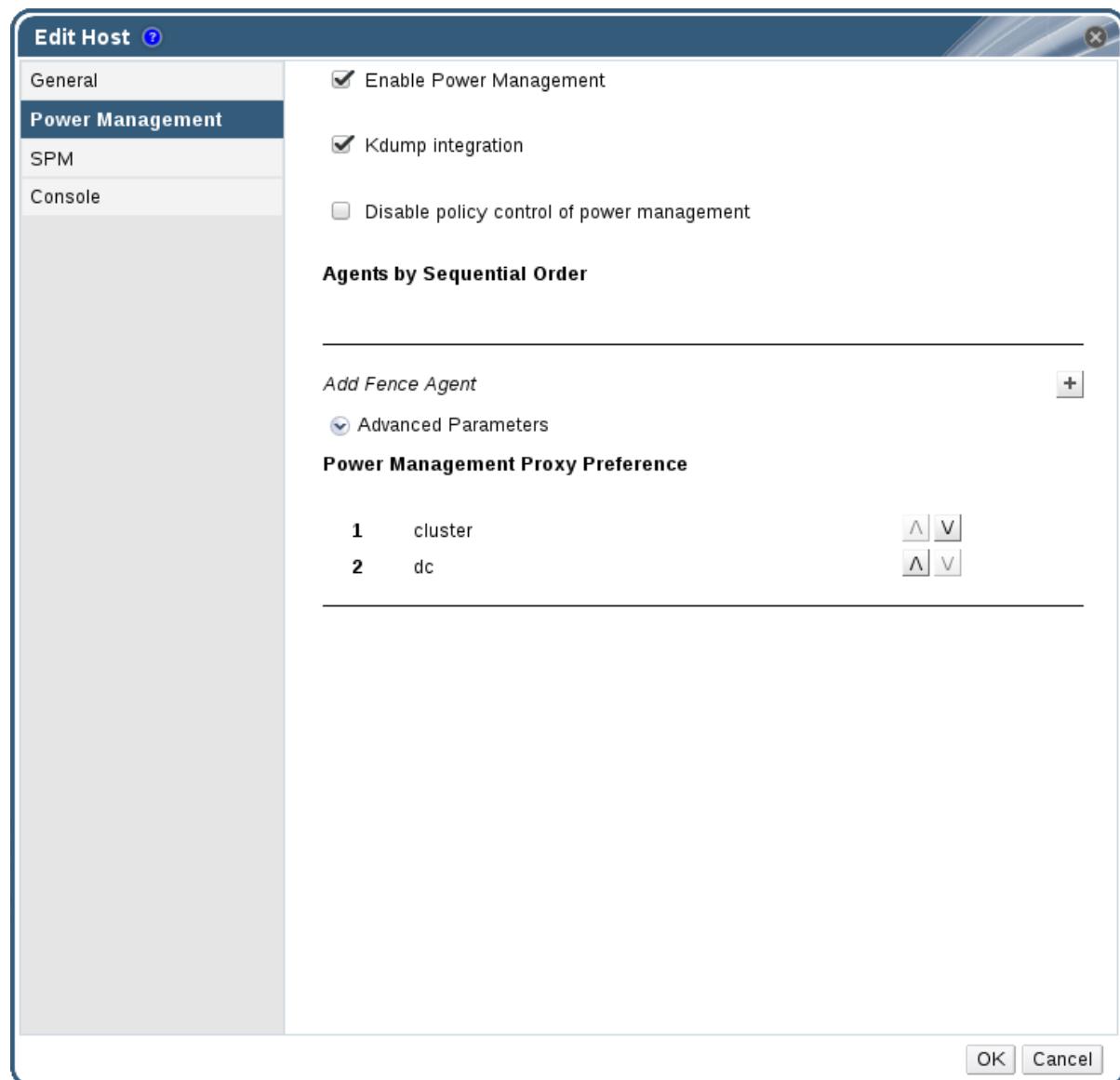
ホストフェンシングのパラメーターは、**New Host** または **Edit Host** ウィンドウの **Power Management** フィールドを使用して設定されます。パワーマネジメントは、RAC (Remote Access Card) などの追加インターフェイスを使って、システムがトラブルのあるホストをフェンスすることを可能にします。

すべての電源管理操作は、Red Hat Virtualization Manager によって直接行われるのではなく、プロキシホストを使用して行われます。電源管理操作には、少なくとも 2 台のホストが必要です。

手順7.16 ホストでのフェンシングパラメーターの設定

1. ホストリソース タブ、ツリーモード、または検索機能を使用して、結果一覧でホストを見つけて選択します。
2. **Edit** をクリックして **Edit Host** ウィンドウを開きます。
3. **Power Management** タブをクリックします。

図7.2 電源管理設定



4. **Enable Power Management** チェックボックスを選択してフィールドを有効にします。
5. **Kdump integration** チェックボックスを選択して、カーネルクラッシュダンプの実行中にホストがフェンシングされないようにします。

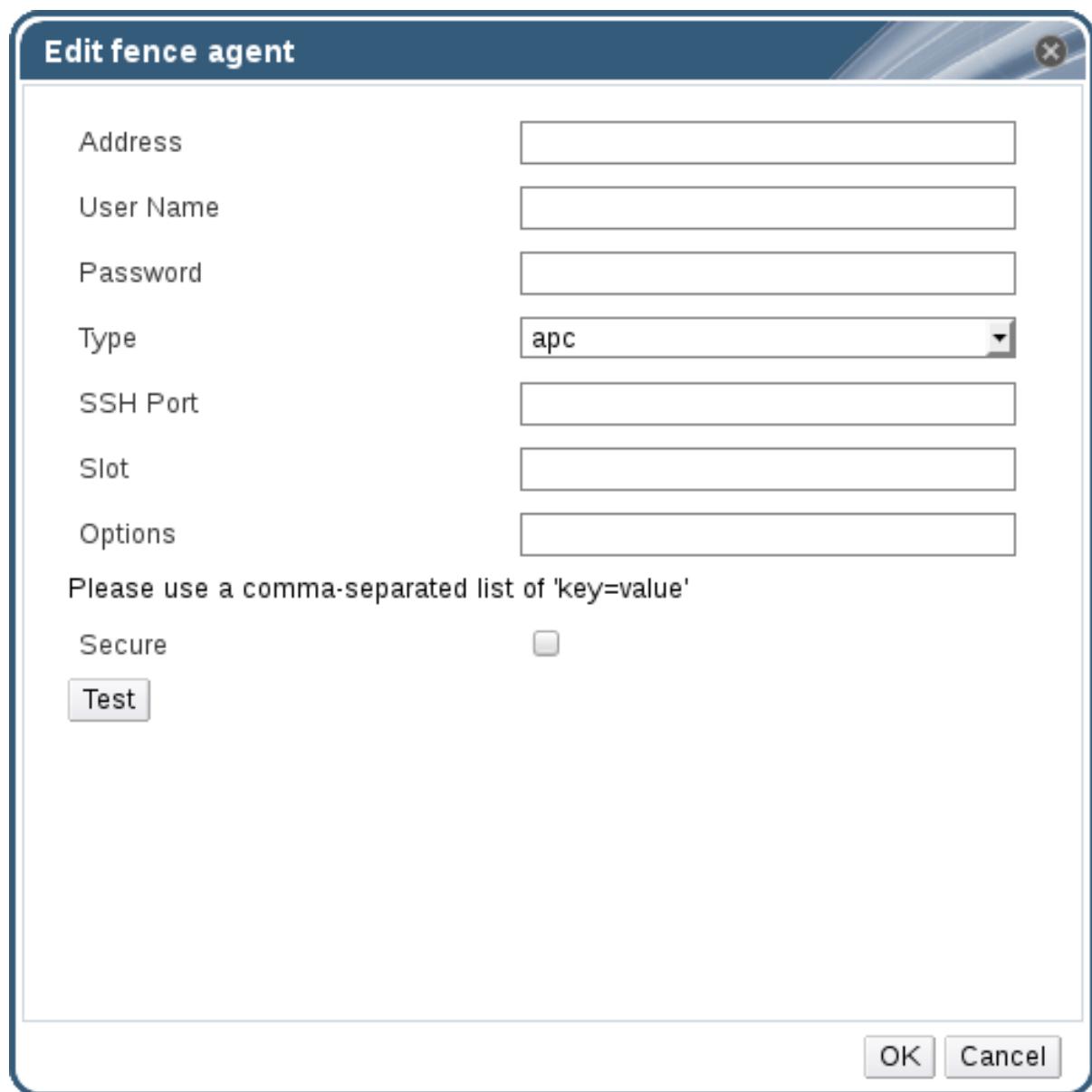


重要

既存のホストで **Kdump 統合** を有効にする場合は、kdump を設定するためにホストを再インストールする必要があります。 「[ホストの再インストール](#)」を参照してください。

6. オプションで、ホストの電源管理をホストのクラスターの **スケジューリング** ポリシーで制御したくない場合は、**Disable policy control of power management** チェックボックスを選択します。
7. プラス(+)ボタンをクリックして、新しい電源管理デバイスを追加します。 **フェンスエージェントの編集** 画面が開きます。

図7.3 フェンスエージェントの編集



8. 電源管理デバイスの アドレス、ユーザー名、および パスワード を入力します。

9. ドロップダウンリストから電源管理デバイスの 種類 を選択します。



注記

カスタムの電源管理デバイスの設定方法は、を参照してください
<https://access.redhat.com/articles/1238743>。

10. ホストとの通信に電源管理デバイスが使用する **SSH Port** 番号を入力します。

11. 電源管理デバイスのブレードを識別するために使用される **Slot** 番号を入力します。

12. 電源管理 デバイスのオプション を入力します。key=value エントリーのコンマ区切りリストを使用します。

13. 電源管理デバイスがホストに安全に接続できるようにするには、**Secure** チェックボックスを選択します。

14. テスト ボタンをクリックして、設定が正しいことを確認します。検証に成功すると、Test Succeeded、Host Status is: on が表示されます。



警告

電源管理パラメーター（ユーザー ID、パスワード、オプションなど）は、Red Hat Virtualization Manager によってセットアップ時にのみテストされ、その後は手動でテストされます。不正なパラメーターに関する警告を無視したり、Red Hat Virtualization Manager で対応する変更を行わずに電源管理ハードウェアでパラメーターを変更したりすると、最も必要なときにフェンシングが失敗する可能性があります。

15. **OK** をクリックして、Edit fence agent ウィンドウを閉じます。
16. 電源管理 タブで、オプションで 詳細 パラメーター を展開し、上下のボタンを使用して、Manager がホストの クラスター と dc （データセンター）でフェンシングプロキシーを検索する順序を指定します。
17. **OK** をクリックします。

ホストのリストに戻ります。ホスト名の横にある感嘆符が消え、電源管理が正常に設定されていることが分かります。

7.6.4. fence_kdump の高度な設定

kdump

ホストを選択して、詳細ペインの General タブで kdump サービスのステータスを表示します。

- **有効:** kdump が正しく設定され、kdump サービスが実行している。
- **無効:** kdump サービスが実行されていない（この場合は、kdump 統合が適切に機能しません）。
- **不明:** kdump ステータスを報告しない古い VDSM バージョンのホストでのみ発生します。

kdump のインストールおよび使用に関する詳細は、[Red Hat Enterprise Linux 7 カーネルクラッシュダンプガイド](#) を参照してください。

fence_kdump

New Host または Edit Host ウィンドウの Power Management タブで Kdump 統合 を有効にすると、標準の fence_kdump 設定が設定されます。環境のネットワーク設定が単純で、Manager の FQDN がすべてのホストで解決可能である場合には、デフォルトの fence_kdump 設定を使用できます。

ただし、fence_kdump の高度な設定が必要な場合もあります。ネットワークが複雑な環境では、Manager、fence_kdump リスナー、またはその両方の設定を手動で変更する必要がある場合があります。たとえば、Kdump 統合 が有効になっているすべてのホストで Manager の FQDN が解決できない場合、engine-config を使用して適切なホスト名または IP アドレスを設定できます。

```
engine-config -s FenceKdumpDestinationAddress=A.B.C.D
```

以下の例の場合も、設定変更が必要な場合があります。

- Manager には 2 つの NIC があり、そのうちの 1 つは公開用で、もう 1 つは fence_kdump メッセージの優先的な送信先となっています。
- fence_kdump のリスナーを別の IP やポートで実行する必要があります。
- パケットロスの可能性を防ぐために、fence_kdump の通知メッセージのカスタムインターバルを設定する必要があります。

デフォルトの設定を変更する必要があるのは、より複雑なネットワーク設定の場合のみであるため、カスタマイズされた fence_kdump 検出設定は、上級ユーザーのみに推奨されます。fence_kdump リスナーの設定オプションは、「[fence_kdump リスナーの設定](#)」を参照してください。Manager での kdump の設定については、「[マネージャーでの fence_kdump の設定](#)」を参照してください。

7.6.4.1. fence_kdump リスナーの設定

fence_kdump リスナーの設定を編集します。これは、デフォルトの設定では十分ではない場合にのみ必要です。

手順7.17 fence_kdump リスナーの手動設定

- /etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/ に新しいファイル（例： **my-fence-kdump.conf**）を作成します。
- 構文 `OPTION=value` を使用してカスタマイズを入力し、ファイルを保存します。



重要

編集した値は、「[マネージャーでの fence_kdump の設定](#)」の fence_kdump Listener Configuration Options の表で説明されているように、**engine-config** で変更する必要があります。

- fence_kdump リスナーを再起動します。

```
# systemctl restart ovirt-fence-kdump-listener.service
```

以下のオプションは、必要に応じてカスタマイズすることができます。

表7.9 追加のリスナー設定オプション

変数	説明	デフォルト	注記
LISTENER_ADDRESS	fence_kdump メッセージを受信するための IP アドレスを定義します。	0.0.0.0	このパラメーターの値を変更する場合は、 engine-config の Fencedump DestinationAddress の値と一致する必要があります。

変数	説明	デフォルト	注記
LISTENER_PORT	fence_kdump メッセージを受信するポートを定義します。	7410	このパラメーターの値を変更する場合は、 engine-config の Fencedump DestinationPort の値と一致する必要があります。
HEARTBEAT_INTERVAL	リスナーのハートビート更新の間隔を秒単位で定義します。	30	このパラメーターの値を変更する場合は、 engine-config の FencedumpListenerTimeout の値の半分以下にする必要があります。
SESSION_SYNC_INTERVAL	リスナーのメモリーホストの kdumping セッションをデータベースに同期させる間隔を秒単位で定義します。	5	このパラメーターの値を変更する場合は、 engine-config の KdumpStartedTimeout の値の半分以下にする必要があります。
REOPEN_DB_CONNECTION_INTERVAL	以前に利用できなかったデータベース接続を再開する間隔を秒単位で定義します。	30	-
KDUMP_FINISHED_TIMEOUT	kdumping ホストからのメッセージを最後に受信してから、ホストの kdump フローが FINISHED とマークされるまでの最大タイムアウトを秒単位で定義します。	60	このパラメーターの値を変更する場合は、 engine-config の FencedumpMessageInterval の値の 2 倍以上である必要があります。

7.6.4.2. マネージャーでの fence_kdump の設定

Manager の kdump 設定を編集します。これは、デフォルトの設定では十分ではない場合にのみ必要です。現在の設定値は以下の方法で確認できます。

```
# engine-config -g OPTION
```

手順7.18 engine-config での Kdump の手動設定

1. **engine-config** コマンドを使用して kdump の設定を編集します。

```
# engine-config -s OPTION=value
```



重要

編集した値は、**Kdump Configuration Options** の表に記載されているように、fence_kdump リスナー設定ファイルでも変更する必要があります。『[fence_kdump リスナーの設定](#)』を参照してください。

2. **ovirt-engine** サービスを再起動します。

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

3. 必要に応じて、**Kdump 統合** を有効にしてすべてのホストを再インストールします（以下の表を参照）。

以下のオプションは **engine-config** を使用して設定できます。

表7.10 Kdump 設定オプション

変数	説明	デフォルト	注記
FenceKdumpDestinationAddress	fence_kdump メッセージの送信先となるホスト名または IP アドレスを定義します。空の場合、マネージャーの FQDN が使用されます。	空の文字列 (Manager FQDN が使用されます)	このパラメーターの値を変更する場合は、fence_kdump リスナー設定ファイルの LISTENER_ADDRESS の値と一致させ、 Kdump 統合 が有効になっているすべてのホストを再インストールする必要があります。
FenceKdumpDestinationPort	fence_kdump メッセージの送信先となるポートを定義します。	7410	このパラメーターの値を変更する場合は、fence_kdump リスナー設定ファイルの LISTENER_PORT の値と一致させ、 Kdump 統合 が有効になっているすべてのホストを再インストールする必要があります。
FenceKdumpMessageInterval	fence_kdump が送信するメッセージの間隔を秒単位で定義します。	5	このパラメーターの値を変更する場合は、fence_kdump リスナー設定ファイルの KDUMP_FINISHED_TIME_OUT の値の半分以下にし、 Kdump 統合 が有効になっているすべてのホストを再インストールする必要があります。

変数	説明	デフォルト	注記
FenceKdumpListenerTimeout	fence_kdump リスナーが生存しているとみなす最後のハートビートからの最大タイムアウトを秒単位で定義します。	90	このパラメーターの値を変更する場合は、fence_kdump リスナー設定ファイルの HEARTBEAT_INTERVAL の値の 2 倍以上でなければなりません。
KdumpStartedTimeout	kdumping ホストからの最初のメッセージを受信するまで(ホストの kdump フローが開始されたことを検出するまで)の最大タイムアウトを秒単位で定義します。	30	このパラメーターの値を変更する場合は、fence_kdump リスナー設定ファイルの SESSION_SYNC_INTERVAL の値の 2 倍以上、 Fence Kdump Message Interval の値を変更する必要があります。

7.6.5. ソフトフェンシングホスト

ホストは予期せぬ問題で応答しなくなることがあります。VDSM は要求に応答できないものの、VDSM に依存している仮想マシンは生きており、アクセス可能です。このような場合は、VDSM を再起動することで VDSM が応答可能な状態に戻り、この問題が解決します。

"SSH Soft Fencing" とは、応答しないホストに対して Manager が SSH 経由で VDSM の再起動を試みるプロセスのことです。Manager が SSH 経由で VDSM の再起動に失敗した場合、外部フェンシングエージェントが設定されていれば、フェンシングの責任は外部フェンシングエージェントに移ります。

SSH でのソフトフェンシングは以下のように動作します。ホストでフェンシングを設定して有効にする必要があります。有効なプロキシーホスト(データセンター内の UP 状態の 2 番目のホスト)が存在する必要があります。Manager とホストの接続がタイムアウトすると、以下のようになります。

- 最初のネットワーク障害では、ホストの状態が接続中に変わります。
- その後、マネージャーは VDSM にステータスの問い合わせを 3 回試みるか、ホストの負荷に応じた間隔で待機します。間隔の長さを決定する式は、設定値 TimeoutToResetVdsInSeconds (デフォルトは 60 秒) + [DelayResetPerVmInSeconds (デフォルトは 0.5 秒)] * (ホスト上で実行している仮想マシンの数) + [DelayResetForSpmInSeconds (デフォルトは 20 秒です)] * 1 (ホストが SPM として実行している場合) または 0 (ホストが SPM として実行されていない場合)。VDSM に応答する最大時間を与えるために、Manager は上記の 2 つのオプションのうち長い方を選択します (VDSM のステータスまたは上記の式で決定された間隔を取得するための 3 回の試行)。
- 間隔が経過したときにホストが応答しない場合は、**vdsm restart** を SSH 経由で実行します。
- vdsm restart** がホストと Manager 間の接続を再確立しない場合、ホストのステータスは **Non Responsive** に変更され、電源管理が設定されている場合、フェンシングは外部フェンシングエージェントに渡されます。



注記

SSH を介したソフトフェンシングは、電源管理が設定されていないホストで実行できます。これはフェンシングとは異なります。フェンシングは、電源管理が設定されているホストでのみ実行できます。

7.6.6. ホストの電源管理機能の利用

概要

電源管理がホストに設定されている場合は、Administration Portal インターフェイスから多くのオプションにアクセスできます。電源管理デバイスはそれぞれカスタマイズ可能な独自のオプションを持っていますが、いずれもホストの起動、停止、再起動の基本的なオプションをサポートしています。

手順7.19 ホストの電源管理機能の利用

1. ホストリソース タブ、ツリーモード、または検索機能を使用して、結果一覧でホストを見つけて選択します。
2. **Power Management** ドロップダウンメニューをクリックします。
3. 以下のオプションのいずれかを選択します。
 - **再起動**: このオプションはホストを停止し、ホストのステータスが **Down** に変わるまで待機します。エージェントがホストのダウンを確認すると、クラスター内の別のホストで高可用仮想マシンが再起動されます。その後、エージェントはこのホストを再起動します。ホストが使用可能な状態になると、ステータスが **Up** と表示されます。
 - **Start**: このオプションはホストを開始し、クラスターに参加させます。使用可能な状態になると、ステータスが **Up** と表示されます。
 - **stop**: このオプションは、ホストの電源をオフにします。このオプションを使用する前に、ホスト上で実行されている仮想マシンがクラスター内の他のホストに移行されていることを確認してください。そうしないと、仮想マシンがクラッシュし、可用性の高い仮想マシンだけが別のホストで再起動されます。ホストが停止している場合、ステータスは **Non-Operational** と表示されます。



重要

1つのホスト上に 2 つのフェンシングエージェントが定義されている場合、それらは同時または連続して使用することができます。同時進行のエージェントの場合、両方のエージェントが Stop コマンドに反応しないとホストは停止せず、一方のエージェントが Start コマンドに反応するとホストは立ち上がります。シーケンシャルエージェントの場合、ホストを起動または停止するには、まずプライマリーエージェントが使用され、それが失敗した場合はセカンダリーエージェントが使用されます。

4. 上記のいずれかのオプションを選択すると、確認ウィンドウが開きます。OK をクリックして確定し、続行します。

結果

選択したアクションが実行されます。

7.6.7. 反応しないホストを手動でフェンシングまたは分離する

概要

ハードウェアの故障などが原因で、ホストが予期せず応答しない状態になる場合、環境のパフォーマンスに大きな影響を及ぼす可能性があります。電源管理デバイスがない場合や、誤って設定されている場合は、ホストを手動で再起動できます。



警告

ホストを手動で再起動しない限り、**Confirm host has been rebooted** オプションを使用しないでください。ホストの実行中にこのオプションを使用すると、仮想マシンのイメージが破損する可能性があります。

手順7.20 反応しないホストを手動でフェンシングまたは隔離する方法

1. ホストタブで、ホストを選択します。ステータスは応答しないと表示される必要があります。
2. システムを手動で再起動します。これは物理的にラボに入り、ホストを再起動することを意味します。
3. 管理ポータルでホストエントリーを右クリックし、**Confirm Host has been rebooted** ボタンを選択します。
4. ホストがシャットダウンまたは再起動されたことを確認するよう要求するメッセージが表示されます。**Approve Operation** チェックボックスを選択し、**OK** をクリックします。

結果

ホストを手動で再起動し、高可用性仮想マシンをアクティブなホストで起動できる。管理者ポータルで手動フェンシングアクションを確認し、ホストがオンラインに戻っている。

7.7. ホストとパーミッション

7.7.1. ホストのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルのすべての側面を管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限された管理者ロールは、特定のリソースに制限される管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、そのデータセンターのストレージを除く、割り当てられたデータセンターの管理者権限のみを持ち、**ClusterAdmin** は割り当てられたクラスターに対してのみ管理者権限を持ちます。

ホスト管理者は、特定のホストのみのシステム管理ロールです。これは、複数のホストを持つクラスターで、各ホストにシステム管理者が必要な場合に有効です。ヘッダーバーの **Configure** ボタンを使用して、環境内のすべてのホストにホスト管理者を割り当てることができます。

ホスト管理者ロールは以下のアクションを許可します。

- ホストの設定編集。
- 論理ネットワークの設定。

- ホストを削除。

また、既存のシステム管理者を削除し、新しいシステム管理者を追加すると、ホストのシステム管理者を変更できます。

7.7.2. ホスト管理者ロールの概要

ホストパーミッションロール

以下の表は、ホスト管理に適用される管理者ロールおよび権限について説明しています。

表7.11 Red Hat Virtualization システム管理者ロール

ロール	権限	注記
HostAdmin	ホスト管理者	特定のホストを設定、管理、および削除できます。特定のホストでネットワーク関連の操作も実行できます。

7.7.3. 管理者またはユーザーロールのリソースへの割り当て

管理者またはユーザーロールをリソースに割り当て、ユーザーがそのリソースにアクセスしたり、管理したりできるようにします。

手順7.21 リソースへのロールの割り当て

1. リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
2. 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
3. **Add** をクリックします。
4. **Search** テキストボックスに既存ユーザーの名前またはユーザー名を入力し、**Go** をクリックします。表示された候補の中からユーザーを選択します。
5. **Role to Assign:** ドロップダウンリストからロールを選択します。
6. **OK** をクリックします。

ユーザーにロールを割り当てました。そのリソースで有効にしたそのロールの継承されたパーミッションが、ユーザーに付与されました。

7.7.4. リソースからの管理者またはユーザーロールの削除

管理者またはユーザーのロールをリソースから削除すると、ユーザーはそのリソースのロールに関連付けられ継承されたパーミッションを失います。

手順7.22 リソースからのロールの削除

1. リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。

2. 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
3. リソースから削除するユーザーを選択します。
4. **Remove** をクリックします。 **Remove Permission** 画面が開き、パーミッションの削除を確認します。
5. **OK** をクリックします。

ユーザーのロールおよび関連付けられたパーミッションをリソースから削除しました。

第8章 ストレージ

Red Hat Virtualization は、仮想ディスクイメージ、ISO ファイル、およびスナップショットに集中ストレージシステムを使用します。ストレージネットワーキングは、以下の方法で実装できます。

- ネットワークファイルシステム(NFS)
- Gluster FS のエクスポート
- CephFS
- その他の POSIX 準拠ファイルシステム
- Internet Small Computer System Interface (iSCSI)
- 仮想化ホストに直接接続されたローカルストレージ
- ファイバーチャネルプロトコル(FCP)
- Parallel NFS (pNFS)

ストレージドメインが接続され、アクティベートされなければデータセンターは初期化されないため、ストレージの設定は新しいデータセンターの前提条件となります。

Red Hat Virtualization のシステム管理者として、仮想化された企業のためにストレージを作成、設定、アタッチ、維持する必要があります。ストレージの種類とその使い方をよく理解しておく必要があります。ストレージアレイベンダーのガイドを読み、ストレージの概念、プロトコル、要件、または一般的な使用方法に関する詳細は、[Red Hat Enterprise Linux Storage Administration Guide](#) を参照してください。

Red Hat Virtualization では、管理ポータルのストレージタブを使用してストレージを割り当て、管理できます。**Storage** results リストには、すべてのストレージドメインが表示され、詳細ペインにはドメインに関する一般的な情報が表示されます。

ストレージドメインを追加するには、管理ポータルに正常にアクセスでき、ステータスが **Up** のホストが1台以上接続されている必要があります。

Red Hat Virtualization には、3種類のストレージドメインがあります。

- **Data Domain:** データドメインは、データセンター内のすべての仮想マシンおよびテンプレートの仮想ハードディスクと OVF ファイルを保持します。さらに、仮想マシンのスナップショットもデータドメインに保存されます。

データドメインは、データセンター間で共有することはできません。複数のタイプ (iSCSI、NFS、FC、POSIX、および Gluster) のデータドメインは、ローカルドメインではなくすべて共有されている場合、同じデータセンターに追加できます。

データセンターに他のタイプのドメインをアタッチする前に、データドメインをアタッチする必要があります。

- **ISO ドメイン :** ISO ドメインは、仮想マシンのオペレーティングシステムおよびアプリケーションのインストールと起動に使用される ISO ファイル（または論理 CD）を格納します。ISO ドメインは、データセンターの物理メディアの必要性を削除します。ISO ドメインは、異なるデータセンター間で共有できます。ISO ドメインは NFS ベースのものしかありません。データセンターに1つの ISO ドメインのみをアタッチできます。
- **エクスポートドメイン :** エクスポートドメインは、データセンターと Red Hat Virtualization 環

境間でイメージをコピーおよび移動するために使用される一時的なストレージリポジトリです。エクスポートドメインは、仮想マシンのバックアップに使用できます。エクスポートドメインは、データセンター間で移動することができますが、同時に1つのデータセンターでしか有効にすることできません。エクスポートドメインは、NFSベースでのみ可能です。データセンターに追加できるエクスポートドメインは1つだけです。



注記

エクスポートストレージドメインは非推奨になりました。ストレージデータドメインはデータセンターから接続を解除し、同じ環境または別の環境にある別のデータセンターにインポートすることができます。仮想マシン、フローティング仮想ディスクイメージ、およびテンプレートは、インポートされたストレージドメインからアタッチされたデータセンターにアップロードできます。ストレージドメインのインポートに関する詳細は、「[既存のストレージドメインのインポート](#)」を参照してください。



重要

Red Hat Virtualization 環境へのストレージの設定と接続は、データセンターのストレージニーズが決定してから開始してください。

8.1. ストレージドメインについて

ストレージドメインとは、共通のストレージインターフェイスを持つイメージの集合体です。ストレージドメインには、テンプレートや仮想マシンの完全なイメージ(スナップショットを含む)、またはISOファイルが格納されています。ストレージドメインは、ブロックデバイス(SAN - iSCSI または FCP)またはファイルシステム(NAS - NFS、GlusterFS、CephFS、またはその他の POSIX 準拠のファイルシステム)のいずれかで設定できます。

NFS では、仮想ディスク、テンプレート、スナップショットはすべてファイルです。

SAN (iSCSI/FCP) では、各仮想ディスク、テンプレート、またはスナップショットは論理ボリュームです。ブロックデバイスは、ボリュームグループと呼ばれる論理エンティティーに集約され、LVM (Logical Volume Manager) によって論理ボリュームに分割されて仮想ハードディスクとして使用されます。LVM の詳細は、「[Red Hat Enterprise Linux Logical Volume Manager Administration Guide](#)」を参照してください。

仮想ディスクには、QCOW2 または RAW のいずれかの形式を使用できます。ストレージのタイプは、スペースまたは事前割り当てのいずれかです。スナップショットは常にスペースですが、RAW または sparse として作成されたディスクに対して取得できます。

同じストレージドメインを共有する仮想マシンは、同じクラスターに属するホスト間で移行することができます。

8.2. NFS ストレージの準備と追加

8.2.1. NFS ストレージの準備

Red Hat Enterprise Linux サーバー上のデータドメインとして機能する NFS 共有を設定します。ISO ドメインが Red Hat Virtualization Manager のインストール手順で作成された場合は、そのドメインを作成する必要はありません。



注記

エクスポートストレージドメインは非推奨になりました。ストレージデータドメインはデータセンターから接続を解除し、同じ環境または別の環境にある別のデータセンターにインポートすることができます。仮想マシン、フローティング仮想ディスクイメージ、およびテンプレートは、インポートされたストレージドメインからアタッチされたデータセンターにアップロードできます。ストレージドメインのインポートに関する詳細は、「[既存のストレージドメインのインポート](#)」を参照してください。

Red Hat Enterprise Linux での NFS の設定および設定については、Red Hat Enterprise Linux 『6 ストレージ管理ガイド』の [ネットワークファイルシステム\(NFS\)](#) または『Red Hat Enterprise Linux 7』ストレージ管理ガイド』の [ネットワークファイルシステム\(NFS\)](#) を参照してください。

Red Hat Virtualization には、特定のシステムユーザー アカウントおよびシステムユーザーグループが必要です。これにより、Manager はストレージドメイン(エクスポートしたディレクトリー)にデータを保管することができます。

手順8.1 必要なシステムユーザー アカウントとシステムユーザーグループの設定

1. **kvm** グループを作成します。

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

2. **kvm** グループに **vdsd** ユーザーを作成します。

```
# useradd vdsd -u 36 -g 36
```

3. エクスポートしたディレクトリーの所有権を 36:36 に設定します。これにより、vdsd:kvm の所有権が付与されます。

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

4. 所有者への読み取りおよび書き込みアクセスを許可し、グループおよびその他のユーザーに読み取り/実行アクセスが付与されるように、ディレクトリーのモードを変更します。

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

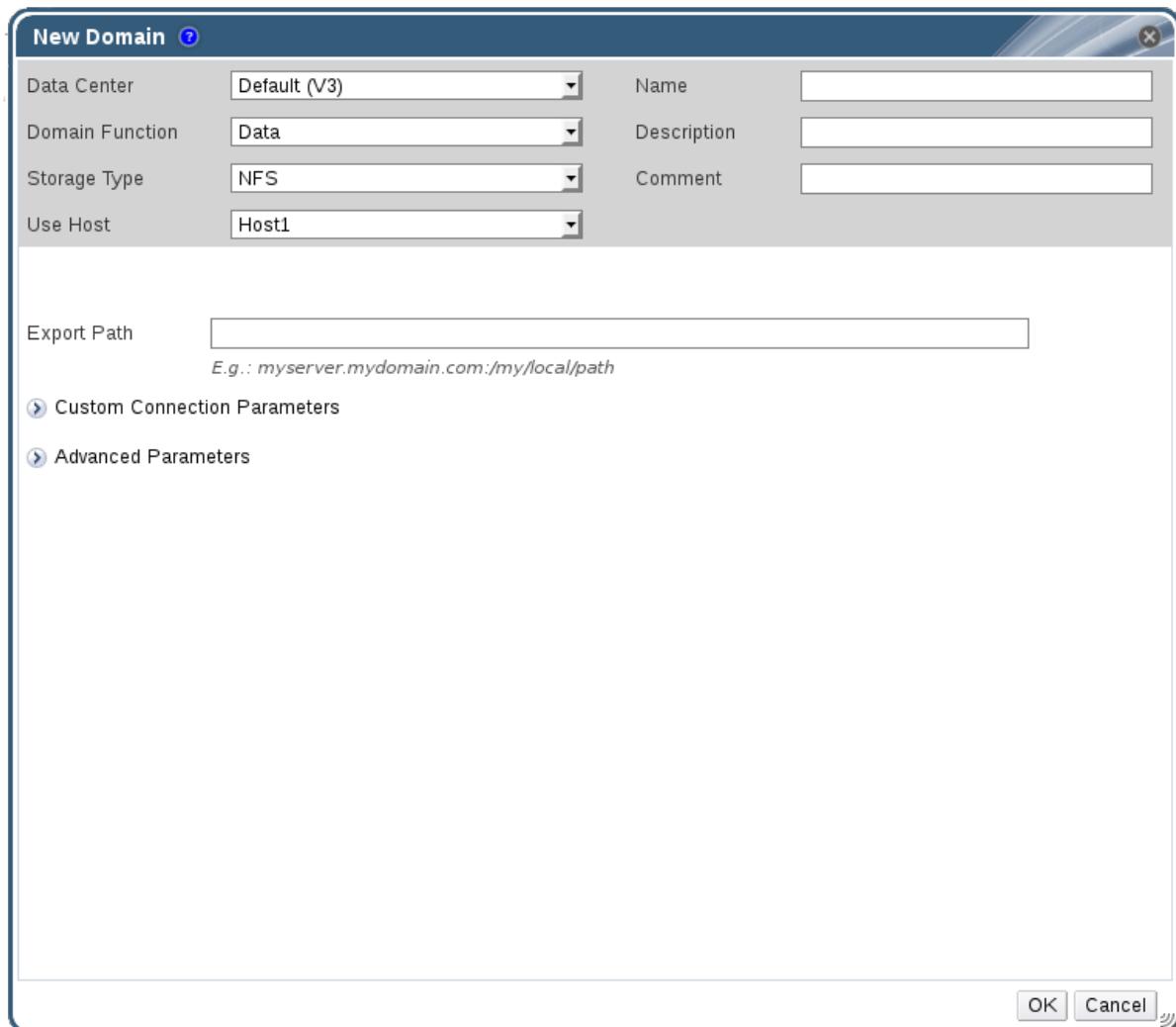
必要なシステムユーザーおよびグループの詳細は、[付録G システムアカウント](#) を参照してください。

8.2.2. NFS ストレージのアタッチ

NFS ストレージドメインを Red Hat Virtualization 環境のデータセンターに接続します。このストレージドメインは、仮想化ゲストイメージと ISO ブートメディアのストレージを提供します。この手順では、共有がすでにエクスポートされていることを前提としています。エクスポートドメインを作成する前に、データドメインを作成する必要があります。同じ手順を使用してエクスポートドメインを作成し、ドメイン機能/ストレージ タイプ一覧で **Export / NFS** を選択します。

1. Red Hat Virtualization Manager 管理ポータルで、**Storage resource** タブをクリックします。
2. **New Domain** をクリックします。

図8.1新しいドメインウィンドウ



3. ストレージドメインの **Name** を入力します。
4. データセンター、ドメイン機能、ストレージタイプ、フォーマット、およびホストリストのデフォルト値を受け入れます。
5. ストレージドメインに使用する **Export Path** を入力します。
エクスポートパスは、JBDS `0:/data` または `domain.example.com:/data` の形式である必要があります。
6. オプションで、詳細パラメーターを設定することができます。
 - a. **Advanced Parameters** をクリックします。
 - b. **Warning Low Space Indicator** フィールドにパーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。
 - c. **Critical Space Action Blocker** フィールドに GB の値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーにエラーメッセージが表示され、ログに記録されます。容量を消費する新規アクションは、一時的であってもすべてブロックされます。
 - d. 削除後にワイプオプションを有効にするには、**Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集することが可能ですが、その場合にはすでに存在していたディスクの削除後にワイププロパティーは変更されません。

7. **OK** をクリックします。

新しい NFS データドメインは **Storage** タブに表示され、ディスクが準備されるまで **Locked** ステータスで表示されます。その後、データドメインはデータセンターに自動的にアタッチされます。

8.2.3. NFS ストレージの増設

NFS ストレージの容量を増やすには、新しいストレージドメインを作成して既存のデータセンターに追加するか、NFS サーバーの利用可能な空き容量を増やすことができます。以前のオプションは、「[NFS ストレージのアタッチ](#)」を参照してください。以下の手順では、既存の NFS サーバーの利用可能な空き容量を増やす方法を説明しています。

手順8.2 既存の NFS ストレージドメインの増加

1. **Storage** resource タブをクリックし、NFS ストレージドメインを選択します。
2. 詳細ペインで、**Data Center** タブをクリックし、**Maintenance** ボタンをクリックしてストレージドメインをメンテナンスマードにします。これにより、既存の共有がアンマウントされ、ストレージドメインのサイズ変更が可能になります。
3. NFS サーバー上で、ストレージのサイズを変更する。Red Hat Enterprise Linux 6™ システムについては、[Red Hat Enterprise Linux 6 Storage Administration Guide](#) を参照してください。Red Hat Enterprise Linux 7™ システムについては、[Red Hat Enterprise Linux 7 Storage Administration Guide](#) を参照してください。
4. 詳細ペインで、**Data Center** タブをクリックし、**Activate** ボタンをクリックしてストレージドメインをマウントします。

8.3. ローカルストレージの準備と追加

8.3.1. ローカルストレージの準備

ホスト上にローカルストレージドメインをセットアップすることができます。ローカルストレージを使用するようにホストを設定すると、ホストは、他のホストを追加できない新しいデータセンターおよびクラスターに自動的に追加されます。複数のホストクラスターでは、すべてのホストがすべてのストレージドメインにアクセスできる必要がありますが、ローカルストレージでは不可能です。単一ホストクラスターで作成された仮想マシンは、移行、フェンス、またはスケジュールできません。必要なシステムユーザーおよびグループの詳細は、[付録G システムアカウント](#) を参照してください。



注記

Red Hat Virtualization Host (RHVH) の再インストール時にローカルストレージドメインを保持する方法は、『[アップグレードガイド](#)』の [RHVHへのアップグレード](#) を参照してください。



重要

Red Hat Virtualization Host (RHVH)では、ローカルストレージに使用されるパスは **/var** ディレクトリーになければなりません。RHVH の場合は、『ローカルストレージの準備の手順で **/var** をディレクトリーに追加』します。

Red Hat Virtualization Host が再インストールされると、**/var** ディレクトリーのローカルストレージが失われます。これを回避するには、外部ストレージをホストマシンにマウントして、ローカルストレージドメインとして使用することができます。ストレージのマウントに関する詳細は、『[Red Hat Enterprise Linux Storage Administration Guide](#)』を参照してください。

手順8.3 ローカルストレージの準備

1. ホストで、ローカルストレージに使用するディレクトリーを作成します。

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

2. **vdsm** ユーザー(UID 36)および **kvm** グループ(GID 36)への読み取り/書き込みアクセスを許可するパーミッションがディレクトリーにあることを確認します。

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

```
# chmod 0755 /data /data/images
```

ローカルストレージを Red Hat Virtualization 環境に追加する準備が整いました。

8.3.2. ローカルストレージの追加

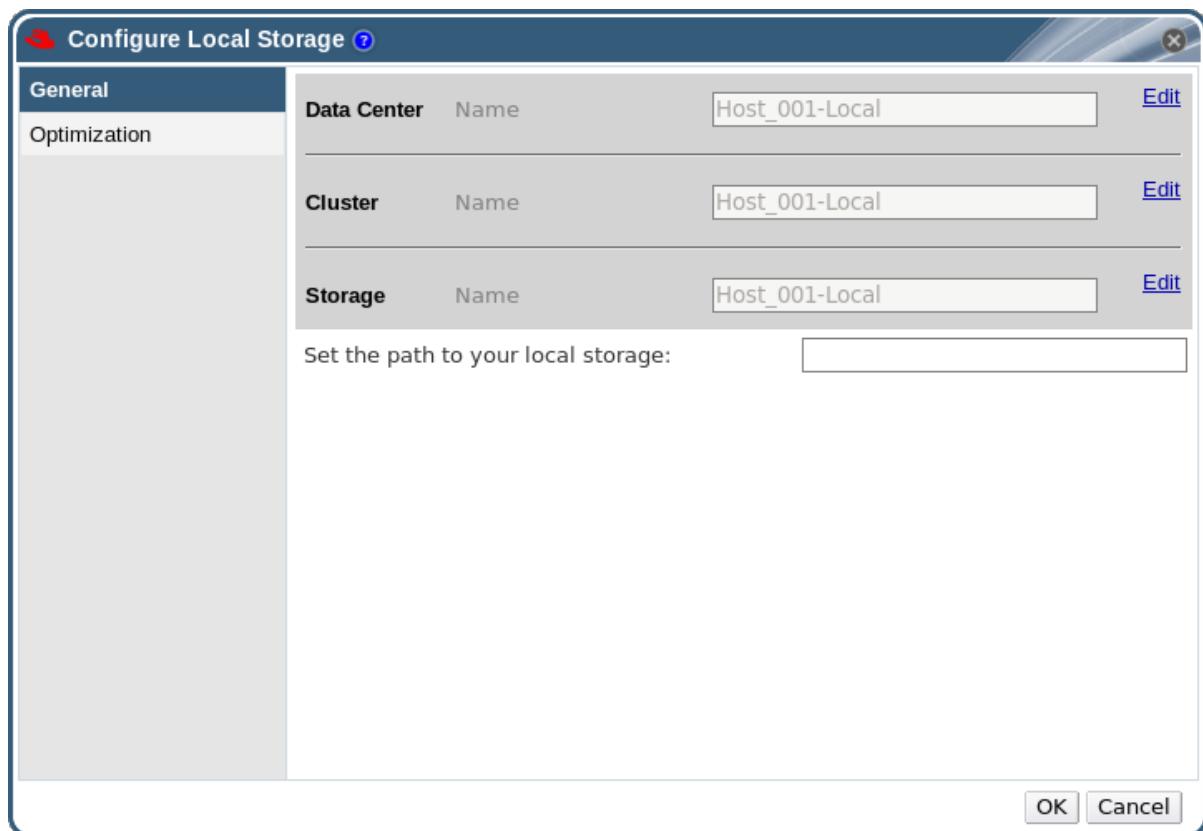
ホストにローカルのストレージを用意している。次に、Manager を使用してホストに追加します。

このようにホストにローカルストレージを追加すると、ホストが新しいデータセンターおよびクラスターに配置されます。ローカルストレージ設定ウィンドウは、データセンター、クラスター、ストレージの作成を1つのプロセスにまとめています。

手順8.4 ローカルストレージの追加

1. **Hosts** resource タブをクリックし、結果一覧でホストを選択します。
2. **Maintenance** をクリックして、メンテナーンスホストの確認ウィンドウを開きます。
3. **OK** をクリックしてメンテナーンスマードを開始します。
4. **Configure Local Storage** をクリックし、**Configure Local Storage** ウィンドウを開きます。

図8.2 ローカルストレージウィンドウの設定



5. **Data Center** フィールド、**Cluster** フィールド、および **Storage** フィールドの横にある **Edit** ボタンをクリックして、ローカルストレージドメインを設定し、名前を付けます。
6. 文字入力フィールドにローカルストレージへのパスを設定します。
7. 該当する場合は、**Optimization** タブを選択して、新しいローカルストレージクラスターのメモリー最適化ポリシーを設定します。
8. **OK** をクリックして設定を保存し、ウィンドウを閉じます。

ホストが、自己のデータセンター内でオンラインになります。

8.4. POSIX 準拠ファイルシステムストレージの追加

POSIX ファイルシステムのサポートにより、通常コマンドラインから手動でマウントするときと同じマウントオプションを使ってファイルシステムをマウントすることができます。この機能は、NFS、iSCSI、または FCP 以外を使用してマウントするストレージへのアクセスを可能にすることを目的としています。

Red Hat Virtualization でストレージドメインとして使用される POSIX 準拠のファイルシステムは、スペースファイルおよびダイレクト I/O をサポートする必要があります。たとえば、Common Internet File System (CIFS) は、ダイレクト I/O をサポートしていないので、Red Hat Virtualization との互換性はありません。



重要

POSIX 準拠のファイルシステムストレージドメインを作成して、NFS ストレージをマウントしないでください。代わりに、NFS ストレージドメインを常に作成します。

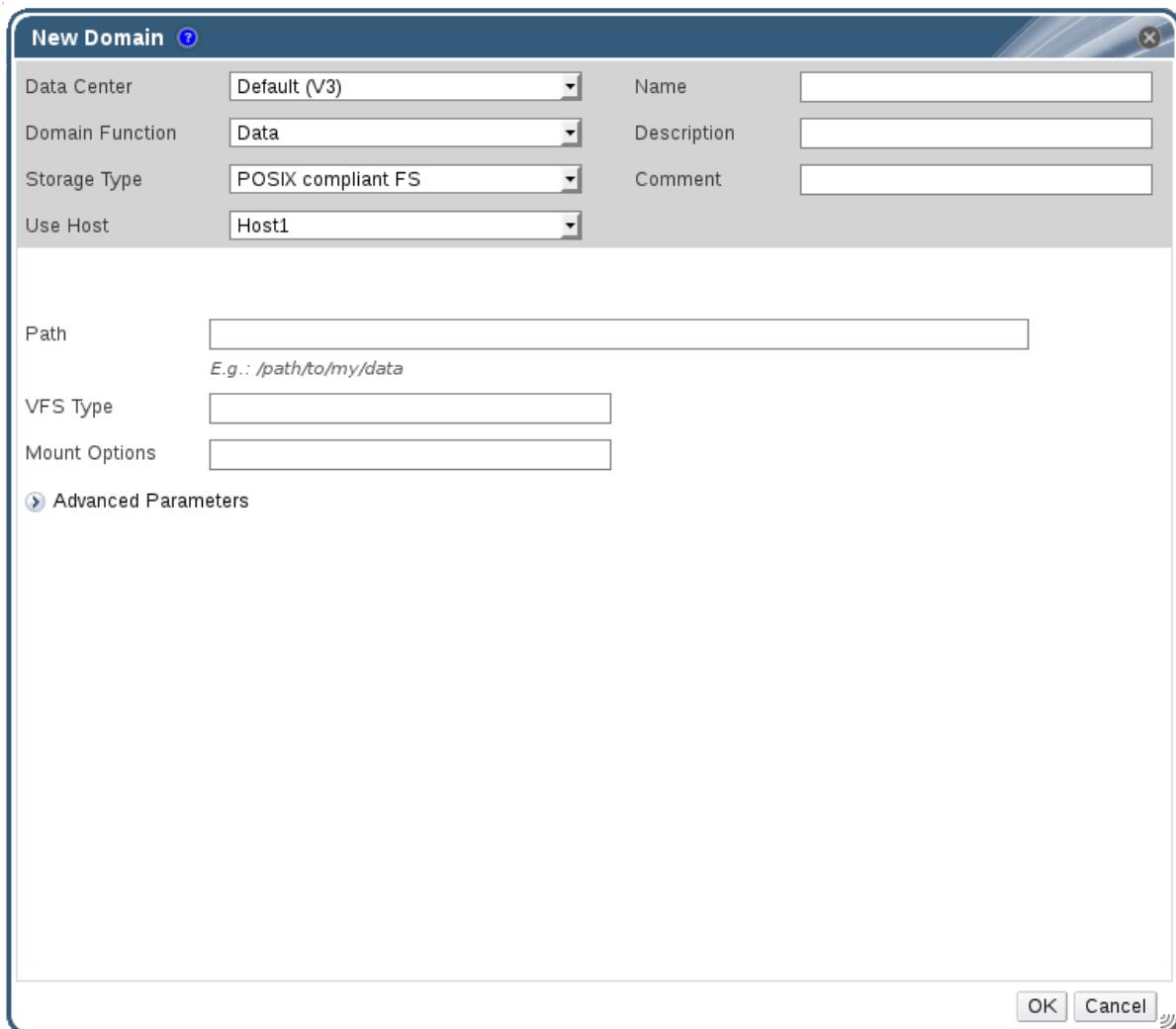
8.4.1. POSIX 準拠ファイルシステムストレージのアタッチ

ストレージドメインとして NFS、iSCSI、または FCP を使用して公開されていない POSIX 準拠のファイルシステムを使用する。

手順8.5 POSIX 準拠ファイルシステムストレージのアタッチ

1. **Storage resource** タブをクリックして、結果一覧で既存のストレージドメインを一覧表示します。
2. **New Domain** をクリックして、**New Domain** ウィンドウを開きます。

図8.3 POSIX ストレージ



3. ストレージドメインの **Name** を入力します。
4. ストレージドメインに関連付ける **データセンター** を選択します。選択したデータセンターのタイプは、**POSIX (POSIX compliant FS)** でなければなりません。または、**(none)** 選択します。
5. **Domain Function / Storage Type** ドロップダウンメニューから **Data / POSIX compliant FS** を選択します。
該当する場合は、ドロップダウンメニューから **Format** を選択します。
6. **Use Host** ドロップダウンメニューからホストを選択します。選択したデータセンター内のホストのみが一覧表示されます。選択したホストは、ストレージドメインの接続に使用されます。

7. 通常 **mount** コマンドで指定するように、POSIX ファイルシステムへのパスを入力します。
8. 通常 **-t** 引数を使用して **mount** コマンドに指定するように、**VFS Type** を入力します。有効な VFS タイプの一覧は、**man mount** を参照してください。
9. 通常 **mount** コマンドに **-o** 引数を指定して指定するように、追加の **Mount Options** を入力します。このマウントオプションはコンマ区切りリストで提示してください。有効なマウントオプションの一覧は、**man mount** を参照してください。
10. オプションで、詳細パラメーターを設定することができます。
 - a. **Advanced Parameters** をクリックします。
 - b. **Warning Low Space Indicator** フィールドにパーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。
 - c. **Critical Space Action Blocker** フィールドに GB の値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーにエラーメッセージが表示され、ログに記録されます。容量を消費する新規アクションは、一時的であってもすべてブロックされます。
 - d. 削除後に **Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集することが可能ですが、その場合にはすでに存在していたディスクの削除後にワイププロパティーは変更されません。
11. **OK** をクリックして新しいストレージドメインをアタッチし、ウィンドウを閉じます。

8.5. ブロックストレージの追加

8.5.1. iSCSI ストレージの追加

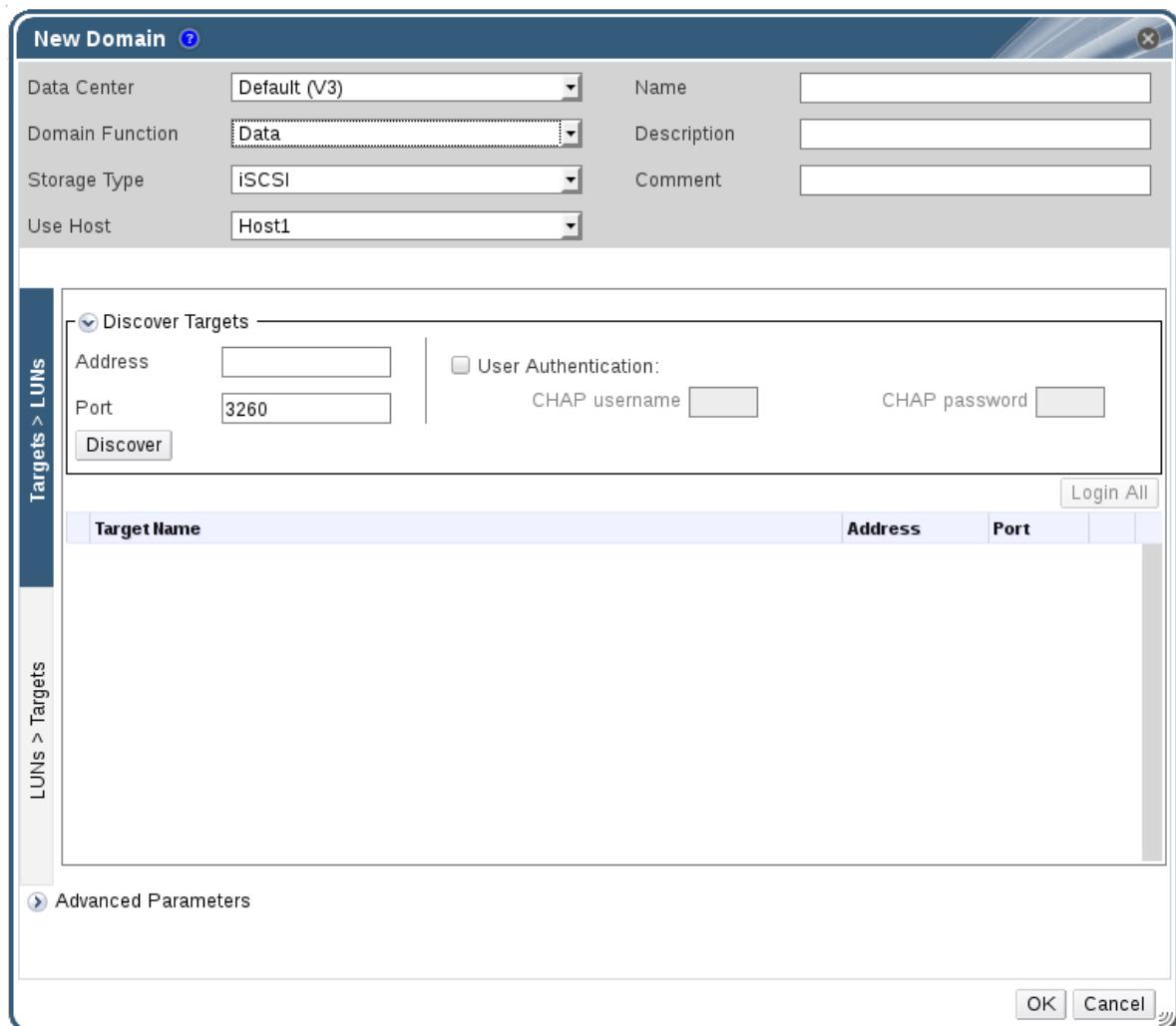
Red Hat Virtualization は、既存の LUN で設定されるボリュームグループからストレージドメインを作成することにより、iSCSI ストレージをサポートします。ボリュームグループおよび LUN は、いずれも同時に複数のストレージドメインにアタッチすることはできません。

Red Hat Enterprise Linux での iSCSI の設定および設定に関する情報は、Red Hat Enterprise Linux 『7 ストレージ管理ガイド』の『Red Hat Enterprise Linux 6 ストレージ管理ガイド』の [iSCSI ターゲットの作成](#) またはオンラインストレージ管理』を参照してください。https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/7/html/Storage_Administration_Guide/ch24.html

手順8.6 iSCSI ストレージの追加

1. **Storage resource** タブをクリックして、結果一覧で既存のストレージドメインを一覧表示します。
2. **新規ドメイン** ボタンをクリックして、**新規ドメイン** ウィンドウを開きます。
3. 新規ストレージドメインの **Name** を入力します。

図8.4 新しい iSCSI ドメイン



4. **Data Center** ドロップダウンメニューを使用して、データセンターを選択します。
5. ドロップダウンメニューを使用して **Domain Function** および **Storage Type** を選択します。選択したドメイン機能との互換性がないストレージドメインタイプは利用できません。
6. **Use Host** フィールドでアクティブなホストを選択します。データセンターの最初のデータドメインではない場合は、データセンターの SPM ホストを選択する必要があります。



重要

ストレージドメインへの通信はすべて、Red Hat Virtualization Manager から直接ではなく、選択したホストを介して行われます。システムには、アクティブなホストが少なくとも1台存在し、選択したデータセンターにアタッチされている必要があります。ストレージドメインを設定する前には、全ホストがストレージデバイスにアクセスできる状態でなければなりません。

7. Red Hat Virtualization Manager は、iSCSI ターゲットを LUN、または LUN を iSCSI ターゲットにマッピングできます。新規ドメイン ウィンドウには、iSCSI がストレージタイプとして選択されていると、未使用的 LUN を持つ既知のターゲットが自動的に表示されます。ストレージを追加するターゲットが一覧にない場合には、ターゲット検出を使用して検索できます。それ以外の場合は、次のステップに進みます。

iSCSI ターゲット検出

1. ターゲットの検出をクリックして、ターゲットの検出オプションを有効にします。ターゲットが検出され、ログインすると、**New Domain** ウィンドウに、環境が未使用の LUN が割り当てられたターゲットが自動的に表示されます。



注記

環境の外部で使用されている LUN も表示されます。

Discover Targets オプションを使用して、多くのターゲットに LUN を追加したり、同じ LUN に複数のパスを追加したりすることができます。

2. **Address** フィールドに iSCSI ホストの完全修飾ドメイン名または IP アドレスを入力します。
 3. **Port** フィールドにターゲットを参照する際にホストに接続するポートを入力します。デフォルトは **3260** です。
 4. ストレージのセキュリティー保護にチャレンジハンドシェイク認証プロトコル(CHAP)を使用している場合は、**ユーザー認証** チェックボックスを選択します。 **CHAP ユーザー名** と **CHAP パスワード** を入力します。



注記

REST API を使用して、ホストごとに各 iSCSI ターゲットに特定の認証情報を定義できるようになりました。詳細は、『REST API Guide』の [Defining Credentials to an iSCSI Target](#) を参照してください。

- 検出ボタンをクリックします。
 - 検出結果から使用するターゲットを選択し、ログインボタンをクリックします。
または、**Login All**をクリックして、検出されたすべてのターゲットにログインします。

または、**Login All** をクリックして、検出されたすべてのターゲットにログインします。



重要

複数のパスのアクセスが必要な場合には、すべての必要なパスでターゲットを検出してログインするようにしてください。ストレージドメインを変更してパスを追加する方法は、現在サポートされていません。

8. 対象のターゲットの横にある + ボタンをクリックします。これにより、エントリーが拡張され、ターゲットに接続されている未使用の LUN がすべて表示されます。
 9. ストレージドメインの作成に使用する各 LUN のチェックボックスを選択します。
 10. オプションで、詳細パラメーターを設定することができます。
 - a. **Advanced Parameters** をクリックします。
 - b. **Warning Low Space Indicator** フィールドにパーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。

- c. **Critical Space Action Blocker** フィールドに GB の値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーにエラーメッセージが表示され、ログに記録されます。容量を消費する新規アクションは、一時的であってもすべてブロックされます。
- d. 削除後に **ワイプオプションを有効にするには、Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集することが可能ですが、その場合にはすでに存在していたディスクの削除後にワイププロパティーは変更されません。

11. **OK** をクリックしてストレージドメインを作成し、ウィンドウを閉じます。

同じターゲットへの複数のストレージ接続パスを設定している場合は、[「Configuring iSCSI Multipathing」](#) の手順に従って iSCSI ボンディングを完了します。

8.5.2. Configuring iSCSI Multipathing

iSCSI マルチパスを使用すると、論理ネットワークと iSCSI ストレージ接続のグループを作成および管理できます。ネットワークパスの失敗によるホストのダウンタイムを防ぐには、ホストと iSCSI ストレージ間で複数のネットワークパスを設定します。設定が完了すると、Manager は同じ iSCSI ボンディングの論理ネットワークに関連する NIC/VLAN を介して、データセンター内の各ホストを各ボンディングされたターゲットに接続します。また、ホストがデフォルトのネットワークを介してトラフィックをルーティングできるようにする代わりに、ストレージトラフィックに使用するネットワークを指定することもできます。このオプションは、少なくとも 1 つの iSCSI ストレージドメインがデータセンターに接続された後にのみ管理ポータルで使用できます。

前提条件

- iSCSI ストレージドメインを作成し、検出して iSCSI ターゲットへのすべてのパスにログインしていることを確認します。
- iSCSI ストレージ接続でボンディングする **非必須** 論理ネットワークを作成していることを確認します。複数の論理ネットワークまたはボンドネットワークを設定して、ネットワークのフェイルオーバーを可能にします。

手順8.7 Configuring iSCSI Multipathing

1. **Data Centers** タブをクリックして、結果リストからデータセンターを選択します。
2. 詳細ペインで、**iSCSI Multipathing** タブをクリックします。
3. **Add** をクリックします。
4. **Add iSCSI Bond** ウィンドウで、ボンドの **Name** および **Description** を入力します。
5. **Logical Networks** 一覧からボンディングに使用するネットワークを選択します。ネットワークは **必須** ではないネットワークである必要があります。



注記

ネットワークの **Required** の指定を変更するには、管理ポータルからネットワークを選択し、**Cluster** タブをクリックして、**Manage Networks** ボタンをクリックします。

6. **Storage Targets** 一覧から選択したネットワークからアクセスするストレージドメインを選択します。同じターゲットへのすべてのパスを選択してください。
7. **OK** をクリックします。

データセンター内の全ホストは、選択した論理ネットワークを介して選択した iSCSI ターゲットに接続されます。

8.5.3. FCP ストレージの追加

Red Hat Virtualization プラットフォームは、既存の LUN で設定されるボリュームグループからストレージドメインを作成することにより、SAN ストレージをサポートします。ボリュームグループおよび LUN は、いずれも同時に複数のストレージドメインにアタッチすることはできません。

Red Hat Virtualization システムの管理者には Storage Area Networks (SAN) の概念に関する作業知識が必要になります。SAN は通常、ホストと外部の共有ストレージ間のトラフィックにファイバーチャネルプロトコル (FCP) を使用します。このため、SAN は FCP ストレージとも呼ばれています。

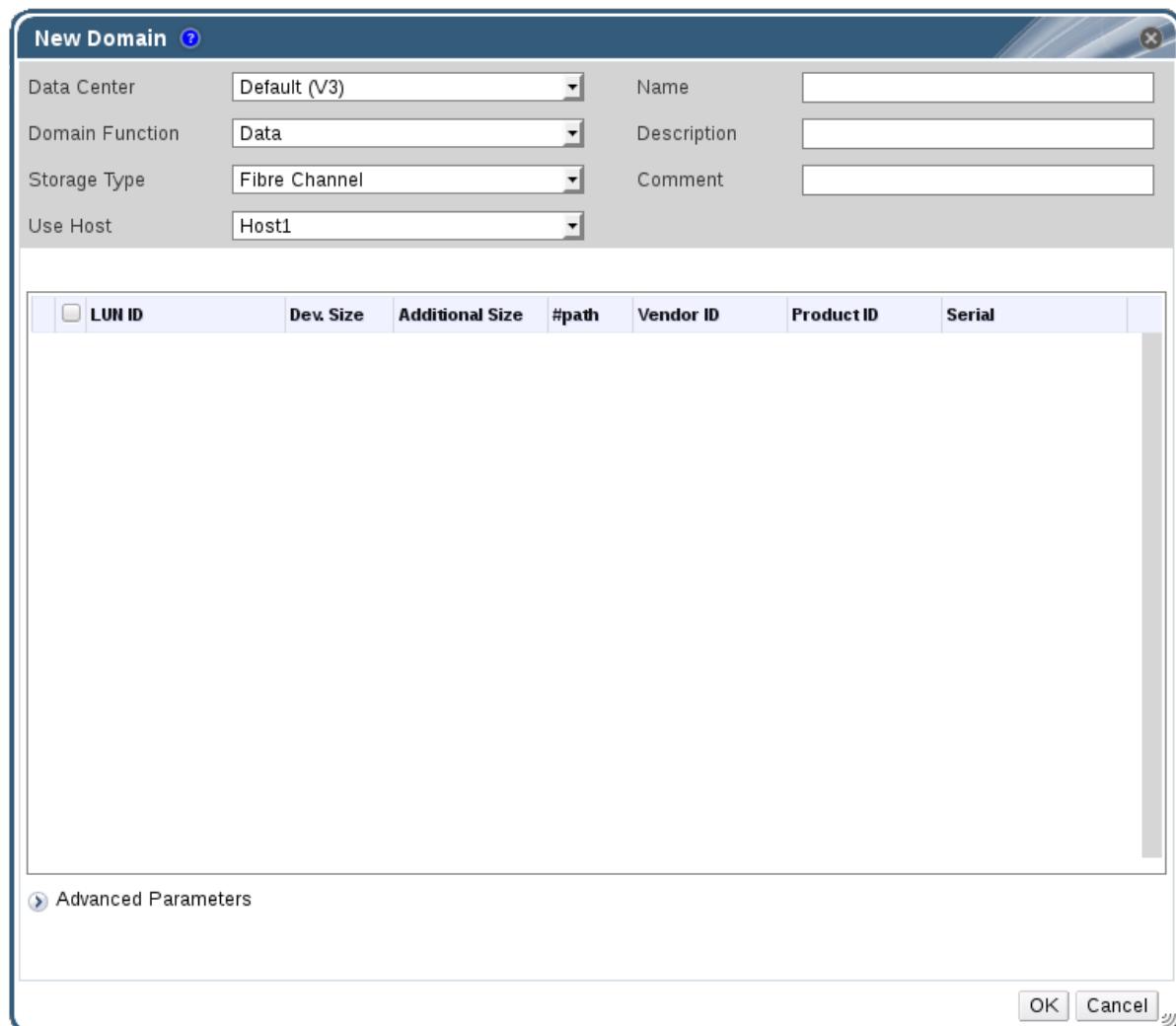
Red Hat Enterprise Linux での FCP またはマルチパスの設定に関する情報は、[ストレージ 管理ガイド](#) および [DM Multipath ガイド](#) を参照してください。

以下の手順では、既存の FCP ストレージをデータドメインとして Red Hat Virtualization 環境にアタッチする方法を説明します。サポートされる他のストレージタイプの詳細は、[8章ストレージ](#) を参照してください。

手順8.8 FCP ストレージの追加

1. Storage resource タブをクリックして、すべてのストレージドメインを一覧表示します。
2. New Domain をクリックして、New Domain ウィンドウを開きます。
3. ストレージドメインの Name を入力します。

図8.5 FCPストレージの追加



4. **Data Center** ドロップダウンメニューを使用して、FCP データセンターを選択します。
適切な FCP データセンターがない場合には (**none**) を選択します。
5. ドロップダウンメニューを使用して **Domain Function** および **Storage Type** を選択します。選択したデータセンターとの互換性がないストレージドメインタイプは選択できません。
6. **Use Host** フィールドでアクティブなホストを選択します。データセンターの最初のデータドメインではない場合は、データセンターの SPM ホストを選択する必要があります。



重要

ストレージドメインへの通信はすべて、Red Hat Virtualization Manager から直接ではなく、選択したホストを介して行われます。システムには、アクティブなホストが少なくとも 1 台存在し、選択したデータセンターにアタッチされている必要があります。ストレージドメインを設定する前には、全ホストがストレージデバイスにアクセスできる状態でなければなりません。

7. **New Domain** ウィンドウには、**Data / Fibre Channel** がストレージタイプとして選択されていると、未使用の LUN を持つ既知のターゲットが自動的に表示されます。**LUN ID** チェックボックスを選択して、利用可能なすべての LUN を選択します。
8. オプションで、詳細パラメーターを設定することができます。

- a. **Advanced Parameters** をクリックします。
 - b. **Warning Low Space Indicator** フィールドにパーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。
 - c. **Critical Space Action Blocker** フィールドに GB の値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーにエラーメッセージが表示され、ログに記録されます。容量を消費する新規アクションは、一時的であってもすべてブロックされます。
 - d. 削除後に **Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集することが可能ですが、その場合にはすでに存在していたディスクの削除後にワイププロパティーは変更されません。
9. **OK** をクリックしてストレージドメインを作成し、ウィンドウを閉じます。

新しいFCPデータドメインが **Storage** タブに表示されます。使用の準備が整っている間、**Locked** ステータスのままになります。準備が整った時点で、自動的にデータセンターにアタッチされます。

8.5.4. iSCSI または FCP ストレージの増設

iSCSI または FCP のストレージサイズを増やす方法は複数あります。

- 新しい LUN を持つ新しいストレージドメインを作成し、既存のデータセンターに追加します。 「[iSCSI ストレージの追加](#)」 を参照してください。
- 新しい LUN を作成し、既存のストレージドメインに追加します。
- 基盤となる LUN のサイズを変更することで、ストレージドメインを拡張します。

Red Hat Enterprise Linux 6™ システムで iSCSI ストレージの作成、設定、またはサイズ変更に関する情報は、[Red Hat Enterprise Linux 6 Storage Administration Guide](#) を参照してください。Red Hat Enterprise Linux 7™ システムについては、[Red Hat Enterprise Linux 7 Storage Administration Guide](#) を参照してください。

以下の手順では、既存のストレージドメインに新しい LUN を追加して、SAN(Storage Area Network)ストレージを拡張する方法を説明します。

手順8.9 既存の iSCSI または FCP ストレージドメインの拡張

1. SAN に新しい LUN を作成します。
2. **Storage resource** タブをクリックし、iSCSI または FCP ドメインを選択します。
3. **Manage Domain** ボタンをクリックします。
4. **Targets > LUNs** をクリックし、**Discover Targets** 拡張ボタンをクリックします。
5. ストレージサーバーの接続情報を入力し、**Discover** ボタンをクリックして接続を開始します。
6. **LUN > Targets** をクリックし、新しく利用可能になった LUN のチェックボックスを選択します。
7. **OK** をクリックして、選択したストレージドメインに LUN を追加します。

これにより、追加した LUN のサイズでストレージドメインが増えます。

基礎となる LUN のサイズを変更してストレージドメインを拡張する場合は、Red Hat Virtualization 管理ポータルで LUN も更新する必要があります。

手順8.10 LUN サイズの更新

1. **Storage resource** タブをクリックし、iSCSI または FCP ドメインを選択します。
2. **Manage Domain** ボタンをクリックします。
3. **LUN > Targets** の順にクリックします。
4. **Additional Size** 列で、LUN の **Add Additional Storage Size** ボタンをクリックして更新します。
5. **OK** をクリックして LUN を更新し、新規のストレージサイズを示します。

8.5.5. Red Hat Virtualization で使用できない LUN

特定の状況では、Red Hat Virtualization Manager では LUN を使用してストレージドメインまたは仮想マシンのハードディスクを作成することはできません。

- 現在の Red Hat Virtualization 環境にすでにある LUN は自動的に使用できなくなります。

図8.6 Red Hat Virtualization 管理ポータルで使用不可 LUN

	LUN ID	Dev. Size	#path	In Use	Vendor ID	Product ID	Serial
<input type="checkbox"/>	1IET_00010001	199GB	1	Used	IET	VIRTUAL-DIS	SIET_VIRTUAL-
<input type="checkbox"/>	1IET_00010004	0GB	1	Free	IET	VIRTUAL-DIS	SIET_VIRTUAL-
<input type="checkbox"/>	1IET_00010003	0GB	1	Free	IET	VIRTUAL-DIS	SIET_VIRTUAL-
<input type="checkbox"/>	1IET_00010002	0GB	1	Free	IET	VIRTUAL-DIS	SIET_VIRTUAL-

- SPM ホストによってすでに使用されている LUN は、使用中のよう表示されます。これらの LUN の内容を強制的に減らすこともできますが、操作が成功する保証はありません。

8.6. 既存のストレージドメインのインポート

8.6.1. 既存のストレージドメインのインポートの概要

データを含まない新しいストレージドメインを追加する他に、既存のストレージドメインをインポートし、それに含まれるデータにアクセスすることもできます。ストレージドメインをインポートする機能により、Manager データベースで障害が発生した場合にデータを復旧でき、あるデータセンターまたは環境から別のデータセンターにデータを移行できます。

以下は、各ストレージドメインタイプのインポートの概要です。

データ

既存のデータストレージドメインをインポートすると、そのデータストレージドメインに含まれるすべての仮想マシンやテンプレートにアクセスできるようになります。ストレージドメインをインポートした後、仮想マシン、フローティングディスクイメージ、テンプレートをデスティネーションデータセンターに手動でインポートする必要があります。データストレージドメインが含む仮想マシンやテンプレートをインポートするプロセスは、エクスポートストレージドメインの場合と同様です。ただし、データストレージドメインには、特定のデータセンター内のすべての仮想マシンとテンプレートが含まれているため、データ復旧や、データセンターや環境間で仮想マシンを大規模に移行する場合は、データストレージドメインのインポートを推奨します。



重要

互換性レベルが 3.5 以降のデータセンターに接続された既存のデータストレージドメインをインポートできます。

ISO

既存の ISO ストレージドメインをインポートすると、ISO ストレージドメインに含まれるすべての ISO ファイルと仮想ディスクにアクセスできます。これらのリソースにアクセスするために、ストレージドメインをインポートした後に追加の操作をする必要はなく、必要に応じて仮想マシンにアタッチすることができます。

Export

既存のエクスポートストレージドメインをインポートすると、エクスポートストレージドメインに含まれるすべての仮想マシンイメージとテンプレートにアクセスできるようになります。エクスポートドメインは仮想マシンのイメージとテンプレートをエクスポートおよびインポートするように設計されているため、環境内または環境間で少数の仮想マシンとテンプレートを移行するには、エクスポートストレージドメインをインポートすることが推奨されます。エクスポートストレージドメインとの間で仮想マシンおよびテンプレートをエクスポートおよびインポートする方法は、

『Virtual Machine Management Guide』の [Exporting and Importing Virtual Machines and Templates](#) を参照してください。



注記

エクスポートストレージドメインは非推奨になりました。ストレージデータドメインはデータセンターから接続を解除し、同じ環境または別の環境にある別のデータセンターにインポートすることができます。仮想マシン、フローティング仮想ディスクイメージ、およびテンプレートは、インポートされたストレージドメインからアタッチされたデータセンターにアップロードできます。

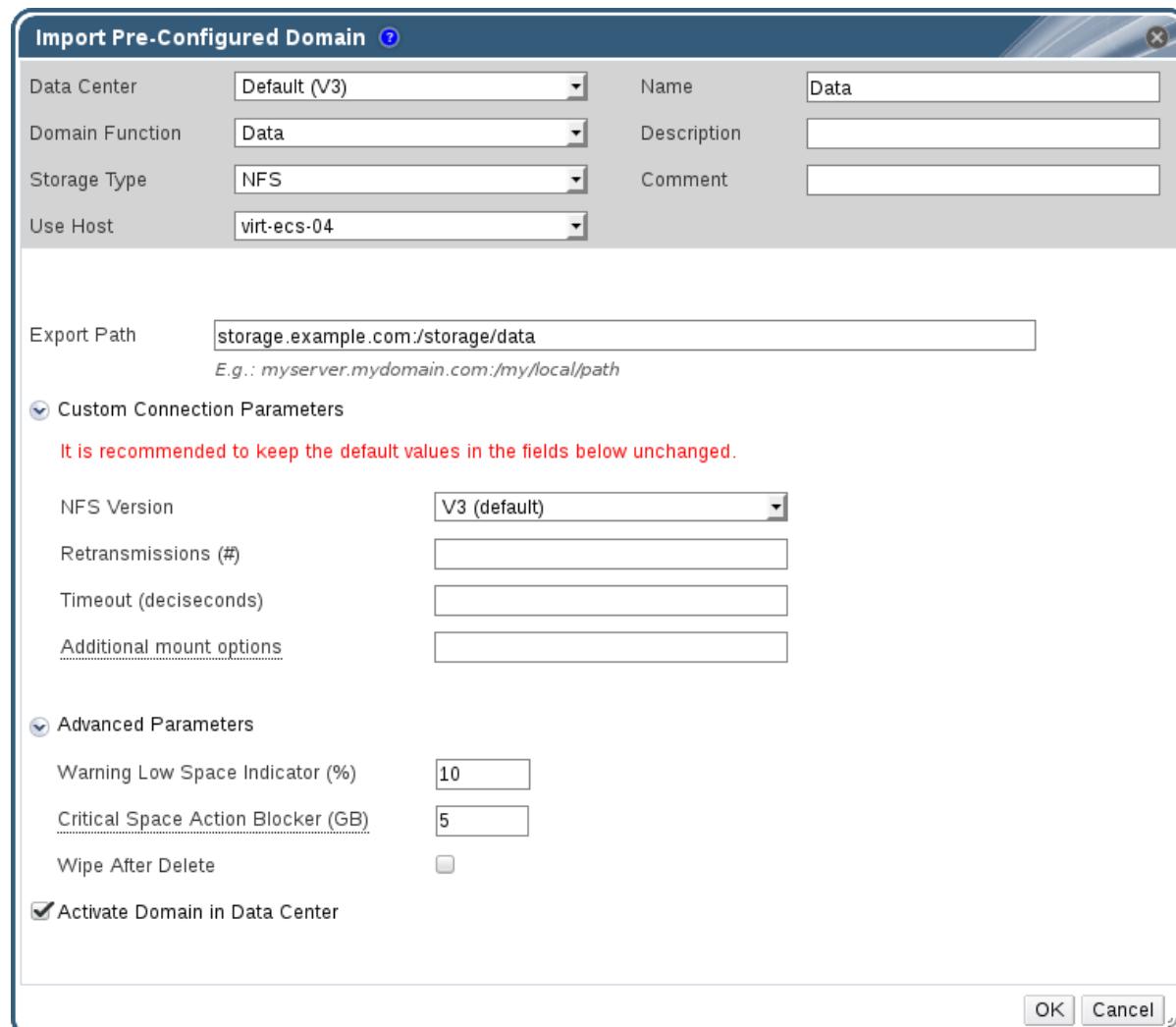
8.6.2. ストレージドメインのインポート

同じ環境または別の環境のデータセンターに以前に接続されていたストレージドメインをインポートします。この手順では、データの破損を防ぐために、ストレージドメインがどの環境のどのデータセンターにも接続されていないことを前提としています。既存のデータストレージドメインをインポートしてデータセンターに接続するには、ターゲットデータセンターを初期化する必要があります。

手順8.11ストレージドメインのインポート

1. **Storage** resource タブをクリックします。
2. **Import Domain** をクリックします。

図8.7 Import Pre-Configured Domain ウィンドウ



3. **Data Center** ドロップダウンリストから、ストレージドメインを接続するデータセンターを選択します。
4. ストレージドメインの名前を入力します。
5. 適切なドロップダウンリストから **Domain Function** および **Storage Type** を選択します。
6. Use host ドロップダウンリストから ホストを 選択します。



重要

ストレージドメインへの通信はすべて、Red Hat Virtualization Manager から直接ではなく、選択したホストを介して行われます。システムには、アクティブなホストが少なくとも 1 台存在し、選択したデータセンターにアタッチされている必要があります。ストレージドメインを設定する前には、全ホストがストレージデバイスにアクセスできる状態でなければなりません。

7. ストレージドメインの詳細を入力します。



注記

ドメイン **機能/ストレージタイプ** リストで選択した値に応じて、ストレージドメインの詳細を指定するためのフィールド。これらのオプションは、新しいストレージドメインの追加に使用できるオプションと同じです。これらのオプションの詳細は、「[ストレージドメインについて](#)」を参照してください。

8. 選択したデータセンターに接続した後にストレージドメインをアクティベートするには、**Activate Domain in Data Center** チェックボックスを選択します。

9. **OK** をクリックします。

ストレージドメインがインポートされ、**Storage** タブに表示されます。これで、仮想マシンとテンプレートをストレージドメインからデータセンターにインポートできます。

8.6.3. 同じ環境内のデータセンター間でのストレージドメインの移行

同じ Red Hat Virtualization 環境内のあるデータセンターから別のデータセンターにストレージドメインを移行して、宛先データセンターがストレージドメインに含まれるデータにアクセスできるようにします。この手順では、ストレージドメインのあるデータセンターから切り離し、別のデータセンターに接続します。

手順8.12 同じ環境内のデータセンター間でのストレージドメインの移行

1. 必要なストレージドメインで実行されているすべての仮想マシンをシャットダウンします。
2. **Storage resource** タブをクリックし、結果リストからストレージドメインを選択します。
3. 詳細ペインの **Data Center** タブをクリックします。
4. **Maintenance** をクリックした後、**OK** をクリックしてストレージドメインをメンテナンスマードに移動します。
5. **Detach** をクリックし、**OK** をクリックしてソースデータセンターからストレージドメインをデタッチします。
6. **アタッチ** をクリックします。
7. 宛先データセンターを選択し、**OK** をクリックします。

ストレージドメインは宛先データセンターにアタッチされ、自動的にアクティブになります。これで、仮想マシンとテンプレートをストレージドメインから宛先データセンターにインポートできます。

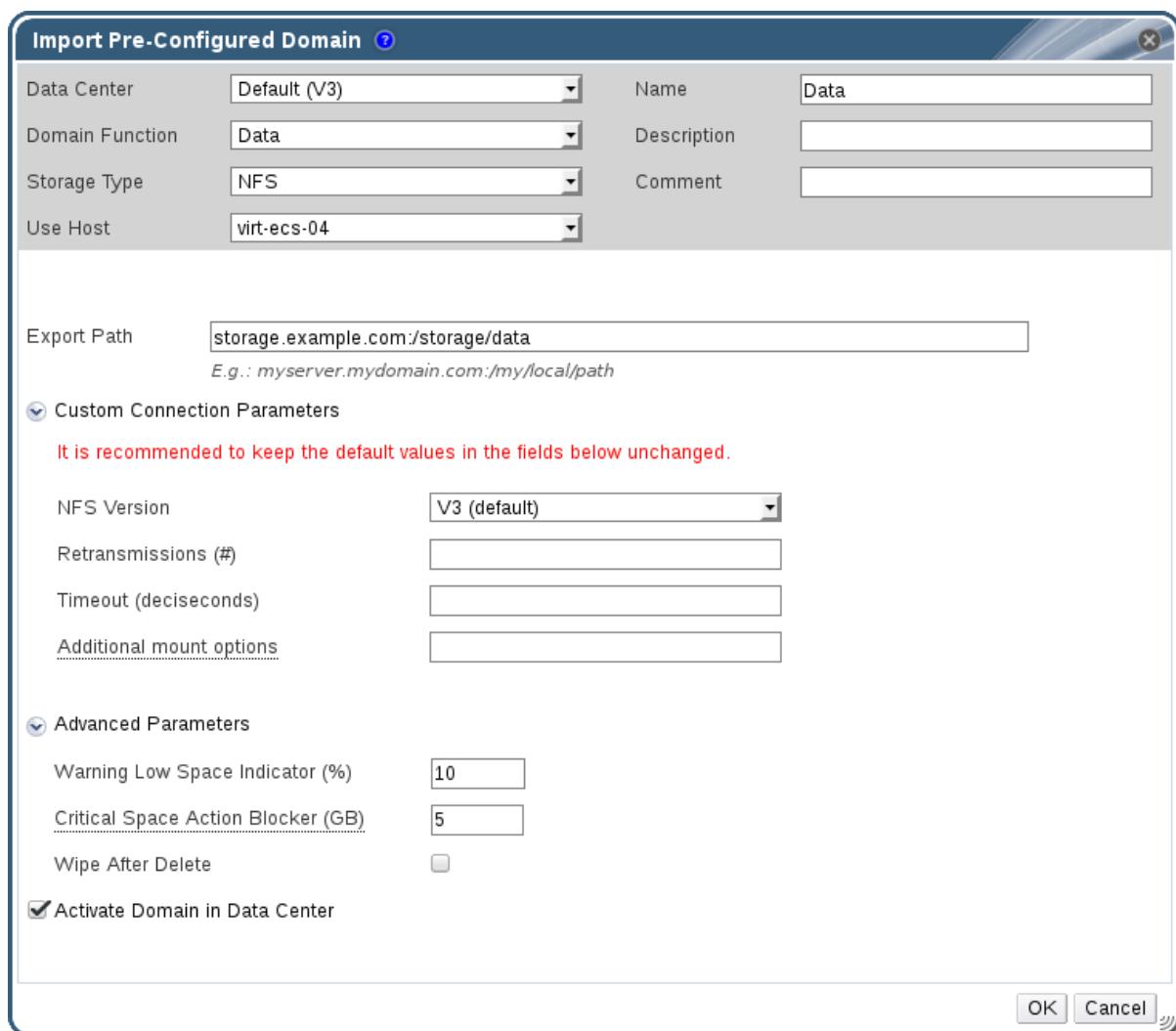
8.6.4. 異なる環境内のデータセンター間でのストレージドメインの移行

ストレージドメインのある Red Hat Virtualization 環境から別の環境に移行して、移行先環境がストレージドメインに含まれるデータにアクセスできるようにします。この手順では、1つの Red Hat Virtualization 環境からストレージドメインを削除し、それを別の環境にインポートします。既存のデータストレージドメインをインポートして Red Hat Virtualization データセンターに接続するには、ストレージドメインのソースデータセンターの互換性レベルが 3.5 以上である必要があります。

手順8.13 異なる環境内のデータセンター間でのストレージドメインの移行

1. ソース環境の管理ポータルにログインします。
2. 必要なストレージドメインで実行されているすべての仮想マシンをシャットダウンします。
3. **Storage resource** タブをクリックし、結果リストからストレージドメインを選択します。
4. 詳細ペインの **Data Center** タブをクリックします。
5. **Maintenance** をクリックした後、**OK** をクリックしてストレージドメインをメンテナンスモードに移動します。
6. **Detach** をクリックし、**OK** をクリックしてソースデータセンターからストレージドメインをデタッチします。
7. **削除** をクリックします。
8. **Remove Storage (s)** ウィンドウで **Format Domain, i.e. Storage Content will be lost!** チェックボックスが選択されていません。この手順では、後で使用できるようにデータをストレージドメインに保存します。
9. **OK** をクリックすると、ソース環境からストレージドメインが削除されます。
10. 宛先環境の管理ポータルにログインします。
11. **Storage resource** タブをクリックします。
12. **Import Domain** をクリックします。

図8.8 Import Pre-Configured Domain ウィンドウ



13. **Data Center** ドロップダウンリストから宛先データセンターを選択します。
14. ストレージドメインの名前を入力します。
15. 適切なドロップダウンリストから **Domain Function** および **Storage Type** を選択します。
16. **Use Host** ドロップダウンリストからホストを選択します。
17. ストレージドメインの詳細を入力します。



注記

Storage Type ドロップダウンリストで選択した値に応じて、ストレージドメインの詳細を指定するためのフィールドが変更されます。これらのオプションは、新しいストレージドメインの追加に使用できるオプションと同じです。これらのオプションの詳細は、「[ストレージドメインについて](#)」を参照してください。

18. ストレージドメインのアタッチ時に自動的にアクティブ化するには、**Activate Domain in Data Center** チェックボックスを選択します。
19. **OK** をクリックします。

ストレージドメインは、新しい Red Hat Virtualization 環境の宛先データセンターに接続され、自動的にアクティブ化されます。これで、インポートしたストレージドメインから宛先データセンターに、仮想マシンおよびテンプレートをインポートできます。

8.6.5. インポート済みデータストレージドメインからの仮想マシンのインポート

Red Hat Virtualization 環境にインポートしたデータストレージドメインから仮想マシンをインポートします。この手順は、インポートされたデータストレージドメインがデータセンターに接続され、アクティブ化されていることを前提としています。

手順8.14 インポートされたデータストレージドメインからの仮想マシンのインポート

1. **Storage** resource タブをクリックします。
2. インポートされたデータストレージドメインをクリックします。
3. 詳細ペインの **VM Import** タブをクリックします。
4. インポートする1つ以上の仮想マシンを選択します。
5. **Import** をクリックします。
6. **Cluster** 一覧から仮想マシンをインポートするクラスターを選択します。
7. **OK** をクリックします。

1つ以上の仮想マシンを環境にインポートしている。インポートされた仮想マシンは、**VM Import** タブの下の一覧に表示されなくなりました。

8.6.6. インポートされたデータストレージドメインからのテンプレートのインポート

Red Hat Virtualization 環境にインポートしたデータストレージドメインからテンプレートをインポートします。この手順は、インポートされたデータストレージドメインがデータセンターに接続され、アクティブ化されていることを前提としています。

手順8.15 インポートされたデータストレージドメインからのテンプレートのインポート

1. **Storage** resource タブをクリックします。
2. インポートされたデータストレージドメインをクリックします。
3. 詳細ペインで **Template Import** タブをクリックします。
4. インポートする1つ以上のテンプレートを選択します。
5. **Import** をクリックします。
6. **Cluster** 一覧からテンプレートをインポートするクラスターを選択します。
7. **OK** をクリックします。

1つ以上のテンプレートを環境にインポートしている。インポートされたテンプレートは、**Template Import** タブの下のリストに表示されなくなります。

8.6.7. インポートされたストレージドメインからのディスクイメージのインポート

詳細ペインの **Disk Import** タブを使用して、インポートされたストレージドメインからフローティング仮想ディスクをインポートします。



注記

Manager にインポートできるのは QEMU 互換ディスクのみです。

手順8.16 ディスクイメージのインポート

1. データセンターにインポートされたストレージドメインを選択します。
2. 詳細ペインで、**Disk Import** をクリックします。
3. 1つ以上のディスクイメージを選択し、**Import** をクリックして **Import Disk (s)** ウィンドウを開きます。
4. 各ディスクに適切なディスクプロファイルを選択します。
5. **OK** をクリックして、選択したディスクをインポートします。

8.6.8. インポートされたストレージドメインからの未登録のディスクイメージのインポート

詳細ペインの **Disk Import** タブを使用して、ストレージドメインからフローティング仮想ディスクをインポートします。Red Hat Virtualization 環境の外部で作成されたフローティングディスクは、Manager には登録されません。ストレージドメインをスキャンして、インポートする未登録のフローティングディスクを特定します。



注記

Manager にインポートできるのは QEMU 互換ディスクのみです。

手順8.17 ディスクイメージのインポート

1. データセンターにインポートされたストレージドメインを選択します。
2. ストレージドメインを右クリックし、**Scan Disks** を選択して、Manager が未登録のディスクを特定できるようにします。
3. 詳細ペインで、**Disk Import** をクリックします。
4. 1つ以上のディスクイメージを選択し、**Import** をクリックして **Import Disk (s)** ウィンドウを開きます。
5. 各ディスクに適切なディスクプロファイルを選択します。
6. **OK** をクリックして、選択したディスクをインポートします。

8.7. ストレージタスク

8.7.1. ISO ストレージドメインの設定

ISOストレージドメインはデータセンターにアタッチされています。ISOイメージはアップロードする必要があります。Red Hat Virtualizationは、正しいユーザーパーミッションでイメージが正しいディレクトリーパスにアップロードされるようにISOアップローダーツールを提供します。

物理メディアからのISOイメージの作成については、本書では説明しません。環境に必要なイメージにアクセスできることを前提とします。

手順8.18 ISOストレージドメインの設定

1. Red Hat Virtualization Managerを実行しているシステムの一時ディレクトリーに、必要なISOイメージをコピーします。
2. Red Hat Virtualization Managerを実行しているシステムに**root**ユーザーとしてログインします。
3. **engine-iso-uploader**コマンドを使用してISOイメージをアップロードします。このアクションには多少時間がかかります。時間は、アップロードされるイメージのサイズと利用可能なネットワーク帯域幅によって異なります。

例8.1 ISOアップローダーの使用

この例では、ISOイメージ**RHEL6.iso**は、NFSを使用して**ISO Domain**というISOドメインにアップロードされます。このコマンドは、管理ユーザー名とパスワードの入力を要求します。ユーザー名は、ユーザー名@ドメインの形式で指定する必要があります。

```
# engine-iso-uploader --iso-domain=ISODomain upload RHEL6.iso
```

ISOイメージがアップロードされ、指定されたISOストレージドメインに表示されます。ストレージドメインが接続されているデータセンターに仮想マシンを作成する際には、利用可能なブートメディアのリストでも利用できます。

8.7.2. ストレージドメインのメンテナンスマードへの移行

ストレージドメインをデタッチおよび削除するには、メンテナンスマードにする必要があります。これは、別のデータドメインをマスターデータドメインとして再指定するために必要です。

LUNを追加してiSCSIドメインを拡張できるのは、ドメインがアクティブな場合のみです。

手順8.19 ストレージドメインのメンテナンスマードへの移行

1. ストレージドメインで実行しているすべての仮想マシンをシャットダウンします。
2. **Storage resource**タブをクリックし、ストレージドメインを選択します。
3. 詳細ペインの**データセンター**タブをクリックします。
4. **Maintenance**をクリックして、**Storage Domain maintenance**の確認ウィンドウを開きます。
5. **OK**をクリックしてメンテナンスマードを開始します。ストレージドメインは非アクティブ化され、結果リストに**Inactive**ステータスが表示されます。

これで、データセンターから非アクティブなストレージドメインを編集、デタッチ、削除、または再アクティブ化できます。



注記

また、関連付けられているデータセンターの詳細ペインの Storage タブを使用して、ドメインをメンテナنسモードにアクティブ化、デタッチ、および配置することもできます。

8.7.3. ストレージドメインの編集

管理ポータルからストレージドメインパラメーターを編集できます。ストレージドメインの状態(アクティブまたは非アクティブ)に応じて、さまざまなフィールドを編集できます。**Data Center**、**Domain Function**、**Storage Type**、**Format**などのフィールドは変更できません。

- **アクティブ:** ストレージドメインがアクティブ状態の場合、**Name**、**Description**、**Comment**、**Warning Low Space Indicator (%)**、**Critical Space Action Blocker (GB)**、および**Wipe After Delete** フィールドを編集できます。**Name** フィールドは、ストレージドメインがアクティブな間のみ編集できます。他のすべてのフィールドは、ストレージドメインが非アクティブのときに編集することもできます。
- **Inactive:** ストレージドメインがメンテナスモードまたはアタッチされていない状態の場合、非アクティブ状態の場合、**Name**、**Data Center**、**Domain Function**、**Storage Type**、および**Format** を除くすべてのフィールドを編集できます。ストレージ接続、マウントオプション、およびその他の高度なパラメーターを編集するには、ストレージドメインを非アクティブにする必要があります。これは、NFS、POSIX、およびローカルストレージタイプでのみサポートされます。



注記

iSCSI ストレージ接続は、管理ポータルを介して編集することはできませんが、REST API を介して編集することができます。『REST API Guide』の [Updating an iSCSI Storage Connection](#) を参照してください。

手順8.20 アクティブなストレージドメインの編集

1. **Storage** resource タブをクリックし、ストレージドメインを選択します。
2. **Manage Domain** をクリックします。
3. 必要に応じて、使用可能なフィールドを編集します。
4. **OK** をクリックします。

手順8.21 非アクティブなストレージドメインの編集

1. **Storage** resource タブをクリックし、ストレージドメインを選択します。
2. ストレージドメインがアクティブな場合は、詳細ペインの **Data Center** タブをクリックし、**Maintenance** をクリックします。
3. **Manage Domain** をクリックします。
4. 必要に応じて、ストレージパスおよびその他の詳細を編集します。新しい接続の詳細は、元の接続と同じストレージタイプである必要があります。
5. **OK** をクリックします。
6. 詳細ペインの **Data Center** タブをクリックし、**Activate** をクリックします。

8.7.4. メンテナンスマードからのストレージドメインのアクティブ化

データセンターのストレージに変更を加えている場合は、ストレージドメインをメンテナンスマードにする必要があります。ストレージドメインをアクティブ化して、使用を再開します。

1. **Storage resource** タブをクリックし、結果一覧で非アクティブなストレージドメインを選択します。
2. 詳細ペインの **データセンター** タブをクリックします。
3. 適切なストレージドメインを選択し、**Activate** をクリックします。



重要

データドメインをアクティブ化する前に ISO ドメインをアクティブ化しようとすると、エラーメッセージが表示され、ドメインはアクティブ化されません。

8.7.5. ストレージドメインの削除

データセンターに、仮想化環境から削除するストレージドメインがあります。

手順8.22 ストレージドメインの削除

1. **Storage resource** タブをクリックし、結果一覧で適切なストレージドメインを選択します。
2. ドメインをメンテナーンスマードに切り替え、非アクティブにします。
3. データセンターからドメインをデタッチします。
4. **Remove** をクリックして、ストレージの **削除の確認** ウィンドウを開きます。
5. 一覧からホストを選択します。
6. **OK** をクリックしてストレージドメインを削除し、ウィンドウを閉じます。

ストレージドメインは環境から完全に削除されます。

8.7.6. ストレージドメインの破棄

エラーが発生したストレージドメインは、通常の手順では削除できない場合があります。ストレージドメインを破棄すると、エクスポートディレクトリを参照せずに、仮想化環境からストレージドメインが強制的に削除されます。

ストレージドメインが破棄されたら、再度使用する前にストレージドメインのエクスポートディレクトリーを手動で修正する必要があります。

手順8.23 ストレージドメインの破棄

1. **Storage resource** タブ、ツリーモード、または検索機能を使用して、結果一覧で適切なストレージドメインを見つけて選択します。
2. ストレージドメインを右クリックし、**Destroy** を選択して **Destroy Storage Domain** の確認 ウィンドウを開きます。
3. **Approve operation** チェックボックスを選択し、**OK** をクリックしてストレージドメインを破棄し、ウィンドウを閉じます。

ストレージドメインが破棄されました。ストレージドメインのエクスポートディレクターを手動でクリーンアップし、それをリサイクルします。

8.7.7. データセンターからストレージドメインをデタッチ

ストレージドメインをデータセンターから切り離し、仮想マシンとテンプレートを別のデータセンターに移行します。

手順8.24 データセンターからストレージドメインをデタッチ

1. **Storage resource** タブをクリックし、結果リストからストレージドメインを選択します。
2. 詳細ペインの **Data Centers** タブをクリックし、ストレージドメインを選択します。
3. **Maintenance** をクリックして、**Maintenance Storage Domain (s)** の確認ウィンドウを開きます。
4. **OK** をクリックしてメンテナンスマードを開始します。
5. **Detach** をクリックして、**Detach Storage** の確認ウィンドウを開きます。
6. **OK** をクリックして、ストレージドメインを切り離します。

ストレージドメインがデータセンターから切り離され、別のデータセンターに接続できるようになりました。

8.7.8. ストレージドメインのデータセンターへのアタッチ

ストレージドメインをデータセンターに接続します。

手順8.25 ストレージドメインのデータセンターへのアタッチ

1. **Storage resource** タブをクリックし、結果リストからストレージドメインを選択します。
2. 詳細ペインの **データセンター** タブをクリックします。
3. **Attach** をクリックして **Attach to Data Center** ウィンドウを開きます。
4. 適切なデータセンターのラジオボタンを選択します。
5. **OK** をクリックしてストレージドメインをアタッチします。

ストレージドメインはデータセンターにアタッチされ、自動的にアクティブになります。

8.7.9. ディスクプロファイル

ディスクプロファイルは、ストレージドメイン内の仮想ディスクのスループットの最大レベルと入出力操作の最大レベルを定義します。ディスクプロファイルは、データセンターで定義されたストレージプロファイルに基づいて作成され、プロファイルを有効にするには、個々の仮想ディスクに手動で割り当てる必要があります。

8.7.9.1. ディスクプロファイルの作成

ディスクプロファイルを作成します。この手順は、ストレージドメインが属するデータセンターの下に1つ以上のストレージサービス品質エントリーがすでに定義されていることを前提としています。

手順8.26 ディスクプロファイルの作成

1. **Storage** resource タブをクリックし、データストレージドメインを選択します。
2. 詳細ペインの **ディスクプロファイル** サブタブをクリックします。
3. **New** をクリックします。
4. 名前 フィールドにディスクプロファイルの名前を入力します。
5. Description フィールドに、ディスクプロファイルの **説明** を入力します。
6. **QoS** 一覧からディスクプロファイルに適用するサービスの品質を選択します。
7. **OK** をクリックします。

ディスクプロファイルを作成し、そのディスクプロファイルをデータストレージドメインでホストされる新しい仮想ディスクに適用できる。

8.7.9.2. ディスクプロファイルの削除

Red Hat Virtualization 環境から既存のディスクプロファイルを削除します。

手順8.27 ディスクプロファイルの削除

1. **Storage** resource タブをクリックし、データストレージドメインを選択します。
2. 詳細ペインの **ディスクプロファイル** サブタブをクリックします。
3. 削除するディスクプロファイルを選択します。
4. **削除** をクリックします。
5. **OK** をクリックします。

ディスクプロファイルを削除し、そのディスクプロファイルは利用できなくなりました。ディスクプロファイルがいずれかの仮想ディスクに割り当てられている場合、ディスクプロファイルはそれらの仮想ディスクから削除されます。

8.7.10. ストレージドメインのヘルステータスの表示

ストレージドメインには、通常のステータスに加えて、外部のヘルステータスがあります。外部の正常性ステータスはプラグインまたは外部システムによって報告されるか、管理者が設定し、ストレージドメインの **Name** の左側に以下のいずれかのアイコンとして表示されます。

- **OK:** No icon
- **情報:** 
- **警告:** 
- **エラー:** 
- **失敗:** 

ストレージドメインのヘルスステータスの詳細を表示するには、ストレージドメインを選択し、Events サブタブをクリックします。

ストレージドメインのヘルスステータスは、REST API を使用して表示することもできます。ストレージドメインでの GET リクエストには、ヘルスステータスを含む **external_status** 要素が含まれます。

events コレクションを介して、REST API でストレージドメインのヘルスステータスを設定できます。詳細は、『REST API Guide』の [Adding Events](#) を参照してください。

8.8. ストレージおよびパーミッション

8.8.1. ストレージドメインのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルのすべての側面を管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限された管理者ロールは、特定のリソースに制限される管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、そのデータセンターのストレージを除く、割り当てられたデータセンターの管理者権限のみを持ち、**ClusterAdmin** は割り当てられたクラスターに対してのみ管理者権限を持ちます。

ストレージ管理者は、特定のストレージドメインのみのシステム管理ロールです。これは、複数のストレージドメインを持つデータセンターで、各ストレージドメインにシステム管理者が必要な場合に有効です。ヘッダーバーの **Configure** ボタンを使用して、環境内のすべてのストレージドメインにストレージ管理者を割り当てます。

ストレージドメイン管理者ロールは、以下のアクションを許可します。

- ストレージドメインの設定の編集。
- ストレージドメインのメンテナンスモードへの切り替え。
- ストレージドメインの削除。



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てるすることができます。

また、既存のシステム管理者を削除し、新しいシステム管理者を追加すると、ストレージドメインのシステム管理者を変更できます。

8.8.2. ストレージ管理者ロールの概要

ストレージドメインパーミッションロール

以下の表は、ストレージドメインの管理に適用される管理者ロールおよび権限について説明しています。

表8.1 Red Hat Virtualization システム管理者ロール

ロール	権限	注記
StorageAdmin	ストレージ管理者	特定のストレージドメインを作成、削除、設定、および管理できます。

ロール	権限	注記
GlusterAdmin	Gluster Storage 管理者	Gluster ストレージボリュームを作成、削除、設定、および管理できます。

8.8.3. 管理者またはユーザーロールのリソースへの割り当て

管理者またはユーザーロールをリソースに割り当て、ユーザーがそのリソースにアクセスしたり、管理したりできるようにします。

手順8.28 リソースへのロールの割り当て

- リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
- 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
- Add** をクリックします。
- Search** テキストボックスに既存ユーザーの名前またはユーザー名を入力し、**Go** をクリックします。表示された候補の中からユーザーを選択します。
- Role to Assign:** ドロップダウンリストからロールを選択します。
- OK** をクリックします。

ユーザーにロールを割り当てました。そのリソースで有効にしたそのロールの継承されたパーミッションが、ユーザーに付与されました。

8.8.4. リソースからの管理者またはユーザーロールの削除

管理者またはユーザーのロールをリソースから削除すると、ユーザーはそのリソースのロールに関連付けられ継承されたパーミッションを失います。

手順8.29 リソースからのロールの削除

- リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
- 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
- リソースから削除するユーザーを選択します。
- Remove** をクリックします。**Remove Permission** 画面が開き、パーミッションの削除を確認します。
- OK** をクリックします。

ユーザーのロールおよび関連付けられたパーミッションをリソースから削除しました。

第9章 RED HAT GLUSTER STORAGE の使用

9.1. RED HAT GLUSTER STORAGE ノード

9.1.1. Red Hat Gluster Storage ノードの追加

Red Hat Gluster Storage ノードを Gluster 対応クラスターに追加し、GlusterFS ボリュームとブリックを Red Hat Virtualization 環境に組み込みます。

この手順では、適切な [互換バージョン](#) の Gluster 対応クラスターと Red Hat Gluster Storage ノードがすでに設定されていることを前提としています。Red Hat Gluster Storage ノードの設定に関する情報は、[Red Hat Gluster Storage インストールガイド](#) を参照してください。互換性マトリックスの詳細は、[Red Hat Gluster Storage バージョンの互換性とサポート](#) を参照してください。

手順9.1 Red Hat Gluster Storage ノードの追加

1. **Hosts** resource タブをクリックして、結果一覧のホストを一覧表示します。
2. **New** をクリックして、**New Host** ウィンドウを開きます。
3. ドロップダウンメニューを使用して、Red Hat Gluster Storage ノードの **Data Center** および **Host Cluster** を選択します。
4. Red Hat Gluster Storage ノードの **Name**、**Address**、および **SSH Port** を入力します。
5. Red Hat Gluster Storage ノードで使用する認証方法を選択します。
 - パスワード認証を使用するには、root ユーザーのパスワードを入力します。
 - **SSH PublicKey** フィールドに表示されるキーを Red Hat Gluster Storage ノードの `/root/.ssh/authorized_keys` にコピーして、公開鍵認証を使用します。
6. **OK** をクリックしてノードを追加し、ウィンドウを閉じます。

Red Hat Virtualization 環境に Red Hat Gluster Storage ノードを追加している。環境内のノードのボリュームおよびブリックリソースを使用できるようになりました。

9.1.2. Red Hat Gluster Storage ノードの削除

Red Hat Virtualization 環境から Red Hat Gluster Storage ノードを削除します。

手順9.2 Red Hat Gluster Storage ノードの削除

1. ホストリソースタブ、ツリーモード、または検索機能を使用して、結果一覧で Red Hat Gluster Storage ノードを見つけて選択します。
2. **Maintenance** をクリックして、メンテナーンスホストの確認ウィンドウを開きます。
3. **OK** をクリックして、ホストをメンテナーンスマードに切り替えます。
4. **Remove** をクリックして、**Remove Host (s)** 確認ウィンドウを開きます。
5. ノードにボリュームブリックがある場合、またはノードが応答しない場合は **Force Remove** チェックボックスを選択します。

6. **OK** をクリックしてノードを削除し、ウィンドウを閉じます。

Red Hat Gluster Storage ノードが環境から削除され、**Hosts** タブに表示されなくなりました。

9.2. ストレージドメインとしての RED HAT GLUSTER STORAGE の使用

9.2.1. Red Hat Gluster Storage (GlusterFS)ボリュームの概要

Red Hat Gluster Storage ボリュームは、複数の Red Hat Gluster Storage サーバーから単一のグローバル namespace にストレージを統合します。ボリュームはブリックのコレクションです。各ブリックは、信頼できるストレージプールの Red Hat Gluster Storage Server のマウントポイントまたはディレクトリーです。

Red Hat Gluster Storage の管理操作のほとんどは、ボリュームで行われます。

管理ポータルを使用して、新しいボリュームを作成および起動できます。**Volumes** タブから、Red Hat Gluster Storage クラスターでボリュームを監視できます。

ボリュームは管理ポータルから作成および管理できますが、管理ポータルを使用してボリュームに追加する前に、ブリックを個別の Red Hat Gluster Storage ノードに作成する必要があります。

9.2.2. Gluster Storage の用語

表9.1データセンターのプロパティー

用語	定義
ブリック	<p>ブリックは、ストレージの GlusterFS の基本単位であり、信頼できるストレージプールのサーバーのエクスポートディレクトリーで表されます。ブリックは、以下の形式でサーバーをエクスポートディレクトリーと組み合わせることで表現されます。</p> <p>SERVER:EXPORT</p> <p>以下に例を示します。</p> <p>myhostname:/exports/myexportdir/</p>
Block Storage	ブロック特殊ファイルまたはブロックデバイスは、システムがブロック形式でデータを移動するデバイスに対応します。これらのデバイスノードは、多くの場合、ハードディスク、CD-ROM ドライブ、メモリーリージョンなどのアドレス指定可能なデバイスを表します。Red Hat Gluster Storage は、拡張属性を持つ XFS ファイルシステムをサポートします。
Cluster	リンクされたコンピューターの信頼できるプール。これは、1台のコンピューターを形成する多くの点で密接に機能します。Red Hat Gluster Storage の用語では、クラスターは信頼できるストレージプールと呼ばれます。
クライアント	ボリュームをマウントするマシン（これはサーバーでもあります）。

用語	定義
分散ファイルシステム	複数のクライアントが、信頼できるストレージプール内の複数のサーバー/ブリックに分散したデータを同時にアクセスできるようにするファイルシステム。複数の場所間でのデータ共有は、すべての分散ファイルシステムに基本となります。
Geo レプリケーション	Geo レプリケーションは、ローカルエリアネットワーク(LAN)、Wide Area Network (WAN)、およびインターネット全体で、サイトから別のサイトへの継続的な非同期および増分レプリケーションサービスを提供します。
glusterd	信頼できるストレージプールのすべてのサーバーで実行する必要がある Gluster 管理デーモン。
メタデータ	メタデータは、1つ以上の他のデータに関する情報を提供するデータです。
N-way レプリケーション	ローカル同期データレプリケーションは通常、キャプライスまたは Amazon Web Services アベイラビリティゾーン全体にデプロイされます。
Namespace	名前空間は、一意の識別子またはシンボルの論理グループを保持するために作成された抽象コンテナーまたは環境です。Red Hat Gluster Storage の信頼される各ストレージプールは、単一の namespace を、信頼できるストレージプール内のすべてのファイルを含む POSIX マウントポイントとして公開します。
POSIX	Portable Operating System Interface (Unix 用)は、アプリケーションプログラミングインターフェイス (API)を定義するために IEEE によって指定される関連標準ファミリーの名前と、UNIX オペレーティングシステムのバリアントと互換性のあるソフトウェアのシェルおよびユーティリティーインターフェイスです。Red Hat Gluster Storage は、完全に POSIX 互換のファイルシステムをエクスポートします。
RAID	RAID(Redundant Array of Inexpensive Disks)は、冗長性によりストレージの信頼性を強化し、複数の低成本で信頼性が低いディスクドライブコンポーネントを、アレイ内のすべてのドライブが相互に依存する論理ユニットに統合する技術です。
RRDNS	Round Robin Domain Name Service (RRDNS) は、アプリケーションサーバー間で負荷を分散する方法です。RRDNS は、DNS サーバーのゾーンファイルに同じ名前と異なる IP アドレスを持つ複数の A レコードを作成して実装されます。
Server	データが保存される実際のファイルシステムをホストするマシン（仮想マシンまたはベアメタル）。

用語	定義
スケールアップストレージ	ストレージデバイスの容量を増やしますが、これは単一のディメンションでのみあります。たとえば、信頼できるストレージプールの1台のコンピューターにディスク容量を追加するとします。
スケールアウトストレージ	複数のディメンションのストレージデバイスの機能を増やします。たとえば、信頼できるストレージプールにサーバーを追加すると、信頼できるストレージプールのCPU、ディスク容量、およびスループットが向上します。
サブボリューム	サブボリュームは、少なくとも1つのトランスレーターによって処理された後のブリックです。
トランスレーター	トランスレーターは1つ以上のサブボリュームに接続し、それらのボリュームで操作を行い、サブボリューム接続を提供します。
信頼済みストレージプール	ストレージプールは、ストレージサーバーの信頼済みネットワークです。最初のサーバーを起動すると、ストレージプールはそのサーバーのみで設定されます。
ユーザー空間	ユーザー空間で実行しているアプリケーションは、アクセスの調整にカーネルを使用する代わりにハードウェアと直接対話しません。ユーザー空間アプリケーションは通常、カーネル領域のアプリケーションよりも移植可能です。Glusterはユーザー空間アプリケーションです。
Virtual File System (VFS)	VFSは、標準のLinuxファイルシステムに関連するすべてのシステムコールを処理するカーネルソフトウェア層です。これは、複数の種類のファイルシステムへの共通のインターフェイスを提供します。
ボリュームファイル	ボリュームファイルはGlusterFSプロセスで使用される設定ファイルです。ボリュームファイルは、通常 <code>/var/lib/glusterd/vols/VOLNAME</code> に保存されます。
ボリューム	ボリュームは、ブリックの論理コレクションです。Gluster管理操作のほとんどは、ボリュームで行われます。

9.2.3. Red Hat Gluster Storage ボリュームをストレージドメインとして割り当てる

ストレージドメインとして直接使用するRed Hat Virtualization ManagerにRed Hat Gluster Storageボリュームを追加します。これは、Red Hat Storage Glusterノードの追加とは異なります。これにより、Red Hat Virtualization Manager内からのノードのボリュームおよびブリックの制御が可能になり、Gluster対応クラスターは必要ありません。

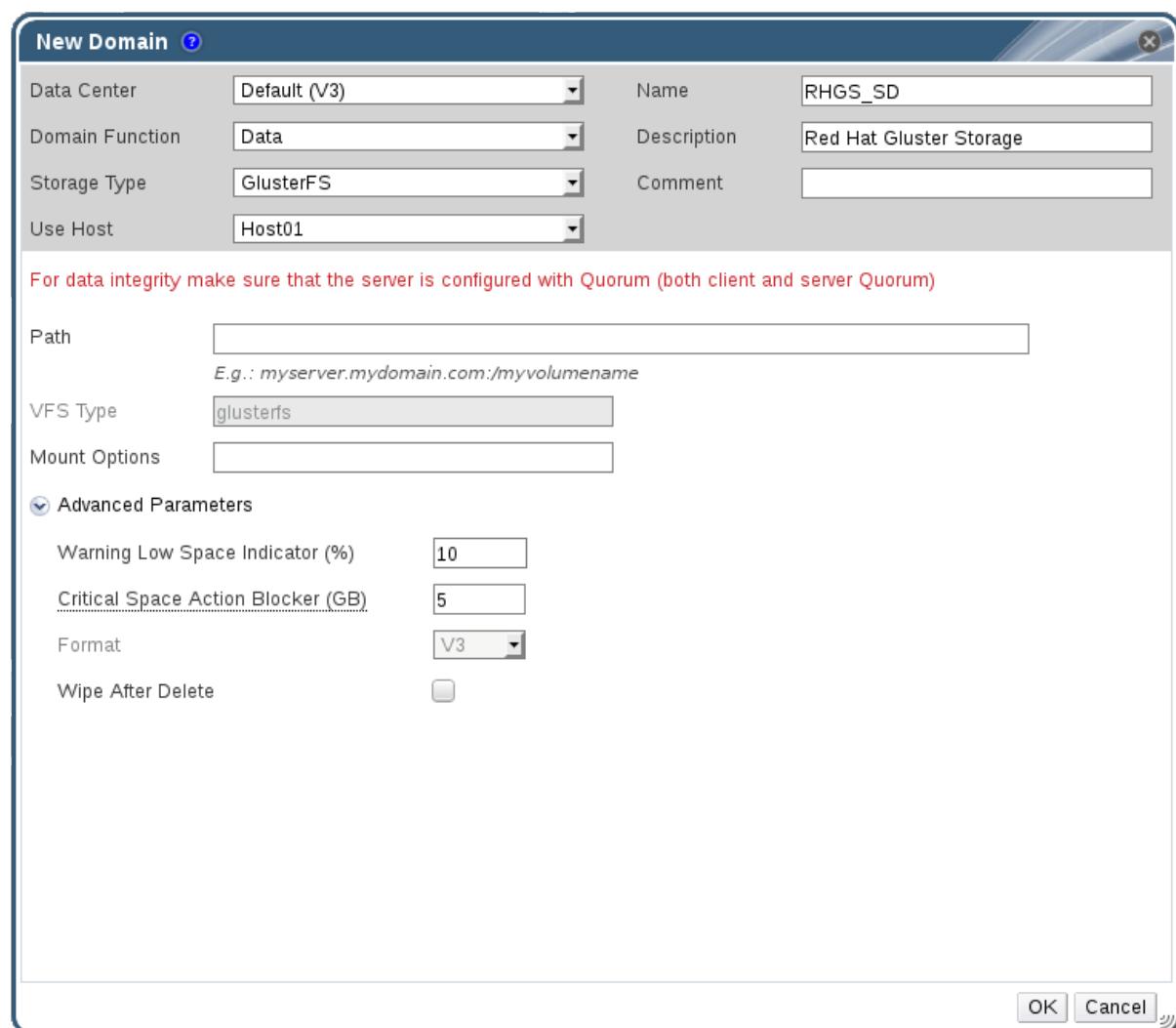
ホストをマウントするには、glusterfs パッケージ、glusterfs-fuse パッケージ、および glusterfs-cli パッケージをインストールする必要があります。glusterfs-cli パッケージは、カスタマーportalの **rh-common-rpms** チャンネルから入手できます。

Red Hat Gluster Storage ノードの設定に関する情報は、[Red Hat Gluster Storage インストールガイド](#) を参照してください。Red Hat Storage Gluster ボリュームで使用するホストの準備に関する詳細は、[Configuring Red Hat Virtualization with Red Hat Gluster Storage Guide](#) を参照してください。互換性マトリックスの詳細は、[Red Hat Gluster Storage バージョンの互換性とサポート](#) を参照してください。

手順9.3 ストレージドメインとしての Red Hat Gluster Storage ボリュームの追加

1. **Storage** resource タブをクリックして、結果一覧で既存のストレージドメインを一覧表示します。
2. **New Domain** をクリックして、**New Domain** ウィンドウを開きます。

図9.1 Red Hat Gluster Storage



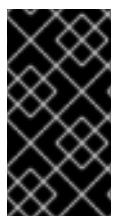
3. ストレージドメインの **Name** を入力します。
4. ストレージドメインに関連付ける **データセンター** を選択します。
5. **Domain Function** ドロップダウンリストから **Data** を選択します。
6. **Storage Type** ドロップダウンリストから **GlusterFS** を選択します。

7. **Use Host** ドロップダウンリストからホストを選択します。選択したデータセンター内のホストのみが一覧表示されます。ボリュームをマウントするには、選択したホストに glusterfs パッケージおよび glusterfs-fuse パッケージがインストールされている必要があります。
8. **Path** フィールドに、Red Hat Gluster Storage サーバーの IP アドレスまたは FQDN を入力し、ボリューム名をコロンで区切って入力します。
9. 通常 **mount** コマンドに **-o** 引数を指定して指定するように、追加の **Mount Options** を入力します。このマウントオプションはコンマ区切りリストで提示してください。有効なマウントオプションの一覧は、**man mount** を参照してください。
10. オプションで、詳細パラメーターを設定することができます。
 - a. **Advanced Parameters** をクリックします。
 - b. **Warning Low Space Indicator** フィールドにパーセンテージ値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーに警告メッセージが表示され、ログに記録されます。
 - c. **Critical Space Action Blocker** フィールドに GB の値を入力します。ストレージドメインの空き容量がこの値を下回ると、ユーザーにエラーメッセージが表示され、ログに記録されます。容量を消費する新規アクションは、一時的であってもすべてブロックされます。
 - d. 削除後に **Wipe After Delete** チェックボックスを選択します。このオプションは、ドメインの作成後に編集することが可能ですが、その場合にはすでに存在していたディスクの削除後にワイププロパティーは変更されません。
11. **OK** をクリックしてボリュームをストレージドメインとしてマウントし、ウィンドウを閉じます。

9.2.4. ストレージボリュームの作成

管理ポータルを使用して、新しいボリュームを作成できます。新しいボリュームを作成する場合は、ボリュームを設定するブリックを指定し、ボリュームを分散、複製、またはストライプ化するかを指定する必要があります。

ボリュームに追加する前に、ブリックディレクトリーまたはマウントポイントを作成する必要があります。



重要

異なるホストからエクスポートされたブリックをボリュームに統合する場合は、複製されたボリュームを使用することが推奨されます。複製されたボリュームは、ボリューム内の複数のブリック間でファイルのコピーを作成し、ホストがフェンスされたときにデータの損失を防ぎます。

手順9.4 ストレージボリュームの作成

1. **Volumes** resource タブをクリックして、結果一覧の既存のボリュームを一覧表示します。
2. **New** をクリックして、**New Volume** ウィンドウを開きます。
3. ドロップダウンメニューを使用して、データセンター および ボリュームクラスター を選択します。
4. ボリュームの **Name** を入力します。

5. ドロップダウンメニューを使用して、ボリュームの **タイプ** を選択します。
6. アクティブな場合は、適切な **トランSPORTタイプ** チェックボックスを選択します。
7. **Add Bricks** ボタンをクリックして、ボリュームに追加するブリックを選択します。ブリックは、Red Hat Gluster Storage ノードで外部に作成する必要があります。
8. アクティブな場合は、**Gluster**、**NFS**、および **CIFS** のチェックボックスを使用して、ボリュームに使用される適切なアクセスプロトコルを選択します。
9. **Allow Access From** フィールドに、IP アドレスまたはホスト名のコンマ区切りリストとしてボリュームアクセス制御を入力します。

* ワイルドカードを使用して IP アドレスまたはホスト名の範囲を指定できます。
10. **Optimize for Virt Store** オプションを選択して、仮想マシンストレージのボリュームを最適化するパラメーターを設定します。このボリュームをストレージドメインとして使用する場合は、これを選択します。
11. **OK** をクリックしてボリュームを作成します。新しいボリュームが追加され、**Volume** タブに表示されます。

Red Hat Gluster Storage ボリュームを追加している。これで、ストレージに使用できるようになりました。

9.2.5. ボリュームへのブリックの追加

概要

新しいブリックを追加することで、ボリュームを拡張できます。少なくとも1つのブリックを分散ボリュームに追加し、2つのブリックから複製されたボリュームに、ストレージ領域を拡張するときに4つのブリックの倍数をストライプ化ボリュームに追加する必要があります。

手順9.5 ボリュームへのブリックの追加

1. ナビゲーションペインの **Volumes** タブで、ブリックを追加するボリュームを選択します。
2. Details ペインから **Bricks** タブをクリックします。
3. **Add Bricks** をクリックし、**Add Bricks** ウィンドウを開きます。
4. **Server** ドロップダウンメニューを使用して、ブリックが存在するサーバーを選択します。
5. **Brick Directory** のパスを入力します。ディレクトリーがすでに存在している必要があります。
6. **Add** をクリックします。ブリックは、ボリュームのブリックの一覧に表示され、サーバーアドレスとブリックディレクトリ名が表示されます。
7. **OK** をクリックします。

結果

新しいブリックがボリュームに追加され、ブリックがボリュームの **Bricks** タブに表示されます。

9.2.6. ブリックウィンドウの追加設定の説明

表9.2 ブリックタブプロパティーの追加

フィールド名	説明
Volume Type	ボリュームの種別を表示します。このフィールドは変更できません。ボリュームの作成時に設定されていました。
Server	ブリックがホストされるサーバー。
ブリックディレクトリー	ブリックディレクトリーまたはマウントポイント。

9.2.7. 仮想マシンイメージの保存への Red Hat Gluster Storage ボリュームの最適化

管理ポータルを使用して仮想マシンイメージを保存するために Red Hat Gluster Storage ボリュームを最適化します。

仮想マシンを保存するためにボリュームを最適化するには、Manager はボリュームに仮想化固有のパラメーターを設定します。

ボリュームは、作成時に仮想マシンを保存するように最適化するには、**Virt Store の Optimize** チェックボックスを選択するか、または **Volumes** リソースタブから **Optimize for Virt Store** ボタンを使用して作成後に最適化できます。



重要

ボリュームが 3 つ以上のノード間で複製される場合は、ノード間でデータの不整合を回避するために、ボリュームが仮想ストレージに最適化されていることを確認します。

別の方法として、Red Hat Gluster Storage ノードの 1 つにアクセスし、ボリュームグループを **virt** に設定する方法があります。これにより、**cluster.quorum-type** パラメーターが **auto** に設定され、**cluster.server-quorum-type** パラメーターが **server** に設定されます。

```
# gluster volume set VOLUME_NAME group virt
```

ボリューム情報を一覧表示して、ボリュームのステータスを確認します。

```
# gluster volume info VOLUME_NAME
```

9.2.8. ボリュームの起動

概要

ボリュームの作成後、または既存のボリュームを停止したら、使用する前にボリュームを起動する必要があります。

手順9.6 ボリュームの起動

- ボリューム タブで、起動するボリュームを選択します。

Shift キーまたは **Ctrl** キーを使用して、起動する複数のボリュームを選択できます。

- Start** ボタンをクリックします。

ボリュームのステータスが **Up** に変わります。

結果

仮想マシンのストレージにボリュームを使用できるようになりました。

9.2.9. ボリュームのチューニング

概要

ボリュームをチューニングすると、パフォーマンスに影響を与えることができます。ボリュームを調整するには、それらにオプションを追加します。

手順9.7 ボリュームのチューニング

1. **Volumes** タブをクリックします。

ボリュームの一覧が表示されます。

2. 調整するボリュームを選択し、Details ペインから **Volume Options** タブをクリックします。

ボリュームオプション タブには、ボリュームに設定されたオプションの一覧が表示されます。

3. **Add** をクリックしてオプションを設定します。**Add Option** ダイアログボックスが表示されます。ドロップダウンリストから Option Key を選択し、オプションの値を入力します。

4. **OK** をクリックします。

オプションは設定され、**Volume Options** タブに表示されます。

結果

ストレージボリュームのオプションを調整している。

9.2.10. ボリュームオプションの編集

概要

ボリュームにオプションを追加して、ボリュームを調整している。ストレージボリュームのオプションを変更できます。

手順9.8 ボリュームオプションの編集

1. **Volumes** タブをクリックします。

ボリュームの一覧が表示されます。

2. 編集するボリュームを選択し、Details ペインから **Volume Options** タブをクリックします。

ボリュームオプション タブには、ボリュームに設定されたオプションの一覧が表示されます。

3. 編集するオプションを選択します。**Edit** をクリックします。**Edit Option** ダイアログボックスが表示されます。オプションに新しい値を入力します。

4. **OK** をクリックします。

編集されたオプションが **Volume Options** タブに表示されます。

結果

ボリュームのオプションを変更している。

9.2.11. ボリュームのリセットオプション

概要

オプションをリセットして、デフォルト値に戻すことができます。

1. **Volumes** タブをクリックします。
ボリュームの一覧が表示されます。
2. ボリュームを選択し、Details ペインから **Volume Options** タブをクリックします。
ボリュームオプション タブには、ボリュームに設定されたオプションの一覧が表示されます。
3. リセットするオプションを選択します。 **Reset** をクリックします。ダイアログボックスが表示され、リセットオプションの確認が求められます。
4. **OK** をクリックします。
選択したオプションがリセットされます。



注記

Reset All ボタンをクリックすると、すべてのボリュームオプションをリセットできます。ダイアログボックスが表示され、リセットオプションの確認が求められます。 **OK** をクリックします。すべてのボリュームオプションは、選択したボリュームに対してリセットされます。

結果

ボリュームオプションを default にリセットしている。

9.2.12. ボリュームからのブリックの削除

概要

クラスターがオンラインになり、利用可能である間は、必要に応じてボリュームを縮小できます。たとえば、ハードウェアやネットワークの障害により、分散ボリュームでアクセスできなくなるブリックを削除する必要がある場合があります。

手順9.9 ボリュームからのブリックの削除

1. ナビゲーションペインの **Volumes** タブで、ブリックを削除するボリュームを選択します。
2. Details ペインから **Bricks** タブをクリックします。
3. 削除するブリックを選択します。 **Remove Bricks** をクリックします。
4. ウィンドウが開き、削除の確認が求められます。 **OK** をクリックして確定します。

結果

ブリックはボリュームから削除されます。

9.2.13. Red Hat Gluster Storage ボリュームの停止

ボリュームが起動したら、これを停止できます。

手順9.10 ボリュームの停止

1. **Volumes** タブで、停止するボリュームを選択します。

Shift キーまたは **Ctrl** キーを使用して、停止する複数のボリュームを選択できます。

2. **Stop** をクリックします。

9.2.14. Red Hat Gluster Storage ボリュームの削除

クラスターからボリュームまたは複数のボリュームを削除できます。

1. ボリューム タブで、削除するボリュームを選択します。
2. **削除** をクリックします。ダイアログボックスが表示され、削除の確認が求められます。**OK** をクリックします。

9.2.15. ボリュームのリバランス

概要

ボリュームへのブリックを追加または削除してボリュームを拡張するか、または縮小された場合は、ボリューム上のデータをサーバー間でリバランスする必要があります。

手順9.11 ボリュームのリバランス

1. **Volumes** タブをクリックします。
- ボリュームの一覧が表示されます。
2. リバランスするボリュームを選択します。
3. **Rebalance** をクリックします。

結果

選択したボリュームがリバランスされます。

9.3. クラスターおよび GLUSTER フック

9.3.1. Gluster フックの管理

Gluster フックはボリュームのライフサイクル拡張機能です。Manager から Gluster フックを管理できます。フックコンテンツタイプが **Text** の場合は、フックの内容を表示できます。

Manager を使用して以下を実行できます。

- ホストで利用可能なフックの一覧を表示します。
- フックのコンテンツおよびステータスを表示します。

- フックを有効または無効にします。
- フックの競合を解決します。

9.3.2. フックの一覧表示

概要

環境内の Gluster フックを一覧表示します。

手順9.12 フックの一覧表示

1. **Cluster resource** タブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. **Gluster Hooks** サブタブを選択し、詳細ペインにフックを一覧表示します。

結果

環境に Gluster フックを一覧表示している。

9.3.3. フックの内容の表示

概要

環境内の Gluster フックの内容を表示します。

手順9.13 フックの内容の表示

1. **Cluster resource** タブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. **Gluster Hooks** サブタブを選択し、詳細ペインにフックを一覧表示します。
3. コンテンツタイプ **Text** のフックを選択し、**View Content** ボタンをクリックして **Hook Content** ウィンドウを開きます。

結果

お使いの環境でフックの内容を確認している。

9.3.4. フックの有効化または無効化

概要

Gluster フックを有効または無効にすることにより、Gluster フックのアクティビティーを切り替えます。

手順9.14 フックの有効化または無効化

1. **Cluster resource** タブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. **Gluster Hooks** サブタブを選択し、詳細ペインにフックを一覧表示します。

3. フックを選択し、**Enable** または **Disable** ボタンのいずれかをクリックします。フックはクラスターのすべてのノードで有効または無効になります。

結果

環境内の Gluster フックのアクティビティーを切り替えている。

9.3.5. フックの更新

概要

デフォルトでは、Manager はエンジンおよびクラスター内のすべてのサーバーでインストールされたフックのステータスを確認し、定期的なジョブを1時間ごとに実行して新規フックを検出します。同期ボタンをクリックすると、フックを手動で更新できます。

手順9.15 フックの更新

1. **Cluster resource** タブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. **Gluster Hooks** サブタブを選択し、詳細ペインにフックを一覧表示します。
3. **同期** ボタンをクリックします。

結果

フックは、詳細ペインで同期され、更新されます。

9.3.6. 競合の解決

フックは **Cluster** タブの **Gluster Hooks** サブタブに表示されます。競合の原因となったフックは感嘆符で表示されます。これは、コンテンツに競合があるか、またはクラスター内のサーバー全体でフックのステータスがないか、1つ以上のサーバーにフックスクリプトが欠落していることを示します。これらの競合は、Manager を介して解決できます。サーバーのフックはエンジンデータベースと定期的に同期され、フックに対して以下の競合が発生する可能性があります。

- コンテンツの競合：フックの内容はサーバー間で異なります。
- Conflict がありません：クラスターの1つ以上のサーバーにフックがありません。
- Status Conflict - フックのステータスはサーバー間で異なります。
- 複数の競合：フックには前述の競合の2つ以上の組み合わせがあります。

9.3.7. コンテンツの競合の解決

概要

サーバーおよびエンジン全体で一貫性のないフックには、競合があるものとしてフラグが付けられます。競合を解決するには、すべてのサーバーとエンジン間でコピーするフックのバージョンを選択する必要があります。

手順9.16 コンテンツの競合の解決

1. **Cluster resource** タブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。

2. **Gluster Hooks** サブタブを選択し、詳細ペインにフックを一覧表示します。
3. 競合するフックを選択し、**Resolve Conflicts** ボタンをクリックして **Resolve Conflicts** ウィンドウを開きます。
4. ソースの一覧からエンジンまたはサーバーを選択し、そのフックの内容を表示し、コピーするフックのバージョンを確立します。



注記

フックの内容は、すべてのサーバーおよびエンジンで上書きされます。

5. **Use content from** ドロップダウンメニューを使用して、優先サーバーまたはエンジンを選択します。
6. **OK** をクリックして競合を解決し、ウィンドウを閉じます。

結果

選択したサーバーのフックはすべてのサーバーにコピーされ、エンジンは環境全体で一貫性を保つようにします。

9.3.8. 欠落しているフックの競合の解決

概要

すべてのサーバーに存在しないフックとエンジンには競合のフラグが付けられます。競合を解決するには、すべてのサーバーとエンジンにコピーするフックのバージョンを選択するか、不足しているフックを完全に削除します。

手順9.17 欠落しているフックの競合の解決

1. **Cluster resource** タブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. **Gluster Hooks** サブタブを選択し、詳細ペインにフックを一覧表示します。
3. 競合するフックを選択し、**Resolve Conflicts** ボタンをクリックして **Resolve Conflicts** ウィンドウを開きます。
4. ステータスが **Enabled** のソースを選択し、フックの内容を表示します。
5. フックをすべてサーバーにコピーするか、欠落しているフックを削除します。後者は、エンジンとすべてのサーバーからフックを削除します。
6. **OK** をクリックして競合を解決し、ウィンドウを閉じます。

結果

選択した解決策に応じて、フックは完全に環境から削除されるか、またはすべてのサーバーでコピーされ、エンジンが環境全体で一貫性を保つようにします。

9.3.9. ステータスの競合の解決

概要

サーバー全体で一貫したステータスを持たないフックとエンジンには、競合のあるフラグが付けられます。競合を解決するには、環境内のすべてのサーバーで実施するステータスを選択します。

手順9.18 ステータスの競合の解決

1. **Cluster resource** タブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. **Gluster Hooks** サブタブを選択し、詳細ペインにフックを一覧表示します。
3. 競合するフックを選択し、**Resolve Conflicts** ボタンをクリックして **Resolve Conflicts** ウィンドウを開きます。
4. **Hook Status** を **有効** または **無効** にするに設定します。
5. **OK** をクリックして競合を解決し、ウィンドウを閉じます。

結果

フックに選択されたステータスはエンジン全体で適用され、サーバーは環境全体で一貫性を保つことができます。

9.3.10. 複数の競合の解決

概要

フックは2つ以上の競合の組み合わせを持つことができます。これらはすべて、**Resolve Conflicts** ウィンドウで同時または個別に解決できます。この手順では、フックのすべての競合を解決し、エンジンと環境内のすべてのサーバー全体で一貫性を保つようにします。

手順9.19 複数の競合の解決

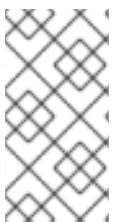
1. **Cluster resource** タブ、ツリーモード、または検索機能を使用して、結果一覧でクラスターを見つけて選択します。
2. **Gluster Hooks** サブタブを選択し、詳細ペインにフックを一覧表示します。
3. 競合するフックを選択し、**Resolve Conflicts** ボタンをクリックして **Resolve Conflicts** ウィンドウを開きます。
4. 適切な手順に従って、影響を受ける競合ごとに解決を選択します。
5. **OK** をクリックして競合を解決し、ウィンドウを閉じます。

結果

すべての競合を解決し、フックがエンジンとすべてのサーバー全体で一貫性を保つようにしました。

9.3.11. Gluster 同期の管理

Gluster Sync 機能は定期的に GlusterFS から最新のクラスター設定を取得し、engine DB と同じように同期します。このプロセスは、Manager から実行できます。クラスターを選択すると、ユーザーには、選択したクラスターからホストをインポートするか、または既存のホストをデタッチするオプションが提供されます。クラスターにホストがある場合は、Gluster Sync を実行できます。



注記

Manager は、ホストがストレージクラスターに追加されたか、またはストレージクラスターから削除されているかを継続的に監視します。ホストの追加または削除が検出されると、クラスターの **General** タブにアクション項目が表示されます。ここで、ホストをクラスターにインポートするまたはデタッチを選択できます。

第10章 POOLS

10.1. 仮想マシンプールの概要

仮想マシンプールは、すべて同じテンプレートのクローンであり、特定のグループ内の任意のユーザーがオンデマンドで使用できる仮想マシンのグループです。仮想マシンプールを使用すると、管理者はユーザー向けに一連の一般化された仮想マシンを迅速に設定できます。

ユーザーは、プールから仮想マシンを取得することにより、仮想マシンプールにアクセスします。ユーザーがプールから仮想マシンを取得すると、プール内の仮想マシン（使用可能な場合）のいずれかが提供されます。その仮想マシンは、プールのベースとなったテンプレートと同じオペレーティングシステムと設定を持ちますが、ユーザーが仮想マシンを使用するたびにプールの同じメンバーを受け取るとは限りません。ユーザーは、プールの設定に応じて、同じ仮想マシンプールから複数の仮想マシンを取得することもできます。

仮想マシンプールはデフォルトでステートレスです。つまり、仮想マシンのデータは再起動後も持続しません。ただし、プールはステートフルになるように設定できるため、前のユーザーが行った変更を保持できます。ただし、ユーザーが仮想マシンプールから取得した仮想マシンのコンソールオプションを設定する場合、それらのオプションは、その仮想マシンプールのそのユーザーのデフォルトとして設定されます。



注記

プールから取得した仮想マシンは、管理ポータルからアクセスしたときにステートレスではありません。これは、管理者が必要に応じてディスクに変更を書き込める必要があります。

原則として、プール内の仮想マシンは、ユーザーが取得したときに起動され、ユーザーが終了したときにシャットダウンされます。ただし、仮想マシンプールには、事前に起動した仮想マシンを含めることができます。事前に起動した仮想マシンは稼働状態に保たれ、ユーザーが使用するまでアイドル状態のままになります。これにより、ユーザーはそのような仮想マシンの使用をすぐに開始できますが、これらの仮想マシンは、アイドル状態のために使用されていないときでもシステムリソースを消費します。

10.2. 仮想マシンプールタスク

10.2.1. 仮想マシンプールの作成

一般的なテンプレートに基づいて作成された複数の仮想マシンを含む仮想マシンプールを作成できます。

手順10.1 仮想マシンプールの作成

1. **Pools** タブをクリックします。
2. **New** ボタンをクリックして **New Pool** ウィンドウを開きます。
3. ドロップダウンリストを使用して **Cluster** を選択するか、選択したデフォルトを使用します。
4. テンプレート ドロップダウンメニューを使用して必要なテンプレートおよびバージョンを選択するか、選択したデフォルトを使用します。テンプレートは、プール内のすべての仮想マシンの標準設定を提供します。

5. オペレーティングシステム ドロップダウンリストを使用してオペレーティングシステムを選択するか、テンプレートで提供されるデフォルトを使用します。
6. **Optimized for** ドロップダウンリストを使用して、デスクトップの使用またはサーバーの使用のために仮想マシンを最適化します。
7. **Name** および **Description**、任意の **Comments**、およびプールの **Number of VMs** を入力します。
8. **Prestarted VMs** フィールドに、事前起動する仮想マシンの数を入力します。
9. 1人 のユーザーがセッションで実行できる 1 ユーザーあたりの仮想マシンの最大数 を選択します。最小値は 1 です。
10. **Delete Protection** チェックボックスを選択して、削除保護を有効にします。
11. 必要に応じて、**Show Advanced Options** ボタンをクリックし、以下の手順を実行します。
 - a. **Type** タブをクリックします。
 - i. プール タイプを選択します。
 - **manual**: 管理者は、仮想マシンをプールに明示的に返す責任があります。
 - **Automatic** - 仮想マシンは自動的に仮想マシンプールに戻ります。
 - b. **Console** タブをクリックします。
 - i. **Override SPICE Proxy** チェックボックスを選択します。
 - ii. **Overridden SPICE proxy address** テキストフィールドで、グローバル SPICE プロキシーをオーバーライドする SPICE プロキシーのアドレスを指定します。
12. **OK** をクリックします。

指定した数の同一の仮想マシンを使用して仮想マシンプールを作成および設定しました。これらの仮想マシンは、**Virtual Machines** リソースタブまたは **Pools** リソースタブの詳細ペインで表示できます。プール内の仮想マシンは、アイコンによって独立した仮想マシンと区別されます。

10.2.2. 新しいプールとプールの編集ウィンドウの設定およびコントロールの説明

10.2.2.1. 新しいプールと編集プールの一般設定の説明

以下の表は、仮想マシンプールに固有の **New Pool** ウィンドウおよび **Edit Pool** ウィンドウの **General** タブに必要な情報の詳細を示しています。その他のすべての設定は、**New Virtual Machine** ウィンドウの設定と同じです。

表10.1 一般的な 設定

フィールド名	説明
Template	仮想マシンプールのベースとなるテンプレートおよびテンプレートサブバージョン。テンプレートの最新のサブバージョンに基づいてプールを作成する場合、プール内のすべての仮想マシンを再起動すると、再起動時に最新のテンプレートバージョンが自動的に受信されます。仮想マシンのテンプレートの設定に関する詳細は、『Virtual Machine Management Guide』の Virtual Machine General Settings Explained および Explanation of Settings in the New Template and Edit Template Windows を参照してください。
説明	仮想マシンプールの意味のある説明。
Comment	仮想マシンプールに関するプレーンテキストの人間が判読できるコメントを追加するフィールド。
Prestarted VMs	仮想マシンプール内の仮想マシンが取得される前に開始され、ユーザーが取得する状態に維持される仮想マシンの数を指定できます。このフィールドの値は、0 から仮想マシンプール内の仮想マシンの総数の間でなければなりません。
VM の数/プール内の VM の数を次のように増やす	作成して仮想マシンプールで使用できるようにする仮想マシンの数を指定できます。編集ウィンドウでは、仮想マシンプール内の仮想マシンの数を指定された数だけ増やすことができます。デフォルトでは、プールに作成できる仮想マシンの最大数は 1000 です。この値は、 engine-config コマンドの MaxVmsInPool キーを使用して設定できます。
ユーザーあたりの VM の最大数	1人のユーザーが一度に仮想マシンプールから取得できる仮想マシンの最大数を指定できます。このフィールドの値は、1 から 32,767 の間でなければなりません。
Delete Protection	プール内の仮想マシンが削除されないようにすることができます。

10.2.2.2. 新規およびプールタイプ設定の編集の説明

以下の表は、New Pool ウィンドウおよび Edit Pool ウィンドウの Type タブで必要な情報の詳細を示しています。

表10.2 タイプ設定

フィールド名	説明
--------	----

フィールド名	説明
Pool Type	<p>このドロップダウンメニューでは、仮想マシンプールのタイプを指定できます。以下のオプションを設定できます。</p> <ul style="list-style-type: none"> 自動: ユーザーが仮想マシンプールから取得した仮想マシンの使用を終了すると、その仮想マシンは自動的に仮想マシンプールに戻されます。 手動: ユーザーが仮想マシンプールから取得した仮想マシンの使用を終了すると、管理者が仮想マシンを手動で返す場合にのみ、その仮想マシンは仮想マシンプールに戻されます。
Stateful Pool	仮想マシンが別のユーザーに渡されたときに、プール内の仮想マシンの状態を保持するかどうかを指定します。これは、前のユーザーが行った変更が仮想マシンに保持されることを意味します。

10.2.2.3. 新しいプールおよびプールコンソール設定の編集の説明

以下の表は、仮想マシンプールに固有の **New Pool** ウィンドウまたは **Edit Pool** ウィンドウの **Console** タブに必要な情報の詳細を示しています。その他のすべての設定は、**New Virtual Machine** および **Edit Virtual Machine** ウィンドウの設定と同じです。

表10.3 コンソールの設定

フィールド名	説明
Override SPICE proxy	このチェックボックスを選択し、グローバル設定で定義された SPICE プロキシーの上書きを有効にします。この機能は、ユーザー（ユーザーインターフェース経由で接続するなど）がホストが存在するネットワーク外にある場合に役に立ちます。
SPICE プロキシーアドレスのオーバーライド	SPICE クライアントが仮想マシンに接続するプロキシー。このプロキシーは、Red Hat Virtualization 環境用に定義されたグローバル SPICE プロキシーと、仮想マシンプールが属するクラスター用に定義された SPICE プロキシー（存在する場合）の両方をオーバーライドします。アドレスは以下の形式でなければなりません。

`protocol://[host]:[port]`

10.2.2.4. 仮想マシンプールのホスト設定の説明

以下の表は、**New Pool** ウィンドウおよび **Edit Pool** ウィンドウの **Host** タブで利用可能なオプションの詳細を示しています。

表10.4 仮想マシンプール: ホスト設定

フィールド名	サブ要素	説明
Start Running On		<p>仮想マシンを実行する優先ホストを定義します。以下のいずれかを選択します。</p> <ul style="list-style-type: none"> ● Any Host in Cluster - 仮想マシンはクラスター内の利用可能な任意のホストで起動し、実行できます。 ● Specific - 仮想マシンはクラスター内の特定のホストで実行を開始します。ただし、Manager または管理者は、仮想マシンの移行および高可用性設定に応じて、仮想マシンをクラスター内の別のホストに移行することができます。利用可能なホスト一覧から、特定のホストまたはホストのグループを選択します。
Migration Options	Migration mode	<p>仮想マシンの実行および移行オプションを定義します。このオプションを使用しない場合、仮想マシンはそのクラスターのポリシーに従って実行または移行されます。</p> <ul style="list-style-type: none"> ● Allow manual and automatic migration: 環境のステータスに応じて、または管理者が手動で、仮想マシンのあるホストから別のホストに移行することができます。 ● Allow manual migration only: 仮想マシンは、管理者によって手動でしか移行できません。 ● Do not allow migration: 仮想マシンを自動または手動で移行することはできません。

フィールド名	サブ要素	説明
	Use custom migration policy	<p>移行コンバージェンスポリシーを定義します。チェックボックスをオフのままにすると、ホストがポリシーを決定します。</p> <ul style="list-style-type: none"> ● legacy - 3.6 バージョンのレガシーアクション。vds.conf のオーバーライドは引き続き適用されます。ゲストエージェントフックメカニズムが無効になっている。 ● 最小ダウンタイム: 一般的な状況で仮想マシンを移行できるようにします。仮想マシンは、ダウンタイムを大幅に発生しません。移行は、長時間(QEMU の反復により最大 500 ミリ秒)後に仮想マシンの移行が収束されない場合に中止されます。ゲストエージェントフックメカニズムが有効になっている。 ● Suspend workload if needed: 仮想マシンが負荷の高いワークロードを実行している場合など、ほとんどの状況で仮想マシンを移行できるようにします。仮想マシンでは、より大きなダウンタイムが発生する可能性があります。移行は、極端なワークロードに対して中止される場合があります。ゲストエージェントフックメカニズムが有効になっている。
	Use custom migration downtime	<p>このチェックボックスを選択すると、ライブマイグレーション中に仮想マシンがダウンできる最大時間をミリ秒単位で指定できます。ワークロードおよび SLA の要件に従って、各仮想マシンに異なる最大ダウンタイムを設定します。VDSM のデフォルト値を使用するには 0 を入力します。</p>

フィールド名	サブ要素	説明
	自動コンバージション	<p>Legacy 移行ポリシーでのみアクリベートされます。仮想マシンのライブマイグレーション中に自動コンバージェンスが使用されるかどうかを設定できます。負荷が大きいが大きい仮想マシンでは、ライブマイグレーション中に行われる転送速度よりも速くメモリーがダーティーなり、移行が収束できなくなります。QEMU の自動調整機能を使用すると、仮想マシン移行の収束を強制的に実行できます。QEMU は、コンバージェンスの欠如を自動的に検出し、仮想マシン上の vCPU のスロットルダウンをトリガーします。オートコンバージェンスはデフォルトで無効になっています。</p> <ul style="list-style-type: none"> ● クラスターレベルで設定される自動収束設定を使用するには、Inherit from cluster setting を選択します。このオプションはデフォルトで選択されます。 ● Auto Converge を選択してクラスター設定またはグローバル設定を上書きし、仮想マシンの自動調整を許可します。 ● Don't Auto Converge を選択してクラスター設定またはグローバル設定を上書きし、仮想マシンの自動収束を防ぎます。

フィールド名	サブ要素	説明
	Enable migration compression	<p>Legacy 移行ポリシーでのみアクトイベートされます。このオプションを使用すると、仮想マシンのライブマイグレーション中に移行圧縮を使用するかどうかを設定できます。この機能は、Xor Binary Zero Run-Length-Encoding を使用して、メモリー書き込みを必要とするワークロードまたはスペースメモリー更新パターンを使用するアプリケーションに対して、仮想マシンのダウンタイムと合計移行時間を短縮します。移行圧縮は、デフォルトでは無効になっています。</p> <ul style="list-style-type: none"> ● クラスターレベルで設定される圧縮設定を使用するには、Inherit from cluster setting を選択します。このオプションはデフォルトで選択されます。 ● Compress を選択してクラスター設定またはグローバル設定を上書きし、仮想マシンの圧縮を許可します。 ● Don't compress を選択してクラスター設定またはグローバル設定を上書きし、仮想マシンの圧縮を防ぎます。
	Pass-Through Host CPU	このチェックボックスを選択すると、仮想マシンは配置されているホストの物理 CPU の機能を利用できます。このオプションは、 Do not allow migration が選択されている場合にのみ有効にできます。
Configure NUMA	NUMA Node Count	仮想マシンに割り当てる仮想 NUMA ノードの数。 Tune Mode が Preferred の場合、この値を 1 に設定する必要があります。

フィールド名	サブ要素	説明
	Tune Mode	<p>メモリーを割り当てるために使用されるメソッド。</p> <ul style="list-style-type: none"> ● strict: ターゲットノードにメモリーを割り当てることができない場合は、メモリー割り当てに失敗します。 ● 推奨: メモリーは、1つの優先ノードから割り当てられます。十分なメモリーが利用できない場合は、他のノードからメモリーを割り当てることができます。 ● Interleave: メモリーはラウンドロビンアルゴリズムでノード全体に割り当てられます。
	NUMA Pinning	<p>NUMA Topology ウィンドウを開きます。このウィンドウには、ホストの合計 CPU、メモリー、NUMA ノード、および仮想マシンの仮想 NUMA ノードが表示されます。右側のボックスから左側の NUMA ノードに各 vNUMA をクリックアンドドラッグすることで、仮想 NUMA ノードをホストの NUMA ノードに固定します。</p>

10.2.3. 仮想マシンプールの編集

10.2.3.1. 仮想マシンプールの編集

仮想マシンプールが作成された後、そのプロパティーを編集できます。仮想マシンプールの編集時に使用できるプロパティーは、新しい仮想マシンプールの作成時に利用可能なプロパティーと同じですが、**Number of VMs** プロパティーが **Increase number of VMs in pool by** に置き換えられる点が異なります。



注記

仮想マシンプールを編集する場合、導入された変更は新しい仮想マシンにのみ影響します。導入された変更の時点ですでに存在していた仮想マシンは影響を受けません。

手順10.2 仮想マシンプールの編集

1. **Pools** resource タブをクリックし、結果リストから仮想マシンプールを選択します。
2. **Edit** をクリックして **Edit Pool** ウィンドウを開きます。
3. 仮想マシンプールのプロパティーを編集します。

4. **OK** をクリックします。

10.2.3.2. プール内の仮想マシンの事前起動

仮想マシンプール内の仮想マシンは、デフォルトでパワーダウンされています。ユーザーがプールから仮想マシンを要求すると、マシンの電源がオンになり、ユーザーに割り当てられます。対照的に、事前に起動した仮想マシンはすでに実行しており、ユーザーへの割り当てを待機しているため、ユーザーがマシンにアクセスできるようになるまで待機する時間が短縮されます。事前に起動した仮想マシンがシャットダウンすると、プールに戻され、元の状態に復元されます。事前に起動した仮想マシンの最大数は、プール内の仮想マシンの数です。

事前に起動した仮想マシンは、ユーザーが特に割り当てられていない仮想マシンにすぐにアクセスする必要がある環境に適しています。自動プールのみが仮想マシンを事前に起動できます。

手順10.3 プール内の仮想マシンの事前起動

1. **Pools** resource タブ、ツリーモード、または検索機能を使用して、結果一覧で仮想マシンプールを見つけて選択します。
2. **Edit** をクリックして **Edit Pool** ウィンドウを開きます。
3. **Prestarted VMs** フィールドに、事前起動する仮想マシンの数を入力します。
4. **Pool** タブを選択します。**Pool Type** が **Automatic** に設定されていることを確認します。
5. **OK** をクリックします。

プールに事前に起動した仮想マシンが多数設定している。事前に起動したマシンが実行されており、使用可能です。

10.2.3.3. 仮想マシンプールへの仮想マシンの追加

仮想マシンプールで最初にプロビジョニングされた数よりも多くの仮想マシンが必要な場合は、プールにマシンを追加します。

手順10.4 仮想マシンプールへの仮想マシンの追加

1. **Pools** resource タブ、ツリーモード、または検索機能を使用して、結果一覧で仮想マシンプールを見つけて選択します。
2. **Edit** をクリックして **Edit Pool** ウィンドウを開きます。
3. **Increase number of VMs in pool by** フィールドに、追加する仮想マシンの数を入力します。
4. **OK** をクリックします。

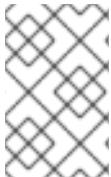
仮想マシンプールに仮想マシンを追加している。

10.2.3.4. 仮想マシンプールからの仮想マシンのデタッチ

仮想マシンを仮想マシンプールからデタッチできます。仮想マシンを切り離すと、その仮想マシンがプールから削除され、独立した仮想マシンになります。

手順10.5 仮想マシンプールからの仮想マシンのデタッチ

1. **Pools** resource タブ、ツリーモード、または検索機能を使用して、結果一覧で仮想マシンプールを見つけて選択します。
2. 実行中の仮想マシンの割り当てを解除できないため、仮想マシンのステータスが **Down** であることを確認します。
3. 詳細ペインの **仮想マシン** タブをクリックして、プール内の仮想マシンを一覧表示します。
4. 1つまたは複数の仮想マシンを選択し、**Detach** をクリックして、**Detach Virtual Machine (s)** 確認ウィンドウを開きます。
5. **OK** をクリックして、プールから仮想マシンの割り当てを解除します。



注記

仮想マシンは環境に存在し、**Virtual Machines** リソースタブから表示およびアクセスできます。アイコンが変化して、デタッチされた仮想マシンが独立した仮想マシンであることを示すことに注意してください。

仮想マシンプールから仮想マシンをデタッチしている。

10.2.4. 仮想マシンプールの削除

データセンターから仮想マシンプールを削除できます。最初に、プール内のすべての仮想マシンを削除またはデタッチする必要があります。プールから仮想マシンを切り離すと、それらは独立した仮想マシンとして保持されます。

手順10.6 仮想マシンプールの削除

1. **Pools** resource タブ、ツリーモード、または検索機能を使用して、結果一覧で仮想マシンプールを見つけて選択します。
2. **Remove** をクリックして、**Remove Pool (s)** 確認ウィンドウを開きます。
3. **OK** をクリックしてプールを削除します。

データセンターからプールを削除しました。

10.3. プールおよびパーミッション

10.3.1. 仮想マシンプールのシステムパーミッションの管理

システム管理者は **SuperUser** として、管理ポータルのすべての側面を管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限された管理者ロールは、特定のリソースに制限される管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、そのデータセンターのストレージを除く、割り当てられたデータセンターの管理者権限のみを持ち、**ClusterAdmin** は割り当てられたクラスターに対してのみ管理者権限を持ちます。

仮想マシンプールの管理者は、データセンター内の仮想マシンプールのシステム管理ロールです。このロールは、特定の仮想マシンプール、データセンター、または仮想化環境全体に適用できます。これは、異なるユーザーが特定の仮想マシンプールリソースを管理できるようにするのに役立ちます。

仮想マシンプールの管理者ロールは、以下のアクションを許可します。

- プールの作成、編集、および削除。

- プールからの仮想マシンを追加およびデタッチ。



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てることができます。

10.3.2. 仮想マシンプール管理者ロールの概要

プールパーティションロール

以下の表は、プール管理に適用される管理者ロールおよび権限について説明しています。

表10.5 Red Hat Virtualization システム管理者ロール

ロール	権限	注記
VmPoolAdmin	仮想プールのシステム管理者ロール。	仮想プールを作成、削除、および設定できます。仮想プールユーザーを割り当ておよび削除し、仮想マシンに基本操作を実行できます。
ClusterAdmin	クラスター管理者	特定のクラスター内のすべての仮想マシンプールを使用、作成、削除、および管理できます。

10.3.3. 管理者またはユーザーロールのリソースへの割り当て

管理者またはユーザーロールをリソースに割り当て、ユーザーがそのリソースにアクセスしたり、管理したりできるようにします。

手順10.7 リソースへのロールの割り当て

1. リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
2. 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
3. **Add** をクリックします。
4. **Search** テキストボックスに既存ユーザーの名前またはユーザー名を入力し、**Go** をクリックします。表示された候補の中からユーザーを選択します。
5. **Role to Assign:** ドロップダウンリストからロールを選択します。
6. **OK** をクリックします。

ユーザーにロールを割り当てました。そのリソースで有効にしたそのロールの継承されたパーミッションが、ユーザーに付与されました。

10.3.4. リソースからの管理者またはユーザーロールの削除

管理者またはユーザーのロールをリソースから削除すると、ユーザーはそのリソースのロールに関連付けられ継承されたパーミッションを失います。

手順10.8 リソースからのロールの削除

1. リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
2. 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
3. リソースから削除するユーザーを選択します。
4. **Remove** をクリックします。 **Remove Permission** 画面が開き、パーミッションの削除を確認します。
5. **OK** をクリックします。

ユーザーのロールおよび関連付けられたパーミッションをリソースから削除しました。

10.4. 信頼できるコンピュートプール

信頼できるコンピュートプールは、Intel Trusted Execution Technology (Intel TXT) に基づくセキュアなクラスターです。信頼できるクラスターは、Intel の OpenAttestation によって検証されるホストのみを許可します。これは、ホワイトリストデータベースに対してホストのハードウェアおよびソフトウェアの整合性を測定します。信頼できるホストおよびそれらで実行されている仮想マシンには、高いレベルでセキュリティーを確保する必要があるタスクを割り当てることができます。Intel TXT、信頼できるシステム、およびテストの詳細は、を参照してください <https://software.intel.com/en-us/articles/intel-trusted-execution-technology-intel-txt-enabling-guide>。

信頼できるコンピュートプールを作成するには、以下の手順を行います。

- Manager が OpenAttestation サーバーと通信するように設定する。
- 信頼できるクラスターを作成して、信頼できるホストだけを実行できるようにする。
- 信頼できるホストを信頼できるクラスターに追加する。OpenAttestation サーバーによって信頼されていることを確認するには、ホストが OpenAttestation エージェントを実行している必要があります。

OpenAttestation サーバーのインストール、ホストに OpenAttestation エージェントをインストールし、ホワイトリストデータベースを作成する方法は、を参照してください <https://github.com/OpenAttestation/OpenAttestation/wiki>。

10.4.1. OpenAttestation サーバーの Manager への接続

信頼されたクラスターを作成する前に、Red Hat Virtualization Manager が OpenAttestation サーバーを認識するように設定する必要があります。 **engine-config** を使用して、OpenAttestation サーバーの FQDN または IP アドレスを追加します。

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

必要に応じて、以下の設定を変更することもできます。

表10.6 engine-config の OpenAttestation 設定

オプション	デフォルト値	説明
AttestationServer	oat-server	OpenAttestation サーバーの FQDN または IP アドレス。これは、Manager が OpenAttestation サーバーと通信するように設定する必要があります。
AttestationPort	8443	Manager との通信に OpenAttestation サーバーが使用するポート。
AttestationTruststore	TrustStore.jks	OpenAttestation サーバーとの通信のセキュリティーを保護するために使用されるトラストストア。
AttestationTruststorePass	password	トラストストアのアクセスに使用されるパスワード。
AttestationFirstStageSize	10	クイック初期化に使用されます。この値は、適切な理由なしで変更することは推奨されません。
SecureConnectionWithOATServers	true	OpenAttestation サーバーとのセキュアな通信を有効または無効にします。
PollUri	AttestationService/resources/PolIHosts	OpenAttestation サービスへのアクセスに使用される URI。

10.4.2. 信頼できるクラスターの作成

信頼できるクラスターは OpenAttestation サーバーと通信して、ホストのセキュリティーを評価します。ホストが信頼できるクラスターに追加されると、OpenAttestation サーバーはホワイトリストデータベースに対してホストのハードウェアおよびソフトウェアを測定します。仮想マシンは、信頼されるクラスターの信頼済みホスト間で移行できるので、セキュアな環境での高可用性を可能にします。

手順10.9 信頼できるクラスターの作成

1. **Clusters** タブを選択します。
2. **New** をクリックします。
3. クラスターの **Name** を入力します。
4. **Enable Virt Service** ラジオボタンを選択します。
5. **Scheduling Policy** タブで、**Enable Trusted Service** チェックボックスを選択します。
6. **OK** をクリックします。

10.4.3. 信頼できるホストの追加

Red Hat Enterprise Linux ホストは、信頼できるクラスターに追加し、OpenAttestation サーバーがホワイトリストデータベースに対して、このホストを測定できます。OpenAttestation サーバーで信頼されるようにするには、ホストが以下の要件を満たす必要があります。

- BIOS で Intel TXT が有効になっている。
- OpenAttestation エージェントがインストールされ、実行されている。
- ホストで実行されているソフトウェアは、OpenAttestation サーバーのホワイトリストデータベースと一致します。

手順10.10 信頼できるホストの追加

1. **Hosts** タブを選択します。
2. **New** をクリックします。
3. **Host Cluster** ドロップダウンリストから信頼できるクラスターを選択します。
4. ホストの **名前** を入力します。
5. ホストの **Address** を入力します。
6. ホストの **root パスワード** を入力します。
7. **OK** をクリックします。

ホストが信頼できるクラスターに追加されると、OpenAttestation サーバーにより評価されます。ホストが OpenAttestation サーバーで信頼されていない場合には、**Non Operational** の状態に移行するため、信頼できるクラスターから削除する必要があります。

第11章 仮想ディスク

11.1. 仮想マシンストレージを理解する

Red Hat Virtualization は、NFS、iSCSI、FCP の 3 つのストレージタイプをサポートしています。

それぞれのタイプで、Storage Pool Manager (SPM) と呼ばれるホストが、ホストとストレージ間のアクセスを管理します。SPM ホストは、ストレージプール内にフルアクセスできる唯一のノードです。SPM はストレージドメインのメタデータとプールのメタデータを変更できます。他のすべてのホストは、仮想マシンのハードディスクイメージデータにのみアクセスできます。

デフォルトでは、NFS、ローカル、または POSIX 準拠のデータセンターでは、SPM は、ファイルシステム内のファイルとしてシンプロビジョニングされた形式を使用して仮想ディスクを作成します。

iSCSI およびその他のブロックベースのデータセンターでは、SPM は、提供された論理ユニット番号 (LUN) の上にボリュームグループを作成し、仮想ディスクとして使用する論理ボリュームを作成します。ブロックベースのストレージ上の仮想ディスクは、デフォルトで事前に割り当てられています。

仮想ディスクが事前に割り当てられている場合は、GB 単位で指定されたサイズの論理ボリュームが作成されます。仮想マシンは、**kpartx**、**vgscan**、**vgchange**、または **mount** を使用して Red Hat Enterprise Linux サーバーにマウントして、仮想マシンのプロセスまたは問題を調査できます。

仮想ディスクがシンプロビジョニングされる場合は、1GB の論理ボリュームが作成されます。論理ボリュームは、仮想マシンが実行しているホストによって継続的に監視されます。使用量がしきい値に近づくとすぐに、ホストは SPM に通知し、SPM は論理ボリュームを 1GB 拡張します。ホストは、論理ボリュームが拡張された後、仮想マシンを再開する責任があります。仮想マシンが一時停止状態になる場合は、SPM が時間内にディスクを拡張できなかったことを意味します。これは、SPM がビジー状態であるか、十分なストレージスペースがない場合に発生します。

事前に割り当てられた(RAW)形式の仮想ディスクは、シンプロビジョニング(QCOW2)形式の仮想ディスクよりも書き込み速度が大幅に高速です。シンプロビジョニングは、仮想ディスクの作成にかかる時間が大幅に短縮されます。シンプロビジョニング形式は、I/O を多用しない仮想マシンに適しています。I/O 書き込みが多い仮想マシンには、事前に割り当てられた形式が推奨されます。仮想マシンが 4 秒ごとに 1GB を超える書き込みを実行できる場合は、可能な場合は事前に割り当てられたディスクを使用してください。

11.2. 仮想ディスクの概要

Red Hat Virtualization は、事前割り当て（シックプロビジョニング）および **Sparse**（シンプロビジョニング）ストレージオプションを備えています。

- 事前割り当て

事前に割り当てられた仮想ディスクは、仮想マシンに必要なすべてのストレージを事前に割り当てます。たとえば、仮想マシンのデータパーティション用に事前に割り当てられた 20 GB の論理ボリュームは、作成直後に 20GB のストレージスペースを占有します。

- スパース

スパース割り当てを使用すると、管理者は仮想マシンに割り当てるストレージの合計を定義できますが、ストレージは必要な場合にのみ割り当てられます。

たとえば、20 GB のシンプロビジョニングされた論理ボリュームは、最初に作成されたときに 0 GB のストレージスペースを占有します。オペレーティングシステムがインストールされると、インストールされたファイルのサイズを占める可能性があり、データが最大 20GB のサイ

ズまで追加されるにつれて大きくなり続けます。

ディスクのサイズは、各仮想マシンおよびテンプレートの **Disks** サブタブに一覧表示されます。ディスクの仮想サイズは、仮想マシンが使用できるディスク領域の合計量です。これは、ディスクの作成または編集時に **Size (GB)** フィールドに入力した数です。ディスクの **Actual Size** は、これまでに仮想マシンに割り当てられたディスク容量です。事前に割り当てられたディスクは、両方のフィールドに同じ値を表示します。スパースディスクは、割り当てられたディスク領域の量に応じて、**Virtual Size** フィールドの値から **Actual Size** フィールドに異なる値を表示する場合があります。



注記

Cinder 仮想ディスクを作成する場合には、ディスクの形式およびタイプは Cinder によって内部で処理され、Red Hat Virtualization では管理されません。

次の表に、ストレージの種類と形式の可能な組み合わせを示します。

表11.1 許可されたストレージの組み合わせ

ストレージ	形式	タイプ	注記
NFS または iSCSI/FCP	RAW または QCOW2	スパースまたは事前割り当て	
NFS	RAW	事前割り当て	仮想ディスクに定義されたストレージの量に等しい初期サイズのファイルで、フォーマットはありません。
NFS	RAW	スパース	初期サイズがゼロに近く、フォーマットされていないファイル。
NFS	QCOW2	スパース	初期サイズがゼロに近く、QCOW2 形式であるファイル。後続のレイヤーは QCOW2 形式になります。
SAN	RAW	事前割り当て	仮想ディスクに定義されたストレージの量に等しい初期サイズのブロックデバイスで、フォーマットはありません。

ストレージ	形式	タイプ	注記
NFS または iSCSI/FCP	RAW または QCOW2	スパースまたは事前割り当て	
SAN	QCOW2	スパース	初期サイズが仮想ディスクに定義されたサイズ（現在は1GB）よりもはるかに小さく、必要に応じて領域を割り当てるQCOW2フォーマット（現在は1GBの増分）を持つブロックデバイス。

11.3. 削除後に仮想ディスクをワイプするための設定

wipe_after_delete フラグは、**Wipe After Delete** チェックボックスから管理ポータルに表示されるため、仮想ディスクが削除されると、使用データをゼロに置き換えます。デフォルトである `false` に設定すると、ディスクを削除すると、それらのブロックが再利用できますが、データは消去されません。したがって、ブロックがゼロに戻されていないため、このデータが回復される可能性があります。

wipe_after_delete フラグは、ブロックストレージでのみ機能します。NFSなどのファイルストレージでは、ファイルシステムがデータが存在しないことを確認するため、このオプションは何もしません。

仮想ディスクに対して **wipe_after_delete** を有効にすると、より安全になり、仮想ディスクに機密データが含まれている場合に推奨されます。これはより集中的な操作であり、ユーザーはパフォーマンスの低下と削除時間の延長を経験する可能性があります。



注記

削除後のワイプ機能は安全な削除と同じではなく、データがストレージから削除されることを保証することはできません。同じストレージ上に作成された新しいディスクが古いディスクからのデータを公開しないことだけです。

wipe_after_delete フラグのデフォルトは、セットアッププロセス中に `true` に変更できます(『インストールガイド』の [Red Hat Virtualization Manager の設定](#) を参照)、または Red Hat Virtualization Manager のエンジン設定ツールを使用して変更できます。設定の変更を有効にするためにエンジンを再起動します。



注記

wipe_after_delete フラグのデフォルトを変更しても、すでに存在するディスクの **Wipe After Delete** プロパティーは変更されません。

手順11.1 エンジン設定ツールを使用して SANWipeAfterDelete をデフォルトの True に設定する

1. `--set` アクションを指定してエンジン設定ツールを実行します。

```
# engine-config --set SANWipeAfterDelete=true
```

2. 変更を有効にするには、エンジンを再起動します。

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

ホストにある `/var/log/vdsm/vdsm.log` ファイルをチェックして、仮想ディスクが正常に消去および削除されたことを確認できます。

消去に成功すると、ログファイルにはエントリー `storage_domain_id/volume_id` が含まれ、が削除されます。以下に例を示します。

```
a9cb0625-d5dc-49ab-8ad1-72722e82b0bf/a49351a7-15d8-4932-8d67-512a369f9d61 was zeroed  
and will be deleted
```

削除に成功すると、ログファイルには VG で終了したエントリー (`storage_domain_id LVs: list_of_volume_ids, img: image_id`) が含まれます。以下に例を示します。

```
finished with VG:a9cb0625-d5dc-49ab-8ad1-72722e82b0bf LVs: {'a49351a7-15d8-4932-8d67-  
512a369f9d61': imgsPar(imgs=['11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d'], parent='00000000-0000-  
0000-0000-000000000000'), img: 11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d}
```

消去に失敗すると、ログメッセージ `zeroing storage_domain_id/volume_id failed` が表示されます。`Zero and remove this volume manually` が表示され、削除に失敗すると `Remove failed for some of VG: storage_domain_id zeroed volumes: list_of_volume_ids` が表示されます。

11.4. RED HAT VIRTUALIZATION の共有可能ディスク

一部のアプリケーションでは、サーバー間でストレージを共有する必要があります。Red Hat Virtualization では、仮想マシンのハードディスクを **共有可能** としてマークし、それらのディスクを仮想マシンに割り当てることができます。このようにして、単一の仮想ディスクを複数のクラスター対応ゲストが使用できます。

共有ディスクは、すべての状況で使用されるわけではありません。クラスター化されたデータベースサーバーやその他の高可用性サービスなどのアプリケーションには、共有ディスクが適しています。クラスターに対応していない複数のゲストに共有ディスクを接続すると、ディスクへの読み取りと書き込みが調整されていないため、データが破損する可能性があります。

共有ディスクのスナップショットを撮ることはできません。スナップショットが取得された仮想ディスクは、後で共有可能としてマークすることはできません。

ディスクを作成するとき、または後でディスクを編集することによって、ディスクを共有可能としてマークできます。

11.5. RED HAT VIRTUALIZATION の読み取り専用ディスク

一部のアプリケーションでは、管理者が読み取り専用の権限でデータを共有する必要があります。これは、仮想マシンの詳細ペインの **Disks** タブから仮想マシンに接続されているディスクを作成または編集し、**Read Only** チェックボックスを選択して実行できます。これにより、管理者が書き込み権限を維持しながら、単一のディスクを複数のクラスター対応ゲストが読み取ることができます。

仮想マシンの実行中は、ディスクの読み取り専用ステータスを変更することはできません。



重要

ジャーナルファイルシステムをマウントするには、読み取り/書き込みアクセスが必要です。 **Read Only** オプションの使用は、そのようなファイルシステム(**EXT3**、**EXT4**、**XFS**など)を含む仮想ディスクには適していません。

11.6. 仮想ディスクタスク

11.6.1. Floating 仮想ディスクの作成



重要

Floating 仮想ディスクの作成はテクノロジープレビュー機能です。テクノロジープレビュー機能は、Red Hat の実稼働環境でのサービスレベルアグリーメント (SLA) ではサポートされていないため、Red Hat では実稼働環境での使用を推奨していません。テクノロジープレビューの機能は、最新の製品機能をいち早く提供して、開発段階で機能のテストを行いフィードバックを提供していただくことを目的としています。

Red Hat のテクノロジープレビュー機能のサポートについての詳細は、を参照してください <https://access.redhat.com/support/offering/techpreview/>。

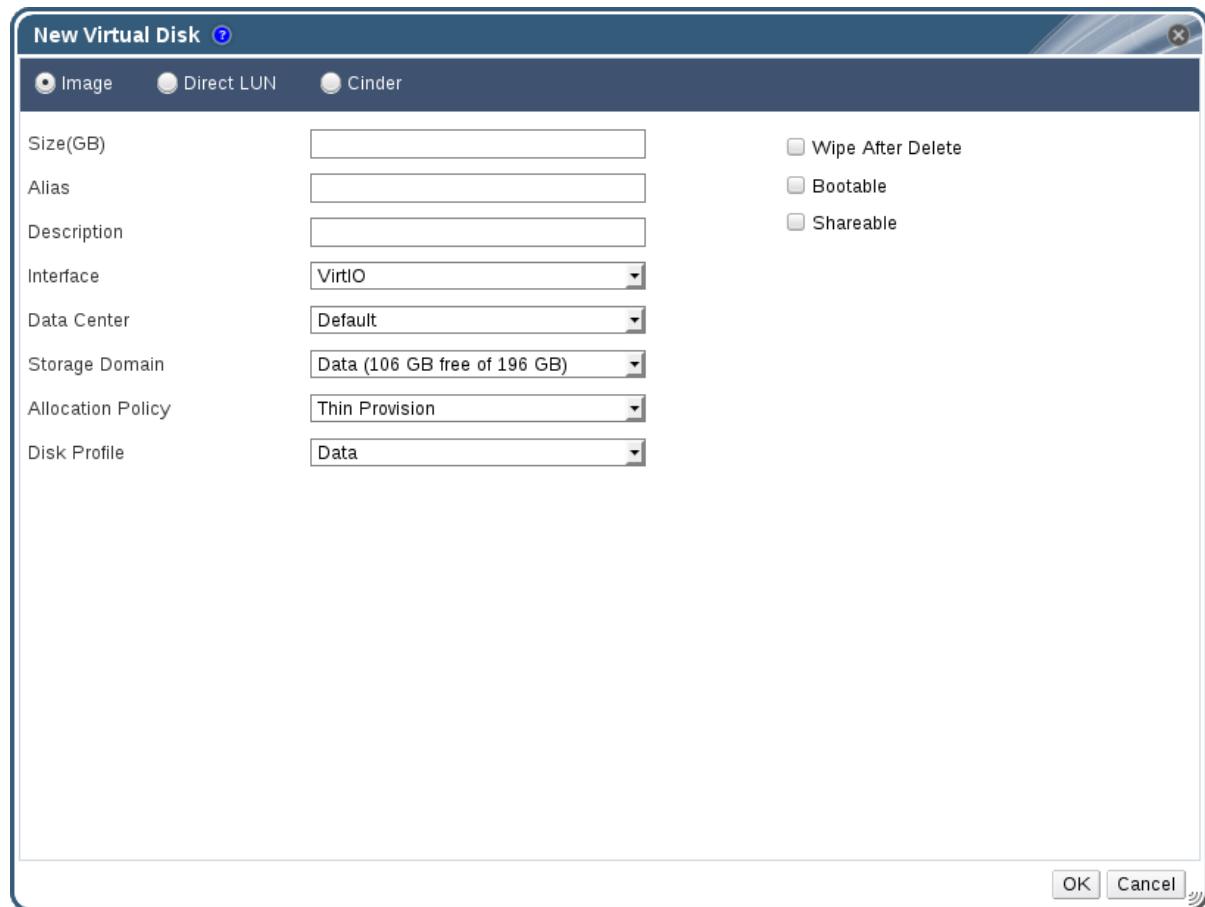
どの仮想マシンにも属さない仮想ディスクを作成できます。次に、このディスクを単一の仮想マシンにアタッチしたり、ディスクが共有可能な場合は複数の仮想マシンにアタッチしたりできます。

イメージ ディスクの作成は、Manager によって完全に管理されます。ダイレクト LUN ディスクには、外部で準備済みのターゲットがすでに存在している必要があります。Cinder ディスクには、外部プロバイダー ウィンドウを使用して Red Hat Virtualization 環境に追加された OpenStack ボリュームのインスタンスへのアクセスが必要です。詳細は、「ストレージ管理用の OpenStack Volume (Cinder) インスタンスの追加」を参照してください。

手順11.2 Floating 仮想ディスクの作成

1. **Disks** resource タブを選択します。
2. **New** をクリックします。

図11.1 Add Virtual Disk ウィンドウ



3. ラジオボタンを使用して、仮想ディスクを **イメージ**、**Direct LUN**、または **Cinder** ディスクにするかを指定します。
4. 仮想ディスクに必要なオプションを選択します。オプションは、選択したディスクタイプに基づいて変更します。各ディスクタイプの各オプションの詳細は、[「新しい仮想ディスクウィンドウの設定の説明」](#) を参照してください。
5. **OK** をクリックします。

11.6.2. 新しい仮想ディスクウィンドウの設定の説明

表11.2 新しい仮想ディスク設定：イメージ

フィールド名	説明
Size(GB)	新しい仮想ディスクのサイズ (GB 単位)。
エイリアス	仮想ディスクの名前。最大で 40 文字に制限されます。
Description	仮想ディスクの説明。このフィールドは推奨されますが、必須ではありません。

フィールド名	説明
Interface	<p>ディスクが仮想マシンに提示する仮想インターフェイス。 VirtIO は高速ですが、ドライバーが必要です。Red Hat Enterprise Linux 5 以降には、これらのドライバーが含まれます。Windows にはこれらのドライバーは含まれていませんが、ゲストツール ISO または仮想フロッピーディスクからインストールできます。 IDE デバイスは特別なドライバーを必要としません。</p> <p>インターフェイスタイプは、ディスクが接続されているすべての仮想マシンを停止した後に更新できます。</p>
Data Center	仮想ディスクが利用できるデータセンター。
Storage Domain	仮想ディスクが保存されるストレージドメイン。ドップダウンリストには、特定のデータセンターで使用可能なすべてのストレージドメインが表示され、ストレージドメインで使用可能な合計容量と現在使用可能な容量も表示されます。
Allocation Policy	<p>新しい仮想ディスクのプロビジョニングポリシー。</p> <ul style="list-style-type: none"> ● 事前 割り当てでは、仮想ディスクの作成時に、ディスクのサイズ全体をストレージドメインに割り当てます。事前に割り当てられたディスクの仮想サイズと実際のサイズは同じです。事前に割り当てられた仮想ディスクは、シンプロビジョニングされた仮想ディスクよりも作成に時間がかかりますが、読み取りと書き込みのパフォーマンスが向上します。サーバーやその他の I/O を多用する仮想マシンには、事前に割り当てられた仮想ディスクをお勧めします。仮想マシンが 4 秒ごとに 1GB を超える書き込みを実行できる場合は、可能な場合は事前に割り当てられたディスクを使用してください。 ● シンプロビジョニングは、仮想ディスクの作成時に 1GB を割り当て、ディスクを拡張できるサイズの最大制限を設定します。ディスクの仮想サイズは最大制限です。ディスクの実際のサイズは、これまでに割り当てられたスペースです。シンプロビジョニングされたディスクは、事前に割り当てられたディスクよりも作成が早く、ストレージのオーバーコミットが可能です。デスクトップには、シンプロビジョニングされた仮想ディスクが推奨されます。

フィールド名	説明
ディスクプロファイル	仮想ディスクに割り当てられたディスクプロファイル。ディスクプロファイルは、ストレージドメイン内の仮想ディスクのスループットの最大量と入出力操作の最大レベルを定義します。ディスクプロファイルは、データセンター用に作成されたストレージのサービス品質エントリーに基づいて、ストレージドメインレベルで定義されます。
Wipe After Delete	仮想ディスクが削除されたときに機密資料を削除するための強化されたセキュリティーを有効にすることができます。
Bootable	仮想ディスクで起動可能フラグを有効にすることができます。
Shareable	一度に複数の仮想マシンに仮想ディスクを接続できます。

Direct LUN 設定は、**Targets > LUNs** または **LUNs > Targets** のいずれかで 確認 できます。ターゲット > **LUN** は、検出されたホストに従って利用可能な LUN をソートしますが、**LUN > Targets** は LUN を1つ表示します。

表11.3 新しい仮想ディスク設定：ダイレクト LUN

フィールド名	説明
エイリアス	仮想ディスクの名前。最大で 40 文字に制限されます。
Description	仮想ディスクの説明。このフィールドは推奨されますが、必須ではありません。デフォルトでは、LUN ID の最後の 4 文字がフィールドに挿入されます。 デフォルトの動作は、 engine-config コマンドを使用して PopulateDirectLUNDiskDescriptionWithLUNId 設定キーを適切な値に設定することで設定できます。設定キーは、完全な LUN ID を使用する場合は -1 に設定でき、この機能を無視する場合は 0 に設定できます。正の整数は、説明に LUN ID の対応する文字数を入力します。詳細は、「 engine-config コマンドの構文 」を参照してください。

フィールド名	説明
インターフェイス	<p>ディスクが仮想マシンに提示する仮想インターフェイス。 VirtIO は高速ですが、ドライバーが必要です。Red Hat Enterprise Linux 5 以降には、これらのドライバーが含まれます。Windows にはこれらのドライバーは含まれていませんが、ゲストツール ISO または仮想フロッピーディスクからインストールできます。IDE デバイスは特別なドライバーを必要としません。</p> <p>インターフェイスタイプは、ディスクが接続されているすべての仮想マシンを停止した後に更新できます。</p>
Data Center	仮想ディスクが利用できるデータセンター。
ホストの使用	LUN がマウントされるホスト。データセンター内の任意のホストを選択できます。
Storage Type	追加する外部 LUN のタイプ。 iSCSI または ファイルチャネル から選択できます。
Discover Targets	<p>このセクションは、iSCSI 外部 LUN を使用し、Targets > LUNs が選択されている場合に展開できます。</p> <p>アドレス - ターゲットサーバーのホスト名または IP アドレス。</p> <p>ポート - ターゲットサーバーへの接続を試みるポート。デフォルトのポートは 3260 です。</p> <p>ユーザー認証 - iSCSI サーバーにはユーザー認証が必要です。iSCSI 外部 LUN を使用している場合は、User Authentication フィールドが表示されます。</p> <p>CHAP username - LUN にログインする権限を持つユーザーのユーザー名。このフィールドは、User Authentication チェックボックスが選択されている場合にアクセスできます。</p> <p>CHAP password - LUN にログインする権限を持つユーザーのパスワード。このフィールドは、User Authentication チェックボックスが選択されている場合にアクセスできます。</p>
Bootable	仮想ディスクで起動可能フラグを有効にすることができます。
Shareable	一度に複数の仮想マシンに仮想ディスクを接続できます。

フィールド名	説明
Enable SCSI Pass-Through	Interface が VirtIO-SCSI に設定されている場合に使用できます。このチェックボックスをオンになると、物理 SCSI デバイスを仮想ディスクにパススルーできます。SCSI パススルーハーが有効になっている VirtIO-SCSI インターフェイスには、SCSI 廃棄のサポートが自動的に含まれています。このチェックボックスが選択されていない場合、仮想ディスクはエミュレートされた SCSI デバイスを使用します。
Allow Privileged SCSI I/O	Enable SCSI Pass-Through チェックボックスがオフになっている場合に使用できます。このチェックボックスをオフになると、フィルターリングされていない SCSI Generic I/O (SG_IO) アクセスが有効になり、ディスク上で特権 SG_IO コマンドが許可されます。これは永続的な予約に必要です。

Discover Targets セクションにフィールドに入力し、**Discover** をクリックしてターゲットサーバーを検出します。次に、**Login All** ボタンをクリックしてターゲットサーバーで利用可能な LUN を一覧表示し、各 LUN の横にあるラジオボタンを使用して、追加する LUN を選択します。

LUN を仮想マシンのハードディスクイメージとして直接使用すると、仮想マシンとそのデータの間の抽象化レイヤーが削除されます。

ダイレクト LUN を仮想マシンのハードディスクイメージとして使用する場合は、次の考慮事項を考慮する必要があります。

- ダイレクト LUN ハードディスクイメージのライブストレージ移行はサポートされていません。
- ダイレクト LUN ディスクは、仮想マシンのエクスポートには含まれません。
- ダイレクト LUN ディスクは、仮想マシンのスナップショットには含まれていません。

関連するデータセンターにディスクを作成するパーミッションがある OpenStack ボリュームストレージドメインがない場合には、**Cinder** 設定フォームが無効になります。**Cinder** ディスクには、外部プロバイダー ウィンドウを使用して Red Hat Virtualization 環境に追加された OpenStack ボリュームのインスタンスへのアクセスが必要です。詳細は、「[ストレージ管理用の OpenStack Volume \(Cinder\) インスタンスの追加](#)」を参照してください。

表11.4 新しい仮想ディスク設定 : Cinder

フィールド名	説明
Size(GB)	新しい仮想ディスクのサイズ (GB 単位)。
エイリアス	仮想ディスクの名前。最大で 40 文字に制限されます。
Description	仮想ディスクの説明。このフィールドは推奨されますが、必須ではありません。

フィールド名	説明
Interface	<p>ディスクが仮想マシンに提示する仮想インターフェイス。 VirtIO は高速ですが、ドライバーが必要です。Red Hat Enterprise Linux 5 以降には、これらのドライバーが含まれます。Windows にはこれらのドライバーは含まれていませんが、ゲストツール ISO または仮想フロッピーディスクからインストールできます。IDE デバイスは特別なドライバーを必要としません。</p> <p>インターフェイスタイプは、ディスクが接続されているすべての仮想マシンを停止した後に更新できます。</p>
Data Center	仮想ディスクが利用できるデータセンター。
Storage Domain	仮想ディスクが保存されるストレージドメイン。ドロップダウンリストには、特定のデータセンターで使用可能なすべてのストレージドメインが表示され、ストレージドメインで使用可能な合計容量と現在使用可能な容量も表示されます。
Volume Type	仮想ディスクのボリュームタイプ。ドロップダウンリストには、利用可能なすべてのボリュームタイプが表示されます。このボリュームタイプは、OpenStack Cinder で管理および設定されます。
Bootable	仮想ディスクで起動可能フラグを有効にすることができます。
Shareable	一度に複数の仮想マシンに仮想ディスクを接続できます。

11.6.3. ライブストレージ移行の概要

仮想ディスクは、それらが接続されている仮想マシンの実行中に、あるストレージドメインから別のストレージドメインに移行できます。これは、ライブストレージ移行と呼ばれます。実行中の仮想マシンに接続されているディスクが移行されると、そのディスクのイメージチェーンのスナップショットがソースストレージドメインに作成され、イメージチェーン全体が宛先ストレージドメインに複製されます。そのため、ソースストレージドメインと宛先ストレージドメインの両方に、ディスクイメージチェーンとスナップショットの両方をホストするのに十分なストレージスペースがあることを確認してください。移行が失敗した場合でも、ライブストレージの移行が試行されるたびに新しいスナップショットが作成されます。

ライブストレージ移行を使用する場合は、次の点を考慮してください。

- 一度に複数のディスクをライブマイグレーションできます。
- 同じ仮想マシンの複数のディスクは複数のストレージドメインにまたがって存在できますが、各ディスクのイメージチェーンは単一のストレージドメインに存在する必要があります。

- 同じデータセンター内の任意の 2 つのストレージドメイン間でディスクをライブマイグレーションできます。
- ダイレクト LUN ハードディスクイメージまたは共有可能としてマークされたディスクをライブマイグレーションすることはできません。

11.6.4. 仮想ディスクの移動

仮想マシンに接続されている、またはフローティング仮想ディスクとして機能する仮想ディスクを、あるストレージドメインから別のストレージドメインに移動します。実行中の仮想マシンに接続されている仮想ディスクを移動できます。これは、ライブストレージ移行と呼ばれます。または、続行する前に仮想マシンをシャットダウンします。

ディスクを移動するときは、次の点を考慮してください。

- 複数のディスクを同時に移動できます。
- 同じデータセンター内の任意の 2 つのストレージドメイン間でディスクを移動できます。
- テンプレートに基づいて作成され、シンプロビジョンストレージ割り当てオプションを使用した仮想マシンに仮想ディスクが接続されている場合は、仮想マシンが仮想ディスクと同じストレージドメインに基づいていたテンプレートのディスクをコピーする必要があります。

手順11.3 仮想ディスクの移動

- Disks** タブを選択します。
- 移動する仮想ディスクを 1 つ以上選択します。
- Move** をクリックして、**Move Disk (s)** ウィンドウを開きます。
- Target** リストから、仮想ディスクを移動するストレージドメインを選択します。
- 必要に応じて、**Disk Profile** リストからディスクのプロファイルを選択します。
- OK** をクリックします。

仮想ディスクはターゲットストレージドメインに移動し、移動中にステータスが **Locked** になります。

11.6.5. ディスクインターフェイスタイプの変更

ユーザーは、ディスクの作成後にディスクのインターフェイスタイプを変更できます。これにより、既存のディスクを、異なるインターフェイスタイプを必要とする仮想マシンに接続できます。たとえば、**VirtIO**インターフェイスを使用するディスクは、**VirtIO-SCSI** または **IDE**インターフェイスを必要とする仮想マシンに接続できます。これにより、バックアップと復元、または障害復旧の目的でディスクを移行する柔軟性が提供されます。共有可能ディスクのディスクインターフェイスは、仮想マシンごとに更新することもできます。これは、共有ディスクを使用する各仮想マシンが異なるインターフェイスタイプを使用できることを意味します。

ディスクインターフェイスタイプを更新するには、最初にディスクを使用するすべての仮想マシンを停止する必要があります。

手順11.4 ディスクインターフェイスタイプの変更

- Virtual Machines** タブを選択し、適切な仮想マシンを停止します。

2. **Disks** サブタブからディスクを選択し、**Edit** をクリックします。
3. インターフェイスリストから新しいインターフェイスタイプを選択し、**OK** をクリックします。

これで、仮想マシンはディスクに別の仮想インターフェイスを使用します。

以下の手順は、異なるインターフェイスタイプを必要とする別の仮想マシンにディスクを割り当てる方法を示しています。

手順11.5 別のインターフェイスタイプを使用して別の仮想マシンにディスクを接続

1. **Virtual Machines** タブを選択し、適切な仮想マシンを停止します。
2. ディスクの割り当てを解除する仮想マシンを選択します。
3. **Disks** サブタブからディスクを選択し、**Remove** をクリックします。
4. 仮想マシンタブで、ディスクが割り当てられる新しい仮想マシンを選択します。
5. **アタッチ** をクリックします。
6. **Attach Virtual Disks** ウィンドウでディスクを選択し、**Interface** ドロップダウンメニューから適切なインターフェイスを選択します。
7. **OK** をクリックします。

11.6.6. 仮想ディスクのコピー

概要

あるストレージドメインから別のストレージドメインに仮想ディスクをコピーできます。コピーしたディスクは仮想マシンに接続できます。

手順11.6 仮想ディスクのコピー

1. **Disks** タブを選択します。
2. コピーする仮想ディスクを選択します。
3. **Copy** ボタンをクリックして、**Copy Disk (s)** ウィンドウを開きます。
4. 必要に応じて、**Alias** テキストフィールドにエイリアスを入力します。
5. **Target** ドロップダウンメニューを使用して、仮想ディスクのコピー先となるストレージドメインを選択します。
6. **OK** をクリックします。

結果

仮想ディスクはターゲットストレージドメインにコピーされ、コピー中にステータスが **Locked** になります。

11.6.7. ストレージドメインへのディスクイメージのアップロード

QEMU 互換の仮想ディスクイメージは、ローカルマシンから Red Hat Virtualizationストレージドメインにアップロードし、仮想マシンに割り当てることができます。

仮想ディスクイメージタイプは QCOW2 または Raw のいずれかである必要があります。QCOW2 ディスクイメージから作成されたディスクは共有できず、QCOW2 ディスクイメージファイルにはバックアップファイルを含めることはできません。

前提条件:

- **engine-setup** の実行時にイメージ I/O プロキシーを設定する必要があります。 詳細は、『インストールガイド』の [Red Hat Virtualization Manager の設定](#) を参照してください。
- 管理ポータルへのアクセスに使用される Web ブラウザーに必要な認証局をインポートする必要があります。
- このアップロード手順を実行するには、Internet Explorer 10、Firefox 35、または Chrome 13 以降が必要です。以前のバージョンのブラウザーは、必要な HTML5 API をサポートしていません。



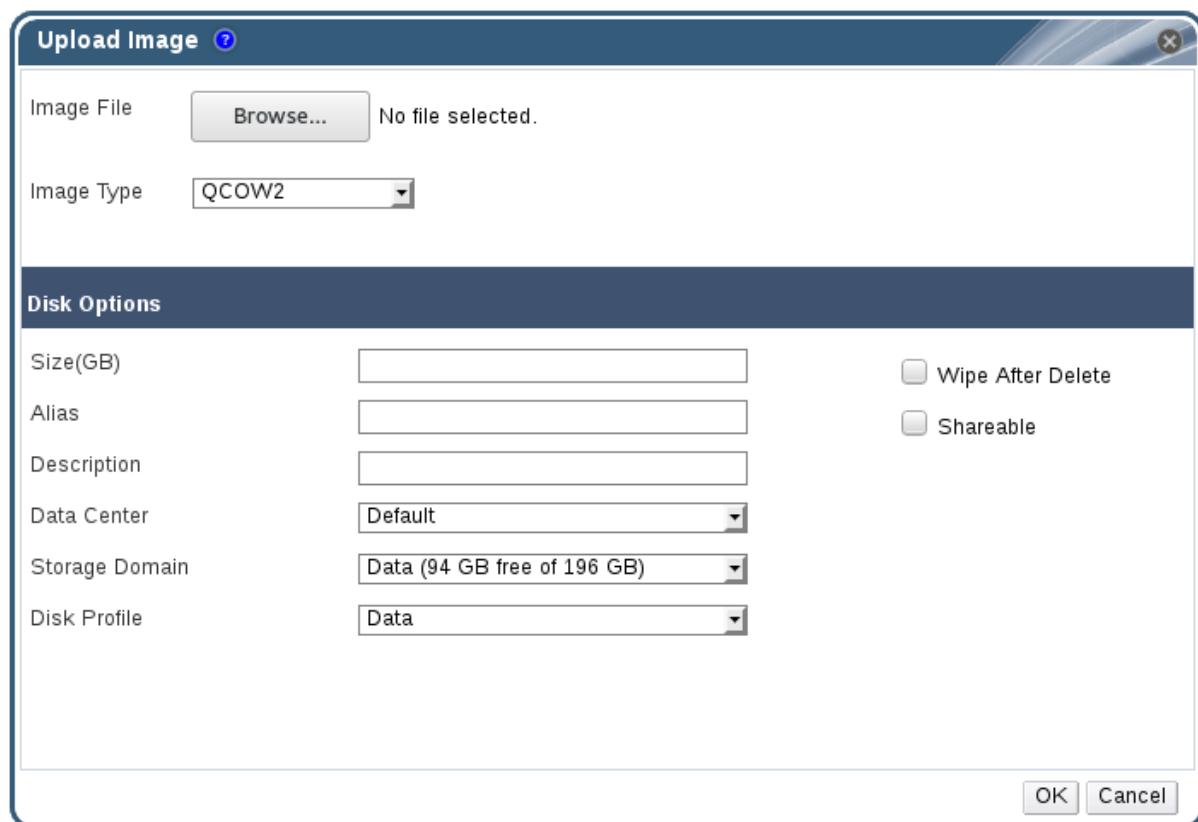
注記

認証局をインポートするには、https://engine_address/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA を参照して、すべての信頼設定を選択します。 [Firefox](#)、[Internet Explorer](#)、または [Google Chrome](#) に認証局をインストールする手順を参照してください。

手順11.7 ストレージドメインへのディスクイメージのアップロード

1. Upload Image 画面を開きます。
 - **Disks** タブで、**Upload** ドロップダウンから **Start** を選択します。
 - または、**Storage** タブでストレージドメインを選択し、**Disks** サブタブを選択し、**Upload** ドロップダウンメニューから **Start** を選択します。

図11.2 イメージのアップロード画面



2. イメージの アップロード 画面で 参照 をクリック し、ローカルディスクのイメージを選択します。
3. **Image Type** を QCOW2 または Raw に設定します。
4. **Disk Option** フィールドに入力します。関連するフィールドの説明は、「[新しい仮想ディスク ウィンドウの設定の説明](#)」を参照してください。
5. **OK** をクリックします。

進捗バーには、アップロードのステータスが表示されます。Upload ドロップダウンからアップロードを一時停止、キャンセル、または再開することもできます。

11.6.8. インポートされたストレージドメインからのディスクイメージのインポート

詳細ペインの **Disk Import** タブを使用して、インポートされたストレージドメインからフローティング仮想ディスクをインポートします。



注記

Manager にインポートできるのは QEMU 互換ディスクのみです。

手順11.8 ディスクイメージのインポート

1. データセンターにインポートされたストレージドメインを選択します。
2. 詳細ペインで、**Disk Import** をクリックします。
3. 1つ以上のディスクイメージを選択し、**Import** をクリックして **Import Disk (s)** ウィンドウを開きます。

4. 各ディスクに適切なディスクプロファイルを選択します。
5. **OK** をクリックして、選択したディスクをインポートします。

11.6.9. インポートされたストレージドメインからの未登録のディスクイメージのインポート

詳細ペインの **Disk Import** タブを使用して、ストレージドメインからフローティング仮想ディスクをインポートします。Red Hat Virtualization 環境の外部で作成されたフローティングディスクは、Manager には登録されません。ストレージドメインをスキャンして、インポートする未登録のフローティングディスクを特定します。



注記

Manager にインポートできるのは QEMU 互換ディスクのみです。

手順11.9 ディスクイメージのインポート

1. データセンターにインポートされたストレージドメインを選択します。
2. ストレージドメインを右クリックし、**Scan Disks** を選択して、Manager が未登録のディスクを特定できるようにします。
3. 詳細ペインで、**Disk Import** をクリックします。
4. 1つ以上のディスクイメージを選択し、**Import** をクリックして **Import Disk (s)** ウィンドウを開きます。
5. 各ディスクに適切なディスクプロファイルを選択します。
6. **OK** をクリックして、選択したディスクをインポートします。

11.6.10. OpenStack Image サービスからの仮想ディスクイメージのインポート

概要

OpenStack Image サービスが外部プロバイダーとして Manager に追加されている場合は、OpenStack Image サービスが管理する仮想ディスクイメージを Red Hat Virtualization Manager にインポートすることができます。

1. **Storage** resource タブをクリックし、結果リストから OpenStack Image Service ドメインを選択します。
2. 詳細ペインの **Images** タブで、インポートするイメージを選択します。
3. **Import** をクリックして **Import Image (s)** ウィンドウを開きます。
4. **Data Center** ドロップダウンメニューから、仮想ディスクイメージをインポートするデータセンターを選択します。
5. **Domain Name** ドロップダウンメニューから、仮想ディスクイメージを保存するストレージドメインを選択します。
6. オプションで **Quota** ドロップダウンメニューからクオータを選択し、クオータを仮想ディスクイメージに適用します。

7. **OK** をクリックしてイメージをインポートします。

結果

イメージはフローティングディスクとしてインポートされ、**Disks** resource タブの結果一覧に表示されます。これで、仮想マシンに接続できます。

11.6.11. OpenStack Image Service への仮想ディスクのエクスポート

概要

仮想ディスクは、外部プロバイダーとして Manager に追加された OpenStack Image Service にエクスポートできます。

1. **Disks** resource タブをクリックします。
2. エクスポートするディスクを選択します。
3. **Export** ボタンをクリックして、**Export Image (s)** ウィンドウを開きます。
4. **Domain Name** ドロップダウンリストから、ディスクのエクスポート先となる OpenStack Image Service を選択します。
5. クォータを適用する場合は、**Quota** ドロップダウンリストからディスクのクォータを選択します。
6. **OK** をクリックします。

結果

仮想ディスクは、指定された OpenStack Image サービスにエクスポートされ、仮想ディスクイメージとして管理されます。



重要

仮想ディスクは、複数のボリュームを持たない場合、シンプロビジョニングされず、スナップショットがない場合にのみエクスポートできます。

11.7. 仮想ディスクおよびパーティション

11.7.1. 仮想ディスクのシステムパーティションの管理

システム管理者は **SuperUser** として、管理ポータルのすべての側面を管理します。他のユーザーに特定の管理ロールを割り当てることができます。このような制限された管理者ロールは、特定のリソースに制限される管理者権限をユーザーに付与する際に役立ちます。たとえば、**DataCenterAdmin** ロールは、そのデータセンターのストレージを除く、割り当てられたデータセンターの管理者権限のみを持ち、**ClusterAdmin** は割り当てられたクラスターに対してのみ管理者権限を持ちます。

Red Hat Virtualization Manager では、デフォルトの仮想ディスクユーザーロールが 2 つ提供されますが、デフォルトの仮想ディスク管理者ロールはありません。ユーザーロールの 1 つである **DiskCreator** ロールにより、ユーザーportalからの仮想ディスクの管理が可能になります。このロールは、特定の仮想マシン、データセンター、特定のストレージドメイン、または仮想化環境全体に適用することができます。これは、異なるユーザーが異なる仮想リソースを管理できるようにするために役立ちます。

仮想ディスク作成者ロールは、以下のアクションを許可します。

- 仮想マシンまたは他のリソースに関連付けられた仮想ディスクの作成、編集、および削除。
- 仮想ディスクのユーザーパーミッションを編集します。



注記

ロールやパーミッションは、既存のユーザーにのみ割り当てることができます。

11.7.2. 仮想ディスクユーザー ロールの概要

仮想ディスクユーザー パーミッション ロール

以下の表は、ユーザー ポータルでの仮想ディスクの使用および管理に適用されるユーザー ロールと権限について説明しています。

表11.5 Red Hat Virtualization システム管理者 ロール

ロール	権限	注記
DiskOperator	仮想ディスクユーザー。	仮想ディスクの使用、表示、編集が可能です。仮想ディスクが接続されている仮想マシンを使用するパーミッションを継承します。
DiskCreator	割り当てられたクラスターまたはデータセンター内の仮想ディスクを作成、編集、管理、および削除できる。	このロールは特定の仮想ディスクには適用されません。 Configure ウィンドウで環境全体のユーザーにこのロールを適用します。また、特定のデータセンター、クラスター、またはストレージドメインにこのロールを適用することもできます。

11.7.3. 管理者またはユーザー ロールのリソースへの割り当て

管理者またはユーザー ロールをリソースに割り当て、ユーザーがそのリソースにアクセスしたり、管理したりできるようにします。

手順11.10 リソースへのロールの割り当て

- リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
- 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
- Add** をクリックします。
- Search** テキストボックスに既存ユーザーの名前またはユーザー名を入力し、**Go** をクリックします。表示された候補の中からユーザーを選択します。
- Role to Assign:** ドロップダウンリストからロールを選択します。
- OK** をクリックします。

ユーザーにロールを割り当てました。そのリソースで有効にしたそのロールの継承されたパーミッションが、ユーザーに付与されました。

11.7.4. リソースからの管理者またはユーザーロールの削除

管理者またはユーザーのロールをリソースから削除すると、ユーザーはそのリソースのロールに関連付けられ継承されたパーミッションを失います。

手順11.11 リソースからのロールの削除

1. リソースタブ、ツリーモード、または検索機能を使用してリソースを検索し、結果一覧で選択します。
2. 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承されたパーミッションを一覧表示します。
3. リソースから削除するユーザーを選択します。
4. **Remove** をクリックします。**Remove Permission** 画面が開き、パーミッションの削除を確認します。
5. **OK** をクリックします。

ユーザーのロールおよび関連付けられたパーミッションをリソースから削除しました。

第12章 外部プロバイダー

12.1. RED HAT VIRTUALIZATION における外部プロバイダーの紹介

Red Hat Virtualization Manager 自体によって管理されるリソースに加えて、Red Hat Virtualization は外部ソースによって管理されるリソースを利用することもできます。外部プロバイダーと呼ばれるこれらのリソースのプロバイダーは、仮想化ホスト、仮想マシンイメージ、ネットワークなどのリソースを提供できます。

Red Hat Virtualization は現在、以下の外部プロバイダーをサポートしています。

ホストプロビジョニング用の Red Hat Satellite

Satellite は、物理ホストと仮想ホストの両方のライフサイクルのすべての側面を管理するためのツールです。Red Hat Virtualization では、Satellite によって管理されるホストを、Red Hat Virtualization Manager に仮想化ホストとして追加して使用できます。Manager に Satellite インスタンスを追加した後、新しいホストを追加するときにその Satellite インスタンスで使用可能なホストを検索することにより、Satellite インスタンスによって管理されるホストを追加できます。Red Hat Satellite のインストールおよび Red Hat Satellite を使用したホストの管理に関する詳細は、[インストールガイド](#) および [ホスト設定ガイド](#) を参照してください。

イメージ管理用の OpenStack Image Service (Glance)

OpenStack Image Service は、仮想マシンイメージのカタログを提供します。Red Hat Virtualization では、これらのイメージを Red Hat Virtualization Manager にインポートして、フローティングディスクとして使用したり、仮想マシンに接続してテンプレートに変換したりできます。OpenStack Image Service を Manager に追加すると、どのデータセンターにも接続されていないストレージドメインとして表示されます。Red Hat Virtualization 環境の仮想ディスクは、仮想ディスクイメージとして OpenStack Image Service にエクスポートすることもできます。

ネットワークプロビジョニング用の OpenStack Networking (Neutron)

OpenStack Networking は、ソフトウェア定義ネットワークを提供します。Red Hat Virtualization では、OpenStack Networking が提供するネットワークを Red Hat Virtualization Manager にインポートして、あらゆる種類のトラフィックを伝送し、複雑なネットワークトポロジーを作成するのに使用します。OpenStack Networking を Manager に追加した後に、手動でインポートして OpenStack Networking が提供するネットワークにアクセスすることができます。

ストレージ管理用の OpenStack ボリューム (Cinder)

OpenStack Volume は、仮想ハードドライブの永続的なブロックストレージ管理機能を提供します。OpenStack Cinder ボリュームは Ceph Storage によりプロビジョニングされます。Red Hat Virtualization では、OpenStack ボリュームストレージ上にディスクを作成することができます。このストレージは、フローティングディスクとして使用したり、仮想マシンにアタッチしたりできます。OpenStack ボリュームを Manager に追加した後に、OpenStack ボリュームが提供するストレージにディスクを作成することができます。

仮想マシンプロビジョニング用の VMware

VMware で作成された仮想マシンは、V2V (virt-v2v)を使用して変換し、Red Hat Virtualization 環境にインポートできます。VMware プロバイダーを Manager に追加した後、それが提供する仮想マシンをインポートできます。V2V 変換は、インポート操作の一部として、指定されたプロキシホストで実行されます。

ネットワークプロビジョニング用の外部ネットワークプロバイダー

サポート対象の外部ソフトウェア定義のネットワークプロバイダーには、OpenStack REST API を実装するプロバイダーが含まれます。OpenStack Networking (Neutron) とは異なり、Neutron エー

ジェントはホスト上の仮想インターフェイスドライバーの実装としては使用されません。代わりに、仮想インターフェイスドライバーは、外部ネットワークプロバイダーの実装者が提供する必要があります。

すべての外部リソースプロバイダーは、入力にあった単一のウィンドウを使用して追加されます。Red Hat Virtualization 環境で提供されるリソースを使用するには、リソースプロバイダーを追加する必要があります。

12.2. 外部プロバイダーの追加

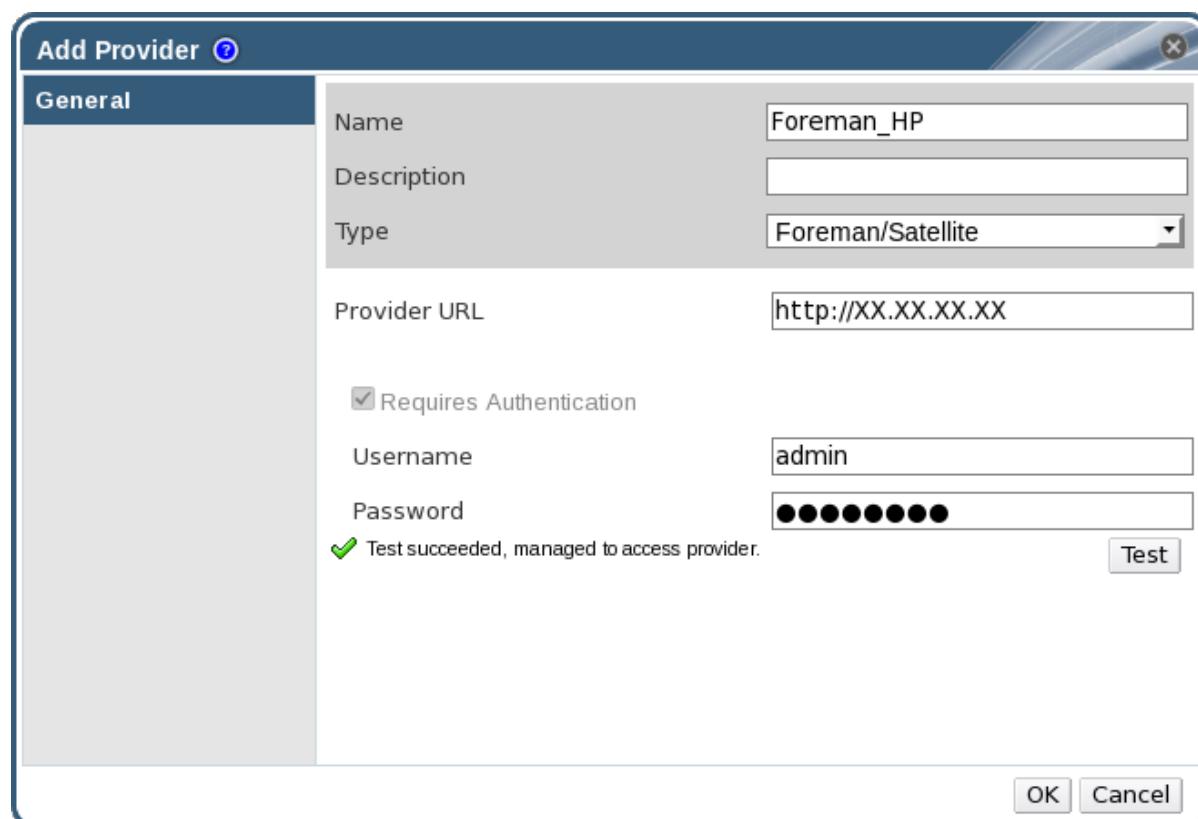
12.2.1. ホストのプロビジョニング用の Red Hat Satellite インスタンスの追加

ホストプロビジョニング用の Satellite インスタンスを Red Hat Virtualization Manager に追加します。Red Hat Virtualization 4.0 は Red Hat Satellite 6.1 でサポートされています。

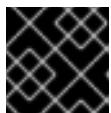
手順12.1 ホストプロビジョニング用の Satellite インスタンスの追加

1. ツリーペインで **External Providers** エントリーを選択します。
2. **Add** をクリックして **Add Provider** ウィンドウを開きます。

図12.1 Add Provider ウィンドウ



3. **Name** および **Description** を入力します。
4. タイプリストから **Foreman/Satellite** が選択されていることを確認します。
5. Satellite インスタンスがインストールされているマシンの URL または完全修飾ドメイン名を **Provider URL** テキストフィールドに入力します。ポート番号を指定する必要はありません。

**重要**

IP アドレスを使用して Satellite インスタンスを追加することはできません。

6. Satellite インスタンスの **ユーザー名** と **パスワード** を入力します。Satellite プロビジョニングポータルへのログインに使用するのと同じユーザー名とパスワードを使用する必要があります。
7. 認証情報をテストします。
 - a. **Test** をクリックして、提供された認証情報を使用して Satellite インスタンスで正常に認証できるかどうかをテストします。
 - b. Satellite インスタンスが SSL を使用する場合は、**Import provider certificates** ウィンドウが開きます。**OK** をクリックして、Satellite インスタンスが提供する証明書をインポートします。

**重要**

Manager がインスタンスと通信できるようにするには、Satellite インスタンスが提供する証明書をインポートする必要があります。

8. **OK** をクリックします。

Satellite インスタンスを Red Hat Virtualization Manager に追加し、提供するホストを操作できる。

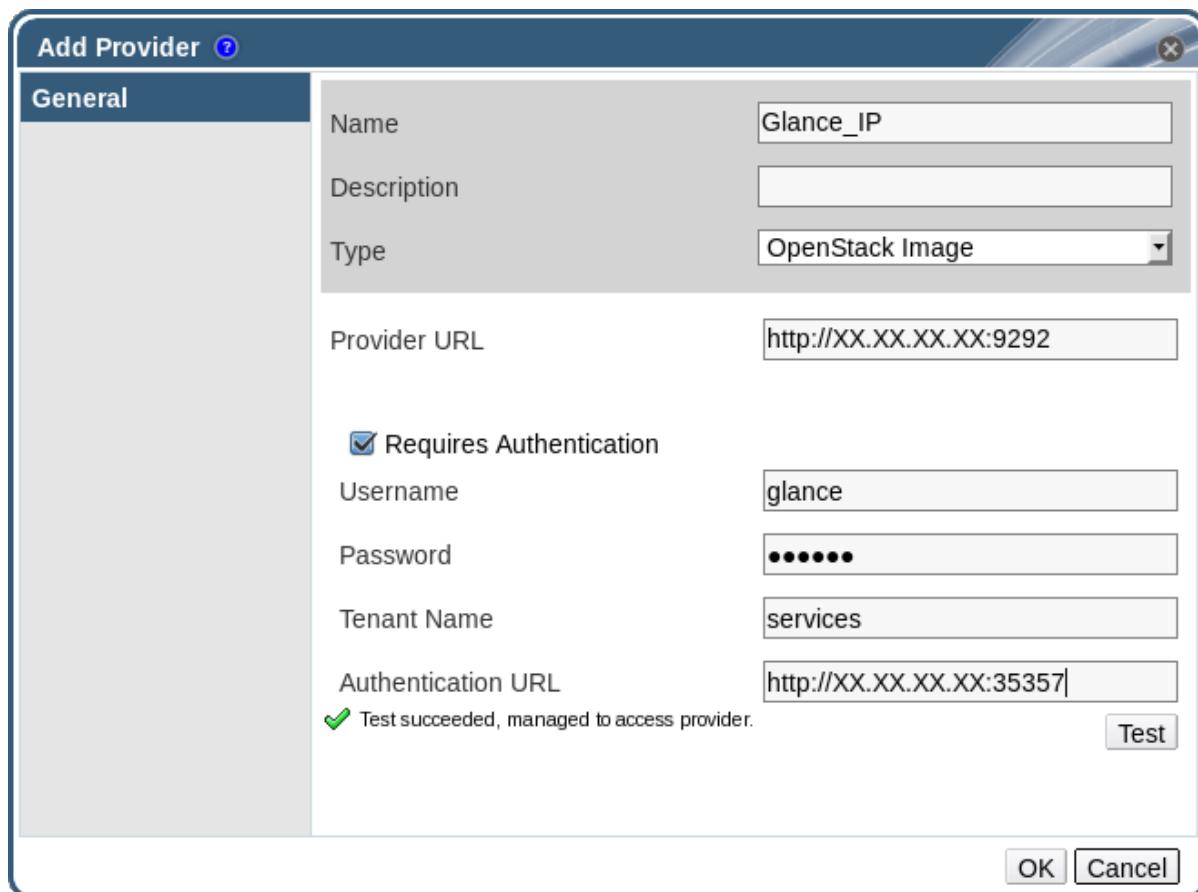
12.2.2. イメージ管理用の OpenStack Image (Glance) インスタンスの追加

Red Hat Virtualization Manager にイメージ管理用の OpenStack Image (Glance) インスタンスを追加します。

手順12.2 イメージ管理用の OpenStack Image (Glance) インスタンスの追加

1. ツリーペインで **External Providers** エントリーを選択します。
2. **Add** をクリックして **Add Provider** ウィンドウを開きます。

図12.2 Add Provider ウィンドウ



3. **Name** および **Description** を入力します。
4. タイプリストから **OpenStack Image** を選択します。
5. OpenStack Image インスタンスがインストールされているマシンの URL または完全修飾ドメイン名を **Provider URL** テキストフィールドに入力します。
6. 必要に応じて、**Requires Authentication** チェックボックスを選択し、OpenStack Image インスタンスの **ユーザー名**、**パスワード**、**テナント名**、および **認証 URL** を入力します。Keystone に登録した OpenStack Image ユーザーのユーザー名とパスワード、OpenStack Image インスタンスが所属するテナント、Keystone サーバーの URL とポートを使用する必要があります。
7. 認証情報をテストします。
 - a. **Test** をクリックして、提供された認証情報を使用して OpenStack Image インスタンスで正常に認証できるかどうかをテストします。
 - b. OpenStack Image インスタンスが SSL を使用している場合は、**Import provider certificates** ウィンドウが開きます。**OK** をクリックして、OpenStack Image インスタンスが提供する証明書をインポートします。



重要

Manager がインスタンスと通信できるようにするには、OpenStack Image インスタンスが提供する証明書をインポートする必要があります。

8. **OK** をクリックします。

OpenStack Image インスタンスを Red Hat Virtualization Manager に追加し、提供するイメージを操作できるようになりました。

12.2.3. ネットワークプロビジョニング用の OpenStack Networking (Neutron) インスタンスの追加

ネットワークプロビジョニング用の OpenStack Networking (Neutron) インスタンスを Red Hat Virtualization Manager に追加します。OpenStack Neutron REST API を実装する他のサードパーティーネットワークプロバイダーを追加するには、「[外部ネットワークプロバイダーの追加](#)」を参照してください。



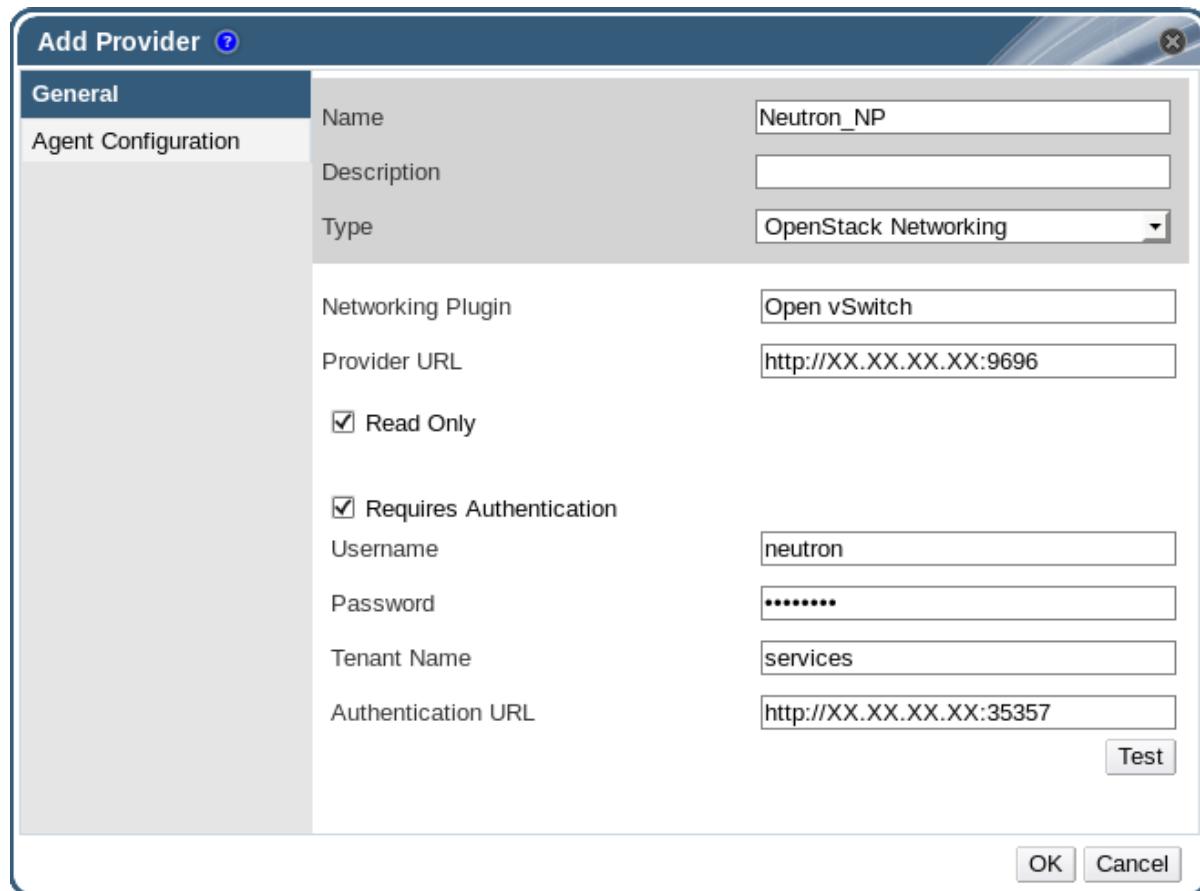
重要

Red Hat Virtualization は、外部ネットワークプロバイダーとして Red Hat OpenStack Platform 8、9、および 10 をサポートします。

手順12.3 ネットワークプロビジョニング用の OpenStack Networking (Neutron) インスタンスの追加

1. ツリーペインで **External Providers** エントリーを選択します。
2. **Add** をクリックして **Add Provider** ウィンドウを開きます。

図12.3 Add Provider ウィンドウ



3. **Name** および **Description** を入力します。
4. タイプリストから、**OpenStack Networking** を選択します。
5. **Networking Plugin** フィールドで **Open vSwitch** が選択されていることを確認します。

6. OpenStack Networking インスタンスがインストールされているマシンの URL または完全修飾ドメイン名を **Provider URL** テキストフィールドに入力し、その後にポート番号を入力します。デフォルトでは、**Read Only** チェックボックスが選択されます。これにより、ユーザーが OpenStack Networking インスタンスを変更できなくなります。



重要

セットアップが Red Hat でサポートされるようにするには、**Read Only** チェックボックスをオンのままにしておく必要があります。

7. 必要に応じて、**Requires Authentication** チェックボックスを選択し、OpenStack Networking インスタンスのユーザー名、パスワード、テナント名、および **認証 URL** を入力します。Keystone に登録されている OpenStack Networking ユーザーのユーザー名とパスワード、OpenStack Networking インスタンスが所属するテナント、および Keystone サーバーの URL とポートを使用する必要があります。
8. 認証情報をテストします。
 - a. **Test** をクリックして、提供された認証情報を使用して OpenStack Networking インスタンスで正常に認証できるかどうかをテストします。
 - b. OpenStack Networking インスタンスが SSL を使用している場合は、**Import provider certificates** ウィンドウが開きます。**OK** をクリックして、OpenStack Networking インスタンスが提供する証明書をインポートし、Manager がインスタンスと通信できるようにします。

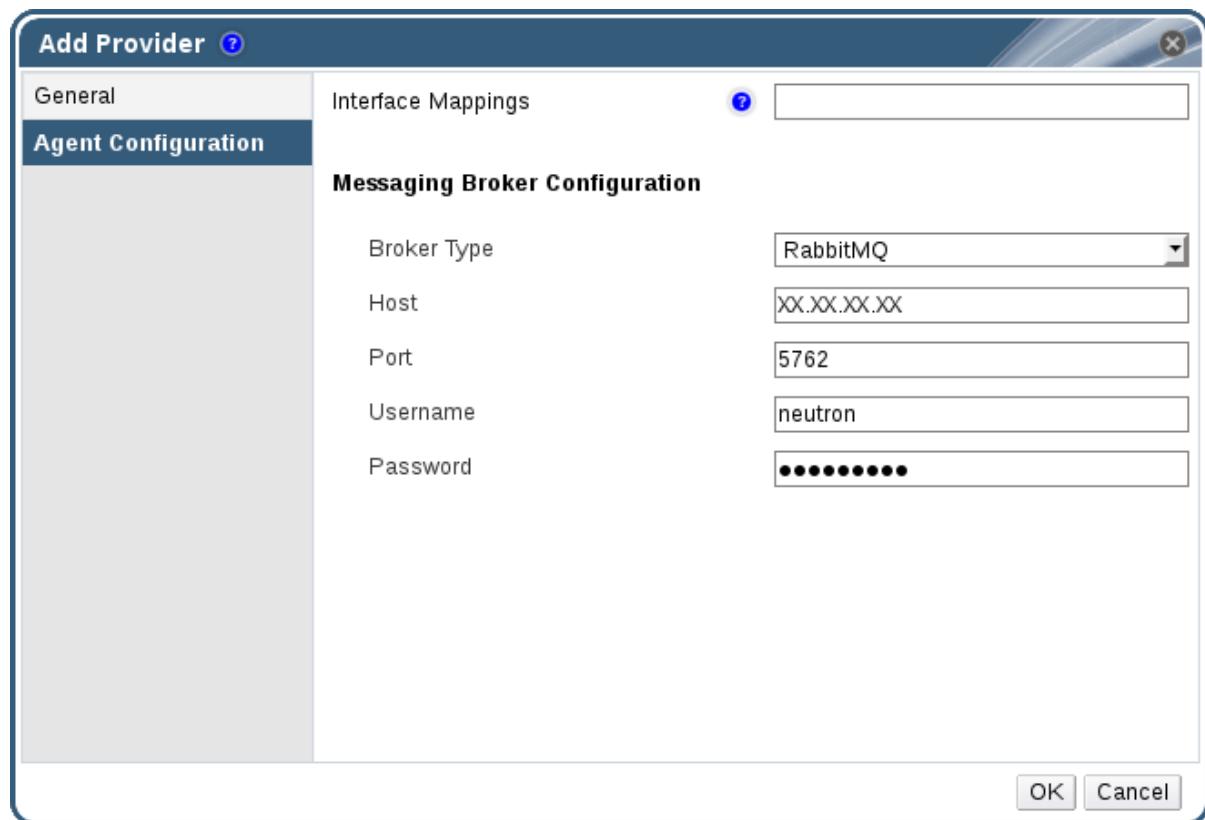


警告

以下の手順は、テクノロジープレビューとしてのみ提供されます。Red Hat Virtualization がサポートするのは、事前設定された Neutron ホストだけです。

9. **Agent Configuration** タブをクリックします。

図12.4 エージェント設定タブ



10. **Interface Mappings** フィールドに、Open vSwitch エージェントのインターフェイスマッピングのコンマ区切りリストを入力します。
11. **Broker Type** 一覧から OpenStack Networking インスタンスが使用するメッセージブローカータイプを選択します。
12. メッセージブローカーがホストされるホストの URL または完全修飾ドメイン名を入力します。
13. メッセージブローカーに接続する **Port** を入力します。メッセージブローカーが SSL を使用するように設定されていない場合は、このポート番号は 5762 で、SSL を使用するように設定されている場合は 5761 となります。
14. メッセージブローカーインスタンスに登録されている OpenStack Networking ユーザーのユーザー名およびパスワードを入力します。
15. **OK** をクリックします。

OpenStack Networking インスタンスが Red Hat Virtualization Manager に追加されました。提供されているネットワークを使用する前に、ネットワークを Manager にインポートしてください。「[外部プロバイダーからのネットワークのインポート](#)」を参照してください。

12.2.4. ストレージ管理用の OpenStack Volume (Cinder) インスタンスの追加



重要

ストレージ管理に OpenStack Volume (Cinder) インスタンスを使用することはテクノロジープレビュー機能です。テクノロジープレビュー機能は、Red Hat の実稼働環境でのサービスレベルアグリーメント (SLA) ではサポートされていないため、Red Hat では実稼働環境での使用を推奨していません。テクノロジープレビューの機能は、最新の製品機能をいち早く提供して、開発段階で機能のテストを行いフィードバックを提供していくことを目的としています。

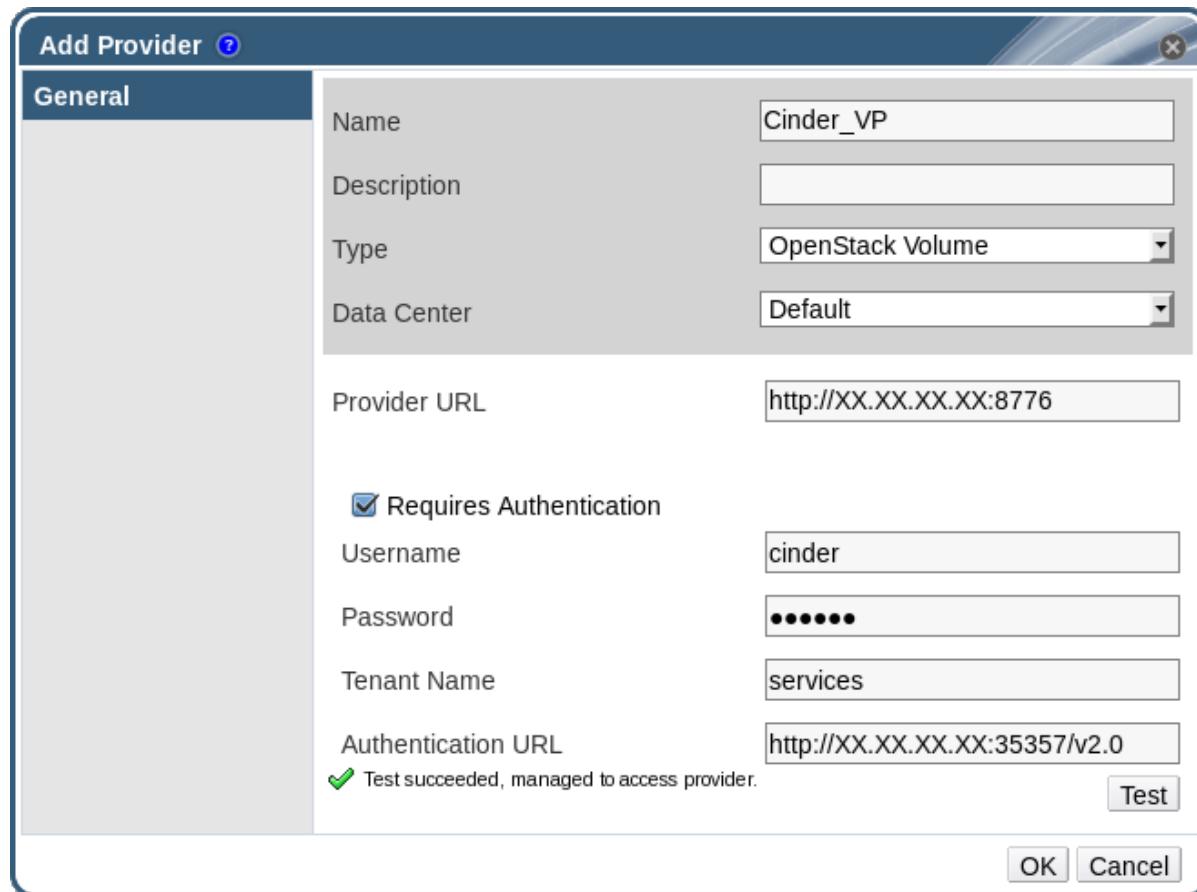
Red Hat のテクノロジープレビュー機能のサポートについての詳細は、[を参照してください](https://access.redhat.com/support/offering/techpreview/) <https://access.redhat.com/support/offering/techpreview/>。

Red Hat Virtualization Manager にストレージ管理用の OpenStack Volume (Cinder) インスタンスを追加します。OpenStack Cinder ボリュームは Ceph Storage によりプロビジョニングされます。

手順12.4 ストレージ管理用の OpenStack Volume (Cinder) インスタンスの追加

1. ツリーペインで **External Providers** エントリーを選択します。
2. **Add** をクリックして **Add Provider** ウィンドウを開きます。

図12.5 Add Provider ウィンドウ



3. **Name** および **Description** を入力します。
4. タイプの一覧から **OpenStack Volume** を選択します。
5. OpenStack Volume ストレージボリュームを接続するデータセンターを選択します。
6. OpenStack Volume インスタンスがインストールされているマシンの URL または完全修飾ドメイン名を **Provider URL** テキストフィールドに入力します。

7. 必要に応じて、**Requires Authentication** チェックボックスを選択し、OpenStack Volume インスタンスのユーザー名、パスワード、テナント名、および認証 URL を入力します。Keystone に登録されている OpenStack Volume ユーザーのユーザー名とパスワード、OpenStack Volume インスタンスが所属するテナント、Keystone サーバーの URL、ポート、および API バージョンを使用する必要があります。
8. **Test** をクリックして、提供された認証情報を使用して OpenStack Volume インスタンスで正常に認証できるかどうかをテストします。
9. **OK** をクリックします。
10. クライアント Ceph 認証(cephx)が有効になっている場合は、以下の手順も完了する必要があります。cephx プロトコルはデフォルトで有効になっています。
 - a. Ceph サーバーで、**ceph auth get-or-create** コマンドを使用して **client.cinder** ユーザーの新しい秘密鍵を作成します。cephx に関する詳細は、[Cephx Config Reference](#) を参照してください。新規ユーザー のキー 作成に関する詳細は、Cephx 設定リファレンス を参照してください。**client.cinder** ユーザーにキーがすでに存在する場合は、同じコマンドを使用してキーを取得します。
 - b. 管理ポータルで、**Providers** 一覧から新たに作成された Cinder 外部プロバイダーを選択します。
 - c. **Authentication Keys** サブタブをクリックします。
 - d. **New** をクリックします。
 - e. **Value** フィールドに秘密鍵を入力します。
 - f. 自動生成される **UUID** をコピーするか、テキストフィールドに既存の UUID を入力します。
 - g. Cinder サーバーで、前の手順の UUID と **cinder** ユーザーを **/etc/cinder/cinder.conf** に追加します。

```
rbd_secret_uuid = UUID
rbd_user = cinder
```

OpenStack Volume インスタンスを Red Hat Virtualization Manager に追加し、それが提供するストレージボリュームと連携できる。OpenStack ボリューム(Cinder)ディスクの作成に関する詳細は、「[Floating 仮想ディスクの作成](#)」を参照してください。

12.2.5. 仮想マシンプロバイダーとしての VMware インスタンスの追加

VMware vCenter インスタンスを追加して、仮想マシンを VMware から Red Hat Virtualization Manager にインポートします。

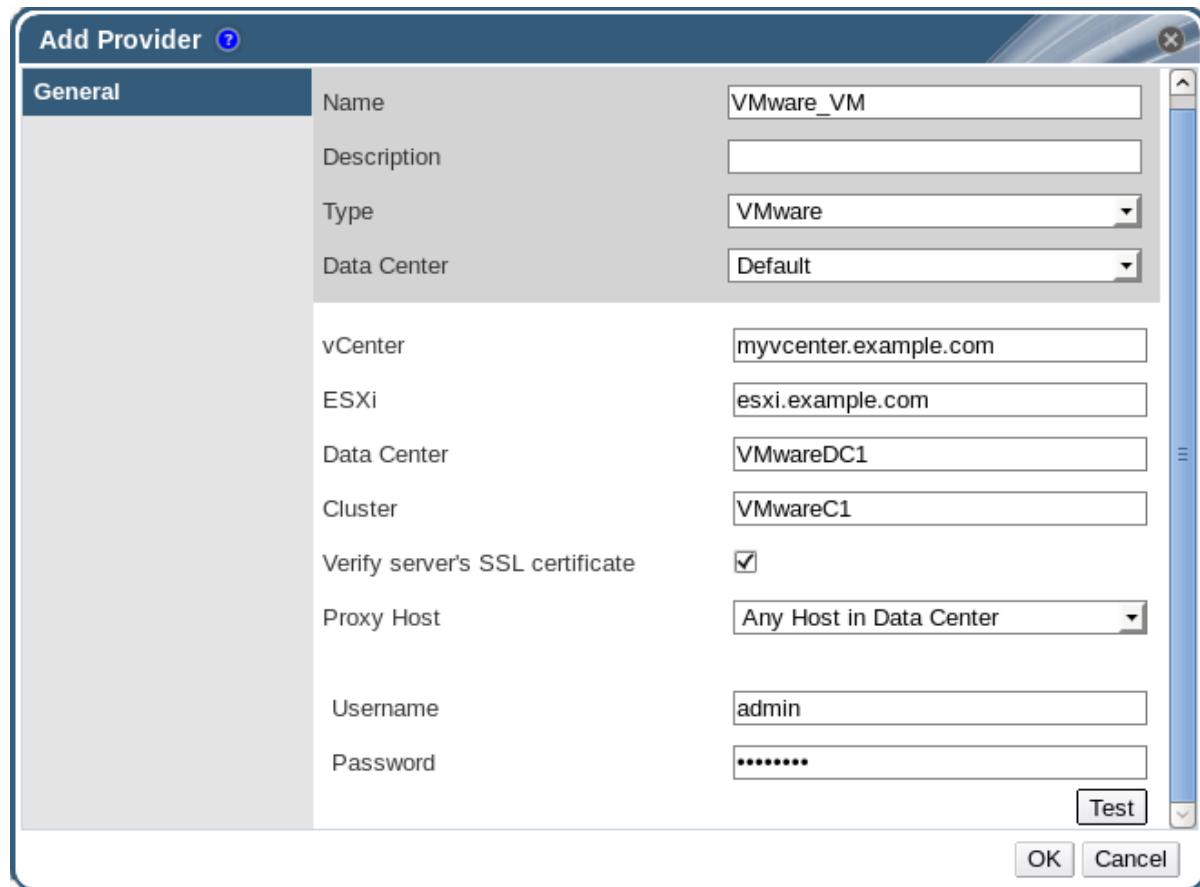
Red Hat Virtualization は、V2V を使用して、VMware 仮想マシンをインポートする前に正しい形式に変換します。virt-v2v パッケージが少なくとも 1 つのホストにインストールされている。virt-v2v パッケージは、Red Hat Virtualization Host (RHVH) ではデフォルトで利用できますが、Red Hat Enterprise Linux ホストにインストールする必要があります。Red Hat Enterprise Linux ホストは、Red Hat Enterprise Linux 7.2 以降である必要があります。

手順12.5 仮想マシンプロバイダーとしての VMware vCenter インスタンスの追加

1. ツリーペインで **External Providers** エントリーを選択します。

2. **Add** をクリックして **Add Provider** ウィンドウを開きます。

図12.6 Add Provider ウィンドウ



3. **Name** および **Description** を入力します。
4. タイプの一覧から **VMware** を選択します。
5. VMware 仮想マシンをインポートする **Data Center** を選択するか、**Any Data Center** を選択して、(Virtual Machines タブの Import 機能を使用して)個々のインポート操作中に宛先データセンターを指定します。
6. **vCenter** フィールドに VMware vCenter インスタンスの IP アドレスまたは完全修飾ドメイン名を入力します。
7. 仮想マシンのインポート元となるホストの IP アドレスまたは完全修飾ドメイン名を **ESXi** フィールドに入力します。
8. 指定した ESXi ホストが存在するデータセンターの名前を **Data Center** フィールドに入力します。
9. ESXi ホストと Manager との間で SSL 証明書を交換した場合は、**Verify server's SSL certificate** をチェックしたままにし、ESXi ホストの証明書を確認します。そうでない場合は、オプションの選択を解除します。
10. 仮想マシンのインポート操作中に **Proxy Host** として機能するように、virt-v2v がインストールされている、選択したデータセンター内のホストを選択します。このホストは、VMware vCenter 外部プロバイダーのネットワークに接続できる必要があります。上記の **Any Data Center** を選択した場合は、ここでホストを選択することはできませんが、代わりに、個別のインポート操作時にホストを指定できます(Virtual Machines タブの Import 機能を使用)。

11. VMware vCenter インスタンスの **Username** および **Password** を入力します。ユーザーは、仮想マシンが置かれている VMware データセンターおよび ESXi ホストにアクセスできる必要があります。
12. 認証情報をテストします。
 - a. **Test** をクリックして、提供された認証情報を使用して VMware vCenter インスタンスで正常に認証できるかどうかをテストします。
 - b. VMware vCenter インスタンスが SSL を使用する場合は、**Import provider certificates** ウィンドウが開きます。**OK** をクリックして、VMware vCenter インスタンスが提供する証明書をインポートします。



重要

Manager がインスタンスと通信できるようにするには、VMware vCenter インスタンスが提供する証明書をインポートする必要があります。

13. **OK** をクリックします。

VMware vCenter インスタンスを Red Hat Virtualization Manager に追加し、それが提供する仮想マシンをインポートできます。詳細は、『Virtual Machine Management Guide』の [Importing a Virtual Machine from a VMware Provider](#) を参照してください。

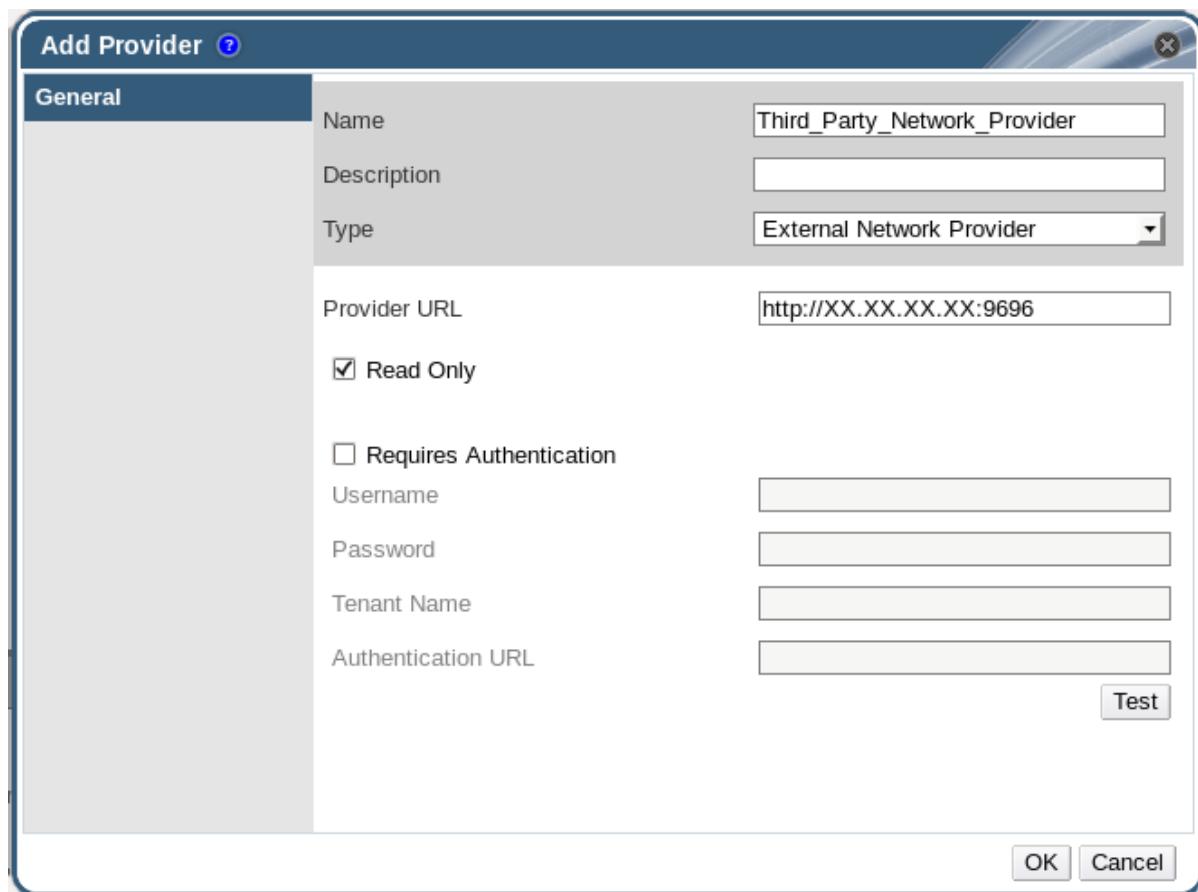
12.2.6. 外部ネットワークプロバイダーの追加

OpenStack Neutron REST API を実装する任意のネットワークプロバイダーを Red Hat Virtualization に追加できます。仮想インターフェイスドライバーは、外部ネットワークプロバイダーの実装者が提供する必要があります。ネットワークプロバイダーおよび仮想インターフェイスドライバーの参照実装は、および https://github.com/mmirecki/ovirt-provider-mock/blob/master/docs/driver_instalation から入手 <https://github.com/mmirecki/ovirt-provider-mock> できます。

手順12.6 ネットワークプロビジョニング用の外部ネットワークプロバイダーの追加

1. ツリーペインで **External Providers** エントリーを選択します。
2. **Add** をクリックします。

図12.7 Add Provider ウィンドウ



3. **Name** および **Description** を入力します。
4. タイプリストから 外部ネットワークプロバイダー を 選択します。
5. 外部ネットワークプロバイダーがインストールされているマシンの URL または完全修飾ドメイン名を **Provider URL** テキストフィールドに入力し、その後にポート番号を入力します。デフォルトでは、**Read-Only** チェックボックスがオンになっています。これにより、ユーザーは外部ネットワークプロバイダーを変更できなくなります。



重要

セットアップが Red Hat でサポートされるようにするには、**Read-Only** チェックボックスをオンのままにしておく必要があります。

6. 必要に応じて、**Requires Authentication** チェックボックスを選択し、外部ネットワークプロバイダーの **Username**、**Password**、**Tenant Name**、および **Authentication URL** を入力します。
7. 認証情報をテストします。
 - a. **Test** をクリックして、提供された認証情報を使用して外部ネットワークプロバイダーで正常に認証できるかどうかをテストします。
 - b. 外部ネットワークプロバイダーが SSL を使用している場合は、**Import provider certificates** ウィンドウが開きます。**OK** をクリックして外部ネットワークプロバイダーが提供する証明書をインポートし、Manager がインスタンスと通信できるようにします。

Red Hat Virtualization Manager に外部ネットワークプロバイダーを追加している。提供するネットワー

クを使用する前に、ホストに仮想インターフェイスドライバーをインストールし、ネットワークをインポートする必要があります。ネットワークをインポートするには、「[外部プロバイダーからのネットワークのインポート](#)」を参照してください。

12.2.7. プロバイダーの一般設定の説明を追加

Add Provider ウィンドウの **General** タブでは、外部プロバイダーのコアの詳細を登録できます。

表12.1 プロバイダーの追加: 一般設定

設定	説明
Name	Manager でプロバイダーを表す名前。
説明	プロバイダーのプレーンテキストで人間が読める形式の説明。
タイプ	<p>外部プロバイダーのタイプ。この設定を変更すると、プロバイダーの設定に使用できるフィールドが変更されます。</p> <p>Foreman/Satellite</p> <ul style="list-style-type: none"> Provider URL: Satellite インスタンスをホストするマシンの URL または完全修飾ドメイン名。URL または完全修飾ドメイン名の末尾にポート番号を追加する必要はありません。 Requires Authentication: プロバイダーに認証が必要であるかどうかを指定できます。Foreman/Satellite が選択されている場合、認証は必須です。 ユーザー名: Satellite インスタンスに接続するためのユーザー名このユーザー名は、Satellite インスタンスのプロビジョニングポータルへのログインに使用されるユーザー名でなければなりません。デフォルトでは、このユーザー名は admin です。 パスワード: 上記のユーザー名が認証されるパスワード。このパスワードは、Satellite インスタンスのプロビジョニングポータルへのログインに使用するパスワードでなければなりません。 <p>OpenStack Image</p> <ul style="list-style-type: none"> Provider URL: OpenStack Image サービスがホストされるマシンの URL または完全修飾ドメイン名。OpenStack Image Service のポート番号を URL または完全修飾ドメイン名の末尾に追加する必要があります。デフォルトでは、このポート番号は 9292 です。 Requires Authentication: OpenStack Image サービスにアクセスするために認証が必要であるかどうかを指定できます。

設定	説明
	<ul style="list-style-type: none"> ユーザー名: OpenStack Image サービスに接続するためのユーザー名このユーザー名は、OpenStack Image サービスが所属する Keystone インスタンスに登録されている OpenStack Image サービスのユーザー名でなければなりません。デフォルトでは、このユーザー名は glance です。 パスワード: 上記のユーザー名が認証されるパスワード。このパスワードは、OpenStack Image サービスが所属する Keystone インスタンスに登録されている OpenStack Image サービスのパスワードでなければなりません。 テナント名: OpenStack Image サービスが所属する OpenStack テナントの名前。デフォルトでは、これは サービス です。 認証URL: OpenStack Image サービスが認証する Keystone サーバーの URL およびポート。 <h3>OpenStack ネットワーキング</h3> <ul style="list-style-type: none"> Networking プラグイン: OpenStack Networking サーバーに接続するためのネットワークプラグイン。Open vSwitch は唯一のオプションで、デフォルトで選択されています。 Provider URL: OpenStack Networking インスタンスがホストされるマシンの URL または完全修飾ドメイン名。OpenStack Networking インスタンスのポート番号を、URL または完全修飾ドメイン名の末尾に追加する必要があります。デフォルトでは、このポート番号は 9696 です。 Read Only: OpenStack Networking インスタンスを管理ポータルから変更できるかどうかを指定できます。 Requires Authentication: OpenStack Networking サービスへのアクセスに認証が必要であるかどうかを指定できます。 ユーザー名: OpenStack Networking インスタンスに接続するためのユーザー名。このユーザー名は、OpenStack Networking インスタンスが所属する Keystone インスタンスに登録されている OpenStack Networking のユーザー名でなければなりません。デフォルトでは、このユーザー名は neutron です。 パスワード: 上記のユーザー名が認証されるパスワード。このパスワードは、OpenStack Networking インスタンスが所属する Keystone インスタンスに登録されている OpenStack Networking のパスワードでなければなりません。 テナント名: OpenStack Networking インスタンスが所属する OpenStack テナントの

設定	説明
	名前。デフォルトでは、これは サービス です。
<ul style="list-style-type: none"> ● 認証 URL: OpenStack Networking インスタンスが認証する Keystone サーバーの URL およびポート。 	
OpenStack ボリューム	
<ul style="list-style-type: none"> ● データセンター: OpenStack ボリュームのストレージボリュームが接続するデータセンター。 ● Provider URL: OpenStack Volume インスタンスがホストされるマシンの URL または完全修飾ドメイン名。OpenStack Volume インスタンスのポート番号を、URL または完全修飾ドメイン名の末尾に追加する必要があります。デフォルトでは、このポート番号は 8776 です。 ● Requires Authentication: OpenStack ボリュームサービスへのアクセスに認証が必要であるかどうかを指定できます。 ● ユーザー名: OpenStack Volume インスタンスに接続するためのユーザー名。このユーザー名は、OpenStack Volume インスタンスが所属する Keystone インスタンスに登録されている OpenStack Volume のユーザー名でなければなりません。デフォルトでは、このユーザー名は cinder です。 ● パスワード: 上記のユーザー名が認証されるパスワード。このパスワードは、OpenStack Volume インスタンスが所属する Keystone インスタンスに登録されている OpenStack Volume のパスワードでなければなりません。 ● テナント名: OpenStack Volume インスタンスが所属する OpenStack テナントの名前。デフォルトでは、これは サービス です。 ● 認証 URL: OpenStack ボリュームインスタンスが認証する Keystone サーバーの URL およびポート。 	
VMware	
<ul style="list-style-type: none"> ● Data Center: VMware 仮想マシンがインポートされるデータセンターを指定するか、Any Data Center を選択して、(Virtual Machines タブの Import 機能を使用して)個々のインポート操作中に宛先データセンターを指定します。 ● vCenter: VMware vCenter インスタンスの IP アドレスまたは完全修飾ドメイン名。 ● ESXi: 仮想マシンのインポート元となるホストの IP アドレスまたは完全修飾ドメイン名。 	

設定	説明
	<ul style="list-style-type: none"> ● Data Center: 指定された ESXi ホストが存在するデータセンターの名前。 ● クラスター: 指定された ESXi ホストが存在するクラスターの名前。 ● Verify server's SSL certificate: 接続時に ESXi ホストの証明書を検証するかどうかを指定します。 ● Proxy Host: 仮想マシンのインポート操作中にホストとして機能するように、選択したデータセンターで virt-v2v がインストールされているホストを選択します。このホストは、VMware vCenter 外部プロバイダーのネットワークに接続できる必要があります。Any Data Center を選択した場合は、ここでホストを選択することはできませんが、代わりに、個別のインポート操作時にホストを指定できます(Virtual Machines タブの Import 機能を使用)。 ● ユーザー名: VMware vCenter インスタンスに接続するためのユーザー名。ユーザーは、仮想マシンが置かれている VMware データセンターおよび ESXi ホストにアクセスできる必要があります。 ● パスワード: 上記のユーザー名が認証されるパスワード。 <p>外部ネットワークプロバイダー</p> <ul style="list-style-type: none"> ● Provider URL: 外部ネットワークプロバイダーがホストされるマシンの URL または完全修飾ドメイン名。外部ネットワークプロバイダーのポート番号を URL または完全修飾ドメイン名の末尾に追加する必要があります。デフォルトでは、このポート番号は 9696 です。 ● Read Only: 管理ポータルから外部ネットワークプロバイダーを変更できるかどうかを指定できます。 ● Requires Authentication: 外部ネットワークプロバイダーにアクセスするために認証が必要であるかどうかを指定できます。 ● ユーザー名: 外部ネットワークプロバイダーに接続するためのユーザー名。 ● パスワード: 上記のユーザー名が認証されるパスワード。 ● 認証 URL: 外部ネットワークプロバイダーが認証する認証サーバーの URL およびポート。
Test	ユーザーが指定の認証情報をテストすることを許可します。このボタンは、すべてのプロバイダータイプで使用できます。

12.2.8. プロバイダーエージェントの設定設定に関する説明の追加

Add Provider ウィンドウの **Agent Configuration** タブを使用すると、ユーザーはネットワークプラグインの詳細を登録できます。このタブは、**OpenStack Networking** プロバイダータイプでのみ使用できます。

表12.2 プロバイダーの追加: 一般設定

設定	説明
インターフェイスマッピング	ラベル:インターフェイス形式のマッピングのコンマ区切りリスト。
プローカータイプ	OpenStack Networking インスタンスが使用するメッセージプローカータイプ。 RabbitMQ または Qpid を選択します。
ホスト	メッセージプローカーがインストールされているマシンの URL または完全修飾ドメイン名。
ポート	上記のホストとの接続を確立するためのリモートポート。デフォルトでは、SSL がホストで有効でない場合は、このポートは 5762 に、SSL が有効な場合は 5761 になります。
Username	上記のメッセージプローカーを使用して OpenStack Networking インスタンスを認証するためのユーザー名。デフォルトでは、このユーザー名は neutron です。
Password	上記のユーザー名が認証されるパスワード。

12.3. 外部プロバイダーの編集

12.3.1. 外部プロバイダーの編集

手順12.7 外部プロバイダーの編集

- ツリーペインで **External Providers** エントリーを選択します。
- 編集する外部プロバイダーを選択します。
- Edit** ボタンをクリックして、**Edit Provider** ウィンドウを開きます。
- プロバイダーの現在の値を推奨値に変更します。
- OK** をクリックします。

12.4. 外部プロバイダーの削除

12.4.1. 外部プロバイダーの削除

手順12.8 外部プロバイダーの削除

1. ツリーペインで **External Providers** エントリーを選択します。
2. 削除する外部プロバイダーを選択します。
3. **削除** をクリックします。
4. **Remove Provider (s)** ウィンドウで **OK** をクリックして、このプロバイダーの削除を確認します。

パート III. 環境の管理

第13章 バックアップおよび移行

13.1. RED HAT VIRTUALIZATION MANAGER のバックアップおよび復元

13.1.1. Red Hat Virtualization Manager のバックアップ - 概要

engine-backup ツールを使用して、Red Hat Virtualization Manager の定期的なバックアップを作成します。このツールは、エンジンデータベースと設定ファイルを単一のファイルにバックアップし、**ovirt-engine** サービスを中断せずに実行できます。

13.1.2. engine-backup コマンドの構文

engine-backup コマンドは、次の 2 つの基本モードのいずれかで機能します。

```
# engine-backup --mode=backup
```

```
# engine-backup --mode=restore
```

これらの 2 つのモードは、バックアップの範囲とエンジンデータベースのさまざまな認証情報を指定できる一連のパラメーターによってさらに拡張されます。パラメーターとその機能の完全なリストについては、**engine-backup --help** を実行します。

Basic Options

--mode

コマンドがバックアップ操作を実行するか、復元操作を実行するかを指定します。**backup** と **restore** の 2 つのオプションを使用できます。これは必須パラメーターです。

--file

バックアップモードでバックアップを取得するファイルのパスおよび名前、ならびに復元モードでバックアップデータを読み取るファイルのパスおよび名前を指定します。これは、バックアップモードと復元モードの両方で必須のパラメーターです。

--log

バックアップまたは復元操作のログが書き込まれるファイルのパスおよび名前を指定します。このパラメーターは、バックアップモードと復元モードの両方で必要です。

--scope

バックアップまたは復元操作の範囲を指定します。4 つのオプションがあります。**all** は、すべてのデータベースおよび設定データをバックアップまたは復元します。**files** は、システム上のファイルのみをバックアップまたは復元します。**db** は、Manager データベースのみをバックアップまたは復元します。**dwhdb** は、Data Warehouse データベースのみをバックアップまたは復元します。デフォルトのスコープは **all** です。

--scope パラメーターは、同じ **engine-backup** コマンドで複数回指定できます。

Manager Database Options

以下のオプションは、**restore** モードで **engine-backup** コマンドを使用する場合にのみ利用できます。以下のオプション構文は、Manager データベースの復元に適用されます。Data Warehouse データベー

スを復元するための同じオプションがあります。Data Warehouse オプションの構文は **engine-backup --help** を参照してください。

--provision-db

復元先の Manager データベースバックアップ用の PostgreSQL データベースを作成します。これは、PostgreSQL データベースがまだ設定されていないリモートホストまたは新規インストールでバックアップを復元する場合に必要なパラメーターです。

--change-db-credentials

バックアップ自体に保存されている認証情報以外の認証情報を使用して、Manager データベースを復元するための代替認証情報を指定できます。このパラメーターで必要な追加パラメーターは、**engine-backup --help** を参照してください。

--restore-permissions または **--no-restore-permissions**

データベースユーザーの権限を復元します（または復元しません）。バックアップを復元するときは、これらのパラメーターの1つが必要です。



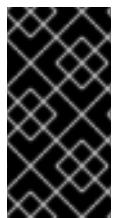
注記

バックアップに追加のデータベースユーザーの許可が含まれている場合、**--restore-permissions** および **--provision-db**（または **--provision-dwh-db**）オプションを使用してバックアップを復元すると、無作為にパスワードが設定された追加のユーザーが作成されます。追加のユーザーが復元したシステムにアクセスする必要がある場合は、これらのパスワードを手動で変更する必要があります。を参照してください <https://access.redhat.com/articles/2686731>。

13.1.3. engine-backup コマンドを使用したバックアップの作成

Red Hat Virtualization Manager は、Manager がアクティブなときに **engine-backup** コマンドを使用してバックアップできます。以下のオプションのいずれかを **--scope** に追加し、実行するバックアップを指定します。

- **all**: Manager 上のすべてのデータベースおよび設定ファイルの完全バックアップ
- **files**: システム上のファイルのみのバックアップ
- **db**: Manager データベースのみのバックアップ
- **dwhdb**: データウェアハウスデータベースのみのバックアップ



重要

データベースを Red Hat Virtualization Manager の新規インストールに復元するには、データベースのバックアップだけでは不十分です。Manager では設定ファイルへのアクセスも必要です。デフォルト以外のスコープを指定するバックアップ。**all** は **files** スコープまたはファイルシステムのバックアップと一緒に指定する必要があります。

手順13.1 engine-backup コマンドの使用例

1. Red Hat Virtualization Manager を実行しているマシンにログインします。
2. バックアップを作成します。

例13.1 完全バックアップの作成

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

例13.2 Manager データベースのバックアップの作成

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

db オプションは、Data Warehouse データベースをバックアップする **dwhdb** に置き換えます。

バックアップを含む **tar** ファイルは、指定したパスとファイル名を使用して作成されます。

バックアップを含む **tar** ファイルを使用して、環境を復元できるようになりました。

13.1.4. **engine-backup** コマンドを使用したバックアップの復元

engine-backup コマンドを使用してバックアップを復元するには、復元先によっては、バックアップを作成するよりも多くの手順が必要です。たとえば、**engine-backup** コマンドを使用して、Red Hat Virtualization の既存インストールに加えて、ローカルまたはリモートのデータベースを使用して、Red Hat Virtualization の新規インストールにバックアップを復元できます。



重要

バックアップは、バックアップと同じメジャーリリースの環境にのみ復元できます。たとえば、Red Hat Virtualization バージョン 4.0 環境のバックアップは、別の Red Hat Virtualization バージョン 4.0 環境にのみ復元できます。バックアップファイルに含まれる Red Hat Virtualization のバージョンを表示するには、バックアップファイルを展開し、展開されたファイルのルートディレクトリーにある **version** ファイルの値を読み取ります。

13.1.5. バックアップを新規インストールに復元する

engine-backup コマンドを使用すると、Red Hat Virtualization Manager の新規インストールにバックアップを復元できます。以下の手順は、ベースオペレーティングシステムがインストールされており、Red Hat Virtualization Manager に必要なパッケージがインストールされていても、**engine-setup** コマンドがまだ実行されていないマシンで実行する必要があります。この手順は、バックアップを復元するマシンから1つまたは複数のバックアップファイルにアクセスできることを前提としています。

手順13.2 バックアップを新規インストールに復元する

- Manager マシンにログインします。エンジンデータベースをリモートホストに復元する場合は、そのホストにログオンして、関連するアクションを実行する必要があります。同様に、Data Warehouse をリモートホストにも復元する場合は、そのホストにログオンして、関連するアクションを実行する必要があります。
- 完全バックアップまたはデータベースのみのバックアップを復元します。
 - 完全バックアップを復元します。

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db --
restore-permissions
```

完全バックアップの一部として Data Warehouse も復元される場合は、追加のデータベースをプロビジョニングします。

```
engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db --
provision-dwh-db --restore-permissions
```

- 設定ファイルとデータベースバックアップを復元して、データベースのみのバックアップを復元します。

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

上記の例では、Manager データベースのバックアップを復元します。

```
# engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --
log=log_file_name --provision-dwh-db --restore-permissions
```

上記の例では、Data Warehouse データベースのバックアップを復元します。

成功すると、次の出力が表示されます。

```
You should now run engine-setup.  
Done.
```

3. 次のコマンドを実行し、プロンプトに従って復元された Manager を設定します。

```
# engine-setup
```

Red Hat Virtualization Manager は、バックアップに保存されているバージョンに復元されました。新しい Red Hat Virtualization システムの完全修飾ドメイン名を変更するには、「[oVirt エンジンの名前変更ツール](#)」を参照してください。

13.1.6. バックアップを復元して既存のインストールを上書き

engine-backup コマンドは、Red Hat Virtualization Manager がすでにインストールおよび設定されているマシンにバックアップを復元できます。これは、インストールのバックアップを作成し、そのインストールの変更を実行してから、バックアップからインストールを復元する場合に便利です。



重要

バックアップを復元して既存のインストールを上書きする場合は、**engine-backup** コマンドを使用する前に、**engine-cleanup** コマンドを実行して既存のインストールをクリーンアップする必要があります。**engine-cleanup** コマンドはエンジンデータベースのみを消去し、データベースをドロップしたり、そのデータベースを所有するユーザーを削除したりしないため、ユーザーとデータベースがすでに存在しているため、新しいデータベースを作成したり、データベースの認証情報を指定する必要はありません。

手順13.3 バックアップを復元して既存のインストールを上書き

- Red Hat Virtualization Manager マシンにログインします。
- 設定ファイルを削除し、Manager に関連付けられているデータベースをクリーンアップします。

```
# engine-cleanup
```

- 完全バックアップまたはデータベースのみのバックアップを復元します。

- 完全バックアップを復元します。

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --restore-permissions
```

- 設定ファイルおよびデータベースバックアップを復元して、データベースのみのバックアップを復元します。

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

上記の例では、Manager データベースのバックアップを復元します。必要に応じて、Data Warehouse データベースも復元します。

```
# engine-backup --mode=restore --scope=dwhdb --file=file_name --log=log_file_name --restore-permissions
```

成功すると、次の出力が表示されます。

```
You should now run engine-setup.  
Done.
```

- 次のコマンドを実行し、プロンプトに従ってファイアウォールを再設定し、**ovirt-engine** サービスが正しく設定されていることを確認します。

```
# engine-setup
```

13.1.7. 異なる認証情報を使用したバックアップの復元

engine-backup コマンドは、Red Hat Virtualization Manager がすでにインストールおよび設定されているマシンにバックアップを復元できますが、バックアップ内のデータベースの認証情報は、バックアップを復元するマシンのデータベースの認証情報とは異なります。これは、インストールのバックアップを取り、バックアップから別のシステムにインストールを復元する場合に役立ちます。



重要

バックアップを復元して既存のインストールを上書きする場合は、**engine-backup** コマンドを使用する前に、**engine-cleanup** コマンドを実行して既存のインストールをクリーンアップする必要があります。**engine-cleanup** コマンドはエンジンデータベースのみを消去し、データベースをドロップしたり、そのデータベースを所有するユーザーを削除したりしないため、ユーザーとデータベースがすでに存在しているため、新しいデータベースを作成したり、データベースの認証情報を指定する必要はありません。ただし、エンジンデータベースの所有者の認証情報がわからない場合は、バックアップを復元する前に認証情報を変更する必要があります。

手順13.4 異なる認証情報を使用したバックアップの復元

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. 以下のコマンドを実行し、プロンプトに従って Manager に関連付けられたデータベースの設定ファイルを削除し、クリーンアップします。

```
# engine-cleanup
```

3. engine データベースの所有者のパスワードが不明な場合は、そのユーザーのパスワードを変更します。

 1. postgresql コマンドラインを入力します。

```
# su postgres
$ psql
```

2. engine データベースを所有するユーザーのパスワードを変更します。

```
postgres=# alter role user_name encrypted password 'new_password';
```

必要に応じて、**ovirt_engine_dwh** データベースを所有するユーザーに対してこれを繰り返します。

4. **--change-db-credentials** パラメーターを使用して完全バックアップまたはデータベースのみのバックアップを復元し、新しいデータベースの認証情報を渡します。Manager にローカルなデータベースの *database_location* は **localhost** です。



注記

以下の例では、パスワードを指定せずにデータベースごとに **--password** オプションを使用します。これにより、各データベースのパスワードの入力が求められます。コマンド自体でこれらのオプションにパスワードを指定できますが、パスワードはシェル履歴に保存されるため、この方法は推奨されません。または、各データベースに **--passfile=password_file** オプションを使用して、対話式プロンプトなしに、パスワードを **engine-backup** ツールに安全に渡すことができます。

- 完全バックアップを復元します。

```
# 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
```

Data Warehouse も完全バックアップの一部として復元される場合は、追加のデータベースの改訂された認証情報を含めます。

```
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
```

- 設定ファイルおよびデータベースバックアップを復元して、データベースのみのバックアップを復元します。

```
# 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
```

上記の例では、Manager データベースのバックアップを復元します。

```
# 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
```

上記の例では、Data Warehouse データベースのバックアップを復元します。

成功すると、次の出力が表示されます。

```
You should now run engine-setup.  
Done.
```

5. 次のコマンドを実行し、プロンプトに従ってファイアウォールを再設定し、**ovirt-engine** サービスが正しく設定されていることを確認します。

```
# engine-setup
```

13.1.8. エンジンデータベースのリモートサーバーデータベースへの移行

Red Hat Virtualization Manager の初期設定後に、**engine** データベースをリモートのデータベースサーバーに移行できます。**engine-backup** を使用してデータベースのバックアップを作成し、新しいデータベースサーバーで復元します。この手順は、新しいデータベースサーバーに Red Hat Enterprise Linux 7 がインストールされ、適切なサブスクリプションが設定されていることを前提としています。『インストールガイド』の必要なエンタitleメントへのサブスクライブ を参照してください。

手順13.5 データベースの移行

1. Red Hat Virtualization Manager マシンにログインし、**ovirt-engine** サービスを停止して、エンジンのバックアップに干渉しないようにします。

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

2. **engine** データベースのバックアップを作成します。

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

3. バックアップファイルを新規データベースサーバーにコピーします。

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

4. 新しいデータベースサーバーにログインし、**engine-backup** をインストールします。

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

5. 新しいデータベースサーバーでデータベースを復元します。*FILE_NAME* は、Manager からコピーしたバックアップファイルです。

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

6. データベースが移行されたので、**ovirt-engine** サービスを開始します。

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

13.2. バックアップおよび RESTORE API を使用した仮想マシンのバックアップおよび復元

13.2.1. バックアップおよび Restore API

バックアップおよび復元 API は、仮想マシンのフルバックアップまたはファイルレベルのバックアップと復元を実行できる機能のコレクションです。API は、ライブスナップショットや REST API などの Red Hat Virtualization のいくつかのコンポーネントを組み合わせて、独立したソフトウェアプロバイダーが提供するバックアップソフトウェアを含む仮想マシンに接続できる一時ボリュームを作成して操作します。

サポートされているサードパーティのバックアップベンダーについては、[Red Hat Marketplace](#) の Red Hat Virtualization Ecosystem を参照してください。



注記

REST API の使用方法は、『REST API Guide』の [The Backup and Restore API](#) を参照してください。

13.2.2. 仮想マシンのバックアップ

バックアップおよび復元 API を使用して、仮想マシンをバックアップします。この手順では、バックアップを作成する仮想マシンと、バックアップを管理するためのソフトウェアがインストールされている仮想マシンの 2 つの仮想マシンがあることを前提としています。

手順13.6 仮想マシンのバックアップ

1. REST API を使用して、バックアップを作成する仮想マシンのスナップショットを作成します。

```
POST /api/vms/11111111-1111-1111-1111-111111111111/snapshots/ HTTP/1.1
```

```
Accept: application/xml
Content-type: application/xml

<snapshot>
  <description>BACKUP</description>
</snapshot>
```



注記

仮想マシンのスナップショットを作成すると、スナップショットの作成時と同様に、仮想マシンの設定データのコピーが、スナップショットの **初期化** で **設定** 属性の **data** 属性に保存されます。



重要

共有可能としてマークされているディスクや、直接 LUN ディスクに基づくディスクのスナップショットを作成することはできません。

- スナップショットの下の **data** 属性から仮想マシンの設定データを取得します。

```
GET /api/vms/11111111-1111-1111-1111-111111111111/snapshots/11111111-1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

- スナップショットのディスク ID およびスナップショット ID を特定します。

```
GET /api/vms/11111111-1111-1111-1111-111111111111/snapshots/11111111-1111-1111-1111-111111111111/disks HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

- スナップショットをバックアップ仮想マシンに接続し、ディスクをアクティブ化します。

```
POST /api/vms/22222222-2222-2222-2222-222222222222/disks/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

<disk id="11111111-1111-1111-1111-111111111111">
  <snapshot id="11111111-1111-1111-1111-111111111111"/>
  <active>true</active>
</disk>
```

- バックアップ仮想マシンのバックアップソフトウェアを使用して、スナップショットディスク上のデータをバックアップします。

- バックアップ仮想マシンからスナップショットディスクの割り当てを解除します。

```
DELETE /api/vms/22222222-2222-2222-2222-222222222222/disks/11111111-1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

```
<action>
  <detach>true</detach>
</action>
```

- 必要に応じて、スナップショットを削除します。

```
DELETE /api/vms/11111111-1111-1111-1111-111111111111/snapshots/11111111-1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

別の仮想マシンにインストールされたバックアップソフトウェアを使用して、一定の時点における仮想マシン状態のバックアップを作成しました。

13.2.3. 仮想マシンの復元

バックアップおよび Restore API を使用してバックアップされた仮想マシンを復元します。この手順は、前のバックアップの管理に使用されたソフトウェアがインストールされているバックアップ仮想マシンがあることを前提としています。

手順13.7 仮想マシンの復元

- 管理ポータルで、バックアップを復元するフローティングディスクを作成します。Floating ディスクの作成方法の詳細は、「[Floating 仮想ディスクの作成](#)」を参照してください。
- ディスクをバックアップ仮想マシンに接続します。

```
POST /api/vms/22222222-2222-2222-2222-222222222222/disks/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

<disk id="11111111-1111-1111-1111-111111111111">
</disk>
```

- バックアップソフトウェアを使用して、バックアップをディスクに復元します。
- バックアップ仮想マシンからディスクの割り当てを解除します。

```
DELETE /api/vms/22222222-2222-2222-2222-222222222222/disks/11111111-1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml

<action>
  <detach>true</detach>
</action>
```

- 復元される仮想マシンの設定データを使用して、新しい仮想マシンを作成します。

```
POST /api/vms/ HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

```
<vm>
  <cluster>
    <name>cluster_name</name>
  </cluster>
  <name>NAME</name>
  ...
</vm>
```

6. ディスクを新規の仮想マシンにアタッチします。

```
POST /api/vms/33333333-3333-3333-3333-333333333333/disks/ HTTP/1.1
```

```
Accept: application/xml
```

```
Content-type: application/xml
```

```
<disk id="11111111-1111-1111-1111-111111111111">
</disk>
```

バックアップおよび Restore API を使用して作成されたバックアップを使用して、仮想マシンを復元している。

第14章 RED HAT SATELLITE でのエラータ管理

Red Hat Virtualization は、Red Hat Virtualization Manager の Red Hat Satellite からエラータを表示するように設定できます。これにより、管理者は、ホスト、仮想マシン、および Manager が Red Hat Satellite プロバイダーに関連付けられた後に、それらのエラータとその重要性に関する更新を受け取ることができます。管理者は、必要なホスト、仮想マシン、または Manager で更新を実行して、それらの更新を適用できます。Red Hat Satellite の詳細は、[Red Hat Satellite ユーザーガイド](#) を参照してください。

Red Hat Virtualization 4.0 は、Red Hat Satellite 6.1 によるエラータ管理をサポートします。



重要

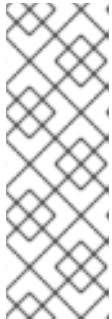
Satellite サーバーでは、Manager、ホスト、および仮想マシンは、FQDN で識別されます。これにより、外部コンテンツのホスト ID を Red Hat Virtualization で維持する必要がなくなります。

Manager、ホスト、および仮想マシンを管理していた Satellite アカウントには、管理者権限とデフォルトの組織セットが必要です。

手順14.1 Red Hat Virtualization エラータの設定

Manager、ホスト、および仮想マシンを Red Hat Satellite プロバイダーに関連付けるには、最初に Manager をプロバイダーに関連付ける必要があります。次に、ホストは同じプロバイダーに関連付けられ、設定されます。最後に、仮想マシンは同じプロバイダーに関連付けられ、設定されます。

- 必要な Satellite サーバーを外部プロバイダーとして追加して Manager を関連付けます。詳細は、[「ホストのプロビジョニング用の Red Hat Satellite インスタンスの追加」](#) を参照してください。



注記

Manager は、コンテンツホストとして Satellite サーバーに登録され、katello-agent パッケージがインストールされている必要があります。

ホスト登録の設定方法の詳細は、『Red Hat Satellite ユーザーガイド』の登録のためのホストの設定を参照してください。ホストの登録および katello-agent パッケージのインストール方法は、『Red Hat Satellite ユーザーガイド』の登録を参照してください。

- オプションで、使用可能なエラータを表示するように必要なホストを設定します。詳細は、[「ホストの Satellite エラータ管理の設定」](#) を参照してください。
- オプションで、使用可能なエラータを表示するように必要な仮想マシンを設定します。必要な仮想マシンを設定する前に、関連するホストを設定する必要があります。詳細は、『Virtual Machine Management Guide』の Configuring Red Hat Satellite Errata Management for a Virtual Machine を参照してください。

手順14.2 Red Hat Virtualization Manager エラータの表示

- ツリーペインで エラータ エントリーを選択します。
- Security**、Bugs、または Enhancements チェックボックスをクリックすると、これらのエラータタイプのみが表示されます。

ホストで利用可能なエラーライフサイクルの表示に関する詳細は、仮想マシン『管理ガイド の 仮想マシン の Red Hat Satellite エラーライフサイクル の表示 を参照し』 てください。『[ホスト Errata の表示](#)』

第15章 ユーザーとロール

15.1. ユーザーの概要

Red Hat Virtualization には、ローカルドメインと外部ドメインの 2 種類のユーザードメインがあります。Manager のインストールプロセス中に、**内部** ドメインと呼ばれるデフォルトのローカルドメインとデフォルトのユーザー **admin** が作成されます。

ovirt-aaa-jdbc-tool を使用して、**内部** ドメインに追加のユーザーを作成できます。ローカルドメインに作成されたユーザー アカウントは、ローカルユーザーとして知られています。また、Red Hat Directory Server、Active Directory、OpenLDAP、その他多くのサポート対象オプションなどの外部 Directory Server を Red Hat Virtualization 環境にアタッチし、外部ドメインとして使用することも可能です。外部ドメインに作成されたユーザー アカウントは、ディレクトリユーザーとして知られています。

ローカルユーザーとディレクトリユーザーの両方が、環境で機能する前に、管理ポータルを介して適切なロールおよび権限を割り当てる必要があります。ユーザー ロールには、エンドユーザーと管理者の 2 つの主要なタイプがあります。エンドユーザー ロールは、ユーザー ポータルから仮想リソースを使用および管理します。管理者のロールは、管理ポータルを使用してシステムインフラストラクチャーを維持します。ロールは、仮想マシンやホストなどの個々のリソースのユーザーに割り当てることも、クラスターやデータセンターなどのオブジェクトの階層に割り当てることもできます。

15.2. DIRECTORY SERVER の概要

インストール時に、Red Hat Virtualization Manager は**内部** ドメインに **admin** ユーザーを作成します。このユーザーは、**admin@internal** とも呼ばれます。このアカウントは、環境の初期設定およびトラブルシューティングに使用することを目的としています。外部 Directory Server を接続し、ディレクトリユーザーを追加し、適切なロールとパーミッションが割り当てられたと、必要なければ **admin@internal** ユーザーを無効にできます。サポートされるディレクトリサーバーは以下のとおりです。

- 389ds
- 389ds RFC-2307 Schema
- Active Directory
- FreeIPA
- Red Hat Identity Management (IdM)
- Novell eDirectory RFC-2307 スキーマ
- OpenLDAP RFC-2307 Schema
- OpenLDAP Standard Schema
- Oracle Unified Directory RFC-2307 スキーマ
- RFC-2307 スキーマ (汎用)
- Red Hat Directory Server (RHDS)
- Red Hat Directory Server (RHDS) RFC-2307 Schema
- iPlanet



重要

Red Hat Virtualization Manager (nios)と IdM (ipa-server)を同じシステムにインストールすることはできません。IdM は、Red Hat Virtualization Manager で必要な mod_ssl パッケージと互換性がありません。



重要

Active Directory をディレクトリーサーバーとして使用し、テンプレートと仮想マシンの作成に **sysprep** を使用する場合は、Red Hat Virtualization 管理ユーザーをドメインの制御に委譲する必要があります。

- コンピューターをドメインに参加させる
- グループのメンバーシップを変更する

Active Directory でのユーザー アカウントの作成に関する詳細は、を参照してください
<http://technet.microsoft.com/en-us/library/cc732336.aspx>。

Active Directory での制御の委任に関する情報は、を参照してください
<http://technet.microsoft.com/en-us/library/cc732524.aspx>。

15.3. 外部 LDAP プロバイダーの設定

15.3.1. 外部 LDAP プロバイダーの設定 (対話型セットアップ)

ovirt-engine-extension-aaa-ldap 拡張を使用すると、ユーザーは外部ディレクトリーの設定を簡単にカスタマイズできます。**ovirt-engine-extension-aaa-ldap** 拡張機能は、さまざまな LDAP サーバータイプをサポートしており、ほとんどの LDAP タイプのセットアップを支援する対話型セットアップスクリプトが提供されています。

LDAP サーバーの種類が対話型セットアップスクリプトにリストされていない場合、またはさらにカスタマイズしたい場合は、設定ファイルを手動で編集できます。詳細は、「[外部 LDAP プロバイダーの設定 \(手動による方法\)](#)」を参照してください。

Active Directory の例は、「[Active Directory の接続](#)」を参照してください。

前提条件:

- DNS または LDAP サーバーのドメイン名を知っている必要があります。ラウンドロビンポリシーおよびフェイルオーバー ポリシーもサポートされます。
- LDAP サーバーと Manager の間に安全な接続を設定するには、PEM でエンコードされた CA 証明書が準備されていることを確認してください。詳細は、「[Manager と LDAP サーバー間の SSL または TLS 接続の設定](#)」を参照してください。
- 匿名検索がサポートされていない限り、検索ユーザーとして使用するディレクトリーサーバーで、すべてのユーザーおよびグループを参照するパーミッションを持つユーザーが利用できる必要があります。検索ユーザーの識別名(DN)を書き留めます。ディレクトリーサーバーの管理ユーザーを使用しないでください。
- LDAP サーバーへの検索およびログインクエリーを実行するために、少なくとも 1 セットのアカウント名とパスワードを用意します。

手順15.1 外部 LDAP プロバイダーの設定

1. Red Hat Virtualization Manager で、LDAP 拡張パッケージをインストールします。

```
# yum install ovirt-engine-extension-aaa-ldap-setup
```

2. **ovirt-engine-extension-aaa-ldap-setup** を実行して、対話型セットアップを開始します。

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. プロファイル名を指定します。プロファイル名は、ログインページでユーザーに表示されます。この例では、**redhat.com** を使用しています。



注記

ドメインの設定後にプロファイルの名前を変更するには、**/etc/ovirt-engine/extensions.d/redhat.com-authn.properties** ファイルの **ovirt.engine.aaa.authn.profile.name** 属性を編集します。エンジンサービスを再起動して、変更を適用します。

```
Please specify profile name that will be visible to users:redhat.com
```

図15.1 管理ポータルのログインページ



注記

ユーザーは、初めてログインするときに、ドロップダウンリストから目的のプロファイルを選択する必要があります。その後、情報はブラウザーの Cookie に保存され、ユーザーが次にログインしたときに事前に選択されます。

4. 対応する番号を入力して、LDAP タイプを選択します。LDAP サーバーがどのスキーマであるかわからない場合は、LDAP サーバータイプの標準スキーマを選択してください。Active Directory の場合は、「[Active Directory の接続](#)」の手順に従います。

```
Available LDAP implementations:  
1 - 389ds  
2 - 389ds RFC-2307 Schema
```

3 - Active Directory
 4 - IPA
 5 - Novell eDirectory RFC-2307 Schema
 6 - OpenLDAP RFC-2307 Schema
 7 - OpenLDAP Standard Schema
 8 - Oracle Unified Directory RFC-2307 Schema
 9 - RFC-2307 Schema (Generic)
 10 - RHDS
 11 - RHDS RFC-2307 Schema
 12 - iPlanet
 Please select: 10

5. **Enter** を押してデフォルトを受け入れ、LDAP サーバー名のドメイン名解決を設定します。

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]:

6. 対応する番号を入力して DNS ポリシーメソッドを選択します。

1 - Single server
 2 - DNS domain LDAP SRV record
 3 - Round-robin between multiple hosts
 4 - Failover between multiple hosts
 Please select:

- オプション1の場合、**/etc/resolv.conf** に一覧表示されている DNS サーバーを使用して IP アドレスを解決します。**/etc/resolv.conf** ファイルが正しい DNS サーバーで更新されていることを確認します。

完全修飾ドメイン名(FQDN)または LDAP サーバーの IP アドレスを入力します。SRV レコードで **dig** コマンドを使用して、ドメイン名を見つけることができます。SRV レコードは、_service._protocol. ドメイン名の形式を取ります。例：**dig _ldap._tcp.redhat.com SRV**

- オプション2には、DNS サーバーのドメイン名を入力します。DNS 検索は、SRV レコードを検索して LDAP サーバーのドメイン名を見つけるために実行されます。
- オプション3には、LDAP サーバーのスペース区切りのリストを入力します。サーバーの FQDN または IP アドレスのいずれかを使用します。このポリシーは、LDAP サーバー間の負荷分散を提供します。クエリーは、ラウンドロビンアルゴリズムに従ってすべての LDAP サーバーに分散されます。
- オプション4には、スペースで区切られた LDAP サーバーのリストを入力します。サーバーの FQDN または IP アドレスのいずれかを使用します。このポリシーは、クエリーに応答するデフォルトの LDAP サーバーとなる最初の LDAP サーバーを定義します。最初のサーバーが使用できない場合、クエリーはリストの次の LDAP サーバーに移動します。

7. LDAP サーバーがサポートする安全な接続方法を選択し、PEM でエンコードされた CA 証明書を取得する方法を指定します。ファイルオプションを使用すると、証明書へのフルパスを指定できます。URL オプションを使用すると、証明書への URL を指定できます。インラインオプションを使用して、証明書の内容をターミナルに貼り付けます。システムオプションを使用すると、すべての CA ファイルのデフォルトの場所を指定できます。セキュアでないモードが選択されている場合、接続は TLS を使用して暗号化されますが、証明書の検証はスキップされます。

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 Idaps protocol.
Use plain for test environments only.
Please select protocol to use (startTLS, Idaps, plain) [startTLS]: *startTLS*
Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure): *File*
Please enter the password:

**注記**

LDAPS は、セキュアソケットリンクを介したライトウェイトディレクトリーアクセスプロトコルの略です。SSL 接続の場合は、**Idaps** オプションを選択します。

PEM でエンコードされた CA 証明書の作成に関する詳細は、[「Manager と LDAP サーバー間の SSL または TLS 接続の設定」](#) を参照してください。

- 検索ユーザーの識別名 (DN) を入力します。ユーザーには、Directory Server 上のすべてのユーザーとグループを参照するためのアクセス許可が必要です。検索ユーザーは、LDAP アノテーションで指定する必要があります。匿名検索が許可されている場合は、入力せずに **Enter** を押します。

Enter search user DN (empty for anonymous):

uid=user1,ou=Users,dc=test,dc=redhat,dc=com

Enter search user password:

- 検索およびログイン機能をテストして、LDAP サーバーが Red Hat Virtualization 環境に正しく接続されていることを確認します。ログインクエリーには、アカウント名とパスワードを入力します。検索クエリーで、ユーザー アカウントの場合は **Principal** を選択し、グループ アカウントの場合は **Group** を選択します。ユーザー アカウントのグループ アカウント情報を返す場合は、**Resolve Groups** に **Yes** を入力します。**Done** を選択してセットアップを完了します。3 つの設定ファイルが作成され、画面出力に表示されます。

NOTE:

It is highly recommended to test drive the configuration before applying it into engine.

Perform at least one Login sequence and one Search 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

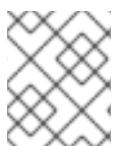
[INFO] Stage: Package installation

[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
```

- エンジンサービスを再起動します。作成したプロファイルは、管理ポータルおよびユーザー ポータルのログインページで利用できるようになります。LDAP サーバー上のユーザーアカウントに適切なロールとパーミッションを割り当てるには、たとえば、ユーザー ポータルにログインするには、「[管理ポータルからのユーザータスクの管理](#)」を参照してください。

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



注記

詳細は、[/usr/share/doc/ovirt-engine-extension-aaa-ldap-<version>](#) の LDAP 認証および承認拡張 README ファイルを参照してください。

15.3.2. Active Directory の接続

前提条件:

- Active Directory フォレスト名を知っている必要があります。フォレスト名は、ルートドメイン名とも呼ばれます。
- Active Directory フォレスト名を解決できる DNS サーバーを Manager の [/etc/resolv.conf](#) ファイルに追加するか、Active Directory DNS サーバーを書き留めて、対話型セットアップスクリプトのプロンプトが表示されたら入力する必要があります。
- LDAP サーバーと Manager の間に安全な接続を設定するには、PEM でエンコードされた CA 証明書が準備されていることを確認してください。詳細は、「[Manager と LDAP サーバー間の SSL または TLS 接続の設定](#)」を参照してください。
- 匿名検索がサポートされていない限り、検索ユーザーとして使用するには、すべてのユーザーとグループを参照する権限を持つユーザーが Active Directory で利用可能である必要があります。検索ユーザーの識別名(DN)を書き留めます。Active Directory の管理ユーザーを使用しないでください。
- Active Directory への検索およびログインクエリーを実行するために、少なくとも 1 セットのアカウント名とパスワードを用意します。

手順15.2 外部 LDAP プロバイダーの設定

- Red Hat Virtualization Manager で、LDAP 拡張パッケージをインストールします。

```
# yum install ovirt-engine-extension-aaa-ldap-setup
```

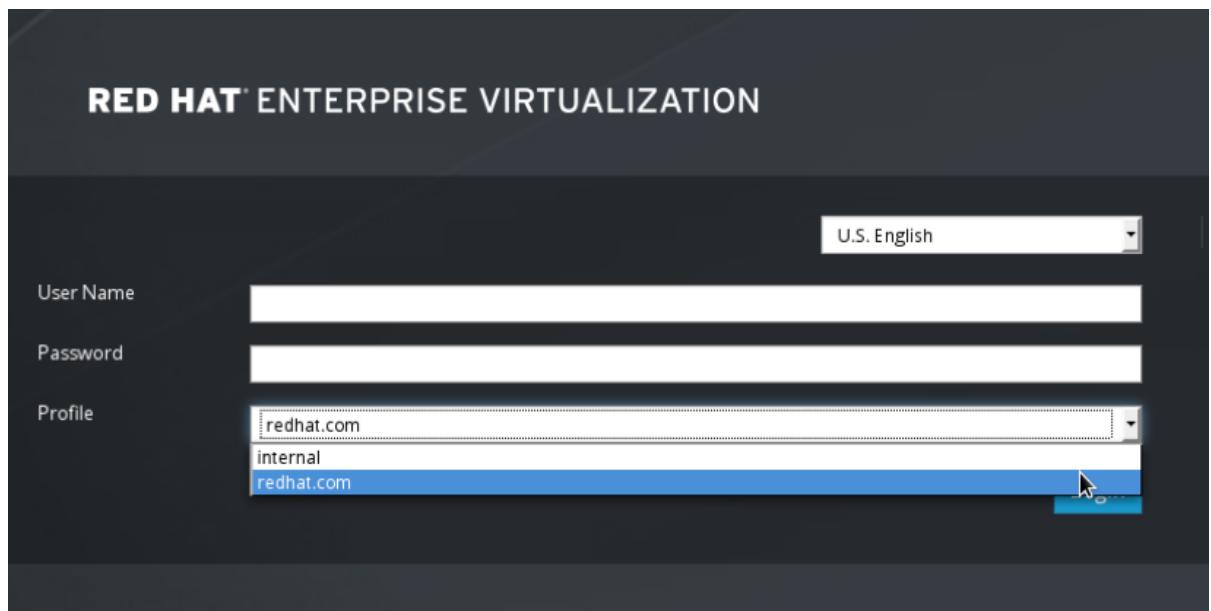
2. **ovirt-engine-extension-aaa-ldap-setup** を実行して、対話型セットアップを開始します。

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. プロファイル名を指定します。プロファイル名は、ログインページでユーザーに表示されます。この例では、**redhat.com** を使用しています。

```
Please specify profile name that will be visible to users:redhat.com
```

図15.2 管理ポータルのログインページ



注記

ユーザーは、初めてログインするときに、ドロップダウンリストから目的のプロファイルを選択する必要があります。その後、情報はブラウザーの Cookie に保存され、ユーザーが次にログインしたときに事前に選択されます。

4. 対応する番号を入力して、LDAP タイプを選択します。この手順の後の LDAP 関連の質問は、LDAP タイプによって異なります。

```
Available LDAP implementations:
```

- 1 - 389ds
 - 2 - 389ds RFC-2307 Schema
 - 3 - Active Directory
 - 4 - IPA
 - 5 - Novell eDirectory RFC-2307 Schema
 - 6 - OpenLDAP RFC-2307 Schema
 - 7 - OpenLDAP Standard Schema
 - 8 - Oracle Unified Directory RFC-2307 Schema
 - 9 - RFC-2307 Schema (Generic)
 - 10 - RHDS
 - 11 - RHDS RFC-2307 Schema
 - 12 - iPlanet
- Please select: 3

- Active Directory フォレスト名を入力します。フォレスト名が Manager の DNS で解決できない場合、スクリプトにより、スペースで区切られた Active Directory サーバー名のリストを入力するように求められます。

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*

- LDAP サーバーがサポートする安全な接続方法を選択し、PEM でエンコードされた CA 証明書を取得する方法を指定します。ファイルオプションを使用すると、証明書へのフルパスを指定できます。URL オプションを使用すると、証明書への URL を指定できます。インラインオプションを使用して、証明書の内容をターミナルに貼り付けます。システムオプションを使用すると、すべての CA ファイルの場所を指定できます。安全でないオプションを使用すると、startTLS を安全でないモードで使用できます。

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:



注記

LDAPS は、セキュアソケットリンクを介したライトウェイトディレクトリーアクセスプロトコルの略です。SSL 接続の場合は、**ldaps** オプションを選択します。

PEM でエンコードされた CA 証明書の作成に関する詳細は、[「Manager と LDAP サーバー間の SSL または TLS 接続の設定」](#) を参照してください。

- 検索ユーザーの識別名 (DN) を入力します。ユーザーには、Directory Server 上のすべてのユーザーとグループを参照するためのアクセス許可が必要です。検索ユーザーは LDAP アノテーションである必要があります。匿名検索が許可されている場合は、入力せずに **Enter** を押します。

Enter search user DN (empty for anonymous):

uid=user1,ou=Users,dc=test,dc=redhat,dc=com

Enter search user password:

- 検索およびログイン機能をテストして、LDAP サーバーが Red Hat Virtualization 環境に正しく接続されていることを確認します。ログインクエリーには、アカウント名とパスワードを入力します。検索クエリーで、ユーザー アカウントの場合は **Principal** を選択し、グループ アカウントの場合は **Group** を選択します。ユーザー アカウントのグループ アカウント情報を返す場合は、**Resolve Groups** に **Yes** を入力します。**Done** を選択してセットアップを完了します。3つの設定ファイルが作成され、画面出力に表示されます。

NOTE:

It is highly recommended to test drive the configuration before applying it into engine.

Perform at least one Login sequence and one Search 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

```

9. 作成したプロファイルは、管理ポータルおよびユーザーportalのログインページで利用できるようになります。LDAP サーバー上のユーザーアカウントに適切なロールとパーミッションを割り当てるには、たとえば、ユーザーportalにログインするには、「[管理ポータルからのユーザータスクの管理](#)」を参照してください。



注記

詳細は、**/usr/share/doc/ovirt-engine-extension-aaa-ldap-version** の LDAP 認証および承認拡張 README ファイルを参照してください。

15.3.3. 外部 LDAP プロバイダーの設定 (手動による方法)

ovirt-engine-extension-aaa-ldap 拡張機能は LDAP プロトコルを使用してディレクトリサーバーにアクセスし、完全にカスタマイズ可能です。ユーザーportalまたは管理ポータル機能へのシングルサインオンを有効にしない限り、Kerberos 認証は必要ありません。

前のセクションの対話型セットアップ方法でユースケースがカバーされていない場合は、設定ファイルを手動で変更して LDAP サーバーを接続できます。次の手順では、一般的な詳細を使用します。具体的な値は、設定によって異なります。

手順15.3 外部 LDAP プロバイダーの設定 (手動による方法)

1. Red Hat Virtualization Manager で、LDAP 拡張パッケージをインストールします。

```
# yum install ovirt-engine-extension-aaa-ldap
```

2. LDAP 設定テンプレートファイルを **/etc/ovirt-engine** ディレクトリーにコピーします。テンプレートファイルは、アクティブなディレクトリー(ad)およびその他のディレクトリータイプ(単純な)で利用できます。この例では、単純な設定テンプレートを使用しています。

```
# cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple/. /etc/ovirt-engine
```

3. 管理ポータルおよびユーザーportalのログインページでユーザーに表示するプロファイル名に一致するように、設定ファイルの名前を変更します。

```
# 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. LDAP サーバーの種類のコメントを解除し、ドメインとパスワードのフィールドを更新して、LDAP プロパティ設定ファイルを編集します。

```
# vi /etc/ovirt-engine/aaa/example.properties
```

例15.1 プロファイルの例: LDAP サーバーセクション

```
# 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}
```

TLS または SSL プロトコルを使用して LDAP サーバーと対話するには、LDAP サーバーのルート CA 証明書を取得し、それを使用して公開鍵ストアファイルを作成します。次の行のコメントを解除し、公開キーストアファイルへのフルパスとファイルにアクセスするためのパスワードを指定します。



注記

パブリックキーストアファイルの作成方法の詳細は、「[Manager と LDAP サーバー間の SSL または TLS 接続の設定](#)」を参照してください。

例15.2 プロファイルの例: キーストアセクション

```
# 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. 認証設定ファイルを確認します。管理ポータルおよびユーザーportalのログインページでユーザーに表示されるプロファイル名は、**ovirt.engine.aaa.authn.profile.name**によって定義されます。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。すべてのフィールドをデフォルトのままにすることができます。

```
# vi /etc/ovirt-engine/extensions.d/example-authn.properties
```

例15.3 認証設定ファイルの例

```
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. 許可設定ファイルを確認してください。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。すべてのフィールドをデフォルトのままにすることができます。

```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

例15.4 許可設定ファイルの例

```
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
```

- 設定プロファイルの所有権および権限が適切であることを確認してください。

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
# chmod 600 /etc/ovirt-engine/aaa/example.properties
```

- エンジンサービスを再起動します。

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

- 作成した *example* プロファイルは、管理ポータルおよびユーザーportalのログインページで利用できるようになりました。LDAP サーバーのユーザー アカウントに適切なパーミッションを付与するには、たとえば、ユーザー portal にログインするには、「[管理ポータルからのユーザータスクの管理](#)」を参照してください。



注記

詳細は、[/usr/share/doc/ovirt-engine-extension-aaa-ldap-version](#) の LDAP 認証および承認拡張 README ファイルを参照してください。

15.3.4. 外部 LDAP プロバイダーの削除

この手順では、外部で設定された LDAP プロバイダーとそのユーザーを削除する方法を示します。

手順15.4 外部 LDAP プロバイダーの削除

- LDAP プロバイダー設定ファイルを削除し、デフォルトの名前 **profile1** を置き換えます。

```
# 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
```

- ovirt-engine** サービスを再起動します。

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

- 管理ポータルの **Users** リソースタブで、このプロバイダーのユーザー(**Authorization provider** が **profile1-authz** であるユーザー)を選択し、**Remove** をクリックします。

15.4. SINGLE SIGN-ON 用の LDAP および KERBEROS の設定

シングルサインオンにより、ユーザーはパスワードを再入力せずにユーザー portal または管理ポータルにログインできます。認証情報は Kerberos サーバーから取得されます。管理ポータルとユーザー portal へのシングルサインオンを設定するには、**ovirt-engine-extension-aaa-misc** および **ovirt-engine-extension-aaa-ldap** の 2 つの拡張機能と、**mod_auth_gssapi** と **mod_session** の 2 つの Apache モジュールを設定する必要があります。Kerberos を含まない Single Sign-On を設定できますが、これはこのドキュメントの範囲外です。



注記

ユーザーportalへのシングルサインオンが有効になっている場合、仮想マシンへのシングルサインオンはできません。ユーザーportalへのシングルサインオンを有効にすると、ユーザーportalはパスワードを受け入れる必要がないため、パスワードを委譲して仮想マシンにサインインすることはできません。

この例では、以下を前提としています。

- 既存の KeyDistributionCenter (KDC) サーバーは、MIT バージョンの Kerberos5 を使用します。
- KDC サーバーに対する管理者権限があります。
- Kerberos クライアントは、Red Hat Virtualization Manager とユーザーマシンにインストールされます。
- kadmin** ユーティリティーは、Kerberos サービスプリンシパルおよび **keytab** ファイルを作成するために使用されます。

この手順には、次のコンポーネントが含まれます。

On the KDC server

- Red Hat Virtualization Manager で Apache サービスのサービスプリンシパルと **keytab** ファイルを作成します。

Red Hat Virtualization Manager の場合

- 認証および許可拡張パッケージと Apache Kerberos 認証モジュールをインストールします。
- 拡張ファイルを設定します。

手順15.5 Apache サービス用の Kerberos の設定

- KDC サーバーで、**kadmin** ユーティリティーを使用して、Red Hat Virtualization Manager で Apache サービスのサービスプリンシパルを作成します。サービスプリンシパルは、Apache サービスの KDC への参照 ID です。

```
# kadmin
kadmin> addprinc -randkey HTTP/fqdn-of-rhevm@REALM.COM
```

- Apache サービスの **keytab** ファイルを生成します。**keytab** ファイルは共有の秘密鍵を保存します。

```
kadmin> ktadd -k /tmp/http.keytab HTTP/fqdn-of-rhevm@REALM.COM
```

```
kadmin> quit
```

- KDC サーバーから Red Hat Virtualization Manager に **keytab** ファイルをコピーします。

```
# scp /tmp/http.keytab root@rhevm.example.com:/etc/httpd
```

Red Hat Virtualization Manager の操作手順

- Red Hat Virtualization Manager で、キータブの所有権と権限が適切であることを確認します。

```
# chown apache /etc/httpd/http.keytab
```

```
# chmod 400 /etc/httpd/http.keytab
```

- 認証拡張パッケージ、LDAP 拡張パッケージ、および **mod_auth_gssapi** および **mod_sessionApache** モジュールをインストールします。

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

- SSO 設定テンプレートファイルを **/etc/ovirt-engine** ディレクトリーにコピーします。テンプレートファイルは、Active Directory (**ad-sso**) およびその他のディレクトリータイプ(**simple-sso**)で利用できます。この例では、単純な SSO 設定テンプレートを使用しています。

```
# cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple-sso/. /etc/ovirt-engine
```

- ovirt-sso.conf** を Apache 設定ディレクトリーに移動します。

```
# mv /etc/ovirt-engine/aaa/ovirt-sso.conf /etc/httpd/conf.d
```

- 認証方法ファイルを確認します。レルムは **keytab** ファイルから自動的にフェッチされるため、このファイルを編集する必要はありません。

```
# vi /etc/httpd/conf.d/ovirt-sso.conf
```

例15.5 認証方法ファイルの例

```
<LocationMatch ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/token-http-auth)|^/ovirt-engine/api>
<If "req('Authorization') !~ /^(Bearer|Basic)/i">
    RewriteEngine on
    RewriteCond %{LA-U:REMOTE_USER} ^(.*)$
    RewriteRule ^(.*)$ - [L,NS,P,E=REMOTE_USER:%1]
    RequestHeader set X-Remote-User %{REMOTE_USER}s

    AuthType GSSAPI
    AuthName "Kerberos Login"

    # Modify to match installation
    GssapiCredStore keytab:/etc/httpd/http.keytab
    GssapiUseSessions On
    Session On
    SessionCookieName ovirt_gssapi_session path=/private;httponly;secure;

    Require valid-user
    ErrorDocument 401 "<html><meta http-equiv=\"refresh\" content=\"0; url=/ovirt-engine/sso/login-unauthorized\"/><body><a href=\"/ovirt-engine/sso/login-
```

```

    unauthorized">Here</a></body></html>"  

  </If>  

</LocationMatch>

```

6. 管理ポータルおよびユーザー ポータルのログインページでユーザーに表示するプロファイル名に一致するように、設定ファイルの名前を変更します。

```

# 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. LDAP サーバーの種類のコメントを解除し、ドメインとパスワードのフィールドを更新して、LDAP プロパティ設定ファイルを編集します。

```
# vi /etc/ovirt-engine/aaa/example.properties
```

例15.6 プロファイルの例: LDAP サーバーセクション

```

# 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}

```

TLS または SSL プロトコルを使用して LDAP サーバーと対話するには、LDAP サーバーのルート CA 証明書を取得し、それを使用して公開鍵ストアファイルを作成します。次の行のコメントを解除し、公開キーストアファイルへのフルパスとファイルにアクセスするためのパスワードを指定します。



注記

パブリックキーストアファイルの作成方法の詳細は、「[Manager と LDAP サーバー間の SSL または TLS 接続の設定](#)」を参照してください。

例15.7 プロファイルの例: キーストアセクション

```
# 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. 認証設定ファイルを確認します。管理ポータルおよびユーザーportalのログインページでユーザーに表示されるプロファイル名は、**ovirt.engine.aaa.authn.profile.name** によって定義されます。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。すべてのフィールドをデフォルトのままにすることができます。

```
# vi /etc/ovirt-engine/extensions.d/example-http-authn.properties
```

例15.8 認証設定ファイルの例

```
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. 許可設定ファイルを確認してください。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。すべてのフィールドをデフォルトのままにすることができます。

```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

例15.9 許可設定ファイルの例

```
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. 認証マッピング設定ファイルを確認します。設定プロファイルの場所は、LDAP 設定ファイルの場所と一致する必要があります。設定プロファイルの拡張名は、認証設定ファイルの **ovirt.engine.aaa.authn.mapping.plugin** 値と一致させる必要があります。すべてのフィールドをデフォルトのままにすることができます。

```
# vi /etc/ovirt-engine/extensions.d/example-http-mapping.properties
```

例15.10 認証マッピング設定ファイルの例

```

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. 設定ファイルの所有権および権限が適切であることを確認してください。

```

# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties

# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-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-authn.properties

# chmod 640 /etc/ovirt-engine/extensions.d/example-http-mapping.properties

# chmod 640 /etc/ovirt-engine/extensions.d/example-authz.properties

```

12. Apache サービスおよび **ovirt-engine** サービスを再起動します。

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

15.5. ユーザーの承認

15.5.1. ユーザー認証モデル

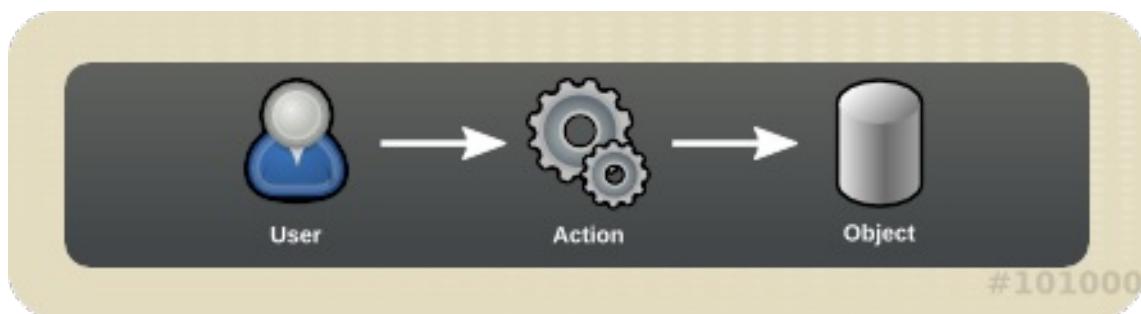
Red Hat Virtualization は、3つのコンポーネントの組み合わせに基づいて承認制御を適用します。

- アクションを実行するユーザー
- 実行されているアクションのタイプ
- アクションが実行されるオブジェクト

15.5.2. ユーザーアクション

アクションを正常に実行するには、ユーザーが、動作対象のオブジェクトに適切なパーミッションを持っている必要があります。各アクションタイプはパーミッションに対応します。システムには多数のパーミッションがあるため、簡素化するために以下のパーミッションがあります。

図15.3 アクション



重要

いくつかのアクションは、複数のオブジェクトに対して実行されます。たとえば、テンプレートを別のストレージドメインにコピーすると、テンプレートと宛先ストレージドメインの両方に影響します。アクションを実行するユーザーは、アクションが影響を与えるすべてのオブジェクトに対して適切な権限を持っている必要があります。

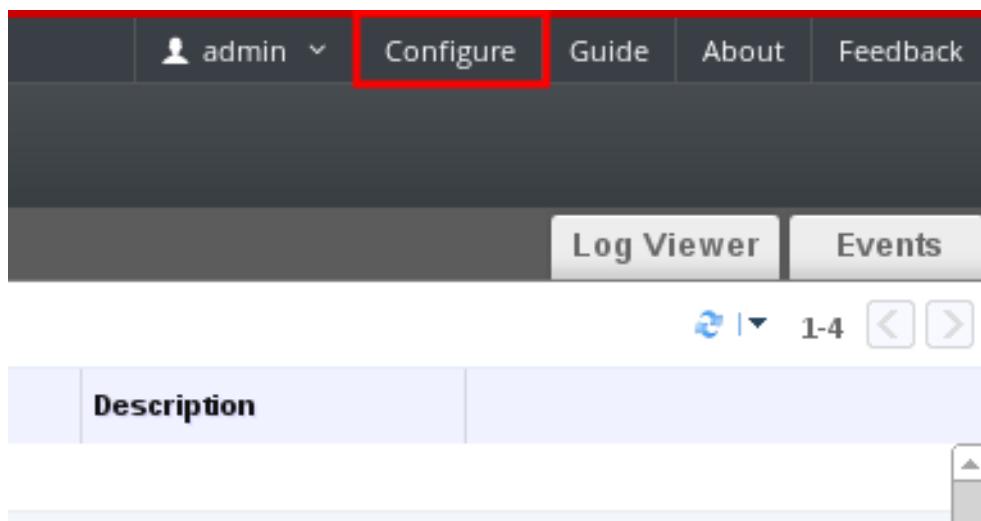
15.6. 管理ポータルからのユーザータスクの管理

15.6.1. ユーザーの追加およびユーザーportalパーミッションの割り当て

ユーザーを追加してロールおよび権限を割り当てる前に、ユーザーをすでに作成しておく必要があります。この手順で割り当てられたロールと権限により、ユーザーにユーザーportalにログインして仮想マシンの作成を開始するパーミッションが付与されます。この手順は、グループアカウントにも適用されます。

手順15.7 ユーザーの追加およびユーザーportalパーミッションの割り当て

1. ヘッダーバーで **Configure** をクリックし、**Configure** ウィンドウを開きます。 **System Permissions** をクリックします。



2. **Add** をクリックして、**Add System Permission to User** ウィンドウを開きます。
3. **Search** でプロファイルを選択します。プロファイルは、検索するドメインです。検索テキストフィールドに名前の名前または一部を入力し、**GO** をクリックします。または、**GO** をクリックして、すべてのユーザーとグループのリストを表示します。
4. 適切なユーザーまたはグループのチェックボックスを選択します。
5. **Role to Assign** で割り当てる適切なロールを選択します。 **UserRole** ロールは、ユーザー アカウントに、ユーザー ポータルにログインするパーミッションを付与します。
6. **OK** をクリックします。

ユーザー ポータルにログインして、ユーザー アカウントにログインするパーミッションがあることを確認します。

15.6.2. ユーザー情報の表示

各ユーザーに関する詳細情報は、**Users** タブで表示できます。

手順15.8 ユーザー情報の表示

1. **Users** タブをクリックして、承認されたユーザーの一覧を表示します。
2. ユーザーを選択するか、結果一覧にユーザーが表示されない場合は検索を実行します。
3. 選択したユーザーの詳細ペインが表示され、通常は **General** タブにドメイン名、電子メール、ユーザーのステータスなどの一般情報が表示されます。
4. 他のタブでは、ユーザーのグループ、権限、割り当て、およびイベントを表示できます。
たとえば、ユーザーが属するグループを表示するには、**Directory Groups** タブをクリックします。

15.6.3. リソースでのユーザー パーミッションの表示

ユーザーには、特定のリソースまたはリソースの階層のパーミッションを割り当することができます。各リソースに割り当てられたユーザーとそのパーミッションを表示できます。

手順15.9 リソースでのユーザー権限の表示

- リソースタブをクリックし、結果一覧でリソースを選択します。
- 詳細ペインの **Permissions** タブをクリックして、割り当てられたユーザー、ユーザーのロール、および選択したリソースに対する継承された権限を一覧表示します。

15.6.4. ユーザーの削除

ユーザー アカウントが必要なくなったら、Red Hat Virtualization から削除します。

手順15.10 ユーザーの削除

- Users** タブをクリックして、承認されたユーザーの一覧を表示します。
- 削除するユーザーを選択します。ユーザーが仮想マシンを実行していないことを確認します。
- 削除** ボタンをクリックします。削除の確認を求めるメッセージが表示されます。**OK** をクリックします。

ユーザーは Red Hat Virtualization から削除されますが、外部ディレクトリーからは削除されません。

15.6.5. ログインしたユーザーの表示

現在ログインしているユーザーを、セッション時間やその他の詳細とともに表示できます。ツリーペインで **Active User Sessions** エントリーをクリックして、ログインしている各ユーザーのセッションの詳細を表示します。

Active User Sessions タブには、**Session DB ID**、**User Name**、**Authorization provider**、**User id**、**Source IP**、**Session Start Time**、および **Session Last Active Time** が表示されます。

15.6.6. ユーザーセッションの終了

現在ログインしているユーザーのセッションを終了することができます。

手順15.11 ユーザーセッションの終了

- ツリーペインで **Active User Sessions** エントリーをクリックします。
- 終了するユーザー セッションを選択します。
- セッションの終了** をクリックします。
- OK** をクリックします。

15.7. コマンドラインからのユーザー タスクの管理

15.7.1. ユーザーの管理

ovirt-aaa-jdbc-tool ツールを使用して、内部 ドメインのユーザー アカウントを管理できます。このツールを使用して行った変更はすぐに有効になり、**ovirt-engine** サービスを再起動する必要はありません。ユーザー オプションの完全なリストについては、**ovirt-aaa-jdbc-tool user --help** を実行してください。このセクションでは、一般的な例を示します。

手順15.12 ユーザーの作成

この手順では、ユーザーの作成、ユーザーパスワードの設定、および Red Hat Virtualization 環境の追加方法を説明します。

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. ユーザーアカウントを新規作成します。オプションで **--attribute** を使用してアカウントの詳細を指定します。オプションの完全なリストについては、**ovirt-aaa-jdbc-tool user add --help** を実行してください。

```
# ovirt-aaa-jdbc-tool user add test1 --attribute=firstName=John --attribute=lastName=Doe
adding user test1...
user added successfully
```

3. パスワードを設定します。**--password-valid-to** の値を設定する必要があります。設定しないと、パスワードの有効期限はデフォルトで現在の時間に設定されます。日付形式は **yyyy-MM-dd HH:mm:ssX** です。この例では、**-0800** は GMT から 8 時間を引いたものを表します。その他のオプションについては、**ovirt-aaa-jdbc-tool user password-reset --help** を実行してください。

```
# 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
```



注記

デフォルトでは、内部ドメインのユーザーアカウントのパスワードポリシーには次の制限があります。

- 6 文字以上。
- パスワード変更中は、過去に使用した 3 つのパスワードを再度設定することはできません。

パスワードポリシーおよびその他のデフォルト設定の詳細は、**ovirt-aaa-jdbc-tool settings show** を実行します。

4. 管理ポータルで新たに作成されたユーザーを追加し、ユーザーに適切なロールとパーミッションを割り当てます。詳細は、「[ユーザーの追加およびユーザー ポータル パーミッションの割り当て](#)」を参照してください。

手順15.13 ユーザー情報の表示

この手順では、ユーザーアカウント情報を表示する方法を説明します。管理ポータルの **Users** タブよりも多くの情報が表示されます。

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. 以下のコマンドを実行します。

```
# ovirt-aaa-jdbc-tool user show test1
```

手順15.14 ユーザー情報の編集

この手順では、ユーザーアカウント情報を更新する方法を説明します。

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. 以下のコマンドを実行してユーザー情報を編集します。この例では、メールアドレスを更新します。

```
# ovirt-aaa-jdbc-tool user edit test1 --attribute=email=jdoe@example.com
```

手順15.15 ユーザーの削除

この手順では、ユーザーアカウントを削除する方法を示します。

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. ユーザーを削除します。

```
# ovirt-aaa-jdbc-tool user delete test1
```

3. 管理ポータルからユーザーを削除します。詳細は、「[ユーザーの削除](#)」を参照してください。

15.7.2. 内部管理ユーザーのパスワード変更

内部管理ユーザー(**admin@internal**)のパスワードをリセットするには、**ovirt-aaa-jdbc-tool** ツールを使用します。パスワードの変更を有効にするために **ovirt-engine** サービスを再起動する必要はありません。

デフォルトでは、内部ドメインのユーザーアカウントのパスワードポリシーには次の制限があります。

- 6 文字以上。
- パスワード変更中は、過去に使用した 3 つのパスワードを再度設定することはできません。

パスワードポリシーおよびその他のデフォルト設定の詳細は、**ovirt-aaa-jdbc-tool settings show** を実行します。

手順15.16 内部管理ユーザーのパスワードのリセット

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. インタラクティブモードでパスワードを変更するには、以下のコマンドを実行します。
--password-valid-to の値を設定する必要があります。設定しないと、パスワードの有効期限はデフォルトで現在の時間に設定されます。日付形式は **yyyy-MM-dd HH:mm:ssX** です。この例では、**Z** は UTC 時間を表します。その他のオプションについては、**ovirt-aaa-jdbc-tool user password-reset --help** を実行してください。

```
# ovirt-aaa-jdbc-tool user password-reset admin --password-valid-to="2025-08-01 12:00:00Z"
```

15.7.3. 内部管理ユーザーの無効化

engine-setup 中に作成された **admin@internal** ユーザーを含む、ローカルドメインのユーザーを無効にすることができます。デフォルトの管理ユーザーを無効にする前に、完全な管理 者 権限を持つ環境に少なくとも1人のユーザーがあることを確認します。

手順15.17 内部管理ユーザーの無効化

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. **SuperUser** ロールの別のユーザーが環境に追加されていることを確認します。詳細は、「[ユーザーの追加およびユーザーポートルパーミッションの割り当て](#)」を参照してください。
3. デフォルトの **admin** ユーザーを無効にします。

```
# ovirt-aaa-jdbc-tool user edit admin --flag=+disabled
```



注記

無効にしたユーザーを有効にするには、**ovirt-aaa-jdbc-tool user edit username --flag=-disabled** を実行します。

15.7.4. グループの管理

ovirt-aaa-jdbc-tool ツールを使用して、内部ドメインのグループアカウントを管理できます。グループアカウントの管理は、ユーザー アカウントの管理に似ています。グループオプションの完全なリストについては、**ovirt-aaa-jdbc-tool group --help** を実行してください。このセクションでは、一般的な例を示します。

手順15.18 グループの作成

この手順では、グループアカウントを作成し、ユーザーをグループに追加し、グループの詳細を表示する方法を示します。

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. 新規グループを作成します。

```
# ovirt-aaa-jdbc-tool group add group1
```

3. ユーザーをグループに追加します。ユーザーが作成されている必要があります。

```
# ovirt-aaa-jdbc-tool group-manage useradd group1 --user=test1
```



注記

group-manage オプションの完全なリストについては、**ovirt-aaa-jdbc-tool group-manage --help** を実行してください。

4. グループアカウントの詳細を表示します。

```
# ovirt-aaa-jdbc-tool group show group1
```

- 新しく作成したグループを管理ポータルに追加し、グループに適切なロールと権限を割り当てます。グループ内のユーザーは、グループのロールおよび権限を継承します。詳細は、「[ユーザーの追加およびユーザー ポータル パーミッションの割り当て](#)」を参照してください。

手順15.19 ネストされたグループの作成

この手順では、グループ内にグループを作成する方法を示します。

- Red Hat Virtualization Manager がインストールされているマシンにログインします。
- 最初のグループを作成します。

```
# ovirt-aaa-jdbc-tool group add group1
```

- 2番目のグループを作成します。

```
# ovirt-aaa-jdbc-tool group add group1-1
```

- 2番目のグループを最初のグループに追加します。

```
# ovirt-aaa-jdbc-tool group-manage groupadd group1 --group=group1-1
```

- 管理ポータルに最初のグループを追加し、グループに適切なロールおよび権限を割り当てます。詳細は、「[ユーザーの追加およびユーザー ポータル パーミッションの割り当て](#)」を参照してください。

15.7.5. ユーザーおよびグループのクエリー

query モジュールを使用すると、ユーザーおよびグループ情報をクエリーできます。オプションの完全なリストについては、**ovirt-aaa-jdbc-tool query --help** を実行してください。

手順15.20 すべてのユーザーまたはグループアカウントの詳細の一覧表示

この手順では、すべてのアカウント情報を一覧表示する方法を示します。

- Red Hat Virtualization Manager がインストールされているマシンにログインします。
- ユーザーアカウントの詳細をすべて表示します。

```
# ovirt-aaa-jdbc-tool query --what=user
```

- すべてのグループアカウントの詳細を一覧表示します。

```
# ovirt-aaa-jdbc-tool query --what=group
```

手順15.21 フィルタリングされたアカウントの詳細の一覧表示

この手順では、アカウント情報を一覧表示するときにフィルターを適用する方法を示します。

- Red Hat Virtualization Manager がインストールされているマシンにログインします。
- 文字 j で始まる名前でユーザーアカウントの詳細を一覧表示します。

```
# ovirt-aaa-jdbc-tool query --what=user --pattern="name=j**"
```

- department 属性が マーケティングに設定されているグループを一覧表示します。

```
# ovirt-aaa-jdbc-tool query --what=group --pattern="department=marketing"
```

15.7.6. アカウント設定の管理

デフォルトのアカウント設定を変更するには、**ovirt-aaa-jdbc-tool** 設定 モジュールを使用します。

手順15.22 アカウント設定の更新

この手順では、デフォルトのアカウント設定を更新する方法を示します。

1. Red Hat Virtualization Manager がインストールされているマシンにログインします。
2. 次のコマンドを実行して、使用可能なすべての設定を表示します。

```
# ovirt-aaa-jdbc-tool setting show
```

3. 必要な設定を変更します。

- この例では、すべてのユーザーアカウントのデフォルトのログインセッション時間を 60 分に更新します。デフォルト値は 10080 分です。

```
# ovirt-aaa-jdbc-tool setting set --name=MAX_LOGIN_MINUTES --value=60
```

- この例では、ユーザーアカウントがロックされる前に、ユーザーが実行できるログイン試行の失敗回数を更新します。デフォルト値は 5 です。

```
# ovirt-aaa-jdbc-tool setting set --name=MAX_FAILURES_SINCE_SUCCESS --value=3
```



注記

ロックされたユーザーアカウントのロックを解除するには、**ovirt-aaa-jdbc-tool user unlock test1** を実行します。

15.8. 追加のローカルドメインの設定

デフォルトの 内部 ドメイン以外の追加のローカルドメインの作成もサポートされています。これは、**ovirt-engine-extension-aaa-jdbc** 拡張機能を使用して実行でき、外部のディレクトリーサーバーをアタッチせずに複数のドメインを作成できますが、エンタープライズ環境ではユースケースは一般的ではない場合があります。

追加で作成されたローカルドメインは、標準の Red Hat Virtualization アップグレード中に自動的にアップグレードされることではなく、将来のリリースごとに手動でアップグレードする必要があります。追加のローカルドメインの作成と、ドメインのアップグレード方法に関する詳細は、**/usr/share/doc/ovirt-engine-extension-aaa-jdbc-version/README.admin** の README ファイルを参照してください。

第16章 クオータとサービスレベル契約ポリシー

16.1. クオータの概要

クオータは、Red Hat Virtualization で提供されるリソース制限ツールです。クオータは、ユーザー権限によって設定された制限のレイヤーの上にある制限のレイヤーと考えることができます。

クオータはデータセンターオブジェクトです。

Quota を使用すると、Red Hat Virtualization 環境の管理者は、メモリー、CPU、およびストレージへのユーザーアクセスを制限できます。クオータは、管理者がユーザーに割り当てることができるメモリーリソースとストレージリソースを定義します。その結果、ユーザーは自分に割り当てられたリソースのみを利用できます。クオータリソースが使い果たされると、Red Hat Virtualization はそれ以上のユーザーアクションを許可しません。

クオータには 2 つの異なる種類があります。

表16.12 種類のクオータ

クオータタイプ	定義
実行時クオータ	このクオータは、CPU やメモリーなどのランタイムリソースの消費を制限するものです。
ストレージクオータ	このクオータは、利用可能なストレージの量を制限します。

SELinux などのクオータには 3 つのモードがあります。

表16.2 クオータモード

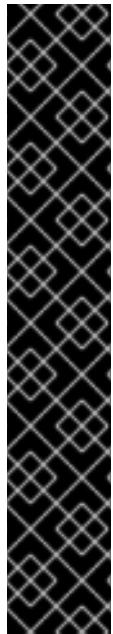
クオータモード	機能
Enforced	このモードでは、監査モードで設定したクオータが有効になり、クオータの影響を受けるグループまたはユーザーにリソースが制限されます。
Audit	このモードでは、クオータ設定を変更できます。このモードを選択して、ランタイムクオータの量と、影響を受けるユーザーが利用できるストレージクオータの量を増減します。
Disabled	このモードは、クオータによって定義されたランタイムとストレージの制限をオフにします。

ユーザーが仮想マシンを実行しようとすると、仮想マシンの仕様が、該当するクオータに設定されているストレージ許容量およびランタイム許容量と比較されます。

仮想マシンを起動すると、クオータの対象となる実行中のすべての仮想マシンの集約リソースがクオータで定義された許容量を超える場合、Manager は仮想マシンの実行を拒否します。

ユーザーが新しいディスクを作成すると、要求されたディスクサイズが、該当するクォータでカバーされる他のすべてのディスクの合計ディスク使用量に追加されます。新しいディスクが、クォータで許可されている量を超える合計ディスク使用量を取得した場合、ディスクの作成は失敗します。

クォータでは、同じハードウェアのリソース共有が可能です。ハードとソフトのしきい値をサポートします。管理者は、クォータを使用してリソースにしきい値を設定できます。これらのしきい値は、ユーザーの視点から、そのリソースの 100% 使用率として表示されます。お客様が予期せずに、このしきい値を超えた場合に発生する障害を防ぐため、インターフェイスは、しきい値を一時的に超えることができる猶予量をサポートしています。しきい値を超えると、お客様に警告が送信されます。



重要

クォータは、仮想マシンの実行時に制限をいくつか課します。これらの制限を無視すると、仮想マシンと仮想ディスクを使用できない状況が発生する可能性があります。

クォータが強制モードで実行している場合、クォータが割り当てられていない仮想マシンとディスクは使用できません。

仮想マシンの電源をオンにするには、その仮想マシンにクォータを割り当てる必要があります。

仮想マシンのスナップショットを作成するには、仮想マシンに関連付けられているディスクにクォータが割り当てられている必要があります。

仮想マシンからテンプレートを作成する場合、テンプレートで使用するクォータを選択するように求められます。これにより、テンプレート（およびテンプレートから作成される将来のすべてのマシン）が、テンプレートの生成元の仮想マシンおよびディスクとは異なるクォータを消費するように設定できます。

16.2. 共有クォータおよび個別定義されたクォータ

SuperUser 権限を持つユーザーは、個々のユーザーのクォータまたはグループのクォータを作成できます。

Active Directory ユーザーに対してグループクォータを設定することができます。10人のユーザーのグループに1TB のストレージのクォータが与えられている場合、10人のユーザーのうち1人がテラバイト全体を満たしてしまうと、グループ全体がクォータを超過してしまい、10人のユーザーのうち誰も自分のグループに関連するストレージを使用できなくなるのです。

個々のユーザーのクォータは、個々のユーザーにのみ設定されます。個々のユーザーが自分のストレージまたはランタイムクォータをすべて使い切ると、ユーザーはクォータを超え、ユーザーは自分のクォータに関連付けられたストレージを使用できなくなります。

16.3. クォータアカウンティング

クォータがコンシューマーまたはリソースに割り当てられると、そのコンシューマーによる、またはストレージ、vCPU、またはメモリーに関連するリソースに対する各アクションにより、クォータの消費またはクォータの解放が発生します。

クォータはユーザーのリソースへのアクセスを制限する上限として機能するため、クォータの計算はユーザーの実際の現在の使用とは異なる場合があります。クォータは、現在の使用量ではなく、最大増加の可能性に対して計算されます。

例16.1 アカウンティングの例

ユーザーは、1つの vCPU と 1024 MB のメモリーを備えた仮想マシンを実行します。このアクションは、そのユーザーに割り当てられた1つの vCPU と 1024 MB のクオータを消費します。仮想マシンが停止すると、1つの vCPU と 1024 MB の RAM が解放され、そのユーザーに割り当てられたクオータに戻ります。実行時のクオータ消費は、コンシューマーの実際の実行時にのみ考慮されます。

あるユーザーが 10GB の仮想シンプロビジョンディスクを作成します。実際のディスク使用量は、そのディスクのうち 3GB しか使用されていないことを示している場合があります。ただし、クォータ消費量は 10 GB であり、そのディスクの最大拡張可能性です。

16.4. データセンターにおけるクオータモードの有効化および変更

この手順では、データセンターのクオータモードを有効または変更します。クオータを定義する前に、クオータモードを選択する必要があります。この手順の手順を実行するには、管理ポータルにログインする必要があります。

監査 モードを使用してクオータをテストし、期待通りに動作することを確認します。クオータを作成または変更するには、クオータを **Audit** モードにする必要はありません。

手順16.1 データセンターでのクオータの有効化および変更

1. ナビゲーションペインの **データセンター** タブをクリックします。
2. Navigation Pane に表示されるデータセンターの一覧から、編集するクオータポリシーを持つデータセンターを選択します。
3. ナビゲーションペインの左上にある **Edit** をクリックします。
Edit Data Center ウィンドウが開きます。
4. **Quota Mode** ドロップダウンメニューで、クオータモードを **Enforced** に変更します。
5. **OK** をクリックします。

データセンターレベルでクオータモードを有効にしました。テスト中にクオータモードを **Audit** に設定した場合は、クオータ設定を有効にするためにクオータモードを **Enforced** に変更する必要があります。

16.5. 新しいクオータポリシーの作成

監査モードまたは強制モードのいずれかでクオータモードを有効にしました。データセンターのリソース使用量を管理するためのクオータポリシーを定義する必要があります。

手順16.2 新しいクオータポリシーの作成

1. ツリーモードでは、データセンターを選択します。 **Quota** タブがナビゲーションペインに表示されます。
2. ナビゲーションペインの **Quota** タブをクリックします。
3. ナビゲーションメニューで **Add** をクリックします。 **New Quota** ウィンドウが開きます。
4. **Name** フィールドに意味のある名前を入力します。

Description フィールドに意味のある名前を入力します。

5. **New Quota** ウィンドウの **Memory & CPU** セクションで、緑色のスライダーを使用して **Cluster Threshold** を設定します。
6. **New Quota** ウィンドウの **Memory & CPU** セクションで、青いスライダーを使用して **Cluster Grace** を設定します。
7. **All Clusters** または **Specific Clusters** ラジオボタンを選択します。 **Specific Clusters** を選択した場合は、クォータポリシーを追加するクラスターのチェックボックスを選択します。
8. **Edit** をクリックして **Edit Quota** ウィンドウを開きます。
9. **Memory** フィールドで、**Unlimited** ラジオボタン（クラスターでメモリリソースを無制限に使用できるようにする）を選択するか、**limit to** ラジオボタンを選択して、このクォータで設定されたメモリー量を設定します。**limit to** ラジオボタンを選択した場合は、**MB** フィールドにメモリークォータをメガバイト(MB)で入力します。
10. **CPU** フィールドで、**Unlimited** ラジオボタンまたは **limit to** ラジオボタンのいずれかを選択して、このクォータで設定されたCPUの量を設定します。**limit to** ラジオボタンを選択した場合は、**vCpus** フィールドにvCPUの数を入力します。
11. **Edit Quota** ウィンドウで **OK** をクリックします。
12. **New Quota** ウィンドウの **Storage** セクションで、緑色のスライダーを使用して **Storage Threshold** を設定します。
13. **New Quota** ウィンドウの **Storage** セクションで、青色のスライダーを使用して **Storage Grace** を設定します。
14. **All Storage Domains** または **Specific Storage Domains** ラジオボタンを選択します。 **Specific Storage Domains** を選択した場合は、クォータポリシーを追加するストレージドメインのチェックボックスを選択します。
15. **Edit** をクリックして **Edit Quota** ウィンドウを開きます。
16. **Storage Quota** フィールドで、**Unlimited** ラジオボタン（ストレージの無制限使用を許可する）または **limit to** ラジオボタンを選択して、クォータがユーザーを制限するストレージの量を設定します。**limit to** ラジオボタンを選択した場合は、**GB** フィールドにストレージクォータサイズをギガバイト(GB)で入力します。
17. **Edit Quota** ウィンドウで **OK** をクリックします。 **New Quota** ウィンドウに戻ります。
18. **New Quota** ウィンドウで **OK** をクリックします。

結果

新しいクォータポリシーを作成している。

16.6. クォータしきい値の設定の説明

表16.3 クォータしきい値および猶予期間

設定	定義
----	----

設定	定義
クラスターしきい値	データセンターごとに利用可能なクラスターリソースの量。
クラスターの猶予	データセンターのクラスターしきい値を使い切った後のデータセンターで利用可能なクラスターの量。
ストレージのしきい値	データセンターごとに利用可能なストレージリソースの量。
ストレージの猶予	データセンターのストレージしきい値を使い切った後のデータセンターで利用可能なストレージの量。

クオータが 20% の猶予で 100 GB に設定されている場合、使用者は 120 GB のストレージを使用した後、ストレージの使用をブロックされます。同じクオータのしきい値が 70% に設定されている場合、使用者は 70 GB のストレージ消費量を超えると警告を受け取ります(ただし、120 GB のストレージ消費量に達するまでストレージを消費できます)。しきい値および猶予の両方は、クオータを基準にして設定されます。しきい値はソフト制限と考えることができます。それを超えると警告が生成されます。猶予はハード制限として考えられ、それを超えると、これ以上ストレージリソースを消費できなくなります。

16.7. オブジェクトへのクオータの割り当て

概要

この手順では、仮想マシンをクオータに関連付ける方法を説明します。

手順16.3 仮想マシンへのクオータの割り当て

- ナビゲーションペインで、クオータを追加する予定の仮想マシンを選択します。
- Edit** をクリックします。Edit Virtual Machine ウィンドウが表示されます。
- 仮想マシンが消費するクオータを選択します。これを行うには、Quota ドロップダウンを使用します。
- OK** をクリックします。

結果

選択した仮想マシンのクオータを指定している。

概要

この手順では、仮想ディスクをクオータに関連付ける方法を説明します。

手順16.4 仮想ディスクへのクオータの割り当て

- ナビゲーションペインで、クオータを追加する予定のディスクがある仮想マシンを選択します。
- 詳細ペインで、クオータに関連付ける予定のディスクを選択します。

3. **Edit** をクリックします。Edit Virtual Disk ウィンドウが表示されます。
4. 仮想ディスクが消費するクオータを選択します。
5. **OK** をクリックします。

結果

選択した仮想ディスクのクオータを指定している。



重要

仮想マシンを機能させるには、仮想マシンに関連付けられているすべてのオブジェクトに対してクオータを選択する必要があります。仮想マシンに関連付けられているオブジェクトのクオータを選択しないと、仮想マシンは機能しません。この状況で Manager が出力するエラーは一般的なものであり、仮想マシンに関連付けられているすべてのオブジェクトにクオータを関連付けていないため、エラーが出力されたかどうかを判断するのは困難です。クオータが割り当てられていない仮想マシンのスナップショットを作成することはできません。仮想ディスクにクオータが割り当てられていない仮想マシンのテンプレートを作成することはできません。

16.8. クオータを使用してユーザーごとにリソースを制限する

概要

この手順では、クオータを使用して、ユーザーがアクセスできるリソースを制限する方法について説明します。

手順16.5 クオータへのユーザーの割り当て

1. ツリーで、ユーザーに関連付けるクオータを持つデータセンターをクリックします。
2. ナビゲーションペインで **Quota** タブをクリックします。
3. ナビゲーションペインのリストでターゲットクオータを選択します。
4. 詳細ペインの **Consumers** タブをクリックします。
5. 詳細ペインの上部にある **Add** をクリックします。
6. 検索 フィールドに、クオータに関連付けるユーザーの名前を入力します。
7. **GO** をクリックします。
8. ターゲットユーザーの名前を含む行の左側にあるチェックボックスを選択します。
9. Assign Users and Groups to Quota ウィンドウの右下にある **OK** をクリックします。

結果

しばらくすると、ユーザーは詳細ペインの **Consumers** タブに表示されます。

16.9. クオータの編集

概要

この手順では、既存のクォータを変更する方法について説明します。

手順16.6 クォータの編集

1. ツリーペインで、クォータを編集するデータセンターをクリックします。
2. ナビゲーションペインの **Quota** タブをクリックします。
3. 編集するクォータの名前をクリックします。
4. ナビゲーションペインで **編集** をクリックします。
5. **Edit Quota** ウィンドウが開きます。必要に応じて、**Name** フィールドに意味のある名前を入力します。
6. 必要に応じて、**Description** フィールドに意味のある説明を入力できます。
7. **All Clusters** ラジオボタンまたは **Specific Clusters** ラジオボタンを選択します。**Cluster Threshold** および **Cluster Grace** スライダーを、メモリーと CPU スライダー上の希望の位置に移動します。
8. **All Storage Domains** ラジオボタンまたは **Specific Storage Domains** ラジオボタンを選択します。**Storage Threshold** および **Storage Grace** スライダーを **Storage** スライダー上の希望の位置に移動します。
9. **Edit Quota** ウィンドウで **OK** をクリックし、新しいクォータ設定を確認します。

結果

既存のクォータを変更している。

16.10. クォータの削除

概要

この手順では、クォータを削除する方法について説明します。

手順16.7 クォータの削除

1. ツリーペインで、クォータを編集するデータセンターをクリックします。
2. ナビゲーションペインの **Quota** タブをクリックします。
3. 削除するクォータの名前をクリックします。
4. タブ行の下にあるナビゲーションペインの上部にある **削除** をクリックします。
5. **Remove Quota (s)** ウィンドウで **OK** をクリックして、このクォータの削除を確認します。

結果

クォータを削除しました。

16.11. サービスレベルアグリーメントポリシーの実施

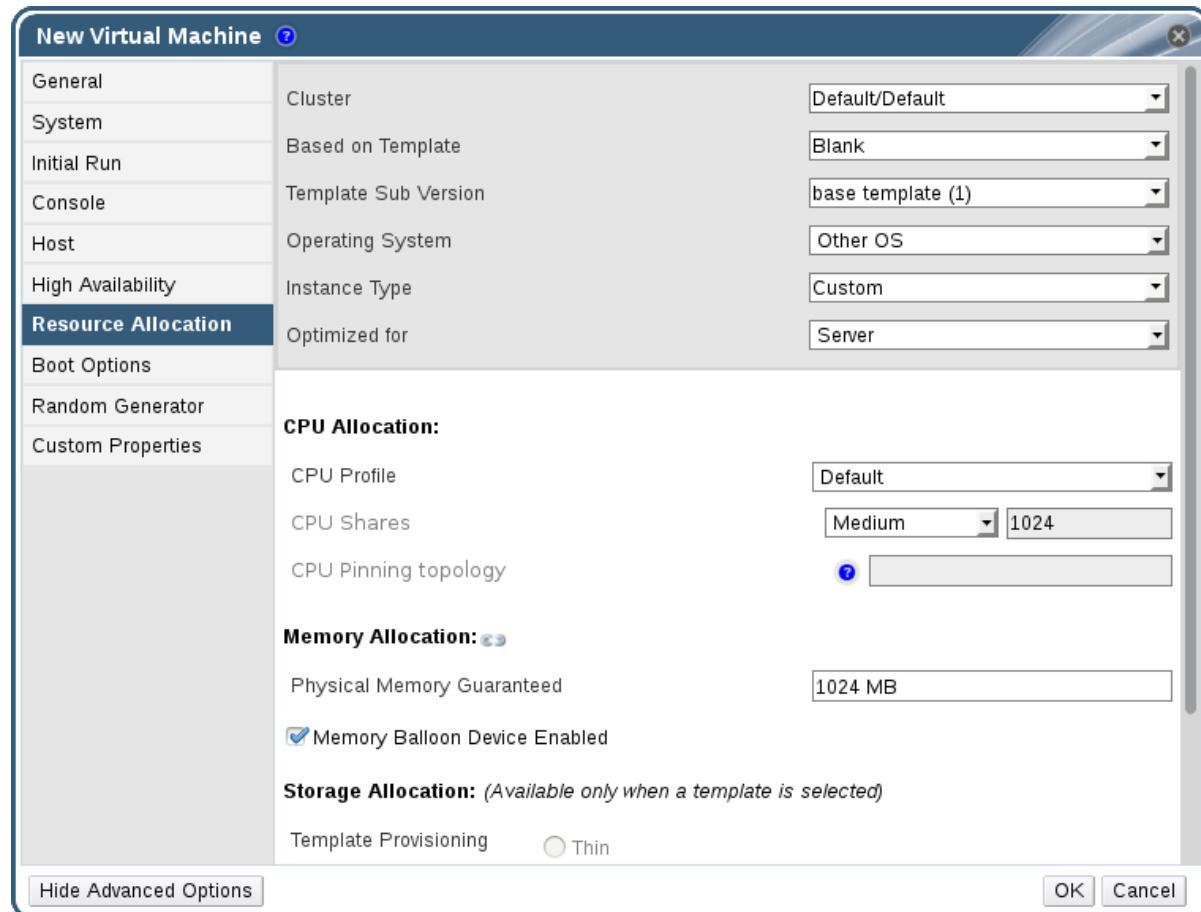
概要

この手順では、サービスレベルアグリーメントの CPU 機能を設定する方法について説明します。

手順16.8 サービスレベルアグリーメントの CPU ポリシーの設定

1. ナビゲーションパネルで **New VM** を選択します。
2. **Show Advanced Options** を選択します。
3. **Resource Allocation** タブを選択します。

図16.1 サービスレベルアグリーメントポリシーの適用 - CPU 割り当てメニュー



4. **CPU 共有** を指定します。可能なオプションは、**Low**、**Medium**、**High**、**Custom**、および**Disabled** です。**High** に設定された仮想マシンは、**Medium** の 2 倍の共有を受け取り、**Medium** に設定された仮想マシンは、**Low** に設定された仮想マシンの 2 倍の共有を受け取ります。**disabled** では、VDSM が共有の異議申し立てを決定するために古いアルゴリズムを使用するように指示を出します。通常、これらの条件で異議申し立てられたファイル共有の数は 1020 です。

結果

サービスレベルアグリーメントの CPU ポリシーを設定している。ユーザーの CPU 消費は、設定したポリシーで制御されるようになりました。

第17章 イベント通知

17.1. 管理ポータルでのイベント通知の設定

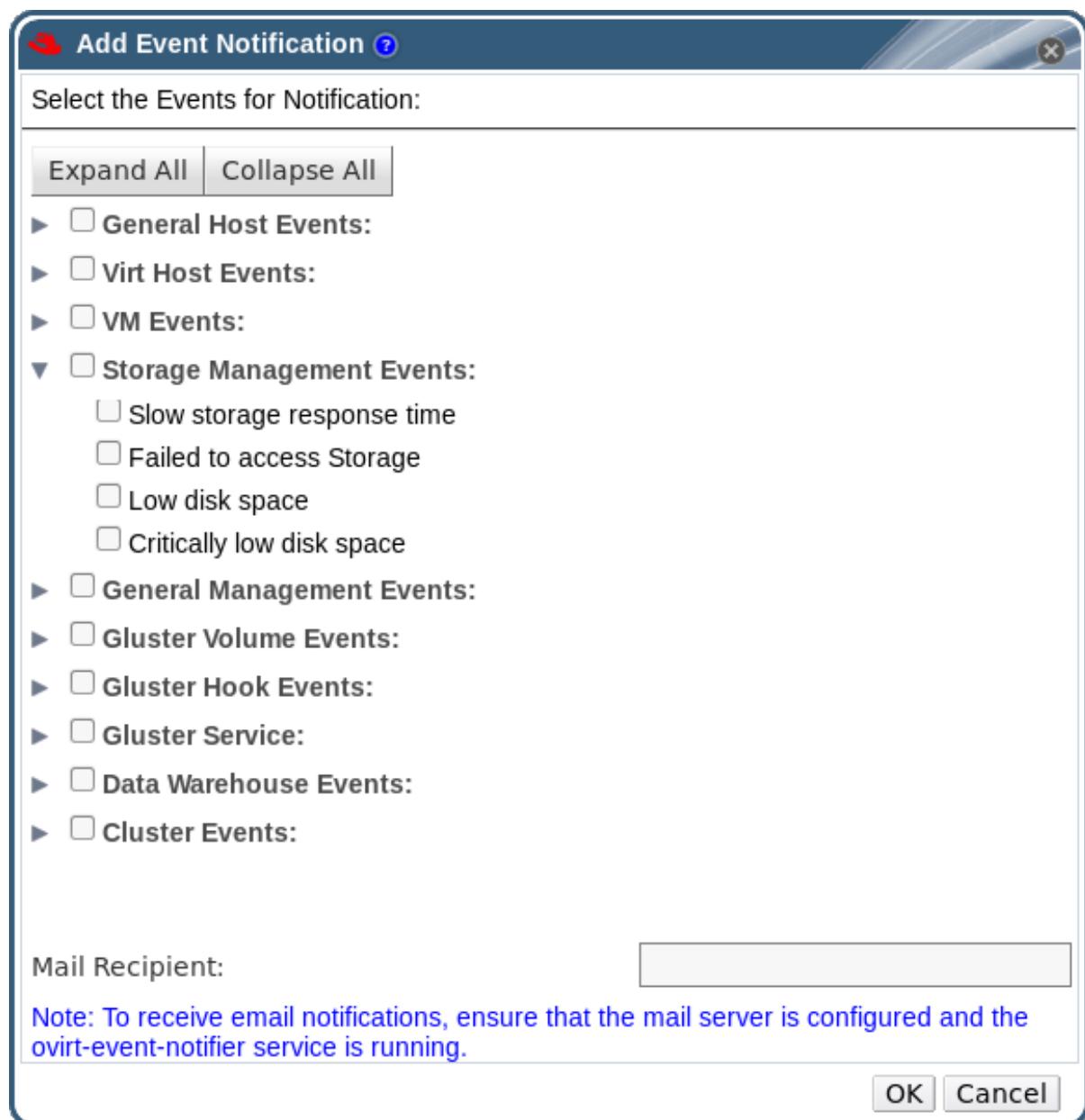
概要

Red Hat Virtualization Manager は、Red Hat Virtualization Manager が管理する環境で特定のイベントが発生したときに、指定されたユーザーに電子メールで通知できます。この機能を使用するには、メッセージを配信するようにメール転送エージェントを設定する必要があります。管理ポータルから設定できるのは、メール通知のみです。SNMP トラップは Manager マシンで設定する必要があります。

手順17.1 イベント通知の設定

1. 適切な変数でメール転送エージェントを設定していることを確認します。
2. **Users** resource タブ、ツリーモード、または検索機能を使用して、イベント通知の送信先となるユーザーを見つけて選択します。
3. 詳細ペインの **Event Notifier** タブをクリックして、ユーザーに通知されるイベントを一覧表示します。この一覧は、そのユーザーのイベント通知を設定していない場合は空白になります。
4. **Manage Events** をクリックし、**Add Event Notification** ウィンドウを開きます。

図17.1 Add Events Notification ウィンドウ



5. イベントを表示するには、**Expand All** ボタンまたはサブジェクト固有の展開ボタンを使用します。
6. 適切なチェックボックスを選択します。
7. **Mail Recipient** フィールドにメールアドレスを入力します。
8. **OK** をクリックして変更を保存し、ウィンドウを閉じます。
9. Red Hat Virtualization Manager で **ovirt-engine-notifier** サービスを追加し、起動します。これにより、加えた変更が有効になります。

```
# systemctl daemon-reload
# systemctl enable ovirt-engine-notifier.service
# systemctl restart ovirt-engine-notifier.service
```

結果

指定されたユーザーは、Red Hat Virtualization 環境のイベントに基づいて電子メールを受け取るようになりました。選択したイベントは、そのユーザーの **Event Notifier** タブに表示されます。

17.2. 管理ポータルでのイベント通知のキャンセル

概要

ユーザーが不要な電子メール通知を設定していて、それらをキャンセルしたいと考えています。

手順17.2 イベント通知の取り消し

1. **Users** タブで、ユーザーまたはグループを選択します。
2. 詳細ペインの **Event Notifier** タブを選択して、ユーザーがメール通知を受信するイベントを一覧表示します。
3. **Manage Events** をクリックし、**Add Event Notification** ウィンドウを開きます。
4. イベントを表示するには、**Expand All** ボタン、またはサブジェクト固有の展開ボタンを使用します。
5. 該当するチェックボックスをオフになると、そのイベントの通知が解除されます。
6. **OK** をクリックして変更を保存し、ウィンドウを閉じます。

結果

ユーザーの不要なイベント通知をキャンセルしている。

17.3. OVIRT-ENGINE-NOTIFIER.CONF のイベント通知のパラメーター

イベント通知設定ファイルは、`/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf` にあります。

表17.1 ovirt-engine-notifier.conf variables

変数名	デフォルト	備考
SENSITIVE_KEYS	none	ログに記録されないキーのコンマ区切りのリスト。
JBOSS_HOME	/opt/rh/eap7/root /usr/share/wildfly /	Manager が使用する JBoss アプリケーションサーバーの場所。
ENGINE_ETC	/etc/ovirt-engine	Manager が使用する etc ディレクトリーの場所。
ENGINE_LOG	/var/log/ovirt-engine	Manager が使用する logs ディレクトリーの場所。
ENGINE_USR	/usr/share/ovirt-engine	Manager が使用する usr ディレクトリーの場所。

変数名	デフォルト	備考
ENGINE_JAVA_MODULEPATH	<code> \${ENGINE_USR}/modules</code>	JBoss モジュールが追加されるファイルパス。
NOTIFIER_DEBUG_ADDRESS	none	通知機能が使用する Java 仮想マシンのリモートデバッグを実行するために使用できるマシンのアドレス。
NOTIFIER_STOP_TIME	30	サービスがタイムアウトするまでの時間(秒単位)。
NOTIFIER_STOP_INTERVAL	1	タイムアウトカウンターをインクリメントする時間(秒)。
INTERVAL_IN_SECONDS	120	サブスクリーバーにメッセージをディスパッチするインスタンス間の間隔(秒単位)。
IDLE_INTERVAL	30	低優先度タスクが実行される間隔(秒単位)。
DAYS_TO_KEEP_HISTORY	0	この変数は、ディスパッチされたイベントが履歴テーブルに保持される日数を設定します。この変数が設定されていない場合、イベントは履歴テーブルに無期限に残ります。
FAILED_QUERIES_NOTIFICATION_THRESHOLD	30	通知メールが送信された後に失敗したクエリーの数。通知メールは、通知のフェッチに最初に失敗した後、この変数で指定された失敗の数に到達するたびに1回送信されます。 0 または 1 を指定した場合は、失敗するたびに電子メールが送信されます。
FAILED_QUERIES_NOTIFICATION_RECIPIENTS	none	通知メールの送信先となる受信者のメールアドレス。メールアドレスはコンマで区切る必要があります。この項目は、 FILTER 変数によって非推奨とされました。
DAYSTOSENDONSTARTUP	0	通知機能の開始時に処理および送信される古いイベントの日数。

変数名	デフォルト	備考
FILTER	exclude:*	電子メール通知のトリガーと受信者を決定するために使用されるアルゴリズム。この変数の値は、 include または exclude 、 event 、および recipient の組み合わせから設定される。たとえば、 include:VDC_START(smtp:mail@example.com) \${FILTER} ようになります。
MAIL_SERVER	none	SMTP メールサーバーアドレス。必須。
MAIL_PORT	25	通信に使用されるポート。使用できる値には、プレーン SMTP の場合は 25 、SSL を使用した SMTP の場合は 465 、および TLS を使用した SMTP の場合は 587 が含まれます。
MAIL_USER	none	ユーザー認証のために SSL が有効な場合は、この変数を設定する必要があります。この変数は、MAIL_FROM 変数が設定されていない場合に from ユーザーアドレスを指定するためにも使用されます。一部のメールサーバーでは、この機能をサポートしていません。アドレスは RFC822 形式です。
SENSITIVE_KEYS	\${SENSITIVE_KEY} S},MAIL_PASSWORD	メールサーバーで認証が必要な場合、または SSL または TLS が有効になっている場合は、ユーザーを認証するために必要です。
MAIL_PASSWORD	none	メールサーバーで認証が必要な場合、または SSL または TLS が有効になっている場合は、ユーザーを認証するために必要です。
MAIL_SMTP_ENCRYPTION	none	通信に使用する暗号の種類を指定します。可能な値は none 、 ssl 、 tls です。
HTML_MESSAGE_FORMAT	false	この変数が true に設定されている場合、メールサーバーは HTML フォーマットでメッセージを送信します。
MAIL_FROM	none	この変数は、メールサーバーでサポートされている場合、RFC822 形式で送信者アドレスを指定します。

変数名	デフォルト	備考
MAIL_REPLY_TO	none	この変数は、メールサーバーでサポートされている場合、送信メールの返信先アドレスを RFC822 形式で指定します。
MAIL_SEND_INTERVAL	1	IDLE_INTERVAL ごとに送信される SMTP メッセージの数
MAIL_RETRIES	4	失敗する前に電子メールの送信を試行する回数。
SNMP_MANAGER	none	SNMP マネージャーとして機能するマシンの IP アドレスまたは完全修飾ドメイン名。エントリーはスペースで区切る必要があります。ポート番号を含めることができます。たとえば、 manager1.example.com manager2.example.com:164 です。
SNMP_COMMUNITY	public	デフォルトの SNMP コミュニティー。
SNMP_OID	1.3.6.1.4.1.2312.13.1.1	アラートのデフォルトのトラップオブジェクト識別子。この OID が定義されると、すべてのトラップタイプがイベント情報とともに SNMP マネージャーに送信されます。デフォルトのトラップを変更すると、生成されたトラップが Manager の管理情報ベースに準拠するのを防ぎます。
ENGINE_INTERVAL_IN_SECONDS	300	Manager がインストールされているマシンを監視する間隔(秒単位)。間隔は、監視が完了した時点から測定されます。
ENGINE_MONITOR_RETRIES	3	通知機能が、障害後の指定された間隔で Manager がインストールされているマシンのステータスを監視しようとする回数。
ENGINE_TIMEOUT_IN_SECONDS	30	通知機能が障害後に指定された間隔で Manager がインストールされているマシンの状況を監視しようとするまで待機する時間(秒単位)。
IS_HTTPS_PROTOCOL	false	JBoss がセキュアモードで実行されている場合、このエントリーは true に設定する必要があります。
SSL_PROTOCOL	TLS	SSL が有効な場合に JBoss Configuration コネクターが使用するプロトコル。

変数名	デフォルト	備考
SSL_IGNORE_CERTIFICATE_ERRORS	false	JBoss がセキュアモードで実行しており、SSL エラーを無視する場合は、この値を true に設定する必要があります。
SSL_IGNORE_HOST_VERIFICATION	false	JBoss がセキュアモードで実行しており、ホスト名の検証が無視される場合は、この値を true に設定する必要があります。
REPEAT_NON_RESPONSIVE_NOTIFICATION	false	この変数は、Manager がインストールされているマシンが応答しない場合に、繰り返し失敗メッセージをサブスクリーバーに送信するかどうかを指定します。
ENGINE_PID	/var/lib/ovirt-engine/ovirt-engine.pid	Manager の PID のパスおよびファイル名。

17.4. SNMP トラップを送信するための RED HAT VIRTUALIZATION MANAGER の設定

Simple Network Management Protocol トラップを1つ以上の外部 SNMP マネージャーに送信するように Red Hat Virtualization Manager を設定します。SNMP トラップには、システムイベント情報が含まれます。これらは、Red Hat Virtualization 環境を監視するために使用されます。SNMP マネージャーに送信されるトラップの数およびタイプは、Red Hat Virtualization Manager 内で定義できます。

この手順では、トラップを受信するように1つ以上の外部 SNMP マネージャーを設定し、以下の情報をすることを前提としています。

- SNMP マネージャーとして機能するマシンの IP アドレスまたは完全修飾ドメイン名。必要に応じて、マネージャーがトラップ通知を受け取るポートを決定します。デフォルトでは UDP ポート 162 です。
- SNMP コミュニティ。複数の SNMP マネージャーは単一のコムニティに所属できます。管理システムとエージェントは、同じコムニティ内にある場合にのみ通信できます。デフォルトのコムニティは **public** です。
- アラートのトラップオブジェクト識別子。Red Hat Virtualization Manager は、デフォルトの OID 1.3.6.1.4.1.2312.13.1.1 を提供します。この OID が定義されると、すべてのトラップタイプがイベント情報とともに SNMP マネージャーに送信されます。デフォルトのトラップを変更すると、生成されたトラップが Manager の管理情報ベースに準拠するのを防ぎます。



注記

Red Hat Virtualization Manager は、**/usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt** および **/usr/share/doc/ovirt-engine/mibs/REDHAT-MIB.txt** で管理情報ベースを提供します。続行する前に、SNMP マネージャーに MIB を読み込みます。

デフォルトの SNMP 設定値は、Manager のイベント通知デーモン設定ファイル **/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf** にあります。次の手順で概説する値

は、このファイルで提供されているデフォルト値またはサンプル値に基づいています。**ovirt-engine-notifier.conf** ファイルを編集するのではなく、オーバーライドファイルを定義して、アップグレードなどのシステムの変更後も設定オプションを保持することが推奨されます。

手順17.3 Manager での SNMP トラップの設定

- Manager で SNMP 設定ファイルを作成します。

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

- SNMP マネージャー、SNMP コミュニティー、および OID を以下の形式で指定します。

```
SNMP_MANAGER="manager1.example.com manager2.example.com:162"
SNMP_COMMUNITY=public
SNMP_OID=1.3.6.1.4.1.2312.13.1.1
```

- SNMP マネージャーに送信するイベントを定義します。

例17.1 イベントの例

すべてのイベントをデフォルトの SNMP プロファイルに送信します。

```
FILTER="include:*(snmp:) ${FILTER}"
```

重大度 **ERROR** または **ALERT** のすべてのイベントをデフォルトの SNMP プロファイルに送信します。

```
FILTER="include:ERROR(snmp:) ${FILTER}"
```

```
FILTER="include:ALERT(snmp:) ${FILTER}"
```

VDC_START のイベントを指定されたメールアドレスに送信します。

```
FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"
```

VDC_START 以外のすべてのイベントをデフォルトの SNMP プロファイルに送信します。

```
FILTER="exclude:VDC_START include:*(snmp:) ${FILTER}"
```

これは、**ovirt-engine-notifier.conf** で定義されるデフォルトのフィルターです。このフィルターを無効にしたり上書きフィルターを適用しないと、通知は送信されません。

```
FILTER="exclude:*
```

VDC_START は、使用可能な監査ログメッセージの例です。監査ログメッセージの完全なリストは、**/usr/share/doc/ovirt-engine/AuditLogMessages.properties** にあります。または、SNMP マネージャー内で結果をフィルタリングします。

- ファイルを保存します。

- ovirt-engine-notifier** サービスを開始し、このサービスが起動時に開始することを確認します。

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

SNMP マネージャーをチェックして、トラップを受け取っていることを確認します。



注記

通知サービスを実行するには、**SNMP_MANAGER**、**MAIL_SERVER**、またはその両方を **/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf** またはオーバーライドファイルで適切に定義する必要があります。

第18章 ユーティリティー

18.1. oVIRT エンジンの名前変更ツール

18.1.1. oVirt エンジンの名前変更ツール

engine-setup コマンドをクリーンな環境で実行すると、コマンドは、セットアッププロセス中に提供された Manager の完全修飾ドメイン名を使用する多数の証明書およびキーを生成します。Manager の完全修飾ドメイン名を後で変更する必要がある場合(たとえば、Manager をホストしているマシンを別のドメインに移行したため)、完全修飾ドメイン名のレコードを更新して、新しい名前を反映する必要があります。**ovirt-engine-rename** コマンドは、このタスクを自動化します。

ovirt-engine-rename コマンドは、以下の場所にある Manager の完全修飾ドメイン名のレコードを更新します。

- /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
- /etc/ovirt-engine/imageuploader.conf.d/10-engine-setup.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

ovirt-engine-rename コマンドは、Manager が実行される Web サーバーの新しい証明書を作成しますが、エンジンや認証局の証明書には影響しません。このため、特に Red Hat Enterprise Virtualization 3.2 以前からアップグレードされた環境では、**ovirt-engine-rename** コマンドの使用に伴うリスクがあります。したがって、可能な場合は **engine-cleanup** および **engine-setup** を実行して Manager の完全修飾ドメイン名を変更することが推奨されます。

18.1.2. oVirt Engine Rename コマンドの構文

ovirt-engine-rename コマンドの基本的な構文は次のとおりです。

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

このコマンドは、次のオプションも受け入れます。

--newname=[new name]

ユーザーの操作なしで、Manager の新しい完全修飾ドメイン名を指定できます。

--log=[file]

名前変更操作のログが書き込まれるファイルのパスおよび名前を指定できます。

--config=[file]

名前変更操作にロードする設定ファイルのパスおよびファイル名を指定できます。

--config-append=[file]

名前変更操作に追加する設定ファイルのパスおよびファイル名を指定できます。このオプションを使用して、応答ファイルのパスおよびファイル名を指定できます。

--generate-answer=[file]

応答先となるファイルのパスとファイル名を指定でき、**ovirt-engine-rename** コマンドで変更された値が記録されます。

18.1.3. oVirt エンジンの名前変更ツールの使用

概要

ovirt-engine-rename コマンドを使用して、Manager の完全修飾ドメイン名のレコードを更新できます。

このツールは、Manager がローカル ISO またはデータストレージドメインを提供しているかどうかを確認します。その場合、ツールは、操作を続行する前に、ストレージに接続されている仮想マシンまたはストレージドメインをイジェクト、シャットダウン、またはメンテナンスマードにするようにユーザーに促します。これにより、仮想マシンが仮想ディスクとの接続を失うことがなくなり、名前の変更プロセス中に ISO ストレージドメインが接続を失うのを防ぐことができます。

手順18.1 Red Hat Virtualization Manager の名前変更

1. 新しい完全修飾ドメイン名に、DNS およびその他の関連するレコードをすべて準備します。
2. DHCP を使用している場合は、DHCP サーバーの設定を更新します。
3. Manager のホスト名を更新します。
4. 以下のコマンドを実行します。

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

5. プロンプトが表示されたら、**Enter** を押してエンジンサービスを停止します。

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

6. プロンプトが表示されたら、Manager の新しい完全修飾ドメイン名を入力します。

```
New fully qualified server name:[new name]
```

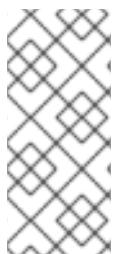
結果

ovirt-engine-rename コマンドは、Manager の完全修飾ドメイン名のレコードを更新します。

18.2. エンジン設定ツール

18.2.1. エンジン設定ツール

エンジン設定ツールは、Red Hat Virtualization 環境のグローバル設定を設定するためのコマンドラインユーティリティーです。このツールは、エンジンデータベースに格納されているキーと値のマッピングのリストと対話し、個々のキーの値を取得して設定し、使用可能なすべての設定キーおよび値のリストを取得できるようにします。さらに、Red Hat Virtualization 環境の設定レベルごとに異なる値を保管できます。



注記

設定キーの値を取得または設定するために、Red Hat Virtualization Manager も Red Hat JBoss Enterprise Application Platform も実行している必要はありません。設定キー値とキーのマッピングはエンジンデータベースに保存されるため、**postgresql** サービスの実行中に更新することができます。その後、**ovirt-engine** サービスが再起動されたときに変更が適用されます。

18.2.2. engine-config コマンドの構文

Red Hat Virtualization Manager がインストールされているマシンからエンジン設定ツールを実行することができます。使用方法の詳細については、そのコマンドのヘルプ出力を印刷してください。

```
# engine-config --help
```

一般的なタスク:

使用可能な設定キーを一覧表示します

```
# engine-config --list
```

使用可能な設定値を一覧表示します。

```
# engine-config --all
```

設定キーの値を取得します。

```
# engine-config --get [KEY_NAME]
```

[KEY_NAME] を優先キーの名前に置き換えて、指定されたバージョンのキーの値を取得します。--cver パラメーターを使用して、取得する値の設定バージョンを指定します。バージョンを指定しない場合は、既存のすべてのバージョンの値が返されます。

キーの設定値を設定します。

```
# engine-config --set [KEY_NAME]=[KEY_VALUE] --cver=[VERSION]
```

[KEY_NAME] を設定する特定のキーの名前に置き換え、[KEY_VALUE] を設定する値に置き換えます。複数の設定バージョンがある環境では、[VERSION] を指定する必要があります。

変更を読み込むために ovirt-engine サービスを再起動します。

変更を有効にするには、ovirt-engine サービスを再起動する必要があります。

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

18.3. イメージアップローダーツール

18.3.1. イメージアップローダーツール

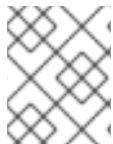


注記

エクスポートストレージドメインは非推奨になりました。ストレージデータドメインはデータセンターから接続を解除し、同じ環境または別の環境にある別のデータセンターにインポートすることができます。仮想マシン、フローティング仮想ディスクイメージ、およびテンプレートは、インポートされたストレージドメインからアタッチされたデータセンターにアップロードできます。ストレージドメインのインポートに関する詳細は、「[既存のストレージドメインのインポート](#)」を参照してください。

engine-image-uploader コマンドを使用すると、エクスポートストレージドメインを一覧表示し、OVF または OVA 形式の仮想マシンイメージをエクスポートストレージドメインにアップロードし、Red Hat Virtualization Manager で自動的に認識できます。

OVA は OVF ファイルの tar アーカイブです。



注記

イメージアップローダーは、Red Hat Virtualization によって作成された gzip 圧縮 OVF ファイルまたは OVA ファイルのみをサポートします。

OVF には、以下の形式のイメージとマスター・ディレクトリーが含まれています。

```

|-- images
|   |-- [Image Group UUID]
|       |--- [Image UUID (this is the disk image)]
|       |--- [Image UUID (this is the disk image)].meta
|-- master
|   |--vms
|       |--- [UUID]
|           |--- [UUID].ovf

```

18.3.2. engine-image-uploader コマンドの構文

イメージアップローダーコマンドの基本的な構文は以下の通りです。

```

engine-image-uploader [options] list
engine-image-uploader [options] upload [file].[file]...[file]

```

イメージアップローダーコマンドは、*list* および *upload* の 2 つのアクションをサポートします。

- *list* アクションは、イメージをアップロードできるエクスポートストレージドメインを一覧表示します。
- *upload* アクションは、指定したエクスポートストレージドメインにイメージをアップロードします。

イメージアップローダーコマンドを使用する場合は、上記のアクションのいずれかを指定する必要があります。さらに、アップロードアクションを使用するには、少なくとも 1 つのローカルファイルを指定する必要があります。

engine-image-uploader コマンドをさらに絞り込むためのいくつかのパラメーターがあります。これらのパラメーターのデフォルトは、**/etc/ovirt-engine/imageuploader.conf** ファイルで設定できます。

一般的なオプション

-h, --help

イメージアップローダーコマンドの使用方法に関する情報を表示します。

--conf-file=[PATH]

コマンドが使用する設定ファイルとして [PATH] を設定します。デフォルトは **etc/ovirt-engine/imageuploader.conf** です。

--log-file=[PATH]

[PATH] をログ出力の書き込みに使用する特定のファイル名として設定します。デフォルトは **/var/log/ovirt-engine/ovirt-image-uploader/ovirt-image-uploader-[date].log** です。

--cert-file=[PATH]

[PATH] をエンジンを検証する証明書として設定します。デフォルトは **/etc/pki/ovirt-engine/ca.pem** です。

--insecure

エンジンの検証を試行しないことを指定します。

--quiet

quiet モードを設定し、コンソール出力を最小限に抑えます。

-v, --verbose

verbose モードを設定し、より多くのコンソール出力を提供します。

-f, --force

アップロードするソースファイルのファイル名が宛先エクスポートドメインの既存ファイルと同じ場合は、強制モードが必要です。このオプションでは、既存のファイルを強制的に上書きします。

Red Hat Virtualization Manager のオプション

-u [USER], --user=[USER]

コマンドの実行に認証情報が使用されるユーザーを指定します。[USER] は、[username]@[domain] の形式で指定されます。ユーザーは指定のドメインに存在し、Red Hat Virtualization Manager に認識されている必要があります。

-r [FQDN], --engine=[FQDN]

イメージをアップロードする Red Hat Virtualization Manager の IP アドレスまたは完全修飾ドメイン名を指定します。イメージアップローダーは、Red Hat Virtualization Manager がインストールされているのと同じマシンから実行されていると想定されています。デフォルト値は **localhost:443** です。

ストレージドメインのエクスポートオプション

次のオプションは、イメージをアップロードするエクスポートドメインを指定します。これらのオプションと一緒に使用することはできません。-e オプションまたは -n オプションのいずれかを使用する必要があります。

-e [EXPORT_DOMAIN], --export-domain=[EXPORT_DOMAIN]

ストレージドメイン EXPORT_DOMAIN をアップロードの宛先として設定します。

-n [NFSSERVER], --nfs-server=[NFSSERVER]

アップロードの宛先として NFS パス [NFSSERVER] を設定します。

インポートオプション

次のオプションを使用すると、イメージがエクスポートドメインにアップロードされるときに、アップロードされるイメージの属性をカスタマイズできます。

-i, --ovf-id

イメージの UUID が更新されないことを指定します。デフォルトでは、コマンドはアップロードされるイメージ用に新しい UUID を生成します。これにより、アップロードするイメージの ID と環境にすでにあるイメージとの間に競合が発生しなくなります。

-d, --disk-instance-id

イメージ内の各ディスクのインスタンス ID の名前が変更されないことを指定します。デフォルトでは、コマンドはアップロードされるイメージ内のディスク用に新しい UUID を生成します。これにより、アップロードするイメージ上のディスクと環境にすでにあるディスクとの間に競合が発生しなくなります。

-m, --mac-address

イメージ内のネットワークコンポーネントがイメージから削除されないことを指定します。デフォルトでは、コマンドは、アップロード中のイメージからネットワークインターフェイスカードを削除し、環境にある他の仮想マシンのネットワークカードとの競合を防ぎます。このオプションを使用しない場合には、管理ポータルを使用して新たにインポートされたイメージにネットワークインターフェイスカードを追加できます。また、Manager は MAC アドレスの競合がないことを確認できます。

-N [NEW_IMAGE_NAME], --name=[NEW_IMAGE_NAME]

アップロードするイメージの新しい名前を指定します。

18.3.3. イメージアップローダーと互換性のある OVF アーカイブの作成

概要

engine-image-uploader ツールを使用してアップロードできるファイルを作成できます。

手順18.2 イメージアップローダーと互換性のある OVF アーカイブの作成

- Manager を使用して空のエクスポートドメインを作成します。空のエクスポートドメインを使用すると、どのディレクトリーに仮想マシンが含まれているかを簡単に確認できます。
- 作成した空のエクスポートドメインに仮想マシンをエクスポートします。
- エクスポートドメインとして機能するストレージサーバーにログインし、NFS 共有のルートを見つけ、そのマウントポイントの下にある サブディレクトリーに変更します。新しいエクスポートドメインから開始しましたが、エクスポートされるディレクトリーには1つのディレクトリーのみがあります。これには、**images/** および **master/** ディレクトリーが含まれます。
- tar -zcvf my.ovf images/ master/** コマンドを実行して、tar/gzip OVF アーカイブを作成します。
- 作成された OVF ファイルを（この例では **my.ovf**）に付与すると、**engine-image-uploader** コマンドを使用して Red Hat Virtualization Manager にインポートできます。

結果

配布できる圧縮された OVF イメージファイルを作成している。**engine-image-uploader** コマンドを使用して、イメージを Red Hat Virtualization 環境にアップロードできるように付与できます。

18.3.4. 基本的な engine-image-uploader 使用例

以下は、engine uploader コマンドを使用してエクスポートストレージドメインを一覧表示する方法の例になります。

例18.1 イメージアップローダーを使用したエクスポートストレージドメインの一覧表示

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

Open Virtualization Format (OVF) ファイルをアップロードする方法の例を以下に示します。

例18.2 イメージアップローダーを使用したファイルのアップロード

```
# engine-image-uploader -e myexportdom upload myrhel6.ovf
Please provide the REST API password for the admin@internal oVirt Engine user (CTRL+D to
abort):
```

18.4. USB フィルターエディター

18.4.1. USB Filter Editor のインストール

USB Filter Editor は、**usbfilter.txt** ポリシーファイルを設定するために使用される Windows ツールです。このファイルで定義されたポリシールールは、クライアントマシンから Red Hat Virtualization Manager を使用して管理される仮想マシンへの特定の USB デバイスの自動パススルーを許可または拒否します。ポリシーファイルは、以下の場所にある Red Hat Virtualization Manager にあります。

/etc/ovirt-engine/usbfilter.txt

USB フィルターポリシーへの変更は、Red Hat Virtualization Manager サーバーの **ovirt-engine** サービスが再起動しない限り、反映されません。

Content Delivery Network から **USBFilterEditor.msi** ファイルをダウンロードし
<https://rhn.redhat.com/rhn/software/channel/downloads/Download.do?cid=20703> ます。

手順18.3 USB Filter Editor のインストール

1. Windows マシンで、コンテンツ配信ネットワークから取得した **USBFilterEditor.msi** インストーラーを起動します。
2. インストールウィザードの手順に従います。特に指定がない限り、USB フィルターエディターは、Windows のバージョンに応じて、デフォルトで **C:\Program Files\RedHat\USB Filter Editor** または **C:\Program Files (x86)\RedHat\USB Filter Editor** のいずれかにインストールされます。
3. デスクトップに USB フィルターエディターのショートカットアイコンが作成されます。



重要

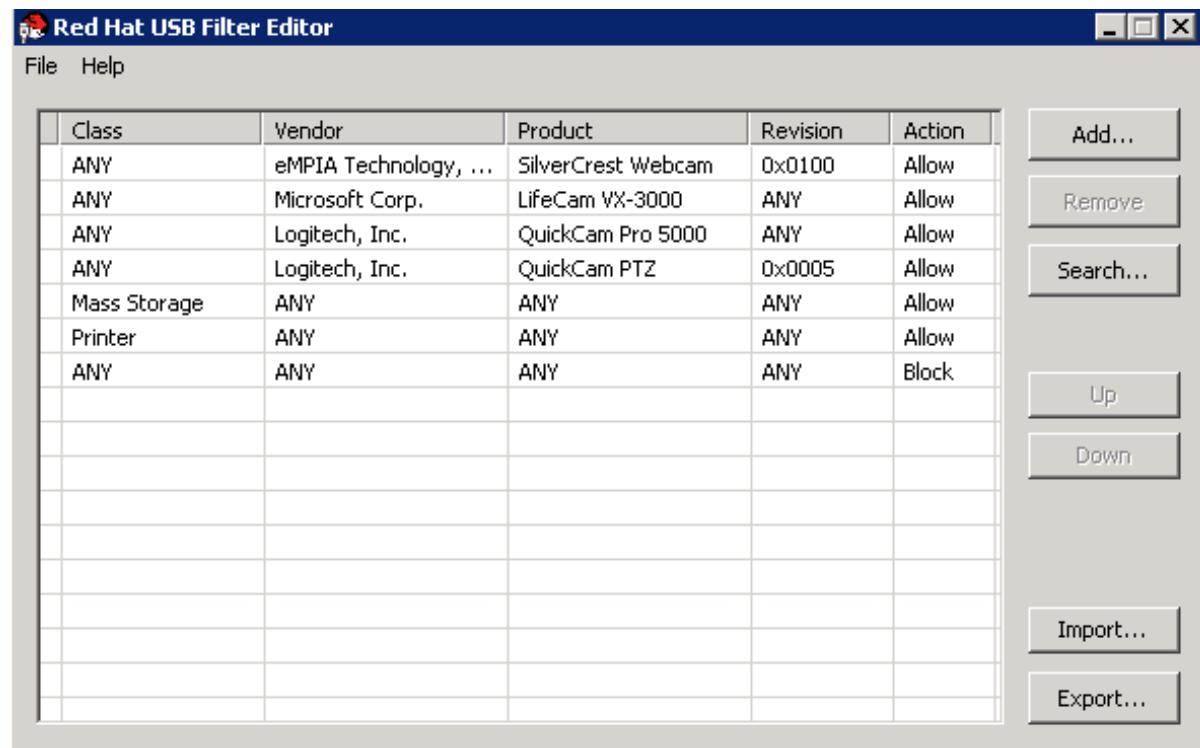
セキュアコピー (SCP) クライアントを使用して、Red Hat Virtualization Manager から フィルターポリシーをインポートおよびエクスポートします。Windows マシン用のセキュアコピーツールは WinSCP (<http://winscp.net>) です。

デフォルトの USB デバイスピリシーは、仮想マシンに USB デバイスへの基本的なアクセスを提供します。ポリシーを更新して、追加の USB デバイスの使用を許可します。

18.4.2. USB フィルターエディターインターフェイス

- デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックします。

図18.1 Red Hat USB フィルターエディター



Red Hat USB Filter Editor インターフェイスには、各 USB デバイスの **Class**、**Vendor**、**Product**、**Revision**、および **Action** が表示されます。許可された USB デバイスは、**Action** 列で **Allow** に設定されています。禁止されているデバイスは **Block** に設定されます。

表18.1 USB エディターフィールド

Name	説明
クラス	USB デバイスのタイプ(プリンター、大容量ストレージコントローラーなど)。
Vendor	選択したタイプの製造元。
製品	特定の USB デバイスモデル。
リビジョン	製品の改訂。
アクション	指定されたデバイスを許可またはブロックします。

USB デバイスポリシールールは、リストされている順序で処理されます。**Up** ボタンおよび**Down** ボタンを使用して、リスト内の上または下にルールを移動します。USB Filter Editor で明示的に許可されない限り、すべての USB デバイスが拒否されるようにするには、ユニバーサル ブロック ルールを最下位のエントリーとして残す必要があります。

18.4.3. USB ポリシーの追加

概要

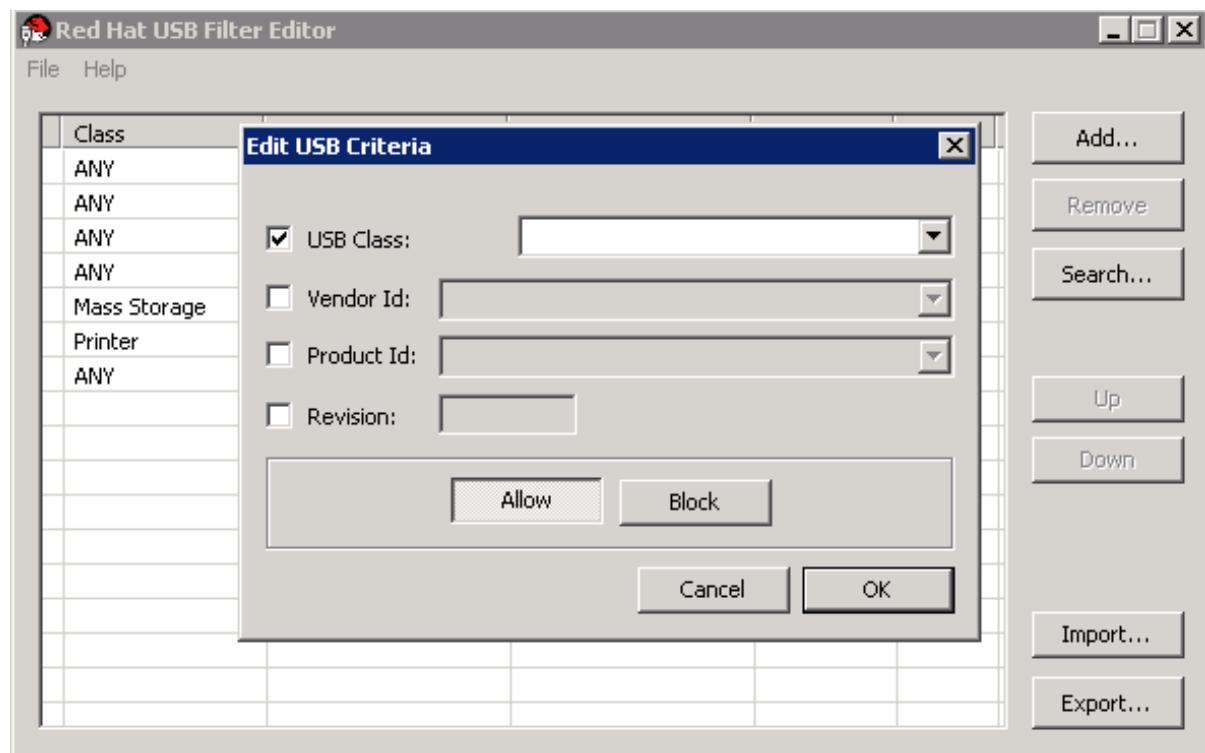
USB フィルターエディターに USB ポリシーを追加します。

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックして、エディターを開きます。

手順18.4 USB ポリシーの追加

1. 追加 ボタンをクリックします。Edit USB Criteria ウィンドウが開きます。

図18.2 USB 条件の編集



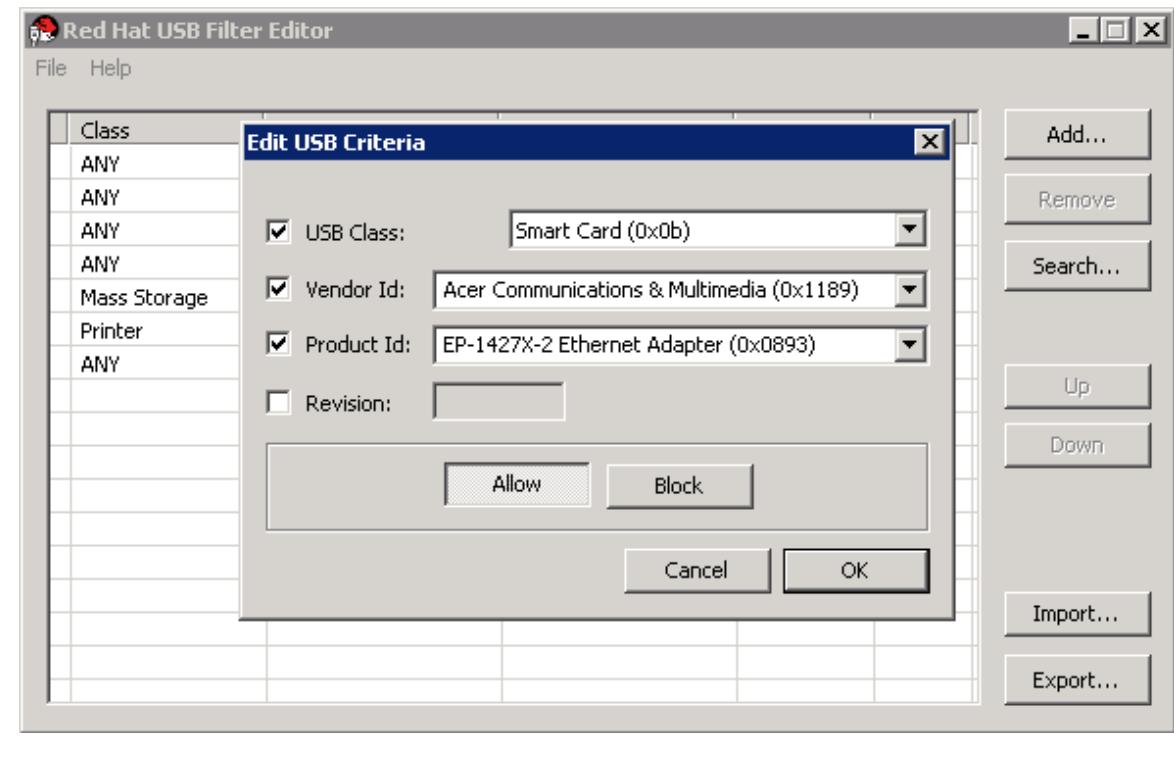
2. USB Class、Vendor ID、Product ID、および Revision のチェックボックスおよびリストを使用してデバイスを指定します。

Allow ボタンをクリックして、仮想マシンが USB デバイスを使用できるようにします。 **Block** ボタンをクリックして、仮想マシンの USB デバイスを禁止します。

OK をクリックすると、選択したフィルタールールがリストに追加され、ウィンドウが閉じます。

例18.3 デバイスの追加

以下は、メーカーの Acer Communications & Multimedia の USB クラス Smartcard デバイス EP-1427X-2 Ethernet Adapter を許可されたデバイスのリストに追加する方法の例です。



3. File → Save で変更を保存します。

結果

USB Filter Editor に USB ポリシーが追加されました。USB フィルター ポリシーを有効にするには、Red Hat Virtualization Manager にエクスポートする必要があります。

18.4.4. USB ポリシーの削除

概要

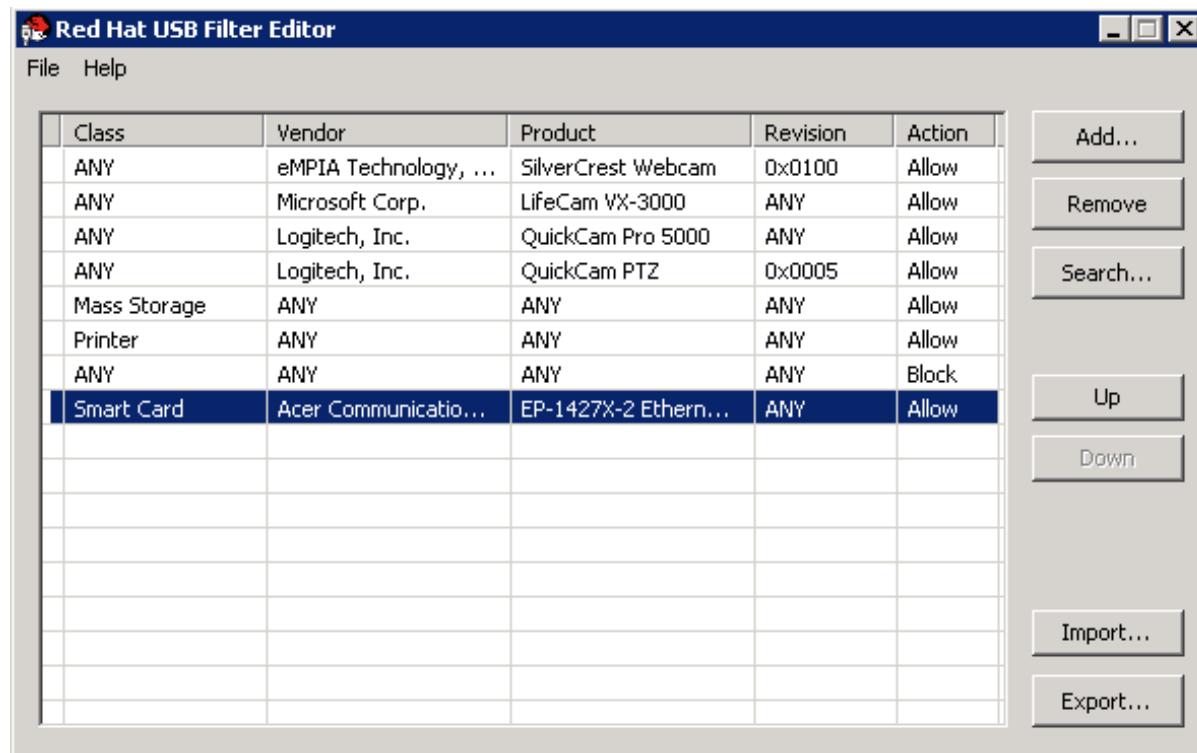
USB フィルターエディターから USB ポリシーを削除します。

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックして、エディターを開きます。

手順18.5 USB ポリシーの削除

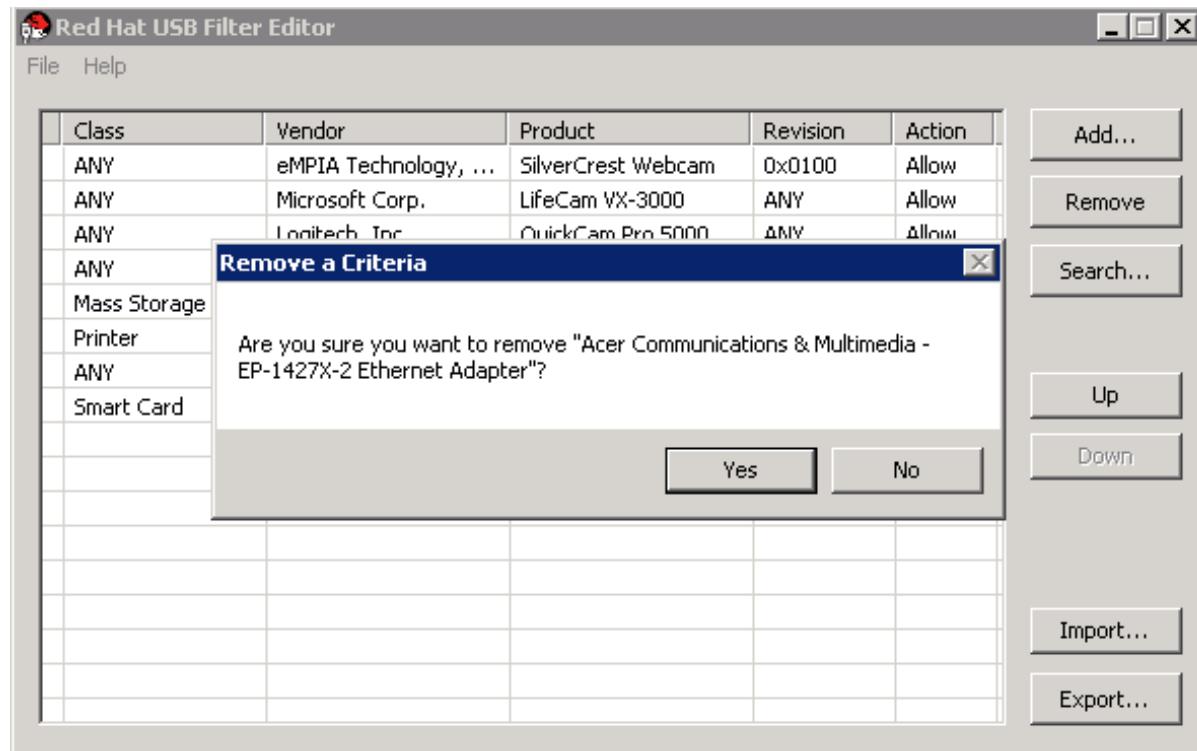
1. 削除するポリシーを選択します。

図18.3 USB ポリシーを選択します。



2. 削除 をクリックします。ポリシーを削除することを確認するメッセージが表示されます。

図18.4 USB 条件の編集



3. **Yes** をクリックして、ポリシーを削除することを確認します。

4. **File → Save** で変更を保存します。

結果

USB フィルターエディターから USB ポリシーを削除しました。USB フィルターポリシーを有効にするには、Red Hat Virtualization Manager にエクスポートする必要があります。

18.4.5. USB デバイスピリシーの検索

概要

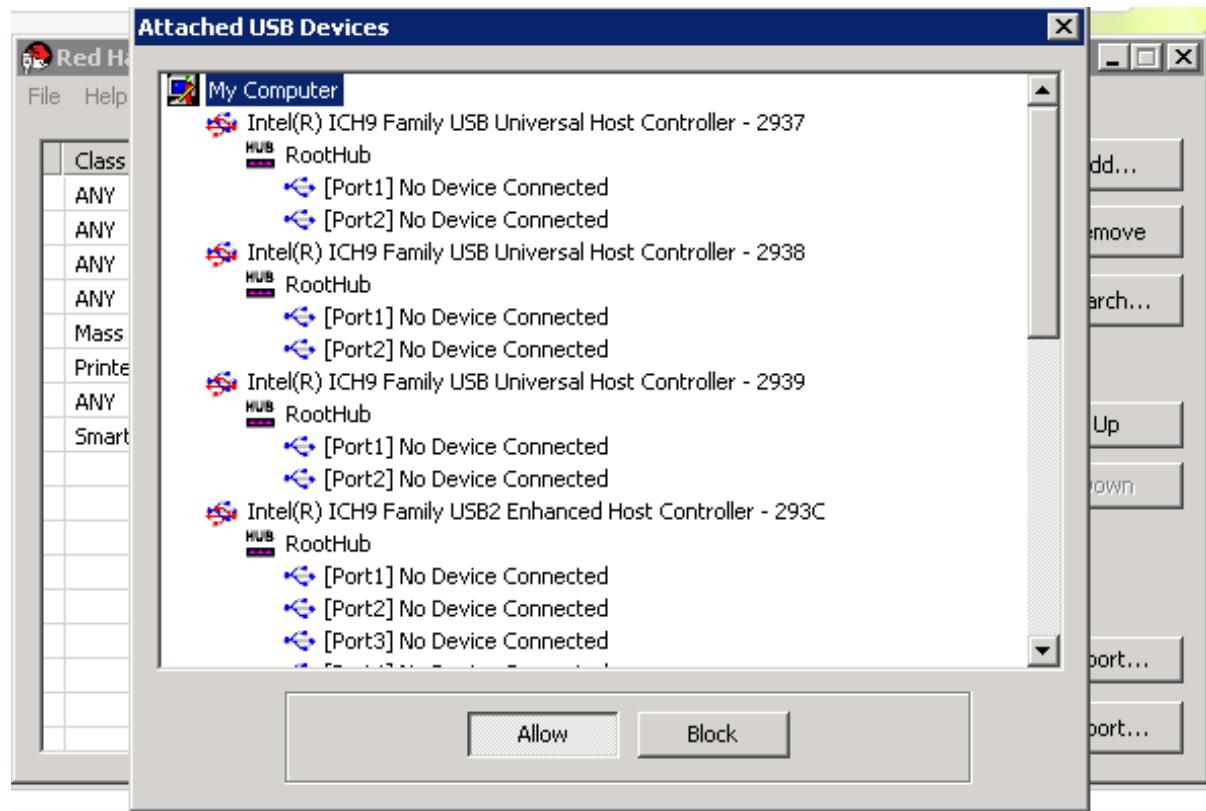
接続されている USB デバイスを検索して、USB フィルターエディターで許可またはブロックします。

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックして、エディターを開きます。

手順18.6 USB デバイスピリシーの検索

1. Search をクリックします。Attached USB Devices ウィンドウには、接続されているすべてのデバイスの一覧が表示されます。

図18.5 接続されている USB デバイス



2. デバイスを選択し、必要に応じて Allow または Block をクリックします。選択したデバイスをダブルクリックして、ウィンドウを閉じます。デバイスのポリシールールがリストに追加されます。
3. Up ボタンおよび Down ボタンを使用して、リスト内の新しいポリシールールの位置を変更します。
4. File → Save で変更を保存します。

結果

接続されている USB デバイスを検索しました。USB フィルターポリシーを有効にするには、Red Hat Virtualization Manager にエクスポートする必要があります。

18.4.6. USB ポリシーのエクスポート

概要

更新されたポリシーを有効にするには、USB デバイスピリシーの変更をエクスポートして Red Hat Virtualization Manager にアップロードする必要があります。ポリシーをアップロードし、**ovirt-engine** サービスを再起動します。

デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックして、エディターを開きます。

手順18.7 USB ポリシーのエクスポート

1. **Export** をクリックすると、**Save As** ウィンドウが開きます。
2. ファイル名が **usbfilter.txt** のファイルを保存します。
3. WinSCP などのセキュアコピークライアントを使用して、**usbfilter.txt** ファイルを Red Hat Virtualization Manager を実行しているサーバーにアップロードします。ファイルは、サーバー上の以下のディレクトリーに配置する必要があります。
/etc/ovirt-engine/
4. Red Hat Virtualization Manager を実行しているサーバーで **root** ユーザーとして、**ovirt-engine** サービスを再起動します。

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

結果

USB デバイスピリシーは、Red Hat Virtualization 環境で実行されている仮想マシンに実装されます。

18.4.7. USB ポリシーのインポート

概要

編集する前に、既存の USB デバイスピリシーをダウンロードして USB フィルターエディターにインポートする必要があります。

手順18.8 USB ポリシーのインポート

1. WinSCP などのセキュアコピークライアントを使用して、**usbfilter.txt** ファイルを Red Hat Virtualization Manager を実行しているサーバーにアップロードします。ファイルは、サーバー上の以下のディレクトリーに配置する必要があります。
/etc/ovirt-engine/
2. デスクトップの USB Filter Editor ショートカットアイコンをダブルクリックして、エディターを開きます。
3. **Import** をクリックして **Open** ウィンドウを開きます。
4. サーバーからダウンロードした **usbfilter.txt** ファイルを開きます。

結果

USB Filter Editor で USB デバイスピリシーを編集できます。

18.5. ログコレクターツール

18.5.1. ログコレクター

ログ収集ツールは、Red Hat Virtualization Manager に含まれています。これにより、サポートを要求するときに、Red Hat Virtualization 環境全体から関連するログを簡単に収集できます。

ログ収集コマンドは **ovirt-log-collector** です。**root** ユーザーとしてログインし、Red Hat Virtualization 環境の管理認証情報を提供する必要があります。**ovirt-log-collector -h** コマンドは、**ovirt-log-collector** コマンドのすべての有効なオプションのリストを含む使用情報を表示します。

18.5.2. ovirt-log-collector コマンドの構文

ログコレクターコマンドの基本構文は以下の通りです。

```
ovirt-log-collector [options] list [all, clusters, datacenters]
ovirt-log-collector [options] collect
```

サポートされる 2 つの操作モードは **list** および **collect** です。

- **list** パラメーターは、Red Hat Virtualization Manager に接続されているホスト、クラスター、またはデータセンターを一覧表示します。リストされたオブジェクトに基づいてログコレクションをフィルタリングできます。
- **collect** パラメーターは、Red Hat Virtualization Manager からのログ収集を実行します。収集されたログは、**/tmp/logcollector** ディレクトリ下のアーカイブファイルに配置されます。**ovirt-log-collector** コマンドは、各ログに特定のファイル名を割り当てます。

別のパラメーターが指定されていない限り、使用可能なホストを、それらが属するデータセンターおよびクラスターと一緒にリストすることがデフォルトのアクションとなります。特定のログを取得するために、ユーザー名とパスワードを入力するように求められます。

ovirt-log-collector コマンドをさらに絞り込むパラメーターが多数あります。

一般的なオプション

--version

使用中のコマンドのバージョン番号を表示し、プロンプトに戻る。

-h, --help

コマンドの使用情報を表示し、プロンプトに戻ります。

--conf-file=PATH

ツールが使用する設定ファイルとして *PATH* を設定します。

--local-tmp=PATH

ログが保存されるディレクトリーとして *PATH* を設定します。デフォルトのディレクトリーは **/tmp/logcollector** です。

--ticket-number=TICKET

SOS レポートに関連付けるチケットまたはケース番号として *TICKET* を設定します。

--upload=FTP_SERVER

FTP を使用して、取得されるログの宛先として *FTP_SERVER* を設定します。Red Hat のサポート担当者からアドバイスがない限り、このオプションは使用しないでください。

--log-file=PATH

コマンドがログ出力に使用する特定のファイル名として *PATH* を設定します。

--quiet

quiet モードを設定し、コンソール出力を最小限に抑えます。デフォルトでは、*quiet* モードはオフになっています。

-v, --verbose

verbose モードを設定し、より多くのコンソール出力を提供します。デフォルトでは、*verbose* モードはオフになっています。

Red Hat Virtualization Manager のオプション

これらのオプションはログコレクションをフィルタリングし、Red Hat Virtualization Manager の認証の詳細を指定します。

これらのパラメーターを、特定のコマンドと組み合わせることができます。たとえば、**ovirt-log-collector --user=admin@internal --cluster ClusterA,ClusterB --hosts "SalesHost"*** はユーザーを **admin@internal** として指定し、ログコレクションをクラスター A および B の **SalesHost** ホストのみに制限します。

--no-hypervisors

ログコレクションから仮想化ホストを省略します。

--one-hypervisor-per-cluster

各クラスターから1台のホスト (存在する場合は SPM) のログを収集します。

-u USER, --user=USER

ログイン用のユーザー名を設定します。*USER* は、ユーザー@ドメインの形式で指定されます。ここで、*user* はユーザー名で、*domain* は使用中のディレクトリーサービスドメインです。ユーザーはディレクトリーサービスに存在し、Red Hat Virtualization Manager に認識されている必要があります。

-r FQDN, --rhevm=FQDN

ログの収集元となる Red Hat Virtualization Manager サーバーの完全修飾ドメイン名を設定します。*FQDN* は、Manager の完全修飾ドメイン名に置き換えられます。ログコレクターは、Red Hat Virtualization Manager と同じローカルホストで実行していると想定されています。デフォルト値は **localhost** です。

-c CLUSTER, --cluster=CLUSTER

Red Hat Virtualization Manager からのログに加えて、指定された *CLUSTER* 内の仮想化ホストからログを収集します。含めるクラスターは、クラスター名または一致パターンのコンマ区切りリストで指定する必要があります。

-D DATACENTER, --data-center=DATACENTER

Red Hat Virtualization Manager からのログに加えて、指定された *DATACENTER* の仮想化ホストからログを収集します。含めるデータセンターは、データセンター名または一致パターンのコンマ区切りリストで指定する必要があります。

-H HOSTS_LIST, --hosts=HOSTS_LIST

Red Hat Virtualization Manager からのログに加えて、指定された *HOSTS_LIST* 内の仮想化ホストからログを収集します。含めるホストは、ホスト名、完全修飾ドメイン名、または IP アドレスのコンマ区切りリストで指定する必要があります。一致パターンも有効です。

SSH 設定

--ssh-port=PORT

仮想化ホストとの SSH 接続に使用するポートとして *PORT* を設定します。

-k KEYFILE, --key-file=KEYFILE

仮想化ホストへのアクセスに使用される公開 SSH キーとして *KEYFILE* を設定します。

--max-connections=MAX_CONNECTIONS

仮想化ホストからのログの最大同時 SSH 接続として *MAX_CONNECTIONS* を設定します。デフォルトは **10** です。

PostgreSQL データベースのオプション

データベースユーザー名とデータベース名は、デフォルト値から変更されている場合は、**pg-user** および **dbname** パラメーターを使用して指定する必要があります。

データベースがローカルホスト上にない場合は、**pg-dbhost** パラメーターを使用します。オプションの **pg-host-key** パラメーターを使用して、リモートログを収集します。リモートログ収集を成功させるには、PostgreSQL SOS プラグインをデータベースサーバーにインストールする必要があります。

--no-postgresql

データベースのコレクションを無効にします。ログコレクターは Red Hat Virtualization Manager PostgreSQL データベースに接続し、**--no-postgresql** パラメーターが指定されていない限り、データをログレポートに追加します。

--pg-user=USER

データベースサーバーへの接続に使用するユーザー名として *USER* を設定します。デフォルトは **postgres** です。

--pg-database=DBNAME

データベースサーバーへの接続に使用するデータベース名として *DBNAME* を設定します。デフォルトは **rhevdm** です。

--pg-dbhost=DBHOST

データベースサーバーのホスト名として *DBHOST* を設定します。デフォルトは **localhost** です。

--pg-host-key=KEYFILE

データベースサーバーの公開 ID ファイル（秘密鍵）として *KEYFILE* を設定します。この値はデフォルトでは設定されていません。データベースがローカルホストに存在しない場合にのみ必要です。

18.5.3. ログコレクターの基本的な使用法

追加のパラメーターを指定せずに **ovirt-log-collector** コマンドを実行すると、デフォルトの動作では、Red Hat Virtualization Manager とそのアタッチされたホストからすべてのログを収集します。また、**--no-postgresql** パラメーターが追加されない限り、データベースログを収集します。次の例では、ログコレクターを実行して、Red Hat Virtualization Manager と接続されている 3 つのホストからすべてのログを収集します。

例18.4 ログコレクターの使用法

```
# 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
```

18.6. ISO アップローダーツール

18.6.1. ISO アップローダーツール

ISO アップローダーは、ISO イメージを ISO ストレージドメインにアップロードするツールです。これは、Red Hat Virtualization Manager の一部としてインストールされます。

ISO uploader コマンドは **engine-iso-uploader** です。このコマンドを使用するには、**root** ユーザーとしてログインし、Red Hat Virtualization 環境の管理認証情報を提供する必要があります。**engine-iso-uploader -h** コマンドは、**engine-iso-uploader** コマンドのすべての有効なオプションのリストを含む使用情報を表示します。

18.6.2. engine-iso-uploader コマンドの構文

ISO uploader コマンドの基本的な構文は、以下のとおりです。

```
engine-iso-uploader [options] list
engine-iso-uploader [options] upload [file].[file]...[file]
```

ISO uploader コマンドは、**list**、および **upload** の 2 つのアクションをサポートします。

- **list** アクションは、ISO ファイルをアップロードできる ISO ストレージドメインを一覧表示します。Red Hat Virtualization Manager は、インストールプロセス中に Manager がインストールされているマシンにこの一覧を作成します。
- **upload** アクションは、スペースで区切られた単一の ISO ファイルまたは複数の ISO ファイルを指定された ISO ストレージドメインにアップロードします。デフォルトでは NFS が使用されますが、SSH も利用可能です。

ISO uploader コマンドを使用する場合は、上記のアクションのいずれかを指定する必要があります。さらに、**アップロード** アクションを使用するには、少なくとも1つのローカルファイルを指定する必要があります。

engine-iso-uploader コマンドをさらに絞り込むためのいくつかのパラメーターがあります。

一般的なオプション

--version

ISO uploader コマンドのバージョンを表示します。

-h, --help

ISO uploader コマンドの使用方法に関する情報を表示します。

--conf-file=[PATH]

コマンドが使用する設定ファイルとして [PATH] を設定します。デフォルトは **/etc/ovirt-engine/isouploader.conf** です。

--log-file=[PATH]

[PATH] をログ出力の書き込みに使用する特定のファイル名として設定します。デフォルトは **/var/log/ovirt-engine/ovirt-iso-uploader/ovirt-iso-uploader[date].log** です。

--cert-file=[PATH]

[PATH] をエンジンを検証する証明書として設定します。デフォルトは **/etc/pki/ovirt-engine/ca.pem** です。

--insecure

エンジンの検証を試行しないことを指定します。

--nossl

エンジンへの接続に SSL を使用しないことを指定します。

--quiet

quiet モードを設定し、コンソール出力を最小限に抑えます。

-v, --verbose

verbose モードを設定し、より多くのコンソール出力を提供します。

-f, --force

アップロードするソースファイルのファイル名が宛先 ISO ドメインの既存のファイルと同じである場合は、強制モードが必要です。このオプションでは、既存のファイルを強制的に上書きします。

Red Hat Virtualization Manager のオプション

-u [USER], --user=[USER]

コマンドの実行に認証情報が使用されるユーザーを指定します。[USER] は、[username]@[domain] の形式で指定されます。ユーザーは指定のドメインに存在し、Red Hat Virtualization Manager に認識されている必要があります。

-r [FQDN], --engine=[FQDN]

イメージをアップロードする Red Hat Virtualization Manager の IP アドレスまたは完全修飾ドメイン名を指定します。イメージアップローダーは、Red Hat Virtualization Manager がインストールされているのと同じマシンから実行されていると想定されています。デフォルト値は **localhost:443** です。

ISO ストレージドメインのオプション

次のオプションは、イメージがアップロードされる ISO ドメインを指定します。これらのオプションと一緒に使用することはできません。-i オプションまたは -n オプションのいずれかを使用する必要があります。

-i, --iso-domain=[ISODOMAIN]

アップロードの宛先としてストレージドメイン [ISODOMAIN] を設定します。

-n, --nfs-server=[NFSSERVER]

アップロードの宛先として NFS パス [NFSSERVER] を設定します。

接続オプション

ISO アップローダーは、デフォルトで NFS を使用してファイルをアップロードします。これらのオプションは、代わりに SSH ファイル転送を指定します。

--ssh-user=[USER]

アップロードに使用する SSH ユーザー名として [USER] を設定します。デフォルトは **root** です。

--ssh-port=[PORT]

SSH への接続時に使用するポートとして [PORT] を設定します。

-k [KEYFILE], --key-file=[KEYFILE]

SSH 認証に使用する公開鍵として [KEYFILE] を設定します。キーが設定されていない場合、**--ssh-user=[USER]** で指定したユーザーのパスワードを入力するように求められます。

18.6.3. NFS サーバーの指定

例18.5 NFS サーバーへのアップロード

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

18.6.4. 基本的な ISO アップローダーの使用法

以下の例は、ISO アップローダーとリストパラメーターを示しています。最初のコマンドは、利用可能な ISO ストレージドメインを一覧表示します。コマンドでユーザーが指定されていないため、**admin@internal** ユーザーが使用されます。2番目のコマンドは、指定された ISO ドメインに NFS 経由で ISO ファイルをアップロードします。

例18.6 ドメインの一覧表示およびイメージのアップロード

```
# 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):
```

18.6.5. VirtIO およびゲストツールのイメージファイルの ISO ストレージドメインへのアップロード

以下の例は、**virtio-win.iso**、**virtio-win_x86.vfd**、**virtio-win_amd64.vfd**、および **rhev-tools-setup.iso** イメージファイルを **ISODomain** にアップロードするコマンドを示しています。

例18.7 VirtIO およびゲストツールのイメージファイルのアップロード

```
# engine-iso-uploader --iso-domain=[ISODomain] upload /usr/share/virtio-win/virtio-win.iso
/usr/share/virtio-win/virtio-win_x86.vfd /usr/share/virtio-win/virtio-win_amd64.vfd /usr/share/rhev-
guest-tools-iso/rhev-tools-setup.iso
```

18.6.6. VirtIO およびゲストツールのイメージファイル

Windows 仮想マシンの VirtIO ドライバーを含む virtio-win ISO および Virtual Floppy Drive (VFD) イメージと、Windows 仮想マシンの Red Hat Virtualization ゲストツールを含む rhev-tools-setup ISO は、ドメインのインストールおよび設定時に ISO ストレージドメインにコピーされます。

これらのイメージファイルは、仮想マシンにインストールし、パフォーマンスとユーザービリティを向上させるソフトウェアを提供します。最新の virtio-win ファイルおよび 2009-tools-setup ファイルは、Red Hat Virtualization Manager のファイルシステムの以下のシンボリックリンクからアクセスできます。

- **/usr/share/virtio-win/virtio-win.iso**
- **/usr/share/virtio-win/virtio-win_x86.vfd**
- **/usr/share/virtio-win/virtio-win_amd64.vfd**
- **/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso**

これらのイメージファイルは、インストールプロセスによってローカルで作成されていない ISO ストレージドメインに手動でアップロードする必要があります。**engine-iso-uploader** コマンドを使用して、これらのイメージを ISO ストレージドメインにアップロードします。アップロードされると、イ

メージファイルを仮想マシンにアタッチして使用することができます。

18.7. エンジンバキュームツール

18.7.1. エンジンバキュームツール

Engine Vacuum ツールは、テーブルを更新してデッド行を削除することで PostgreSQL データベースを維持し、ディスクスペースを再利用できるようにします。 **VACUUM** コマンドとそのパラメーターの詳細は、[PostgreSQL のドキュメント](#) を参照してください。

Engine Vacuum コマンドは **engine-vacuum** です。 **root** ユーザーとしてログインし、Red Hat Virtualization 環境の管理認証情報を提供する必要があります。

または、**engine-setup** コマンドを使用して、既存のインストールをカスタマイズするときに Engine Vacuum ツールを実行できます。

```
$ 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/9.2/static/sql-vacuum.html
(Yes, No) [No]:
```

Yes オプションは、Engine Vacuum ツールをフルバキューム冗長モードで実行します。

18.7.2. エンジンバキュームモード

エンジンバキュームは、Standard と Full の 2 つのモードで実行されます。

Standard Vacuum

頻繁に標準的なバキュームを行うことをお勧めします。

標準のバキュームは、テーブルとインデックスのデッドローバージョンを削除し、スペースを将来の再利用に使用できるものとしてマークします。頻繁に更新されるテーブルは、定期的にバキュームする必要があります。しかし、標準的なバキュームでは、そのスペースを OS に戻すことはできません。

パラメーターのない標準バキュームは、現在のデータベース内のすべてのテーブルを処理します。

Full Vacuum

日常的な使用には完全バキュームは推奨されませんが、テーブル内からかなりの量のスペースを再利用する必要がある場合にのみ実行する必要があります。

完全バキュームは、デッドスペースのないテーブルファイルの新しいコピーを書き込むことによってテーブルを圧縮し、それによってオペレーティングシステムがスペースを再利用できるようにします。フルバキュームには時間がかかる場合があります。

完全バキュームでは、操作が完了して古いコピーが削除されるまで、テーブルの新しいコピー用に追加のディスクスペースが必要です。フルバキュームにはテーブルの排他的ロックが必要なため、テーブルの他の使用と並行して実行することはできません。

18.7.3. エンジンバキュームの構文

Engine Vacuum コマンドの基本的な構文は次のとおりです。

```
engine-vacuum
```

```
engine-vacuum [option]
```

オプションを指定せずに **engine-vacuum** コマンドを実行すると、標準のバキュームが実行されます。

engine-vacuum コマンドをさらに絞り込むためのいくつかのパラメーターがあります。

一般的なオプション

-h --help

engine-vacuum コマンドの使用方法に関する情報を表示します。

-a

標準のバキュームを実行し、データベースを分析して、オプティマイザーの統計を更新します。

-A

バキューム処理を行わずに、データベースを解析し、オプティマイザーの統計情報を更新します。

-f

完全な vacuum を実行します。

-v

詳細モードで実行して、より多くのコンソール出力を提供します。

-t [table_name]

特定の1つテーブルまたは複数のテーブルを vacuum します。

```
engine-vacuum -f -v -t vm_dynamic -t vds_dynamic
```

パート IV. 環境に関する情報の収集

第19章 ログファイル

19.1. RED HAT VIRTUALIZATION MANAGER のインストールログファイル

表19.1 インストール

ログファイル	説明
/var/log/ovirt-engine/engine-cleanup-yyyy_mmdd_hh_mm_ss.log	engine-cleanup コマンドからログに記録します。これは、Red Hat Virtualization Manager のインストールをリセットするために使用されるコマンドです。コマンドが実行するたびにログが生成されます。実行の日付と時刻は、複数のログが存在できるようにするためにファイル名で使用されます。
/var/log/ovirt-engine/engine-db-install-yyyy_mmdd_hh_mm_ss.log	rhevdm データベースの作成および設定の詳細を示す engine-setup コマンドからログに記録します。
/var/log/ovirt-engine/ovirt-engine-dwh-setup-yyyy_mmdd_hh_mm_ss.log	ovirt-engine-dwh-setup コマンドからログに記録します。これは、レポート用に ovirt_engine_history データベースを作成するために使用されるコマンドです。コマンドが実行するたびにログが生成されます。実行の日付と時刻は、複数のログが同時に存在できるようにするためにファイル名で使用されます。
/var/log/ovirt-engine/setup/ovirt-engine-setup-yyyymmddhhmmss.log	engine-setup コマンドからログに記録します。コマンドが実行するたびにログが生成されます。実行の日付と時刻は、複数のログが同時に存在できるようにするためにファイル名で使用されます。

19.2. RED HAT VIRTUALIZATION MANAGER ログファイル

表19.2 サービス活動

ログファイル	説明
/var/log/ovirt-engine/engine.log	すべての Red Hat Virtualization Manager GUI クラッシュ、Active Directory ルックアップ、データベースの問題、およびその他のイベントを反映します。
/var/log/ovirt-engine/host-deploy	Red Hat Virtualization Manager からデプロイされたホストのログファイル。
/var/lib/ovirt-engine/setup-history.txt	Red Hat Virtualization Manager に関するパッケージのインストールおよびアップグレードを追跡します。

19.3. SPICE ログファイル

SPICE のログファイルは、SPICE の接続に関する問題をトラブルシューティングする際に有用です。SPICE デバッグを開始するには、ログレベルを **debugging** に変更します。次に、ログの場所を特定します。

ゲストマシンへのアクセスに使用されるクライアントおよびゲストマシン自体の両方に、SPICE ログファイルがあります。クライアント側のログの場合、**console.vv** ファイルがダウンロードされているネイティブクライアントを使用して SPICE クライアントを起動した場合は、**remote-viewer** コマンドを使用してデバッグを有効にし、ログ出力を生成します。

19.3.1. ハイパーバイザー SPICE サーバーの SPICE ログ

表19.3 ハイパーバイザー SPICE サーバーの SPICE ログ

ログタイプ	ログの場所	ログレベルを変更するには、以下を実行します。
ホスト/ハイパーバイザー SPICE サーバー	/var/log/libvirt/qemu/(guest_name).log	ゲストを起動する前に、ホスト/ハイパーバイザーで export SPICE_DEBUG_LEVEL=5 を実行します。この変数は QEMU によって解析され、システム全体で実行すると、システム上のすべての仮想マシンのデバッグ情報が出力されます。このコマンドは、クラスター内の各ホストで実行する必要があります。このコマンドは、各クラスターではなく、各ホスト/ハイパーバイザーにのみ機能します。

19.3.2. ゲストマシンの SPICE ログ

表19.4 ゲストマシンの spice-vdagent ログ

ログタイプ	ログの場所	ログレベルを変更するには、以下を実行します。
Windows ゲスト	C:\Windows\Temp\vdagent.log C:\Windows\Temp\vdservice.log	該当なし

ログタイプ	ログの場所	ログレベルを変更するには、以下を実行します。
Red Hat Enterprise Linux ゲスト	journalctl を root ユーザーとして使用します。	<p>spice-vdagentd サービスをデバッグモードで実行するには、root ユーザーとして SPICE_VDAGENTD_EXTRA_ARGS="-d -d" のエントリーで /etc/sysconfig/spice-vdagentd ファイルを作成します。</p> <p>コマンドラインからデバッグモードで spice-vdagent を実行するには、次の手順に従います。</p> <pre>\$ killall - u \$USER spice-vdagent \$ spice-vdagent -x -d [-d] [& tee spice-vdagent.log]</pre>

19.3.3. **console.vv** ファイルを使用して起動された SPICE クライアントの SPICE ログ

Linux クライアントマシンの場合:

1. **--spice-debug** オプションを指定して **remote-viewer** コマンドを実行し、SPICE デバッグを有効にします。プロンプトが表示されたら、接続 URL を入力します（例：
`spice://[virtual_machine_IP]:[port]`）。

```
# remote-viewer --spice-debug
```

2. デバッグパラメーターで SPICE クライアントを実行し、これに .vv ファイルを渡すには、**console.vv** ファイルをダウンロードし、**--spice-debug** オプションを指定して **remote-viewer** コマンドを実行し、**console.vv** ファイルへのフルパスを指定します。

```
# remote-viewer --spice-debug /path/to/console.vv
```

Windows クライアントマシンの場合:

1. **virt-viewer** 2.0-11.el7ev 以降のバージョンでは、**virt-viewer.msi** は **virt-viewer** および **debug-viewer.exe** をインストールします。
2. **spice-debug** 引数を指定して **remote-viewer** コマンドを実行し、コマンドをコンソールへのパスで指示します。

```
remote-viewer --spice-debug path\to\console.vv
```

3. ログを表示するには、仮想マシンに接続します。GDB を実行しているコマンドプロンプトが表示され、**remote-viewer** の標準出力と標準エラーが出力されます。

19.4. RED HAT VIRTUALIZATION ホストのログファイル

表19.5

ログファイル	説明
/var/log/vdsdm/libvirt.log	libvirt のログファイル。
/var/log/vdsdm/spm-lock.log	Storage Pool Manager ロールでリースを取得するホストの機能の詳細を示すログファイル。ホストがリースを取得、解放、更新、または更新に失敗したときのログの詳細。
/var/log/vdsdm/vdsdm.log	仮想化ホスト上のマネージャーのエージェントである VDSM のログファイル。
/tmp/ovirt-host-deploy-@DATE@.log	ホストデプロイメントログ。ホストが正常にデプロイされた後、/var/log/ovirt-engine/host-deploy/ovirt-@DATE@-@HOST@-@CORRELATION_ID@.log としてコピーされます。

19.5. 仮想化ホストのロギングサーバーの設定

ホストはログファイルを生成および更新し、その動作や問題点を記録しています。これらのログファイルを一元的に収集すると、デバッグが簡素化されます。

この手順は、集中ログサーバーで使用する必要があります。別のロギングサーバーを使用するか、この手順を使用して Red Hat Virtualization Manager でホストロギングを有効にすることができます。

手順19.1 仮想化ホストのロギングサーバーの設定

1. rsyslog トラフィックを許可するように SELinux を設定します。

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

2. /etc/rsyslog.conf を編集し、以下の行を追加します。

```
$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
```

以下をコメント解除します。

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

3. rsyslog サービスを再起動します。

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

これで、集中ログサーバーは、仮想化ホストから メッセージとセキュアなログを受信し、保存するよう設定されました。

第20章 プロキシー

20.1. SPICE プロキシー

20.1.1. SPICE プロキシーの概要

SPICE プロキシーは、SPICE クライアントがハイパーバイザーを接続するネットワークの外部にある場合に SPICE クライアントを仮想マシンに接続するために使用されるツールです。SPICE プロキシーの設定は、マシンに **Squid** をインストールし、ファイアウォールを通過するプロキシートラフィックを許可するように **iptables** を設定することで設定されます。SPICE プロキシーをオンにするには、Manager で **engine-config** を使用して、キー **SpiceProxyDefault** をプロキシーの名前とポートで設定される値に設定します。SPICE プロキシーをオフにするには、Manager で **engine-config** を使用して、キー **SpiceProxyDefault** が設定されている値を削除します。



重要

SPICE プロキシーは、スタンドアロン SPICE クライアントと組み合わせてのみ使用でき、SPICE HTML5 または noVNC を使用して仮想マシンに接続することはできません。

20.1.2. SPICE プロキシーマシンの設定

この手順では、マシンを SPICE プロキシーとして設定する方法を説明します。SPICE プロキシーを使用すると、ネットワークの外部から Red Hat Virtualization ネットワークに接続できるようになります。この手順で **Squid** を使用してプロキシーサービスを提供します。

手順 20.1 Red Hat Enterprise Linux への Squid のインストール

1. プロキシーマシンに **Squid** をインストールします。

```
# yum install squid
```

2. **/etc/squid/squid.conf** を開きます。以下を、

```
http_access deny CONNECT !SSL_ports
```

以下のように変更します。

```
http_access deny CONNECT !Safe_ports
```

3. プロキシーを起動します。

```
# systemctl start squid.service
```

4. デフォルトの squid ポートを開きます。

```
# iptables -A INPUT -p tcp --dport 3128 -j ACCEPT
```

5. この **iptables** ルールを永続化します。

```
# service iptables save
```

これで、マシンを SPICE プロキシーとして設定できました。ネットワークの外部から Red Hat Virtualization ネットワークに接続する前に、SPICE プロキシーをアクティブにします。

20.1.3. SPICE プロキシーの有効化

この手順では、SPICE プロキシーをアクティブ化（またはオン）する方法について説明します。

手順20.2 SPICE プロキシーのアクティブ化

- Manager で engine-config ツールを使用してプロキシーを設定します。

```
# engine-config -s SpiceProxyDefault=someProxy
```

- ovirt-engine サービスを再起動します。

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

プロキシーには以下の形式が必要です。

```
protocol://[host]:[port]
```



注記

Red Hat Enterprise Linux 6.7、Red Hat Enterprise Linux 7.2 以降に同梱された SPICE クライアントのみが、HTTPS プロキシーをサポートしています。古いクライアントは HTTP のみをサポートします。古いクライアントに HTTPS が指定されている場合、クライアントはプロキシー設定を無視し、ホストへの直接接続を試みます。

SPICE Proxy がアクティブ（オン）になりました。SPICE プロキシーを介して Red Hat Virtualization ネットワークに接続できるようになりました。

20.1.4. SPICE プロキシーをオフにする

この手順では、SPICE プロキシーをオフに（非アクティブ化）する方法を説明します。

手順20.3 SPICE プロキシーをオフにする

- Manager にログインします。

```
$ ssh root@[IP of Manager]
```

- 以下のコマンドを実行し、SPICE プロキシーをクリアします。

```
# engine-config -s SpiceProxyDefault=""
```

- Manager を再起動します。

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

■ SPICE プロキシーが非アクティブ(オフ)になりました。SPICE プロキシーを介して Red Hat Virtualization ネットワークに接続できなくなりました。

20.2. SQUID プロキシー

20.2.1. Squid プロキシーのインストールおよび設定

概要

本セクションでは、ユーザーportalにSquidプロキシーをインストールして設定する方法を説明します。Squidプロキシーサーバーは、コンテンツアクセラレーターとして使用されます。頻繁にビューされたコンテンツをキャッシュし、帯域幅を削減し、応答時間を改善します。

手順20.4 Squid プロキシーの設定

1. Squid プロキシーサーバーの HTTPS ポートのキーペアと証明書を取得します。このキーペアは、別の SSL/TLS サービスのキーペアを取得するのと同じ方法で取得できます。キーペアは、秘密キーと署名付き証明書を含む 2 つの PEM ファイルの形式です。この手順では、**proxy.key** および **proxy.cer** という名前であることを前提としています。



注記

キーペアと証明書は、エンジンの認証局を使用して生成することもできます。プロキシーの秘密鍵および証明書がすでにあり、エンジン認証局でそれを生成したくない場合は、次の手順にスキップしてください。

2. プロキシーのホスト名を選択します。次に、プロキシーの証明書の識別名の他のコンポーネントを選択します。



注記

エンジン自体が使用するのと同じ国と同じ組織名を使用することが推奨されます。Manager がインストールされているマシンにログインし、次のコマンドを実行して、この情報を見つけます。

```
# openssl x509 -in /etc/pki/ovirt-engine/ca.pem -noout -subject
```

このコマンドは次のようなものを出力します。

```
subject= /C=US/O=Example Inc./CN=engine.example.com.81108
```

ここで関連部分は **/C=US/O=Example Inc.** です。これを使用して、プロキシーの証明書の完全な識別名を作成します。

```
/C=US/O=Example Inc./CN=proxy.example.com
```

3. プロキシーマシンにログインし、証明書署名要求を生成します。

```
# openssl req -newkey rsa:2048 -subj '/C=US/O=Example Inc./CN=proxy.example.com' -nodes -keyout proxy.key -out proxy.req
```



重要

証明書の識別名の周りにある引用符を含める必要があります。**-nodes** オプションは、秘密鍵が暗号化されないようにします。これは、プロキシーサーバーを起動するのにパスワードを入力する必要がないことを意味します。

このコマンドは、**proxy.key** と **proxy.req** の 2 つのファイルを生成します。**proxy.key** は秘密鍵です。このファイルを安全に保持します。**proxy.req** は証明書署名要求です。**proxy.req** には、特別な保護は必要ありません。

- 署名付き証明書を生成するには、証明書署名要求ファイルをプロキシーマシンからマネージャーマシンにコピーします。

```
# scp proxy.req engine.example.com:/etc/pki/ovirt-engine/requests/.
```

- Manager マシンにログインし、証明書に署名します。

```
# /usr/share/ovirt-engine/bin/pki-enroll-request.sh --name=proxy --days=3650 --subject='/C=US/O=Example Inc./CN=proxy.example.com'
```

これにより、証明書が署名され、10 年間 (3650 日) 有効になります。必要に応じて、証明書の有効期限が早くなるように設定します。

- 生成された証明書ファイルは **/etc/pki/ovirt-engine/certs** ディレクトリーにあり、**proxy.cer** という名前を指定する必要があります。プロキシーマシンで、このファイルを Manager マシンから現在のディレクトリーにコピーします。

```
# scp engine.example.com:/etc/pki/ovirt-engine/certs/proxy.cer .
```

- proxy.key** と **proxy.cer** の両方がプロキシーマシンに存在することを確認します。

```
# ls -l proxy.key proxy.cer
```

- Squid プロキシサーバーパッケージをプロキシーマシンにインストールします。

```
# yum install squid
```

- 秘密鍵と署名済み証明書を、プロキシーがアクセスできる場所（例：**/etc/squid** ディレクトリー）に移動します。

```
# cp proxy.key proxy.cer /etc/squid/.
```

- squid** ユーザーが、これらのファイルを読み取れるようにパーミッションを設定します。

```
# chgrp squid /etc/squid/proxy.*  
# chmod 640 /etc/squid/proxy.*
```

- Squid プロキシーは、エンジンが使用する証明書を検証する必要があります。Manager 証明書をプロキシーマシンにコピーします。この例では、ファイルパス **/etc/squid** を使用します。

```
# scp engine.example.com:/etc/pki/ovirt-engine/ca.pem /etc/squid/.
```



注記

デフォルトの CA 証明書は、Manager マシンの `/etc/pki/ovirt-engine/ca.pem` にあります。

12. **squid** ユーザーが、証明書ファイルを読み取れるようにパーミッションを設定します。

```
# chgrp squid /etc/squid/ca.pem
# chmod 640 /etc/squid/ca.pem
```

13. SELinux が Enforcing モードの場合は、**semanage** ツールを使用してポート 443 のコンテキストを変更して、Squid がポート 443 を使用できるようにします。

```
# yum install policycoreutils-python
# semanage port -m -p tcp -t http_cache_port_t 443
```

14. 既存の Squid 設定ファイルを以下に置き換えます。

```
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
cache_peer_access engine allow all
ssl_bump allow all
http_access allow all
```

15. Squid プロキシサーバーを再起動します。

```
# systemctl restart squid.service
```

16. 完全な URL を使用してユーザーportalに接続します。以下に例を示します。

```
https://proxy.example.com/UserPortal/org.ovirt.engine.ui.userportal.UserPortal/UserPortal.html
```



注記

https://proxy.example.com/UserPortal などの短い URL は動作しません。これらの短い URL は、302 応答コードと Location ヘッダーを使用してアプリケーションサーバーによって長い URL にリダイレクトされます。Red Hat Enterprise Linux の Squid のバージョンは、これらのヘッダーの書き換えをサポートしていません。



注記

デフォルト設定の Squid プロキシーは、15 分のアイドル時間後に接続を終了します。Squid Proxy がアイドル状態の接続を終了するまでの時間を増やすには、**squid.conf** の **read_timeout** オプションを調整します（例：**read_timeout 10 hours**

20.3. WEBSOCKET プロキシー

20.3.1. WebSocket プロキシーの概要

Websocket プロキシーにより、ユーザーは noVNC および SPICE HTML5 コンソールを介して仮想マシンに接続できます。以前のバージョンでは、WebSocket プロキシーは Red Hat Virtualization Manager マシンでのみ実行できるようになりましたが、プロキシーはネットワークにアクセスできる任意のマシンで実行できるようになりました。

WebSocket プロキシーは、初期設定時に Red Hat Virtualization Manager マシンまたは（インストールガイドの [Red Hat Virtualization Manager の設定](#) を参照）、または別のマシンに WebSocket プロキシーを『インストールして設定できます（インストールガイド』の別のマシン [への WebSocket プロキシーの『インストール』](#) を参照してください）。

WebSocket プロキシーは、Manager マシンから別のマシンに移行することもできます。『[WebSocket プロキシーを別のマシンに移行する](#)』を参照してください。



注記

SPICE HTML5 サポートは、テクノロジープレビュー機能です。テクノロジープレビュー機能は、Red Hat サービスレベルアグリーメント (SLA) では完全にサポートされておらず、機能的に完全でない可能性があり、実稼働環境での使用を目的とはしていません。ですが、近々発表予定のプロダクトイノベーションをリリースに先駆けてご提供することで、お客様には機能性をテストし、開発プロセス中にフィードバックをお寄せいただくことができます。

20.3.2. WebSocket プロキシーを別のマシンに移行する

セキュリティーまたはパフォーマンスの理由から、websocket プロキシーは Red Hat Virtualization Manager を実行しない別のマシンで実行できます。WebSocket プロキシーを Manager マシンから別のマシンに移行する手順では、Manager マシンから WebSocket プロキシー設定を削除してから、別のマシンにプロキシーをインストールします。

engine-cleanup コマンドを使用して、Manager マシンから WebSocket プロキシーを削除できます。

手順20.5 WebSocket プロキシーを別のマシンに移行する

1. Manager マシンで **engine-cleanup** を実行して、必要な設定を削除します。

```
# engine-cleanup
```

2. すべてのコンポーネントを削除するよう求められたら **No** と入力し、Enter を押します。

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

3. エンジンを削除するかどうかを問われたら **No** と入力し、Enter を押します。

```
Do you want to remove the engine? (Yes, No) [Yes]: No
```

4. WebSocket プロキシーを削除するよう求められたら **Yes** と入力し、Enter を押します。

```
Do you want to remove the WebSocket proxy? (Yes, No) [No]: Yes
```

他のコンポーネントを削除するかどうかを問われたら、**No** を選択します。

5. 別のマシンにプロキシーをインストールし、設定します。手順は、『[インストールガイドの別](#) のマシンへの [WebSocket プロキシー](#) のインストール』を参照してください。

付録A VDSM およびフック

A.1. VDSM

VDSM サービスは、Red Hat Virtualization Hosts (RHVH) および Red Hat Enterprise Linux ホストを管理するために Red Hat Virtualization Manager により使用されます。VDSM は、ホストのストレージ、メモリー、ネットワークリソースを管理監視します。また、仮想マシンの作成、統計収集、ログ収集、およびその他のホスト管理タスクを調整します。VDSM は、Red Hat Virtualization Manager により管理される各ホスト上でデーモンとして実行されます。クライアントからの XML-RPC 呼び出しに応答します。Red Hat Virtualization Manager は VDSM クライアントとして機能します。

A.2. VDSM フック

VDSM はフックを介して拡張可能です。フックは、重要なイベントが発生したときにホスト上で実行されるスクリプトです。サポートされるイベントが発生すると、VDSM はホスト上の `/usr/libexec/vdsm/hooks/nn_event-name/` にある実行可能なフックスクリプトを英数字順に実行します。慣例により、各フックスクリプトには、ファイル名の前に含まれる 2 衔の番号が割り当てられ、スクリプトが実行される順序が明確になります。任意のプログラミング言語でフックスクリプトを作成できますが、この章に含まれる例では Python が使用されます。

イベントのホストで定義されたすべてのスクリプトが実行されることに注意してください。特定のフックがホストで実行される仮想マシンのサブセットに対してのみ実行される必要がある場合は、仮想マシンに関連付けられた **カスタムプロパティー** を評価することで、フックスクリプト自体がこの要件を処理するようにする必要があります。



A.3. フックを使用した VDSM の拡張

この章では、イベント駆動型フックを使用して VDSM を拡張する方法について説明します。フックを使用して VDSM を拡張することは実験的な技術であり、この章は経験豊富な開発者を対象としています。仮想マシンにカスタムプロパティーを設定することで、フックスクリプトに仮想マシン固有のパラメーターを追加で渡すことができます。

A.4. サポートされている VDSM イベント

表A.1 サポートされている VDSM イベント

Name	説明
before_vm_start	仮想マシンが起動する前。

Name	説明
after_vm_start	仮想マシンの起動後。
before_vm_cont	仮想マシンが続行する前。
after_vm_cont	仮想マシンが続行した後。
before_vm_pause	仮想マシンが一時停止する前。
after_vm_pause	仮想マシンが一時停止した後。
before_vm_hibernate	仮想マシンが休止状態になる前。
after_vm_hibernate	仮想マシンが休止した後。
before_vm_dehibernate	仮想マシンが休止状態でなくなる前。
after_vm_dehibernate	仮想マシンが休止状態になった後。
before_vm_migrate_source	仮想マシンを移行する前に、移行が行われているソースホストで実行します。
after_vm_migrate_source	仮想マシンの移行後、移行が行われているソースホストで実行します。
before_vm_migrate_destination	仮想マシンを移行する前に、移行が行われている移行先ホストで実行します。
after_vm_migrate_destination	仮想マシンの移行後、移行が行われている移行先ホストで実行します。
after_vm_destroy	仮想マシンの破棄後。
before_vdsm_start	VDSM がホストで開始される前。 before_vdsm_start フックはユーザー root として実行され、VDSM プロセスの環境を継承しません。
after_vdsm_stop	VDSM がホストで停止した後。 after_vdsm_stop フックはユーザー root として実行され、VDSM プロセスの環境を継承しません。
before_nic_hotplug	NIC が仮想マシンにホットプラグされる前。
after_nic_hotplug	NIC が仮想マシンにホットプラグされた後。
before_nic_hotunplug	NIC が仮想マシンからホットプラグを抜かれる前。

Name	説明
after_nic_hotunplug	NIC が仮想マシンからホットプラグを抜かれる後。
after_nic_hotplug_fail	NIC を仮想マシンにホットプラグが失敗した後。
after_nic_hotunplug_fail	NIC が仮想マシンからホットプラグを抜かれた後。
before_disk_hotplug	ディスクが仮想マシンにホットプラグされる前。
after_disk_hotplug	ディスクが仮想マシンにホットプラグされた後。
before_disk_hotunplug	ディスクが仮想マシンからのホットプラグを抜かれる前。
after_disk_hotunplug	ディスクが仮想マシンからのホットプラグを抜かれた後。
after_disk_hotplug_fail	ディスクを仮想マシンにホットプラグが失敗した後。
after_disk_hotunplug_fail	ディスクが仮想マシンからホットプラグを抜かれた後。
before_device_create	カスタムプロパティーをサポートするデバイスを作成する前。
after_device_create	カスタムプロパティーをサポートするデバイスを作成した後。
before_update_device	カスタムプロパティーをサポートするデバイスを更新する前。
after_update_device	カスタムプロパティーをサポートするデバイスを更新した後。
before_device_destroy	カスタムプロパティーをサポートするデバイスを破棄する前。
after_device_destroy	カスタムプロパティーをサポートするデバイスを破棄した後。
before_device_migrate_destination	デバイスを移行する前に、移行が行われている宛先ホストで実行します。
after_device_migrate_destination	デバイスの移行後、移行が行われている移行先ホストで実行します。

Name	説明
before_device_migrate_source	デバイスを移行する前に、移行が行われているソースホストで実行します。
after_device_migrate_source	デバイスの移行後、移行が行われているソースホストで実行します。
after_network_setup	ホストマシンの起動時にネットワークを設定した後。
before_network_setup	ホストマシンを起動するときにネットワークを設定する前。

A.5. VDSM フック環境

ほとんどのフックスクリプトは **vdsm** ユーザーとして実行され、VDSM プロセスの環境を継承します。例外は、**before_vdsm_start** および **after_vdsm_stop** イベントによってトリガーされるフックスクリプトです。これらのイベントによってトリガーされるフックスクリプトは **root** ユーザーとして実行され、VDSM プロセスの環境を継承しません。

A.6. VDSM フックドメイン XML オブジェクト

フックスクリプトが開始されると、**_hook_domxml** 変数が環境に追加されます。この変数には、関連する仮想マシンの libvirt ドメイン XML 表現のパスが含まれています。以下に概説するように、いくつかのフックはこのルールの例外です。

以下のフックの **_hook_domxml** 変数には、仮想マシンではなく NIC の XML 表現が含まれます。

- ***_nic_hotplug_***
- ***_nic_hotunplug_***
- ***_update_device**
- ***_device_create**
- ***_device_migrate_***



重要

before_migration_destination および **before_dehibernation** フックは現在、ソースホストからドメインの XML を受信します。配信先のドメインの XML には様々な差異が生じます。

VDSM では、仮想マシンの定義に libvirt domain XML 形式を使用します。libvirt ドメイン XML 形式の詳細は、<http://libvirt.org/formatdomain.html> を参照してください。仮想マシンの UUID はドメイン XML から推測できますが、環境変数 **vmlid** としても利用できます。

A.7. カスタムプロパティーの定義

Red Hat Virtualization Manager によって受け入れられ、次にカスタムフックに渡されるカスタムプロパティーは **engine-config** コマンドを使用して定義されます。このコマンドは、Red Hat Virtualization Manager がインストールされているホストで **root** ユーザーとして実行します。

UserDefinedVMProperties および **CustomDeviceProperties** 設定キーは、サポートされているカスタムプロパティーの名前を格納するために使用されます。名前付きの各カスタムプロパティーの有効な値を定義する正規表現も、これらの設定キーに含まれています。

複数のカスタムプロパティーはセミコロンで区切られます。設定キーを設定すると、そこに含まれている既存の値が上書きされることに注意してください。新規および既存のカスタムプロパティーを組み合わせる場合は、キーの値を設定するために使用されるコマンドのすべてのカスタムプロパティーを含める必要があります。

設定キーが更新されたら、新しい値を有効にするために **ovirt-engine** サービスを再起動する必要があります。

例A.1 仮想マシンのプロパティー - スマートカードのカスタムプロパティーの定義

1. 次のコマンドを使用して、**UserDefinedVMProperties** 設定キーによって定義された既存のカスタムプロパティーを確認します。

```
# engine-config -g UserDefinedVMProperties
```

以下の出力で示されているように、カスタムプロパティー **memory** はすでに定義されています。正規表現 **^[0-9]+\$** は、カスタムプロパティーに数字のみが含まれるようにします。

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 3.6
UserDefinedVMProperties: version: 4.0
UserDefinedVMProperties : memory=^[0-9]+$ version: 4.0
```

2. **memory** カスタムプロパティーは **UserDefinedVMProperties** 設定キーにすでに定義されているため、新しいカスタムプロパティーを追加する必要があります。追加のカスタムプロパティーである **smartcard** が設定キーの値に追加されます。新しいカスタムプロパティーは、**true** または **false** の値を保持できます。

```
# engine-config -s UserDefinedVMProperties='memory=^[0-9]+$;smartcard=^(true|false)$'
--cver=4.0
```

3. **UserDefinedVMProperties** 設定キーで定義されたカスタムプロパティーが正しく更新されていることを確認します。

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

4. 最後に、設定の変更を有効にするには、**ovirt-engine** サービスを再起動する必要があります。

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

例A.2 デバイスプロパティー：*interface* カスタムプロパティーの定義

- 次のコマンドを使用して、**CustomDeviceProperties** 設定キーで定義されている既存のカスタムプロパティーを確認します。

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

以下の出力に示されるように、カスタムプロパティーはまだ定義されていません。

```
# engine-config -g CustomDeviceProperties
CustomDeviceProperties: version: 3.6
CustomDeviceProperties: version: 4.0
```

- interface** カスタムプロパティーはまだ存在しないため、そのまま追加できます。この例では、**speed** サブプロパティーの値は 0 ~ 99999 の範囲に設定され、**duplex** サブプロパティーの値は **full** または **half** のいずれかの選択に設定されます。

```
# engine-config -s CustomDeviceProperties="{type=interface;prop={speed=^(0-9]{1,5});duplex=^(full|half)}}" --cver=4.0
```

- CustomDeviceProperties** 設定キーで定義されたカスタムプロパティーが正しく更新されていることを確認します。

```
# 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
```

- 最後に、設定の変更を有効にするには、**ovirt-engine** サービスを再起動する必要があります。

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

A.8. 仮想マシンのカスタムプロパティーの設定

Red Hat Virtualization Manager でカスタムプロパティーを定義したら、仮想マシンでの設定を開始できます。カスタムプロパティーは、管理ポータルの **New Virtual Machine** および **Edit Virtual Machine** ウィンドウの **Custom Properties** タブに設定されます。

Run Virtual Machine (s) ダイアログボックスからカスタムプロパティーを設定することもできます。**Run Virtual Machine (s)** ダイアログボックスから設定されたカスタムプロパティーは、次にシャットダウンされるまで仮想マシンにのみ適用されます。

Custom Properties タブには、定義済みのカスタムプロパティーのリストから選択する機能があります。カスタムプロパティーキーを選択すると、追加のフィールドが表示され、そのキーの値を入力できます。+ ボタンをクリックしてキーと値のペアを追加し、- ボタンをクリックしてそれらを削除します。

A.9. VDSM フックでの仮想マシンのカスタムプロパティーの評価

仮想マシンの **Custom Properties** フィールドに設定された各キーは、フックスクリプトを呼び出すときに環境変数として追加されます。カスタムプロパティー フィールドの検証に使用される正規表現は保護を提供しますが、スクリプトでは、提供された入力が期待どおりと一致するかも確認する必要があります。

例A.3 カスタムプロパティーの評価

この短い Python の例では、カスタムプロパティー **key1** が存在することを確認します。カスタムプロパティーが設定されている場合は、その値が標準エラーに出力されます。カスタムプロパティーが設定されていないと、アクションは実行されません。

```
#!/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. VDSM フックモジュールの使用

VDSM には Python フックモジュールが付属しており、VDSM フックスクリプトのヘルパー関数を提供します。このモジュールは例として提供されており、Python で記述された VDSM フックにのみ関連しています。

フックモジュールは、仮想マシンの libvirt XML の DOM オブジェクトへの読み取りをサポートします。フックスクリプトは Python の組み込み **xml.dom** ライブラーー^{<http://docs.python.org/release/2.6/library/xml.dom.html>} を使用してオブジェクトを操作できます。

変更されたオブジェクトは、フックモジュールを使用して libvirt XML に保存して戻すことができます。フックモジュールは、フック開発をサポートするために次の機能を提供します。

表A.2 フックモジュール機能

Name	引数	説明
tobool	string	文字列 "true" または "false" を布尔値に変換
read_domxml	-	仮想マシンの libvirt XML を DOM オブジェクトに読み込みます。
write_domxml	DOM オブジェクト	DOM オブジェクトから仮想マシンの libvirt XML を書き込みます。

A.11. VDSM フックの実行

before_vm_start スクリプトは、ドメイン XML を編集して、仮想マシンが libvirt に到達する前に仮想

マシンの VDSM の定義を変更できます。その際には注意が必要です。フックスクリプトは VDSM の動作を混乱させる可能性があり、バグのあるスクリプトは Red Hat Virtualization 環境の停止につながる可能性があります。特に、ドメインの UUID を変更しないようにし、十分な背景知識がない限り、ドメインからデバイスを削除しようとしてください。

before_vdsdm_start と **after_vdsdm_stop** の両方のフックスクリプトが **root** ユーザーとして実行されます。システムへの **root** アクセスを必要とする他のフックスクリプトは、特権の昇格に **sudo** コマンドを使用して記述する必要があります。これをサポートするには、**/etc/sudoers** を更新して、**vdsdm** ユーザーがパスワードを再入力せずに **sudo** を使用できるようにする必要があります。これは、フックスクリプトが非対話的に実行されるために必要です。

例A.4 VDSM フックの **sudo** の設定

この例では、**sudo** コマンドは、**vdsdm** ユーザーが **root** として **/bin/chown** コマンドを実行できるように設定されます。

1. **root** として仮想化ホストにログインします。
2. テキストエディターで **/etc/sudoers** ファイルを開きます。
3. 次の行をファイルに追加します。

```
vdsdm ALL=(ALL) NOPASSWD: /bin/chown
```

これは、**vdsdm** ユーザーが **root** ユーザーとして **/bin/chown** コマンドを実行することができることを指定します。**NOPASSWD** パラメーターは、**sudo** を呼び出すときにユーザーがパスワードの入力を要求されないことを示しています。

この設定変更により、VDSM フックは **sudo** コマンドを使用して **/bin/chown** を **root** として実行できるようになりました。この Python コードは、**sudo** を使用して、ファイル **/my_file** で **/bin/chown** を **root** として実行します。

```
retcode = subprocess.call( ["/usr/bin/sudo", "/bin/chown", "root", "/my_file"] )
```

フックスクリプトの標準エラーストリームは、VDSM のログに収集されます。この情報は、フックスクリプトをデバッグするのに使用されます。

A.12. VDSM フックの戻りコード

フックスクリプトは、[表A.3 「フックリターンコード」](#) に表示される戻りコードの1つを返す必要があります。戻りコードは、さらにフックスクリプトが VDSM によって処理されるかどうかを判別します。

表A.3 フックリターンコード

コード	説明
0	フックスクリプトは正常に終了しました
1	フックスクリプトが失敗しました。他のフックを処理する必要があります

コード	説明
2	フックスクリプトが失敗しました。これ以上フックを処理する必要はありません
>2	予約

A.13. VDSM フックの例

このセクションで提供されているフックスクリプトの例は、Red Hat では厳密にはサポートされていません。ソースに関係なく、システムにインストールするすべてのフックスクリプトが、環境に対して徹底的にテストされていることを確認する必要があります。

例A.5 NUMA ノードのチューニング

目的:

このフックスクリプトを使用すると、**numaset** カスタムプロパティーに基づいて NUMA ホストのメモリー割り当てを調整できます。カスタムプロパティーが設定されていない場合、アクションは実行されません。

Configuration String:

```
numaset=^(interleave|strict|preferred):[^\]?\\d+(-\\d+)?([^\]?\\d+(-\\d+)?)*$
```

使用される正規表現により、特定の仮想マシンの **numaset** カスタムプロパティーは割り当てモード（**インターリーブ**、**厳格**、**優先**）と使用するノードの両方を指定できます。2つの値はコロン（:）で区切られます。正規表現を使用すると、**nodeset** を以下のように指定できます。

- 特定のノード（ノード1のみを使用することを指定する **numaset=strict:1**）、または
- ノードの範囲が使用される（ノード1から4が使用されることを指定する **numaset=strict:1-4**）、または
- 特定のノードが使用されていないこと（ノード3が使用されていないことを指定する **numaset = strict:^ 3**）、または
- 上記のコンマ区切りの組み合わせ（**numaset=strict:1-4,6** は、ノード1から4、および6を使用することを指定します）。

スクリプト:

/usr/libexec/vdsmd/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)
```

付録B カスタムネットワークプロパティー

B.1. BRIDGE_OPTS パラメーターの説明

表B.1 bridge_opts パラメーター

パラメーター	説明
forward_delay	ブリッジがリスニング状態とラーニング状態で費やす時間をデシ秒単位で設定します。この時点ですスイッチングループが検出されない場合、ブリッジは転送状態になります。これにより、通常のネットワーク操作の前に、ネットワークのトラフィックおよびレイアウトを検査する時間ができます。
gc_timer	ガベージコレクションの時間をデシ秒単位で設定します。その後、転送データベースがチェックされ、タイムアウトしたエントリーが消去されます。
group_addr	一般的なクエリーを送信する場合は、0に設定します。グループ固有のクエリー、またはグループとソース固有のクエリーを送信する場合は、IP マルチキャストアドレスに設定します。
group_fwd_mask	ブリッジがリンクローカルグループアドレスを転送できるようにします。この値をデフォルトから変更すると、非標準のブリッジ動作が可能になります。
hash_elasticity	ハッシュテーブルで許可されるチェーンの最大長。次の新しいマルチキャストグループが追加されるまで有効になりません。再ハッシュ後にこれが満たされない場合は、ハッシュの競合が発生し、スヌーピングが無効になります。
hash_max	ハッシュテーブルのバケット数の最大値。これはすぐに有効になり、現在のマルチキャストグループエントリーの数より少ない値に設定することはできません。値は2の累乗でなければなりません。
hello_time	hello メッセージを送信してからネットワークトポジー内のブリッジの位置を通知するまでの時間間隔をデシ秒単位で設定します。このブリッジがスパングツリールートブリッジである場合にのみ適用されます。
hello_timer	最後の hello メッセージが送信されてからの時間(デシ秒単位)。

パラメーター	説明
max_age	他のルートブリッジから hello メッセージを受け取つてから、そのブリッジがデッドとなったとみなされ、引き継ぎが開始されるまでの最大時間をデシ秒単位で設定します。
multicast_last_member_count	ホストから leave group メッセージを受け取った後、マルチキャストグループに送信する last member クエリーの回数を設定します。
multicast_last_member_interval	最後のメンバークエリー間の時間をデシ秒単位で設定します。
multicast_membership_interval	ブリッジがホストへのマルチキャストトラフィックの送信を停止する前に、ブリッジがマルチキャストグループのメンバーからの応答を待機する時間をデシ秒単位で設定します。
multicast_querier	ブリッジがマルチキャストクエリーをアクティブに実行するかどうかを設定します。ブリッジが他のネットワークホストからマルチキャストホストメンバーシップクエリーを受信すると、そのホストはクエリーを受け取った時刻にマルチキャストクエリー間隔を加えた時間に基づいて追跡されます。ブリッジが後でそのマルチキャストメンバーシップのトラフィックを転送しようとした場合、またはクエリーを実行しているマルチキャストルーターと通信している場合は、このタイマーはクエリアーの有効性を確認します。有効な場合、マルチキャストトラフィックはブリッジの既存のマルチキャストメンバーシップテーブル経由で配信されます。有効でなくなると、トラフィックはすべてのブリッジポートを介して送信されます。マルチキャストメンバーシップのあるブロードキャストドメインは、パフォーマンス向上させるために少なくとも1つのマルチキャストクエリーを実行する必要があります。
multicast_querier_interval	ホストから受け取った最後のマルチキャストホストメンバーシップクエリー間の最大時間をデシ秒単位で設定して、それがまだ有効であることを確認します。
multicast_query_use_ifaddr	ブール値。デフォルトは0です。この場合、クエリアーはIPv4メッセージの送信元アドレスとして0.0.0.0を使用します。これを変更すると、ブリッジIPが送信元アドレスとして設定されます。

パラメーター	説明
multicast_query_interval	マルチキャストメンバーシップの有効性を確保するために、ブリッジによって送信されるクエリーメッセージ間の時間をデシ秒単位で設定します。このとき、またはブリッジがそのメンバーシップのマルチキャストクエリーを送信するように要求された場合、ブリッジは、チェックが要求された時間と multicast_query_interval に基づいて、自身のマルチキャストクエリーアの状態をチェックします。このメンバーシップのマルチキャストクエリーが最後の multicast_query_interval 内に送信された場合、それは再度送信されません。
multicast_query_response_interval	ホストが送信後のクエリーに応答できる時間の長さ（デシ秒単位）。multicast_query_interval の値以下である必要があります。
multicast_router	マルチキャストルーターが接続されているポートの有効/無効を設定します。1つ以上のマルチキャストルーターを備えたポートは、すべてのマルチキャストトラフィックを受信します。値 0 は完全に無効になり、値 1 はシステムがクエリーに基づいてルーターの存在を自動的に検出できるようにし、値 2 はポートが常にすべてのマルチキャストトラフィックを受信できるようにします。
multicast_snooping	スヌーピングの有効/無効を切り替えます。スヌーピングにより、ブリッジはルーターとホスト間のネットワークトラフィックをリッスンし、適切なリンクへのマルチキャストトラフィックをフィルタリングするためのマップを維持します。このオプションを使用すると、ユーザーはハッシュの競合により自動的に無効になった場合にスヌーピングを再度有効にできます。ただし、ハッシュの競合が解決されていない場合は、スヌーピングは再度有効になりません。
multicast_startup_query_count	メンバーシップ情報を決定するのに起動時に送信されるクエリーの数を設定します。
multicast_startup_query_interval	メンバーシップ情報を決定するために起動時に送信されるクエリー間の時間をデシ秒単位で設定します。

B.2. RED HAT VIRTUALIZATION MANAGER を使用するように RED HAT VIRTUALIZATION MANAGER を設定する方法

管理ポータルから、ホストネットワークインターフェイスカードの ethtool プロパティーを設定できます。`ethtool_opts` キーはデフォルトでは使用できないため、エンジン設定ツールを使用して Manager に追加する必要があります。ホストに必要な VDSM フックパッケージもインストールする必要があります。

手順B.1 ethtool_opts キーの Manager への追加

- Manager で以下のコマンドを実行してキーを追加します。

```
# engine-config -s UserDefinedNetworkCustomProperties=ethtool_opts=.* --cver=4.0
```

- ovirt-engine** サービスを再起動します。

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

- ethtool プロパティーを設定するホストに、VDSM フックパッケージをインストールします。Red Hat Virtualization Host ではこのパッケージがデフォルトで利用可能ですが、Red Hat Enterprise Linux ホストにインストールする必要があります。

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

ethtool_opts キーが管理ポータルで利用できるようになりました。ethtool プロパティーを論理ネットワークに適用するには、「[ホストのネットワークインターフェイスの編集とホストへの論理ネットワークの割り当て](#)」を参照してください。

B.3. FCOE を使用するように RED HAT VIRTUALIZATION MANAGER を設定する方法

管理ポータルから、ホストネットワークインターフェイスカードの Fibre Channel over Ethernet (FCoE) プロパティーを設定できます。**fcoe** キーはデフォルトでは利用できないため、エンジン設定ツールを使用して Manager に追加する必要があります。以下のコマンドを実行して、**fcoe** がすでに有効になっているかどうかを確認できます。

```
# engine-config -g UserDefinedNetworkCustomProperties
```

ホストに必要な VDSM フックパッケージもインストールする必要があります。ホストの FCoE カードによっては、特別な設定が必要になる場合があります。『Red Hat Enterprise Linux Storage Administration Guide』の [Configuring a Fibre Channel over Ethernet Interface](#) を参照してください。

手順B.2 Manager への fcoe キーの追加

- Manager で以下のコマンドを実行してキーを追加します。

```
# engine-config -s UserDefinedNetworkCustomProperties='fcoe=^(enable|dcb|auto_vlan)=(yes|no),?)*$'
```

- ovirt-engine** サービスを再起動します。

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

- FCoE プロパティーを設定する各 Red Hat Enterprise Linux ホストに VDSM フックパッケージをインストールします。Red Hat Virtualization Host (RHVH) では、デフォルトでパッケージが利用可能です。

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

fcoe キーが管理ポータルで利用できるようになりました。FCoE プロパティーを論理ネットワークに適用するには、「[ホストのネットワークインターフェイスの編集とホストへの論理ネットワークの割り当て](#)」を参照してください。

付録C RED HAT VIRTUALIZATION ユーザーインターフェイスプラグイン

C.1. RED HAT VIRTUALIZATION ユーザーインターフェイスプラグイン

Red Hat Virtualization は、非標準の機能を公開するプラグインをサポートしています。これにより、Red Hat Virtualization 管理ポータルを使用して他のシステムと統合することが容易になります。各インターフェイスプラグインは、Red Hat Virtualization で使用するためにパッケージ化および配布できるユーザーインターフェイス拡張機能のセットを表します。

Red Hat Virtualization のユーザーインターフェイスプラグインは、JavaScript プログラミング言語を使用して、クライアントで直接管理ポータルと統合します。プラグインは管理ポータルにより呼び出され、Web ブラウザーの JavaScript ランタイムで実行されます。User Interface プラグインは、JavaScript 言語とそのライブラリーを使用することができます。

実行時の主要なイベントで、管理ポータルは、管理ポータルからプラグインへの通信を表すイベントハンドラー関数を介して個々のプラグインを呼び出します。管理ポータルは複数のイベントハンドラー関数をサポートしていますが、プラグインはその実装にのみ関係する関数を宣言します。各プラグインは、プラグインを管理ポータルで使用する前に、関連するイベントハンドラー関数をプラグインブートストラップシーケンスの一部として登録する必要があります。

ユーザーインターフェイス拡張機能を駆動するプラグインから管理ポータルへの通信を容易にするために、管理ポータルはプラグイン API を個々のプラグインが使用できるグローバル(トップレベル)の pluginApi JavaScript オブジェクトとして公開します。各プラグインは個別の pluginApi インスタンスを取得し、管理ポータルがプラグインのライフサイクルに関して各プラグインのプラグイン API 関数呼び出しを制御できるようにします。

C.2. RED HAT VIRTUALIZATION USER INTERFACE PLUGIN LIFECYCLE

C.2.1. Red Hat Virtualization User Interface Plug-in のライフサイクル

User Interface Plug-in の基本的なライフサイクルは、3つのステージに分けられます。

1. プラグインの検出。
2. プラグインの読み込み。
3. プラグインブートストラップ。

C.2.2. Red Hat Virtualization ユーザーインターフェイスプラグインの検出

プラグイン記述子の作成は、プラグイン検出プロセスの最初のステップです。プラグイン記述子には、重要なプラグインメタデータおよびオプションのデフォルトのプラグイン固有の設定が含まれています。

管理ポータルの HTML ページリクエスト(**HTTP GET**)の処理の一環として、ユーザーインターフェイスプラグインインフラストラクチャーはローカルファイルシステムからプラグイン記述子を検出し、ロードしようとします。プラグイン記述子ごとに、インフラストラクチャーは、デフォルトのプラグイン固有の設定(存在する場合)をオーバーライドし、プラグインの実行時の動作を微調整するのに使用される、対応するプラグインユーザー設定もロードしようとします。プラグインのユーザー設定は任意です。記述子と対応するユーザー設定ファイルをロードした後、oVirt Engine はユーザーインターフェイスプラグインデータを集約し、ランタイム評価のために管理ポータルの HTML ページに埋め込みます。

デフォルトでは、プラグイン記述子は **\$ENGINE_USR/ui-plug-ins** にあり、oVirt Engine ローカル設定で定義されている **ENGINE_USR=/usr/share/ovirt-engine** のデフォルトマッピングがあります。プラグイン記述子は JSON 形式の仕様に準拠することが期待されていますが、プラグイン記述子では、JSON 形式の仕様に加えて (* と // の両方の) Java/C++ スタイルのコメントを使用できます。

デフォルトでは、プラグインのユーザー設定ファイルは **\$ENGINE_ETC/ui-plug-ins** にあり、oVirt Engine ローカル設定で定義されている **ENGINE_ETC=/etc/ovirt-engine** のデフォルトマッピングがあります。プラグインのユーザー設定ファイルは、プラグイン記述子と同じコンテンツ形式の規則に準拠する必要があります。



注記

プラグインのユーザー設定ファイルは、通常、<**descriptorFileName>-config.json** 命名規則に従います。

C.2.3. Red Hat Virtualization User Interface Plug-in のロード

プラグインが検出され、そのデータが管理ポータルの HTML ページに埋め込まれた後、管理ポータルは、アプリケーションの起動の一部としてプラグインを読み込もうとします（アプリケーションの起動の一部として読み込まれないように設定した場合を除く）。

検出されたプラグインごとに、管理ポータルはホストページの読み込みに使用される HTML iframe 要素を作成します。プラグインホストページは、プラグインのブートストラッププロセスを開始するために必要です。このプロセス（ブートストラッププロセス）は、プラグインの iframe 要素のコンテキストでプラグインコードを評価するために使用されます。ユーザーインターフェイスプラグインインフラストラクチャーは、ローカルファイルシステムからのプラグインリソースファイル（プラグインホストページなど）の提供をサポートします。プラグインホストページが iframe 要素に読み込まれ、プラグインコードが評価されます。プラグインコードが評価された後、プラグインはプラグイン API を使用して管理ポータルと通信します。

C.2.4. Red Hat Virtualization ユーザインターフェイスプラグインブートストラップ

一般的なプラグインブートストラップシーケンスは、次の手順で設定されます。

手順C.1 プラグインブートストラップシーケンス

1. 指定されたプラグインの pluginApi インスタンスを取得します
2. ランタイムプラグイン設定オブジェクトを取得（オプション）
3. 関連するイベントハンドラー関数の登録
4. UI プラグインインフラストラクチャーにプラグインの初期化を進めるよう通知します。

次のコードは、上記の手順を実際に示すものです。

```
// 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({
    // UilInit event handler function.
    UilInit: function() {
        // Handle UilInit event.
        window.alert('Favorite music band is ' + config.band);
    }
});

// Notify UI plug-in infrastructure to proceed with plug-in initialization.
api.ready();
```

C.3. ユーザーインターフェイスプラグイン関連のファイルとその場所

表C.1 UI プラグイン関連のファイルとその場所

File	場所	備考
プラグイン記述子ファイル（メタデータ）	/usr/share/ovirt-engine/ui-plugins/my-plugin.json	
プラグインユーザー設定ファイル	/etc/ovirt-engine/ui-plugins/my-plugin-config.json	
プラグインリソースファイル	/usr/share/ovirt-engine/ui-plugins/<resourcePath>/PluginHostPage.html	<resourcePath> は、プラグイン記述子の対応する属性によって定義されます。

C.4. ユーザーインターフェイスプラグインのデプロイメント例

以下の手順に従って、Red Hat Virtualization Manager 管理ポータルへのサインイン時に **Hello World!** プログラムを実行するユーザーインターフェイスプラグインを作成します。

手順C.2 Hello World!のデプロイプラグイン

1. /usr/share/ovirt-engine/ui-plugins/helloWorld.json の Manager で以下のファイルを作成して、プラグイン記述子を作成します。

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

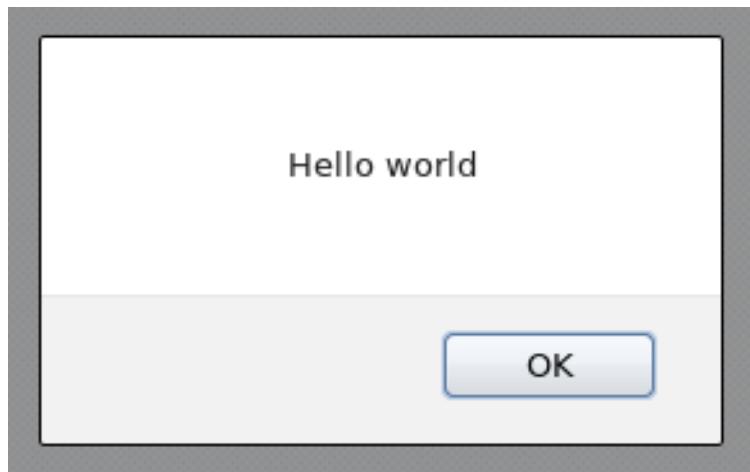
2. /usr/share/ovirt-engine/ui-plugins/hello-files/start.html の Manager で以下のファイルを作成して、プラグインホストページを作成します。

```
<!DOCTYPE html><html><head>
```

```
<script>
  var api = parent.pluginApi('HelloWorld');
  api.register({
    Uilnt: function() { window.alert('Hello world'); }
  });
  api.ready();
</script>
</head><body></body></html>
```

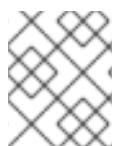
Hello World! プラグインが正常に実装されている場合は、管理ポータルにログインすると、この画面が表示されます。

図C.1 Hello World!の実装の成功プラグイン



C.5. RED HAT サポートプラグインの使用

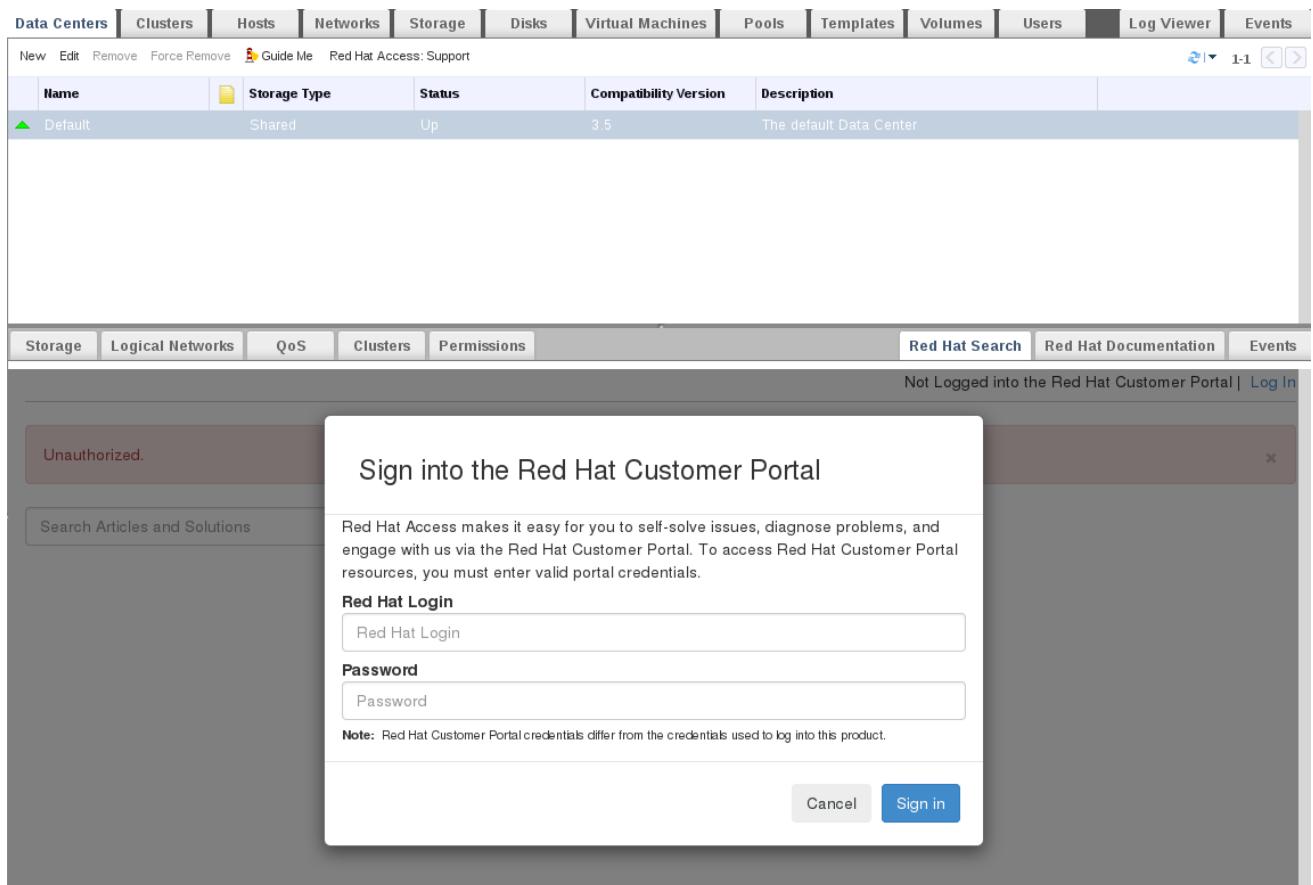
Red Hat Access プラグインを使用すると、Red Hat Virtualization 管理ポータルから Red Hat アクセスサービスを使用できます。Red Hat ログイン認証情報を使用してログインする必要があります。Red Hat Access プラグインは、ログインしていないタイミングを検出します。ログインしていない場合は、ログインウィンドウが開きます。



注記

Red Hat Virtualization 管理ポータルの認証情報は、ユーザーの Red Hat ログインと同じではありません。

図C.2 Red Hat サポートプラグイン - ログインウィンドウ



ログインすると、Red Hat カスタマー ポータルにアクセスできるようになります。Red Hat Support Plug-in は、詳細ペインと、Red Hat Virtualization 管理ポータルのいくつかのコンテキストメニューから入手できます。検索バーを使用して Red Hat Access データベースを検索します。検索結果は、詳細ペインの左側のナビゲーションリストに表示されます。

図C.3 Red Hat サポートプラグイン - 左矢印のナビゲーションリストでの結果のクエリー

The screenshot shows the Red Hat Virtualization Administrator Portal interface. At the top, there's a navigation bar with tabs for Data Centers, Clusters, Hosts, Networks, Storage, Disks, Virtual Machines, Pools, Templates, Volumes, Users, Log Viewer, and Events. Below the navigation bar is a toolbar with New, Edit, Remove, Force Remove, Guide Me, and Red Hat Access: Support buttons. The main content area displays a table for Data Centers, with one row for 'Default' (Storage Type: Shared, Status: Up, Compatibility Version: 3.5, Description: The default Data Center). Below the table are tabs for Storage, Logical Networks, QoS, Clusters, and Permissions, along with links for Red Hat Search, Red Hat Documentation, and Events. On the left, a sidebar titled 'Recommendations' lists several items, with 'RHEV: Troubleshooting RHEV-M Installation' currently selected. To the right of the sidebar, sections for Environment (Red Hat Enterprise Virtualization Manager (RHEV-M) v.3.0) and Issue (describing troubleshooting for RHEV-M installation) are shown. A search bar at the top left contains 'RHEV'.

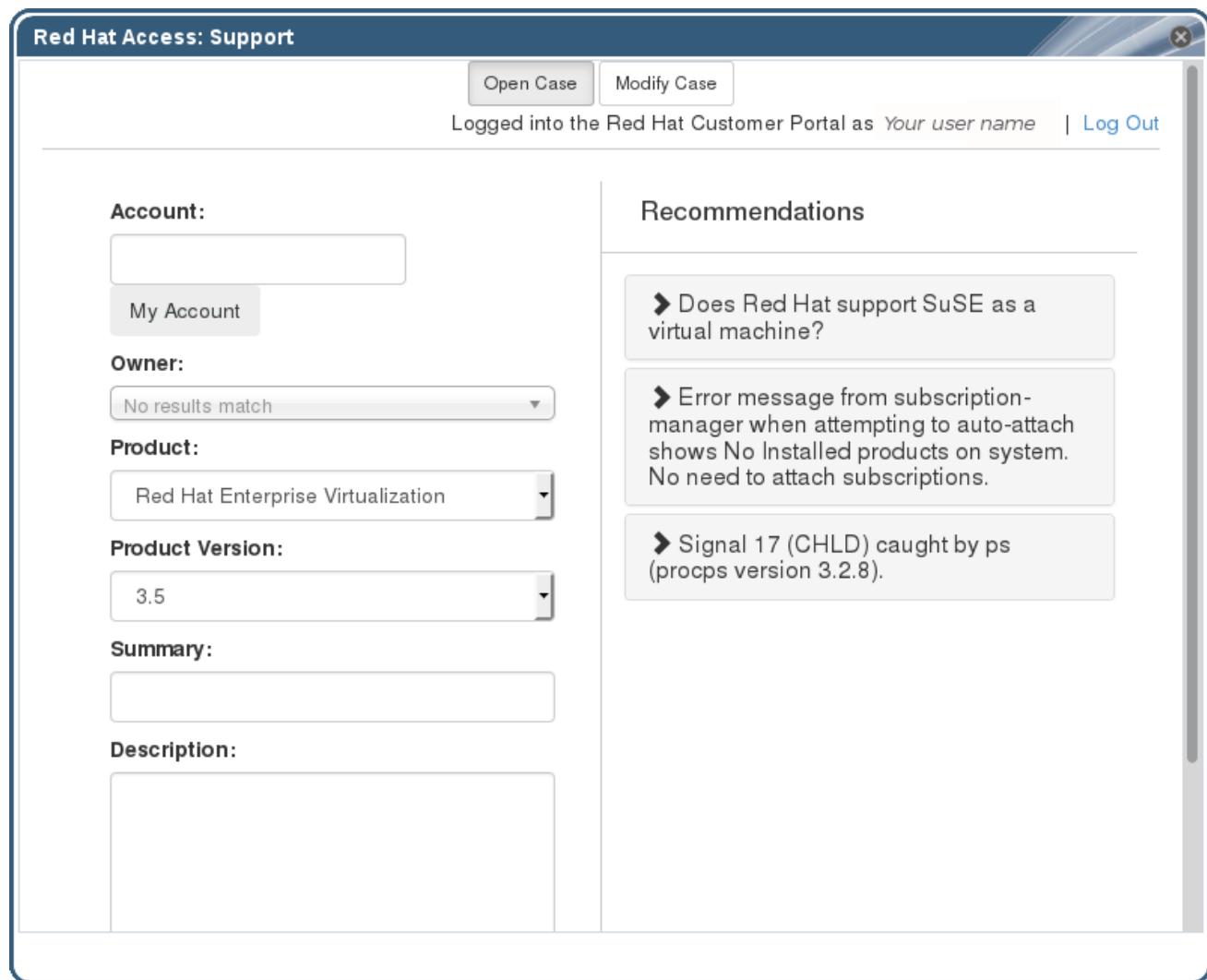
Red Hat Virtualization Administrator Portal のコンテキストメニューを右クリックし、Red Hat Support Plug-in にアクセスします。

図C.4 コンテキストメニューを右クリックして Red Hat サポートプラグインにアクセスする

The screenshot shows the Red Hat Virtualization Administrator Portal interface. At the top, there's a navigation bar with tabs for Data Centers, Clusters, Hosts, Networks, Storage, and Disks. Below the navigation bar is a toolbar with New, Edit, Remove, Force Remove, Guide Me, and Red Hat Access: Support buttons. The main content area displays a table for Data Centers, with one row for 'Default' (Name: Default, Storage Type: Shared, Status: Up). A context menu is open over the 'Default' entry, listing options: New, Edit, Remove, Force Remove, Guide Me, Re-Initialize Data Center, and Red Hat Access: Support. The 'Red Hat Access: Support' option is highlighted. The 'Red Hat Access: Support' button in the toolbar is also highlighted.

Open New Support Case を選択するか、既存のケースボタンを変更して、新しいサポートケースを作成するか、既存のケースを変更します。

図C.5 Red Hat サポートプラグイン - 新しいサポートケースを開く



Red Hat ドキュメント タブを選択して、現在画面上にある管理ポータルの一部に関連するドキュメントを開きます。

図C.6 Red Hat サポートプラグイン - ドキュメントへのアクセス

The screenshot shows a web-based administration interface for Red Hat Virtualization. At the top, there's a navigation bar with tabs for Data Centers, Clusters, Hosts, Networks, Storage, Disks, Virtual Machines, Pools, Templates, Volumes, Users, Log Viewer, and Events. Below the navigation bar is a toolbar with New, Edit, Remove, Force Remove, Guide Me, and Red Hat Access: Support buttons. A search bar at the top right contains the text '1-1'.

Name	Storage Type	Status	Compatibility Version	Description
Default	Shared	Up	3.5	The default Data Center

Below the table, there are links for Storage, Logical Networks, QoS, Clusters, and Permissions. On the right side, there are links for Red Hat Search, Red Hat Documentation, and Events. The Red Hat logo and the word 'redhat.' are visible on the left, and 'RED HAT DOCUMENTATION' is on the right.

Administration Guide

Chapter 4. Data Centers

- [4.1. Introduction to Data Centers](#)
- [4.2. The Storage Pool Manager](#)
- [4.3. SPM Priority](#)
- [4.4. Using the Events Tab to Identify Problem Objects in Data Centers](#)
- [4.5. Data Center Tasks](#)
- [4.6. Data Centers and Storage Domains](#)
- [4.7. Data Centers and Permissions](#)

4.1. Introduction to Data Centers

A data center is a logical entity that defines the set of resources used in a specific environment. A data center is considered a container resource, in that it is comprised of logical resources, in the form of clusters and hosts; network resources, in the form of logical networks and physical NICs; and storage resources, in the form of storage domains.

付録D RED HAT VIRTUALIZATION および SSL

D.1. RED HAT VIRTUALIZATION MANAGER SSL/TLS 証明書の置き換え



警告

`/etc/pki` ディレクトリーまたはサブディレクトリーのパーミッションおよび所有権は変更しないでください。`/etc/pki` および `/etc/pki/ovirt-engine` ディレクトリーのパーミッションは、デフォルトの 755 のままにする必要があります。

組織のサードパーティ CA 証明書を使用して、HTTPS 経由で接続するユーザーに Red Hat Virtualization Manager を識別するには、以下の手順を使用します。



注記

HTTPS 接続にサードパーティの CA 証明書を使用しても、Manager とホストとの間の認証に使用される証明書には影響しません。マネージャによって生成された自己署名証明書を引き続き使用します。

前提条件

- サードパーティの CA 証明書。これは、使用する証明書を発行した CA(認証局)の証明書です。PEM ファイルとして提供されます。証明書チェーンは、ルート証明書まで完全である必要があります。チェーンの順序は重要であり、最後の中間証明書からルート証明書までなければなりません。この手順では、サードパーティの CA 証明書が `/tmp/3rd-party-ca-cert.pem` で提供されることを前提としています。
- Apache httpd で使用する秘密鍵パスワードを含めることはできません。この手順では、`/tmp/apache.key` にあることを前提としています。
- CA が発行する証明書。この手順では、`/tmp/apache.cer` にあることを前提としています。

CA から秘密鍵と証明書を P12 ファイルで受け取った場合は、次の手順を使用してそれらを抽出します。その他のファイル形式については、CA にお問い合わせください。秘密鍵と証明書を抽出したら、[Red Hat Virtualization Manager の Apache SSL 証明書の置き換え](#) に進みます。

手順D.1 P12 バンドルからの証明書および秘密鍵の抽出

内部 CA は、内部で生成された鍵と証明書を `/etc/pki/ovirt-engine/keys/apache.p12` の P12 ファイルに保存します。Red Hat では、新しいファイルを同じ場所に保存することを推奨します。以下の手順では、新しい P12 ファイルが `/tmp/apache.p12` にあることを前提としています。

- 現在の `apache.p12` ファイルをバックアップします。

```
# cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12.bck
```

- 現在のファイルを新しいファイルに置き換えます。

```
# cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

3. 秘密鍵と証明書を必要な場所に抽出します。ファイルがパスワードで保護されている場合は、- **passin pass: password** を追加し、passwordを必要な パスワードに置き換える必要があります。

```
# 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

Red Hat Virtualization の新規インストールでは、この手順のすべてのステップを完了する必要があります。商用署名証明書が設定されている Red Hat Enterprise Virtualization 3.6 環境からアップグレードした場合は、実行する必要がある手順は1、8、および9のみです。

手順D.2 Red Hat Virtualization Manager Apache SSL 証明書の置き換え

1. CA 証明書をホスト全体のトラストストアに追加します。

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ca-trust/source/anchors
```

```
# update-ca-trust
```

2. Manager は、**/etc/pki/ovirt-engine/ca.pem** にシンボリックリンクされている **/etc/pki/ovirt-engine/apache-ca.pem** を使用するように設定されています。シンボリックリンクを削除します。

```
# rm /etc/pki/ovirt-engine/apache-ca.pem
```

3. CA 証明書を **/etc/pki/ovirt-engine/apache-ca.pem** として保存します。

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ovirt-engine/apache-ca.pem
```

4. 既存の秘密鍵と証明書をバックアップします。

```
# 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
```

5. 秘密鍵を必要な場所にコピーします。

```
# cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

6. 証明書を必要な場所にコピーします。

```
# cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

7. Apache サーバーを再起動します。

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

8. 新しいトラストストア設定ファイルを作成します。

```
# vi /etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf
```

以下の内容を追加して、ファイルを保存します。

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

9. **ovirt-engine** サービスを再起動します。

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

10. 証明書を置き換えると、ログコレクターが失敗する可能性があります。これを防ぐには、新しいログコレクター設定ファイルを作成します。

```
# vi /etc/ovirt-engine/logcollector.conf.d/99-custom-ca-cert.conf
```

以下の内容を追加して、ファイルを保存します。

```
[LogCollector]
cert-file=/etc/pki/ovirt-engine/apache-ca.pem
```

ユーザーは、HTTPS トラフィックの暗号化に使用される証明書の信頼性について警告せずに、管理ポータルおよびユーザー ポータルに接続できるようになりました。

D.2. MANAGER と LDAP サーバー間の SSL または TLS 接続の設定

Red Hat Enterprise Virtualization Manager と LDAP サーバーとの間にセキュアな接続を設定するには、LDAP サーバーのルート CA 証明書を取得し、ルート CA 証明書を Manager にコピーし、PEM でエンコードされた CA 証明書を作成します。キーストアタイプは、Java でサポートされている任意のタイプになります。以下の手順では、Java KeyStore (JKS) 形式を使用します。



注記

PEM でエンコードされた CA 証明書の作成と証明書のインポートに関する詳細は、**/usr/share/doc/ovirt-engine-extension-aaa-ldap-<version>** の README ファイルの **X.509 CERTIFICATE TRUST STORE** セクションを参照してください。

手順D.3 PEM でエンコードされた CA 証明書の作成

- Red Hat Virtualization Manager で、LDAP サーバーのルート CA 証明書を **/tmp** ディレクトリーにコピーし、**keytool** を使用してルート CA 証明書をインポートし、PEM でエンコードされた CA 証明書を作成します。以下のコマンドは、**/tmp/myrootca.pem** でルート CA 証明書をインポートし、**/etc/ovirt-engine/aaa/** の下に PEM でエンコードされた CA 証明書 **myrootca.jks** を作成します。証明書の場所とパスワードを書き留めます。インターラクティブ セットアップツールを使用している場合は、これが必要なすべての情報です。LDAP サーバーを手動で設定している場合は、残りの手順に従って設定ファイルを更新してください。

```
$ keytool -importcert -noprompt -trustcacerts -alias myrootca -file /tmp/myrootca.pem -keystore /etc/ovirt-engine/aaa/myrootca.jks -storepass password
```

2. **/etc/ovirt-engine/aaa/profile1.properties** ファイルを証明書情報で更新します。



注記

`\${local:_basedir}` は、LDAP プロパティー設定ファイルが存在するディレクトリーで、**/etc/ovirt-engine/aaa** ディレクトリーを参照します。PEM でエンコードされた CA 証明書を別のディレクトリーに作成した場合は、**`\${local:_basedir}`** を証明書へのフルパスに置き換えます。

- startTLS (推奨) を使用するには、以下を行います。

```
# 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
```

- SSL を使用するには、以下を行います。

```
# 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
```

外部 LDAP プロバイダーの設定を続行するには、「[外部 LDAP プロバイダーの設定 \(対話型セットアップ\)](#)」を参照してください。シングルサインオン用の LDAP および Kerberos の設定を続行するには、「[Single Sign-On 用の LDAP および Kerberos の設定](#)」を参照してください。

付録E 検索、ブックマーク、およびタグの使用

E.1. 検索

E.1.1. Red Hat Virtualization での検索

管理ポータルでは、仮想マシン、ホスト、ユーザーなど、数千のリソースを管理できます。検索を実行するには、検索バーに検索クエリー（フリーテキストまたは構文ベース）を入力します。検索条件をブックマークとして保存しておけば、検索結果を必要とするたびに検索条件を再入力する必要はありません。検索では大文字小文字の区別はありません。

E.1.2. 検索構文と例

Red Hat Virtualization リソースの検索クエリーの構文は以下のとおりです。

result type: {criteria} [sortby sort_spec]

構文の例

以下の例は、検索クエリーの使用方法と、Red Hat Virtualization が検索クエリーの構築を支援する方法を理解するのに役立ちます。

表E.1 検索クエリーの例

例	結果
Hosts: Vms.status = up	稼働中の仮想マシンを実行しているすべてのホストの一覧を表示します。
Vms: domain = qa.company.com	指定されたドメインで稼働しているすべての仮想マシンの一覧を表示します。
Vms: users.name = Mary	ユーザー名が Mary のユーザーに属する全仮想マシンの一覧を表示します。
Events: severity > normal sortby time	重大度が Normal よりも高いすべての Events の一覧を表示します。

E.1.3. 自動完了の検索

管理ポータルは、有効で強力な検索クエリーの作成に役立つ自動補完を提供します。検索クエリーの各部分を入力すると、検索の次の部分を選択するドロップダウンリストが、Search Bar の下に開きます。一覧から選択して、検索の次の部分の入力/選択を続けたり、オプションを無視したりして、手動でクエリーを入力を続けたりできます。

以下の表は、管理ポータルの自動補完がクエリーの構築を助けるする方法の例を示しています。

Hosts: Vms.status = down

表E.2 自動補完を使用した検索クエリーの例

入力	表示されているリスト項目	アクション
h	Hosts (1つのオプションのみ)	ホストまたはホストを選択します。 タイプ Hosts
Hosts:	すべてのホストプロパティー	タイプ v
Hosts: v	v で始まるホストプロパティー	Vms を選択または入力 Vms
Hosts: Vms	すべての仮想マシンプロパティー	タイプ s
Hosts: Vms.s	s で始まるすべての仮想マシンプロパティー	status を選択または入力 status
Hosts: Vms.status	= !=	選択または入力 = !=
Hosts: Vms.status =	すべてのステータス値	選択または入力 down

E.1.4. 検索結果タイプオプション

結果のタイプを使用すると、以下のタイプのリソースを検索できます。

- **Vms**、仮想マシンの一覧
- ホストの一覧
- **pools**: プールの一覧
- **template**: テンプレートの一覧
- **event**: イベントのリスト。
- **Users**、ユーザーのリスト。
- **cluster**、クラスターの一覧。
- **datacenter**: データセンターの一覧
- **Storage**、ストレージドメインのリスト。

各タイプのリソースには、一意のプロパティーセットと、関連付けられたその他のリソースタイプのセットがあるため、各検索タイプには、有効な構文の組み合わせがあります。自動補完機能を使用して、有効なクエリーも簡単に作成できます。

E.1.5. 検索基準

クエリーのコロンの後に検索条件を指定できます。{criteria} の構文は以下のようになります。

<prop><operator><value>

または

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

例

以下の表は、構文の部分を示しています。

表E.3 検索基準の例

部分	説明	値	例	注記
prop	検索対象リソースのプロパティ。リソース種別のプロパティー(obj-type を参照)、またはタグ(カスタムタグ)にすることもできます。	検索対象を特定のプロパティーを持つオブジェクトに制限します。たとえば、status プロパティーでオブジェクトを検索します。	状態	該当なし
obj-type	検索対象のリソースに関連付けることができるリソースタイプ。	これは、データセンター や仮想マシンなどのシステムオブジェクトです。	Users	該当なし
operator	比較演算子。	= != (等しくない) > < >= <=	該当なし	値オプションは obj-type によって異なります。

部分	説明	値	例	注記
値	その式が何と比較されるか。	String Integer ランキング 日付 (Regional Settings に応じた書式設定)	Jones 256 normal	<ul style="list-style-type: none"> ワイルドカードは文字列内で使用できます。 "" (間にスペースがない 2つの引用符のセット) は、初期化されていない (空の) 文字列を表すために使用できます。 スペースが含まれる文字列または日付を二重引用符で囲む必要があります

E.1.6. 検索: 複数の基準およびワイルドカード

ワイルドカードは文字列の構文の `<value>` 部分で使用できます。たとえば、`m` で始まるすべてのユーザーを検索するには、`m*` を入力します。

ブール演算子の **AND** および **OR** を使用して、2つの基準を持つ検索を実行できます。以下に例を示します。

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

このクエリーは、名前が `m` で始まるユーザーに対して実行中の仮想マシンをすべて返します。

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

このクエリーは、名前が `m` で始まるユーザーに対して `paris-loc` でタグ付けされたすべての仮想マシンを返します。

AND または **OR** を使用せずに 2つの基準を指定した場合、**AND** が暗黙的に指定されます。**AND** は **OR** よりも優先され、**OR** は暗黙の **AND** よりも優先されます。

E.1.7. 検索: 検索順序の決定

返される情報の並び替え順序は、**sortby** を使用して決定できます。並べ替え方向 (昇順は **asc**、降順は **desc**) を含めることができます。

以下に例を示します。

events: severity > normal sortby time desc

このクエリーは、重大度が Normal よりも大きいすべての Events を時刻でソートして返します (降順)。

E.1.8. データセンターの検索

以下の表は、データセンターのすべての検索オプションを示しています。

表E.4 データセンターの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Clusters.clusters-prop	プロパティータイプによります。	データセンターに関連付けられたクラスターのプロパティ。
name	String	データセンターの名前。
description	String	データセンターの説明
type	String	データセンターのタイプ。
status	リスト	データセンターの可用性
sortby	リスト	返された結果をリソースプロパティの一つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Datacenter: type = nfs and status != up

以下の例では、以下が含まれるデータセンターの一覧を返します。

- NFS のストレージタイプおよび up 以外のステータス

E.1.9. クラスターの検索

以下の表は、クラスターのすべての検索オプションについて説明しています。

表E.5 クラスターの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Datacenter.datacenter-prop	プロパティータイプによります。	クラスターに関連付けられたデータセンターのプロパティ。

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Datacenter	String	クラスターが属するデータセンター。
name	String	ネットワーク上のクラスターを識別する一意の名前。
description	String	クラスターの説明。
initialized	String	クラスターのステータスを示す true または False。
sortby	リスト	返された結果をリソースプロパティの一つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Clusters: initialized = true or name = Default

この例では、以下のクラスターの一覧を返します。

- initialized、または
- 名前付きのデフォルト

E.1.10. ホストの検索

以下の表は、ホストの全検索オプションを示しています。

表E.6 ホストの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
\Vms.Vms-prop	プロパティータイプによります。	ホストに関連付けられた仮想マシンのプロパティー。
Templates.templates-prop	プロパティータイプによります。	ホストに関連付けられたテンプレートのプロパティー。
Events.events-prop	プロパティータイプによります。	ホストに関連付けられたイベントのプロパティー。
Users.users-prop	プロパティータイプによります。	ホストに関連付けられたユーザーのプロパティー。

プロパティ(リソースまたはリソースタイプの)	タイプ	説明(参照)
name	String	ホストの名前。
status	リスト	ホストの可用性。
external_status	String	外部システムおよびプラグインによって報告されるホストのヘルステータス。
cluster	String	ホストが属するクラスター。
address	String	ネットワーク上のホストを識別する一意の名前。
cpu_usage	Integer	使用される処理能力の割合。
mem_usage	Integer	使用されるメモリーの割合。
network_usage	Integer	ネットワーク使用率の割合。
load	Integer	特定のタイムスライスで、プロセッサーごとにランタイムキューで実行されるのを待機しているジョブ。
version	Integer	オペレーティングシステムのバージョン番号。
cpus	Integer	ホスト上の CPU 数。
memory	Integer	使用可能なメモリーの量。
cpu_speed	Integer	CPU の処理速度。
cpu_model	String	CPU のタイプ。
active_vms	Integer	現在実行中の仮想マシンの数。
migrating_vms	Integer	現在移行中の仮想マシンの数。
committed_mem	Integer	コミットされたメモリーの割合
tag	String	ホストに割り当てられたタグ。
type	String	ホストのタイプ。

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
datacenter	String	ホストが属するデータセンター。
sortby	リスト	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Hosts: cluster = Default and Vms.os = rhel6

以下の例では、以下のホストの一覧を返します。

- Default クラスターおよび Red Hat Enterprise Linux 6 オペレーティングシステムを実行しているホスト仮想マシンの一部です。

E.1.11. ネットワークの検索

以下の表は、ネットワークの全検索オプションを説明しています。

表E.7 ネットワークの検索

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
Cluster_network.clusternetwork-prop	プロパティータイプによります。	ネットワークに関連付けられたクラスターのプロパティ。
Host_Network.hostnetwork-prop	プロパティータイプによります。	ネットワークに関連付けられたホストのプロパティ。
name	String	ネットワークを識別するための人が判読可能な名前。
description	String	ネットワークを記述するキーワードまたはテキスト。オプションでネットワークの作成時に使用されます。
vlanid	Integer	ネットワークの VLAN ID。
stp	String	Spanning Tree Protocol (STP) がネットワークで有効または無効になっているかどうか。
mtu	Integer	論理ネットワークの最大伝送単位。

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
vmnetwork	String	ネットワークが仮想マシントラフィックのみに使用されているかどうか。
datacenter	String	ネットワークが接続されているデータセンター。
sortby	リスト	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Network: mtu > 1500 and vmnetwork = true

以下の例では、ネットワークの一覧を返します。

- 最大伝送単位が 1500 バイトを超える場合
- これは、仮想マシンのみが使用するように設定されます。

E.1.12. ストレージの検索

以下の表は、ストレージのすべての検索オプションについて説明しています。

表E.8 ストレージの検索

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
Hosts.hosts-prop	プロパティータイプによります。	ストレージに関連付けられたホストのプロパティー。
Clusters.clusters-prop	プロパティータイプによります。	ストレージに関連付けられたクラスターのプロパティー。
name	String	ネットワーク上のストレージを識別する一意の名前。
status	String	ストレージドメインのステータス。
external_status	String	外部システムおよびプラグインによって報告されるストレージドメインのヘルスステータス。

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
datacenter	String	ストレージが属するデータセンター。
type	String	ストレージのタイプ。
size	Integer	ストレージのサイズ。
used	Integer	使用中のストレージの量。
committed	Integer	コミットされるストレージの量。
sortby	リスト	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Storage: size > 200 or used < 50

以下の例では、以下が含まれるストレージの一覧を返します。

- 200 GB を超える合計ストレージ容量
- 50 GB 未満の使用ストレージ領域。

E.1.13. ディスクの検索

以下の表は、ディスクの全検索オプションを示しています。

表E.9 ディスクの検索

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
Datacenters.datacenters-prop	プロパティータイプによります。	ディスクに関連付けられたデータセンターのプロパティー。
Storages.storages-prop	プロパティータイプによります。	ディスクに関連付けられたストレージのプロパティー。
alias	String	ネットワーク上のストレージを識別する人が判読可能な名前。
description	String	ディスクを記述するキーワードまたはテキスト。オプションでディスクの作成時に使用されます。

プロパティ（リソースまたはリソースタイプの）	タイプ	説明（参照）
provisioned_size	Integer	ディスクの仮想サイズ
size	Integer	ディスクのサイズ。
actual_size	Integer	ディスクに割り当てられる実際のサイズ。
creation_date	Integer	ディスクが作成された日付。
bootable	String	ディスクを起動できるかどうか。有効な値は 0 、 1 、 yes 、 no のいずれかです。
shareable	String	ディスクを一度に複数の仮想マシンにアタッチできるかどうか。有効な値は 0 、 1 、 yes 、 no のいずれかです。
format	String	ディスクの形式。 unused 、 unassigned 、 cow 、 raw のいずれかです。
status	String	ディスクのステータス。 unassigned 、 ok 、 locked 、 invalid 、 illegal のいずれかです。
disk_type	String	ディスクのタイプ。 image または lun のいずれか。
number_of_vms	Integer	ディスクがアタッチされている仮想マシンの数。
vm_names	String	ディスクがアタッチされている仮想マシンの名前。
quota	String	仮想ディスクで強制されるクォータの名前。
sortby	リスト	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Disk: format = cow and provisioned_size > 8

この例では、以下が含まれる仮想ディスクの一覧を返します。

- QCOW: シンプロビジョニング、フォーマットとしても知られています。
- 8 GB を超える割り当て済みディスクサイズ。

E.1.14. ボリュームの検索

以下の表は、ボリュームのすべての検索オプションについて説明しています。

表E.10 ボリュームの検索

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
Volume.cluster-prop	プロパティータイプによります。	ボリュームに関連付けられたクラスターのプロパティー。
Cluster	String	ボリュームに関連付けられたクラスターの名前。
name	String	ボリュームを識別する、人が判読可能な名前。
type	String	distribute、replicate、distributed_replicate、stripe、またはdistributed_stripe のいずれか。
transport_type	Integer	TCP または RDMA のいずれか。
replica_count	Integer	レプリカの数。
stripe_count	Integer	ストライプの数。
status	String	ボリュームのステータスUp またはDown のいずれかです。
sortby	リスト	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Volume: transport_type = rdma and stripe_count >= 2

この例では、以下が含まれるボリュームの一覧を返します。

- RDMA に設定されたトランSPORTタイプ
- 2つ以上のストライプがある。

E.1.15. 仮想マシンの検索

以下の表は、仮想マシンのすべての検索オプションについて説明しています。

表E.11 仮想マシンの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Hosts.hosts-prop	プロパティータイプによります。	仮想マシンに関連付けられたホストのプロパティ。
Templates.templates-prop	プロパティータイプによります。	仮想マシンに関連付けられたテンプレートのプロパティ。
Events.events-prop	プロパティータイプによります。	仮想マシンに関連付けられたイベントのプロパティ。
Users.users-prop	プロパティータイプによります。	仮想マシンに関連付けられたユーザーのプロパティ。
Storage.storage-prop	プロパティータイプによります。	仮想マシンに関連付けられたストレージデバイスのプロパティ。
Vnic.mac-prop	プロパティータイプによります。	仮想マシンに関連付けられたMACアドレスのプロパティ。
name	String	仮想マシンの名前。
status	リスト	仮想マシンの可用性
ip	Integer	仮想マシンのIPアドレス。
uptime	Integer	仮想マシンが実行されている期間(分単位)。
domain	String	これらのマシンをグループ化するドメイン(通常は Active Directory ドメイン)。
os	String	仮想マシンの作成時に選択されたオペレーティングシステム。
creationdate	日付	仮想マシンが作成された日付。
address	String	ネットワーク上の仮想マシンを識別する一意の名前。
cpu_usage	Integer	使用される処理能力の割合。

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
mem_usage	Integer	使用されるメモリーの割合。
network_usage	Integer	使用されるネットワークの割合。
memory	Integer	定義された最大メモリー。
apps	String	仮想マシンに現在インストールされているアプリケーション。
cluster	リスト	仮想マシンが属するクラスター。
pool	リスト	仮想マシンが属する仮想マシンプール。
loggedinuser	String	仮想マシンに現在ログインしているユーザーの名前。
tag	リスト	仮想マシンが属するタグ。
datacenter	String	仮想マシンが属するデータセンター。
type	リスト	仮想マシンタイプ(サーバーまたはデスクトップ)。
quota	String	仮想マシンに関連付けられたクオータの名前。
description	String	仮想マシンを記述するキーワードまたはテキスト。オプションとして、仮想マシンの作成時に使用されます。
sortby	リスト	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。
next_run_configuration_exists	ブール値	仮想マシンに保留中の設定変更があります。

例

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

この例では、仮想マシンの一覧を返します。ここでは、以下のようになります。

- 仮想マシンのベースとなるテンプレートは Win で始まり、仮想マシンが任意のユーザーに割り当てられます。

例

Vms: cluster = Default and os = windows7

この例では、仮想マシンの一覧を返します。ここでは、以下のようになります。

- 仮想マシンが属するクラスターの名前は Default で、仮想マシンは Windows 7 オペレーティングシステムを実行しています。

E.1.16. プールの検索

以下の表は、プールの全検索オプションを示しています。

表E.12 プールの検索

プロパティー (リソースまたはリソースタイプの)	タイプ	説明 (参照)
name	String	プールの名前。
description	String	プールの説明。
type	リスト	プールのタイプ。
sortby	リスト	返された結果をリソースプロパティーの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

Pools: type = automatic

この例では、以下が含まれるプールの一覧を返します。

- 自動のタイプ

E.1.17. テンプレートの検索

以下の表は、テンプレートの全検索オプションを示しています。

表E.13 テンプレートの検索

プロパティー (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Vms.Vms-prop	String	テンプレートに関連付けられた仮想マシンのプロパティー。

プロパティ（リソースまたはリソースタイプの）	タイプ	説明（参照）
Hosts.hosts-prop	String	テンプレートに関連付けられたホストのプロパティ。
Events.events-prop	String	テンプレートに関連付けられたイベントのプロパティ。
Users.users-prop	String	テンプレートに関連付けられたユーザーのプロパティ。
name	String	テンプレートの名前。
domain	String	テンプレートのドメイン。
os	String	オペレーティングシステムのタイプ。
creationdate	Integer	テンプレートが作成された日付。 日付の形式は mm/dd/yy です。
childcount	Integer	テンプレートから作成された仮想マシンの数。
mem	Integer	定義されたメモリー。
description	String	テンプレートの説明。
status	String	テンプレートのステータス
cluster	String	テンプレートに関連付けられたクラスター。
datacenter	String	テンプレートに関連付けられたデータセンター。
quota	String	テンプレートに関連付けられたクォータ。
sortby	リスト	返された結果をリソースプロパティの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

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

以下の例では、テンプレートのリストを返します。ここでは、以下のようになります。

- テンプレートから派生した仮想マシンで、通常以上の重大度のイベントが発生し、仮想マシンはまだ実行されています。

E.1.18. ユーザーの検索

以下の表は、ユーザーの全検索オプションについて説明しています。

表E.14 ユーザーの検索

プロパティ (リソースまたはリソースタイプの)	タイプ	説明 (参照)
Vms.Vms-prop	プロパティータイプによります。	ユーザーに関連付けられた仮想マシンのプロパティ。
Hosts.hosts-prop	プロパティータイプによります。	ユーザーに関連付けられたホストのプロパティ。
Templates.templates-prop	プロパティータイプによります。	ユーザーに関連付けられたテンプレートのプロパティ。
Events.events-prop	プロパティータイプによります。	ユーザーに関連するイベントのプロパティ。
name	String	ユーザーの名前。
lastname	String	ユーザーの名字を。
username	String	ユーザーの一意の名前。
department	String	ユーザーが属する部。
group	String	ユーザーが属するグループ。
title	String	ユーザーのタイトル。
status	String	ユーザーの状態。
role	String	ユーザーのロール。
tag	String	ユーザーが属するタグ。
pool	String	ユーザーが属するプール。
sortby	リスト	返された結果をリソースプロパティの1つで並べ替えます。

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
page	Integer	表示する結果のページ番号。

例

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

この例では、以下が含まれるユーザーの一覧を返します。

- 通常の重大度より大きいイベントが仮想マシンで実行され、仮想マシンがまだ実行中である。
- ユーザーの仮想マシンは一時停止されます。

E.1.19. イベントの検索

以下の表は、イベントの検索に使用できるすべての検索オプションについて説明しています。自動補完は、必要に応じて多くのオプションに対して提供されます。

表E.15 イベントの検索

プロパティー(リソースまたはリソースタイプの)	タイプ	説明(参照)
Vms.Vms-prop	プロパティータイプによります。	イベントに関連付けられた仮想マシンのプロパティー。
Hosts.hosts-prop	プロパティータイプによります。	イベントに関連付けられたホストのプロパティー。
Templates.templates-prop	プロパティータイプによります。	イベントに関連付けられたテンプレートのプロパティー。
Users.users-prop	プロパティータイプによります。	イベントに関連付けられたユーザーのプロパティー。
Clusters.clusters-prop	プロパティータイプによります。	イベントに関連付けられたクラスターのプロパティー。
Volumes.Volumes-prop	プロパティータイプによります。	イベントに関連付けられたボリュームのプロパティー。
type	リスト	イベントのタイプ。
severity	リスト	イベントの重大度: Warning/Error/Normal
message	String	イベントタイプの説明。

プロパティ（リソースまたはリソースタイプの）	タイプ	説明（参照）
time	リスト	イベントが発生した日。
username	String	イベントに関連付けられたユーザー名。
event_host	String	イベントに関連付けられたホスト。
event_vm	String	イベントに関連付けられた仮想マシン。
event_template	String	イベントに関連付けられたテンプレート。
event_storage	String	イベントに関連付けられたストレージ。
event_datacenter	String	イベントに関連付けられたデータセンター。
event_volume	String	イベントに関連付けられたボリューム。
correlation_id	Integer	イベントの識別番号。
sortby	リスト	返された結果をリソースプロパティの1つで並べ替えます。
page	Integer	表示する結果のページ番号。

例

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

この例では、以下のイベント一覧を返します。

- イベントは、ホスト **gonzo.example.com** で実行中の **testdesktop** という名前の仮想マシンで発生しました。

E.2. ブックマーク

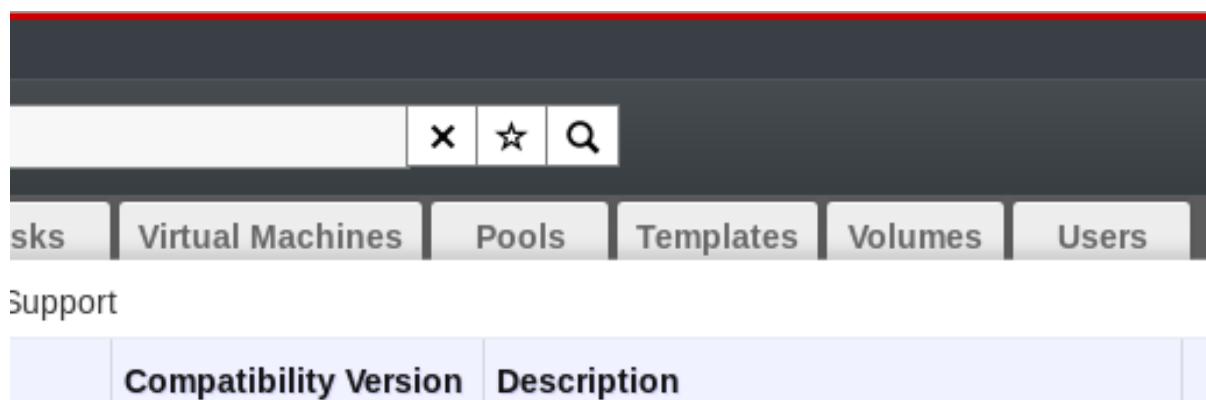
E.2.1. クエリー文字列をブックマークとして保存

ブックマークは、検索クエリーを記憶し、他のユーザーとの共有するために使用できます。

手順E.1 クエリー文字列をブックマークとして保存

1. 検索バーに希望の検索クエリーを入力し、検索を実行します。
2. 検索バーの右側にある star-shaped **Bookmark** ボタンをクリックして、**New Bookmark** ウィンドウを開きます。

図E.1 ブックマークアイコン



3. ブックマークの **Name** を入力します。
4. **検索文字列** フィールドを編集します（該当する場合）。
5. **OK** をクリックしてクエリーをブックマークとして保存し、ウィンドウを閉じます。
6. 検索クエリーが保存され、ブックマークペインに表示されます。

後で再利用できるように検索クエリーをブックマークとして保存しました。ブックマークペインを使用して、ブックマークを見つけて選択します。

E.2.2. ブックマークの編集

ブックマークの名前および検索文字列を変更できます。

手順E.2 ブックマークの編集

1. 画面の左端にある **Bookmarks** タブをクリックします。
2. 編集するブックマークを選択します。
3. **Edit** ボタンをクリックして、**Edit Bookmark** ウィンドウを開きます。
4. 必要に応じて **Name** および **Search string** フィールドを変更します。
5. **OK** をクリックして編集したブックマークを保存します。

ブックマークされた検索クエリーを編集している。

E.2.3. ブックマークの削除

ブックマークが必要なくなったら、その設定を削除します。

手順E.3 ブックマークの削除

1. 画面の左端にある **Bookmarks** タブをクリックします。

2. 削除するブックマークを選択します。
3. **Remove** ボタンをクリックして、**Remove Bookmark** ウィンドウを開きます。
4. **OK** をクリックして、選択したブックマークを削除します。

ブックマークされた検索クエリーを削除しました。

E.3. タグ

E.3.1. タグを使用して Red Hat Virtualization とのやり取りをカスタマイズ

Red Hat Virtualization プラットフォームをセットアップし、要件に合わせて設定したら、タグを使用して作業方法をカスタマイズできます。タグはシステム管理者にとって1つの主な利点を提供します。これにより、システムリソースをグループまたはカテゴリーに分類できます。これは、仮想化環境に多くのオブジェクトが存在し、管理者が特定のオブジェクトセットに集中したい場合に便利です。

このセクションでは、タグの作成と編集、ホストまたは仮想マシンへの割り当て、タグを基準として使用した検索などの方法について説明します。タグは、企業のニーズに合わせて、構造に一致する階層に配置できます。

管理ポータル Tags は、**Tags** ペインを使用して作成、変更、および削除できます。

E.3.2. タグの作成

タグを作成して、タグを使用して検索結果を絞り込みできるようにします。

手順E.4 タグの作成

1. 画面の左側にある **Tags** タブをクリックします。
2. タグを作成するノードを選択します。たとえば、最上位レベルで作成するには、ルートノードをクリックします。
3. **New** ボタンをクリックして **New Tag** ウィンドウを開きます。
4. 新規タグの **Name** および **Description** を入力します。
5. **OK** をクリックしてタグを作成します。

新しいタグが作成され、**Tags** タブに表示されます。

E.3.3. タグの変更

タグの名前と説明を編集できます。

手順E.5 タグの変更

1. 画面の左側にある **Tags** タブをクリックします。
2. 変更するタグを選択します。
3. **Edit** をクリックして **Edit Tag** ウィンドウを開きます。
4. 必要に応じて **Name** および **Description** フィールドを変更します。

5. **OK** をクリックして編集したタグを保存します。

タグのプロパティーを変更している。

E.3.4. タグの削除

タグが不要になったら、それを削除します。

手順E.6 タグの削除

1. 画面の左側にある **Tags** タブをクリックします。
2. 削除するタグを選択します。
3. **Remove** をクリックして、**Remove Tag (s)** ウィンドウを開きます。このメッセージは、タグを削除するとタグのすべての子孫も削除されることを警告します。
4. **OK** をクリックして、選択したタグを削除します。

タグとその子孫をすべて削除しました。タグは、アタッチされたすべてのオブジェクトからも削除されます。

E.3.5. オブジェクトに対するタグの追加および削除

ホスト、仮想マシン、およびユーザーにタグを割り当てたり、削除したりできます。

手順E.7 オブジェクトに対するタグの追加および削除

1. リソースタブをクリックし、タグ付けまたはタグ付け解除するオブジェクトを選択します。
2. **Assign Tags** ボタンをクリックして **Assign Tags** ウィンドウを開きます。
3. チェックボックスを選択してタグをオブジェクトに割り当てるか、選択を解除してオブジェクトからタグの割り当てを解除します。
4. **OK** をクリックします。

指定したタグが、選択したオブジェクトのカスタムプロパティーとして追加または削除されます。

E.3.6. タグを使用したオブジェクトの検索

- **tag** プロパティーとしてタグを使用し、検索条件として目的の値または値のセットを使用して、検索クエリーを入力します。

指定された基準でタグ付けされたオブジェクトは結果リストに表示されます。

付録F ブランド化

F.1. ブランド化

F.1.1. Manager の再ブランド化

ポップアップウィンドウで使用されるアイコンや表示されるテキスト、Welcome ページに表示されるリンクなど、Red Hat Virtualization Manager のさまざまな側面をカスタマイズできます。これにより、Manager のブランドを変更し、管理者およびユーザーに表示される最終的なルックアンドフィールを細かく制御することができます。

Manager のカスタマイズに必要なファイルは、Manager がインストールされているシステムの **/etc/ovirt-engine/branding/** ディレクトリーにあります。ファイルは、グラフィカルユーザーインターフェイスの様々な側面をスタイルするために使用されるカスケードスタイルシートファイルのセットと、Manager の様々なコンポーネントに組み込まれるメッセージとリンクを含むプロパティーファイルのセットで設定されています。

コンポーネントをカスタマイズするには、そのコンポーネントのファイルを編集して変更を保存します。次にそのコンポーネントを開いたり更新したりすると、変更が適用されます。

F.1.2. ログイン画面

ログイン画面は、管理ポータルとユーザーポータルの両方が使用するログイン画面です。カスタマイズできるログイン画面の要素は次のとおりです。

- ボーダー
- 左側のヘッダーイメージ
- 右側のヘッダーイメージ
- ヘッダーテキスト

ログイン画面のクラスは **common.css** にあります。

F.1.3. 管理ポータルの画面

管理ポータルの画面は、管理ポータルにログインする際に表示されるメイン画面です。カスタマイズできる管理ポータル画面の要素は、以下のとおりです。

- ロゴ
- 左側のバックグラウンドイメージ
- センターのバックグラウンドイメージ
- 右側のバックグラウンドイメージ
- ロゴの右側にあるテキスト

管理ポータル画面のクラスは **web_admin.css** にあります。

F.1.4. ユーザーポータル画面

ユーザーportal画面は、ユーザーportalにログインする際に表示される画面です。カスタマイズできるユーザーportal画面の要素は次のとおりです。

- 口ゴ
- センターのバックグラウンドイメージ
- 右側のバックグラウンドイメージ
- メイングリッド周辺の境界線
- **Logged in user** ラベルの上のテキスト

ユーザーportal画面のクラスは、**user_portal.css** にあります。

F.1.5. ポップアップウィンドウ

ポップアップウィンドウは、ホストまたは仮想マシンなどのエンティティーの作成、編集、または更新を可能にする Manager のすべてのウィンドウです。カスタマイズできるポップアップウィンドウの要素は次のとおりです。

- ボーダー
- 左側のヘッダーイメージ
- ヘッダーセンターアイメージ(繰り返し)

ポップアップウィンドウのクラスは **common.css** にあります。

F.1.6. タブ

ユーザーportalには、Basic ビューと Extended ビューを切り替えるためのメインタブと、Extended ビューが選択されている場合の画面左側のタブの 2 種類のタブがあります。管理portalの多くのポップアップウィンドウにはタブも含まれます。カスタマイズ可能なこれらのタブの要素は次のとおりです。

- Active
- 非アクティブ

タブのクラスは **common.css** および **user_portal.css** にあります。

F.1.7. Welcome ページ

Welcome ページは、Manager のホームページにアクセスする際に最初に表示されるページです。全体的なルックアンドフィールをカスタマイズするだけでなく、テンプレートファイルを編集して、追加のドキュメントや内部 Web サイトのページへのリンクを追加するなどの変更を加えることもできます。カスタマイズできる Welcome Page の要素は次のとおりです。

- ページタイトル
- ヘッダー(左、中央、右)
- エラーメッセージ
- 転送するリンクおよびそのリンクに関連するメッセージ

Welcome ページのクラスは **welcome_style.css** にあります。

テンプレートファイル

Welcome Page のテンプレートファイルは、**HTML**、**HEAD**、または **BODY** タグが含まれない **welcome_page.template** の名前の通常の HTML ファイルです。このファイルはウェルカムページ自体に直接挿入され、ウェルカムページに表示されるコンテンツのコンテナーとして機能します。そのため、このファイルを編集して、新しいリンクを追加したり、コンテンツ自体を変更したりする必要があります。テンプレートファイルのもう1つの機能は、ウェルカムページの処理時に **messages.properties** ファイルの対応するテキストに置き換えられる **{user_portal}** などのプレースホルダーテキストが含まれていることです。

F.1.8. Page Not Found ページ

Page Not Found ページは、Red Hat Virtualization Manager で見つからないページへのリンクを開くと表示されるページです。カスタマイズできる Page Not Found ページの要素は以下のとおりです。

- ページタイトル
- ヘッダー(左、中央、右)
- エラーメッセージ
- 転送するリンクおよびそのリンクに関連するメッセージ

Page Not Found ページのクラスは **welcome_style.css** にあります。

付録G システムアカウント

G.1. システムアカウント

G.1.1. Red Hat Virtualization Manager のユーザーアカウント

rhevm パッケージがインストールされると、Red Hat Virtualization をサポートするために多数のシステムユーザーアカウントが作成されます。各システムユーザーには、デフォルトのユーザー ID (UID) があります。作成されるシステムユーザーアカウントは、以下のとおりです。

- **vdsm** ユーザー(UID 36) NFS ストレージドメインをマウントおよびアクセスするサポートツールに必要です。
- **ovirt** ユーザー(UID 108)。**ovirt-engine** Red Hat JBoss Enterprise Application Platform インスタンスの所有者。
- **ovirt-vmconsole** ユーザー(UID 4 98)ゲストのシリアルコンソールに必要です。

G.1.2. Red Hat Virtualization Manager グループ

rhevm パッケージがインストールされると、Red Hat Virtualization をサポートするために多数のシステムユーザーグループが作成されます。各システムユーザーグループには、デフォルトのグループ ID (GID) があります。作成されるシステムユーザーグループは、以下のとおりです。

- **kvm** グループ(GID 36) グループメンバーには以下が含まれます。
 - **vdsm** ユーザー。
- **ovirt** グループ(GID 108)。グループメンバーには以下が含まれます。
 - **ovirt** ユーザー。
- **ovirt-vmconsole** グループ(GID 4 98) グループメンバーには以下が含まれます。
 - **ovirt-vmconsole** ユーザー。

G.1.3. 仮想化ホストのユーザーアカウント

vdsm パッケージおよび qemu-kvm-rhev パッケージがインストールされると、仮想化ホストに多数のシステムユーザーアカウントが作成されます。各システムユーザーには、デフォルトのユーザー ID (UID) があります。作成されるシステムユーザーアカウントは、以下のとおりです。

- **vdsm** ユーザー(UID 36)
- **qemu** ユーザー(UID 107)
- **sanlock** ユーザー(UID 179)
- **ovirt-vmconsole** ユーザー(UID 4 98)



重要

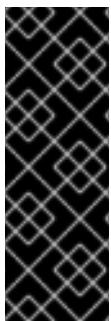
割り当てられるユーザー ID (UID) およびグループ ID (GID) は、システムによって異なる場合があります。**vdsm** ユーザーは **36** の UID に修正され、**kvm** グループは **36** の GID に固定されます。

UID **36** または GID **36** がシステム上の別のアカウントによってすでに使用されている場合は、vdsm パッケージおよび qemu-kvm-rhev パッケージのインストール時に競合が発生します。

G.1.4. 仮想化ホストグループ

vdsm パッケージおよび qemu-kvm-rhev パッケージがインストールされると、仮想化ホストに多数のシステムユーザーグループが作成されます。各システムユーザーグループには、デフォルトのグループ ID (GID) があります。作成されるシステムユーザーグループは、以下のとおりです。

- **kvm** グループ(GID **36**)グループメンバーには以下が含まれます。
 - **qemu** ユーザー。
 - **sanlock** ユーザー。
- **qemu** グループ(GID **107**)グループメンバーには以下が含まれます。
 - **vdsm** ユーザー。
 - **sanlock** ユーザー。
- **ovirt-vmconsole** グループ(GID **498**)グループメンバーには以下が含まれます。
 - **ovirt-vmconsole** ユーザー。



重要

割り当てられるユーザー ID (UID) およびグループ ID (GID) は、システムによって異なる場合があります。**vdsm** ユーザーは **36** の UID に修正され、**kvm** グループは **36** の GID に固定されます。

UID **36** または GID **36** がシステム上の別のアカウントによってすでに使用されている場合は、vdsm パッケージおよび qemu-kvm-rhev パッケージのインストール時に競合が発生します。